"The Threat Library is a knowledge base of techniques used by the enemies of anarchists and other rebels - a breakdown and classification of actions that can be used against us. Ultimately, the Threat Library is a tool to help you to think through what mitigations should be enacted in a specific project, and a way to navigate resources that go into more depth on these subjects. In other words, it helps you to arrive at appropriate Operational Security (OpSec) for your threat model."

Layout by the Counter-Surveillance Resource Center (csrc.link)

Threat Library

Counter-Surveillance Resource Center

csrc.link/threat-library

2023-08-05

Contents

8.3.2 Time Period

The time period consists of a mandatory start year, and an optional end year:

- If the actions targeted by the operation are known, the start year should be when the earliest action took place. Otherwise, it should be the first year when we can be certain the operation was active.
- If the operation was followed by a trial, the end year should be when the sentences against the comrades targeted by the operation were finalized. Otherwise, it should be the last year when we know the operation was active. If an operation or the trial following it are still ongoing, no end year should be listed.

  Example: the **Panico (p. 61)** operation in Italy became known with house raids in 2017, but targeted two actions that took place in 2016 and 2017. It was followed by a trial in 2019 and an final appeal in 2021. In the Threat Library, its start year is set to 2016 and its end year to 2021.

8.3.3 Description

The operation description presents the context of the operation, for readers who may have never heard of it before.

The first paragraph of the description should generally give brief summaries of:

- the initial event through which the operation became known (often arrests or a house raid)
- the actions targeted by the operation
- the accusations or charges against the people that were arrested as part of the operation

Additional paragraphs can provide more context if needed. If the operation was followed by a trial, a last paragraph should give a brief summary of the sentences that resulted from it.

8.3.4 Techniques

Each operation includes a table of techniques that were used in the operation, with brief descriptions of how they were used. A technique should be included in this table if it provides actionable knowledge to our readers, i.e. if comrades can read its description and use what they read to adapt their threat model or behaviour.

When possible, all information in a technique's description should be supported by a reference, generally a link to an online publication made by comrades. If information comes from a non-public source (such as your own knowledge), of course it's fine to not include a reference.

8 Contribute to the Threat Library

8.1 Contact

Is there a **technique (p. 17)**, **mitigation (p. 46)**, or **repressive operation (p. 59)** that you think is missing? Would you like to edit one that is currently listed? To contribute to the Threat Library, whether through additions, improvements, criticism or feedback, get in touch with us:

csrc@riseup.net [1]

8.2 Translations

To coordinate translations across the CSRC project, we use the collaborative localization platform Weblate. To translate the Threat Library to a new language or improve an existing translation, register an account on the Weblate instance used by CSRC[2] (you'll need an email address) and follow the instructions[3]. All languages are welcome.

8.3 Repressive operations

To contribute a new repressive operation to the Threat Library, please provide us with:

- a name
- a time period
- a brief description
- a summary of techniques that were used in the operation

8.3.1 Name

The name of the operation should be the name that has been most widely used by comrades in publications or discussions.

> Example: the case of the anarchists arrested in a park in Hamburg, Germany in 2019 has been widely reported in German as the "Parkbank 3"; the English name of the corresponding Threat Library operation is "The three from the park bench".

If no such name exists, the name should be derived from the most significant elements of the case.

[1] PGP: https://csrc.link/csrc.asc
[2] https://weblate.anarchyplanet.org
[3] https://weblate.anarchyplanet.org/projects/csrc/#information

1 About the Threat Library

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

1.1 What is Threat Modeling?

Threat modeling is a conceptual exercise that aims to help you identify threats, how you might be vulnerable to these threats, and what mitigations can sufficiently protect you without obstructing you from accomplishing your goals. This exercise is best done in the context of a specific project, collaboratively with the comrades you'll be working with, in **outdoor and device-free conversations (p. 54)**.

1.2 What is the Threat Library?

A precondition to threat modeling is understanding enemy behaviour. The Threat Library is a knowledge base of **techniques (p. 17)** used by the enemies of anarchists and other rebels - a breakdown and classification of actions that can be used against us. These techniques are organized into a set of **tactics (p. 15)** to help provide context for the technique.

Tactics represent the '*why*' of a technique, the reason for performing an action. A state enemy has three distinct but potentially overlapping tactics:

- Deterrence ('The enemy is trying to prevent you from achieving your objectives.')
- Incrimination ('The enemy is trying to link you to an illegal activity.')
- Arrest ('The enemy is trying to arrest you.')

Techniques represent '*how*' an enemy achieves a tactical objective by performing an action. For example, an enemy may install covert surveillance devices that can be used later for incrimination.

These techniques are linked to specific **repressive operations (p. 59)** that are known to have used them, which also allows insight into the context of different **countries (p. 66)**. Each technique is paired with potential **mitigations (p. 46)** that you can take, which can help to render the technique ineffective.

Ultimately, the Threat Library is a tool to help you to think through what mitigations should be enacted in a specific project, and a way to navigate resources that go into more depth on these subjects. In other words, it helps you to arrive at appropriate Operational Security[2] (OpSec) for your threat model.

Centrally located information about repressive techniques can have an immobilizing effect; by collecting every possible approach available to our adversaries, it can make the police seem all powerful. The intent of the Threat Library is neither to minimize nor exaggerate the repressive capacities of the State, but rather to understand its options, and more importantly, how these options are used in different contexts (through the **repressive operations (p. 59)**).

[1] https://csrc.link/#keimeno-ton-prophulakismenon-tes-neas-philadelpheias
[2] https://csrc.link/read/csrc-bulletin-1-en.html#header-a-base-to-stand-on-distinguishing-opsec-and-security-culture

It is worth emphasizing that the vast majority of anarchist attacks are not successfully prosecuted. Operational Security can stymie the progress of investigations, even when they have lots of resources, or in contexts with a relatively small anarchist space. For example, frustrated investigators in Bremen (Germany)[1] and Grenoble (France)[2] have spoken to the media about their failure to repress any of the arsons that have taken place in both locations over the years, which they attribute to the **mitigations (p. 46)** that the arsonists took.

1.3 Limitations of the Threat Library

The Threat Library is by design a very technical approach to anti-repression - threat modeling occurs on the level of actions and so does not attempt to contribute to the social question; how to evade the enclosure repression seeks, how to intervene in social tensions, etc. Although we must develop the means to enable us to minimize the likelihood of imprisonment, struggles for freedom are not primarily a technical affair but a social one.

Such a technical approach should also not make us overlook the psychological and emotional aspects of our struggles and our lives. As much as possible, we advise our readers to take time before, during and after an action to discuss with all comrades involved and make sure that everyone's emotional needs are taken into account.

Although the Threat Library tries to cover the dangers that anarchists may encounter in their struggles as comprehensively as possible, it is meant to grow over time with contributions, and will never be complete. This is especially true since our enemies might develop with new and unanticipated techniques. Thus, to avoid getting a sense of false safety from using the Threat Library, we encourage our readers to use other sources of knowledge, to stay critical and to always take into account their personal contexts when making important decisions.

[1] https://csrc.link/#die-sind-doch-nicht-dumm-die-nehmen-ihr-handy-naturlich-nicht-mit

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

7.8 United States

Repressive operations:

Repression of the first Jane's Revenge arson (p. 65)

7 Countries

7.1 Belarus

Repressive operations:

7.2 Chile

Repressive operations:

7.3 France

Repressive operations:

7.4 Germany

Repressive operations:

7.5 Greece

Repressive operations:

7.6 Italy

Repressive operations:

7.7 Russia

Repressive operations:

2 Tutorial: Suggested Use of the Threat Library with Attack Trees

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

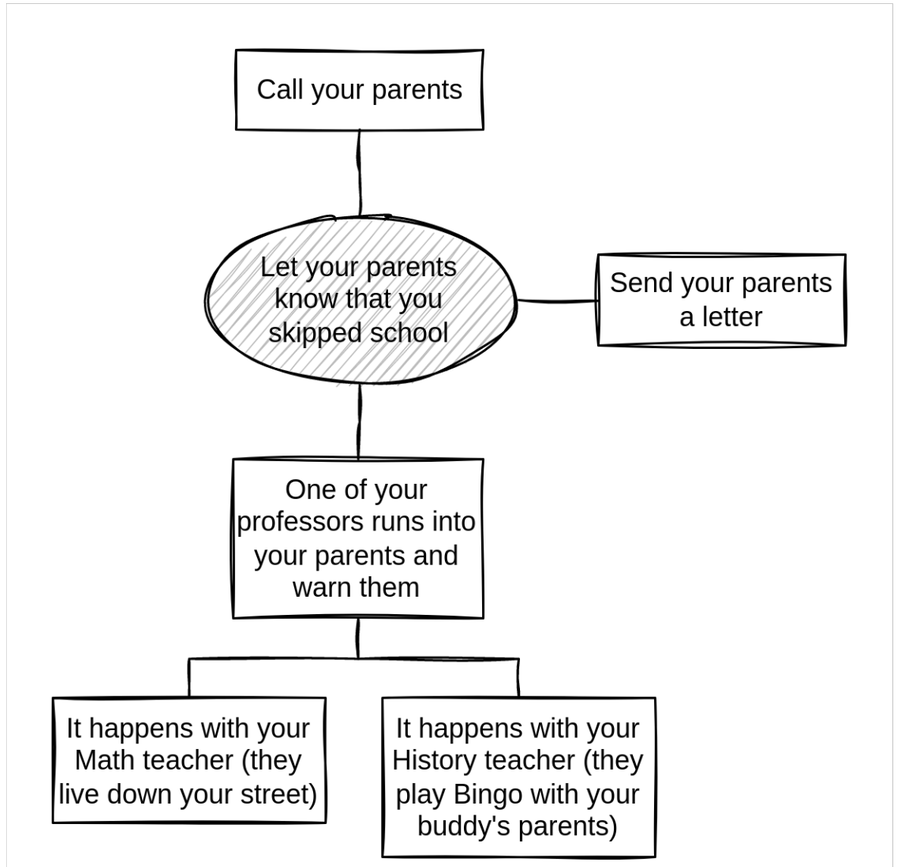
2.1 A Simple Example: Skipping a School Day

Let's start with a simple example before we think about a real one. You're a kid in school and you and your buddy want to skip a school day but don't want your parents to know. The adversary is the school system.

You start by drawing the root node: it represents the goal of the adversary. The goal in this example is letting your parents know that you skipped. The school could call your parents or send them a letter. Or one of your professors could run into your respective parents and warn them - this could happen with your Math teacher who lives down your street, or your History teacher who plays Bingo with your buddy's parents every week-end. Child nodes are different ways of achieving a parent node, and you grow the tree by identifying these children.

Notice how child nodes are conditions, and at least one of them must be satisfied to make the direct parent node true. If you can trace a path where each node is satisfied from the farthest node on a branch to the root, the attack is complete.

So together with your buddy, you decide to skip a day when you don't have either Math or History. The night before skipping, you'll cut your parents phone lines (blame it on the mice), and intercept their mail in the following days. You're happy to have come up with a great plan.



"Skipping school" attack tree

2.2 A Real Example: A Riot in a Big City in the United States

Let's say that you are preparing for a riot in a big city in the United States with some comrades. You want to do some damage, but don't want to get caught… You turn to the Threat Library for help. You print this zine and gather with your comrades **outdoors and without electronic devices (p. 54)**.

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

2.2.1 Draw the Attack Tree

In this example, the adversary is the State and its cops, and their goal is to obtain enough evidence of your participation in riots to convince a judge to convict you. You draw the root node.

You then add the immediate child nodes, next to the root. At this stage, an exhaustive list of possibilities is better than a partial list of feasibilities. The tree can grow in all four directions, to make it more compact.

6.14 Repression of Lafarge factory sabotage

Countries: **France (p. 66)**
Date: 2022 - ?
Techniques used:
Forensics > DNA (p. 24)
House raid (p. 30)
Mass surveillance > Video surveillance (p. 35)

On June 5th, 2023, about fifteen people were raided and arrested in France, accused of participating to the December 2022 sabotage of a factory operated by the French industrial company Lafarge[1]. The sabotage, which happened during the day and involved between 100 and 200 activists[2], caused around 6 million euros of damage.

On June 20th, 2023, about eighteen additional people were raided and arrested in France, some of them in connection with the Lafarge sabotage[3].

6.15 Repression of the first Jane's Revenge arson

Countries: **United States (p. 67)**
Date: 2022 - ?
Techniques used:
Forensics > DNA (p. 24)
Forensics > Handwriting analysis (p. 28)
Mass surveillance > Video surveillance (p. 35)
Physical surveillance > Covert (p. 38)

In March 2023, a comrade was arrested[4] and accused of a May 2022 arson against the headquarters of an anti-abortion group[5]. The arson was the first of 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 from 1969 to 1973 in the United States).

6.16 Berlin 2023 railway conspiracy case

Countries: **Germany (p. 66)**
Date: 2023 - ?
Techniques used:
Covert surveillance devices > Aerial (p. 19)

In February 2023, a few minutes after midnight during a routine surveillance flight, the helicopter of the German federal police identified two comrades on railway tracks close to Berlin[6]. Three police cars were dispatched to the location and the people were arrested, suspected of an arson attempt against the railway infrastructure.

[1] https://sansnom.noblogs.org/archives/16978
[2] https://reporterre.net/Sabotage-de-l-usine-Lafarge-deux-premieres-mises-en-examen
[3] https://reporterre.net/Nouvelle-serie-de-perquisitions-a-la-zad-et-en-France
[4] https://www.washingtontimes.com/news/2023/mar/28/hridindu-sankar-roychowdhury-arrested-charged-fire
[5] https://janesrevenge.noblogs.org/2022/05/08/first-communique
[6] https://csrc.link/#wir-haben-eine-verabredung

In April 2022[1] and October 2022[2] several apartments and cellars, a print shop and a library were raided by cops as part of an investigation against the alleged editors of the German anarchist newspaper *Zündlumpen* published from 2019 to 2021.

During the April 2022 raid on the print shop, cops seized thousands of books, zines and newspapers, as well as all printing equipment and materials, seemingly in an attempt to disrupt the printing capacity of local anarchists.

6.12 The three from the park bench

Countries: **Germany (p. 66)**
Date: 2019 - ?
Techniques used:
Mass surveillance > Video surveillance (p. 35)
Physical surveillance > Covert (p. 38)

In 2019, three comrades were arrested while sitting on a park bench late at night in Hamburg[3], accused of carrying incendiary devices[4] and planning to commit the arson of a specific building whose address was written on a piece of paper found on them. Two of the arrested comrades were being tailed by cops for a few hours before the arrest took place.

In a 2020 trial, the comrades were sentenced to between 19 and 22 months of prison[5]. The sentences were confirmed in a 2022 appeal[6].

6.13 Belarusian anarcho-partisans

Countries: **Belarus (p. 66)**
Date: 2020 - 2021
Techniques used:
Extra-legal violence (p. 23)
Mass surveillance > Civilian snitches (p. 34)

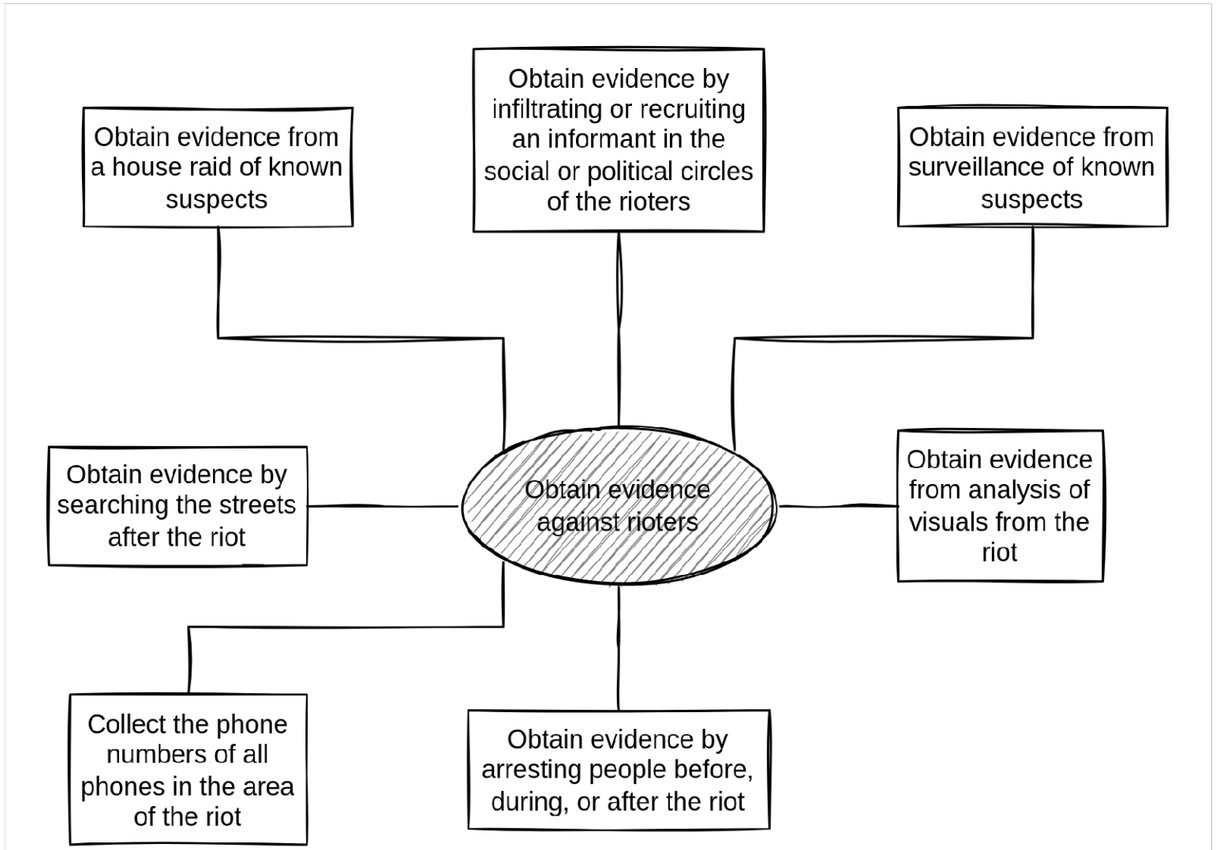
In 2020, four anarchists set fire to police buildings and to vehicles on the parking lot of a prosecutor's office[7]. Soon after, they were arrested by border guards while attempting to cross the Belarus-Ukraine border.

In the first days of their detention, the anarchists were tortured[8]. Eventually, all four took responsibility for carrying out the actions of which they were accused.

After a trial in 2021 they were sentenced to prison, with sentences ranging from 18 to 20 years[9].

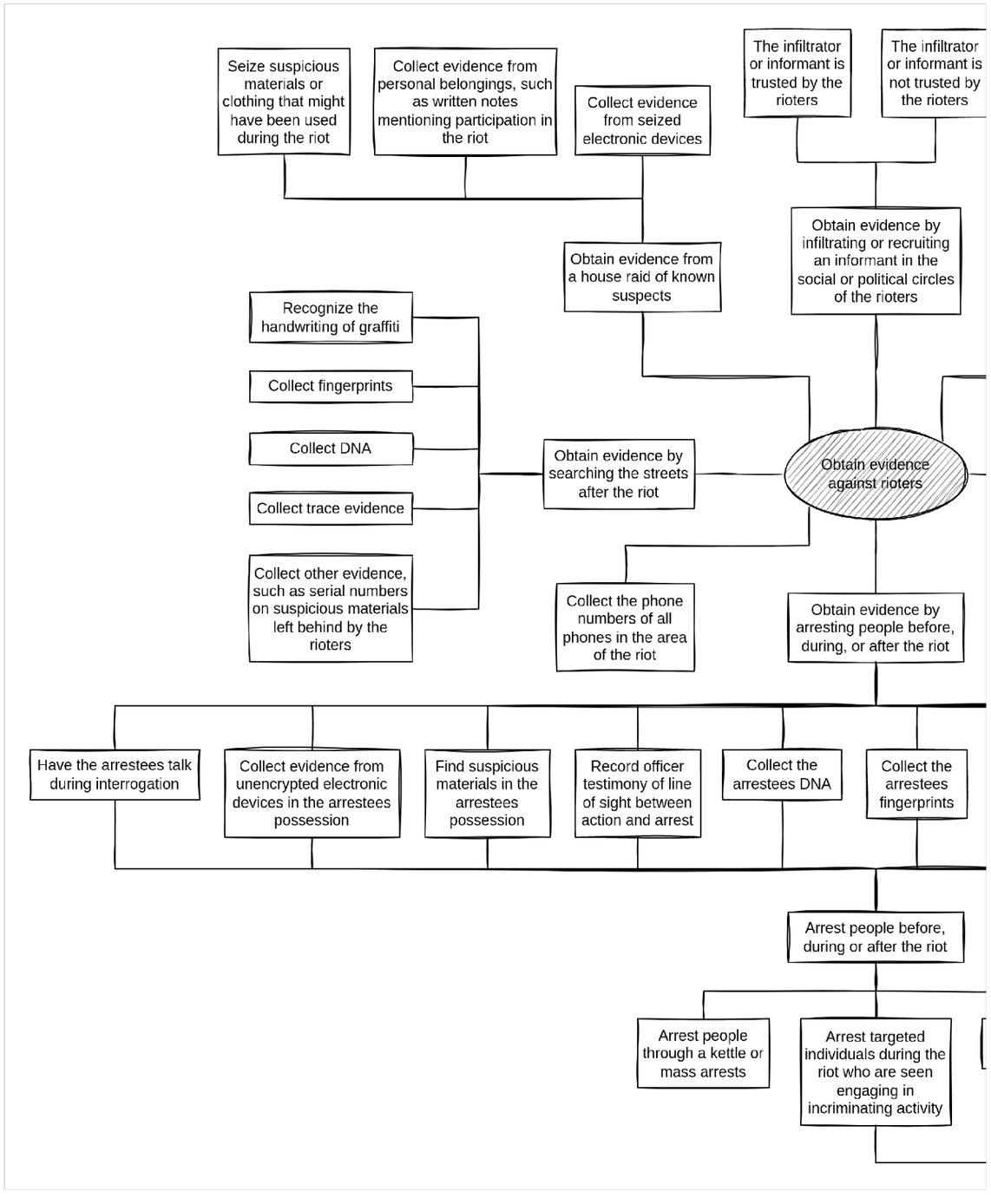
[1] https://zuendlappen.noblogs.org/post/2022/05/07/muenchen-ueber-razzien-und-ein-%c2%a7129-verfahren-gegen-anarchistinnen-und-den-raub-einer-druckerei
[2] https://de.indymedia.org/node/234616
[3] https://csrc.link/#surveillance-and-other-nuisances.html
[4] https://parkbanksolidarity.blackblogs.org/509
[5] https://parkbanksolidarity.blackblogs.org/end-of-the-trial-two-imprisoned-comrades-on-the-streets-again
[6] 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
[7] https://pramen.io/en/2020/11/open-letter-in-support-of-belarus-anarchist-revolutionaries
[8] https://pramen.io/en/2021/12/blood-on-your-hands-regarding-information-about-torture-of-anarcho-partisans
[9] https://abc-belarus.org/en/2021/12/22/18-to-20-years-imprisonment-for-belarusian-anarcho-partisans

"Riot" attack tree (root node)



"Riot" attack tree (first nodes)

You use the Threat Library to help expand the tree - reading about techniques enables you to better understand all of the options available to your adversary. Creating attack trees requires a certain mind-set and takes practice. The tree is done when no additional substeps are needed to complete an action, and all attacks are represented that you can think of.



"Riot" attack tree (complete, left part)

Date: 2017 - 2020
Techniques used:

Extra-legal violence (p. 23)

At the end of 2017 and the beginning of 2018, about ten anarchists and antifascists were arrested in Penza and Saint Petersburg[1], accused of being part of an underground organization called 'Network' that was planning terrorist attacks in anticipation of Russia's 2018 presidential elections and the FIFA World Cup[2]. Some of them were also accused of attempting to sell large quantities of drugs. Most of them were tortured in the early stages of their detention by Russia's Federal Security Service (FSB).

According to investigation files and other information, the initial arrests that started the investigation occurred because of the involvement of most of the defendants from Penza in the drug business[3].

After two trials in 2020, seven alleged members of the 'Network' organization in Penza were sentenced to prison with sentences ranging from 6 to 18 years[4], and two alleged members in Saint Petersburg were sentenced to 5 and a half and 7 years in prison respectively[5].

6.10 2019–2020 case against Mónica and Francesco

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

Forensics > DNA (p. 24)
Forensics > Facial recognition (p. 27)
Forensics > Handwriting analysis (p. 28)
Mass surveillance > Civilian snitches (p. 34)
Mass surveillance > Video surveillance (p. 35)

In 2020, anarchists Mónica Caballero and Francisco Solar were arrested in Chile, accused of sending parcel bombs to a police station and an ex-Minister of Interior in 2019, and placing bombs in a park in an attempt to harm cops in 2020[6]. Both were charged with attempted murder.

6.11 Repression against Zündlumpen

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

Forensics > DNA (p. 24)
Targeted digital surveillance > Authentication bypass (p. 40)
Targeted digital surveillance > Service provider collaboration (p. 44)

[1] https://web.archive.org/web/20210724133854/https://a2day.net/network-underground
[2] https://www.amnesty.org/en/wp-content/uploads/2021/05/EUR4696252018ENGLISH.pdf
[3] https://web.archive.org/web/20210724130151/https://a2day.net/the-dark-side-of-the-network-case
[4] https://therussianreader.com/2020/02/10/network-penza-sentences
[5] https://anarchistsworldwide.noblogs.org/post/2020/06/23/saint-petersburg-russia-we-can-dance-if-we-want-to-sentencing-of-the-network-case-defendants
[6] https://csrc.link/#about-orwell-and-the-case-of-monica-and-francisco

In 2021, the comrade accused of the ATM arson was sentenced to 5 years in prison while all comrades were acquitted for the parcel bombs (for lack of evidence[1]), although one of them had spent two and a half years in prison before being acquitted.

6.7 Renata

Countries: **Italy (p. 66)**
Date: 2016 - 2019
Techniques used:
Covert surveillance devices > Audio (p. 19)
Extra-legal violence (p. 23)
Forensics > DNA (p. 24)
House raid (p. 30)

In February 2019, 50 house raids took place, mainly in Trentino, and seven anarchist comrades were arrested as part of an operation dubbed 'Renata'[2]. Other comrades were arrested in May 2019. Arrested comrades were accused of participating in an 'associazione sovversiva' ('criminal association') and carrying out various arsons and explosive attacks from 2016 to 2018, including an explosive attack against the headquarters of 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 9 months to two years and 6 months.

6.8 Bialystok

Countries: **Italy (p. 66)**
Date: 2017 - 2022
Techniques used:
Forensics > Gait recognition (p. 28)
International cooperation (p. 33)

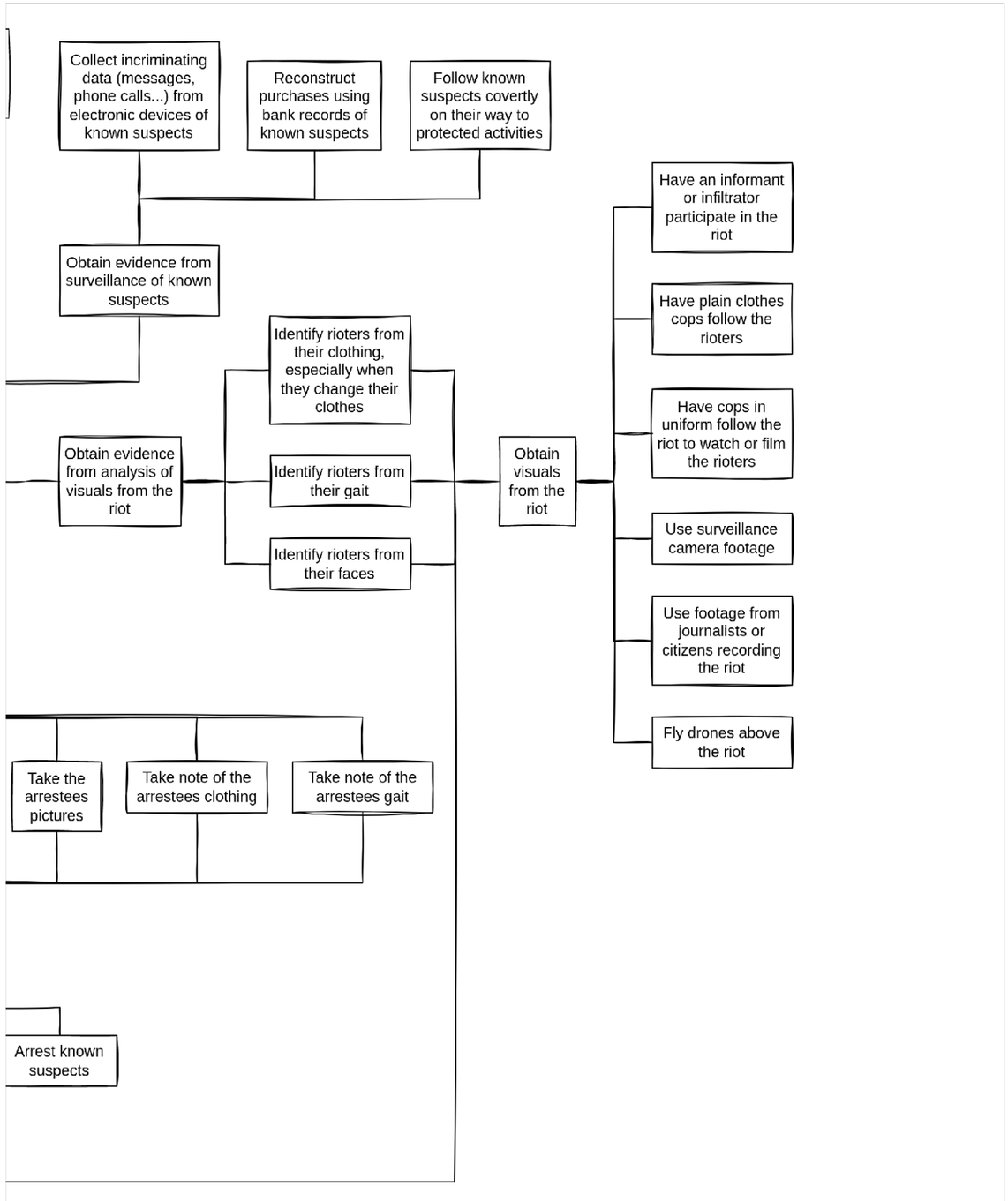
In June 2020, house raids took place in the 'Bencivenga Occupato' squat in Rome and other places, and seven anarchist comrades were arrested in Italy, Spain and France as part of an operation dubbed 'Bialystok'[3]. They were accused of participating in an 'associazione sovversiva' (criminal association) and of various minor offenses related to initiatives in solidarity with comrades accused in the **Panico operation (p. 61)**. Two of them were respectively accused of carrying out an explosive attack against a police station in 2017, and an arson attack against cars linked to ENI (an Italian multinational oil and gas company) in 2019.

After a trial in 2022, some comrades were acquitted and some were sentenced to prison, with sentences ranging from 45 days to one year[4].

6.9 Network

Countries: **Russia (p. 66)**

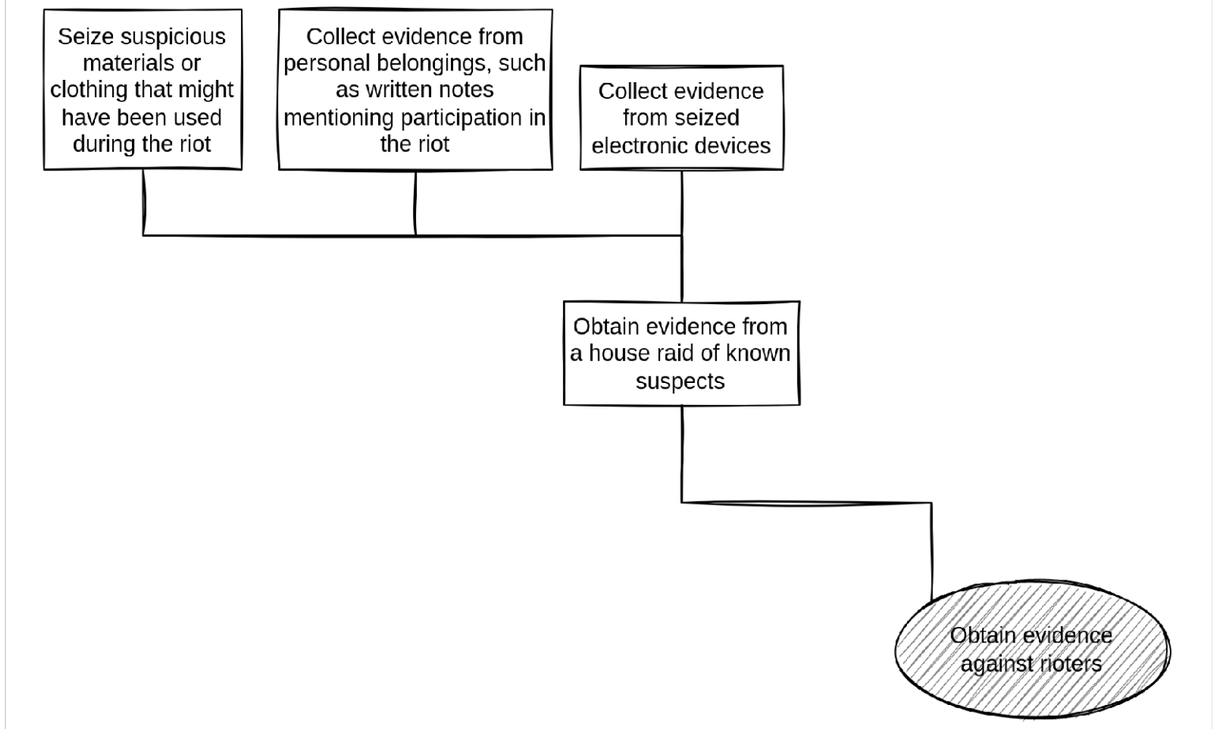
[1]https://actforfree.noblogs.org/post/2021/10/06/italy-op-prometeo-beppe-robert-and-nat-acquitted
[2]https://malacoda.noblogs.org/anarchici-imprigionati
[3]https://malacoda.noblogs.org/anarchici-imprigionati
[4]https://actforfree.noblogs.org/post/2022/10/31/italy-the-first-grade-sentence-concerning-the-trial-following-theoperation-bialystok



"Riot" attack tree (complete, right part)

2.2.2 For Each Branch of the Tree...

For each branch of the tree, you try to match nodes with techniques from the Threat Library, then decide which mitigations to implement, and how they will be implemented. You start with the branch "Obtain evidence from a house raid of known suspects".



"Riot" attack tree (house raid branch)

Identify Techniques

For this branch, you identify the following matches:

- "Obtain evidence from a house raid of known suspects" matches **House raid (p. 30)**
- "Collect evidence from seized electronic devices" matches **Targeted digital surveillance: Physical access (p. ??)** because they would access your electronic devices and **Targeted digital surveillance: Authentication bypass (p. ??)** if they try to guess your passwords or break your encryption
- The other nodes don't match anything, they're just part of the house raid

are burning') which contained information on 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 using a nautical flare during a gathering in front of the prison where the other comrades were kept[1]. In November 2019 another comrade, Peppe, was arrested and accused of sending a parcel bomb in 2016 to a company which participated in the management of a migrant detention center[2]. In July 2020 Carla, who was on the run since the first arrests, was arrested in France and extradited to Italy.

After a trial in 2021[3]-2023, several comrades were sentenced to prison, with sentences ranging from 1 year to 4 years and 2 months[4].

6.5 Panico

Countries: **Italy (p. 66)**
Date: 2016 - 2023
Techniques used:
Forensics > DNA (p. 24)

In 2017, house raids took place in Florence and several anarchist comrades were arrested as part of an operation dubbed 'Panico'[5]. Up to 35 comrades will be accused during this operation[6]. Some comrades were accused of carrying out an explosive attack against a fascist bookstore in 2017 and an arson attack against a police station in 2016. Other comrades were accused of various other actions.

After a trial in 2019, an appeal in 2021[7] and a ruling by the Court of cassation in 2023[8], two comrades were sentenced to 8 years in prison, while others were sentenced to prison sentences ranging from a few months to three years and a half.

6.6 Prometeo

Countries: **Italy (p. 66)**
Date: 2016 - 2021
Techniques used:
Forensics > DNA (p. 24)
Mass surveillance > Video surveillance (p. 35)
Targeted digital surveillance > Service provider collaboration (p. 44)

In 2019, three anarchist comrades were arrested as part of an operation dubbed 'Prometeo'[9]. They were accused of sending parcel bombs to prosecutors and a prison administration director in 2017. One of the comrades was also accused of carrying out an arson against an ATM in 2016.

[1] https://macerie.org/index.php/2019/05/23/incendio-al-carcere-boba-arrestato
[2] https://roundrobin.info/2019/12/verona-una-perquisizione-e-un-arresto
[3] https://roundrobin.info/2021/10/op-scintilla-inizio-del-processo-e-volantino
[4] https://ilrovescio.info/2023/01/18/torino-sentenza-di-primo-grado-del-processo-scintilla
[5] https://malacoda.noblogs.org/anarchici-imprigionati
[6] https://insuscettibilediravvedimento.noblogs.org/post/2019/07/18/it-en-italia-richieste-di-condanna-al-processo-per-loperazione-panico
[7] https://ilrovescio.info/2021/05/05/sentenza-dappello-processo-panico
[8] https://lanemesi.noblogs.org/post/2023/07/15/sentenza-di-cassazione-del-processo-panico-14-luglio-2023
[9] https://malacoda.noblogs.org/anarchici-imprigionati

In 2008, six comrades were arrested and accused of preparing acts of terrorism, possession or manufacture of explosive or incendiary devices, and arson or attempted arson - including an attempted arson on an electrical cabinet in 2006 and an attempted arson on a police tow truck in 2007[1]. This operation was documented by comrades in a series of zines titled 'Mauvaises intentions[2]'.

After a trial in 2012, five comrades were sentenced to prison, with sentences ranging from one to three years in prison[3].

6.3 Nea Filadelphia case

Countries: **Greece (p. 66)**
Date: 2011 - 2016
Techniques used:
Forensics > DNA (p. 24)
Physical surveillance > Covert (p. 38)

In 2013, several comrades were arrested in Nea Filadelphia, a suburb of Athens[4]. Four of them were accused of having carried out bank robberies[5] that took place in 2011[6] and 2013[7].

After a trial in 2014, two comrades were sentenced to 16 years in prison[8]. After a different trial in 2014[9] and an appeal in 2016[10] the two other were sentenced to 9 and 11 years in prison respectively.

6.4 Scintilla

Countries: **Italy (p. 66)**
Date: 2015 - 2023
Techniques used:
Covert surveillance devices > Audio (p. 19)
Door knocks (p. 22)
Forensics > DNA (p. 24)
Forensics > Gait recognition (p. 28)
International cooperation (p. 33)

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 dubbed 'Scintilla'[11]. Some of them were accused of carrying out several arson and explosive attacks between 2015 and 2018 against migrant detention centers and other targets[12]. Some of them were accused of publishing a zine called 'I cieli bruciano' ('The skies

[1] https://infokiosques.net/spip.php?article597
[2] https://csrc.link/#mauvaises-intentions
[3] https://juralib.noblogs.org/2012/06/25/mauvaises-intentions-paris-rendu-du-proces-antiterroriste-de-mai-2012
[4] https://web.archive.org/web/20201027031238/http://actforfree.nostate.net/?p=15472
[5] https://machorka.espivblogs.net/2013/11/06/concerning-the-arrests-of-comrades-in-nea-philadelphia-on-304-athens
[6] https://abcsolidaritycell.espivblogs.net/archives/130
[7] https://machorka.espivblogs.net/2016/02/26/appeal-trial-for-the-double-bank-robbery-velvendo-case-greece
[8] https://machorka.espivblogs.net/2014/10/02/announcement-of-sentences-in-the-velvedo-double-robbery-case-11014-athens
[9] https://abcsolidaritycell.espivblogs.net/archives/tag/g-naxakis
[10] https://anarhija.info/library/grecia-l-ultimo-aggiornamento-sul-processo-d-appello-per-rapina-a-pirgetos-con-anarchic-en
[11] https://malacoda.noblogs.org/anarchici-imprigionati
[12] https://attaque.noblogs.org/post/2020/08/06/saint-etienne-arrestation-de-carla-recherchee-dans-le-cadre-de-loperation-scintilla

Decide Which Mitigations to Implement

Then you look at the mitigations the Threat Library suggests for these techniques, and you choose which ones you want to implement. It's best to start with techniques that were matched closer to the root node, and then work you way up the branch. You decide to implement:

- For "House raid", **Preparing for repression (p. 56)**, **Preparing for house raids (p. 55)** and **Stash spot or safe house (p. 57)**. You don't want to implement **Clandestinity (p. 49)** because you don't want to take that path.
- For the two "Targeted digital surveillance" techniques, **Digital best practices (p. 51)** is the only mitigation that makes sense in your context.

Decide How Mitigations Will Be Implemented

And finally, you decide how to implement the mitigations you listed. Reading their entries on the Threat Library can give you some ideas. It's useful to think about how *likely* and *impactful* the corresponding techniques would be if they were used, because then you can know how much energy to put into the mitigations. You decide on the following implementations:

- "Preparing for repression": since you and your comrades all live in the same place, the risk is that you all get arrested after a house raid. You will make sure other comrades know how to support you if this happens.
- "Preparing for house raids": you decide to keep the hammers on the tool shelf, but you will stop storing the fireworks under the beds.
- "Stash spot or safe house": you decide to install a small water-proof box buried in a nearby forest to store the fireworks. When one of you accesses it, they need to wear gloves and make sure there's no one around.
- "Digital best practices": your devices are already encrypted, and you don't use them to talk about the riots anyway. You need to research if a phone's encryption works when it's turned on and locked as you're not sure about that. Then you move to the next branch, until the whole tree is covered.

2.2.3 Perform an Action Review

After the riot, you and your comrades take some time for an action review: in **outdoor and device-free conversations (p. 54)** you discuss what went well and what went wrong, and if there is room for improvement in how you implemented the mitigations.

2.3 Additional Tips On Using the Threat Library

The home page[1] of the Threat Library provides an overview of all the tactics and techniques, as well as buttons that allow you to hide or show specific techniques. For example, this can be used to only show techniques that fit in your threat model, in order to better visualize the remaining techniques that might apply to your context. If you follow our suggested process above and draw your own attack trees, the overview can help you to think of any relevant techniques that are missing from your tree.

[1] https://csrc.link/threat-library

If you wish, you can **contribute (p. ??)** to the Threat Library. Possible contributions include, but are not limited to:

- writing about a repressive operation that isn't already covered
- suggesting the addition of new techniques or mitigations that you think should be covered
- any suggested edits on the text itself
- attack trees for different types of projects

6 Repressive operations

6.1 Scripta Manent

Countries: **Italy (p. 66)**
Date: 2003 - 2023
Techniques used:
Forensics > DNA (p. 24)
Forensics > Handwriting analysis (p. 28)
Forensics > Linguistics (p. 29)
House raid (p. 30)
Targeted digital surveillance > Malware (p. 42)

In 2016, 32 house raids took place in various regions of Italy and several anarchist comrades were arrested as part of an operation dubbed 'Scripta Manent'[1]. Up to 22 comrades will be under investigation during this operation. They were accused of forming or participating in an 'associazione sovversiva con finalità di terrorismo' (criminal association for the purpose of terrorism), referring to attacks claimed by the 'Federazione Anarchica Informale' (FAI, Informal Anarchist Federation) since 2003[2]. 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 managing radical websites.

The contents of several previous investigations were merged into Scripta Manent.

A first trial took place in 2017-2019, an appeal in 2020, and two other rulings in 2022[3] and 2023[4]. 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.

6.2 Mauvaises intentions

Countries: **France (p. 66)**
Date: 2006 - 2012
Techniques used:
Forensics > DNA (p. 24)
Network mapping (p. 37)
Physical surveillance > Overt (p. 39)
Targeted digital surveillance > Service provider collaboration (p. 44)

[1] https://malacoda.noblogs.org/anarchici-imprigionati
[2] https://tracesoffire.espivblogs.net/2016/09/13/italy-naples-september-carrion-operation-scripta-manent
[3] https://actforfree.noblogs.org/post/2022/07/10/italy-cassation-of-the-scripta-manent-trial
[4] 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

Covert surveillance devices > Aerial (p. 19)
Covert surveillance devices > Video (p. 21)
Physical surveillance > Covert (p. 38)

There are three types of surveillance detection: passive, active, and counter-surveillance. Passive surveillance detection involves developing an awareness for indications of surveillance, without deviating from your normal routines whatsoever. Active surveillance detection involves the use of preplanned maneuvers intended to reveal a physical surveillance effort - doing something above and beyond your normal routine. Counter-surveillance is a form of active surveillance detection that involves a third-party (not the target of surveillance) watching for signs and/or details of a surveillance effort along a preplanned route.

Avoid blatantly acknowledging or shaking surveillance if you notice something – this will draw more attention, and invite the enemy to adapt.

See the related mitigation **Anti-surveillance (p. 46)**.

5.28 Tamper-evident preparation

Techniques addressed by this mitigation:

Targeted digital surveillance > Authentication bypass (p. 40)
Targeted digital surveillance > Physical access (p. 43)

Tamper-evident preparation will make it possible to discern when something has been **physically accessed (p. ??)** - it's not possible to prevent a powerful enemy from obtaining physical access to your computer when you are away, but it should be possible to be able to detect when they do.

This spans from simple methods, like painting nail polish over the screws on your laptop to identify any attempts to open it, all the way to a highly customized laptop that will brick itself if opened under certain conditions.

5.29 Transportation by bike

Techniques addressed by this mitigation:

Covert surveillance devices > Location (p. 20)
Mass surveillance > Video surveillance (p. 35)
Physical surveillance > Covert (p. 38)

Transportation by bike has several advantages for **surveillance detection (p. 57)** and **anti-surveillance (p. 46)**. It is more difficult for a surveillance effort to tail a bike than a car or someone on foot, especially without being detected. There are also far fewer locations to hide a **tracking device (p. ??)** on a bike than on/in a car.

Unlike a car, **searching (p. 48)** a bike allows us to say whether a tracking device is present or not with a high degree of confidence. Additionally, bikes are more difficult to identify than cars by **video surveillance (p. ??)** - the make and model can be obscured, and there is no license plate.

In a six month-long **physical surveillance (p. 38)** operation against a comrade in France, the police regularly lost track of him while he was biking.

3 Tactics

3.1 Deterrence

Uses techniques:

Door knocks (p. 22)
Extra-legal violence (p. 23)
Increased police presence (p. 31)
Mass surveillance (p. 34)

In some contexts, in addition to or instead of other tactics authorities may attempt to prevent or discourage troublemakers from making trouble in the first place. This can be because they are unable or unwilling to incriminate or arrest the troublemakers, or because they believe that discouraging them is a good complementary strategy. We call this process *deterrence*.

3.2 Incrimination

Uses techniques:

Canine trackers (p. 17)
Covert house search (p. 18)
Covert surveillance devices (p. 18)
Door knocks (p. 22)
Evidence fabrication (p. 22)
Extra-legal violence (p. 23)
Forensics (p. 23)
House raid (p. 30)
Infiltrators (p. 31)
Informants (p. 32)
International cooperation (p. 33)
Interrogation techniques (p. 33)
Mass surveillance (p. 34)
Network mapping (p. 37)
Parallel construction (p. 38)
Physical surveillance (p. 38)
Targeted ID checks (p. 40)
Targeted digital surveillance (p. 40)

In many countries, in order to arrest troublemakers and remove them from society - usually through imprisonment - authorities must be able to convince a judge of their illicit activities. To this end, the relevant authorities will attempt to find evidence of these activites. Depending on the context and people involved, judges may be more or less easy to convince. We call this process *incrimination*.

3.3 Arrest

Uses techniques:

Alarm systems (p. 17)

Canine trackers (p. 17)
Guards (p. 30)
House raid (p. 30)
Increased police presence (p. 31)
International cooperation (p. 33)
Targeted ID checks (p. 40)

In order to remove troublemakers from society - usually through imprisonment - authorities must be able to locate them physically and arrest them.

5.25 Reconnaissance

Techniques addressed by this mitigation:

Alarm systems (p. 17)
Mass surveillance > Routine police surveillance (p. 35)
Mass surveillance > Video surveillance (p. 35)

Reconnaissance precedes **action planning (p. 49)** - it involves the purposeful collection of information about a target, which can be done digitally or physically. Taking repressive techniques into account during the reconnaissance phase will enable you to leave a smaller trace.

For example, the path to be taken to and from the action site can be selected on the basis of minimal **surveillance camera (p. ??)** coverage, and an appropriate clothing change location can be selected with similar considerations. The corporation website listing CEO names can be visited exclusively by using **digital best practices (p. 51)**. Physical reconnaissance should be paired with **anonymous dress (p. 46)** due to the possibility of being witnessed or recorded on site, and should be considered a 'protected activity' which is preceeded by **anti-surveillance (p. 46)**.

5.26 Stash spot or safe house

Techniques addressed by this mitigation:

Covert house search (p. 18)
Covert surveillance devices > Video (p. 21)
Forensics > Ballistics (p. 24)
Forensics > Trace evidence (p. 29)
House raid (p. 30)

There are two approaches to storing incriminating action materials; stash spots and safe houses. A stash spot is a location where action materials can be hidden, and won't be stumbled upon - outdoor locations are better for minimizing **DNA (p. 50)** traces which will accumulate in the places we frequent. A safe house is an apartment that is unknown to law enforcement so is unlikely to be subject to a house raid – but if they do become aware of the location they could more easily collect the DNA of people who visit due to it being indoors.

To find stash spots some creativity will be needed, but some options are in a forest far away from a trail where you won't be witnessed by hikers, or in an abandoned building tucked away somewhere. A benefit of this approach is that its location can be changed frequently with minimal effort.

To establish a safe house, sometimes an apartment or garage is rented for this dedicated purpose with a **fake ID (p. 52)** and cash. A less involved approach is to use the living space of someone who is trusted and willing to take the risk this complicity entails, but is far enough removed from networks which are subject to surveillance.

Accessing a stash spot or a safe house should be considered a 'protected activity', proceeded by **anti-surveillance (p. 46)**. When accessing it, consider wearing **anonymous dress (p. 46)** and **tamper-evident preparation (p. 58)** in case something goes wrong and **covert surveillance cameras (p. ??)** are ever installed to identify you, as happened in Italy with motion-activated hunt cameras in a forest stash spot[1].

5.27 Surveillance detection

Techniques addressed by this mitigation:

[1]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

All phones and computers should have **Full Disk Encryption (p. 52)**, and be turned off overnight or when you are out, so that the encryption can be effective. Materials that are used in actions and can appear to have a 'legitimate' purpose should be stored where they belong and not together (gloves with the cleaning stuff, etc.). Action materials without a 'legitimate' purpose should be kept in a **stash spot or safe house (p. 57)**, or at worst they should only transition through the house for a very limited amount of time. In most contexts we do not think that it makes sense to avoid storing anarchist literature at home, but specific guides to sketchy things should be avoided.

5.23 Preparing for repression

Techniques addressed by this mitigation:
Extra-legal violence (p. 23)
House raid (p. 30)

Repression often hits hardest when we aren't prepared for it. Finding yourself in a holding cell wondering who will be your lawyer, walk your dog, call your job, or pay your bail is rough. Such preparation may seem emotionally draining, but we find it actually liberates us to act more freely. Preparation can involve more immediate or longer term dimensions.

In the immediate wake of an arrest, make sure that your comrades know what to do if you've been snatched, with redundancy in case several arrests occur. This might involve sharing the login information for a work email, a house key, arranging for people to care for children, pay rent or bail, etc. Longer term preparations could include making sure that your projects can continue in the case of your imprisonment, which can sometimes be as straight forward as sharing a password in advance. Some comrades train martial arts in order to be better equipped to navigate the violence between prisoners that is prevalent in many contexts.

If drug possession is highly criminalized in your context, you should consider staying away from them. Investigators can use drug charges to apply pressure for the crimes they are actually interested by.

Preparation also involves psychological and emotional dimensions; being put in a cage is an attack on these levels as well. Preparation for this can range from speaking with formerly incarcerated comrades about their experience, to something direct such as an experience related in Claudio Lavazza's autobiography[1] where he secluded himself in a house in the mountains for a month, to prepare for the possibility of his imprisonment.

5.24 Prisoner support

Techniques addressed by this mitigation:
Informants (p. 32)

Beyond the ethical imperative to support our prisoners, people are less likely to turn informant when they feel supported and connected to the movements that they risked their freedom for. Organizing material, logistical, and emotional support for comrades behind bars is crucial.

Common prisoner support initiatives include writing letters, financial support for the prisoners or their close ones, continuing the projects or struggles in which imprisoned comrades cannot participate anymore due to their situation, and in general showing solidarity in ways that are meaningful to the comrades behind bars. On rare occasions, comrades have managed to help others escape from prison.

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

4 Techniques

4.1 Alarm systems

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

Alarm systems protect buildings and other physical or digital infrastructure by sending an alert signal when unauthorized access is detected. The alert signal may lead to the quick intervention of a security team or police forces in order to investigate the situation.

For physical infrastructure, modern alarm systems will typically include sensors to detect unauthorized access to an area outside of normal operating hours. Sensors include infrared movement detectors, sensors that detect the opening of doors, and many other type of sensors[1]. The alert signal can be sent through a wired or wireless connection - low-cost modern systems often send the signal over the mobile phone network.

For digital infrastructure, intrusion detection systems[2] monitor for any activity that could suggest a hack is underway. An incident response team will be notified to attempt to contain and repair any compromise.

Mitigations

Attack (p. 47): Alarm systems - or the communication lines they require to send alert signals - can be destroyed in advance or during an action. Wireless alert signals can also be jammed with an appropriate jammer device.

Note however that some alarm systems work by periodically or continuously sending signals, even when nothing abnormal is detected. In such cases, the destruction of the alarm system will result in the interruption of its signal, which may be interpreted as an alert and trigger an intervention.

When carrying out a cyber action, the use of defense evasion techniques[3] can enable the hack to go undetected.

Reconnaissance (p. 57): When possible, target buildings or infrastructure can be surveyed in advance in order to assess the presence of an alarm system, and the type and position of sensors or other alarm devices.

4.2 Canine trackers

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

A canine unit at the scene of a crime can follow a scent it is provided by its handler. This is more difficult in urban areas with higher population density than rural areas. Bodies of water can interrupt the scent trail and pepper spray on the trail can even temporarily take the dog out of commission.

Mitigations

Careful action planning (p. 49): If there is a possibility of a canine tracking unit being deployed after an action, you can plan to cross a river or use pepper spray during your exit.

[1] https://en.wikipedia.org/wiki/Security_alarm#Sensor_types
[2] https://en.wikipedia.org/wiki/Intrusion_detection_system
[3] https://en.wikipedia.org/wiki/Intrusion_detection_system_evasion_techniques

4.3 Covert house search

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

A covert house search is when police conduct a search of a living space when the occupants are out of the space. This can be an opportunity for them to gather information or install **covert surveillance devices (p. 18)**.

When the searched space has locked doors a covert method of entry is required, such as picking the locks or asking the building's owner for cooperation. Often they will want to avoid the occupants learning that the operation has taken place so they will refrain from seizing materials or moving things around.

Additionally, garbage can be covertly seized from in front of a house with less effort, in the hope of finding written notes or forensic traces like DNA samples.

Mitigations

Clandestinity (p. 49): The State will not know where comrades who take the path of clandestinity live, so a covert house search becomes less likely.

Physical intrusion detection (p. 55): A covert house search can be detected with the right preparation.

Preparing for house raids (p. 55): This involves minimizing the presence of materials which could be harmful in the event of a covert house search.

Stash spot or safe house (p. 57): Action materials without a 'legitimate' purpose should be kept in a stash spot or safe house, or at worst they should only pass through your house for a very limited amount of time.

4.4 Covert surveillance devices

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

Electronic devices can be hidden in diverse ways to enable data collection that would not be possible without them. They can be installed in homes, in/on a car, in a building across the street to record the comings and goings of a target's home, and even on a tree in a forest. Such an installation will typically be conducted by a technician accompanied by surveillance officers.

They can be installed for long-term surveillance and stay in place for weeks, months or years before being removed by their installers – or in some cases, being found by the people under surveillance. They can also be installed for short-term surveillance of specific events.

The collected data is often transmitted over the cellular network using a SIM card included in the device, but other transmission methods are also possible, such as WiFi, Bluetooth, or transmission over arbitrary radio frequencies. Some devices never transmit the collected data, and need to be physically accessed for the data to be retrieved.

It is common for their use to be legally justified by the target's own threat mitigation practices (such as never **self-incriminating (p. 47)** over digital communications) making other repressive techniques ineffective.

See Ears and Eyes[1] and the hidden devices topic[2].

[1]https://csrc.link/earsandeyes
[2]https://csrc.link/#topic=hidden-devices

It is not possible to deem indoor spaces, including cars, free of **covert surveillance devices (p. 18)**, even after an exhaustive **bug search (p. 48)**. It is not possible to deem electronic devices free of **targeted malware (p. ??)** that could turn them into covert microphones. As a result, any sensitive or incriminating conversations should occur outdoors and without any electronic devices.

Outdoor conversations can be recorded with hidden microphones or long-range parabolic microphones during a **physical surveillance (p. 38)** operation (with effective ranges of up to 300 metres). For example, in Italy in 2019[1] a microphone was hidden inside a fake stone in front of a jail where gatherings were often happening. As a result, it is best to have sensitive discussions while walking, or for larger group discussions where being on the move would be too difficult, holding them in spaces that change regularly and are difficult to mic [difficult to mic is vague here].

The practice of shutting down cellphones, removing their batteries or putting them in Faraday bags during outdoor conversations generates **metadata (p. 53)** about who is having sensitive conversations, when, and where - it is best to simply leave such devices at home. In addition, a Faraday bag will do nothing to prevent audio being captured, just prevent it from being transmitted, which could just happen when the phone reconnects to the network if the phone is infected by **malware (p. ??)**.

See the security culture topic[2].

5.21 Physical intrusion detection

Techniques addressed by this mitigation:

Covert house search (p. 18)
Covert surveillance devices > Audio (p. 19)
Covert surveillance devices > Location (p. 20)
Covert surveillance devices > Video (p. 21)
Evidence fabrication (p. 22)
Targeted digital surveillance > Physical access (p. 43)

Physical access to a space can be detected with motion-activated cameras which send remote notifications - in case the camera is discovered and tampered with. It can be positioned with the home entrance(s) in the camera's line of sight, or somewhere discreet to listen for noises. It can be exclusively turned on before you leave the house, programmed with a countdown delay, and turned off as soon as you are back.

Using Haven[3], an extra Android phone can be turned into a motion, sound, vibration and light detector, watching for intruders. Notifications of intrusion events can be sent over Signal, and event logs and captured media can be remotely accessed through a Tor Onion Service.

5.22 Preparing for house raids

Techniques addressed by this mitigation:

Covert house search (p. 18)
House raid (p. 30)

Preparing for house raids involves minimizing the presence of materials which would be harmful in the event of a **house raid (p. 30)** or **covert house search (p. 18)**.

[1]https://csrc.link/earsandeyes/#cuneo-2019-06
[2]https://csrc.link/#topic=security-culture
[3]https://guardianproject.github.io/haven

The 'need to know' principle is that sensitive information should only be shared if necessary, and to the degree necessary. This makes repression more difficult by controlling the flow of information through networks in order to make them more opaque from the outside and harder to disrupt. Bragging goes against the 'need to know' principle.

For example, people not involved in an action should know nothing about it. People who have a specific and limited role in an action might not need to know who else is involved other than the person they are directly communicating with.

One coordinating structure that embodies this principle is the 'spokes council' – individuals meet from various affinity groups for a project without revealing everyone involved to one another. This principle should be weighed against its tendency to form 'choke-points' of coordination - if one individual is always the coordinating bridge between affinity groups, this can lend itself to gate-keeping dynamics, as well as making further coordination impossible in the scenario of this person's imprisonment.

See the security culture topic[1].

5.19 Network map exercise

Techniques addressed by this mitigation:

Infiltrators (p. 31)
Informants (p. 32)
Network mapping (p. 37)
Targeted digital surveillance > Physical access (p. 43)

A practice that takes a network as the starting point, rather than the relationships of an individual, will be more resilient to infiltration attempts. If we individually critically examine all the links in our networks instead of removing ourselves from parts of them, we provide greater security to our network and to ourselves.

In the absence of being routed out of networks, covert operatives end up building credentials through association, building intensive social profiles on everyone, finding pressure points to cause conflict within networks, entrapping people, and monitoring our daily lives.

A 'base of safety' list emerges out of asking yourself a series of structured questions that reveal your level of safety with all the individuals involved in your networks. This exercise is to sharpen our ability to make informed and critical choices about the people we associate with. Analyzing relationships in this manner can be effective in both mapping and realizing a network of relative safety, while bringing to light any additional information you should seek in the hopes of strengthening the links in your network. The Network Map is the visualization of the list of people in your network, the density and nature of connections between individuals, and distinguishing a 'base of safety' from people you would like to know more about. This exercise is intended to be performed in periods of relative calm.

For instructions on how this can be done, see Stop hunting sheep: a guide to creating safer networks[2]. Such a network map would be invaluable to investigators, it is essentially what they are constructing during **network mapping (p. 37)**, so it should be burned immediately after use.

5.20 Outdoor and device-free conversations

Techniques addressed by this mitigation:

Covert surveillance devices > Audio (p. 19)
Mass surveillance > Video surveillance (p. 35)

[1] https://csrc.link/#topic=security-culture
[2] https://csrc.link/#stop-hunting-sheep

4.4.1 Aerial

As drones become less expensive and more available to police departments, their use for covert aerial surveillance becomes more common.

For example, during the 2019 insurrection in Chile, drones were used to follow rioters after they changed in order to facilitate arrest.

A drone would be a valuable asset in a physical surveillance effort to lessen the likelihood of losing a tail at night. Surveillance planes are also occasionally used, and are much more covert than helicopters. They can be used to surveil entire cities for retrospective location-tracking, photographing up to 32 square miles every second which allows for the slow-motion reconstruction of virtually all outdoor movement[1]. They can also be used for targeted surveillance[2], with high-quality video at night.

See the aerial surveillance topic[3].

Mitigations

Anonymous dress (p. 46): Changing into anonymous dress when in a location that is hidden from aerial visibility can help prevent a surveillance effort from re-establishing contact when you emerge into an open area.

Anti-surveillance (p. 46): Locations that cut off visibility from above - an underground metro system, a mall complex with many entrances, a forest with lots of tree coverage, etc. - can be incorporated into an anti-surveillance route.

Attack (p. 47): In the context of demonstrations, drones can be downed with fireworks, be hacked, or blinded with lasers. See also 5 widely accessible ways to take down drones[4].

Surveillance detection (p. 57): Some drones should be audible and visible, depending on their altitude and your surroundings.

Repressive operations

Berlin 2023 railway conspiracy case (p. 65): The arrested comrades were spotted, at night, by a helicopter on a routine surveillance flight, presumably equipped with night-vision equipment[5]. A text[6] relates that in 2022, during another routine surveillance flight close to Berlin the same helicopter had its position lights switched off and the sound of its rotor blades muffled to avoid detection: 'Although the helicopter could still be heard, the noise was diminished. This can lead to misjudging the distance of the helicopter or, if mixed with other noise such as a highway, to not being aware of the approaching problem until it's too late.'.

4.4.2 Audio

Microphones can be installed anywhere within range of where conversations may be had - a living room, a car dashboard, a regular meeting place outdoors, etc. Playing loud music in the background or whispering are not effective mitigations to these sensitive and precise devices.

[1] https://theintercept.com/2020/04/09/baltimore-police-aerial-surveillance
[2] https://theintercept.com/document/2021/08/31/motion-to-suppress-aerial-surveillance-evidence-in-u-s-vs-muhammed-momtaz-alazhari
[3] https://csrc.link/#topic=aerial-surveillance
[4] https://csrc.link/#cinq-manieres-a-la-portee-de-tous-pour-abattre-un-drone
[5] https://csrc.link/#wir-haben-eine-verabredung
[6] https://kontrapolis.info/9821

Covert microphones can be extremely small – only a few millimeters – especially if they only record locally (on a SD card for example) and do not transmit their recordings.

See Ears and Eyes[1] and the hidden devices topic[2].

Mitigations

Bug search (p. 48): Hidden microphones can be located with the appropriate techniques and tools, and eventually removed.

Digital best practices (p. 51): Cellphones and computers can be turned into covert audio recording devices through **malware (p. ??)**. Using security-oriented operating systems and other digital best practices makes malware installation less likely.

Outdoor and device-free conversations (p. 54): Sensitive conversations should not happen indoors, in cars, or at habitual outdoor locations.

Physical intrusion detection (p. 55): Intrusion detection can allow you to detect if an adversary has conducted a covert house visit to install microphones.

Repressive operations

Scintilla (p. 60): A covert microphone hidden in a squat for two years and a half captured discussions which were used by investigators to prove that the accused comrades knew each other, regularly talked together, worried about the creation of a DNA database and the impossibility of resisting DNA collection or discussed the writing of a text to be published[3].

See the corresponding Ears and Eyes case[4].

Renata (p. 62): Six covert microphones and a camera were found in a house following the operation[5]. The microphones were found in the living room, in the corridor and in the bedrooms. The camera was found inside the intercom.

See the corresponding Ears and Eyes case[6].

4.4.3 Location

Location tracking devices will typically be installed on the target's regular means of transportation; their car or bike. They often use GPS to obtain their own location, but alternatives such as GLONASS or satellite phone services are also possible.

An older method used by these devices was to obtain their own location by transmitting radio waves received by an operator nearby (for example in a vehicle following the target's vehicle), but this is rarely used nowadays.

See Ears and Eyes[7] and the hidden devices topic[8].

[1] https://csrc.link/earsandeyes
[2] https://csrc.link/#topic=hidden-devices
[3] https://macerie.org/index.php/2019/03/12/le-orecchie-della-pedrotta
[4] https://csrc.link/earsandeyes/#torino-2019-03
[5] https://roundrobin.info/2019/03/trento-sei-microspie-e-una-telecamera-immagini-pesanti
[6] https://csrc.link/earsandeyes/#trento-2019-03
[7] https://csrc.link/earsandeyes
[8] https://csrc.link/#topic=hidden-devices

5.16 Gloves

Techniques addressed by this mitigation:

Forensics > DNA (p. 24)
Forensics > Fingerprints (p. 27)

Certain types of gloves can prevent leaving fingerprint on objects that you touch, and conceal hand features like skin color or tattoos. Gloves that are too thin are useless as they will leave print impressions (e.g. surgical gloves). Some materials will transfer prints between objects (e.g. latex or leather gloves).

Always use gloves to handle any tools you'll be bringing to an action so that you don't leave any fingerprints on them. It is easier to avoid leaving fingerprints on something in the first place than to rely on removing prints with a rag soaked in acetone, which can be less effective with some surface types. For example, on metal objects, the oil on your fingers can etch an imprint that can only be effectively removed with sandpaper.

Gloves can also prevent leaving DNA traces on objects that you touch. The best gloves for DNA traces are non-permeable; a new pair of dish washing gloves are best, and also cover the wrist region. Prior to putting on the gloves, thumb holes can be made in long sleeves of a shirt to prevent the sleeve from hiking up during use and exposing arm hairs and skin. Dish washing gloves won't be appropriate in a context like a demo - use a new pair of work gloves that have a thick impermeable coating on the palms and fingers. All gloves will transfer DNA traces between objects, so you need to put them on carefully and not touch your skin afterwards - see the related mitigation **DNA minimization protocols (p. 50)**.

Additionally, fingerprints (and DNA) can be left on the inside of gloves, so they should be disposed of appropriately.

See the fingerprints topic[1] and Handschuhe[2] (in German).

5.17 Metadata erasure and resistance

Techniques addressed by this mitigation:

Forensics > Digital (p. 26)

Metadata is data about the data. For example, a PDF file will embed the information of the computer that created it, and an image file will embed the serial number of the phone that took it. A printed zine will often have an invisible watermark[3] identifying the make and model of the printer it came from.

In **encrypted (p. 52)** digital communications, metadata would encompass any unencrypted information, like the receiver and sender address in PGP-encrypted emails. Metadata resistance refers to how much metadata about the communication is left unencrypted - Cwtch[4] is a highly metadata resistant option.

5.18 Need to know principle

Techniques addressed by this mitigation:

Evidence fabrication (p. 22)
Infiltrators (p. 31)
Informants (p. 32)
Network mapping (p. 37)

[1] https://csrc.link/#topic=fingerprints
[2] https://militanz.blackblogs.org/163-2
[3] https://anonymousplanet-ng.org/guide.html#watermarking
[4] https://cwtch.im

our adversaries and on time[1] and cost[2] estimations of brute-forcing modern cryptosystems, we recommend 7-word Diceware[3] passwords. You can generate such passwords with KeePassXC (select the "Passphrase" tab when generating a password) or with physical dice[4].

Use end-to-end encrypted messaging, ideally something that is decentralized and metadata-resistant like Briar[5] and Cwtch[6]. If you need to use emails, encrypt them with PGP and register an address with a trusted service provider[7].

To secure your home network, use OpenWrt[8] for a router and pfSense[9] for a firewall. All network traffic that doesn't go through Tor should go through a reputable VPN to prevent ISPs (Internet Service Providers) from logging the websites you visit, and to complicate being targeted with **malware (p. ??)**.

5.14 Encryption

Techniques addressed by this mitigation:

Forensics > Digital (p. 26)
Mass surveillance > Mass digital surveillance (p. 34)
Targeted digital surveillance > IMSI-catcher (p. 41)
Targeted digital surveillance > Malware (p. 42)
Targeted digital surveillance > Network forensics (p. 43)
Targeted digital surveillance > Service provider collaboration (p. 44)

Encryption is a process that renders data unintelligible to anyone who doesn't possess the decryption keys (often a password). Encryption can be for data 'in movement' (like encrypted messages) or 'at rest' (like the files stored on your computer).

Using encryption can significantly impair investigative efforts by impairing **network mapping (p. 37)**; the contact lists on a phone or computer are unrecoverable, as are message contents or recipient identity. Encryption of all 'at rest' data (Full Disk Encryption) will minimize the repercussions of a **house raid (p. 30)** or **covert house search (p. 18)** when the device is turned off, encryption of all 'in movement' data (messages, phone calls, etc) will impair any **targeted surveillance (p. 40)** effort. **Device compromise (p. ??)** renders encryption irrelevant - if you can read it so can an enemy.

Outdoor and device-free conversations (p. 54) should still be exclusively used for any incriminating conversations. Encryption is a harm-reduction measure, not a panacea.

5.15 Fake ID

Techniques addressed by this mitigation:

Targeted ID checks (p. 40)

A fake identity document is an important resource for **clandestinity (p. 49)**, in order to avoid arrest in the event of a police control. Using a fake ID is also one approach to establishing a **safe house (p. 57)**.

[1] https://blog.elcomsoft.com/2020/08/breaking-luks-encryption
[2] https://blog.1password.com/cracking-challenge-update
[3] https://en.wikipedia.org/wiki/Diceware
[4] https://www.eff.org/dice
[5] https://briarproject.org
[6] https://cwtch.im
[7] https://riseup.net/en/security/resources/radical-servers
[8] https://openwrt.org/
[9] https://pfsense.org

Mitigations

Bug search (p. 48): Location tracking devices can be located with the appropriate techniques and tools, and eventually removed.

Digital best practices (p. 51): Mobile phones can be turned into covert tracking devices through **malware (p. ??)**, and by default triangulate your location through connection to cell towers. Leaving your phone at home mitigates this risk.

Physical intrusion detection (p. 55): Intrusion detection can allow you to detect if an adversary has conducted a covert house visit to install a location tracker on your vehicle or bike.

Transportation by bike (p. 58): Unlike a car, **searching (p. 48)** a bike allows us to say whether a tracking device is present or not with a high degree of confidence. Bikes should be stored indoors to force the adversary to conduct a covert house visit in order to install a tracker.

4.4.4 Video

Photographs and/or video can be taken by devices that have a line of sight on the target; a front entrance to a home or social center, a motion-activated hunt cam in a tree directed at a forest **stash spot (p. 57)**, in a living room to be able to see what a target takes out of their bag even as they are being careful to not speak indoors, etc.

See Ears and Eyes[1] and the hidden devices topic[2].

Mitigations

Bug search (p. 48): Hidden cameras can be located with the appropriate techniques and tools, and eventually removed.

Digital best practices (p. 51): The cameras on phones and computers can be turned into covert video surveillance devices through **malware (p. ??)**. Using security-oriented operating systems and other digital best practices makes malware installation less likely. During sensitive computer use, have your screen facing a wall which you can search thoroughly for covert cameras (rather than, for example, a window or a TV).

Physical intrusion detection (p. 55): Intrusion detection can allow you to detect if an adversary has conducted a covert house visit to install video cameras.

Stash spot or safe house (p. 57): Even if you don't speak about illegal activities at home, a video camera can capture your non-verbal activities, so it is best to keep incriminating materials at a stash spot or safe house or, if brought home, to keep them in bags and out of sight.

Surveillance detection (p. 57): It is occasionally possible to identify new cameras that have been positioned to face the entrance(s) to your home through developing a baseline awareness of your surroundings so you can be acutely attuned to anything unusual or out of place. Such cameras have been found in cars, in neighboring apartments, and outdoors.

[1] https://csrc.link/earsandeyes
[2] https://csrc.link/#topic=hidden-devices

4.5 Door knocks

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

Police will occasionally come knocking without a warrant in order to create paranoia, to see who is willing to talk to them and could potentially be recruited as an **informant (p. 32)**, and to gather information from the people who do talk. By logging who you call or visit immediately after they come knocking, police can achieve **network mapping (p. 37)**.

Mitigations

Avoiding self-incrimination (p. 47): Simply don't talk to police who come knocking - instead, alert your networks and consider making it public.

Digital best practices (p. 51): Surveilling who you get in touch with after cops come knocking will be more difficult if you are using digital best practices.

Repressive operations

Scintilla (p. 60): In May 2019, cops knocked on the door of Boba under the pretext of giving an oral notice to another comrade[1]. Once inside however, they revealed an arrest warrant for Boba, arrested him and searched the house.

4.6 Evidence fabrication

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

Evidence fabrication can involve anything from lying in a police report to planting incriminating materials, though this can be exposed during trial if not well executed.

For example, police in Baltimore (United States) were not aware that their body cams continued recording in the period after being turned off, and captured themselves planting drugs in the bag of a suspect. Depending on context, such evidence fabrication can be either common or rare.

A common practice of investigators, prosecutors and judges is to 'invent a story', bringing together facts and theories in order to reach their pre-determined hypothesis about a case. This widespread strategy is one of the reasons that it is important to prevent cops from gathering any information about us, because enough information (even mundane) can be woven into a narrative for their purposes.

Mitigations

Need to know principle (p. 53): Evidence fabrication will be more difficult with less information about our lives; the need to know principle controls the flow of information through networks in order to make them more opaque from the outside and harder to disrupt.

Physical intrusion detection (p. 55): Intrusion detection can allow you to detect if an adversary has covertly visited your house to plant evidence.

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

See blabladn[1] for a comprehensive overview of the DNA forensics literature, and protocol suggestions, and the DNA topic[2].

5.13 Digital best practices

Techniques addressed by this mitigation:

Covert surveillance devices > Audio (p. 19)
Covert surveillance devices > Location (p. 20)
Covert surveillance devices > Video (p. 21)
Door knocks (p. 22)
Forensics > Digital (p. 26)
Mass surveillance > Mass digital surveillance (p. 34)
Network mapping (p. 37)
Targeted digital surveillance > Authentication bypass (p. 40)
Targeted digital surveillance > Malware (p. 42)
Targeted digital surveillance > Network forensics (p. 43)
Targeted digital surveillance > Physical access (p. 43)
Targeted digital surveillance > Service provider collaboration (p. 44)

The foundation of digital best practices is to limit technology's reach into your life. For example, if you have a cellphone, leave it at home to avoid the possibility of location tracking. That said, digital devices should be equipped with open source and security-oriented Operating Systems, and configured with best practices in mind.

This excludes Windows, macOS, iPhones and stock Android. In short, use GrapheneOS[3] for mobile phones, Debian[4] or Qubes OS[5] for computers used in daily life, and Tails[6] for sensitive computer use (writing and sending communiques, moderating a sketchy website, research for actions, reading articles that may be criminalized, etc.). All devices should have **Full Disk Encryption (p. 52)** enabled.

Tails is an Operating System installed on a USB device. It is unique in being designed for anonymity and leaving no trace on your computer[7] - all internet connections are forced through the Tor network, and everything runs in the computer's memory (which is irrecoverable after the computer is shut down). See the official website[8] for user-friendly installation instructions and great documentation.

Use strong passwords:

- Most of your passwords (e.g. passwords used to log into websites) should be generated by and stored in a password manager - we recommend KeePassXC[9]. You'll never have to memorize or even type them so they can be very long and random, make them 40 random characters. You can generate such passwords with KeePassXC (select the "Password" tab when generating a password).

- Passwords typed when starting up your encrypted devices will, however, need to be memorized. Assuming you use one of the Operating Systems described above, based on our best knowledge of the capabilities of

[1]https://csrc.link/#blabladn
[2]https://csrc.link/#topic=dna
[3]https://grapheneos.org
[4]https://debian.org
[5]https://qubes-os.org
[6]https://tails.boum.org
[7]https://tails.boum.org/about/index.en.html
[8]https://tails.boum.org
[9]https://keepassxc.org

in order to pre-emptively make targeting that organization more difficult. However, clandestinity is also used in response to repression in order to evade imprisonment, or after a prison escape.

See the clandestinity topic[1].

5.10 Compartmentalization

Techniques addressed by this mitigation:

Network mapping (p. 37)
Targeted digital surveillance > Malware (p. 42)
Targeted digital surveillance > Network forensics (p. 43)

Security by compartmentalization allows you to compartmentalize distinct projects or aliases, so that they cannot be connected, and so that the compromise of one is isolated from the compromise of others. This can occur in digital projects, but can also be applied to any context. A non-digital application of this principle is using a different identity in distinct contexts.

Compartmentalization can be a useful aid for consistently applying mitigations within a project. For example, an email account associated with an anarchist project may want to be consistent about **never providing information (p. 47)** within that channel that could be useful for deanonymization, whereas in a different project that could be acceptable.

See Qubes OS[2] for an Operating System with this security model.

5.11 Computer and mobile forensics

Techniques addressed by this mitigation:

Targeted digital surveillance > Malware (p. 42)
Targeted digital surveillance > Physical access (p. 43)

Computer and mobile forensics are extremely technical disciplines aiming to identify compromise on a computer or phone. False negatives are common.

See Practical Linux Forensics[3] for a comprehensive introduction to the skill-set on the platform that is most relevant to anarchists, and the Mobile Verification Toolkit[4], neither of which should give a false sense of security due to the likelihood of false negatives.

5.12 DNA minimization protocols

Techniques addressed by this mitigation:

Forensics > DNA (p. 24)

We are constantly shedding DNA in various forms; skin cells, hair, saliva, blood, and sweat are all sources of DNA, and unlike fingerprints they can never be reliably removed from an object once contaminated. DNA minimization protocols are intended to enable the manipulation of objects without leaving DNA traces on them. As you would expect, these protocols aim to eliminate skin cells, hair, air-born saliva particles, blood and sweat making contact with the objects. The chemical destruction of DNA is often also involved.

[1] https://csrc.link/#topic=clandestinity
[2] https://www.qubes-os.org/faq/#how-does-qubes-os-provide-security
[3] https://csrc.link/#practical-linux-forensics
[4] https://csrc.link/#mobile-verification-toolkit

4.7 Extra-legal violence

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

State forces can use physical and psychological extra-legal violence, and in some contexts extra-legal assassinations.

In Russia and Belarus, several anarchists have been tortured in recent years after their arrest by State agents. Reported acts of torture in those countries include: [1].

Mitigations

Preparing for repression (p. 56): Preparing for repression can be especially important if your context involves the risk of torture after an arrest. One may want to prepare psychologically for it.

Torture often occur immediatly after the detention, while nobody knows where the person is and there is no lawyer. Depending on the context, involving a lawyer or publicizing the acts of torture can help to pressure authorities to make them stop. It is possible to set up protocols in advance that allow a network to learn when someone is missing, in order to react quickly to their disappearance: for example, members of a group can connect once a day to an encrypted messaging platform to send each other a message.

Repressive operations

Belarusian anarcho-partisans (p. 64): In the first days of their detention, the anarchists were tortured[2].

Network (p. 62): Most of the defendants were tortured by Russia's Federal Security Service (FSB) agents in the early stages of their detention in order to obtain (often fabricated) statements that could later be used to charge and convict them[3]. Most of the defendants that were tortured later retracted their statements and spoke publicly about the torture they had received.

Renata (p. 62): During the house raids in February 2019, one of the arrested comrades was forced to his knees by a cop who put a gun to his temple[4].

4.8 Forensics

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

Forensics is the application of science to investigations for evidence collection, preservation, and analysis, so has a broad focus; DNA analysis, fingerprint analysis, blood stain pattern analysis, firearms examination and ballistics, tool mark analysis, serology, toxicology, hair and fiber analysis, footwear and tire tread analysis, drug chemistry, paint and glass analysis, linguistics, digital audio video and photo analysis, etc. Forensic scientists will often testify as 'expert witnesses' in trials. In addition to linking a suspect's identity to a crime, forensics is often used to link discrete crimes together.

[1] beating, suffocating with a plastic bag or pillow, pouring water in the nose and mouth, hanging by the legs or by tied hands, electric shocks, torture with a screwdriver, making people do squats until they collapse, sexual violence, and the deprivation of sleep, food and drink.
[2] https://pramen.io/en/2021/12/blood-on-your-hands-regarding-information-about-torture-of-anarcho-partisans
[3] https://web.archive.org/web/20210724133854/https://a2day.net/network-underground
[4] https://infernourbano.altervista.org/che-si-sappia-comunicato-dal-trentino

4.8.1 Arson

Fire investigations have two distinct stages: fire scene investigation, which focuses on evidence at the location of the fire, and fire debris analysis, which focuses on evidence removed from the location and analyzed in a laboratory.

Fire scene investigation is much more difficult if the 'flashover' point has been reached - where a room becomes so hot that every ignitable surface will burst into flames. This stage concerns itself with determining whether a fire was intentionally set, and identifying the point of origin of a fire.

Fire debris analysis focuses on ignitable liquid residues (ILRs) and aims to identify any potential accelerant traces and their chemical composition - these samples are generally located with dogs at the scene.

Mitigations

Anonymous purchases (p. 46): If accelerant can be identified and traced back to a gas station brand, then purchasing anonymously prevents police from linking that accelerant to your identity.

Careful action planning (p. 49): The same purchase of accelerant should not be reused for distinct actions, which runs the risk of tying them together.

4.8.2 Ballistics

Forensic ballistics involves the examination of evidence from firearms. When a bullet is fired from a gun, the gun leaves microscopic marks on the bullet and cartridge case. These marks are like ballistic fingerprints.

If investigators recover bullets from a crime scene, forensic examiners can test-fire a suspect's gun, then compare the marks on the crime scene bullet to marks on the test-fired bullet. Cartridge cases are compared in the same way.

Mitigations

Anonymous purchases (p. 46): Anonymous purchase of firearms and ammunition is more challenging, but not impossible. Generally this will involve connections to organized criminal networks or fraud.

Stash spot or safe house (p. 57): To conduct ballistic analysis, the adversary must have the firearm in their possession for comparison which can be prevented by the use of a stash spot or safe house.

4.8.3 DNA

With the exception of red blood cells, every cell in your body has DNA. We are constantly shedding DNA in various forms; skin cells, hair, saliva, blood, and sweat are all sources of DNA. Variations in genetic code are used to identify individuals.

Police have DNA databases for comparison purposes, often obtained during arrests or as part of sentencing. DNA has been used for identification purposes since 1985, and is often treated as a 'gold standard' during trial. DNA found at a crime scene may be partial or 'mixed' - not all samples are sufficient to make a comparison, but the required amount is decreasing with technological advancements.

See blabladn[1] for a comprehensive overview of the DNA forensics literature, and the DNA topic[2].

[1]https://csrc.link/#blabladn
[2]https://csrc.link/#topic=dna

drilled and then covered up). It can help to have the right tools, for example to dismantle electrical outlets in a building or to dismantle the interior of a vehicle.

Detection devices can be bought in specialized stores or on the Internet. Such devices include radio frequency detectors, to detect devices that are transmitting data on radio frequencies at the time of the search, and camera lens detectors to detect cameras. Professional equipment – spectrum analyzers, non-linear junction detectors, thermal imaging systems – can be more efficient, but it is very expensive. It is also possible to pay a specialized company to search for hidden devices, but it is also very expensive, and these companies sometimes have strong links with local authorities.

Unfortunately, 'false negatives' cannot be ruled out; it is always possible that a bug was missed during a search. It is less likely to get a 'false negative' when searching a bike compared to a car because there are far fewer places where a bug can be hidden. **House raids (p. 30)** will occasionally follow the discovery of a covert surveillance device, to enable the seizure of evidence before it can be secured or disposed of in light of the discovery.

See Ears and Eyes[1].

5.8 Careful action planning

Techniques addressed by this mitigation:

Canine trackers (p. 17)
Forensics > Arson (p. 24)
Forensics > DNA (p. 24)
Forensics > Digital (p. 26)
Forensics > Fingerprints (p. 27)
Forensics > Trace evidence (p. 29)
Increased police presence (p. 31)
Mass surveillance > Civilian snitches (p. 34)

Once you have all of the information that you need from the **reconnaissance (p. 57)** stage, it is time to make it actionable with a well-developed plan. Every individual involved needs to have a clear understanding of their role, and how their tasks relate to those of everyone else.

For example - what route to and from the site best fits your needs, and how long will you spend on the action site, taking into consideration the expected timing of a police response? Or, what on your escape route could impair a police chase (for example will police need to exit their vehicle to follow on foot)? Making an action plan is a form of threat modeling - what could go wrong, what mitigations will we be implementing, and how? For example, how will **anti-surveillance (p. 46)** be carried out prior to the action meet up spot?

5.9 Clandestinity

Techniques addressed by this mitigation:

Covert house search (p. 18)
House raid (p. 30)
Targeted ID checks (p. 40)

Clandestinity is the decision to break from one's established identity, and start a new life with a clandestine identity. There are many examples of this path being taken to participate in a particular clandestine organization,

[1]https://csrc.link/earsandeyes

Don't brag about crimes to friends, comrades or cellmates - even if you have a solid basis of trust, the knowledge endangers the person you are telling unnecessarily, and a surveillance operation could overhear.

Digital communications and devices are a hostile terrain; if you don't want it read back to you in court, do not let it pass through your phone as a text message, photo, etc. - regardless of **encryption (p. 52)**. Another treasure trove for investigators is social media, and messages or posts are regularly used in prosecutions. Don't take videos or photographs during riots - these incriminate your networks and should be considered a form of snitching[1].

Refusing to submit ID, fingerprints, and DNA upon arrest can be a viable strategy, but is highly context dependent.

See the related mitigation **Need to know principle (p. 53)**.

5.6 Biometric concealment

Techniques addressed by this mitigation:

Forensics > Facial recognition (p. 27)
Forensics > Gait recognition (p. 28)
Forensics > Handwriting analysis (p. 28)
Forensics > Linguistics (p. 29)
Mass surveillance > Video surveillance (p. 35)

Biometric concealment encompasses any practices that obscure biometric identifiers (unique physical or biological characteristics) that can be used for identification purposes.

In the case of **gait recognition (p. ??)**, this can involve baggy clothing, using umbrellas and a 'funny walk' when on surveillance cameras. For **facial recognition (p. ??)**, masking is used to conceal facial features, and sunglasses or a hat brim are used to conceal eye traits. For **handwriting analysis (p. ??)**, texts are either written digitally, or in the case of graffiti, in ALL CAPITALS with an attention to making the lettering as generic as possible. The utility of **forensic linguistics (p. ??)** can be minimized with brevity and intention.

See the facial recognition topic[2], Who wrote that?[3], and the chapter 'Traces' in Prisma[4].

5.7 Bug search

Techniques addressed by this mitigation:

Covert surveillance devices > Audio (p. 19)
Covert surveillance devices > Location (p. 20)
Covert surveillance devices > Video (p. 21)
Targeted digital surveillance > Authentication bypass (p. 40)
Targeted digital surveillance > IMSI-catcher (p. 41)

Searching for bugs is the active process of trying to detect the presence of **covert surveillance devices (p. 18)** in a place, vehicle, or outdoors. The first technique of this process is a manual, physical search in the suspected environment. Additionally, specialized detection devices can also be used.

If it is suspected that devices were installed recently, it can help to look for things out of place: furniture that has been moved, or parts of walls that have slightly changed color (which could indicate that a hole was

[1]https://rosecitycounterinfo.noblogs.org/2022/08/uprising-lessons
[2]https://csrc.link/#topic=facial-recognition
[3]https://csrc.link/#wer-schreibt-denn-da
[4]https://csrc.link/#prisma

Mitigations

Careful action planning (p. 49): Every step of the plan can be rehearsed with an eye to minimizing DNA traces at the site of the action. This can involve, for example; securing your hair under a hat, cutting any fence holes large enough to pass through without touching the metal, ensuring that any delays on the incendiary device has a backup and has worked as expected in tests conducted under similar conditions (temperature, etc), that surfaces at the action site aren't touched if they don't need to be, that action site surfaces that need to be interacted with (like a door handle) are touched by someone following **DNA minimization protocols (p. 50)**, and that nothing will be left behind accidentally like a bag, tool, or anything falling out of a pocket.

DNA minimization protocols (p. 50): DNA minimization protocols are intended to enable the manipulation of objects without leaving DNA traces. As you would expect, these protocols aim to eliminate skin cells, hair, saliva particles, blood and sweat from making contact with the objects. DNA destruction via chemicals can also be implemented.

Gloves (p. 53): Gloves can prevent leaving DNA traces on objects that you touch.

Repressive operations

Nea Filadelphia case (p. 60): The accusations against several comrades were based on a match between their DNA taken by force during custody and DNA traces found on 'mobile objects' near the robberies[1].

Scripta Manent (p. 59): DNA traces were used to convict Alfredo Cospito[2].

Repression of the first Jane's Revenge arson (p. 65): In May 2022, DNA traces were collected from several items found by investigators on the crime scene, including from a broken window, a glass jar, a lighter, and an intact Molotov cocktail[3]. In March 2023, cops saw the comrade who would later be arrested discard a brown paper bag containing a partially eaten burrito in a public trash. DNA traces collected from the contents of the bag matched the traces collected from the crime scene.

2019-2020 case against Mónica and Francesco (p. 63): Francesco's DNA was alledgedly found on the parcel bomb that was sent to the ex-Minister of Interior, which was defused and didn't explode[4].

Repression of Lafarge factory sabotage (p. 65): In one of the initial raids, cops insisted that those who were under arrest wear surgical masks to protect against Covid, and those arrested accepted. The cops later retrieved the masks for DNA collection[5].

Repression against Zündlumpen (p. 63): The only clue against one suspected editor of the newspaper is that their DNA was found on a cigarette butt in the print shop raided in April 2022[6].

Scintilla (p. 60): The accusation against Peppe was based on a match between DNA traces found inside the parcel bomb and his DNA collected from a cigarette butt during the investigation[7].

[1]https://abcsolidaritycell.espivblogs.net/archives/130
[2]https://insuscettibilediravvedimento.noblogs.org/post/2020/03/29/it-en-italia-su-una-sentenza-e-qualcosa-daltro-un-testo-di-marco-dal-carcere-di-alessandria
[3]https://csrc.link/documentation/First Jane's Revenge arson investigation files.pdf
[4]https://csrc.link/#about-orwell-and-the-case-of-monica-and-francisco
[5]https://sansnom.noblogs.org/archives/16831
[6]https://csrc.link/#the-persecution-of-anarchists-and-cigarette-butts-in-the-bavarian-christian-kingdom
[7]https://roundrobin.info/2019/12/verona-una-perquisizione-e-un-arresto

Renata (p. 62): After being arrested and imprisoned, the comrade accused of the explosive attack against the 'Lega Nord' Treviso headquarters refused DNA collection[1]. Some time after his refusal, prison guards searched his cell and covertly replaced a comb with another one, presumably to obtain the comrade's DNA from hairs on the comb they took.

Panico (p. 61): DNA traces were the only evidence against one of the accused comrades[2].

Mauvaises intentions (p. 59): During police custody, DNA was collected from the comrades' clothes and from plastic cups[3]. In one case, only nine hours elapsed between the collection of a DNA trace in custody and the result of its comparison with another trace previously collected.

The accusations against one comrade were based on a match between his DNA and DNA traces collected on the site of an attempted arson against the electrical cabinet. DNA traces were collected both from a latex glove found nearby and from a bottle inside the cabinet - which did not catch fire because of a failed delay.

The accusations against other comrades were based on a match between their DNA and DNA traces collected from a cigarette that was used as a delay for an incendiary device - the delay failed and the device was found intact below the police tow truck.

Prometeo (p. 61): DNA traces were used to convict the comrade accused of arsoning an ATM[4].

4.8.4 Digital

Digital forensics is concerned with retrieving, storing and analyzing electronic data that can be useful in criminal investigations. This includes information from computers, hard drives, mobile phones and other data storage devices.

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

Mitigations

Avoiding self-incrimination (p. 47): Self-incriminating information should only ever be on a digital device for very intentional reasons such as to write and send a communique, and always through **Tails (p. 51)**.

Careful action planning (p. 49): During investigations into hacking actions, the targets of the hack are analyzed using forensic methods to identify where the attack came from (attribution) - this could involve identifying what tools were used and any other 'signatures'. Using popular rather than custom tooling can help to prevent attribution. If attribution is possible, discrete hacks can be tied together. Implementing operational security during the hack will stand in the way of deanonymization - all Virtual Private Servers (VPS) used should be **bought anonymously (p. 46)**, accessed exclusively through Tails[5], off of your home WiFi.

Digital best practices (p. 51): Tails[6] is 'amnesic' - a forensic examiner's worst nightmare. It is designed to leave no trace on the computer on which it is used.

Encryption (p. 52): Full Disk Encryption with a high quality password should protect against the forensic examination of any phone or computer that is not 'amnesic' like Tails[7]. This type of encryption is only active

[1] https://roundrobin.info/2020/03/aggiornamenti-su-manu-stecco-juan-e-sasha
[2] https://panicoanarchico.noblogs.org
[3] https://infokiosques.net/spip.php?article597
[4] https://roundrobin.info/2021/05/sentenza-beppe
[5] https://tails.boum.org
[6] https://tails.boum.org
[7] https://tails.boum.org

effort to be able to observe), or when you have identified the presence of surveillance and need to evade them immediately (for example, if you are being tailed by fascists).

Anti-surveillance can and should be employed even when there is no specific indication that surveillance is present, to ensure that protected activities remain unobserved. Anti-surveillance should be as covert as possible, so as to not tip off a surveillance effort that you have detected them.

See the related mitigation **Surveillance detection (p. 57)**.

5.4 Attack

Techniques addressed by this mitigation:

Alarm systems (p. 17)
Covert surveillance devices > Aerial (p. 19)
Guards (p. 30)
Increased police presence (p. 31)
Infiltrators (p. 31)
Informants (p. 32)
Mass surveillance > Civilian snitches (p. 34)
Mass surveillance > Routine police surveillance (p. 35)
Mass surveillance > Video surveillance (p. 35)

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

Mass digital surveillance is impossible when the Internet backbone has been taken offline with fiber optic cables cut. Video surveillance is not only dependent on network connectivity, but also on physical cameras that are too decentralized to effectively protect against sabotage. A witness can be intimidated to not testify at an upcoming trial when the car outside their home is torched while they sleep. Informants and infiltrators can be immiserated and attacked in innumerable creative ways. Increased police presence somewhere means the opportunity of decreased police presence somewhere else. Forensic labs can go up in smoke. Police communications depend on TETRA[1] and P25[2] antennas, and police operations depend upon the integrity of their car fleets, stations, and the feelings of safety of individual officers. The possibilities of attack are limited only by one's imagination.

5.5 Avoiding self-incrimination

Techniques addressed by this mitigation:

Door knocks (p. 22)
Forensics > Digital (p. 26)
Interrogation techniques (p. 33)
Mass surveillance > Mass digital surveillance (p. 34)
Network mapping (p. 37)

An enormous number of convictions are based on self-incrimination - behaviours that are essentially snitching on yourself.

Don't talk to cops: in the case of arrest, any communications with authorities beyond the legal requirements (often name, date of birth, and address) should be considered self-incrimination, and depending on your context there may be a precedent of being released without divulging even this information.

[1] https://en.wikipedia.org/wiki/Terrestrial_Trunked_Radio#Usage
[2] https://en.wikipedia.org/wiki/Project_25

5 Mitigations

5.1 Anonymous dress

Techniques addressed by this mitigation:

Covert surveillance devices > Aerial (p. 19)
Mass surveillance > Civilian snitches (p. 34)
Mass surveillance > Video surveillance (p. 35)
Physical surveillance > Overt (p. 39)

Clothing has distinguishing characteristics that can be used to track and identify an individual; a specific footprint left in the mud, textile fibers that are caught on a fence, hair not tucked out of sight, a mask without sufficient coverage, the color and design of a windbreaker, etc. Dressing anonymously means that a photograph taken of you in that instant could not be used to identify you.

Black bloc tactics are an example of anonymous dress being employed in the context of a demonstration - an individual should be indistinguishable from the person beside them. In the context of a nocturnal attack, anonymous dress will likely not be all black in order to not draw unwanted attention, but still defeat identification purposes because it is only used once, is disposed of securely afterwards, and is changed into at an appropriate location that doesn't have surveillance cameras or witnesses.

5.2 Anonymous purchases

Techniques addressed by this mitigation:

Forensics > Arson (p. 24)
Forensics > Ballistics (p. 24)
Mass surveillance > Video surveillance (p. 35)

Anonymous purchases are necessary for any materials that could be tied back to an action. Payments should always be made in cash, interaction with the employee at the cash register should not be memorable. Purchases should be made far in advance, with staggering times and locations to make surveillance footage analysis more challenging. Digital anonymous purchases are also possible with cryptocurrencies like Monero using Tails[1], though these are more involved because the cryptocurrency needs to be laundered sufficiently between purchase and use. Anonymous purchases should be considered a 'protected activity' which is preceeded by **anti-surveillance (p. 46)**.

See Prisma[2] and the related mitigations **anti-surveillance (p. 46)** and **anonymous dress (p. 46)**.

5.3 Anti-surveillance

Techniques addressed by this mitigation:

Covert surveillance devices > Aerial (p. 19)
Physical surveillance > Covert (p. 38)

Anti-surveillance is when you take active measures to 'shake off' an identified or possible surveillance effort. It is used as a standard security practice prior to 'protected activities' (anything you don't want a surveillance

[1]https://anonymousplanet-ng.org/guide.html#your-cryptocurrencies-transactions
[2]https://csrc.link/#prisma

when the device is fully powered down (not locked or sleeping), which is why all devices should be turned off when not in use.

Metadata erasure and resistance (p. 53): File metadata should be wiped before a file is published online or sent to others.

4.8.5 Facial recognition

Facial recognition is a technology capable of matching a human face from a digital image or a video against a database of faces.

It works by pinpointing and measuring facial features from a given image - today, sophisticated facial recognition technology is capable of identifying a masked individual if their eyes and eyebrows are showing. Facial recognition paired with mass **video surveillance (p. ??)** is used to automate the tracking of identified individuals through a space. Its use as evidence at trial does not have consensus.

See the facial recognition topic[1].

Mitigations

Biometric concealment (p. 48): A mask is used to conceal facial features, and sunglasses or a hat with the brim pulled low are used to conceal eyes.

Repressive operations

2019-2020 case against Mónica and Francesco (p. 63): To identify Mónica and Francesco on public video surveillance footage, photos of both of them found on social media were compared to the footage, including comparison of several facial features: distances of the eyes, wrinkles, piercing scars, ear size, mouth and nose shape[2].

4.8.6 Fingerprints

Our skin secretes oil, which we transfer to any object we touch in the form of uniquely identifying fingerprints.

On some surfaces such as metal, an imprint can be etched into the surface itself due to the reaction between the oil and metal, causing the fingerprint to be identifiable even after the surface is wiped with an acetone soaked rag.

Police have fingerprint databases for comparison purposes, often obtained during arrests. Fingerprints found at a crime scene may be partial, distorted, or smudged - sufficient detail needs to be present to make a comparison.

See the fingerprints topic[3].

Mitigations

Careful action planning (p. 49): Any tools used during an action should be fingerprint-free in case they are lost or need to be ditched. Gloves should be worn at the action site.

Gloves (p. 53): Certain types of gloves can prevent leaving fingerprint on objects that you touch.

[1]https://csrc.link/#topic=facial-recognition
[2]https://csrc.link/#about-orwell-and-the-case-of-monica-and-francisco
[3]https://csrc.link/#topic=fingerprints

4.8.7 Gait recognition

Gait is the way that we move, a type of behavioral biometric; gait recognition identifies people by their walking style and pace which are extremely difficult to change.

Each person's gait can be defined by unique measurements such as the locations of ankle, knee, and hip. Gait recognition can enable the identification of people even if their faces are obscured. Advanced gait recognition technologies can identify someone at a great distance even if they intentionally attempt to change their gait.

Mitigations

Biometric concealment (p. 48): Baggy clothing that conceals body shape, umbrellas and a 'funny walk' can be used around surveillance cameras.

Repressive operations

Scintilla (p. 60): Two of the comrades were accused of an arson attack because their gait and walking style were considered compatible with individuals recorded by a video surveillance camera placing a canister of flammable liquid in front of an Italian Post office[1][2].

Bialystok (p. 62): The main evidence against the comrade accused of an explosive attack against a police station was a comparison between his gait and the color of his coat with the corresponding characteristics of an individual recorded by the police station surveillance cameras[3].

4.8.8 Handwriting analysis

Every person has a unique way of writing. Handwriting analysis is a process that relies on knowledge of which characteristics of letter formation are unique and the physiological processes behind writing - the ways in which a person's fine-motor skills can affect their handwriting and leave clues about the author's identity.

Mitigations

Biometric concealment (p. 48): Texts are either written digitally, or in the case of graffiti, in ALL CAPITALS with the goal of making the lettering as generic as possible.

Repressive operations

Scripta Manent (p. 59): Handwriting samples of some of the accused comrades (including notes seized during raids and letters written from prison) were compared to handwritten addresses from unexploded parcel bombs, with the goal to link the comrades to the attacks[4].

Repression of the first Jane's Revenge arson (p. 65): Comparison between cursive graffiti left at the crime scene and the same style of graffiti painted a few months later during a demonstration helped to identify the comrade who would later be arrested[5].

[1] https://macerie.org/index.php/2019/04/17/ultime-da-carceri-e-tribunali
[2] https://attaque.noblogs.org/post/2020/08/06/saint-etienne-arrestation-de-carla-recherchee-dans-le-cadre-de-loperation-scintilla
[3] https://ilrovescio.info/2022/02/02/aggiornamento-sulle-misure-e-sul-processo-per-lop-byalistok
[4] https://lib.anarhija.net/library/operation-scripta-manent-in-italy-2016-2019#toc15
[5] https://csrc.link/documentation/First Jane's Revenge arson investigation files.pdf

Repressive operations

Repression against Zündlumpen (p. 63): A clue against one suspected editor of the newspaper is that she used her bank account to order things that could be used for printing things - her bank records were presumably obtained by cops through the collaboration of the bank[1].

Mauvaises intentions (p. 59): Phone service providers collaboration was used to link phone numbers to civil identities, know which phone numbers were in contact with each other, geolocate phones (both after the fact and in real time) and record phone conversations[2].

Prometeo (p. 61): Investigators distorted conversations obtained by phone tapping to make them look suspicious[3]. During a phone conversation in which one of the accused comrades participated, the sentence 'tutta questa tensione sociale prima o poi scoppierà' ('all this social tension will, sooner or later, explode') was said, and was only partially transcribed in the investigation files as 'prima o poi scoppierà' ('will, sooner or later, explode').

[1] https://csrc.link/#the-persecution-of-anarchists-and-cigarette-butts-in-the-bavarian-christian-kingdom
[2] https://infokiosques.net/spip.php?article597
[3] https://ilrovescio.info/2020/08/23/uno-scritto-di-natascia-dal-carcere-di-piacenza

Network map exercise (p. 54): Critically examining the links in your network can let you decide who you allow to use your devices, on the basis of established trust.

Physical intrusion detection (p. 55): Physical access to a space can be detected with motion-activated cameras which send remote notifications in case the camera is discovered and tampered with.

Tamper-evident preparation (p. 58): Tamper-evident preparation will make it possible to discern when something has been physically accessed - it's not possible to prevent a powerful enemy from obtaining physical access to your computer when you are away, but it should be possible to detect when they do.

4.21.6 Service provider collaboration

Service providers like mobile network operators, Internet Service Providers (ISP), email providers or banks can be asked or legally forced to provide data about your usage of their service. Such collaboration can provide law enforcement with both real-time and past data about the content of unencrypted communications (landline phones, unencrypted email, SMS and normal calls on a mobile phone), **metadata (p. 53)** of encrypted communications (such as the IP address that accessed an email account) or bank account activity, for example.

Mitigations

Digital best practices (p. 51): Using a trusted service provider[1] means that they will refuse to comply with law enforcement requests to access your data, or build their service so that it would be technically impossible to comply with such requests. Using peer-to-peer applications like Cwtch[2] and Briar[3] for communication or OnionShare[4] for file sharing avoids having to put trust in a service provider.

Collaboration of mobile network operators can be mitigated by using anonymous or burner[5] phones: if the adversary doesn't know a phone number, they can't ask the operator for the data. However, several techniques exist to discover a phone number and enable collaboration of the operator:

- Find the phone number in the contact list of another phone.
- Correlate location data from cell towers: if cops know that you were in place A on Monday and in place B on Tuesday, and know from cell towers data that a given phone was the only phone which was also in place A on Monday and in place B on Tuesday, the phone is probably yours.
- Use an **IMSI-catcher (p. ??)** associated with a **physical surveillance (p. 38)** operation: if cops see you call someone and at the same time the IMSI-catcher reports that a nearby phone initiated a call, the phone is probably yours.

Encryption (p. 52): Encryption will limit the ability of untrusted service provider collaboration; for example, the Internet Service Provider will be able to collect much less data on your network activity if you use Tor or a VPN.

[1] https://riseup.net/en/security/resources/radical-servers
[2] https://cwtch.im
[3] https://briarproject.org
[4] https://onionshare.org
[5] https://csrc.link/#burner-phone-best-practices

2019-2020 case against Mónica and Francesco (p. 63): The sticker of the parcel bomb sent to the police station remained intact despite the explosion of the package ; address information written on the sticker was compared to and positively matched with Francesco's handwriting[1].

4.8.9 Linguistics

Forensic linguistics are used for author identification (stylometry); such identification relies on analysis of particular patterns of language use (vocabulary, collocations, spelling, grammar, etc.). Linguistics are also used for voice identification; determining if the voice on a recording is that of the suspect, through acoustic qualities.

See Counteracting Forensic Linguistics[2] and Who wrote that?[3].

Mitigations

Biometric concealment (p. 48): The utility of linguistics can be minimized with brevity and intention.

Repressive operations

Scripta Manent (p. 59): Texts published by some of the accused comrades were compared to claims of responsibility from the Informal Anarchist Federation, with the goal to prove that the comrades had written those claims[4].

4.8.10 Trace evidence

Tiny fragments of physical evidence such as hairs (including pet hairs), gunshot residue, fibers from clothing, flecks of paint or pieces of glass are examples of trace evidence, and can be transferred when two objects touch or when small particles are disbursed by an action or movement. Less frequently included items are soil, cosmetics and fire debris.

Most test methods require magnification and/or chemical analysis. Trace evidence can be used to link people or objects to places, other people or other objects, and often serves as a lead for a particular line of investigation.

See the other physical traces topic[5].

Mitigations

Careful action planning (p. 49): Tools and clothing used during actions should be disposed of securely afterwards - trace evidence can be used to link them to the action site.

Stash spot or safe house (p. 57): Tools that are too expensive to realistically be disposed of after every action can be stored in a stash spot or safe house.

[1] https://csrc.link/#about-orwell-and-the-case-of-monica-and-francisco
[2] https://anonymousplanet.org/guide.html#appendix-a4-counteracting-forensic-linguistics
[3] https://csrc.link/#wer-schreibt-denn-da
[4] https://lib.anarhija.net/library/operation-scripta-manent-in-italy-2016-2019#toc15
[5] https://csrc.link/#topic=other-physical-traces

4.9 Guards

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

Human guards can be hired to protect buildings or other physical infrastructure.

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

Mitigations

Attack (p. 47): Guards can be incapacitated to prevent them from interfering with an action. For example, in their attacks on machinery of logging companies in so-called Chile, Mapuche people have neutralized guards by disarming them[1], tying them up[2] or shooting at them[3].

4.10 House raid

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

A house raid is when police conduct a surprise search of a living space, often accompanied by simultaneous arrests. This will often happen early in the morning so that the inhabitants are still sleeping and taken by surprise. However, if the goal is to obtain electronic devices when they are powered on, the timing is more likely to be during the day.

Generally, all electronic devices will be seized for analysis as well as anything potentially useful for building their case or network mapping; literature, materials that could feasibly be used for actions, clothing, etc. The opportunity is sometimes taken to install covert surveillance devices. In some jurisdictions, police are only supposed to search the rooms of whoever is named in a warrant.

Mitigations

Clandestinity (p. 49): The State will not know where comrades who take the path of clandestinity live, so a house raid becomes less likely. Sometimes a house raid is what prompts clandestinity - charges are made public and if the individual is not home during the raid, they can decide to avoid arrest by going into clandestinity.

Preparing for house raids (p. 55): This involves minimizing the presence of materials which could be harmful in the event of a house raid.

Preparing for repression (p. 56): House raids are often accompanied by arrests - having plans in place in case of arrest can make a big difference.

Stash spot or safe house (p. 57): Action materials without a 'legitimate' purpose should be kept in a stash spot or safe house, or at worst they should only pass through your house for a very limited amount of time.

[1] https://actforfree.noblogs.org/post/2022/08/04/chile-a-fiery-july-in-the-mapuche-territories
[2] https://actforfree.noblogs.org/post/2022/02/28/chile-the-mapuche-struggle-continues-under-a-state-of-emergency
[3] https://actforfree.noblogs.org/post/2021/07/21/chile-mapuche-zone-ignites-after-the-murder-of-pablo-marchant-update

4.21.4 Network forensics

Network forensics involves monitoring and analyzing computer network traffic. Network information is volatile - it is transmitted and then lost, so requires a pro-active and targeted approach. This could involve compromising a home router, or an operator in a van outside monitoring network traffic, or collaboration of the Internet Service Provider.

The proliferation of TLS encryption on the internet makes network forensics much more difficult, though DNS resolution queries can often be captured - this means that the snooper knows what websites you are visiting, but not the content being transmitted.

Tor traffic does not leak DNS resolution queries - a snooper will simply be able to ascertain that Tor is being used, but not what for. However, such data collection could enable Tor correlation attacks[1]. In the prosecution of anarchist hacker Jeremy Hammond, a snitch's testimony was supplemented with data correlating the time that the hacker alias he used in chat rooms was 'online' (obtained using network traffic analysis[2]), and when a **physical surveillance (p. 38)** effort observed him at home.

Mitigations

Compartmentalization (p. 50): If you want to prevent different projects from being associated with one another, avoid leaving footprints through which the network traffic of the projects could be correlated. This can be achieved by using Tails[3] and rebooting between each session, or on Qubes OS[4] by using different Whonix[5] Qubes non-simultaneously.

Digital best practices (p. 51): Using an open source router configured with a strong password will reduce the likelihood of adversaries accessing network forensics via router compromise.

Encryption (p. 52): The encryption mechanisms of the Tor[6] network offer unparalleled anonymity.

4.21.5 Physical access

If an enemy had physical access to your electronic device at any point, you must assume that this device is compromised. Physical access can be used to read unencrypted contents, or to manipulate the device digitally or physically (for example, to install spyware software, or a physical keylogger). Such physical access can be obtained during inspections by border customs, after arrest if you have the device on you, during a **house raid (p. 30)** or **covert house search (p. 18)**, and through an **infiltrator (p. 31)** or **informant (p. 32)** who you trust to use the device.

Mitigations

Computer and mobile forensics (p. 50): Physical access to a device can sometimes be detected after the fact by using computer and mobile forensics.

Digital best practices (p. 51): Don't bring your phone with you when there is a likelihood of arrest, and ideally keep it at home as much as possible.

[1] https://anonymousplanet-ng.org/guide.html#your-anonymized-torvpn-traffic
[2] https://medium.com/beyond-install-tor-signal/case-file-jeremy-hammond-514facc780b8
[3] https://tails.boum.org
[4] https://qubes-os.org
[5] https://whonix.org
[6] https://torproject.org

See the IMSI-catchers topic[1].

Mitigations

Bug search (p. 48): Detecting the presence of an IMSI-catcher during an event or demo can be grounds to convince all attendees to turn off their phones, provide valuable information about the level of surveillance that police are choosing to employ, and eventually, if the location of the IMSI-catcher is discovered, opens up the possibility of destroying it.

Encryption (p. 52): Forcing all phone Internet traffic through Tor or a VPN will limit the ability of an IMSI-catcher to intercept data. Legacy calls and texts should be avoided[2] as they are not encrypted and thus subject to interception by an IMSI-catcher.

4.21.3 Malware

Malware is **mal**icious soft**ware** which will compromise a computer, server or mobile phone. What this malicious software will do is highly context-dependent, but against anarchists it will typically involves visibility into the device through remote screen capture and remote keylogging (recording of the keys struck on a keyboard).

The overwhelming majority of state malware installs happen through phishing, either over email or text based messages (SMS, etc). To be effective, phishing often requires the target to open a malicious file or link. Malware can also be installed through **physical access (p. ??)**, such as by plugging in a malicious USB device.

See the targeted malware topic[3].

Mitigations

Compartmentalization (p. 50): If your digital activities are compartmentalized, compromise of one device (or compartment in the case of QubesOS and other virtualization technologies) cannot extend to others.

Computer and mobile forensics (p. 50): Traces of malicious software on a device can sometimes be detected after the fact by using computer and mobile forensics.

Digital best practices (p. 51): Using security-oriented operating systems and other digital best practices makes malware installation less likely. Phishing awareness is also important - don't open attachments or click links sent to you by people who you don't trust.

Encryption (p. 52): Forcing all traffic through a VPN can complicate network packet injection - an installation vector for some forms of contemporary spyware like Pegasus[4] which don't require you to click on anything.

Repressive operations

Scripta Manent (p. 59): Malware was installed on the computer of one of the accused comrades[5]. According to investigation files the malware, installed remotely through the Internet, targeted a Windows computer and was capable of recording the text typed on the keyboard, taking periodic screenshots, and recording communications sent and received to and from the computer.

[1]https://csrc.link/#topic=imsi-catchers
[2]https://grapheneos.org/faq#cellular-tracking
[3]https://csrc.link/#topic=targeted-malware
[4]https://forbiddenstories.org/about-the-pegasus-project
[5]https://earsandeyes.noblogs.org/post/2019/01/27/more-precisions-keylogger-italy

Repressive operations

Scripta Manent (p. 59): One comrade was arrested after batteries and an electrician's manual were found in his home during a house raid[1].

Repression of Lafarge factory sabotage (p. 65): Among the initial house raids, one raid was particularly thorough: cops searched below mattresses, behind sofa covers and inside each drawer of each piece of furniture, inspected each book, notebook and clothing item as well as the tableware, and emptied packs of pasta and closed jars[2].

Renata (p. 62): During a house raid, cops tried to get into the basement before waking up the comrades in the house, then secretly complained that they were unable to hide what they wanted to hide[3].

4.11 Increased police presence

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

Police increase their presence in a specific place and time for two reasons; to intimidate, and because grouping their forces improves their options for intervention and their responsiveness.

In the context of a rebellious neighborhood, this might look like much more frequent patrols. For a public demonstration, this can involve lining the surrounding streets with intervention units in the hours before it starts, overt surveillance of the starting location from cars, rooftops, etc., and preemptively clustering around anticipated targets such as government buildings.

Mitigations

Attack (p. 47): An increased police presence is often organized in anticipation of a public demonstration, but if the crowd is numerous and fierce enough, this can be inconsequential. For example, even with the years of planning to militarize Hamburg (Germany) for the G20 summit, rioters were able to liberate a neighborhood from police occupation for an entire night[4]. Decentralized and autonomous forces are more agile than the rigid chain of command that police agencies rely on for crowd control.

Careful action planning (p. 49): The police cannot be everywhere all of the time, even with an increased presence in a certain area. Agility, thorough **reconnaissance (p. 57)** and a good escape plan can go a long way. For incendiary attacks, the use of timers can allow an attack to be carried out unobserved right under their noses. Increased police presence somewhere also means the possibility of decreased police presence somewhere else.

4.12 Infiltrators

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

An infiltrator is someone who infiltrates a group or network by posing as someone who they are not. They may be military, police, intelligence, corporate, private contractor, 'patriot', or just someone who is facing imprisonment.

[1]https://web.archive.org/web/20170928080735/http://www.informa-azione.info/italia_repressione_5_nuovi_arresti_e_una_trentina_di_perquisizioni_per_attacchi_federazione_anarchica_informale
[2]https://sansnom.noblogs.org/archives/16978
[3]https://infernourbano.altervista.org/che-si-sappia-comunicato-dal-trentino
[4]https://crimethinc.com/2017/08/07/total-policing-total-defiance-the-2017-g20-and-the-battle-of-hamburg-a-full-account-and-analysis

Stop Hunting Sheep[1] describes five basic infiltrator types:

1. Hang Around: less active, attends meetings, events, collects documents, observes and listens
2. Sleeper: low-key at first, more active later
3. Novice: low political analysis, 'helper', builds trust and credibility over longer term
4. Super Activist: out of nowhere, now everywhere. Joins multiple groups or committees, organizer.
5. Ultra-Militant: advocates militant actions and conflict

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

See the infiltrators topic[2]

Mitigations

Attack (p. 47): Infiltrators can be attacked when uncovered or years later[3] to dissuade the practice - police infiltrators are likely to be less enthusiastic if there is a local precedent of violence against them.

Need to know principle (p. 53): The need to know principle makes repression more difficult by controlling the flow of information through networks in order to make them more opaque from the outside and harder to disrupt - if an infiltrator isn't involved in an action, they shouldn't know who was involved even if it's their own roommate.

Network map exercise (p. 54): A practice that takes a network as its starting point, rather than the relationships of an individual, will be more resilient to infiltration attempts. If we individually critically examine all the links in our networks instead of removing ourselves from parts of them, we provide greater security to our network and to ourselves.

4.13 Informants

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

An informant is someone recruited by the authorities to provide information, often called a snitch.

Several different recruitment strategies exist; targeting people on the periphery of a network who are less committed, people who could face deportation if they don't cooperate, people who have been charged with a different crime and are offered lenient sentencing or immunity in exchange, people who are no longer in a network and harbour feelings of resentment, people who prioritize money over dignity, etc. Informants are useful for **network mapping (p. 37)** and **incrimination (p. 15)**, and are often referred to in court proceedings as a 'confidential source'.

See the informants topic[4].

[1] https://csrc.link/#stop-hunting-sheep
[2] https://csrc.link/#topic=infiltrators-and-informants
[3] https://actforfree.noblogs.org/post/2022/03/12/hamburgermany-incendiary-attack-on-the-car-of-former-police-spy-astrid-oppermann
[4] https://csrc.link/#topic=infiltrators-and-informants

Mitigations

Bug search (p. 48): If a password is being typed in a room where a **hidden camera (p. ??)** may be present, the room can be searched with the appropriate techniques and tools in order to locate and eventually remove such cameras.

Because it's not possible to definitively say that a camera is not present, a user can enter their password while under an opaque sheet or blanket.

Digital best practices (p. 51): Using secure Operating Systems with Full Disk Encryption (FDE) enabled should mitigate authentication bypass attacks. For example, on phones GrapheneOS implements encryption[1] to make guessing the password with brute-force untenable - after 140 failed attempts each is delayed by a full day. In terms of computers, the forensics department of the german federal police was not able to decrypt Linux FDE (called LUKS), used by many Linux systems such as Debian[2] and Tails[3], after a year of effort[4]. FDE on macOS, Windows, iPhone or stock Android should not be relied on.

Tamper-evident preparation (p. 58): Tamper-evident preparation will make it possible to discern when a device has been **physically accessed (p. ??)**.

After a device has been physically accessed by an adversary, it should be considered to be compromised and the user should not authenticate on it ever again. This is because the adversary can image the disk and then compromise the firmware so that as soon as you enter your password, they receive it remotely and can proceed to decrypt the disk image.

Repressive operations

Repression against Zündlumpen (p. 63): In some of the April 2022 raids, immediately after entering, cops seized smartphones and plugged them into power banks, presumably to prevent them from shutting down and going back to an encrypted state[5].

4.21.2 IMSI-catcher

An IMSI-catcher (also referred to as a Stingray) is an eavesdropping device used for intercepting cellular network traffic of all mobile phones in a limited area, including their unique IMSI (International Mobile Subscriber Identity) numbers, as well as all other data (texts, calls, and Internet traffic). It essentially acts as a 'fake' mobile tower between the cell phones and the service provider's real towers.

It can be used for example:

- At a public demonstration, to record the phone numbers of all phones present at the location, and later obtain the names associated with these phone numbers from service providers.
- To intercept the traffic of a target cell phone without having to obtain the cooperation of the service provider through a warrant.
- To intercept the traffic of a target cell phone when the enemy knows where it is used, but doesn't know its phone number.

[1] https://grapheneos.org/faq#encryption
[2] https://debian.org
[3] https://tails.boum.org
[4] https://csrc.link/#observationen-und-andere-argernisse
[5] https://zuendlappen.noblogs.org/post/2022/05/07/muenchen-ueber-razzien-und-ein-%c2%a7129-verfahren-gegen-anarchistinnen-und-den-raub-einer-druckerei

4.20 Targeted ID checks

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

ID checks in the streets preceding or following a riot, around a squat or in a location of struggle can aim to feed intelligence for **network mapping (p. 37)** and incrimination.

Targeted ID checks against specific people can also be an excuse to ask them questions, put pressure on them, or try to take their fingerprints or DNA without their knowledge.

Mitigations

Clandestinity (p. 49): Repressive forces cannot locate people who are in clandestinity for a targeted ID check.

Fake ID (p. 52): If one's official identity is targeted by repression, presenting a fake ID during an ID check can be a solution, as long as the fake ID is not detected as such by the cops.

4.21 Targeted digital surveillance

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

Targeted digital surveillance is employed to compromise the use of digital devices.

Extremely advanced techniques also exist[1] in the arsenal of nation-state actors, though the focus here is on techniques that are more likely to be used.

See the digital surveillance topic[2].

4.21.1 Authentication bypass

Full Disk Encryption (p. 52) is used to protect access to a device - it is what is unlocked during authentication, when you enter your password upon booting a device. This authentication can be bypassed by relying either on human error, weak passwords, or technical exploits.

Ways of bypassing authentication to an encrypted device include:

- accessing the device while it's powered on
- finding the password written down somewhere
- pressuring the device owner into giving the password using legal threats, or in some contexts **extra-legal-violence (p. 23)**
- visual interception: watching the device owner type the password through a **hidden camera (p. ??)** or an **infiltrator (p. 31)**
- brute force: guessing the password through repeated, automated authentication attempts
- compromising the device either through **malware (p. ??)** or **physical access (p. ??)**
- exploiting a flaw at the implementation level of the encryption process

Companies like Cellebrite and Graykey contract out their technology that attacks the authentication on mobile devices, either through exploits or brute force password guessing.

[1] https://anonymousplanet-ng.org/guide.html#some-advanced-targeted-techniques
[2] https://csrc.link/#topic=digital-surveillance

Mitigations

Attack (p. 47): Informants can be attacked when uncovered or years later to dissuade others from cooperating.

Need to know principle (p. 53): The need to know principle makes repression more difficult by controlling the flow of information through networks in order to make them more opaque from the outside and harder to disrupt - if an informant isn't involved in an action, they shouldn't know who was involved even if it's their own roommate.

Network map exercise (p. 54): Evaluating the basis of trust for the various relationships in your network can be a safeguard against placing your trust in individuals who could become informants.

Prisoner support (p. 56): Beyond the ethical imperative to support our prisoners, people are less likely to turn informant when they feel supported and connected to the movements that they risked their freedom for.

4.14 International cooperation

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

Various international organizations (such as Interpol) exist to facilitate sharing information across borders, as well as to arrest and deport fugitives. Intelligence and police agencies from different countries routinely help each other by exchanging information, especially on high-profile cases.

Repressive operations

Scintilla (p. 60): Carla was arrested in France thanks to a cooperation between Italian and French intelligence and police forces[1].

Bialystok (p. 62): In June 2020, comrades were arrested in Spain and France, thanks to a cooperation between italian, spanish and french intelligence and police forces[2].

According to investigation files, during the investigation italian cops tried to target an individual living in Germany[3]. They sent multiple requests to german cops to obtain the extradition of the individual or to have their house searched but the requests were denied.

4.15 Interrogation techniques

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

When interrogating suspects, cops can use a range of interrogation techniques to obtain information from them. This can involve lying, making threats, instilling guilt, shame or pride, trying to appear as friendly or helpful or, on the contrary, as menacing and violent, etc.

For a comprehensive overview of interrogation techniques and how to resist them, see How the police interrogate and how to defend against it[4] (in French and German).

[1] https://attaque.noblogs.org/post/2020/08/06/saint-etienne-arrestation-de-carla-recherchee-dans-le-cadre-de-loperation-scintilla
[2] https://malacoda.noblogs.org/anarchici-imprigionati
[3] https://attaque.noblogs.org/post/2022/02/20/italie-allemagne-de-rome-a-bialystok-en-passant-par-berlin
[4] https://csrc.link/#comment-la-police-interroge-et-comment-sen-defendre

Mitigations

Avoiding self-incrimination (p. 47): Not talking to cops under any circumstance is the best way to resist their interrogation techniques.

4.16 Mass surveillance

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

Mass surveillance includes any surveillance that can be a threat to anarchists but does not have a specific target - the surveillance baseline of our society.

4.16.1 Civilian snitches

A civilian who witnesses a crime and identifies with the state will likely call the police, provide a description of the suspect(s), and potentially even follow them until the police intervene or become a witness in a criminal investigation.

While **reconaissance (p. 57)** can identify the location of **video surveillance cameras (p. ??)**, the habits of a **police patrol (p. ??)**, and a general idea of foot traffic to be expected in the area at different times of the day, avoiding the gaze of civilians often also requires a lookout.

Mitigations

Anonymous dress (p. 46): With anonymous dress, a good citizen should be unable to provide a description of you that would be valuable to police either to facilitate an arrest, or as evidence in court.

Attack (p. 47): If a citizen is following you after an action, they can be scared away with threats or pepper spray. If a citizen is trying to call the police, you can destroy their phone.

Careful action planning (p. 49): Acting at night or in areas with minimal foot traffic will minimize witnesses, and the presence of a lookout can alert to any as soon as they are noticed. Beware of balconies and windows overlooking the scene.

Repressive operations

2019-2020 case against Mónica and Francesco (p. 63): The saleswoman of the cell phone store where Mónica bought a phone that was used as part of the 2020 action, when interrogated by cops, gave a description of a person who investigators matched to Mónica[1].

Belarusian anarcho-partisans (p. 64): While attempting to cross the Belarus-Ukraine border, the anarchists stopped by a shop about 10 kilometers from the border. A shop assistant called the border guards on them, which directly led to their arrest.

4.16.2 Mass digital surveillance

Mass digital surveillance is embedded in the fabric of the technologies of this world, and enables an increasingly granular insight into activities, behaviours, relationships, ideas, and any other valuable data points.

[1]https://csrc.link/#about-orwell-and-the-case-of-monica-and-francisco

your normal routine. Counter-surveillance is a form of active surveillance detection that involves a third-party (not the target of surveillance) watching for signs and/or details of a surveillance effort along a preplanned route.

Transportation by bike (p. 58): Transportation by bike has several advantages for **surveillance detection (p. 57)** and **anti-surveillance (p. 46)**. It is more difficult for a surveillance effort to tail a bike than a car or someone on foot, especially without being detected.

Repressive operations

Nea Filadelphia case (p. 60): The day of the arrests, when one of the comrades visited a cybercafé that was likely under police surveillance, the cops recognized him and started following him[1]. He then moved through the streets of Athens for a few hours, gradually joining the other comrades - some of whom were wanted by the cops[2] - and all of them were arrested.

Repression of the first Jane's Revenge arson (p. 65): In March 2023, cops were covertly observing the comrade who would later be arrested at a distance of approximately 30 meters[3]. The cops observed the comrade discard a paper bag, retrieved it and collected DNA evidence linking the comrade to the crime scene.

The three from the park bench (p. 64): During the evening leading to the arrests, two of the comrades moved through the city on bicycles and were followed by cops on bicycles (and presumably also cops in cars) until their arrest in the park[4]. The cops decided to follow the comrades specifically this evening because it was exactly two years since the G20 summit in Hamburg, and the comrades were suspected of planning an action for the anniversary of the summit. The surveillance had started against one of the accused in March 2018[5].

4.19.2 Overt

Overt physical surveillance targeting a few individuals is rare, and often intended more for creating paranoia as a means of deterring illegal activity rather than incrimination. However, overt physical surveillance of demonstrations and gatherings is standard police practice in order to identify participants, whether to facilitate **network mapping (p. 37)** or to criminally charge individuals for actions carried out during the demonstration.

Mitigations

Anonymous dress (p. 46): Anonymous dress at a demonstration or gathering can prevent an overt surveillance effort from learning your identity.

Repressive operations

Mauvaises intentions (p. 59): During a demonstration, investigators took 180 photos from which they obtained 200 portraits of participants in the demonstration, including ten people that they were able to identify[6].

[1]https://web.archive.org/web/20201027031238/http://actforfree.nostate.net/?p=15472
[2]https://machorka.espivblogs.net/2013/11/06/letter-from-anarchists-argiris-dalios-and-fivos-harisis-from-koridallos-prisons-athens
[3]https://csrc.link/documentation/First Jane's Revenge arson investigation files.pdf
[4]https://csrc.link/#surveillance-and-other-nuisances.html
[5]https://csrc.link/#observationen-und-andere-argernisse
[6]https://infokiosques.net/spip.php?article597

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

4.18 Parallel construction

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

Intelligence and law enforcement agencies do not limit themselves to lawful means in their investigations. Parallel construction is a law enforcement process of building a parallel, or separate, evidentiary basis for an investigation in order to conceal how an investigation was actually conducted.

For example, an intelligence agency collected incriminating digital evidence from a phone without a warrant, so a house raid is carried out to obtain the phone where this evidence can then be 'discovered', so that it is not thrown out during trial for being obtained illegally.

A particular form of parallel construction is evidence laundering, when one police officer gathers evidence illegally and then 'washes' it by passing it to a second officer, who develops it further and delivers it to prosecutors.

4.19 Physical surveillance

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

Physical surveillance can be either covert - when the surveilling individuals do not intend to be detected by their target - or overt when they intend or do not mind being detected by their target.

4.19.1 Covert

Covert physical surveillance is a resource-intensive operation which employs tried-and-true methods that we can understand, take measures against, and potentially detect. A surveillance squad usually has between five and twenty members, and will typically involve staking out the target's house and work, following them when they go out, and the use of **covert surveillance devices (p. 18)** such as video cameras trained on entrances or location devices placed on cars.

See the physical surveillance topic[1].

Mitigations

Anti-surveillance (p. 46): Anti-surveillance is when you take active measures to 'shake off' an identified or possible surveillance effort. It is used as a standard security practice prior to 'protected activities' (anything you don't want a surveillance effort to be able to observe), or when you have identified the presence of surveillance and need to evade them immediately (for example, if you are being tailed by fascists).

Surveillance detection (p. 57): There are three types of surveillance detection: passive, active, and counter-surveillance. Passive surveillance detection involves developing an awareness for indications of surveillance without deviating from your normal routines whatsoever. Active surveillance detection involves the use of preplanned maneuvers intended to reveal a physical surveillance effort - doing something above and beyond

[1]https://csrc.link/#topic=physical-surveillance

The mandates of social control shape everything from how financial transactions are carried out to 'smart' street lamps. The reach of the Internet and digitization into many spheres of life has exponentially multiplied the eyes of the state - from GPS smartphone tracking harvested by data brokers, to biometric screening at borders. Mass digital surveillance aims to collect vast sums of data that can be analyzed for the needs of power; namely, permanent counterinsurgency.

See the digital surveillance topic[1].

Mitigations

Avoiding self-incrimination (p. 47): Self-incriminating information should only ever be on a digital device for very intentional reasons such as to write and send a communique, and always through **Tails (p. 51)**.

Digital best practices (p. 51): Tor[2] renders mass digital surveillance ineffective by anonymizing Internet use. When Tor is not an option, using a VPN will also increase your privacy by routing your Internet traffic through a security-oriented company instead of your Internet Service Provider. Open source and security-oriented Operating Systems and applications limit the data they store or capture about you as much as possible.

Encryption (p. 52): Tor[3] and VPNs encrypt network traffic, preventing observers at certain points in a network from seeing the content.

4.16.3 Routine police surveillance

Police routinely patrol a certain territory, their 'beat' adjacent to their station, in order to establish a visible presence which can provide deterrent effects, and to enable catching people 'red handed'.

In some contexts, unmarked vehicles are used for routine police surveillance as well. Police watch live feeds in CCTV centers, and stand outside of important buildings to watch their surroundings and guard them. International mail is regularly subject to surveillance by customs. ID checks may be used against some people more than others based on racial profiling etc, and ID checks at borders are a way to control the movement of people and to provide a common identifier that can be shared across state and national borders.

Mitigations

Attack (p. 47): In the event of police pursuit after an action, some tactics can slow or stop their chase; crows feet or spike strips, gun fire, barricades, stones, fireworks, etc. A near simultaneous attack on the other side of the neighborhood can serve to distract police patrols. An arson of the cell tower used for their communications would throw all routine police surveillance into disarray.

Reconnaissance (p. 57): Prior to an action, the nearest police station, their shift change schedule, and the patrol patterns can be identified. Routes that are not visible from a police patrol, and which would make a chase difficult (forests, railroad tracks, etc) can be identified.

4.16.4 Video surveillance

Some countries now have more surveillance cameras than citizens. Video surveillance aims to capture the identity of anyone who passes through a space, and to expand its coverage to as much space as possible, for deterrence and incrimination.

[1]https://csrc.link/#topic=digital-surveillance
[2]https://www.torproject.org
[3]https://www.torproject.org

If a crime occurs, relevant video footage can be retroactively analyzed; can the perpetrator be identified by their **face (p. ??)**, **gait (p. ??)**, body characteristics, voice, etc? Was any suspicious activity captured in the period before the crime? Video footage is increasingly processed by algorithms using **facial recognition (p. ??)** to alert authorities to a suspicious behavior or to simply automate the tracking of all individuals throughout their daily lives, to facilitate querying something of interest.

Surveillance cameras can vary widely; in their quality, range, night-vision capacities, the presence of microphones, etc. Many are not integrated into a centrally monitored CCTV network but rather require manually retrieving the footage.

See the topics video surveillance[1] and automated license plate readers[2].

Mitigations

Anonymous dress (p. 46): With anonymous dress, footage from a surveillance camera should be unable to provide a valuable description of you during the action or prior reconnaissance, which could otherwise be used to facilitate an arrest, or as evidence in court.

Anonymous purchases (p. 46): By taking measures to purchase items anonymously, video surveillance from stores should not be able to tie you to materials used in an action.

Attack (p. 47): There are many ways[3] to make surveillance cameras inoperable.

Biometric concealment (p. 48): Avoiding **gait recognition (p. ??)** could involve baggy clothing that conceals body shape, using umbrellas and a 'funny walk' when on surveillance cameras. To avoid **facial recognition (p. ??)**, a mask is used to conceal facial features, and sunglasses or a hat with the brim pulled low are used to conceal eyes.

Outdoor and device-free conversations (p. 54): Sensitive conversations should happen away from surveillance cameras, because they can have microphones.

Reconnaissance (p. 57): The location of surveillance cameras can be identified in advance, and plans can be made to avoid them if possible.

Transportation by bike (p. 58): A bike is much harder to identify than a car, especially if its distinguishing features are minimized. A different stolen bike can be used for each action.

Repressive operations

Repression of the first Jane's Revenge arson (p. 65): CCTV footage helped to identify a vehicle driven by the comrade who would later be arrested, when they were seen entering a parking lot on foot after a demonstration, and the vehicle was seen leaving the same parking lot a few minutes later[4].

2019-2020 case against Mónica and Francesco (p. 63): Public video surveillance footage was extensively used by investigators to reconstruct the movements of Mónica and Francesco during and prior to the attacks, despite the mitigations they were using (taking cabs, changing clothes, wearing disguises)[5].

[1] https://csrc.link/#topic=video-surveillance
[2] https://csrc.link/#topic=automated-license-plate-readers
[3] https://csrc.link/#detruisons-les-cameras
[4] https://csrc.link/documentation/First Jane's Revenge arson investigation files.pdf
[5] https://csrc.link/#about-orwell-and-the-case-of-monica-and-francisco

Repression of Lafarge factory sabotage (p. 65): Investigators obtained CCTV footage of the interior of buses passing close to the action site on the day of the action, which seems to have helped to identify people going to or coming back from the action site[1].

The three from the park bench (p. 64): During the evening leading to the arrests, one of the comrades - while being followed by cops - stopped at a gas station and was seen by the station video-surveillance cameras buying gas and filling up a gas canister[2]. Cops obtained the surveillance footage the following morning.

Prometeo (p. 61): According to the investigation files, two of the accused comrades were seen on a video surveillance camera leaving a shop where investigators believed that the envelopes used to prepare the parcel bombs were bought[3].

4.17 Network mapping

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

Network mapping is the police activity of gaining insight into the connections of any given network, in social and organizational dimensions. It is the reconnaissance stage of police work - understanding a network will enable individuals to be singled out and targeted for extra scrutiny, arrest, or for recruitment as **informants (p. 32)**.

Social media friends lists are the single largest source for this data today, as they do not require warrants.

Mitigations

Avoiding self-incrimination (p. 47): Self-incrimination not only endangers that individual, but also the rest of their network. When possible, refusing to provide police with your identity, photographs, fingerprints or DNA samples can limit their ability to achieve network mapping.

Compartmentalization (p. 50): Using different aliases in distinct contexts can limit the police ability to achieve network mapping. An alias can be specific to a place, a time, or a group of people you interact with.

Digital best practices (p. 51): The social network of an individual can be obscured by limiting digital communications to encrypted devices that are also difficult to infect with malware.

Need to know principle (p. 53): Gossip that could be used for network mapping should be avoided.

Network map exercise (p. 54): As long as they avoid being routed out of networks, infiltrators and informants end up building credentials through association, building intensive social profiles on everyone in the network, finding pressure points to instigate interpersonal and political conflict, entrapping people, and monitoring our daily lives.

Repressive operations

Mauvaises intentions (p. 59): To prove that the accused comrades knew each other, and thus were likely to be accomplices, investigators used several clues[4]:

[1] https://sansnom.noblogs.org/archives/16831
[2] https://csrc.link/#surveillance-and-other-nuisances.html
[3] https://ilrovescio.info/2020/08/23/uno-scritto-di-natascia-dal-carcere-di-piacenza
[4] https://infokiosques.net/spip.php?article597