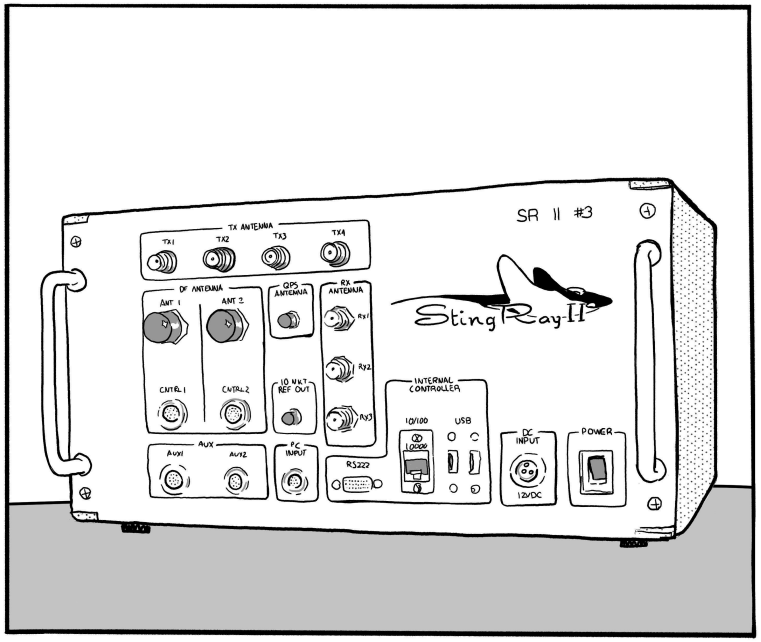
Threat Library

The Threat Library is a knowledge base of repressive techniques, mitigations that can be taken to counter them, and repressive operations where they've been used. The goal is to help anarchists and other rebels understand the options available to their adversaries, develop appropriate threat models, and ultimately succeed in their actions and projects.

Part 3/5

Techniques N–T



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.

November 4, 2025

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

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.

Original text in English

No Trace Project

notrace.how/threat-library

- 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.

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:[27]

- 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.

3.27.5. Physical access

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

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

- Computers, phones, and storage devices (e.g. hard drives, USB sticks, SD cards).
- Printers, cameras, "smart" TVs.
- Vehicles. For example, navigation systems[74] 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 (#4)** is not effective).
- Compromise the device with **malware (p. 41)**.
- Compromise the device with a hardware keylogger.[75]

An adversary can physically access a device:

- During a **house raid (#2)** or a **covert house visit (#1)**.
- After arresting you if you have the device on you.
- During a border control.

[74] https://en.wikipedia.org/wiki/Automotive_navigation_system
[75] https://en.wikipedia.org/wiki/Hardware_keylogger

Contents

3. Techniques

3.19. Network mapping

Used in tactic: **Incrimination**

Network mapping is the process by which an adversary gains insight into the organization and social relationships of a given network. By gaining this insight, an adversary can select individuals for additional scrutiny, arrest, or recruitment as **informants (#2)**.

The State very frequently uses social media friends lists (a form of **open-source intelligence (p. 5)**) 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.

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.

router with **malware (p. 41)**, 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,[47] 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. 7)** operation observed him at home to prove that the alias belonged to him.[72]

Mitigations

Compartmentalization (#4): 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[55] and rebooting between each session.
- Using Qubes OS[68] with different Whonix[73] virtual machines that you use non-simultaneously.

Digital best practices (#4): You can follow digital best practices, and in particular use Tor,[47] 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.

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

[73] https://whonix.org

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.[70]

Repressive operations

Scripta Manent (#5): Malware was installed on the computer of one of the defendants.[71] 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.[8] Of these, one installation was successful (on an iPhone SE 2020) and provided access to a Signal group conversation.

Arrest of Stecco (#5): Investigators attempted to install malware on the smartphone of someone under surveillance.[25] They sent the person an SMS with a link. If the person had clicked on the link, the malware would have been installed, allowing investigators to listen to conversations through the smartphone's microphone. But the person did not click on the link, so the malware was not installed.

3.27.4. Network forensics

Network forensics is the monitoring and analysis of network traffic.

Network information is volatile, it is designed to be transmitted and then lost, so monitoring it requires a proactive approach. Many countries have built network monitoring centers that store massive amounts of network information for days, months, or years to be analyzed later. An adversary can also monitor your network traffic with the **collaboration of your Internet Service Provider (p. 28)**, by compromising your home

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

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

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

Repression against Zündlumpen (#5): Investigators claimed that because N. and M. were partners, they likely committed arson together.[1]

Mauvaises intentions (#5): To prove that the defendants knew each other and were therefore likely accomplices, the investigators used several clues:[2]

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

Operation 8 (#5): Before the raids, investigators spent several months establishing links between people by examining metadata from:[3]

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

Repression of the attack on Clarín's headquarters (#5): After identifying the first defendant, investigators identified the other defendants by establishing links between them. Investigators found that the defen-

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

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

[3] https://putatara.net/2013/11/25/operation-8-the-evidence

dants:[4]

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

3.20. Open-source intelligence

Used in tactic: **Incrimination**

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

Mitigations

Avoiding self-incrimination (#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.[5]

Repression against Zündlumpen (#5): Investigators:[1]

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

Search for a fugitive (#5): Investigators analyzed the posts made by the person on the social media Instagram from 2019 to 2022 and found:[6]

[4]https://notrace.how/documentation/clarin-case-file.pdf
[5]https://notrace.how/resources/#monica-francisco
[6]Private source.

that has been able to install itself without interaction from the target is Pegasus.[65]

- By **physically accessing (p. 45)** the device.

See also:

- "It Could Be Harmful! Spyware Installation Through Social Engineering Attacks in Italy"[66] for an example of malware installed through phishing.
- The "Targeted malware" topic.[67]

Mitigations

Compartmentalization (#4): If an adversary installs malware on a Tails[55] USB stick or a Qubes OS[68] 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[47] or a VPN to make it harder for an adversary to remotely install malware on your digital devices through a targeted network injection.[69]

[65]https://en.wikipedia.org/wiki/Pegasus_(spyware)
[66]https://notrace.how/resources/#could-be-harmful
[67]https://notrace.how/resources/#topic=targeted-malware
[68]https://qubes-os.org
[69]https://en.wikipedia.org/wiki/Packet_injection

Repressive operations

Case against Boris (#5): Investigators used IMSI-catchers during **physical surveillance (p. 7)** 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.[22]

Repression against Zündlumpen (#5): Investigators used an IMSI-catcher to identify the phone number of N.'s mother. They used it both at the mother's home and at her workplace: the correlation of the two uses allowed them to identify the phone number.[23]

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.[6]

December 8 case (#5): Investigators used an IMSI-catcher during **physical surveillance (p. 7)** operations to identify the phone numbers used by some of the defendants.[33]

3.27.3. Malware

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

Malware can be installed on a device:

- Remotely, with interaction from the target. This is typically done through phishing,[64] which often requires the target to open a malicious file or link.
- Remotely, without interaction from the target. This type of malware is often very expensive for the adversary. An example of malware

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

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

Case against Revolutionära fronten (#5): A video of the Stockholm beating, which was filmed and posted online by the Revolutionära fronten, showed that some of the defendants were present during the beating, even though their faces were blurred[7] in the video.[6]

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.[8] 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.[6]

Operation 8 (#5): Investigators obtained information on people from web searches and newspaper articles.[3]

Repression of the attack on Clarín's headquarters (#5): Investigators analyzed social media profiles to establish links between the defendants.[4] The profile of one defendant on the social network Facebook was named "Coctel Molotov" (*Molotov cocktail*), which was considered suspicious.

3.21. Parallel construction

Used in tactic: **Incrimination**

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

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

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

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.

3.22. Physical surveillance

Used in tactic: **Incrimination**

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

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

3.22.1. Aerial

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

Examples of aerial physical surveillance include:

- Observing the crowd during demonstrations or gatherings, often as part of an **overt (p. 17)** surveillance operation.

associated with those phone numbers through the **collaboration of mobile network operators (p. 23)**.

- As part of a **physical surveillance (p. 7)** 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.[63]

Mitigations

Bug search (#4): You can conduct a bug search to detect the presence of an IMSI-catcher.

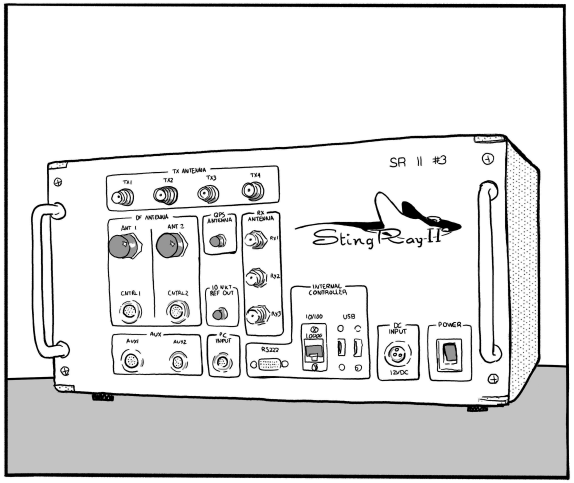
Detecting the presence of an IMSI-catcher can have several benefits:

- 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.

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

3.27.2. IMSI-catcher



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

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

- Their numbers.
- Their IMSI[50] and IMEI[45] 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

- Improving the chances of successfully following the target of surveillance during a **covert (p. 10)** 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[9]).
- Locating suspects as part of routine **police patrols (p. 20)** 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,[10] with high-quality video at night.[11]

See the "Aerial surveillance" topic.[12]

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.

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

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

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

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

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.[13]

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

Repression against Zündlumpen (#5): Drones were used to follow N. and M. in a forest during a covert physical surveillance operation.[1]

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.[14] A text[15] reports that in 2022, during another routine surveillance flight near Berlin, the same helicopter turned off its position lights and muffled the sound of its rotor blades to avoid detection: "Although the helicopter could still be heard, the noise was diminished. This can lead to misjudging the distance of the helicopter or, if mixed with other noise such as a highway, not being aware of the approaching problem until it's too late."

Operation 8 (#5): On the morning of the October 15 raids, a police helicopter was flying over an area where several raids were taking place, seemingly to surveil the area.[16]

Repression of the 2019 uprising in Chile (#5): Drones were used to track rioters leaving riots in order to facilitate their arrest.[17]

Case against Direct Action (#5): After investigators discovered the remote area where members of Direct Action hid the stolen explosives

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

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

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

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

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

- For all Android phones (whether recovered on or off) and one iPhone seized off, they extracted the phones' encrypted partitions and attempted to brute force them from a computer.

Arrest of Stecco (#5): Investigators found the PIN code of the smartphone of someone under surveillance when a camera hidden in a car captured the person entering the code.[25]

Investigators attempted to find the password of a Tails system through brute force using a software called "bruteforce-luks."

2011-2013 case against Jeremy Hammond (#5): Investigators bypassed the authentication of Jeremy Hammond's encrypted laptop, that they had seized in the March 2012 raid.[60] They seemingly achieved the bypass by guessing the laptop's password, which was a very simple password —either "chewy123"[61] or "chewy12345".[62]

Bure criminal association case (#5): Investigators bypassed the authentication of five encrypted hard drives found in raids:[6]

- 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.

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

[61] According to press reports.

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

- 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.[57]

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 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.[58]

The February arrests of N. and M. took place in a public library, while N. and M. were using a computer.[59] Police officers wearing civilian clothes waited until N. and M. had unlocked the computer to reveal themselves and make the arrest, presumably to access the computer while it was unlocked.

Repression of Lafarge factory sabotage (#5): Investigators seized several encrypted smartphones in the raids and attempted to access their encrypted data, with varying results depending on the phone:[8]

- 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.

[57] https://grapheneos.org/faq#encryption

[58] 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

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

they used in bombings, they arranged for a helicopter to fly over the area daily for surveillance purposes.[18]

3.22.2. Covert

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

Mobile

A mobile physical surveillance operation is typically conducted by a surveillance team of five to twenty operators using multiple vehicles, and typically begins with a static phase: staking out the location where the target is believed to be, such as their home or place of employment. When the target leaves the stakeout location, the surveillance team begins following them and the surveillance operation transitions into a mobile phase. The 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 (#1)** installed on the target's vehicle or bike.

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

- Real-time geolocation of the target's phone, obtained with the **collaboration of mobile network operators (p. 23)**.
- **Aerial surveillance (p. 7)**, 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[19] about the principles and techniques of covert physical surveillance.
- Measures Against Surveillance[20] for insights into how police and intelligence agencies conduct covert physical surveillance.
- The "Physical surveillance" topic.[21]

[19] https://notrace.how/resources/#surveillance-countermeasures
[20] https://notrace.how/resources/#measures-surveillance
[21] https://notrace.how/resources/#topic=physical-surveillance

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. 17)**.
- Visual interception: watching the device owner type the encryption password through a **hidden camera (#1)** 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. 41)** 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 (#1)** 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:

- On computers, you can use the Linux FDE called LUKS, which is used by many Linux systems, such as Debian[54] and Tails,[55] and which the forensics department of the German federal police was unable to decrypt after a year of effort.[56]

[54] https://debian.org
[55] https://tails.net
[56] https://notrace.how/resources/#parkbank

- Power company client records.
- Bank records.
- Overseas travel movements, in one case dating back to 1983.
- Trade Me, New Zealand's largest online auction website.

Investigators used the collaboration of the New Zealand Army to find out who, in a list of 58 people, had served in the military, presumably to identify who had military experience that they could use to contribute to the "training camps."

Repression of the attack on Clarín's headquarters (#5): One defendant was identified because he was seen on CCTV footage boarding a bus and he used his partner's electronic bus card to board the bus—investigators presumably obtained his partner's name using the collaboration of the entity that manages the bus card system.[4]

3.27. Targeted digital surveillance

Used in tactic: **Incrimination**

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

Extremely advanced techniques exist[52] 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.[53]

3.27.1. 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.

[52] https://anonymousplanet.org/guide/some-advanced-targeted-techniques
[53] https://notrace.how/resources/#topic=digital-surveillance

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.

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.[22]

Repression against Zündlumpen (#5): Investigators followed N. for 15 days.[23]

Search for a fugitive (#5): In 2022, a surveillance operator conducted, alone, covert physical surveillance of a residence.[6] Three days prior, investigators had obtained the address of the residence through the collaboration of the Supplemental Nutrition Assistance Program,[24] and had also obtained the list of purchases made through the program in the past three months. The operator saw someone drive out of the residence who matched the person's description, but failed to follow them because they were "traveling too fast." The operator then went to a nearby gas station convenience store that appeared frequently on the list of purchases. There, they found the person again. The operator asked a nearby city police officer to assist with arresting the person, but the officer declined, partly because they were in a "non-enforcement

[22] https://rupture.noblogs.org/post/2023/10/04/no-bars
[23] https://notrace.how/resources/#cops-and-robbers
[24] Supplemental Nutrition Assistance Program (SNAP) is a government food-purchasing assistance program. Each month, beneficiaries receive money on a special debit card that is part of an electronic system called electronic benefit transfer (EBT). Beneficiaries can use the card to purchase food.

capacity." The operator then requested assistance from state police, but before state police could intervene, the person had left the gas station. As the person drove away, the operator attempted to grab their wrist. Fifteen minutes later, the operator drove past the residence and saw the person leaving in the passenger seat of a vehicle but failed to follow due to heavy traffic.

Arrest of Stecco (#5): Investigators learned through a hidden microphone installed in a home that someone under surveillance would be traveling by train the next day.[25] The next day, this person and another indeed traveled by train and a large number of surveillance operators were deployed to follow them. There were four operators on the train (two at each end) and two operators waiting at each intermediate station.

Case against Peppy and Krystal (#5): A week before the protest, investigators conducted covert physical surveillance at a local bookstore where they knew people planning the protest were organizing.[26] 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:[27]

- 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:[6]

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

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

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

- 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[45] 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.[6] The bank records of one organization included a 500€ transfer entitled "*participation manif 18 fev*" ("*contribution to the February 18 demonstration*"), in reference to a demonstration in which people attacked a building associated with Cigéo.

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

Operation 8 (#5): Investigators used the collaboration of service providers to obtain information on people from many different sources, including:[3]

- Court records.
- Birth, death, and marriage records.
- Electoral registers.
- Records from Work and Income New Zealand (WINZ),[51] the State agency that provides social services.
- Property ownership records.
- Vehicle ownership records.
- Car registration records.

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

[51] Now called the Department of Work and Income.

- Seize Louna's clothing while she was hospitalized.[49]
- 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.

[49] 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

- 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 (#5): In March 2023, cops secretely observed the person from a distance of about 30 meters.[28] 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 unmarked cars—as they drove to the arson site.[29] 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:[6]

- 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.[30] The cops decided to follow the people specifically that evening because it was exactly two years since the G20

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

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

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

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.[8] This helped investigators identify a person they accused of taking photos with the camera.

Arrest of Stecco (#5): Investigators used the collaboration of several companies:[25]

- The Italian national railway manager (RFI) provided CCTV footage from train stations, lists of tickets purchased from ticket machines, and searches made on ticket machines, even when no tickets were purchased.
- The Italian national railway operator (FSI) provided a list of fines on five different lines and a list of all tickets purchased under a given name in previous months. FSI also enabled an "automated alert" system that would have notified investigators when tickets were purchased under the name.
- Banks provided:
  - The bank records of 59 people, which investigators analyzed to determine if they contained "suspicious" transactions that could indicate financial support for Stecco.
  - The bank records of an anarchist journal, which investigators requested after seeing someone read an issue of the journal in CCTV footage.
- The classified ads website subito.it provided the IP addresses used to log into an account.
- An email service provider provided data related to email addresses.

Case against Peppy and Krystal (#5): A fireworks store provided investigators with records showing that Peppy had purchased fireworks from the store three days before the protest.[26]

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

- Learn that a person (Louna) was hospitalized for burns.[6]
- Obtain Louna's medical file.

- Reduce the maximum cash withdrawal limit of N. in order to force her to make more withdrawals and increase the opportunities of locating her.

Investigators asked several companies to provide information about N.:

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

Search for a fugitive (#5): In 2022, investigators used the collaboration of service providers to obtain information about the person from:[6]

- Facebook, which provided the phone number that had been used to create an account on the social network Instagram. This account shared news about the struggle against the construction of a police training center. The phone number belonged to the person.
- The Supplemental Nutrition Assistance Program,[24] which provided a mailing address, a list of purchases made through the program in the past three months, an email address and a phone number.
- The company employing the person, which provided an email address and a phone number.
- The person's previous employer, who was interviewed but did not provide useful information.

Case against Revolutionära fronten (#5): Investigators used the collaboration of banks to obtain bank statements that showed one of the defendants had made a purchase at a Stockholm supermarket on the day of the Stockholm beating, suggesting that he was in Stockholm that day.[6]

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

Operation 8 (#5): Investigators regularly followed people on foot and in vehicles.[3]

Investigators regularly conducted covert surveillance operations near the "training camps," but did not get close enough to see what was happening and could only hear shots being fired.[6]

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.[31] He then moved through the streets of Athens for a few hours, gradually joining the other people—some of whom were wanted by police[32]—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.[18]

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.[33] 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.

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

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

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

- 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.

3.22.3. Overt

Overt physical surveillance is the direct observation of people or activities when the surveillance operators intend to be, or do not mind being, detected by their targets. This is common practice at demonstrations and gatherings to identify participants, whether to facilitate **network mapping (p. 3)** 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 (#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.[2]

3.23. Physical violence

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

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

In some contexts, physical violence can include torture. For example, in Russia and Belarus, several anarchists have been tortured in recent

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[47] to make it harder for your Internet Service Provider to provide useful information about your Internet activity to an adversary.
- Use trusted online services[48] 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.

Repression against Zündlumpen (#5): Investigators used the collaboration of banks to:[23]

- Analyze the bank records of a suspected editor of the newspaper, including bank records as old as 8 years, to determine if the person had purchased printing equipment.
- Obtain, in real time, the locations of cash withdrawals made by N. When a cash withdrawal took place, investigators would send a patrol to the withdrawal location to try to locate N. However, this did not work, seemingly because the patrol always arrived too late.

[47] https://torproject.org
[48] https://riseup.net/en/security/resources/radical-servers

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).
- 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.

years after being arrested by the State. Reported acts of torture in these countries include:[34]

In some contexts, physical violence can include assassinations.

Mitigations

Need-to-know principle (#4): If you or members of your network are at risk of being tortured by an adversary, you can apply the need-to-know principle so that each person knows as little sensitive information as possible and therefore has as little information as possible to give to torturers.

See "Under the Enemy's Blade: A Search for Anarchist Practices Against Torture"[35] about practices against torture.

Preparing for repression (#4): If you or members of your network are at risk of being tortured by an adversary, you can prepare for that risk. For example, you can:

- Set up communication protocols that allow learning as quickly as possible when someone is arrested, in order to take immediate steps to:
  - Protect the arrested person. In some contexts where torture is limited to the first hours or days of detention, putting pressure on the adversary as soon as possible after the arrest (e.g. by involving lawyers or journalists) may help to stop the torture or limit the severity of the acts of torture.
  - Protect those who are still free, in case the arrested person "talks." This will depend on what the arrested person knows, and can include abandoning **safe houses (#4)**, discontinuing projects, entering **clandestinity (#4)**, etc.
- Prepare psychologically to resist torture.

[34] 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.

[35] https://notrace.how/resources/#under-enemy-blade

See "Under the Enemy's Blade: A Search for Anarchist Practices Against Torture"[35] about practices against torture.

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.[36] 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.[37]

Case against Amos Mbedzi (#5): Mbedzi was tortured in the first days of his detention.[38]

Belarusian anarcho-partisans (#5): The people were tortured in the first days of their detention.[39]

Warsaw 3 (#5): The people were tortured during their arrest and in the first hours of their detention.[40]

Case against Ruslan Siddiqi (#5): Ruslan Siddiqi was tortured for several days after his arrest.[41] Under torture, he confessed to carrying out the train bombing and the attack on the military airfield.

The torture included:[42]

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

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

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

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

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

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

[42] beatings and electric shocks.

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.[33] 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. 7)** operation, but lost sight of them. In the following hour, they geolocated the defendant's phone in real time to locate them. As a result, one hour after losing sight of the defendant, investigators regained sight of them and resumed the physical surveillance operation.

3.26.2. Other

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

Stores

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

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

Additionally, physical stores can provide:

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

Bure criminal association case (#5): Investigators used the collaboration of mobile network operators to:[6]

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

Operation 8 (#5): Investigators used the collaboration of mobile network operators to intercept calls and text messages.[3] The intercepted text messages revealed the dates and locations of the "training camps" and who attended them.

Repression of the attack on Clarín's headquarters (#5): Investigators used the collaboration of mobile network operators to:[4]

- Analyze the activity of some of the defendants' phones at the time of the attack. Several phones were seemingly turned off shortly before the attack and turned back on shortly after, which was considered suspicious. For example, one phone was seemingly turned off ten minutes before the attack and turned back on approximately two hours after.
- Geolocate the phones of some of the defendants retroactively. This showed that:
  - One defendant spent time near the attack site the day before the attack.
  - One defendant was present at the attack site a few minutes before the attack.
- Intercept phone calls. In intercepted calls, some of the defendants expressed solidarity with those targeted by the investigation and concern about being targeted themselves.

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.[17]

3.24. Police patrols

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

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

Means of transportation

Police patrols can use different means of transportation:

- Marked or unmarked vehicles.
- Foot movement.
- **Helicopters, drones and surveillance planes (p. 7)**.

Routine patrols

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

Patrols in response to a threat

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

- A routine patrol stumbling upon the threat by chance.

- **Guards (#2)** or **civilians (#2)**.
- An **alarm system (#1)** (e.g. motion detectors inside a building), either directly or through a security company monitoring the alarm system.
- Police officers monitoring live **CCTV footage (#2)**.
- 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

Repression against Zündlumpen (#5): Investigators sent a police patrol outside of N.'s apartment every night at irregular times to check if she was at her apartment.[23]

Case against Revolutionära fronten (#5): After the nighttime visit to the fascist's house, the fascist called the police, who sent out a patrol.[6] On its way to the house, the patrol stopped the defendants' car, presumably because it looked suspicious, and checked their identities.

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.[2]

Arrest of Stecco (#5): Investigators used the collaboration of mobile network operators to:[25]

- Intercept the calls of more than 40 phones.
- Retroactively analyze the phone activity of 69 phones and one phone booth. In particular, once investigators thought they had found the general area where Stecco was living, they checked:
  - Whether any of the 69 phones had called a phone in the area in the past 6 years.
  - Whether Stecco had called a phone in the area in the 5 years before he went on the run.

Case against Amos Mbedzi (#5): Investigators found Mbedzi's and his comrades' phones at the bombing site, and used the collaboration of mobile network operators to retrospectively geolocate them and analyze their call history.[38] This showed that Mbedzi and his comrades regularly called each other and therefore knew each other, and had traveled together from South Africa to Eswatini the night before the bombing attempt.

Case against Louna (#5): Investigators used the collaboration of mobile network operators to geolocate approximately 30 phones and intercept their calls in real time.[6] 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.

- 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.[22] They regularly listened to the intercepted calls in real time and used information from the calls to adjust ongoing **physical surveillance (p. 7)** operations.

Repression against Zündlumpen (#5): Investigators used the collaboration of mobile network operators to:

- Intercept the calls of N.'s mother.[23] This allowed them to learn that N. was planning to visit her mother for Christmas, which allowed them to place N. under **physical surveillance (p. 7)**.
- Intercept the calls of people suspected of being close to N. and M.[1]

Search for a fugitive (#5): In 2022, investigators used the collaboration of mobile network operators to obtain information about the person's phone over a seven-month period, including:[6]

- Which other phones it had called and when.
- Which cell towers it had connected to and when. However, they did not obtain a more precise geolocation of the phone.

Case against Revolutionära fronten (#5): Investigators used the collaboration of mobile network operators to retroactively geolocate the phones of some of the defendants on the day of the Stockholm beating.[6] This showed that, on that day:

- Some phones had moved to Stockholm, suggesting that their owners had also traveled to Stockholm.
- Some other phones were turned off early in the morning and turned back on late at night, suggesting that their owners may have turned off their phones to avoid being tracked when going to Stockholm.

3.25. Roadblocks

Used in tactics: **Arrest, Incrimination**

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

An adversary can set up roadblocks:

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

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

Mitigations

Attack (#4): You can attack roadblocks to disrupt them.

Careful action planning (#4): You can carefully plan an action to take into account the risk of roadblocks being set up after the action on roads surrounding the action site.

Repressive operations

Operation 8 (#5): On the morning of the October 15 raids, police set up a roadblock on the only road leading to an area where several raids were taking place.[16] For most of the day, cops staffing the roadblock searched, questioned, and photographed people passing on the road.[43]

3.26. Service provider collaboration

Used in tactic: **Incrimination**

Service provider collaboration is the process by which an entity that has information about you because it provides a service to you provides that

[43] https://rnz.co.nz/news/national/135737/ipca-criticises-illegal-searches-during-urewera-raids

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:[44] obtaining service provider information through unauthorized exposure, disclosure, or loss of the information (e.g., a service provider database is hacked and an adversary buys it on the black market).

3.26.1. Mobile network operators

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

They can provide:

- Given a name: the phone numbers registered under that name.
- Given a phone number: the name under which the phone number is registered and the IMEI number[45] of the phone in which the phone number is used.

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

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

- 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. 39)**, or through advanced correlation techniques.[46]
- 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.

[46] 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.