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

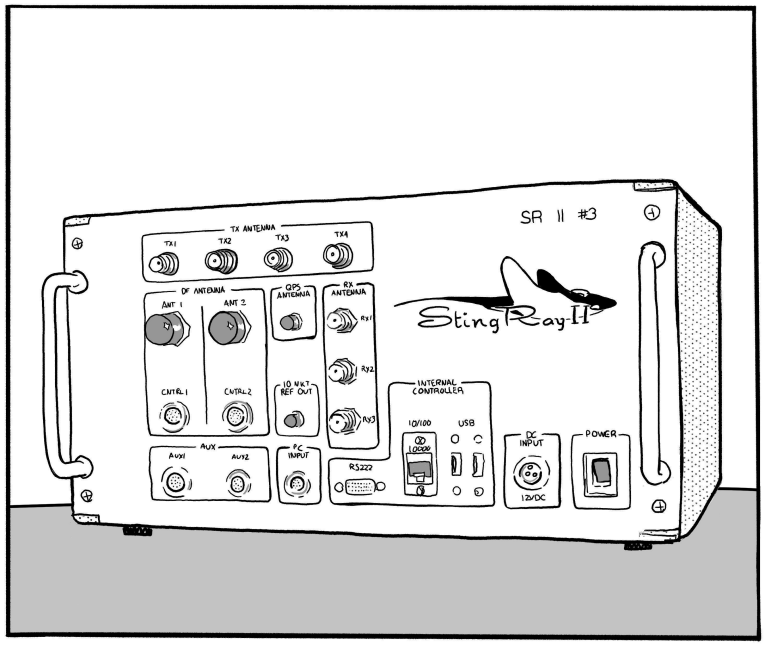
No Trace Project / No trace, no case. A collection of tools to help anarchists and other rebels **understand** the capabilities of their enemies, **undermine** surveillance efforts, and ultimately **act** without getting caught.

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

Threat Library

Part 3/5

Techniques M–T



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

Original 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

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 (#4)** is not effective).
- Compromise the device with **malware (p. 42)**.
- Compromise the device with a hardware keylogger.[71]

An adversary can physically access a device:

- During a **house raid (#2)** or a **covert house visit (#2)**.
- After arresting you if you have the device on you.
- During a border control.
- Through an **infiltrator (#2)** or **informant (#2)** that has access to the device.

Mitigations

Computer and mobile forensics (#4): You can use computer and mobile forensics to detect when a device has been physically accessed by an adversary.

Digital best practices (#4): 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 (#4): An adversary could physically access your digital devices through an **infiltrator (#2)** or **informant (#2)**. 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 (#4): You can use physical intrusion detection to detect when a space has been physically accessed by an adversary.

Tamper-evident preparation (#4): You can use tamper-evident preparation to detect when something has been physically accessed by an adversary.

[71] https://en.wikipedia.org/wiki/Hardware_keylogger

traffic. To mitigate this, you can compartmentalize different digital identities by:

- Using Tails[53] and rebooting between each session.
- Using Qubes OS[68] with different Whonix[69] virtual machines that you use non-simultaneously.

Digital best practices (#4): You can follow digital best practices, and in particular use Tor,[7] to make it harder for an adversary to monitor and analyze your network traffic.

Encryption (#4): 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 (#5): For several days, investigators analyzed the network traffic of the router used by Jeremy Hammond to establish a correlation between:[9]

- 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[70] in modern vehicles can store records of the vehicle location.

[68] https://qubes-os.org
[69] https://whonix.org
[70] https://en.wikipedia.org/wiki/Automotive_navigation_system

Contents

4. Techniques

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

Attack (#4): 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 (#4): 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.

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. 31)**, by compromising your home router with **malware (p. 42)**, 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,[7] 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. 15)** operation observed him at home to prove that the alias belonged to him.[67]

Mitigations

Compartmentalization (#4): An adversary can establish links between different digital identities through the footprints left by their network

[67] https://medium.com/beyond-install-tor-signal/case-file-jeremy-hammond-514facc780b8

Mitigations

Compartmentalization (#4): If an adversary installs malware on a Tails[53] USB stick or a Qubes OS[63] 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 (#4): 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 (#4): 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[7] or a VPN to make it harder for an adversary to remotely install malware on your digital devices through a targeted network injection.[64]

Encryption (#4): 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.[65]

Repressive operations

Scripta Manent (#5): Malware was installed on the computer of one of the defendants.[66] 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 (#5): Investigators made five requests to remotely install spyware.[14] Of these, one installation was

[63] https://www.qubes-os.org

[64] https://en.wikipedia.org/wiki/Packet_injection

[65] https://forbiddenstories.org/about-the-pegasus-project

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

Repressive operations

Fenix (#5): 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.[1]

2019-2020 case against Mónica and Francisco (#5): 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.[2]

Case against Louna (#5): Several civilians helped investigators. In particular:[3]

- 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 (#5): While trying to cross the Belarusian-Ukrainian border, the people stopped at a shop about 10 kilometers from the border.[3] A shopkeeper called the border guards on them, which led directly to their arrest.

Case against Direct Action (#5): Several civilians helped investigators.[4] In particular:

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

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

[3] Private source.

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

- 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.[5]
- 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.

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

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

people Boris was meeting with—and then identified those people by asking mobile network operators for the names corresponding to the phone numbers.[8]

Repression against Zündlumpen (#5): 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.[35]

Bure criminal association case (#5): 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.[3]

December 8 case (#5): Investigators used an IMSI-catcher during **physical surveillance (p. 15)** operations to identify the phone numbers used by some of the defendants.[39]

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[61] 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. 45)** the device.

See the "Targeted malware" topic.[62]

[61]https://en.wikipedia.org/wiki/Phishing
[62]https://notrace.how/resources/#topic=targeted-malware

associated with those phone numbers through the **collaboration of mobile network operators (p. 29)**.

- As part of a **physical surveillance (p. 15)** 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.[60]

Mitigations

Bug search (#4): 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 (#4): 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 (#5): Investigators used IMSI-catchers during **physical surveillance (p. 15)** operations to identify the phone numbers of

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

automated analysis of this data to facilitate the work of law enforcement and intelligence agencies worldwide.

See the "Digital surveillance" topic.[6]

Mitigations

Avoiding self-incrimination (#4): 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 (#4)**).

Digital best practices (#4): You can follow digital best practices to make mass digital surveillance ineffective. For example, you can use Tor[7] 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 (#4): 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).
- Records of **ID checks (#2)**, fines, arrests, investigation proceedings, judicial proceedings, and convictions.

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

Mitigations

Attack (#4): You can destroy cabinets that store police files on paper and data centers that store them digitally.

Repressive operations

Case against Boris (#5): Investigators found out that the DNA on the bottle cap belonged to Boris because his DNA was in France's national DNA database.[8]

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 (#5): 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.[9] 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 (#5): 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.[3]

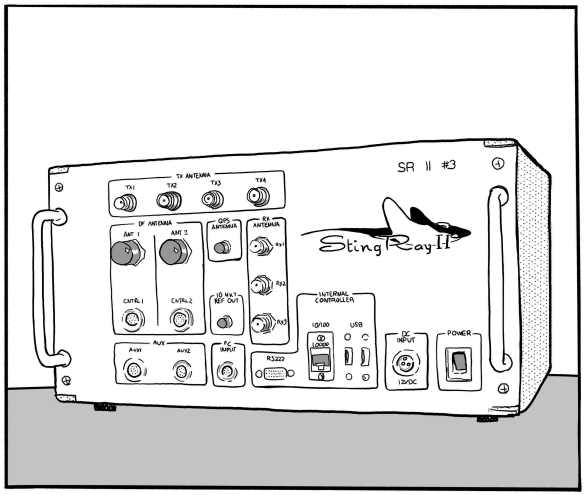
4.18.4. Video surveillance

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.

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

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

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[50] and IMEI[47] 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

- 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 (#5): Investigators bypassed the authentication of Jeremy Hammond's encrypted laptop, that they had seized in the March 2012 raid.[57] They seemingly achieved the bypass by guessing the laptop's password, which was a very simple password—either "chewy123"[58] or "chewy12345".[59]

Bure criminal association case (#5): Investigators bypassed the authentication of five encrypted storage devices found in raids:[3]

- 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.

[57] https://apnews.com/domestic-news-domestic-news-general-news-abae6d15cbf04d75bbbc58225a470f98

[58] According to press reports.

[59] According to *American Kingpin* (Nick Bilton, 2017).

Collection

Sources of CCTV footage include:

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

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

Storage

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

Analysis

An adversary can analyze CCTV footage:

- In real time if the cameras are integrated into a central network. Real-time analysis can take place either as part of routine surveillance or during exceptional events (e.g. demonstrations).
- Retroactively if the CCTV footage has been stored. Retroactive analysis can help identify a suspect by their **face (#2)**, **gait (#2)**, **voice (#2)**, etc.

Analysis of CCTV footage can be performed:

- By humans.
- By automated systems such as automated license plate readers or **facial recognition systems (#2)**.

See also

- You Can't Catch What You Can't See: Against Video Surveillance.[10]

- The topics "Video surveillance"[11] and "Automated license plate readers".[12]

Mitigations

Anonymous dress (#4): You can dress anonymously to prevent an adversary from identifying you from CCTV footage.

Anonymous purchases (#4): You can make anonymous purchases to prevent an adversary from identifying you from CCTV footage of physical stores.

Attack (#4): You can disable[13] surveillance cameras.

Biometric concealment (#4): When filmed by surveillance cameras, you can:

- To prevent **gait recognition (#2)**, 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 (#2)**, 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 (#4): You can conduct sensitive conversations away from surveillance cameras to prevent an adversary from recording those conversations with surveillance cameras equipped with microphones.

Reconnaissance (#4): 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 (#4): 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.

[10] https://notrace.how/resources/#catch-see
[11] https://notrace.how/resources/#topic=video-surveillance
[12] https://notrace.how/resources/#topic=automated-license-plate-readers
[13] https://notrace.how/resources/#destroy-cameras

- On computers, you can use the Linux FDE called LUKS, which is used by many Linux systems, such as Debian[52] and Tails,[53] and which the forensics department of the German federal police was unable to decrypt after a year of effort.[54]
- 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.[55]

Tamper-evident preparation (#4): You can use tamper-evident preparation to detect when a device has been **physically accessed (p. 45)**.

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 (#5): 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.[56]

Repression of Lafarge factory sabotage (#5): Investigators seized several encrypted smartphones in the raids and attempted to access their encrypted data, with varying results depending on the phone:[14]

- 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.

[52] https://debian.org
[53] https://tails.net
[54] https://notrace.how/resources/#parkbank
[55] https://grapheneos.org/faq#encryption
[56] 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

See the "Digital surveillance" topic.[6]

4.26.1. Authentication bypass

Authentication bypass is the process by which an adversary bypasses the **Full Disk Encryption (#4)** that protects access to a digital device. An adversary can achieve authentication bypass through human error, weak passwords, or technical exploits.

An adversary can achieve authentication bypass in the following ways:

- Accessing the device while it is turned on (and therefore its encryption is not effective).
- Finding the encryption password written down somewhere.
- Making the device owner provide the encryption password by using **interrogation techniques (#2)** including, in some contexts, **physical violence (p. 24)**.
- Visual interception: watching the device owner type the encryption password through a **hidden camera (#2)** or an **infiltrator (#2)** or **informant (#2)**.
- Brute force: guessing the encryption password through repeated, automated authentication attempts.
- Compromising the device either through remotely-installed **malware (p. 42)** or **physical access (p. 45)**.
- Exploiting a flaw at the implementation level of the encryption process.

Mitigations

Bug search (#4): Before entering a password in a room where **covert video surveillance devices (#2)** may be present, you can conduct a bug search to locate such devices and eventually remove them.

Digital best practices (#4): 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:

Repressive operations

Case against Boris (#5): 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.[8]

2019-2020 case against Mónica and Francisco (#5): 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).[2]

Repression of Lafarge factory sabotage (#5): 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.[14] In particular, footage of the interiors of buses appears to have helped identify people traveling to and from the action site.[15] Investigators also requested footage from highway toll booths, presumably to identify the occupants of known cars traveling on highways to or from the action site.

Prometeo (#5): 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.[16]

2013 case against Mónica and Francisco (#5): Public CCTV footage was used by investigators to reconstruct the movements of Mónica and Francisco before and after the action.[17] This showed that they were near the action site shortly before the explosion of the device.

Case against Peppy and Krystal (#5): CCTV footage from a bus allowed investigators to identify the license plate of the motorcycle on which

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

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

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

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

Peppy and Krystal arrived at and left the protest site.[18]

Case against Louna (#5): CCTV footage from the arson site showed two people setting fire to the excavator, and one of them burning themselves accidentally.[19]

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.[3]

Repression of the first Jane's Revenge arson (#5): 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.[20]

Bure criminal association case (#5): Investigators used footage from the demonstrations, recorded by surveillance cameras and police forces, to:[3]

- 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 (#5): 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

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

[19] 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

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

- 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[50] and IMEI[47] 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 (#5): Investigators used the collaboration of banks to obtain the bank records of organizations fighting against Cigéo.[3] 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[51] 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.

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

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

Case against Peppy and Krystal (#5): A fireworks store provided investigators with records showing that Peppy had purchased fireworks from the store three days before the protest.[18]

Case against Louna (#5): Investigators used the collaboration of the hospital to:

- Learn that a person (Louna) was hospitalized for burns.[3]
- Obtain Louna's medical file.
- Seize Louna's clothing while she was hospitalized.[19]
- 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.

buying gas and filling a gas can.[21] The cops obtained the CCTV footage the next morning.

Case against Ruslan Siddiqi (#5): Five hours after the bombing, Ruslan Siddiqi was walking away from the bombing site when he was filmed by a surveillance camera.[22] 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 (#2)**.

The State very frequently uses social media friends lists (a form of **open-source intelligence (p. 14)**) for network mapping because they do not require a warrant or legal authorization.

Mitigations

Anonymous phones (#4): You can use anonymous phones to make it harder for an adversary to map your network.

Avoiding self-incrimination (#4): 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.

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

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

Compartmentalization (#4): You can compartmentalize your different identities (or projects) to make it harder for an adversary to map your network.

Digital best practices (#4): You can follow digital best practices, and in particular use end-to-end encrypted messaging applications on encrypted devices, to obscure your social networks and make it harder for an adversary to map your network.

Fake ID (#4): 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 (#4): You can apply the need-to-know principle to make it harder for an adversary to map your network.

Network map exercise (#4): 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 (#5): To prove that the defendants knew each other and were therefore likely accomplices, the investigators used several clues:[23]

- 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.

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

Repression against Zündlumpen (#5): Investigators used the collaboration of banks to:[35]

- 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 (#5): 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.[14] This helped investigators identify a person they accused of taking photos with the camera.

- 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 (#4): 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 (#4): 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[7] to make it harder for your Internet Service Provider to provide useful information about your Internet activity to an adversary.
- Use trusted online services[49] 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 (#4): 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 (#5): 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.

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

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 (#4): 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 (#5): The photos used to identify Mónica and Francisco in public CCTV footage were found on social media.[2]

Repression of Lafarge factory sabotage (#5): Investigators collected metadata from photos of the action posted online, including the name and serial number of a camera.[14] This helped them identify a person they accused of taking the photos.

Bure criminal association case (#5): Investigators visited a Facebook page associated with the struggle against Cigéo and then analyzed the Facebook profiles of everyone who had "liked" the page.[3]

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 (#2) 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 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. 23)** surveillance operation.
- Improving the chances of successfully following the target of surveillance during a **covert (p. 17)** surveillance operation, especially at night.

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

Online services

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

- The content of unencrypted communications you make through the service (e.g. social media posts, unencrypted emails).

- 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 (#5): Investigators used the collaboration of mobile network operators to:[3]

- 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 (#5): 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.[39] 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. 15)** 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.

- 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[24]).
- Locating suspects as part of routine **police patrols (p. 26)** 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,[25] with high-quality video at night.[26]

See the "Aerial surveillance" topic.[27]

Mitigations

Anonymous dress (#4): 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 (#4): 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 (#4): 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.[28]

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

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

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

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

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

Surveillance detection (#4): 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 (#5): The arrested people were discovered at night by a helicopter on a routine surveillance flight, presumably equipped with night-vision equipment.[29] A text[30] 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 (#5): Drones were used to track rioters leaving riots in order to facilitate their arrest.[31]

Case against Direct Action (#5): 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.[4]

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.

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

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

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

- Knowing your phone IMEI number, which they can find by seizing your phone.

Mitigations

Anonymous phones (#4): You can use anonymous phones to make it harder for mobile network operators to provide useful information to an adversary.

Digital best practices (#4): 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 (#4): You can encrypt "in-motion" data to make it harder for mobile network operators to provide useful information to an adversary.

Repressive operations

Case against Boris (#5): Investigators used the collaboration of mobile network operators to intercept calls from Boris's phone or the phones of people close to him.[8] They regularly listened to the intercepted calls in real time and used information from the calls to adjust ongoing **physical surveillance (p. 15)** operations.

Mauvaises intentions (#5): 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.[23]

Case against Louna (#5): Investigators used the collaboration of mobile network operators to geolocate approximately 30 phones and intercept their calls in real time.[3] 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.

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[47] 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 (#4)**).
- Knowing your phone number, which they can find by monitoring or seizing a phone in contact with yours, using an **IMSI-catcher (p. 40)**, or through advanced correlation techniques.[48]

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

[48] 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.

Mobile

A mobile physical surveillance operation is typically conducted by a surveillance team of five to twenty operators using multiple vehicles, and typically begins with a static phase: staking out the location where the target is believed to be, such as their home or place of employment. When the target leaves the stakeout location, the surveillance team begins following them and the surveillance operation transitions into a mobile phase. The 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 (#2)** 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. 29)**.
- **Aerial surveillance (p. 15)**, 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[32] about the principles and techniques of covert physical surveillance.
- Measures Against Surveillance[33] for insights into how police and intelligence agencies conduct covert physical surveillance.
- The "Physical surveillance" topic.[34]

Mitigations

Anti-surveillance (#4): You can conduct anti-surveillance to evade a covert physical surveillance operation.

Surveillance detection (#4): You can conduct surveillance detection to detect a covert physical surveillance operation.

Transportation by bike (#4): 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.

[32] https://notrace.how/resources/#surveillance-countermeasures
[33] https://notrace.how/resources/#measures-surveillance
[34] https://notrace.how/resources/#topic=physical-surveillance

Repressive operations

Repression against Zündlumpen (#5): Investigators sent a police patrol outside a person's apartment every night at irregular times to check if she was at her apartment.[35]

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:[46] 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).

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

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 (#2)** or **civilians (p. 3)**.
- An **alarm system (#2)** (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. 7)**.
- An **infiltrator (#2)** or an **informant (#2)**.

Mitigations

Attack (#4): 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 (#4): 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 (#4): 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

Case against Boris (#5): For several weeks, investigators regularly staked out Boris's home and tailed him as he moved on foot, on bicycles, and in vehicles.[8]

Repression against Zündlumpen (#5): Investigators followed a person for 15 days.[35]

Case against Peppy and Krystal (#5): A week before the protest, investigators conducted covert physical surveillance at a local bookstore where they knew people planning the protest were organizing.[18] 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 (#5): During a physical surveillance operation against Jeremy Hammond's home that lasted several days, investigators established a correlation between:[9]

- 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 (#5): After the arson on the night of May 4 to May 5, 2024, investigators conducted several physical surveillance operations:[3]

- 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.

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

- 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 (#5): In March 2023, cops secretely observed the person from a distance of about 30 meters.[20] 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 (#5): On the night of the June arson, the arsonists were being tailed by a surveillance team—police officers in one or more

first hours of their detention.[44]

Case against Ruslan Siddiqi (#5): Ruslan Siddiqi was tortured for several days after his arrest.[22]

The torture included:[45]

Repression of the 2019 uprising in Chile (#5): 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.[31]

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. 15)**.

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”.

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

[45] beatings and electric shocks.

Mitigations

Preparing for repression (#4): 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 (#5): Most of the defendants were tortured by the Russian Federal Security Service (FSB) in the early stages of their detention in order to obtain (often fabricated) statements that could later be used to charge and convict them.[41] Most of the defendants who were tortured later retracted their statements and spoke publicly about the torture they had received.

Renata (#5): During a house raid, one of the arrested people was forced to his knees by a cop who put a gun to his temple.[42]

Belarusian anarcho-partisans (#5): The people were tortured in the first days of their detention.[43]

Warsaw 3 (#5): The people were tortured during their arrest and in the

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

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

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

unmarked cars—as they drove to the arson site.[36] 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 (#5): Investigators:[3]

- 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 (#5): 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.[21] 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 (#5): 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.[37] He then moved through the streets of Athens for a few hours, gradually joining the other people—

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

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

some of whom were wanted by police[38]—and all of them were arrested.

Case against Direct Action (#5): For several weeks, investigators followed members of Direct Action and some of their friends as they moved on foot and in vehicles.[4]

On at least one occasion, investigators witnessed a member of Direct Action conducting **anti-surveillance (#4)** maneuvers, which they found suspicious.

December 8 case (#5): For several weeks, investigators staked out the homes of some of the defendants and tailed them when they moved.[39] 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. 12)** or to incriminate individuals for actions carried out during the demonstration.

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

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

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 (#4): 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 (#5): 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.[23]

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:[40]

In some contexts, physical violence can include assassinations.

[40]

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.