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

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

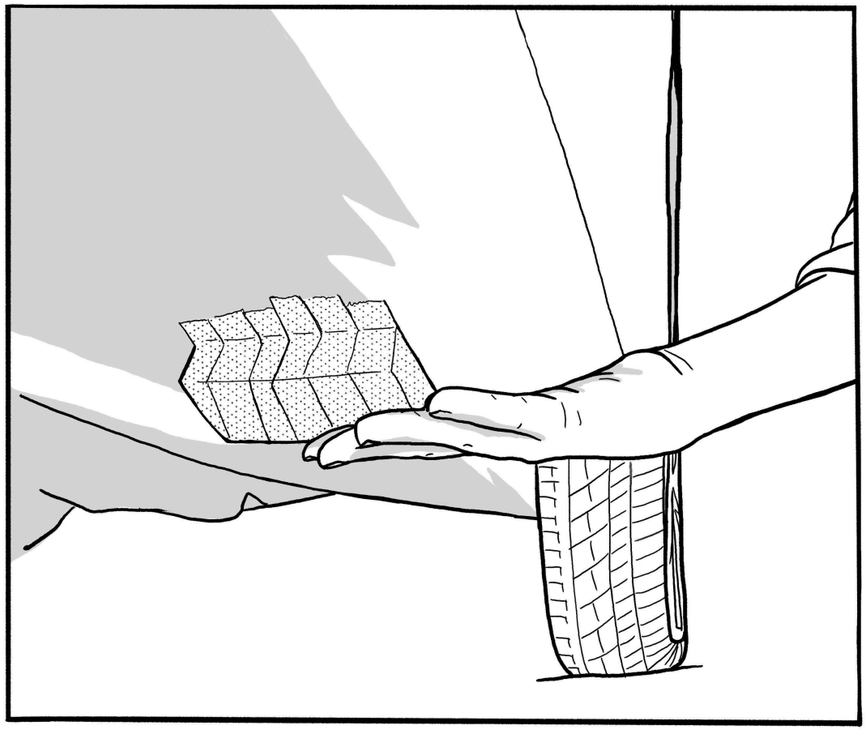
Depending on your context, possession of certain documents may be criminalized or attract unwanted attention—be careful about what zines you print and where you store them.

Threat Library

Part 1/2

Tutorial, Tactics

Techniques



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

Original text in English

No Trace Project

notrace.how/threat-library

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

April 18, 2025

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

to prove that the alias belonged to him.[136]

Mitigations

Compartmentalization (#2): An adversary can establish links between different digital identities through the footprints left by their network traffic. To mitigate this, you can compartmentalize different digital identities by:

- Using Tails[8] and rebooting between each session.
- Using Qubes OS[137] with different Whonix[138] virtual machines that you use non-simultaneously.

Digital best practices (#2): You can follow digital best practices, and in particular use Tor,[93] to make it harder for an adversary to monitor and analyze your network traffic.

Encryption (#2): You can encrypt "in-motion" data to make it harder for an adversary to analyze the data with network forensics.

Repressive operations

2011-2013 case against Jeremy Hammond (#2): For several days, investigators analyzed the network traffic of the router used by Jeremy Hammond to establish a correlation between:[84]

- The times when the traffic showed usage of the Tor network.
- And the times when Jeremy Hammond's online persona was reported as being online by the informant Sabu.

4.26.5. Physical access

Physical access is the process by which an adversary physically accesses an electronic device in order to access its data or compromise it.

Notable examples of electronic devices that an adversary can physically access include:

- Computers, phones, and storage devices (e.g. hard drives, USB sticks, SD cards).
- Printers, cameras, "smart" TVs.
- Vehicles. For example, navigation systems[139] in modern vehicles can store records of the vehicle location.

If an adversary physically accesses a device, they can:

- Read the device unencrypted data, or its encrypted data if it is turned on (and therefore its **encryption (#2)** is not effective).
- Compromise the device with **malware (p. 57)**.
- Compromise the device with a hardware keylogger.[140]

An adversary can physically access a device:

- During a **house raid (p. 35)** or a **covert house visit (p. 16)**.
- After arresting you if you have the device on you.
- During a border control.
- Through an **infiltrator (p. 38)** or **informant (p. 38)** that has access to the device.

Mitigations

Computer and mobile forensics (#2): You can use computer and mobile forensics to detect when a device has been physically accessed by an adversary.

Digital best practices (#2): You can follow digital best practices to mitigate the risk of an adversary physically accessing your digital devices. For example, if you are going to an event or demonstration and you think that you could be arrested, you should not take your phone with you.

Network map exercise (#2): An adversary could physically access your digital devices through an **infiltrator (p. 38)** or **informant (p. 38)**. To mitigate this, you can conduct a network map exercise to help you decide who you trust to access your digital devices.

Physical intrusion detection (#2): You can use physical intrusion detection to detect when a space has been physically accessed by an adversary.

Tamper-evident preparation (#2): You can use tamper-evident preparation to detect when something has been physically accessed by an adversary.

[136] https://medium.com/beyond-install-tor-signal/case-file-jeremy-hammond-514facc780b8
[137] https://qubes-os.org
[138] https://whonix.org
[139] https://en.wikipedia.org/wiki/Automotive_navigation_system
[140] https://en.wikipedia.org/wiki/Hardware_keylogger

4.26.3. Malware

Malware is malicious software installed on a digital device such as a computer, server, or mobile phone, to compromise the device. Malware can do many different things, but against anarchists and other rebels, it typically aims to gain visibility into the compromised device through remote screen capture and remote keylogging (recording the keys pressed on a keyboard), and to track the location of the device (in the case of phones).

Malware can be installed on a device:

- Remotely, typically through phishing[130] via email or text-based messages (SMS, etc.) To be effective, phishing often requires the target to open a malicious file or link.
- By **physical accessing (p. 58)** the device.

See the "Targeted malware" topic.[131]

Mitigations

Compartmentalization (#2): If an adversary installs malware on a Tails[8] USB stick or a Qubes OS[132] virtual machine that you use for different digital identities, they can tie the different identities together. To mitigate this, you can use different Tails USB sticks or Qubes OS virtual machines for different digital identities.

Computer and mobile forensics (#2): You can use computer and mobile forensics to detect traces of malware on a device on which malware is or was installed.

Digital best practices (#2): You can follow digital best practices to make it harder for an adversary to install malware on your digital devices. For example, you can:

- Follow best practices against phishing to make it harder for an adversary to trick you into installing malware on your digital devices.
- Use Tor[93] or a VPN to make it harder for an adversary to remotely install malware on your digital devices through a targeted network injection.[133]

Encryption (#2): You can encrypt "in-motion" data to make it harder for an adversary to install malware through *network packet injection*, an installation vector for some malware, such as Pegasus.[134]

[130]https://en.wikipedia.org/wiki/Phishing
[131]https://notrace.how/resources/#topic=targeted-malware
[132]https://www.qubes-os.org
[133]https://en.wikipedia.org/wiki/Packet_injection
[134]https://forbiddenstories.org/about-the-pegasus-project

Repressive operations

Scripta Manent (#2): Malware was installed on the computer of one of the defendants.[135] The malware, which was installed remotely over the Internet, targeted a Windows computer and was capable of recording text typed on the keyboard, taking periodic screenshots, and recording communications sent and received to and from the computer.

Repression of Lafarge factory sabotage (#2): Investigators made five requests to remotely install spyware.[42] Of these, one installation was successful (on an iPhone SE 2020) and provided access to a Signal group conversation.

4.26.4. Network forensics

Network forensics is the monitoring and analysis of network traffic.

Network information is volatile, it is designed to be transmitted and then lost, so monitoring it requires a proactive approach. Many countries have built network monitoring centers that store massive amounts of network information for days, months, or years to be analyzed later. An adversary can also monitor your network traffic with the **collaboration of your Internet Service Provider (p. 52)**, by compromising your home router with **malware (p. 57)**, or by monitoring your wired or wireless network connection from a surveillance vehicle outside your home.

Because most websites, email providers, and messaging applications use SSL/TLS encryption (the "s" in "https"), an adversary monitoring your network traffic usually knows what websites you visit, but not what you do on those websites. If you use Tor,[93] an adversary monitoring your network traffic knows that you use Tor, but not what websites you visit or what you do on those websites.

Tor is vulnerable to correlation attacks, but such attacks are difficult to set up even for powerful adversaries. An example of a successful correlation attack is the prosecution of anarchist hacker Jeremy Hammond: the times when the alias he used in chat rooms was "online" (obtained through network traffic analysis) were correlated with the times when a **physical surveillance (p. 45)** operation observed him at home

[135]https://earsandeyes.noblogs.org/post/2019/01/27/more-precisions-keylogger-italy

Contents

1. About the Threat Library 4
1.1. Threat modeling 4
1.2. The Threat Library 4
1.3. Limitations 4

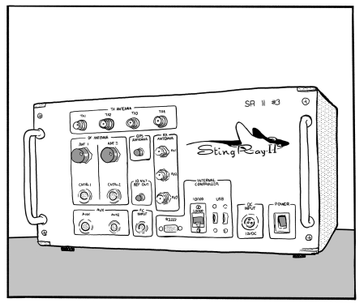
2. Tutorial: Suggested Use of the Threat Library with Attack Trees 6
2.1. A simple example: skipping a school day 6
2.2. A real example: a riot in a big city in the United States 7
2.2.1. Draw the attack tree 7
2.2.2. Identify techniques 11
2.2.3. Identify mitigations 11
2.2.4. Decide how to implement mitigations 12
2.2.5. Burn or digitize your notes 12
2.2.6. Conduct an action review 12
2.3. Assessing risk 12
2.3.1. Impact 13
2.3.2. Likelihood 13
2.3.3. Adversary resources increase risk 13
2.3.4. Mitigations decrease risk 13
2.3.5. Risk and local context 13
2.4. Additional tips on using the Threat Library 13

3. Tactics 14
3.1. Deterrence 14
3.2. Incrimination 14
3.3. Arrest 14

4. Techniques 15
4.1. Alarm systems 15
4.2. Biased interpretation of evidence 15
4.3. Covert house visit 16
4.4. Covert surveillance devices 17
4.4.1. Audio 17
4.4.2. Location 18
4.4.3. Video 19
4.5. Detection dogs 20
4.6. Door knocks 22
4.7. Doxing 22
4.8. Evidence fabrication 22
4.9. Forensics 23
4.9.1. Arson 23
4.9.2. Ballistics 24
4.9.3. DNA 24
4.9.4. Digital 26
4.9.5. Facial recognition 27
4.9.6. Fingerprints 27
4.9.7. Gait recognition 28
4.9.8. Handwriting analysis 30
4.9.9. Linguistics 31
4.9.10. Trace evidence 32

4.10. Guards 35
4.11. House raid 35
4.12. ID checks 37
4.13. Increased police presence 37
4.14. Infiltrators 38
4.15. Informants 38
4.16. International cooperation 39
4.17. Interrogation techniques 40
4.18. Mass surveillance 41
4.18.1. Civilian snitches 41
4.18.2. Mass digital surveillance 41
4.18.3. Police files 42
4.18.4. Video surveillance 42
4.19. Network mapping 44
4.20. Open-source intelligence 45
4.21. Parallel construction 45
4.22. Physical surveillance 45
4.22.1. Aerial 45
4.22.2. Covert 46
4.22.3. Overt 49
4.23. Physical violence 49
4.24. Police patrols 50
4.25. Service provider collaboration 51
4.25.1. Mobile network operators 51
4.25.2. Other 52
4.26. Targeted digital surveillance 54
4.26.1. Authentication bypass 54
4.26.2. IMSI-catcher 56
4.26.3. Malware 57
4.26.4. Network forensics 57
4.26.5. Physical access 58

4.26.2. IMSI-catcher



An IMSI-catcher (also known as a *Stingray*) is a device used to collect information about all mobile phones that are turned on in a limited area (from a few meters to several hundred meters) around it. A passive IMSI-catcher simply listens to the traffic, while an active IMSI-catcher acts as a "fake" cell tower between the phones and the legitimate cell towers.

An IMSI-catcher can collect the following information about the phones around it:

- Their numbers.
- Their IMSI[120] and IMEI[117] numbers.
- Data and metadata about their activity: the content of SMS and regular calls, the list of visited websites, metadata about the use of end-to-end encrypted messaging applications (e.g. when Signal is used and the approximate size of messages sent or received through Signal).

An adversary can use an IMSI-catcher to link people and phone numbers. For example:

- At a public demonstration, to record the phone numbers of all the phones present at the demonstration and later obtain the names associated with those phone numbers through the **collaboration of mobile network operators (p. 51)**.
- As part of a **physical surveillance (p. 45)** operation to record the target's phone number or the phone numbers of people in contact with the target.

An adversary can also use an IMSI-catcher to record phone activity. For example:

- To record the activity of a target phone without requiring the collaboration of the mobile network operator (which, in some contexts, may require a warrant).
- To record the activity of a target phone when the adversary knows where the phone is being used, but doesn't know its phone number.

See the "IMSI-catchers" topic.[129]

Mitigations

Bug search (#2): You can conduct a bug search to detect the presence of an IMSI-catcher.

Detecting the presence of an IMSI-catcher can have several benefits:

- The presence of an IMSI-catcher is a valuable clue as to the level of surveillance employed by an adversary.
- If the IMSI-catcher is used during an event or demonstration, its presence can help you persuade participants to turn off their phones.
- You can destroy the IMSI-catcher (professional IMSI-catchers can be very expensive).

Encryption (#2): You can encrypt a phone "in-motion" data so that if the data is collected by an IMSI-catcher, it cannot be analyzed. For example, you can use end-to-end encrypted messaging applications instead of legacy texts and calls for your phone communications.

Repressive operations

Case against Boris (#2): Investigators used IMSI-catchers during **physical surveillance (p. 45)** operations to identify the phone numbers of people Boris was meeting with—and then identified those people by asking mobile network operators for the names corresponding to the phone numbers.[26]

Repression against Zündlumpen (#2): Investigators used an IMSI-catcher to identify the phone number of a person's mother. They used it both at the mother's home and at her workplace: the correlation of the two uses allowed them to identify the phone number.[39]

Bure criminal association case (#2): Investigators used IMSI-catchers to identify the phone numbers of people who lived in places associated with the struggle against Cigéo or who participated in demonstrations.[21]

December 8 case (#2): Investigators used an IMSI-catcher during **physical surveillance (p. 45)** operations to identify the phone numbers used by some of the defendants.[24]

[129] https://notrace.how/resources/#topic=imsi-catchers

- Making the device owner provide the encryption password by using **interrogation techniques (p. 40)** including, in some contexts, **physical violence (p. 49)**.
- Visual interception: watching the device owner type the encryption password through a **hidden camera (p. 19)** or an **infiltrator (p. 38)** or **informant (p. 38)**.
- Brute force: guessing the encryption password through repeated, automated authentication attempts.
- Compromising the device either through remotely-installed **malware (p. 57)** or **physical access (p. 58)**.
- Exploiting a flaw at the implementation level of the encryption process.

Mitigations

Bug search (#2): Before entering a password in a room where **covert video surveillance devices (p. 19)** may be present, you can conduct a bug search to locate such devices and eventually remove them.

Digital best practices (#2): You can follow digital best practices, and in particular use security-oriented operating systems with Full Disk Encryption (FDE) and strong passwords, to make it harder for an adversary to bypass authentication on your digital devices. For example:

- On computers, you can use the Linux FDE called LUKS, which is used by many Linux systems, such as Debian[122] and Tails,[8] and which the forensics department of the German federal police was unable to decrypt after a year of effort.[123]
- On phones, you can use GrapheneOS, whose FDE makes it difficult for an adversary to guess the encryption password by brute force: after 140 failed attempts, each is delayed for a full day.[124]

Tamper-evident preparation (#2): You can use tamper-evident preparation to detect when a device has been **physically accessed (p. 58)**.

Once a device has been physically accessed by an adversary, you should consider it compromised and never authenticate to it again. This is because, in a worst-case scenario, the adversary may have copied the device's data and compromised its firmware so that when you enter your password, they can remotely obtain it and use it to decrypt the data.

Repressive operations

Repression against Zündlumpen (#2): In some of the April 2022 raids, police seized smartphones immediately after entering and plugged them into power banks, presumably to prevent them from shutting down and reverting to an encrypted state.[125]

Repression of Lafarge factory sabotage (#2): Investigators seized several encrypted smartphones in the raids and attempted to access their encrypted data, with varying results depending on the phone:[42]

- For the iPhones that were seized turned on, they exploited the security vulnerabilities that exist when they are turned on to bypass their encryption and access the encrypted data.
- For all Android phones (whether recovered on or off) and one iPhone seized off, they extracted the phones' encrypted partitions and attempted to brute force them from a computer.

2011-2013 case against Jeremy Hammond (#2): Investigators bypassed the authentication of Jeremy Hammond's encrypted laptop, that they had seized in the March 2012 raid.[126] They seemingly achieved the bypass by guessing the laptop's password, which was a very simple password—either "chewy123"[127] or "chewy12345".[128]

Bure criminal association case (#2): Investigators bypassed the authentication of five encrypted storage devices found in raids:[21]

- One hard drive by using the very simple password "stopcigeo", which they presumably guessed.
- One hard drive by using a password they found on a post-it note under the computer containing the hard drive.
- One hard drive by using a password given to them in custody by the owner of the computer containing the hard drive.
- Two hard drives by using passwords they found in a text document on a previously decrypted hard drive.

[122] https://debian.org
[123] https://notrace.how/resources/#parkbank
[124] https://grapheneos.org/faq#encryption
[125] https://actforfree.noblogs.org/2022/05/13/munich-germany-about-raids-and-a-%c2%a7129-procedure-against-anarchists-and-the-theft-of-a-printing-space
[126] https://apnews.com/domestic-news-domestic-news-general-news-abae6d15cbf04d75bbbc58225a470f98
[127] According to press reports.
[128] According to *American Kingpin* (Nick Bilton, 2017).

1. About the Threat Library

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

1.1. Threat modeling

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

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

1.2. The Threat Library

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

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

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

1.3. Limitations

The Threat Library is by design a very technical approach to anti-repression. Threat modeling is done at the level of actions, and thus does not attempt to contribute to the social question, how to escape the enclosure that repression seeks, how to intervene in social tensions, and so on. Struggles for freedom are not primarily a technical matter, but a social one, and have psychological and emotional effects. As much as possible, we encourage you to take time before, during and after an action to discuss with all the people

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

[2] In fact, the vast majority of anarchist direct actions are not successfully prosecuted. Frustrated investigators in Bremen, Germany,[3] and Grenoble, France,[4] have spoken to the media about their failure to repress any of the arsons that have taken place in both locations over the years, which they attribute to the mitigations taken by the arsonists.

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

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

involved and to make sure that everyone's emotional needs are taken into account.

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

- Seize Louna's clothing while she was hospitalized.[72]
- Obtain the phone number of someone close to Louna that Louna had given to the hospital.
- Obtain CCTV footage from the hospital.
- Obtain information from the hospital's parking payment system.
- Learn the time and place of an appointment Louna had at the hospital a few days after the arson.

Investigators also used the collaboration of several State institutions:

- The Agence nationale des titres sécurisés (ANTS, *National agency for secured documents*) provided scans of identity documents and applications for renewal of identity documents.
- Health insurance organizations provided the personal information of people under investigation and their partners.
- The tax authorities provided the purchase and sale files of houses of Louna's parents and grandparents.

Investigators used the collaboration of several companies:

- Banks provided:
  - Bank information of several people, including many members of Louna's family.
  - IP addresses used to make online bank transfers.
  - Locations where people had withdrawn cash.
- An insurance company provided a person's address and list of roommates.
- The highway operator Vinci provided CCTV footage of highway toll booths.
- The French national railway company (SNCF) provided information about people who had booked seats next to people under investigation, including their photos and bank information.
- The carpooling service BlaBlaCar provided information about people who had used the service, including their photos, bank information, and the trips they had taken.
- The car manufacturer Stellantis provided the IMSI[120] and IMEI[117] numbers of a car's embedded location system. However, investigators were unable to locate the car because, for some unknown reason, it did not transmit its location.

Investigators asked a social housing landlord and a real estate agency to provide them with access cards to apartment buildings.

Bure criminal association case (#2): Investigators used the collaboration of banks to obtain the bank records of organizations fighting against Cigéo.[21] The bank records of one organization included a 500€ transfer entitled "*participation manif 18 fev*" ("*contribution to the February 18 demonstration*"), in reference to a demonstration in which people attacked a building associated with Cigéo.

The owner of a supermarket in a town about 20 km from Bure told investigators that he had seen customers buying an unusually large amount of denatured alcohol (15 liters), and gave the receipt to the investigators.

4.26. Targeted digital surveillance

Used in tactic: **Incrimination**

Targeted digital surveillance is the targeted collection and analysis of digital data and communications.

Extremely advanced techniques exist[121] in the arsenal of nation-State actors, but the focus here is on techniques that are more likely to be used against anarchists and other rebels.

See the "Digital surveillance" topic.[92]

4.26.1. Authentication bypass

Authentication bypass is the process by which an adversary bypasses the **Full Disk Encryption (#2)** that protects access to a digital device. An adversary can achieve authentication bypass through human error, weak passwords, or technical exploits.

An adversary can achieve authentication bypass in the following ways:

- Accessing the device while it is turned on (and therefore its encryption is not effective).
- Finding the encryption password written down somewhere.

[120] An International Mobile Subscriber Identity (IMSI) number is a number that uniquely identifies a SIM card.

[121] https://anonymousplanet.org/guide.html#some-advanced-targeted-techniques

Online services

Websites, email providers, and other online services can provide:

- The content of unencrypted communications you make through the service (e.g. social media posts, unencrypted emails).
- Metadata about encrypted communications you make through the service (e.g. the sender, recipient, and date of encrypted emails).

Postal services

Postal services can allow an adversary to monitor your mail.

State institutions

State institutions can provide any information they have about you, including your address, tax records, health information, etc.

Mitigations

Anonymous purchases (#2): If you need to purchase an item in a store, you can purchase it anonymously to make it harder for an adversary to use the collaboration of the store to link your identity to the item.

Digital best practices (#2): You can follow digital best practices to make it harder for service providers to provide useful information to an adversary. For example, you can:

- Use Tor[93] to make it harder for your Internet Service Provider to provide useful information about your Internet activity to an adversary.
- Use trusted online services[119] that will refuse to comply with an adversary's requests to access your data, or build their service to make it technically impossible to comply with such requests.

Encryption (#2): You can encrypt "in-motion" data to make it harder for service providers to provide useful information to an adversary.

Repressive operations

Case against Boris (#2): Investigators used the collaboration of an email provider to gain real-time access to an email address used by Boris: they were able to see emails sent and received in real time.

Repression against Zündlumpen (#2): Investigators used the collaboration of banks to:[39]

- Analyze the bank records of a suspected editor of the newspaper, including bank records as old as 8 years, to determine if the person had purchased printing equipment.
- Obtain, in real time, the locations of cash withdrawals made by a person they wanted to locate. When a cash withdrawal took place, investigators would send a patrol to the withdrawal location to try to locate the person. However, this did not work, seemingly because the patrol always arrived too late.
- Reduce the maximum cash withdrawal limit of a person they wanted to locate in order to force her to make more withdrawals and increase the opportunities of locating her.

Investigators asked several companies to provide information about a person:

- Mail order companies were asked to provide the shipping addresses used by the person.
- PayPal, Ebay, and similar companies were asked if the person had an account with them and, if so, which addresses were associated with the account.
- The German national railway company (Deutsche Bahn) and the bus operator FlixBus were asked to provide information about the person's travels.
- The person's former vocational school was asked to provide the list of participants in the school's courses, presumably to identify possible contacts of the person.

Repression of Lafarge factory sabotage (#2): Investigators gave the serial number of a camera to the camera manufacturer, and the manufacturer gave them the name of the store where the camera was sold.[42] This helped investigators identify a person they accused of taking photos with the camera.

Case against Peppy and Krystal (#2): A fireworks store provided investigators with records showing that Peppy had purchased fireworks from the store three days before the protest.[14]

Case against Louna (#2): Investigators used the collaboration of the hospital to:

- Learn that a person (Louna) was hospitalized for burns.[21]
- Obtain Louna's medical file.

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

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

There is a lot of information in the Threat Library. It can be overwhelming. How can you use the Threat Library in your life, in a particular project, or when carrying out actions? This tutorial is designed to help you navigate the Threat Library using *attack trees*.[5]

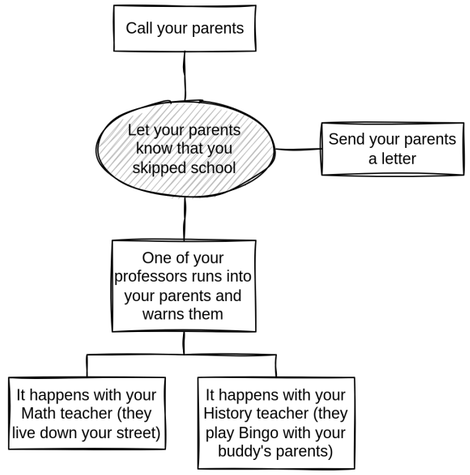
Attack trees are a tool to facilitate a brainstorming exercise on the different ways an adversary could successfully attack you in a given context by representing the attacks—the threats—in a tree structure. They help understand how a plan or project is vulnerable to repression by modeling the options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

You can do this *threat modeling* exercise on your own, but, if you're planning to carry out an action with other people, we recommend that you do it with them. This exercise should benefit both inexperienced and experienced crews. Even if everyone already has strong security practices, it provides a structured way to ensure that no threats are overlooked and that everyone is on the same page about security expectations.

2.1. A simple example: skipping a school day

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

You start by drawing the root node: it represents the adversary's goal. In this example, the goal is to let your parents know that you skipped school. The school could call your parents or send them a letter. Or one of your professors could run into your respective parents and warn them—this could happen with your Math teacher who lives down your street, or your History teacher who plays Bingo with your buddy's parents every weekend. You draw all these nodes (1).



(1) "Skipping school" attack tree.

For a node to be true, one of its successors must be true. For example, for "Let your parents know that you skipped school" to be true, one of the three nodes around it must be true. For "One of your professors runs into your parents and warns them" to be true, one of the two nodes below it must be true. In other words, if you can trace a path from an outermost node to the root node where all the nodes along the path are true, that means that the root node is true, and the attack is complete.

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

[5] For another approach to threat modeling that can also serve as a tutorial to the Threat Library, see Threat Modeling Fundamentals.[6]

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

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

Let's say you and some comrades are preparing for a riot in a big city in the United States. You want to do some damage, but you don't want to get caught… You turn to the Threat Library for help. You print out this zine, take a pen and paper, and meet with your comrades **outdoors and without electronic devices (#2)**.

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

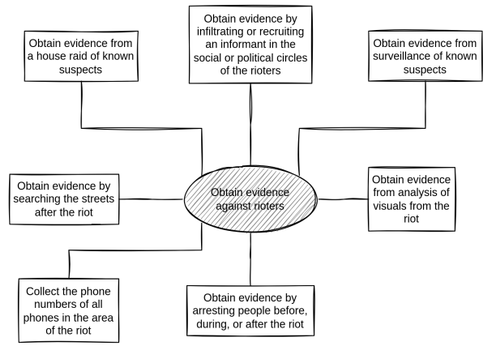
2.2.1. Draw the attack tree

In this example, the adversary is the State and its cops, and their goal is to get enough evidence of your involvement in the riot to convince a judge to convict you. You draw an attack tree to represent the ways they could achieve this goal.[7] You begin with the root node (2).

(2) "Riot" attack tree (root node).

You then add the immediate nodes, next to the root node (3). At this stage, you should add anything you can think of, even if you're not sure it applies to your context. You can grow the tree in all directions, to make it more compact.

[7]For complex actions, you may want to make a temporal distinction and draw an attack tree for each step of the action (e.g. planning, preparation, execution, dissolution).



(3) "Riot" attack tree (first nodes).

You use the Threat Library to help grow the tree—reading about techniques helps you better understand all the options available to your adversary. Creating attack trees requires a certain mindset and takes practice. The tree is complete when no more nodes are needed to complete an attack, and every attack that you can think of is represented (4).

Repressive operations

Case against Boris (#2): Investigators used the collaboration of mobile network operators to intercept calls from Boris's phone or the phones of people close to him.[26] They regularly listened to the intercepted calls in real time and used information from the calls to adjust ongoing **physical surveillance (p. 45)** operations.

Mauvaises intentions (#2): Investigators used the collaboration of mobile network operators to link phone numbers to civil identities, to know which phone numbers were in contact with each other, to geolocate phones (both retrospectively and in real time) and to record phone calls.[44]

Case against Louna (#2): Investigators used the collaboration of mobile network operators to geolocate approximately 30 phones and intercept their calls in real time.[21] In particular, investigators used the intercepted calls to:

- Hear about a meeting outside apartment buildings, set up physical surveillance of those buildings, and arrest two people who went to the meeting.
- Hear Louna make an appointment with a doctor, then contact the doctor to obtain Louna's personal information, including her address and phone number.

Bure criminal association case (#2): Investigators used the collaboration of mobile network operators to:[21]

- Establish links between people.
- Geolocate phones in real time.
- Record a large number of phone conversations, including conversations that took place between the moment a call was placed and the moment it was answered (i.e., while the phone was ringing).
- Identify the phone numbers that were active around Bure during three demonstrations that took place there in February, June, and August 2017, including 55 numbers that were active during all three demonstrations.

December 8 case (#2): Investigators used the collaboration of mobile network operators to geolocate the phones of the defendants and of people close to them in real time and to record unencrypted phone conversations.[24] In particular:

- In one case, investigators could not determine the phone number used by one of the defendants, but had determined that the defendant often moved around with another person, so they geolocated the other person's phone in real time to locate the defendant.
- In one case, investigators followed one of the defendants as part of a **physical surveillance (p. 45)** operation, but lost sight of them. In the following hour, they geolocated the defendant's phone in real time to locate them. As a result, one hour after losing sight of the defendant, investigators regained sight of them and resumed the physical surveillance operation.

4.25.2. Other

Service providers other than mobile network operators can provide information about you to an adversary.

Stores

Physical and digital stores can provide information about purchases made through the store, including:

- Given a name: the items purchased under that name, as well as the dates of the purchases.
- Given an item or category of items: the names of the people who purchased the item, as well as the dates of the purchases.

Additionally, physical stores can provide:

- CCTV footage from cameras operated by the store.
- Testimony from store employees, for example about the physical appearance of a person who made a particular purchase.

Banks

Banks can provide:

- Your bank account activity, including the date, location and amount of any purchase or withdrawal you make with a card.
- CCTV footage from cameras on Automated Teller Machines (ATMs).

Internet service providers

Internet service providers can provide:

- If you follow **digital best practices (#2)** and use Tor: metadata about your Internet activity, such as when you use Internet.
- If you don't use Tor: your Internet activity, including the list of websites you visit.

4.25. Service provider collaboration

Used in tactic: **Incrimination**

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

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

- Spain, a State with a high degree of control over companies located within its jurisdiction, can very easily compel Spanish mobile network operators to provide information on Spanish mobile network users.
- Iran, a State with no diplomatic relations with Canada, cannot compel the Canada Revenue Agency to provide information on Canadian taxpayers.

Both non-State adversaries and the State can obtain service provider information through:

- Corruption: purchasing service provider information sold by corrupt individuals with access to the information (e.g., service provider employees, police officers).
- Data leaks:[116] obtaining service provider information through unauthorized exposure, disclosure, or loss of the information (e.g., a service provider database is hacked and an adversary buys it on the black market).

4.25.1. Mobile network operators

Mobile network operators can provide information about you to an adversary.

They can provide:

- Given a name: the phone numbers registered under that name.
- Given a phone number: the name under which the phone number is registered and the IMEI number[117] of the phone in which the phone number is used.
- Given an IMEI number: the phone number that is used in the phone with that IMEI number.

Additionally, given your phone number, mobile network operators can provide (current and historical) data and metadata about your phone activity:

- The content of SMS and regular calls you make on your phone.
- The list of websites you visit on your phone.
- Your phone physical location.
- Metadata about your use of end-to-end encrypted messaging applications (e.g. when you use Signal and the approximate size of messages sent or received through Signal).

This means that any of the following conditions can allow an adversary, with the collaboration of mobile network operators, to access (current and historical) data and metadata about your phone activity:

- Knowing your name (if your phone is not **anonymous (#2)**).
- Knowing your phone number, which they can find by monitoring or seizing a phone in contact with yours, using an **IMSI-catcher (p. 56)**, or through advanced correlation techniques.[118]
- Knowing your phone IMEI number, which they can find by seizing your phone.

Mitigations

Anonymous phones (#2): You can use anonymous phones to make it harder for mobile network operators to provide useful information to an adversary.

Digital best practices (#2): You can follow digital best practices to make it harder for mobile network operators to provide useful information to an adversary. For example, you can:

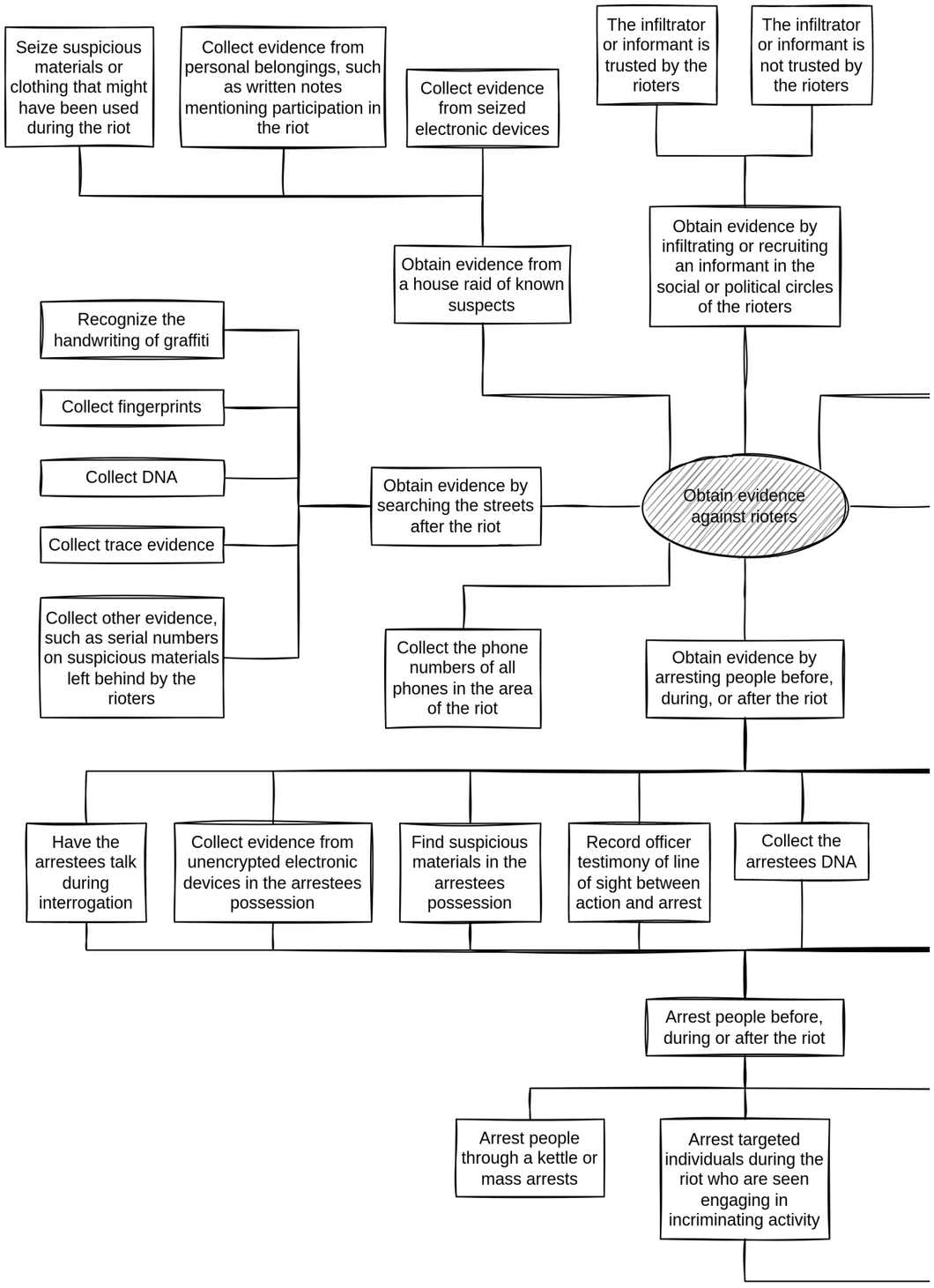
- Not use a phone, or leave your phone at home.
- Use end-to-end encrypted messaging applications on your phone, instead of traditional SMS and calls.

Encryption (#2): You can encrypt "in-motion" data to make it harder for mobile network operators to provide useful information to an adversary.

[116] https://en.wikipedia.org/wiki/Data_breach

[117] An International Mobile Equipment Identity (IMEI) number is a number that uniquely identifies a phone.

[118] For example, if an adversary knows that you were in place A on Monday and in place B on Tuesday, and they know from cell tower data that a particular phone was the only phone that was also in place A on Monday and in place B on Tuesday, they can deduce the phone is yours.



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

to charge and convict them.[113] Most of the defendants who were tortured later retracted their statements and spoke publicly about the torture they had received.

Renata (#2): During a house raid, one of the arrested people was forced to his knees by a cop who put a gun to his temple.[70]

Belarusian anarcho-partisans (#2): The people were tortured in the first days of their detention.[114]

Warsaw 3 (#2): The people were tortured during their arrest and in the first hours of their detention.[89]

Case against Ruslan Siddiqi (#2): Ruslan Siddiqi was tortured for several days after his arrest.[90]

The torture included:[115]

Repression of the 2019 uprising in Chile (#2): In the streets and in custody, police forces and soldiers injured, sexually assaulted, raped, tortured and killed many protesters in what appeared to be a strategic attempt to deter participation in the uprising.[106]

4.24. Police patrols

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

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

Means of transportation

Police patrols can use different means of transportation:

- Marked or unmarked vehicles.
- Foot movement.
- **Helicopters, drones and surveillance planes (p. 45)**.

Routine patrols

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

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

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

[115] beatings and electric shocks.

Patrols in response to a threat

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

- A routine patrol stumbling upon the threat by chance.
- **Guards (p. 35)** or **civilians (p. 41)**.
- An **alarm system (p. 15)** (e.g. motion detectors inside a building), either directly or through a security company monitoring the alarm system.
- Police officers monitoring live **CCTV footage (p. 42)**.
- An **infiltrator (p. 38)** or an **informant (p. 38)**.

Mitigations

Attack (#2): The police can disturb an action. To mitigate this, you can distract them by launching a near-simultaneous attack on the other side of the neighborhood, or disrupt their communications by burning the cell tower used for police communications.

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

Careful action planning (#2): You can carefully plan an action to take into account the risk of routine police patrols interfering with the action, a risk that is always present, except perhaps in remote areas.

Reconnaissance (#2): Before an action, you can identify the nearest police station, their shift change schedule, and patrol patterns, and you can identify routes that are not visible to police patrols and that would make pursuit difficult (forests, railroad tracks, etc.)

Repressive operations

Repression against Zündlumpen (#2): Investigators sent a police patrol outside a person's apartment every night at irregular times to check if she was at her apartment.[39]

the other people—some of whom were wanted by police[111]—and all of them were arrested.

Case against Direct Action (#2): For several weeks, investigators followed members of Direct Action and some of their friends as they moved on foot and in vehicles.[15]

On at least one occasion, investigators witnessed a member of Direct Action conducting **anti-surveillance (#2)** maneuvers, which they found suspicious.

December 8 case (#2): For several weeks, investigators staked out the homes of some of the defendants and tailed them when they moved.[24] In particular:

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

4.22.3. Overt

Overt physical surveillance is the direct observation of people or activities when the surveillance operators intend to be, or do not mind being, detected by their targets. This is common practice at demonstrations and gatherings to identify participants, whether to facilitate **network mapping (p. 44)** or to incriminate individuals for actions carried out during the demonstration.

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

Mitigations

Anonymous dress (#2): You can dress anonymously at a demonstration or other event to make it harder for an overt surveillance operation to identify you.

Repressive operations

Mauvaises intentions (#2): During a demonstration, the investigators took 180 photographs from which they obtained 200 portraits of the demonstrators, including ten people they were able to identify.[44]

4.23. Physical violence

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

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

In some contexts, physical violence can include torture. For example, in Russia and Belarus, several anarchists have been tortured in recent years after being arrested by the State. Reported acts of torture in these countries include:[112]

In some contexts, physical violence can include assassinations.

Mitigations

Preparing for repression (#2): If you or members of your network are at risk of being tortured if you are arrested, you can prepare for that risk. For example:

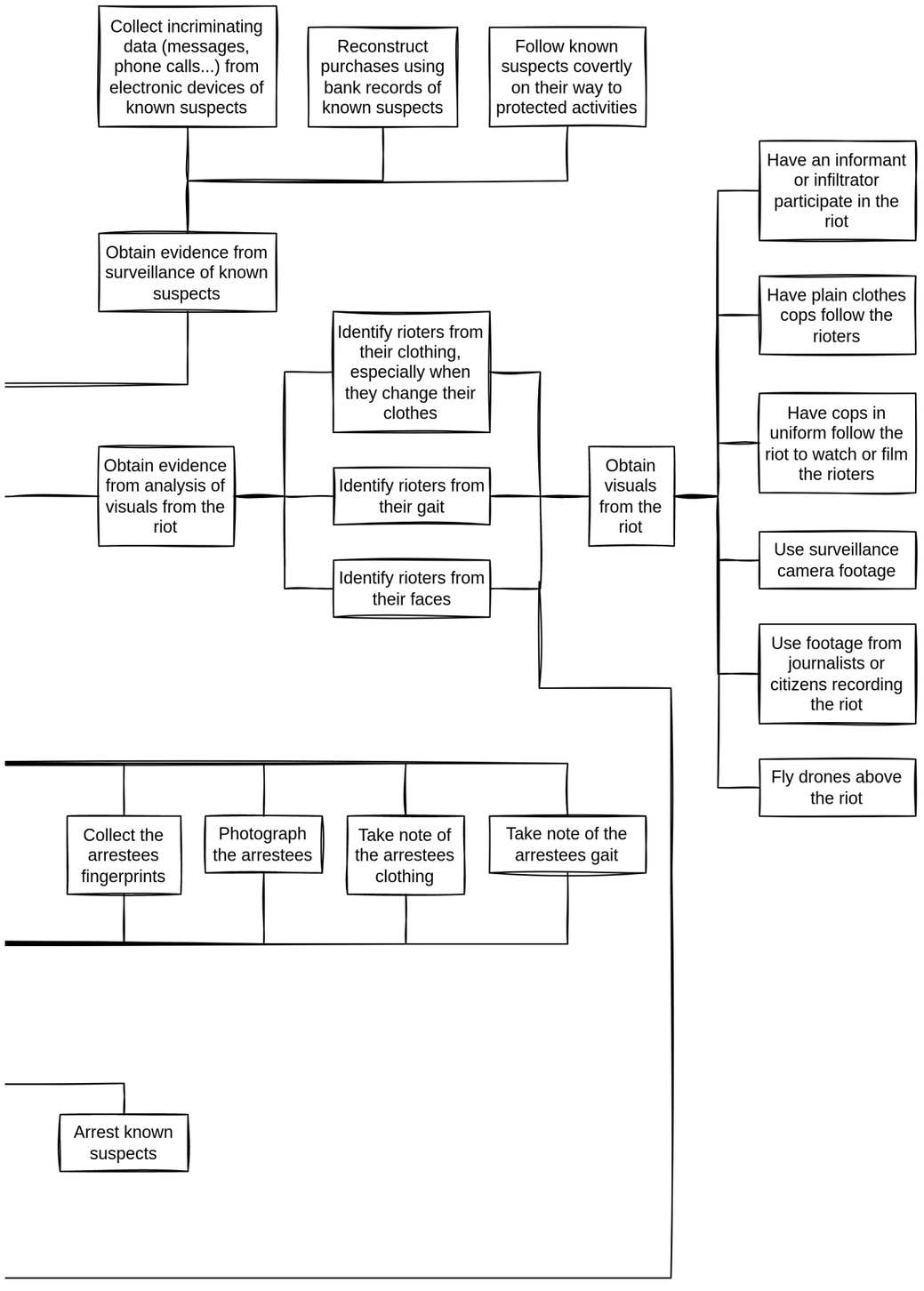
- You can prepare psychologically.
- You can set up protocols in advance that allow the network to learn when someone is missing in order to respond quickly to their disappearance. For example, members of a group may connect to an encrypted messaging application once a day to send each other a message: if a member does not send their daily message, it may mean they have been arrested. Torture often occurs immediately after arrest, while no one knows where the person is and there is no lawyer, so responding quickly after arrest can be crucial.
- Depending on the context, involving a lawyer or publicizing the acts of torture can help put pressure on the authorities to stop.

Repressive operations

Network (#2): Most of the defendants were tortured by the Russian Federal Security Service (FSB) in the early stages of their detention in order to obtain (often fabricated) statements that could later be used

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

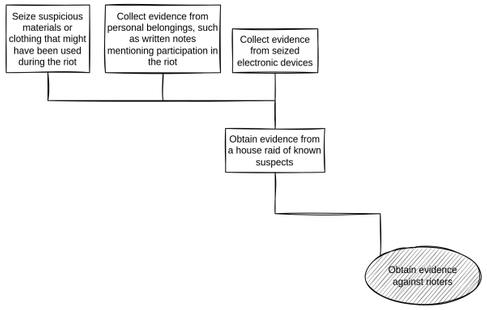
[112] beatings, suffocation with a plastic bag or pillow, pouring water into the nose and mouth, hanging by the legs or by tied hands, electric shocks, torture with a screwdriver, forcing people to do squats until they collapse, sexual violence, and deprivation of sleep, food, and water.



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

2.2.2. Identify techniques

You identify all techniques represented in the tree by matching nodes with techniques from the Threat Library. You do so branch by branch to avoid getting lost: it's best to start with nodes closer to the root node, and then work your way up the branch.



(5) "Riot" attack tree (house raid branch).

You start with the "Obtain evidence from a house raid of known suspects" branch (5):

- "Obtain evidence from a house raid of known suspects" matches **House raid (p. 35)**.
- "Collect evidence from seized electronic devices" matches **Targeted digital surveillance: Physical access (p. 58)** because they would access your electronic devices, and **Targeted digital surveillance: Authentication bypass (p. 54)**, if they try to guess your passwords or break your encryption.
- The other nodes don't match anything, they're just part of the house raid.

At this stage, it can be useful to assess the risks of the techniques you're listing—this will inform whether and how thoroughly you should mitigate each of them. See the section "Assessing Risk", p. 12 for how to assess a technique's risk using the concepts of *likelihood* and *impact*.

Then you move on to the next branch until the whole tree is covered, building a table (6).

Technique	Mitigations	Implementations
House raid (medium risk)		
Physical access (medium risk)		
Authentication bypass (low risk)		

(6) Beginning of the table.

2.2.3. Identify mitigations

Next, you identify the mitigations that you want to implement by looking at the mitigations that the Threat Library suggests for the techniques in the table.

On our example branch (5), you decide to implement:

- For "House raid", **Preparing for repression (#2)**, **Preparing for house raids (#2)** and **Stash spot or safe house (#2)**. You don't want to implement **Clandestinity (#2)** because you decide against going down that road.
- For the two "Targeted digital surveillance" techniques, **Digital best practices (#2)** is the only mitigation that makes sense in your context.

You update the table (7).

Technique	Mitigations	Implementations
House raid (medium risk)	Preparing for repression Preparing for house raids Stash spot or safe house	
Physical access (medium risk)	Digital best practices	
Authentication bypass (low risk)	Digital best practices	

(7) Beginning of the table, with mitigations.

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

Case against Louna (#2): After the arson on the night of May 4 to May 5, 2024, investigators conducted several physical surveillance operations:[21]

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

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

- On October 3, they:
  - Surveilled the homes of Louna's parents and grandparents for 6 hours.
  - Drove by another home of Louna's family several times in a vehicle.
  - Followed a person seen with Louna at the hospital for 4 hours.
- On October 8, they:
  - Surveilled the homes of Louna's parents and grandparents again for 6 hours.
  - Drove by the homes of several members of Louna's family and a person who had accompanied her to the hospital several times.
  - Followed a person seen with Louna at the hospital again for 6 hours.
- On October 10, during the trial of a person opposed to the highway project, they surveilled the interior of the courthouse and the surrounding area.
- On October 12, after hearing about a meeting outside apartment buildings through an intercepted phone call, they surveilled those buildings and arrested two people who went to the meeting, including Louna.

Repression of the first Jane's Revenge arson (#2): In March 2023, cops secretely observed the person from a distance of about 30 meters.[45] The cops watched the person discard a bag, retrieved it, and collected DNA evidence linking the person to the action site.

Case against Jeff Luers (#2): On the night of the June arson, the arsonists were being tailed by a surveillance team—police officers in one or more unmarked cars—as they drove to the arson site.[65] They parked their car close to the arson site, watched by the surveillance team. They got out of their car to continue on foot, at which point the surveillance team lost sight of them. They ran back to their car 10 minutes later, at which point the surveillance team regained sight of them. They drove away from the arson site. More than an hour later, the surveillance team—still tailing the arsonists—heard on the police radio system about a fire at the arson site and asked local police officers to stop the arsonists' car for a roadside check, suspecting that they were involved in the fire. Half an hour later, when fire investigators at the arson site reported that they believed the fire had been set intentionally, the arsonists were arrested.

Bure criminal association case (#2): Investigators:[21]

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

The three from the park bench (#2): During the evening leading up to the arrest, two of the people rode their bikes through the city and were followed by cops on bikes (and presumably also cops in cars) until they were arrested in the park.[98] The cops decided to follow the people specifically that evening because it was exactly two years since the G20 summit in Hamburg and they were suspected of planning an action for the anniversary of the summit.

Nea Filadelphia case (#2): On the day of the arrests, when one person visited a cybercafé that was probably under police surveillance, cops recognized him and started following him.[110] He then moved through the streets of Athens for a few hours, gradually joining

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

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

Examples of mobile physical surveillance techniques include:

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

Mobile physical surveillance may be facilitated by:

- A **tracking device (p. 18)** installed on the target's vehicle or bike.
- Real-time geolocation of the target's phone, obtained with the **collaboration of mobile network operators (p. 51)**.
- **Aerial surveillance (p. 45)**, such as a drone following the target from a distance.

Static

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

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

Arrest

Generally, a surveillance team will not attempt to arrest its target during a covert physical surveillance operation. On rare occasions, however, this may happen if the surveillance team has gathered enough information about the target's activities to incriminate them and deems it necessary to arrest the target immediately (e.g. to prevent a crime).

See also

- Surveillance Countermeasures[107] about the principles and techniques of covert physical surveillance.
- Measures Against Surveillance[108] for insights into how police and intelligence agencies conduct covert physical surveillance.
- The "Physical surveillance" topic.[109]

Mitigations

Anti-surveillance (#2): You can conduct anti-surveillance to evade a covert physical surveillance operation.

Surveillance detection (#2): You can conduct surveillance detection to detect a covert physical surveillance operation.

Transportation by bike (#2): You can use a bike instead of any other type of vehicle: compared to other vehicles or people on foot, a bike is harder to follow by a covert physical surveillance operation, especially without the operation being detected.

Repressive operations

Case against Boris (#2): For several weeks, investigators regularly staked out Boris's home and tailed him as he moved on foot, on bicycles, and in vehicles.[26]

Repression against Zündlumpen (#2): Investigators followed a person for 15 days.[39]

Case against Peppy and Krystal (#2): A week before the protest, investigators conducted covert physical surveillance at a local bookstore where they knew people planning the protest were organizing.[14] They observed Peppy enter the bookstore and leave an hour and a half later.

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

2011-2013 case against Jeremy Hammond (#2): During a physical surveillance operation against Jeremy Hammond's home that lasted several days, investigators established a correlation between:[84]

[107] https://notrace.how/resources/#surveillance-countermeasures
[108] https://notrace.how/resources/#measures-surveillance
[109] https://notrace.how/resources/#topic=physical-surveillance

2.2.4. Decide how to implement mitigations

Finally, you decide how to implement the mitigations in the table. Reading their entries in the Threat Library can give you some ideas. The risk you assessed for each technique helps you to know how much energy to put into the mitigations. You decide on the following implementations:

- "Preparing for repression": Since you and your comrades all live in the same place, there is a risk that you will all be arrested after a house raid. You will make sure that other comrades know how to support you if this happens.
- "Preparing for house raids": You decide to stop storing the fireworks under your bed.
- "Stash spot or safe house": You decide to bury a waterproof container in a nearby forest to store the fireworks. When one of you accesses it, they must wear gloves and make sure there's no one around.
- "Digital best practices": Your devices are already encrypted, and you're not using them to talk about the riots anyway. You have to find out if a phone's encryption works when it's turned on and locked because you're not sure.

At this stage, it can be useful to re-assess the risks of the techniques to make sure that they have been sufficiently lowered by the mitigations you have decided to implement.

You update the table (8).

Technique	Mitigations	Implementations
House raid (~~medium~~ risk) LOW	Preparing for repression Preparing for house raids Stash spot or safe house	Make sure other comrades know what to do in case of house raid: alert lawyers etc. Stop storing fireworks under bed!! Box in forest for fireworks (gloves! make sure no one around!)
Physical access (~~medium~~ risk) LOW	Digital best practices	No talk about riots on phones! Research: does phone encryption works when turned on and locked?
Authentication bypass (low risk)	Digital best practices	(same as above)

(8) Beginning of the table, with mitigations and their implementations.

2.2.5. Burn or digitize your notes

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

1. At the end of the exercise, memorize your notes and then burn them. This approach makes it difficult to later revisit your notes and expand them.
2. At the end of the exercise, digitize your notes by manually copying them to an encrypted USB device using Tails[8] (remember to follow **digital best practices (#2)**). You can use Libreoffice Draw (included in Tails by default) to draw the attack tree. Once the notes are digitized, they shouldn't be printed out because this could leave a trace on the printer, but they can be manually copied to paper again so you can revisit them away from a computer.

2.2.6. Conduct an action review

After the riot, you and your comrades take some time to conduct an action review: in **outdoor and device-free conversations (#2)**, you discuss what went well and what went wrong, and whether there is room for improvement in the coverage of your attack tree or how you implemented the mitigations.

2.3. Assessing risk

Risk is the combined measure of a technique's impact and likelihood. If a technique would have a high impact, but is very unlikely to be used, it might be considered low risk. If a technique would have a medium impact, but is likely to be used, it might be considered high risk. If you consider the risk of a technique to be high, it means that you should apply mitigations for it more thoroughly.

For example, in most contexts, if you are planning to commit arson, the **Forensics: DNA (p. 24)** technique is high risk. This is because it has a high impact (a good DNA match to an arson crime scene is solid evidence in court) and a high likelihood (in most contexts, DNA forensics is systematically used in arson investigations).

[8] https://tails.net

2.3.1. Impact

Impact is a measure of the consequences if a technique is used. It depends on the tactic:

- Deterrence tactic: Impact is determined by whether the target is successfully deterred.
- Incrimination tactic: Impact is determined by how "solid" the evidence gathered is.
- Arrest tactic: Impact is determined by whether the target is successfully apprehended.

2.3.2. Likelihood

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

2.3.3. Adversary resources increase risk

If more resources are devoted to the repression of an action, a given technique may be more likely to be used, increasing its *likelihood*, and be used more thoroughly, increasing its potential *impact*. Broadly speaking, more resources are devoted to the repression of an action if an adversary feels more threatened by it.

For example:

- In most contexts, DNA forensics is systematically used in arson investigations. If the adversary has limited resources, the search might be limited to obvious surfaces such as door handles. If the adversary has more resources—which can be the case if the arson caused a lot of damage—the crime scene is more likely to be extensively searched for DNA evidence.
- In most contexts, if the adversary is the State, actions that are classified as "terrorism" or "threats to national security" will receive an extraordinary amount of resources. The State may devote many resources to actions that took place during an uprising, because the uprising was seen as a threat to the integrity of the State.

2.3.4. Mitigations decrease risk

By taking appropriate mitigations, you become less vulnerable to a technique, decreasing its potential *impact*.

For example, you are vulnerable to DNA forensics because your body constantly sheds DNA. If you apply **DNA minimization protocols (#2)** when committing arson, you become less vulnerable to DNA forensics.

2.3.5. Risk and local context

Understanding the habits and motivations of an adversary in repressing an action can help you to infer the range of repressive techniques they are likely to use, and how thoroughly they will use them. The **repressive operations (#2)** can help you gain an understanding of how a given technique is used in a given context.

2.4. Additional tips on using the Threat Library

The Threat Library Matrix[9] provides an overview of all the tactics and techniques, as well as buttons that allow you to hide or show specific techniques. For example, you might want to show only techniques that fit your threat model to better visualize them. If you follow our suggested process above and draw your own attack tree, the overview can help you think of relevant techniques that are missing from your tree.

The Threat Library welcomes external contributions, such as:

- Changes to existing techniques, mitigations or repressive operations.
- Suggesting the addition of new techniques, mitigations or repressive operations.
- Attack trees for different types of projects.
- Translating the Threat Library to new languages.

See the **contribute section (#2)** for more information.

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

also occasionally used and are much more covert than helicopters.

Examples of aerial physical surveillance include:

- Observing the crowd during demonstrations or gatherings, often as part of an **overt (p. 49)** surveillance operation.
- Improving the chances of successfully following the target of surveillance during a **covert (p. 46)** surveillance operation, especially at night.
- Locating suspects soon after an action took place and the adversary has been alerted, especially in rural areas or at night (in the case of an arson in Germany, a police helicopter responded by flying over the area the same night[99]).
- Locating suspects as part of routine **police patrols (p. 50)** in areas at risk of criminal activity.

Surveillance planes can monitor entire cities, photographing up to 80 square kilometers per second, allowing for the slow-motion reconstruction of virtually any outdoor movement,[100] with high-quality video at night.[101]

See the "Aerial surveillance" topic.[102]

Mitigations

Anonymous dress (#2): If you are being followed by an aerial surveillance operation, you can change into anonymous clothing when you are in a location that is not visible from the air to make it harder for the aerial surveillance operation to re-establish contact with you when you emerge into an open area (this won't work if the surveillance operation is also observing you on the ground).

Anti-surveillance (#2): You can include in an anti-surveillance route locations that would prevent an aerial surveillance operation from following you: an underground metro system, a shopping complex with many entrances, etc.

Attack (#2): During a demonstration, you can take down drones with fireworks, hack them, or blind them with lasers. See also 5 widely accessible ways to take down drones.[103]

Surveillance detection (#2): You can conduct surveillance detection to detect most and helicopters and some drones by listening for potential helicopters and drones: you should be able to hear most of them, depending on their altitude and your surroundings.

Repressive operations

Berlin 2023 railway conspiracy case (#2): The arrested people were discovered at night by a helicopter on a routine surveillance flight, presumably equipped with night-vision equipment.[104] A text[105] reports that in 2022, during another routine surveillance flight near Berlin, the same helicopter turned off its position lights and muffled the sound of its rotor blades to avoid detection: "Although the helicopter could still be heard, the noise was diminished. This can lead to misjudging the distance of the helicopter or, if mixed with other noise such as a highway, not being aware of the approaching problem until it's too late."

Repression of the 2019 uprising in Chile (#2): Drones were used to track rioters leaving riots in order to facilitate their arrest.[106]

Case against Direct Action (#2): After investigators discovered the remote area where members of Direct Action hid the stolen explosives they used in bombings, they arranged for a helicopter to fly over the area daily for surveillance purposes.[15]

4.22.2. Covert

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

Mobile

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

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

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

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

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

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

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

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

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

Fake ID (#2): During an ID check, you can present a fake ID to make it harder for the State to map your network.

Need-to-know principle (#2): You can apply the need-to-know principle to make it harder for an adversary to map your network.

Network map exercise (#2): An adversary can map a network by using infiltrators and informants to monitor the network: infiltrators and informants build credentials through association, build social profiles of people in the network, find pressure points to instigate interpersonal and political conflict, and entrap people. To mitigate this, you can conduct a network map exercise to make your network more resilient to infiltration attempts and help ensure it does not place trust in people who could be or become informants.

Repressive operations

Mauvaises intentions (#2): To prove that the defendants knew each other and were therefore likely accomplices, the investigators used several clues:[44]

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

4.20. Open-source intelligence

Used in tactic: **Incrimination**

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

Mitigations

Avoiding self-incrimination (#2): An adversary can use open-source intelligence to collect information that you publish voluntarily. To mitigate this, you can avoid using social media and generally avoid making any information about yourself or your networks public.

Repressive operations

2019-2020 case against Mónica and Francisco (#2): The photos used to identify Mónica and Francisco in public CCTV footage were found on social media.[37]

Repression of Lafarge factory sabotage (#2): Investigators collected metadata from photos of the action posted online, including the name and serial number of a camera.[42] This helped them identify a person they accused of taking the photos.

Bure criminal association case (#2): Investigators visited a Facebook page associated with the struggle against Cigéo and then analyzed the Facebook profiles of everyone who had "liked" the page.[21]

4.21. Parallel construction

Used in tactic: **Incrimination**

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

For example, an intelligence agency can collect incriminating digital evidence from a phone without a warrant, and then conduct a **house raid (p. 35)** to seize the phone where that evidence can be "discovered" so that it will not be thrown out at trial because it was obtained illegally.

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

4.22. Physical surveillance

Used in tactic: **Incrimination**

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

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

4.22.1. Aerial

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

3. Tactics

3.1. Deterrence

Uses techniques:
Door knocks (p. 22)
Doxing (p. 22)
Increased police presence (p. 37)
Mass surveillance (p. 41)
Physical violence (p. 49)
Police patrols (p. 50)

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

3.2. Incrimination

Uses techniques:
Biased interpretation of evidence (p. 15)
Covert house visit (p. 16)
Covert surveillance devices (p. 17)
Detection dogs (p. 20)
Door knocks (p. 22)
Evidence fabrication (p. 22)
Forensics (p. 23)
House raid (p. 35)
ID checks (p. 37)
Infiltrators (p. 38)
Informants (p. 38)
International cooperation (p. 39)
Interrogation techniques (p. 40)
Mass surveillance (p. 41)
Network mapping (p. 44)
Open-source intelligence (p. 45)
Parallel construction (p. 45)
Physical surveillance (p. 45)
Physical violence (p. 49)
Police patrols (p. 50)
Service provider collaboration (p. 51)
Targeted digital surveillance (p. 54)

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

3.3. Arrest

Uses techniques:
Alarm systems (p. 15)
Detection dogs (p. 20)
Guards (p. 35)
House raid (p. 35)
ID checks (p. 37)
Increased police presence (p. 37)
International cooperation (p. 39)
Police patrols (p. 50)

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

4. Techniques

4.1. Alarm systems

Used in tactic: **Arrest**

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

For physical infrastructure, modern alarm systems typically include sensors that detect unauthorized access to an area outside of normal operating hours. Such sensors include infrared motion detectors, sensors that detect the opening of doors, and many other types of sensors.[10] The alert signal can be sent over a wired or wireless connection—low-cost modern systems often send the signal over the mobile phone network.

For digital infrastructure, intrusion detection systems[11] monitor for any activity that might indicate a hack is in progress. If unauthorized access is detected, an incident response team can be notified to attempt to contain and remediate any compromise.

Mitigations

Attack (#2): You can attack alarm systems or the communication lines they use to send alert signals. For example, you can destroy alarm systems or jam alert signals with a jamming device.

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

Digital best practices (#2): When carrying out a cyber action, you can use digital evasion techniques[12] to prevent intrusion detection systems from detecting the action.

Reconnaissance (#2): Before an action, you can survey the target building or infrastructure to determine the presence of an alarm system, and the type and location of sensors or other alarm devices.

4.2. Biased interpretation of evidence

Used in tactic: **Incrimination**

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

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

Mitigations

Digital best practices (#2): You can follow digital best practices to limit the information an adversary has about you, and therefore limit the information they can interpret in a biased way.

Need-to-know principle (#2): You can apply the need-to-know principle to limit the information an adversary has about you, and therefore limit the information they can interpret in a biased way.

Repressive operations

December 8 case (#2): The case was characterized by a lack of evidence that the defendants were planning a specific attack, and relied instead on interpretation of circumstantial evidence. Examples of this interpretation include:[13]

[10] https://en.wikipedia.org/wiki/Security_alarm#Sensor_types

[11] https://en.wikipedia.org/wiki/Intrusion_detection_system

[12] https://en.wikipedia.org/wiki/Intrusion_detection_system_evasion_techniques

[13] https://soutien812.blackblogs.org/wp-content/uploads/sites/1922/2023/11/CompteRenduProces_A4.pdf

also requested footage from highway toll booths, presumably to identify the occupants of known cars traveling on highways to or from the action site.

Prometeo (#2): Two of the people were allegedly seen on video surveillance leaving a store where investigators believe the envelopes used to prepare the parcel bombs were purchased.[32]

2013 case against Mónica and Francisco (#2): Public CCTV footage was used by investigators to reconstruct the movements of Mónica and Francisco before and after the action.[50] This showed that they were near the action site shortly before the explosion of the device.

Case against Peppy and Krystal (#2): CCTV footage from a bus allowed investigators to identify the license plate of the motorcycle on which Peppy and Krystal arrived at and left the protest site.[14]

Case against Louna (#2): CCTV footage from the arson site showed two people setting fire to the excavator, and one of them burning themselves accidentally.[72]

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

- The license plate of the car that brought Louna to the hospital.
- The faces of the other people in the car.
- One of the people in the car carrying a watering jug. Investigators would later try to find this watering jug during a house raid.

CCTV footage from cameras in several towns was used to try to reconstruct the route of the car that brought Louna to the hospital, and the route Louna took when she left the hospital.[21]

Repression of the first Jane's Revenge arson (#2): CCTV footage helped identify a vehicle driven by the person, when they were seen entering a parking lot on foot after a demonstration, and the vehicle was seen leaving the same parking lot a few minutes later.[45]

Bure criminal association case (#2): Investigators used footage from the demonstrations, recorded by surveillance cameras and police forces, to:[21]

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

The three from the park bench (#2): On the evening leading up to the arrest, one of the people—while being followed by cops—stopped at a gas station and was seen by the station's video surveillance cameras buying gas and filling a gas can.[98] The cops obtained the CCTV footage the next morning.

Case against Ruslan Siddiqi (#2): Five hours after the bombing, Ruslan Siddiqi was walking away from the bombing site when he was filmed by a surveillance camera.[90] About three weeks later, he encountered a local cop who compared him with a photo from the surveillance camera footage and arrested him.

4.19. Network mapping

Used in tactic: **Incrimination**

Network mapping is the process by which an adversary gains insight into the organization and social relationships of a given network. By gaining this insight, an adversary can select individuals for additional scrutiny, arrest, or recruitment as **informants (p. 38)**.

The State very frequently uses social media friends lists (a form of **open-source intelligence (p. 45)**) for network mapping because they do not require a warrant or legal authorization.

Mitigations

Anonymous phones (#2): You can use anonymous phones to make it harder for an adversary to map your network.

Avoiding self-incrimination (#2): An adversary can use information obtained through self-incrimination to endanger not only the individual from whom the information was obtained, but also the rest of their network. To mitigate this, you should not talk to an adversary under any circumstances, and you can avoid providing biometric information (face photograph, fingerprints, DNA) if possible.

Compartmentalization (#2): You can compartmentalize your different identities (or projects) to make it harder for an adversary to map your network.

Digital best practices (#2): You can follow digital best practices, and in particular use end-to-end encrypted messaging applications on encrypted devices, to obscure your social networks and make it harder for an adversary to map your network.

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

- Public transport cameras on buses, trains, highways, etc.
- Home surveillance systems such as Amazon Ring.
- In-vehicle surveillance systems like those found on Teslas.

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

Storage

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

Analysis

An adversary can analyze CCTV footage:

- In real time if the cameras are integrated into a central network. Real-time analysis can take place either as part of routine surveillance or during exceptional events (e.g. demonstrations).
- Retroactively if the CCTV footage has been stored. Retroactive analysis can help identify a suspect by their **face (p. 27)**, **gait (p. 28)**, **voice (p. 31)**, etc.

Analysis of CCTV footage can be performed:

- By humans.
- By automated systems such as automated license plate readers or **facial recognition systems (p. 27)**.

See also

- You Can't Catch What You Can't See: Against Video Surveillance.[94]
- The topics "Video surveillance"[95] and "Automated license plate readers".[96]

Mitigations

Anonymous dress (#2): You can dress anonymously to prevent an adversary from identifying you from CCTV footage.

Anonymous purchases (#2): You can make anonymous purchases to prevent an adversary from identifying you from CCTV footage of physical stores.

Attack (#2): You can disable[97] surveillance cameras.

Biometric concealment (#2): When filmed by surveillance cameras, you can:

- To prevent **gait recognition (p. 28)**, wear baggy clothing that hide your body shape, use an umbrella or other concealing objects, or drastically change your walking style by adopting a "funny walk".
- To prevent **facial recognition (p. 27)**, wear a mask to cover your facial features, and sunglasses or a hat with a low brim to cover your eyes.

Outdoor and device-free conversations (#2): You can conduct sensitive conversations away from surveillance cameras to prevent an adversary from recording those conversations with surveillance cameras equipped with microphones.

Reconnaissance (#2): Before an action, you can identify the location of surveillance cameras at an action site and make plans to avoid them if possible.

Transportation by bike (#2): You can use a bike instead of any other type of vehicle: compared to other vehicles, a bike is much harder to identify on CCTV footage, especially if its distinguishing features are minimized. For example, you can use a different stolen bike for each action you carry out.

Repressive operations

Case against Boris (#2): Soon after the April sabotage, investigators requested CCTV footage from businesses and municipal cameras, and lists of vehicles from automated license plate readers (ALPRs) and speed cameras, all within an extended perimeter of the sabotage site.[26]

2019-2020 case against Mónica and Francisco (#2): Public CCTV footage was extensively used by investigators to reconstruct the movements of Mónica and Francisco before and during the actions, despite the mitigations they took (taking taxis, changing clothes, wearing disguises).[37]

Repression of Lafarge factory sabotage (#2): Immediately after the action, investigators requested CCTV footage from public transportation (buses, train stations, etc.), businesses, home surveillance systems, and municipal cameras, all within an extended perimeter of the action site.[42] In particular, footage of the interiors of buses appears to have helped identify people traveling to and from the action site.[41] Investigators

[94] https://notrace.how/resources/#catch-see
[95] https://notrace.how/resources/#topic=video-surveillance
[96] https://notrace.how/resources/#topic=automated-license-plate-readers
[97] https://notrace.how/resources/#destroy-cameras

- Libre Flot gained combat experience in Rojava, which was interpreted as an attempt to gain experience in order to carry out attacks in France.
- Libre Flot stole fertilizer from a store, intending to use it to create small explosives. The theft was interpreted as an attempt to obtain fertilizer without leaving traces.
- On two occasions, some of the defendants created small explosives from household or agricultural products, and detonated them in isolated areas where the explosions would not damage anything, which was interpreted as tests for possible future attacks (despite the defendants' claims that they were just doing it for fun).
- Some of the defendants participated in airsoft games, which were intepreted as paramilitary trainings.
- Handwritten notes of one of the defendants contained terms and phrases such as "weapons", "recruitment", "cleaning DNA", "incendiary device" and "are we ready for a comrade to be wounded or killed?", which were interpreted as indicative that the defendant was preparing an attack in France (despite the defendant's claims that the notes were about either airsoft or Rojava).
- In private conversations, some of the defendants made light-hearted, boasting comments such as "I want to burn all the banks, all the cops" and "if a police officer was on ground, honestly I would finish him off", which were interpreted as indicative of violent intentions.
- The defendants used secure digital communication tools, which was interpreted as indicative of "clandestine behavior".

4.3. Covert house visit

Used in tactic: **Incrimination**

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

An adversary can conduct a covert house visit to:

- Gather information.
- Install **covert surveillance devices (p. 17)** in the residence.
- Install **malware (p. 57)** on digital devices.

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

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

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

Mitigations

Clandestinity (#2): If you enter clandestinity, an adversary cannot know where you live, and therefore cannot conduct a covert house visit of your home.

Physical intrusion detection (#2): You can use physical intrusion detection to detect a covert house visit.

Preparing for house raids (#2): You can prepare for a covert house visit by minimizing the presence of materials that could be harmful in the event of a visit.

Stash spot or safe house (#2): You can keep action materials that have no "legitimate" purpose in a stash spot or safe house, or at worst, let them pass through your home only for a very limited time.

Repressive operations

Case against Peppy and Krystal (#2): Investigators conducted a covert search of the trash outside the home of Peppy and Krystal, where they found suspicious documents.[14]

Case against Direct Action (#2): After overhearing (presumably during a **physical surveillance (p. 45)** operation) that four members of Direct Action who lived together in a house were leaving the house for two days to go camping, investigators conducted two covert visits of the house over those two days:[15]

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

[14] https://notrace.how/documentation/case-against-peppy-and-krystal-affidavit.pdf
[15] https://archive.org/details/direct-action-memoirsofan-urban-guerrilla

4.4. Covert surveillance devices

Used in tactic: **Incrimination**

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

Where

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

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

When

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

- Most often, when it is retrieved by its installers.
- In some cases, when it is inadvertently discovered and removed by a third party.
- In rare cases, when it is deliberately discovered (through a **bug search (#2)**) and removed by a third party.

Power supply

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

Data transmission

Covert surveillance devices often transmit the data they collect:

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

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

See also

- Ears and Eyes.[16]
- The "Hidden devices" topic.[17]

4.4.1. Audio

A microphone found inside a neon ceiling light in Modena, Italy, in December 2015.[18]

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

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

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

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

Recorded conversations can be used as evidence in court if incriminating matters are discussed, or if they can be misconstrued to appear incriminating in the eyes of a judge. Non-incriminating, mundane conver-

[16] https://notrace.how/earsandeyes
[17] https://notrace.how/resources/#topic=hidden-devices
[18] https://notrace.how/earsandeyes/#modena-2015-12

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

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

See the "Digital surveillance" topic.[92]

Mitigations

Avoiding self-incrimination (#2): An adversary can use mass digital surveillance to retrieve self-incriminating information from a digital device. To mitigate this, you can avoid storing such information on digital devices except for very deliberate reasons (such as writing and sending an action claim while following **digital best practices (#2)**).

Digital best practices (#2): You can follow digital best practices to make mass digital surveillance ineffective. For example, you can use Tor[93] to anonymize your Internet activity, and you can use security-oriented operating systems and applications that limit the data they store or collect about you.

Encryption (#2): You can encrypt "in-motion" data to prevent observers at certain points on the network from analyzing this data.

4.18.3. Police files

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

Notable examples of police files include:

- Databases of government-issued ID documents (ID cards, driving licenses, passports).
- Databases of biometric information (face photographs, fingerprints, DNA).

[92] https://notrace.how/resources/#topic=digital-surveillance
[93] https://torproject.org

- Records of **ID checks (p. 37)**, fines, arrests, investigation proceedings, judicial proceedings, and convictions.

Mitigations

Attack (#2): You can destroy cabinets that store police files on paper and data centers that store them digitally.

Repressive operations

Case against Boris (#2): Investigators found out that the DNA on the bottle cap belonged to Boris because his DNA was in France's national DNA database.[26]

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

2011-2013 case against Jeremy Hammond (#2): Under his online persona, Jeremy Hammond shared in online chats that he had been arrested at the 2004 Republican National Convention, had spent time in a federal prison and in a county jail, and was currently on probation.[84] Investigators were able to verify all of this using police files, which helped them to link Jeremy Hammond's online persona to his real life identity.

Bure criminal association case (#2): Investigators extensively used police files to establish links between people, including databases of driver's licenses and registered vehicles, as well as records of arrests, judicial proceedings and convictions.[21]

4.18.4. Video surveillance

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

Collection

Sources of CCTV footage include:

- Cameras in the street or in other public locations.
- Cameras in private buildings (e.g. shops, offices).

4.18. Mass surveillance

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

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

4.18.1. Civilian snitches

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

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

Mitigations

Anonymous dress (#2): You can dress anonymously to prevent civilians from providing a description of you that would be valuable to an adversary.

Attack (#2): If a civilian follows you after an action, you can scare them off with threats or pepper spray. If a civilian tries to call the police, you can destroy their phone.

Careful action planning (#2): Civilians can observe you during an action and report their observations to an adversary. To mitigate this, you can carry out actions at night or in areas with minimal foot traffic to minimize witnesses, and use a lookout to report the presence of any witnesses as soon as they are noticed. Beware of balconies and windows overlooking the action site.

Repressive operations

Fenix (#2): When Lukáš Borl was in clandestinity his photo and personal information were published on the national police website to encourage civilians to send information about him to the police.[91]

2019-2020 case against Mónica and Francisco (#2): The saleswoman of the cell phone store where Mónica bought a phone that was used as part of the 2020 action, when questioned by investigators, gave a description of a person that the investigators matched to Mónica.[37]

Case against Louna (#2): Several civilians helped investigators. In particular:[21]

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

Belarusian anarcho-partisans (#2): While trying to cross the Belarusian-Ukrainian border, the people stopped at a shop about 10 kilometers from the border.[21] A shopkeeper called the border guards on them, which led directly to their arrest.

Case against Direct Action (#2): Several civilians helped investigators.[15] In particular:

- Journalists told investigators that they had noticed similarities between action claims published by Direct Action and articles in a local quarterly publication called Resistance.
- A hunter, presumably by chance, discovered two wooden structures where members of Direct Action stored the stolen explosives they used in bombings, and alerted the police to the discovery.[73]
- The landlords of the house where four members of Direct Action lived gave investigators the key to the house so they could enter and install hidden microphones.

4.18.2. Mass digital surveillance

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

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

sations can reveal a great deal about the targets of surveillance and help in **network mapping (p. 44)**.

See Ears and Eyes[16] and the "Hidden devices" topic.[17]

Mitigations

Bug search (#2): You can conduct a bug search to locate covert audio surveillance devices and eventually remove them.

Outdoor and device-free conversations (#2): You can conduct sensitive conversations outdoors and without electronic devices to prevent an adversary from recording those conversations with covert audio surveillance devices.

Physical intrusion detection (#2): An adversary often needs to covertly enter a space to install a covert audio surveillance device in the space. You can use physical intrusion detection to detect such a covert entry.

Repressive operations

Renata (#2): Six hidden microphones and a camera were found in a house after the operation.[19] The microphones were found in the living room, hallway, and bedrooms. The camera was found in the intercom system.

See the corresponding Ears and Eyes case.[20]

Case against Louna (#2): A hidden microphone was installed in a vehicle.[21]

Scintilla (#2): Microphones hidden in a house for two and a half years recorded conversations that the investigators used to prove that the defendants knew each other, talked regularly, worried about the creation of a DNA database and the impossibility of resisting DNA collection, and discussed writing a text to be published.[22]

See the corresponding Ears and Eyes case.[23]

Case against Direct Action (#2): Investigators installed hidden microphones:[15]

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

One day, after overhearing (presumably during a **physical surveillance (p. 45)** operation) that a member of Direct Action and his girlfriend were planning to have lunch at a cafe later in the day, investigators, with the cooperation of the cafe owner, quickly took the following steps:

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

December 8 case (#2): A hidden microphone was installed in the truck where Libre Flot lived.[24] When the legal authorization for installing and using the microphone expired after two months, the microphone was remotely deactivated but not removed from the truck. It was removed several months later during the raids.

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

4.4.2. Location

A GPS tracker found under a vehicle in Berlin, Germany, in August 2022.[25]

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

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

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

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

[19] https://roundrobin.info/2019/03/trento-sei-microspie-e-una-telecamera-immagini-pesanti
[20] https://notrace.how/earsandeyes/#trento-2019-03
[21] Private source.
[22] https://macerie.org/index.php/2019/03/12/le-orecchie-della-pedrotta
[23] https://notrace.how/earsandeyes/#torino-2019-03
[24] https://soutien812.blackblogs.org/2024/12/15/affaire-du-8-12-analyse-dune-enquete-preliminaire-pnat-et-dgsi
[25] https://notrace.how/earsandeyes/#berlin-2022-08

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

Collected location data can be used as evidence in court. Non-incriminating, mundane location data can reveal a lot about the targets of surveillance and help in **network mapping (p. 44)**.

See Ears and Eyes[16] and the "Hidden devices" topic.[17]

Mitigations

Bug search (#2): You can conduct a bug search to locate covert location surveillance devices and eventually remove them.

Physical intrusion detection (#2): An adversary often needs to covertly enter the space where a vehicle is parked to install a covert location surveillance device on the vehicle. You can use physical intrusion detection to detect such a covert entry.

Transportation by bike (#2): You can use a bike instead of any other type of vehicle: unlike other vehicles, when you conduct a **bug search (#2)** of a bike you can determine with a high degree of confidence whether or not a covert location surveillance device is installed on the bike.

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

Repressive operations

Case against Boris (#2): GPS tracking devices were placed under several vehicles after investigators learned that Boris—who did not have a driver license—was being transported in them.[26]

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

Case against Louna (#2): Several GPS trackers were installed on vehicles.[21]

Bure criminal association case (#2): Investigators installed a covert location tracker on a vehicle, where it remained for about a month.[21]

December 8 case (#2): A covert location tracker was installed on a vehicle used by Libre Flot.[24]

4.4.3. Video

A camera found in the skylight of a public school in Berlin, Germany, in July 2011.[27]

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

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

- The living room of a target.
- The windows of a building close to the home of a target, with a line of sight on the entrance of the home.
- Close to **stash spots or safe houses (#2)** as has happened in Italy, where motion-activated cameras were installed to monitor a forest stash spot.[28]

Captured images can be used as evidence in court. Non-incriminating, mundane images can reveal a lot about the targets of surveillance and help in **network mapping (p. 44)**.

See Ears and Eyes[16] and the "Hidden devices" topic.[17]

Mitigations

Bug search (#2): You can conduct a bug search to locate covert video surveillance devices and eventually remove them.

Digital best practices (#2): An adversary can install covert video surveillance devices that can film a computer or phone screen, or a computer keyboard. To mitigate this, when using a computer or phone for sensitive activities, you can:

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

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

[28] 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

Repressive operations

Bialystok (#2): In June 2020, people were arrested in Spain and France, thanks to cooperation between Italian, Spanish and French intelligence and police forces.[85]

During the investigation Italian cops tried to target a person living in Germany.[86] They sent several requests to German police to extradite the person or have their house searched but the requests were rejected.

Scintilla (#2): Carla was arrested in France thanks to cooperation between Italian and French intelligence and police forces.[87]

Bure criminal association case (#2): Some of the people that were arrested had participated in demonstrations against the 2017 G20 summit in Hamburg, Germany.[21] Because of this, German investigators cooperated with French investigators, including by being present when the people were interrogated after their arrest.

4.17. Interrogation techniques

Used in tactic: **Incrimination**

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

Interrogation techniques can include lying, making threats, instilling guilt, shame, or pride, trying to appear friendly and helpful or, on the contrary, threatening and violent, etc. In some cases, they can include **physical violence (p. 49)**.

See How the police interrogate and how to defend against it[88] (in French and German) for a comprehensive overview of police interrogation techniques.

Mitigations

Avoiding self-incrimination (#2): You should not talk to an adversary under any circumstances: this is the best way to resist their interrogation techniques.

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

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

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

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

Repressive operations

Case against Boris (#2): When interrogating people close to Boris, investigators used elaborate lies to try to get information from them.[26] For example, the investigators vaguely suspected that the people being interrogated had hosted Boris in April 2020 and wanted to confirm their suspicion, so they asked, "Our investigation revealed that you let [Boris] stay with you in April 2020. How long did he stay with you?"

Warsaw 3 (#2): A few weeks into his detention, one person gave an "extensive" testimony to the police. He claimed this was partly because of two techniques used by one of his lawyers to push him to give this testimony:[89]

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

Case against Ruslan Siddiqi (#2): After his arrest, investigators were unsure of Ruslan Siddiqi's involvement in the bombing.[90] They interrogated him and deduced that he was hiding something. Ruslan Siddiqi recounts: "They started asking various questions about what I was doing on [the day of the bombing]. I made a couple of blunders in my answers, and [the person in civilian clothes] who asked the questions realized that I was hiding something."

December 8 case (#2): When interrogating defendants during custody, investigators:[13]

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

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

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

- Offer someone positive consequences if they become an informant: immunity or leniency in the judicial case in which they are asked to become an informant or in another case, money…

An adversary can use an informant to gather evidence or to **map a network (p. 44)**.

See the "Infiltrators and informants" topic.[76]

Mitigations

Attack (#2): You can attack informants when uncovered or years later to discourage others from becoming informants.

Background checks (#2): You can perform background checks to help ensure that someone in your network is not an informant.

Need-to-know principle (#2): You can apply the need-to-know principle to limit the information a potential informant can obtain about your involvement in actions (if an informant isn't involved in an action, they shouldn't know who is involved even if it's their own roommate).

Network map exercise (#2): You can conduct a network map exercise to help ensure your network does not place trust in people who could be or become informants.

Prisoner support (#2): You can support prisoners from your networks: beyond the ethical imperative of this support, people are less likely to turn informant if they feel supported and connected to the movements for which they risked their freedom.

Repressive operations

Case against Marius Mason (#2): The main evidence against Marius Mason was provided to investigators by his former husband, Frank Ambrose, who had participated in some of the actions with him.[79] Frank Ambrose became an informant after his arrest in 2007 (which was triggered by him throwing incriminating material in a garbage can).[80] For several months, the snitch collaborated extensively with the Federal Bureau of Investigation (FBI), secretly recording 178 phone conversations and face-to-face meetings, and providing information on 15 people.[81]

2011-2013 case against Jeremy Hammond (#2): In June 2011, investigators recruited an associate of Jeremy Hammond, Sabu, as an informant.[82] For several months, Sabu helped investigators build a case against Jeremy Hammond. In exchange for their collaboration Sabu received a lenient sentence: after having spent 7 months in prison (for a bail violation), they were sentenced to time served.[83]

Sabu knew Jeremy Hammond's online persona but did not know his real life identity. To find out Jeremy Hammond's real life identity, investigators used information that he had shared with Sabu in online chats, including that:[84]

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

4.16. International cooperation

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

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

International cooperation can be used to:

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

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

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

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

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

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

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

[84] https://notrace.how/documentation/jeremy-hammond-affidavit.pdf

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

Physical intrusion detection (#2): An adversary often needs to covertly enter a space to install a covert video surveillance device in the space. You can use physical intrusion detection to detect such a covert entry.

Stash spot or safe house (#2): You can keep action materials in a stash spot or safe house to avoid bringing them into your home, where covert video surveillance devices can be present.

Surveillance detection (#2): An adversary can park a surveillance vehicle near your home with a camera that films your home entrance. To mitigate this, you can use the following passive surveillance detection technique. It only works if you live in a place where there aren't too many different vehicles that park, that is, in some residential areas in cities and in most rural areas. Each time you leave or enter your home, you take note of all the vehicles parked on the street that have a line of sight to your home. Trying not to look suspicious, you note their model, color, and license plate number, either remembering the information or writing it down. After doing this for a while, you will become familiar with the "baseline" of vehicles that park on your street, which will be the vehicles of people who live nearby or their guests. Once you're familiar with the baseline, you'll be able to spot vehicles that are not part of that baseline and discreetly examine them to see if they are surveillance vehicles.

Repressive operations

Case against Boris (#2): Cameras were installed in the streets outside Boris's home and outside the home of someone close to him to film the entrances to the homes.[26]

Case against Louna (#2): Cameras were installed to film the entrances of several places where people opposed to the highway project lived.[21]

December 8 case (#2): A camera was installed outside a small cabin used by some of the defendants, filming the cabin.[24] It was seemingly installed about 10 meters from the cabin, on a tree trunk.

4.5. Detection dogs

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

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

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

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

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

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

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

Detecting substances

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

- At an action site or during a **house raid (p. 35)** or **covert house visit (p. 16)** to determine if a substance is present and locate it.
- During an **ID check (p. 37)** to determine if the person being checked is carrying or has been in contact with a substance.

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

Tracking people

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

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

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

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

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

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

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

Scent lineups

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

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

Mitigations

Careful action planning (#2): An adversary can use detection dogs to track you after an action. To mitigate this, when leaving the action site, you can plan to:

- Avoid leaving behind an item that carries your scent, which the adversary could provide to a dog to help the dog track you.
- Break your odor trail, for example by travelling a significant distance on a bike or crossing a large body of water.

Repressive operations

Fenix (#2): In one of the house raids, the police used detection dogs trained to detect explosives.[29]

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

the possibility of a decreased police presence elsewhere.

4.14. Infiltrators

Used in tactic: **Incrimination**

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

Stop Hunting Sheep[75] describes five basic types of infiltrators:

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

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

See the "Infiltrators and informants" topic.[76]

Mitigations

Attack (#2): You can attack infiltrators when uncovered or years later[77] to discourage the practice—police infiltrators are likely to be less enthusiastic if there is a local precedent of violence against them.

Background checks (#2): You can perform background checks to help ensure that someone in your network is not an infiltrator.

Need-to-know principle (#2): You can apply the need-to-know principle to limit the information a potential infiltrator can obtain about your involvement in actions (if an infiltrator isn't involved in an action, they shouldn't know who is involved even if it's their own roommate).

Network map exercise (#2): You can conduct a network map exercise to make your network more resilient to infiltration attempts.

Repressive operations

Fenix (#2): Two police officers infiltrated the network of the defendants for several months.[78] During their infiltration, the two officers:

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

4.15. Informants

Used in tactic: **Incrimination**

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

An adversary can use different strategies to recruit an informant:

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

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

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

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

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

pocket knife taken by a member of Direct Action from the stolen van used in the bombing.

December 8 case (#2): During the raids, investigators found firearms and products that could be used to create explosives.[13]

4.12. ID checks

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

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

Complying with an ID check gives the State information about you, which can help them **map your network (p. 44)**, and can lead to your arrest if you are wanted by them. The consequences of being unable or refusing to comply with an ID check are highly context-dependent, but may include having your biometric information taken by force or without your knowledge, being detained, and being deported out of the country.

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

Mitigations

Avoiding self-incrimination (#2): If possible, you can avoid answering questions or providing biometric information (face photograph, fingerprints, DNA) during an ID check.

Fake ID (#2): During an ID check, if providing your real identity could lead to your arrest or other negative consequences, you can present a fake ID (as long as the fake ID is not recognized as such by the State).

Repressive operations

Case against Boris (#2): Investigators obtained and analyzed records of ID checks made by local police shortly before and after the sabotages, in different perimeters around where the sabotages took place, presumably hoping to find the names of the saboteurs in those records.[26]

4.13. Increased police presence

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

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

Examples of increased police presence include:

- More frequent **police patrols (p. 50)** in a particular area.
- The deployment of police officers and vehicles at a public demonstration. In the hours before a demonstration begins, police officers and vehicles can cluster on the streets around the demonstration or around its expected targets. This clustering can be an opportunity for them to conduct **overt surveillance (p. 49)** before, during, and after the demonstration.

Mitigations

Attack (#2): If you expect the police to increase their presence at a public demonstration, you can organize to make sure the crowd is large and fierce enough: decentralized and autonomous forces are more agile than the rigid chain of command that police agencies rely on for crowd control. For example, despite years of planning to militarize Hamburg, Germany, for the G20 summit, rioters were able to liberate a neighborhood from police occupation for an entire night.[74]

Careful action planning (#2): You can carefully plan an action to mitigate the risk of an increased police presence at the action site. For example:

- You can conduct a thorough **reconnaissance (#2)** of the action site and prepare a good escape plan.
- If you are planning to carry out arson, you can use an incendiary device with a delay so that the device is not activated until after you have left the action site.
- You can take advantage of the fact that an increased police presence in one place means

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

Repression against Zündlumpen (#2): In some of the February 2025 raids, police used detection dogs to locate electronic devices.[30]

Bure criminal association case (#2): Detection dogs were used in one of the raids.[21]

4.6. Door knocks

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

Door knocks are when an adversary comes knocking where you live to intimidate you or get information. Door knocks aim to intimidate or create paranoia, to see who is willing to talk and possibly be recruited as an **informant (p. 38)**, and to gather information from the people who do talk.

By logging who you call or visit immediately after they come knocking, the adversary can **map your network (p. 44)**.

In many countries, it is easier for the State to carry out door knocks than **house raids (p. 35)** because door knocks do not require a warrant or legal authorization.

Mitigations

Avoiding self-incrimination (#2): If an adversary knocks on your door, you can avoid talking to them: instead, alert your networks and consider making the event public.

Digital best practices (#2): You can follow digital best practices to make it harder for an adversary to log who you contact after they knock on your door.

Repressive operations

Scintilla (#2): In May 2019, cops knocked on Boba's door under the pretext of giving a verbal notice to someone else.[31] Once inside, however, they revealed a warrant for Boba's arrest, arrested him, and searched the house.

4.7. Doxing

Used in tactic: **Deterrence**

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

Doxing often uses information obtained through **open-source intelligence (p. 45)**.

Mitigations

Digital best practices (#2): You can follow digital best practices to make it harder for an adversary to dox you.

4.8. Evidence fabrication

Used in tactic: **Incrimination**

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

Notable examples of evidence fabrication include:

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

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

Mitigations

Physical intrusion detection (#2): An adversary often needs to covertly enter a space to plant evidence in the space. You can use physical intrusion detection to detect such a covert entry.

Repressive operations

Prometeo (#2): Investigators distorted conversations obtained through phone interception to make them

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

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

look suspicious.[32] For example, during a phone conversation involving one of the defendants, the phrase "tutta questa tensione sociale prima o poi scoppierà" ("all this social tension will, sooner or later, explode") was said, which was only partially transcribed in the investigation files as "prima o poi scoppierà" ("will, sooner or later, explode").

December 8 case (#2): Investigators mistranscribed or distorted conversations obtained through phone interception or hidden microphones to make them look suspicious.[13] For example, the term "lunettes balistiques" (ballistic goggles) used in a conversation was transcribed as "gilets balistiques" (ballistic vests) by intelligence services, and became "gilets explosifs" (explosive vests) in a report by the prosecutors in charge of the case.

4.9. Forensics

Used in tactic: **Incrimination**

Forensics is the application of science to investigations for the collection, preservation, and analysis of evidence. It has a broad focus: DNA analysis, fingerprint analysis, bloodstain pattern analysis, firearms examination and ballistics, toolmark analysis, serology, toxicology, hair and fiber analysis, footwear and tire tread analysis, drug chemistry, paint and glass analysis, linguistics, digital audio, video, and photographic analysis, etc.

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

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

4.9.1. Arson

Arson forensics (also known as *fire investigation*) is the application of science to the investigation of arson. Arson forensics has two distinct phases: fire scene investigation, which focuses on evidence at the scene of the fire, and fire debris analysis, which focuses on evidence removed from the scene and analyzed in a laboratory.

Fire scene investigation involves determining whether a fire was intentionally set and identifying its point of origin. It becomes much more difficult when the "flashover" point has been reached—when a room becomes so hot that every ignitable surface bursts into flames.

Fire debris analysis focuses on ignitable liquid residues (ILRs) and aims to identify potential traces of accelerant and their chemical composition—these samples are often found by **dogs (p. 20)** at the scene.

Mitigations

Anonymous purchases (#2): An adversary can sometimes identify accelerants and trace them back to a gas station brand, and from there to the identity of the person who purchased the accelerants. To mitigate this, you can purchase accelerants anonymously.

Careful action planning (#2): An adversary can tie actions together if accelerants from the same sources are used in all of them. To mitigate this, you can avoid reusing accelerants from the same source in different actions.

Repressive operations

Case against Louna (#2): A gas detector[33] was unsuccessfully used to detect traces of accelerant in the cab of the burned excavator.[21]

Traces of accelerant were collected:

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

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

Bure criminal association case (#2): Traces of accelerants were collected from items recovered after demonstrations and analyzed.[21]

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

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

Mitigations

Clandestinity (#2): If you enter clandestinity, an adversary cannot know where you live, and therefore cannot raid your home.

Preparing for house raids (#2): You can prepare for a house raid by minimizing the presence of materials that could be harmful in the event of a raid.

Preparing for repression (#2): You can prepare for repression to minimize the impact of house raids.

Stash spot or safe house (#2): You can keep action materials that have no "legitimate" purpose in a stash spot or safe house, or at worst, let them pass through your home only for a very limited time.

Repressive operations

Scripta Manent (#2): One person was arrested after batteries and an electrician's manual were found in his home during a raid.[69]

Renata (#2): During a house raid, cops tried to get into the basement without waking up the people in the house, then privately complained that they were unable to hide what they wanted to hide.[70]

Repression of Lafarge factory sabotage (#2): Among the initial house raids, one was particularly thorough: cops searched under mattresses, behind sofa covers and in every drawer of every piece of furniture, inspected every book, notebook and piece of clothing as well as the dishes, and emptied packages of pasta and sealed jars.[71]

2013 case against Mónica and Francisco (#2): During a raid on the home of Mónica and Francisco, investigators found:[50]

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

Case against Louna (#2): Investigators raided:

- The home of the owner of the car that brought Louna to the hospital.[21] They seized the car during the raid.
- The home of a person suspected of being seen on the CCTV footage from the hospital carrying a watering jug, in the hope of finding the watering jug during the raid and confirming that the person was indeed at the hospital.[72]

Case against Jeff Luers (#2): During the raid of the storage unit, investigators found:[65]

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

Bure criminal association case (#2): During the raids, investigators found:[21]

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

Case against Direct Action (#2): In a raid on the house where four members of Direct Action lived, investigators found:[73]

- Related to the electrical substation bombing: plans of the action site, a copy of the action claim sent after the bombing, and newspaper clippings of articles about the bombing.
- Related to the Litton Industries bombing: photographs and plans of the action site, newspaper clippings of articles about the bombing, and a

[69] 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

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

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

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

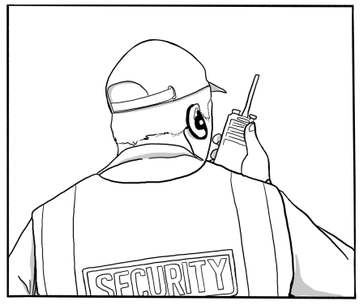
[73] https://web.archive.org/web/20100715145801/http://uniset.ca/other/cs5/27CCC3d142.html

in the fence surrounding the site of the May arson attempt.[65]

December 8 case (#2): During the raids, several objects (a stove, pans, gloves, spatulas) were analyzed for traces of products that could be used to create explosives.[13]

4.10. Guards

Used in tactic: **Arrest**



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

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

Mitigations

Attack (#2): Before or during an action, you can incapacitate guards to prevent them from interfering with the action. For example, in their actions on logging companies machinery in so-called Chile, Mapuche people have neutralized guards by disarming them,[66] tying them up[67] or shooting at them.[68]

Reconnaissance (#2): Before an action, you can identify the presence of guards at the action site.

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

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

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

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

Repressive operations

Case against Louna (#2): In the days preceding the arson, a security guard saw suspicious vehicles driving near the arson site, took photos of them, and, after the arson, provided the photos to investigators.[21]

4.11. House raid

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

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

When

An adversary can conduct a house raid:

- Most often, early in the morning when the occupants of the residence are asleep and taken by surprise.
- In some cases, during the day. This can be the case when one goal of the raid is to seize digital devices while they are turned on (and therefore their **encryption (#2)** is not effective). In this case, the adversary can decide to conduct the house raid during the day because digital devices are more likely to be turned on when their users are awake, which is more likely to be during the day.

Why

An adversary can conduct a house raid to:

- Seize items to find evidence or to do **network mapping (p. 44)**. Commonly seized items include electronic devices, literature, materials that could be used in actions, and clothing. In some cases, the adversary seizes expensive items (e.g., computers, printing equipment) with the goal of disrupting the organizational capacity of their targets.
- Arrest the occupants of the residence.
- Install **covert surveillance devices (p. 17)** in the residence.

Additional considerations

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

4.9.2. Ballistics

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

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

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

Mitigations

Anonymous purchases (#2): An adversary can use ballistic forensics to trace back a firearm or bullet to a seller, and from there to the identity of the person who purchased the firearm or bullet. To mitigate this, you can purchase firearms and bullets anonymously, for example through connections to organized criminal networks or through fraud.

Stash spot or safe house (#2): An adversary needs to have access to a firearm to perform a ballistic analysis on the firearm. To prevent this, you can store the firearm in a stash spot or safe house.

4.9.3. DNA

DNA forensics (also known as *DNA analysis*) is the collection, storage, and analysis of DNA traces for the purpose of matching DNA traces to individuals.

Collection

DNA is the molecule that contains the genetic code of organisms. With the exception of red blood cells, every cell in your body has DNA. You constantly shed DNA into the environment through skin cells, hair, saliva, blood, sweat, etc. DNA traces can be collected from human bodies or the environment and analyzed in specialized laboratories to reveal information about the individuals they came from.

Analysis

Analysis of a DNA trace can provide basic information about the individual it came from, such as their genetic sex. Comparison of two DNA traces can determine whether they belong to the same individual, to individuals who are closely related genetically (e.g., parents and their children, cousins), or to unrelated individuals.

DNA in the environment degrades over time and under certain conditions, and a DNA trace must contain a sufficient amount of undegraded DNA to be successfully analyzed. As technology advances, this amount decreases.

DNA is often treated in trials as the "gold standard", indisputable proof that a person was in contact with the surface where their DNA was found.

DNA databases

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

See also

- Dna You Say? Burn Everything to Burn Longer: A Guide to Leaving No Traces[34] for a comprehensive overview of DNA forensics literature.
- The "DNA" topic.[35]

Mitigations

Careful action planning (#2): An adversary can use DNA forensics to collect DNA at an action site. To mitigate this, you can carefully plan the action to minimize DNA traces at the action site. For example, you can:

- Secure your hair under a hat.
- If you have to cut a fence, cut any fence holes large enough to pass through without touching the fence.
- Ensure that surfaces at the action site are not touched if they do not need to be, and that surfaces that need to be interacted with (such as a

[34] https://notrace.how/resources/#dna-you-say

[35] https://notrace.how/resources/#topic=dna

door handle) are touched by someone following **DNA minimization protocols (#2)**.

- Ensure that any destructive device left at the site (e.g. an incendary device with a delay) has worked as expected in tests conducted under similar conditions (temperature, etc.) The point of this is to make sure that the device will not be recovered intact by an adversary.
- Ensure that nothing is accidentally left behind such as a bag, tool, or anything that falls out of a pocket.

DNA minimization protocols (#2): You can minimize the amount of DNA you leave on a surface to minimize the risk that an adversary can use DNA forensics to draw a valuable conclusion from an analysis of the surface.

Gloves (#2): You can wear gloves to avoid leaving DNA on surfaces you touch.

Repressive operations

Scripta Manent (#2): DNA evidence was used to convict Alfredo Cospito.[36]

Case against Boris (#2): The only evidence against Boris was that his DNA was found on a bottle cap at the foot of one of the burnt antennas from the April sabotage.[26]

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

2019-2020 case against Mónica and Francisco (#2): Francisco's DNA was found on the parcel bomb sent to the former Minister of the Interior, which was defused and didn't explode.[37]

Repression against Zündlumpen (#2): DNA traces were collected from a cigarette butt[38], zines,[39] books, doors, cups, and printing machines.

Renata (#2): After their arrest and imprisonment, the person accused of the explosive attack on the Lega Nord headquarters in Treviso refused to have their DNA taken.[40] Some time after the person's refusal, prison guards searched their cell and secretly replaced one comb with another, presumably to obtain the person's DNA from the hairs on the comb they took.

Repression of Lafarge factory sabotage (#2): In one of the initial raids, police insisted that those arrested wear surgical masks to protect against Covid: the masks were later taken for DNA collection.[41] One person who refused to wear a mask had their underwear confiscated while in police custody, presumably for DNA collection.[42]

Prometeo (#2): DNA traces were used to convict the person accused of burning an ATM.[43]

Mauvaises intentions (#2): During police custody, DNA was collected from the people's clothing and from plastic cups.[44] 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 collected earlier.

The charges against one person were based on a match between their DNA and DNA collected at the scene of the attempted arson of the electrical cabinet. DNA 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 charges against other people were based on a match between their DNA and DNA collected from a cigarette used as a delay for an incendiary device—the delay failed and the device was found intact under the police tow truck.

Case against Louna (#2): DNA traces of Louna were collected from:[21]

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

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

[36] https://insuscettibiledіravvedimento.noblogs.org/post/2020/03/29/it-en-italia-su-una-sentenza-e-qualcosa-daltro-un-testo-di-marco-dal-carcere-di-alessandria
[37] https://notrace.how/resources/#monica-francisco
[38] https://notrace.how/resources/#bavarian-christian
[39] https://notrace.how/resources/#cops-and-robbers
[40] https://roundrobin.info/2020/03/aggiornamenti-su-manu-stecco-juan-e-sasha
[41] https://sansnom.noblogs.org/archives/16831
[42] https://notrace.how/resources/#lafarge
[43] https://roundrobin.info/2021/05/sentenza-beppe
[44] https://infokiosques.net/spip.php?article597

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

An adversary can:

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

See also:

- PRISMA,[62] section "Tool Traces" for a short discussion of tool marks.
- Color Atlas of Forensic Toolmark Identification[52] for a comprehensive overview of tool marks.

Glass

When glass breaks, it produces shards of various sizes.

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

- Two glass objects of different models, or manufactured in different factories, or manufactured in the same factory several weeks apart, may produce shards that can be distinguished by analyzing their properties, including their refractive indices[63] and chemical elements.[64]
- Two glass objects of the same model, manufactured in the same factory during the same week, may produce shards that are indistinguishable.

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

See Handbook of Trace Evidence Analysis,[52] chapter "Interpretation of Glass Evidence" for an overview of glass evidence.

[62] https://notrace.how/resources/#prisma
[63] https://en.wikipedia.org/wiki/Refractive_index
[64] https://en.wikipedia.org/wiki/Chemical_element

Traces of accelerant

Traces of accelerant are covered in the technique **Forensics: Arson (p. 23)**.

Other

Other types of trace evidence include:

- Human and animal hair. Hair can fall from a body at any time. Hair can reveal various information about its owner, including, in some cases, their **DNA (p. 24)**. See Handbook of Trace Evidence Analysis,[52] chapter "Forensic Hair Microscopy" for an overview of hair.
- Paint. A painted object can leave traces of paint on a surface it touches. A trace of paint can reveal information about the object that left it. See Handbook of Trace Evidence Analysis,[52] chapter "Paints and Polymers" for an overview of paint.

Mitigations

Anonymous dress (#2): An adversary can use trace evidence to link clothing to an action site. To mitigate this, you can dress anonymously, and in particular dispose of the clothing after the action.

Anonymous purchases (#2): An adversary can use trace evidence to link objects to an action site. To mitigate this, you can anonymously purchase objects used in the action.

Careful action planning (#2): An adversary can use trace evidence to link objects to an action site. To mitigate this, after the action, you can plan to:

- Dispose of the objects you used during the action.
- If an object is too expensive to discard after each action, store it in a **stash spot or safe house (#2)**.
- If a tool is too expensive to discard after each action, modify it so that an adversary cannot link it to traces it may have left at the action site. For example, you can dispose of the disc of a disc cutter.

Stash spot or safe house (#2): An adversary can use trace evidence to link objects to an action site. To mitigate this, after the action, you can store in a stash spot or safe house objects used in the action that are too expensive to discard after each action.

Repressive operations

Case against Jeff Luers (#2): In the raid of the storage unit, the police found a bolt cutter matching the cuts

Fibers

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

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

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

An adversary can:

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

See Handbook of Trace Evidence Analysis,[52] chapter "Fibers" for an overview of fibers.

Footprints

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

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

- On a hard, dusty surface, a foot may leave a very unique footprint that shows the ridges of the toes, which are as unique as **fingerprints (p. 27)**.
- On a soft surface such as sand, a foot may leave a very generic footprint that shows only a rough outline of the foot.

An adversary can:

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

See Examination and Interpretation of Bare Footprints in Forensic Investigations[61] for an overview of footprints.

Shoeprints

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

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

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

An adversary can:

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

See Footwear Impression Evidence: Detection, Recovery and Examination[52] for a comprehensive overview of shoeprints.

Tool marks

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

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

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

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

Unusable DNA traces were collected from:

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

Repression of the first Jane's Revenge arson (#2): In May 2022, DNA traces were collected from several items found by investigators at the action site, including a broken window, a glass jar, a lighter, and an intact Molotov cocktail.[45] In March 2023, police saw the person discard a bag containing a partially eaten burrito in a public trash can. DNA traces collected from the bag's contents matched those collected at the action site.

Scintilla (#2): The charge against Peppe was based on a match between DNA traces found inside the parcel bomb and his DNA collected from a cigarette butt during the investigation.[46]

Bure criminal association case (#2): DNA traces were collected from:[21]

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

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

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

Nea Filadelphia case (#2): The charges against several people were based on a match between their DNA, taken by force while in custody, and DNA traces found on "mobile objects" near the robberies.[47]

Panico (#2): DNA traces were the only evidence against one of the defendants.[48]

4.9.4. Digital

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

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

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

Mitigations

Avoiding self-incrimination (#2): An adversary can use digital forensics to retrieve self-incriminating information from a digital device. To mitigate this, you can avoid storing such information on digital devices except for very deliberate reasons (such as writing and sending an action claim while following **digital best practices (#2)**).

Digital best practices (#2): An adversary can use digital forensics to retrieve data from a digital device you have used. To mitigate this, you can follow digital best practices and, in particular, use Tails,[8] an "amnesic" operating system designed to leave no trace on the computer it runs on.

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

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

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

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

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

- Use popular rather than custom tools.
- If you use a Virtual Private Server (VPS), **purchase it anonymously (#2)** and access it through Tails.[8]

Encryption (#2): An adversary can use digital forensics to retrieve data from unencrypted digital devices. To mitigate this, you can encrypt your digital devices with Full Disk Encryption and a strong password.

Metadata erasure and resistance (#2): An adversary can use digital forensics to retrieve and analyze metadata. To mitigate this, you can erase metadata from files before publishing them online or sending them to others.

Repressive operations

Bure criminal association case (#2): Investigators analyzed storage devices by automatically extracting files containing the following keywords relevant to the investigation:[21]

- "*Action*".
- "Andra", the agency responsible for the Cigéo project.
- "Bindeuil", the name of the building that was attacked during the June 21, 2017 demonstration.
- "*Hibou*" ("owl"), a name used by people fighting against Cigéo to refer to themselves.
- "*Incendie*" ("fire").

4.9.5. Facial recognition

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

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

Modern facial recognition systems are capable of matching a face image against a large database of faces, even if the face in the image is masked, with only the eyes and eyebrows visible. Facial recognition systems coupled with **mass video surveillance (p. 42)** can be used to automate the tracking of individuals through a space.

See the "Facial recognition" topic.[49]

Mitigations

Anonymous dress (#2): You can wear a mask that adequately covers your face, including your eyebrows and up to the top of your nose.

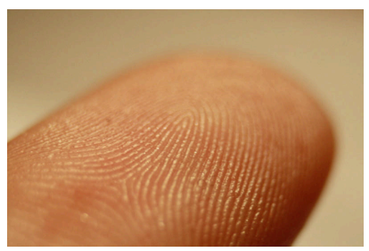
Biometric concealment (#2): You can wear a mask to cover your facial features, and sunglasses or a hat with a low brim to cover your eyes.

Repressive operations

2019-2020 case against Mónica and Francisco (#2): In order to identify Mónica and Francisco on public CCTV footage, photos of both were compared to the footage, including a comparison of several facial features: eye distances, wrinkles, piercing scars, ear size, mouth and nose shape.[37]

2013 case against Mónica and Francisco (#2): The main evidence against Mónica and Francisco was a comparison of photos of both of them with public CCTV footage that showed their uncovered faces while they were in the subway, shortly before or after the action.[50]

4.9.6. Fingerprints



Ridges on a human finger.

[49] https://notrace.how/resources/#topic=facial-recognition
[50] https://notrace.how/documentation/monica-and-francisco-2013-case-file.pdf

- Counteracting Forensic Linguistics.[59]
- Who wrote that?[60]

Mitigations

Biometric concealment (#2): You can hide the acoustic properties of your voice to mitigate voice identification.

Masking your writing style (#2): You can mask your writing style to mitigate author identification.

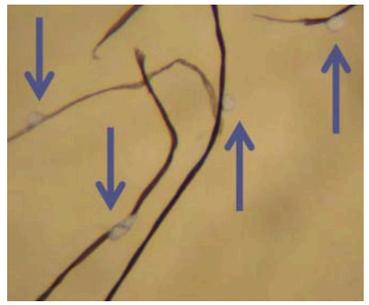
Repressive operations

Scripta Manent (#2): Texts published by some of the defendants were compared with action claims by the Informal Anarchist Federation, with the aim of proving that the defendants had written these claims.[58]

Repression against Zündlumpen (#2): Investigators compared texts from the newspaper *Zündlumpen* with private letters found in house raids, hoping to prove that people had written in the newspaper.[39]

Case against Direct Action (#2): Investigators noticed linguistic similarities between action claims published by Direct Action and articles in a local quarterly publication called Resistance.[15] This led them to identify a contributor to Resistance, who was a friend of members of Direct Action, and place her under **physical surveillance (p. 45)**.

4.9.10. Trace evidence



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

Trace evidence is the small fragments of physical evidence that are transferred between objects, people, and the environment. Trace evidence can be collected and analyzed to establish links between objects, people, and places.

Trace evidence can be:

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

Trace evidence can be transferred:

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

An adversary can use trace evidence to:

- Analyze a trace from an action site to obtain useful information. For example, they can analyze a shoeprint found at an action site to determine the size and model of the shoe that left it, and then search for people who possess shoes of that size and model.
- Link a trace from an action site to an object. For example, they can determine whether textile fibers found on a fence at an action site likely come from clothing that they seized from your home during a **house raid (p. 35)**.
- Link a trace from an object to an action site. For example, they can determine whether shards of glass found on your clothing during your arrest likely come from a window that was recently broken nearby.
- Link traces from different action sites. For example, they can determine whether hammer marks found at different action sites were left by the same hammer, and therefore the actions were likely carried out by the same people.

Trace evidence does not include **fingerprints (p. 27)** and **DNA (p. 24)**, which are considered separate forensic disciplines.

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

Handwriting databases

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

See also

See also Huber and Headrick's Handwriting Identification: Facts and Fundamentals[52] for a comprehensive overview of handwriting analysis.

Mitigations

Biometric concealment (#2): An adversary can identify the characteristics of a writing sample to identify its author. To mitigate this, if you are writing an incriminating text and you want to conceal your handwriting:

- If you don't need to hide that you are concealing your handwriting, you can take as many of the following measures as possible:
  - Hold the writing instrument in an unusual way. For example, if you normally hold a pen in your right hand, hold it in your left hand instead.
  - Use a writing style that produces generic rather than unique characters. For example, use uppercase block letters rather than cursive.
  - Pause for a few seconds between each character to avoid unconsciously falling back into your writing habits.
  - Keep the text as short as possible.
- If you need to hide that you are concealing your handwriting, you can use a handwriting that looks natural but does not feature the characteristics of your normal handwriting. This is difficult and may take years of practice.

Repressive operations

Scripta Manent (#2): Handwriting samples of some of the defendants (including notes seized during raids and letters written from prison) were compared to handwritten addresses on unexploded parcel bombs in an attempt to link the defendants to the attacks.[58]

2019-2020 case against Mónica and Francisco (#2): The labels on the two parcel bombs remained intact —one because the parcel didn't explode, and one despite the explosion of the parcel.[37] The handwritten signatures on the labels were compared and positively matched. This showed that the parcels were sent by the same person.

Repression of the first Jane's Revenge arson (#2): A comparison between the cursive graffiti left at the action site and the same style of graffiti painted a few months later during a demonstration helped identify the person.[45]

4.9.9. Linguistics

Forensic linguistics is the application of linguistic knowledge to identify the author of a text or the person behind a voice. Author identification (also called *stylometry*) is based on the analysis of certain patterns of language use: vocabulary, collocations, spelling, grammar, etc. Voice identification is based on speech sounds (*phonetics*) and the acoustic qualities of the voice.

Author identification

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

- Who wrote an anonymous action claim posted on the Internet or sent to a newspaper.
- Whether multiple anonymous action claims were likely written by the same person or group.
- Who wrote a plan describing illegal activities found during a **house raid (p. 35)**, a **covert house visit (p. 16)** or an arrest.

Voice identification

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

- Who is speaking on a tapped mobile phone or a recording made by a **hidden microphone (p. 17)**.
- Who called the authorities to make a bomb threat.

See also

On the topic of author identification:

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

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

Collection

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

Analysis

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

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

Fingerprint databases

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

Other types of prints

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

See also

See the “Fingerprints” topic.[51]

Mitigations

Careful action planning (#2): An adversary can use fingerprint forensics to collect and analyze fingerprints at an action site. To mitigate this, you can carefully plan the action so that any tools you plan to use during the action are free of fingerprints in case you lose them or have to discard them in a location where they can be recovered by an adversary.

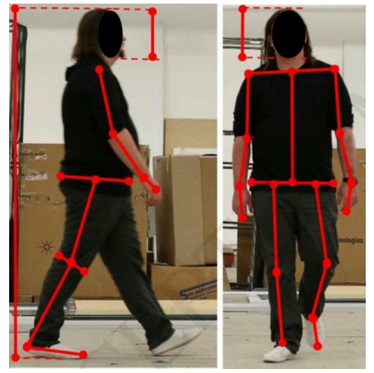
Gloves (#2): You can wear gloves to avoid leaving fingerprints on surfaces you touch.

Repressive operations

Bure criminal association case (#2): Fingerprints were collected from items found during raids, including a notebook, sheets of paper, gas masks, helmets, Molotov cocktails, and containers filled with gasoline or other substances.[21] The vast majority of the fingerprints collected did not match anyone. Some of the fingerprints collected matched individuals in the national fingerprint database.

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

4.9.7. Gait recognition



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

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

Factors of gait

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

- Intrinsic factors: how you learned to walk, your anatomy and physiology, and any injuries or pathologies you may have.

- Extrinsic factors: your clothing and the terrain on which you move (flat or not, with or without obstacles…)

Analysis

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

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

- The quality and frame rate of the footage.
- The lighting in the scene.
- Whether the two people are sufficiently close to the camera, fully visible, taking several steps, and wearing clothing that doesn't excessively hide their gait.
- Whether the two people have a generic or unique gait. For example, a person with a limp has a rather unique gait.
- Whether the two people are seen from similar angles performing the same type of movement (e.g. either walking or running).

Typical scenario

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

- A person is captured by CCTV carrying out an action. They are not recognizable because they are **dressed anonymously (#2)**. The adversary obtains the CCTV footage.
- Based on other evidence, the adversary suspects someone of having carried out the action. They obtain footage of this suspect moving, either through CCTV near their home, CCTV while they are in custody, or a **covert video surveillance device (p. 19)**.
- The adversary compares the person's gait in the first footage to the suspect's gait in the second footage to determine whether or not they could be the same person, and the confidence in that determination.

See also

See Forensic Gait Analysis: Principles and Practice[52] for a comprehensive overview of gait recognition.

Mitigations

Anonymous dress (#2): You can wear baggy clothing to conceal your gait.

Biometric concealment (#2): You can wear baggy clothing that hides your body shape, use an umbrella or other concealing objects, or drastically change your walking style by adopting a "funny walk".

Careful action planning (#2): An adversary can use gait recognition to analyze your gait on CCTV footage at or near an action site. To mitigate this, you can carefully plan the action so you avoid moving with your usual gait near a camera.

Repressive operations

Bialystok (#2): The main evidence against the person accused of an explosive attack on a police station was a comparison of his gait and the color of his coat with the corresponding characteristics of a person recorded by the surveillance cameras of the police station.[54]

Scintilla (#2): Two of the people were accused of arson because their gait and body shapes were considered compatible with people recorded by video surveillance cameras placing a canister of flammable liquid in front of an Italian post office.[55]

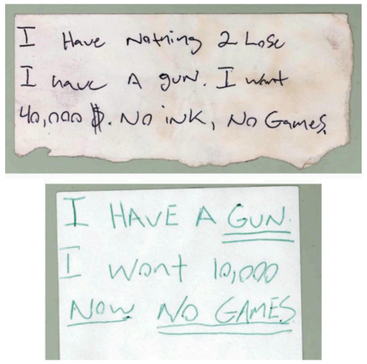
[52] Available on the Surveillance Archive.[53]

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

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

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

4.9.8. Handwriting analysis



Two robbery notes[56] showing similarities in the formation of the number "0".

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

Factors of handwriting

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

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

Analysis

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

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

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

- Whether the baseline[57] is straight or varies throughout the sample.
- The writing slant: the predominant inclination of characters relative to the baseline.

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

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

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