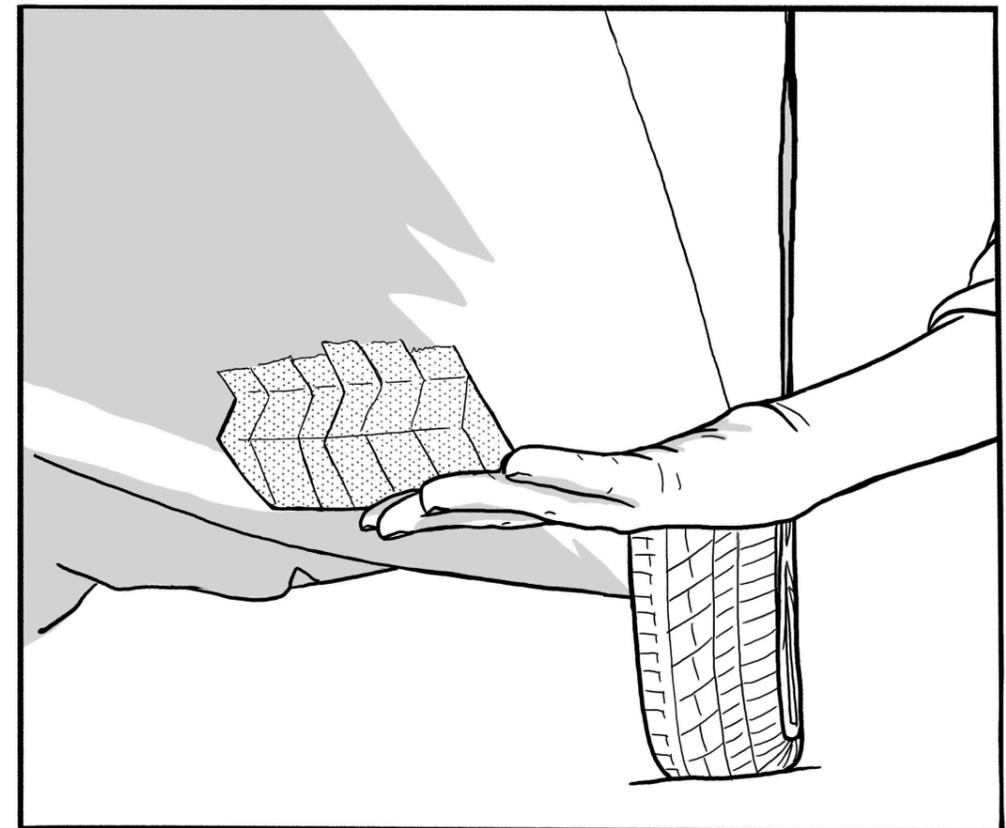


Threat Library

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 1/2 About Tactics Techniques



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.

Threat Library

Part 1/2: About, Tactics, Techniques

Part 2/2: Mitigations, Repressive operations, Countries, Tutorial, Contribute

Original text in English

No Trace Project

notrace.how/threat-library

- Using Qubes OS¹⁵⁰ with different Whonix¹⁵⁵ virtual machines that you use non-simultaneously.

Digital best practices (#2): You can follow digital best practices, and in particular use Tor,¹⁰³ to make it harder for an adversary to monitor and analyze your network traffic.

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

REPRESSIVE OPERATIONS

2011-2013 case against Jeremy Hammond (#2): For several days, investigators analyzed the network traffic of the router used by Jeremy Hammond to establish a correlation between:⁹³

- 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 systems¹⁵⁶ in modern vehicles can store records of the vehicle location.

If an adversary physically accesses a device, they can:

- Read the device unencrypted data, or its encrypted data if it is turned on (and therefore its **encryption (#2)** is not effective).
- Compromise the device with **malware (p. 60)**.
- Compromise the device with a hardware keylogger.¹⁵⁷

¹⁵⁵<https://whonix.org>

¹⁵⁶https://en.wikipedia.org/wiki/Automotive_navigation_system

¹⁵⁷https://en.wikipedia.org/wiki/Hardware_keylogger

An adversary can physically access a device:

- During a **house raid (p. 33)** or a **covert house visit (p. 8)**.
- After arresting you if you have the device on you.
- During a border control.
- Through an **infiltrator (p. 36)** or **informant (p. 37)** that has access to the device.

MITIGATIONS

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

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

Network map exercise (#2): An adversary could physically access your digital devices through an **infiltrator (p. 36)** or **informant (p. 37)**. To mitigate this, you can conduct a network map exercise to help you decide who you trust to access your digital devices.

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

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

virtual machine that you use for different digital identities, they can tie the different identities together. To mitigate this, you can use different Tails USB sticks or Qubes OS virtual machines for different digital identities.

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

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

- Follow best practices against phishing to make it harder for an adversary to trick you into installing malware on your digital devices.
- Use Tor¹⁰³ or a VPN to make it harder for an adversary to remotely install malware on your digital devices through a targeted network injection.¹⁵¹

Encryption (#2): You can encrypt “in-motion” data to make it harder for an adversary to install malware through *network packet injection*, an installation vector for some malware, such as Pegasus.¹⁵²

REPRESSIVE OPERATIONS

Scripta Manent (#2): Malware was installed on the computer of one of the defendants.¹⁵³ The malware, which was installed remotely over the Internet, targeted a Windows computer and was capable of recording text typed on the keyboard, taking periodic screenshots, and recording communications sent and received to and from the computer.

Repression of Lafarge factory sabotage (#2): Investigators made five requests to remotely install spyware.⁵⁰ Of these, one installation was successful (on an iPhone SE 2020) and provided access to a Signal group conversation.

Arrest of Stecco (#2): Investigators attempted to install malware on the smartphone of someone under surveillance.¹⁷ 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. 55), by compromising your home router with **malware** (p. 60), 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,¹⁰³ an adversary monitoring your network traffic knows that you use Tor, but not what websites you visit or what you do on those websites.

Tor is vulnerable to correlation attacks, but such attacks are difficult to set up even for powerful adversaries. An example of a successful correlation attack is the prosecution of anarchist hacker Jeremy Hammond: the times when the alias he used in chat rooms was “online” (obtained through network traffic analysis) were correlated with the times when a **physical surveillance** (p. 45) operation observed him at home to prove that the alias belonged to him.¹⁵⁴

MITIGATIONS

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

- Using Tails⁵⁷ and rebooting between each session.

¹⁵¹https://en.wikipedia.org/wiki/Packet_injection

¹⁵²<https://forbiddenstories.org/about-the-pegasus-project>

¹⁵³<https://earsandeyes.noblogs.org/post/2019/01/27/more-precisions-keylogger-italy>

¹⁵⁴<https://medium.com/beyond-install-tor-signal/case-file-jeremy-hammond-514facc780b8>

Contents

1. About the Threat Library	4
1.1. Threat modeling	4
1.2. The Threat Library	4
1.3. Limitations	4
2. Tactics	6
2.1. Deterrence	6
2.2. Incrimination	6
2.3. Arrest	6
3. Techniques	7
3.1. Alarm systems	7
3.2. Biased interpretation of evidence	7
3.3. Covert house visit	8
3.4. Covert surveillance devices	9
3.4.1. Audio	10
3.4.2. Location	11
3.4.3. Video	12
3.5. Detection dogs	13
3.6. Door knocks	15
3.7. Doxing	15
3.8. Evidence fabrication	16
3.9. Forensics	16
3.9.1. Arson	16
3.9.2. Ballistics	19
3.9.3. DNA	20
3.9.4. Digital	23
3.9.5. Facial recognition	24
3.9.6. Fingerprints	25
3.9.7. Gait recognition	26
3.9.8. Handwriting analysis	27
3.9.9. Linguistics	29
3.9.10. Trace evidence	30
3.10. Guards	33
3.11. House raid	33
3.12. ID checks	35
3.13. Increased police presence	35
3.14. Infiltrators	36
3.15. Informants	37
3.16. International cooperation	38
3.17. Interrogation techniques	38
3.18. Mass surveillance	39
3.18.1. Civilian snitches	39
3.18.2. Mass digital surveillance	40
3.18.3. Police files	41
3.18.4. Video surveillance	41
3.19. Network mapping	44
3.20. Open-source intelligence	44
3.21. Parallel construction	45
3.22. Physical surveillance	45

3.22.1. Aerial	45
3.22.2. Covert	47
3.22.3. Overt	50
3.23. Physical violence	50
3.24. Police patrols	51
3.25. Roadblocks	52
3.26. Service provider collaboration	52
3.26.1. Mobile network operators	52
3.26.2. Other	55
3.27. Targeted digital surveillance	58
3.27.1. Authentication bypass	58
3.27.2. IMSI-catcher	59
3.27.3. Malware	60
3.27.4. Network forensics	61
3.27.5. Physical access	62

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.¹⁴⁵

MITIGATIONS

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

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

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

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

REPRESSIVE OPERATIONS

Case against Boris (#2): Investigators used IMSI-catchers during **physical surveillance (p. 45)** operations to identify the phone numbers of people Boris was meeting with—and then identified those people by asking mobile network operators for the names corresponding to the phone numbers.²²

Repression against Zündlumpen (#2): 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.⁴⁷

¹⁴⁵<https://notrace.how/resources/#topic=imsi-catchers>

Bure criminal association case (#2): Investigators used IMSI-catchers to identify the phone numbers of people who lived in places associated with the struggle against Cigéo or who participated in demonstrations.⁷

December 8 case (#2): Investigators used an IMSI-catcher during **physical surveillance (p. 45)** operations to identify the phone numbers used by some of the defendants.²⁰

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,¹⁴⁶ 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 that has been able to install itself without interaction from the target is Pegasus.¹⁴⁷
- By **physically accessing (p. 62)** the device.

See also:

- “It Could Be Harmful! Spyware Installation Through Social Engineering Attacks in Italy”¹⁴⁸ for an example of malware installed through phishing.
- The “Targeted malware” topic.¹⁴⁹

MITIGATIONS

Compartmentalization (#2): If an adversary installs malware on a Tails⁵⁷ USB stick or a Qubes OS¹⁵⁰

¹⁴⁶<https://en.wikipedia.org/wiki/Phishing>

¹⁴⁷[https://en.wikipedia.org/wiki/Pegasus_\(spyware\)](https://en.wikipedia.org/wiki/Pegasus_(spyware))

¹⁴⁸<https://notrace.how/resources/#could-be-harmful>

¹⁴⁹<https://notrace.how/resources/#topic=targeted-malware>

¹⁵⁰<https://qubes-os.org>

1. About the Threat Library

The February arrests of N. and M. took place in a public library, while N. and M. were using a computer.²⁸ 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 (#2): Investigators seized several encrypted smartphones in the raids and attempted to access their encrypted data, with varying results depending on the phone.⁵⁰

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

Arrest of Stecco (#2): 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.¹⁷

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

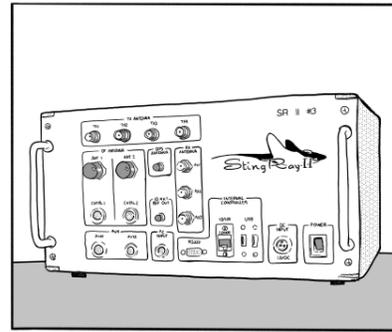
2011-2013 case against Jeremy Hammond (#2): Investigators bypassed the authentication of Jeremy Hammond's encrypted laptop, that they had seized in the March 2012 raid.¹⁴² They seemingly achieved the bypass by guessing the laptop's password, which was a very simple password—either “chewy123”¹⁴³ or “chewy12345”.¹⁴⁴

Bure criminal association case (#2): Investigators bypassed the authentication of five encrypted hard drives found in raids:⁷

- 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.

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 IMSI¹³⁵ and IMEI¹³² numbers.
- Data and metadata about their activity: the content of SMS and regular calls, the list of visited websites, metadata about the use of end-to-end encrypted messaging applications (e.g. when Signal is used and the approximate size of messages sent or received through Signal).

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

- At a public demonstration, to record the phone numbers of all the phones present at the demonstration and later obtain the names associated with those phone numbers through the **collaboration of mobile network operators** (p. 52).
- As part of a **physical surveillance** (p. 45) operation to record the target's phone number or the

No matter what, we make and will continue to make mistakes in the battle against such strong oppressive mechanisms. Mistakes that will always “cost” more compared to the cops' mistakes which are “absorbed.” We must weigh the situations again and ensure that the mistakes which happened once simply can not happen again. We must study and appreciate the accumulated experience of so many years and, taking into account the tendency to prepare for the battles which already took place and not for those that will come, let's be prepared and may luck be on our side...

— anarchist comrades from Greece, in a text¹ detailing the surveillance that led to their arrest, 2013

1.1. Threat modeling

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

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

1.2. The Threat Library

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

- An **adversary** is an entity that wants to prevent you from achieving your goals, from carrying out your actions and projects. Typically your adversary is the State, but depending on your

context you may have other adversaries (e.g., fascist groups).

- A **technique** (or *threat*) is something an adversary does to prevent you from achieving your goals.
- A **mitigation** is something you do to lower the risk of a technique being successful.
- A **tactic** is an adversary's goal when using a technique. In the Threat Library, we organize techniques into three tactics: deterrence, incrimination and arrest.
- A **repressive operation** is a real instance of repression from an adversary against anarchists or other rebels.
- An **action or project** is what you want to accomplish: participate in a riot, publish subversive literature, smash something, burn something...

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

1.3. Limitations

The Threat Library is by design a very technical approach to anti-repression. Threat modeling is done at the level of actions, and thus does not attempt to contribute to the social question, how to escape the enclosure that repression seeks, how to intervene in

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

^a<https://notrace.how/resources/#not-stupid>

^b<https://actforfree.noblogs.org/post/2022/04/17/grenoblefrance-these-saboteurs-of-the-ultra-left-have-been-elusive-for-five-years>

¹<https://notrace.how/resources/#nea-philadelphia>

¹⁴²<https://apnews.com/domestic-news-domestic-news-general-news-abae6d15cbf04d75bbbc58225a470f98>

¹⁴³According to press reports.

¹⁴⁴According to *American Kingpin* (Nick Bilton, 2017).

social tensions, and so on. Struggles for freedom are not primarily a technical matter, but a social one, and have psychological and emotional effects. As much as possible, we encourage you to take time before, during and after an action to discuss with all the people involved and to make sure that everyone's emotional needs are taken into account.

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

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.⁶⁰

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 exist¹³⁷ 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.¹⁰²

3.27.1. Authentication bypass

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

An adversary can achieve authentication bypass in the following ways:

- Accessing the device while it is turned on (and therefore its encryption is not effective).
- Finding the encryption password written down somewhere.
- Making the device owner provide the encryption password by using **interrogation techniques (p. 38)** including, in some contexts, **physical violence (p. 50)**.
- Visual interception: watching the device owner type the encryption password through a **hidden camera (p. 12)** or an **infiltrator (p. 36)** or **informer (p. 37)**.
- Brute force: guessing the encryption password through repeated, automated authentication attempts.
- Compromising the device either through remotely-installed **malware (p. 60)** or **physical access (p. 62)**.

- Exploiting a flaw at the implementation level of the encryption process.

MITIGATIONS

Bug search (#2): Before entering a password in a room where **covert video surveillance devices (p. 12)** may be present, you can conduct a bug search to locate such devices and eventually remove them.

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

- On computers, you can use the Linux FDE called LUKS, which is used by many Linux systems, such as Debian¹³⁸ and Tails,⁵⁷ and which the forensics department of the German federal police was unable to decrypt after a year of effort.¹³⁹
- 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.¹⁴⁰

Tamper-evident preparation (#2): You can use tamper-evident preparation to detect when a device has been **physically accessed (p. 62)**.

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

REPRESSIVE OPERATIONS

Repression against Zündlumpen (#2): In some of the 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.¹⁴¹

¹³⁷<https://anonymouspanet.org/guide/some-advanced-targeted-techniques>

¹³⁸<https://debian.org>

¹³⁹<https://notrace.how/resources/#parkbank>

¹⁴⁰<https://grapheneos.org/faq#encryption>

¹⁴¹<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>

- Seize Louna's clothing while she was hospitalized.⁸⁰
- Obtain the phone number of someone close to Louna that Louna had given to the hospital.
- Obtain CCTV footage from the hospital.
- Obtain information from the hospital's parking payment system.
- Learn the time and place of an appointment Louna had at the hospital a few days after the arson.

Investigators also used the collaboration of several State institutions:

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

Investigators used the collaboration of several companies:

- Banks provided:
 - Bank information of several people, including many members of Louna's family.
 - IP addresses used to make online bank transfers.
 - Locations where people had withdrawn cash.
- An insurance company provided a person's address and list of roommates.
- The highway operator Vinci provided CCTV footage of highway toll booths.
- The French national railway company (SNCF) provided information about people who had booked seats next to people under investigation, including their photos and bank information.
- The carpooling service BlaBlaCar provided information about people who had used the service, including their photos, bank information, and the trips they had taken.
- The car manufacturer Stellantis provided the IMSI¹³⁵ and IMEI¹³² numbers of a car's embedded location system. However, investigators

were unable to locate the car because, for some unknown reason, it did not transmit its location.

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

Bure criminal association case (#2): Investigators used the collaboration of banks to obtain the bank records of organizations fighting against Cigéo.⁷ 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 (#2): Investigators used the collaboration of service providers to obtain information on people from many different sources, including:⁶

- Court records.
- Birth, death, and marriage records.
- Electoral registers.
- Records from Work and Income New Zealand (WINZ),¹³⁶ the State agency that provides social services.
- Property ownership records.
- Vehicle ownership records.
- Car registration records.
- 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 (#2): One defendant was identified because he

¹³⁵An International Mobile Subscriber Identity (IMSI) number is a number that uniquely identifies a SIM card.

¹³⁶Now called the Department of Work and Income.

2. Tactics

2.1. Deterrence

Uses techniques:

- Door knocks (p. 15)
- Doxing (p. 15)
- Increased police presence (p. 35)
- Mass surveillance (p. 39)
- Physical violence (p. 50)
- Police patrols (p. 51)

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

2.2. Incrimination

Uses techniques:

- Biased interpretation of evidence (p. 7)
- Covert house visit (p. 8)
- Covert surveillance devices (p. 9)
- Detection dogs (p. 13)
- Door knocks (p. 15)
- Evidence fabrication (p. 16)
- Forensics (p. 16)
- House raid (p. 33)
- ID checks (p. 35)
- Infiltrators (p. 36)
- Informants (p. 37)
- International cooperation (p. 38)
- Interrogation techniques (p. 38)
- Mass surveillance (p. 39)
- Network mapping (p. 44)
- Open-source intelligence (p. 44)
- Parallel construction (p. 45)
- Physical surveillance (p. 45)
- Physical violence (p. 50)
- Police patrols (p. 51)
- Roadblocks (p. 52)
- Service provider collaboration (p. 52)
- Targeted digital surveillance (p. 58)

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

2.3. Arrest

Uses techniques:

- Alarm systems (p. 7)
- Detection dogs (p. 13)
- Guards (p. 33)
- House raid (p. 33)
- ID checks (p. 35)
- Increased police presence (p. 35)
- International cooperation (p. 38)
- Police patrols (p. 51)
- Roadblocks (p. 52)

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

3. Techniques

3.1. Alarm systems

Used in tactic: **Arrest**

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

For physical infrastructure, modern alarm systems typically include sensors that detect unauthorized access to an area outside of normal operating hours. Such sensors include infrared motion detectors, sensors that detect the opening of doors, and many other types of sensors.³ The alert signal can be sent over a wired or wireless connection—low-cost modern systems often send the signal over the mobile phone network.

For digital infrastructure, intrusion detection systems⁴ monitor for any activity that might indicate a hack is in progress. If unauthorized access is detected, an incident response team can be notified to attempt to contain and remediate any compromise.

MITIGATIONS

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

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

Digital best practices (#2): When carrying out a cyber action, you can use digital evasion techniques⁵

³https://en.wikipedia.org/wiki/Security_alarm#Sensor_types

⁴https://en.wikipedia.org/wiki/Intrusion_detection_system

⁵https://en.wikipedia.org/wiki/Intrusion_detection_system_evasion_techniques

to prevent intrusion detection systems from detecting the action.

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

3.2. Biased interpretation of evidence

Used in tactic: **Incrimination**

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

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

MITIGATIONS

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

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

REPRESSIVE OPERATIONS

Operation 8 (#2): The case was characterized by a lack of evidence that the defendants were planning a specific attack, and relied instead on interpretation of circumstantial evidence.⁶ For example:

⁶<https://putatara.net/2013/11/25/operation-8-the-evidence>

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.
- 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 (#2): In 2022, investigators used the collaboration of service providers to obtain information about the person from:⁷

- 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,¹²² 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 (#2): 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.⁷

Repression of Lafarge factory sabotage (#2): Investigators gave the serial number of a camera to the camera manufacturer, and the manufacturer gave them the name of the store where the camera was sold.⁵⁰ This helped investigators identify a person they accused of taking photos with the camera.

Arrest of Stecco (#2): Investigators used the collaboration of several companies:¹⁷

- 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 (#2): A fireworks store provided investigators with records showing that Peppy had purchased fireworks from the store three days before the protest.¹⁰

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

- Learn that a person (Louna) was hospitalized for burns.⁷
- Obtain Louna's medical file.

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.

Banks

Banks can provide:

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

Internet service providers

Internet service providers can provide:

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

Online services

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

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

Postal services

Postal services can allow an adversary to monitor your mail.

State institutions

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

MITIGATIONS

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

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

- Use Tor¹⁰³ to make it harder for your Internet Service Provider to provide useful information about your Internet activity to an adversary.
- Use trusted online services¹³⁴ that will refuse to comply with an adversary's requests to access your data, or build their service to make it technically impossible to comply with such requests.

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

REPRESSIVE OPERATIONS

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

Repression against Zündlumpen (#2): Investigators used the collaboration of banks to:⁴⁷

- Analyze the bank records of a suspected editor of the newspaper, including bank records as old as

¹³⁴<https://riseup.net/en/security/resources/radical-servers>

- Activities captured by hidden cameras at the “training camps”—training with firearms, learning military tactics, experimenting with Molotov cocktails—were interpreted as preparation for violently seizing control of part of New Zealand's territory.
- In private conversations recorded by microphones installed in vehicles, some defendants made boasting or unserious comments, including about “going to war,” acquiring a long-range sniper rifle, assassinating George W. Bush, or killing Pākehā (New Zealanders of European descent). These comments were interpreted as indicative of violent intentions.⁷

December 8 case (#2): The case was characterized by a lack of evidence that the defendants were planning a specific attack, and relied instead on interpretation of circumstantial evidence.⁸ For example:

- Libre Flot gained combat experience in Rojava, which was interpreted as an attempt to gain experience in order to carry out attacks in France.
- Libre Flot stole fertilizer from a store, intending to use it to create small explosives. The theft was interpreted as an attempt to obtain fertilizer without leaving traces.
- On two occasions, some of the defendants created small explosives from household or agricultural products, and detonated them in isolated areas where the explosions would not damage anything, which was interpreted as tests for possible future attacks (despite the defendants' claims that they were just doing it for fun).
- Some of the defendants participated in airsoft games, which were interpreted as paramilitary trainings.
- Handwritten notes of one of the defendants contained terms and phrases such as “weapons”, “recruitment”, “cleaning DNA”, “incendiary device” and “are we ready for a comrade to be wounded or killed?”, which were interpreted as indicative that the defendant was preparing an attack in France (despite the defendant's claims that the notes were about either airsoft or Rojava).

⁷Private source.

⁸https://web.archive.org/web/20250615210912/https://soutien812.blackblogs.org/wp-content/uploads/sites/1922/2023/11/CompteRenduProces_A4.pdf

- In private conversations, some of the defendants made light-hearted, boasting comments such as “I want to burn all the banks, all the cops” and “if a police officer was on ground, honestly I would finish him off”, which were interpreted as indicative of violent intentions.
- The defendants used secure digital communication tools, which was interpreted as indicative of “clandestine behavior”.

3.3. Covert house visit

Used in tactic: **Incrimination**

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

An adversary can conduct a covert house visit to:

- Gather information.
- Install **covert surveillance devices (p. 9)** in the residence.
- Install **malware (p. 60)** on digital devices.

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

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

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

MITIGATIONS

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

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

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

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

REPRESSIVE OPERATIONS

Repression against Zündlumpen (#2): Investigators made a covert visit of the cabins where N. and M. lived in order to collect **scent samples (p. 13)**.⁹

Case against Peppy and Krystal (#2): Investigators conducted a covert search of the trash outside the home of Peppy and Krystal, where they found suspicious documents.¹⁰

Case against Direct Action (#2): After overhearing (presumably during a **physical surveillance (p. 45)** operation) that four members of Direct Action who lived together in a house were leaving the house for two days to go camping, investigators conducted two covert visits of the house over those two days:¹¹

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

3.4. Covert surveillance devices

Used in tactic: **Incrimination**

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

Where

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

- Microphones and cameras hidden inside the home of a target.
- Location trackers hidden in or on the vehicle of a target.

- Cameras hidden at the windows of a building close to the home of a target, such that the cameras can film the entrance to the home.

When

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

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

Power supply

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

Data transmission

Covert surveillance devices often transmit the data they collect:

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

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

See also

- Ears and Eyes.¹²
- The “Hidden devices” topic.¹³

geolocate phones (both retrospectively and in real time) and to record phone calls.³⁷

Arrest of Stecco (#2): Investigators used the collaboration of mobile network operators to:¹⁷

- 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 (#2): 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.⁵² 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 (#2): Investigators used the collaboration of mobile network operators to geolocate approximately 30 phones and intercept their calls in real time.⁷ In particular, investigators used the intercepted calls to:

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

Bure criminal association case (#2): Investigators used the collaboration of mobile network operators to:⁷

- 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 (#2): Investigators used the collaboration of mobile network operators to intercept calls and text messages.⁶ 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 (#2): Investigators used the collaboration of mobile network operators to:⁶⁰

- 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.

December 8 case (#2): Investigators used the collaboration of mobile network operators to geolocate the phones of the defendants and of people close to them in real time and to record unencrypted phone conversations.²⁰ In particular:

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

⁹<https://de.indymedia.org/node/548259>

¹⁰<https://notrace.how/documentation/case-against-peppy-and-krystal-affidavit.pdf>

¹¹<https://archive.org/details/direct-action-memoirsofan-urban-guerrilla>

¹²<https://notrace.how/earsandeyes>

¹³<https://notrace.how/resources/#topic=hidden-devices>

number¹³² of the phone in which the phone number is used.

- Given an IMEI number: the phone number that is used in the phone with that IMEI number.

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

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

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

- Knowing your name (if your phone is not **anonymous (#2)**).
- Knowing your phone number, which they can find by monitoring or seizing a phone in contact with yours, using an **IMSI-catcher (p. 59)**, or through advanced correlation techniques.¹³³
- Knowing your phone IMEI number, which they can find by seizing your phone.

MITIGATIONS

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

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

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

¹³³For 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.

Encryption (#2): 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 (#2): 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. 45)** operations.

Repression against Zündlumpen (#2): Investigators used the collaboration of mobile network operators to:

- Intercept the calls of N.'s mother.⁴⁷ 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. 45)**.
- Intercept the calls of people suspected of being close to N. and M.⁹

Search for a fugitive (#2): In 2022, investigators used the collaboration of mobile network operators to obtain information about the person's phone over a seven-month period, including:⁷

- 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 (#2): 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.⁷ 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.

Mauvaises intentions (#2): Investigators used the collaboration of mobile network operators to link phone numbers to civil identities, to know which phone numbers were in contact with each other, to

3.4.1. Audio



A microphone found inside a neon ceiling light in Modena, Italy, in December 2015.¹⁴

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

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

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

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

Recorded conversations can be used as evidence in court if incriminating matters are discussed, or if they can be misconstrued to appear incriminating in the eyes of a judge. Non-incriminating, mundane conversations can reveal a great deal about the targets of surveillance and help in **network mapping (p. 44)**. See **Ears and Eyes**¹² and the “Hidden devices” topic.¹³

MITIGATIONS

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

Outdoor and device-free conversations (#2): You can conduct sensitive conversations outdoors and without electronic devices to prevent an adversary

¹⁴<https://notrace.how/earsandeyes/#modena-2015-12>

from recording those conversations with covert audio surveillance devices.

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

REPRESSIVE OPERATIONS

Repression against Zündlumpen (#2): Microphones were installed:⁹

- In a forest, in or around the cabins where N. and M. lived.
- In N.'s car, after N. left it unattended for a few hours.

Renata (#2): Six hidden microphones and a camera were found in a house after the operation.¹⁵ The microphones were found in the living room, hallway, and bedrooms. The camera was found in the intercom system.

See the corresponding **Ears and Eyes** case.¹⁶

Arrest of Stecco (#2): Microphones were installed in two homes, one collective space, and several cars.¹⁷

Case against Louna (#2): A hidden microphone was installed in a vehicle.⁷

Scintilla (#2): Microphones hidden in a house for two and a half years recorded conversations that the investigators used to prove that the defendants knew each other, talked regularly, worried about the creation of a DNA database and the impossibility of resisting DNA collection, and discussed writing a text to be published.¹⁸

See the corresponding **Ears and Eyes** case.¹⁹

Operation 8 (#2): Microphones were installed in several vehicles and homes.⁶

Case against Direct Action (#2): Investigators installed hidden microphones:¹¹

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

¹⁵<https://web.archive.org/web/20201031014052/https://roundrobin.info/2019/03/trento-sei-microspie-e-una-telecamera-immagini-pesanti>

¹⁶<https://notrace.how/earsandeyes/#trento-2019-03>

¹⁷<https://notrace.how/resources/#cose-utili-da-sapere>

¹⁸<https://macerie.org/index.php/2019/03/12/le-orecchie-della-pedrotta>

¹⁹<https://notrace.how/earsandeyes/#torino-2019-03>

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

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

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

December 8 case (#2): A hidden microphone was installed in the truck where Libre Flot lived.²⁰ When the legal authorization for installing and using the microphone expired after two months, the microphone was remotely deactivated but not removed from the truck. It was removed several months later during the raids.

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

3.4.2. Location



A GPS tracker found under a vehicle in Berlin, Germany, in August 2022.²¹

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

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

²⁰<https://web.archive.org/web/20241215183331/https://soutien812.blackblogs.org/2024/12/15/affaire-du-8-12-analyse-dune-enquete-preliminaire-pnat-et-dgsi>

²¹<https://notrace.how/earsandeyes/#berlin-2022-08>

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

- Most often using GPS.
- In some cases, using alternatives to GPS such as GLONASS or satellite phone services.
- In rare cases, by emitting radio waves that are received by a nearby surveillance operator (typically in a vehicle following the target's vehicle).

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

See Ears and Eyes¹² and the “Hidden devices” topic.¹³

MITIGATIONS

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

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

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

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

REPRESSIVE OPERATIONS

Case against Boris (#2): GPS tracking devices were placed under several vehicles after investigators learned that Boris—who did not have a driver license—was being transported in them.²²

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

²²<https://rupture.noblogs.org/post/2023/10/04/no-bars>

REPRESSIVE OPERATIONS

Repression against Zündlumpen (#2): Investigators sent a police patrol outside of N.'s apartment every night at irregular times to check if she was at her apartment.⁴⁷

Case against Revolutionära fronten (#2): After the nighttime visit to the fascist's house, the fascist called the police, who sent out a patrol.⁷ On its way to the house, the patrol stopped the defendants' car, presumably because it looked suspicious, and checked their identities.

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

Careful action planning (#2): 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 (#2): 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.⁸¹ For most of the day, cops staffing the roadblock searched, questioned, and photographed people passing on the road.¹³⁰

¹³⁰<https://rnz.co.nz/news/national/135737/ipca-criticises-illegal-searches-during-urewera-raids>

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 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:¹³¹ 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

¹³¹https://en.wikipedia.org/wiki/Data_breach

¹³²An International Mobile Equipment Identity (IMEI) number is a number that uniquely identifies a phone.

Renata (#2): During a house raid, one of the arrested people was forced to his knees by a cop who put a gun to his temple.⁷⁸

Case against Amos Mbedzi (#2): Mbedzi was tortured in the first days of his detention.⁵²

Belarusian anarcho-partisans (#2): The people were tortured in the first days of their detention.¹²⁸

Warsaw 3 (#2): The people were tortured during their arrest and in the first hours of their detention.⁹⁹

Case against Ruslan Siddiqi (#2): Ruslan Siddiqi was tortured for several days after his arrest.¹⁰⁰

Under torture, he confessed to carrying out the train bombing and the attack on the military airfield.

The torture included:¹²⁹

Repression of the 2019 uprising in Chile (#2): In the streets and in custody, police forces and soldiers injured, sexually assaulted, raped, tortured and killed many protesters in what appeared to be a strategic attempt to deter participation in the uprising.¹¹⁸

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. 45).**

Routine patrols

Routine police patrols usually occur in extended perimeters around police stations. They serve to establish a visible police presence to deter potential

criminals, and occasionally to catch unlucky criminals “red handed”.

Patrols in response to a threat

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

- A routine patrol stumbling upon the threat by chance.
- **Guards (p. 33) or civilians (p. 39).**
- An **alarm system (p. 7)** (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. 41).**
- An **infiltrator (p. 36) or an informant (p. 37).**

MITIGATIONS

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

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

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

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

Repression against Zündlumpen (#2): A GPS tracker was installed on N.'s car.⁹

Arrest of Stecco (#2): GPS trackers were installed on 12 cars.¹⁷

A tracking device was installed on a bike that was suspected of being used by Stecco.

Case against Louna (#2): Several GPS trackers were installed on vehicles.⁷

Bure criminal association case (#2): Investigators installed a covert location tracker on a vehicle, where it remained for about a month.⁷

December 8 case (#2): A covert location tracker was installed on a vehicle used by Libre Flot.²⁰

3.4.3. Video



A camera found in the skylight of a public school in Berlin, Germany, in July 2011.²³

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

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

- The living room of a target.
- The windows of a building close to the home of a target, with a line of sight on the entrance of the home.
- Close to **stash spots or safe houses (#2)** as has happened in Italy, where motion-activated cameras were installed to monitor a forest stash spot.²⁴

Captured images can be used as evidence in court. Non-incriminating, mundane images can reveal a lot

²³<https://notrace.how/earsandeyes/#berlin-2011-07>

²⁴<https://actforfree.noblogs.org/post/2022/06/24/italy-youll-find-us-in-our-place-as-we-cant-stay-in-yours-on-the-diamante-investigation>

about the targets of surveillance and help in **network mapping (p. 44).**

See Ears and Eyes¹² and the “Hidden devices” topic.¹³

MITIGATIONS

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

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

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

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

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

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

¹²⁸<https://pramen.io/en/2021/12/blood-on-your-hands-regarding-information-about-torture-of-anarcho-partisans>
¹²⁹beatings and electric shocks

REPRESSIVE OPERATIONS

Case against Boris (#2): Cameras were installed in the streets outside Boris's home and outside the home of someone close to him to film the entrances to the homes.²²

Repression against Zündlumpen (#2): Cameras were installed.⁹

- In a forest, around the cabins where N. and M. lived.
- In a basement rented by N.
- In the apartments of people suspected of being close to N. and M.
- On a railway bridge with a path for pedestrians and bicycles. Investigators claimed to have recognized M. in the camera footage crossing the bridge on a bicycle around the time an arson occurred a few kilometers from the bridge.

Arrest of Stecco (#2): Cameras were installed.¹⁷

- In front of six homes.
- In cars.
- Inside train stations, providing investigators with real-time access to footage of the stations, which the cameras already installed in the stations did not provide.

Case against Louna (#2): Cameras were installed to film the entrances of several places where people opposed to the highway project lived.⁷

Operation 8 (#2): Cameras were installed at the “training camps” on several occasions.⁶ They were installed shortly before the beginning of the camps and removed shortly after. The goal was to identify who was participating in the camps, what they were doing, and what they were wearing. Footage captured by these cameras showed people:

- Training with firearms.
- Learning military tactics: patrolling, counter-ambush drills, etc.
- Experimenting with Molotov cocktails.

At least one camera was installed outside a person's home.

December 8 case (#2): A camera was installed outside a small cabin used by some of the defendants, filming the cabin.²⁰ It was seemingly installed about 10 meters from the cabin, on a tree trunk.

3.5. Detection dogs

Used in tactics: **Arrest, Incrimination**



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

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

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

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

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

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

Detecting substances

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

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. 44) or to incriminate individuals for actions carried out during the demonstration.

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

MITIGATIONS

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

REPRESSIVE OPERATIONS

Mauvaises intentions (#2): During a demonstration, the investigators took 180 photographs from which they obtained 200 portraits of the demonstrators, including ten people they were able to identify.³⁷

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 years after being arrested by the State. Reported acts of torture in these countries include:¹²⁵

In some contexts, physical violence can include assassinations.

¹²⁵

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

MITIGATIONS

Need-to-know principle (#2): 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”¹²⁶ about practices against torture.

Preparing for repression (#2): 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 (#2)**, discontinuing projects, entering **clandestinity (#2)**, etc.
- Prepare psychologically to resist torture.

See “Under the Enemy's Blade: A Search for Anarchist Practices Against Torture”¹²⁶ about practices against torture.

REPRESSIVE OPERATIONS

Network (#2): Most of the defendants were tortured by the Russian Federal Security Service (FSB) in the early stages of their detention in order to obtain (often fabricated) statements that could later be used to charge and convict them.¹²⁷ Most of the defendants who were tortured later retracted their statements and spoke publicly about the torture they had received.

¹²⁶<https://notrace.how/resources/#under-enemy-blade>

¹²⁷<https://web.archive.org/web/20210724133854/https://a2day.net/network-underground>

accompanied her to the hospital several times.

- Followed a person seen with Louna at the hospital again for 6 hours.
- On October 10, during the trial of a person opposed to the highway project, they surveilled the interior of the courthouse and the surrounding area.
- On October 12, after hearing about a meeting outside apartment buildings through an intercepted phone call, they surveilled those buildings and arrested two people who went to the meeting, including Louna.

Repression of the first Jane's Revenge arson (#2): In March 2023, cops secretly observed the person from a distance of about 30 meters.³⁹ The cops watched the person discard a bag, retrieved it, and collected DNA evidence linking the person to the action site.

Case against Jeff Luers (#2): On the night of the June arson, the arsonists were being tailed by a surveillance team—police officers in one or more unmarked cars—as they drove to the arson site.⁷³ They parked their car close to the arson site, watched by the surveillance team. They got out of their car to continue on foot, at which point the surveillance team lost sight of them. They ran back to their car 10 minutes later, at which point the surveillance team regained sight of them. They drove away from the arson site. More than an hour later, the surveillance team—still tailing the arsonists—heard on the police radio system about a fire at the arson site and asked local police officers to stop the arsonists' car for a roadside check, suspecting that they were involved in the fire. Half an hour later, when fire investigators at the arson site reported that they believed the fire had been set intentionally, the arsonists were arrested.

Bure criminal association case (#2): Investigators:⁷

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

The three from the park bench (#2): During the evening leading up to the arrest, two of the people rode their bikes through the city and were followed by cops on bikes (and presumably also cops in cars) until they were arrested in the park.¹⁰⁸ 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.

Operation 8 (#2): Investigators regularly followed people on foot and in vehicles.⁶

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.⁷

Nea Philadelphia case (#2): On the day of the arrests, when one person visited a cybercafé that was probably under police surveillance, cops recognized him and started following him.¹²³ He then moved through the streets of Athens for a few hours, gradually joining the other people—some of whom were wanted by police¹²⁴—and all of them were arrested.

Case against Direct Action (#2): For several weeks, investigators followed members of Direct Action and some of their friends as they moved on foot and in vehicles.¹¹

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

December 8 case (#2): For several weeks, investigators staked out the homes of some of the defendants and tailed them when they moved.²⁰ 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

¹²³<https://web.archive.org/web/20201027031238/http://actforfree.nostate.net/?p=15472>

¹²⁴<https://machorka.espivblogs.net/2013/11/06/letter-from-anarchists-argiris-dalios-and-fivos-harisis-from-koridallos-prisons-athens>

- At an action site or during a **house raid (p. 33)** or **covert house visit (p. 8)** to determine if a substance is present and locate it.
- During an **ID check (p. 35)** to determine if the person being checked is carrying or has been in contact with a substance.

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

Tracking people

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

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

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

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

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

evidence, but the result of tracking by the second method is not.

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

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

Scent lineups

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

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

See also

See the “Mantrailing” section of “How To Get Things Burning (Security Chapters)”²⁵ for an overview of detection dogs.

MITIGATIONS

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

²⁵<https://notrace.how/resources/#things-burning>

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

REPRESSIVE OPERATIONS

Fenix (#2): In one of the house raids, the police used detection dogs trained to detect explosives.²⁶

Repression against Zündlumpen (#2): In some of the raids, detection dogs were used to locate electronic devices.²⁷

Investigators made a covert visit of the cabins where N. and M. lived and, using handkerchiefs, collected scent samples from objects believed to belong to N. and M.⁹ In the following months, on three occasions, after an arson took place in the region, they brought the handkerchiefs to the arson site and provided them to detection dogs, asking the dogs to locate the scents. The dogs signaled that they located the scents on the remains of firefighters, firefighter packaging, and a canister lid.

In the February 2025 arrests of N. and M., scent samples were collected from their necks.²⁸

Bure criminal association case (#2): Detection dogs were used in one of the raids.⁷

3.6. Door knocks

Used in tactics: **Deterrence, Incrimination**



²⁶<https://antifenix.noblogs.org/post/2015/06/03/interview-with-an-activist-detained-during-operation-fenix>

²⁷<https://actforfree.noblogs.org/2025/03/26/about-the-repressive-operation-in-germany-and-austria-solidarity-with-the-arrested-anarchists>

²⁸<https://actforfree.noblogs.org/2025/07/03/munich-germany-update-on-the-imprisonment-of-the-two-comrades>

Door knocks are when an adversary comes knocking where you live to intimidate you or get information. Door knocks aim to intimidate or create paranoia, to see who is willing to talk and possibly be recruited as an **informant** (p. 37), and to gather information from the people who do talk.

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

In many countries, it is easier for the State to carry out door knocks than **house raids** (p. 33) because door knocks do not require a warrant or legal authorization.

MITIGATIONS

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

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

REPRESSIVE OPERATIONS

Search for a fugitive (#2): In 2025, agents from the Federal Bureau of Investigation (FBI) knocked on doors and asked for information about the person.⁷

Scintilla (#2): In May 2019, cops knocked on Boba's door under the pretext of giving a verbal notice to someone else.²⁹ Once inside, however, they revealed a warrant for Boba's arrest, arrested him, and searched the house.

3.7. Doxing

Used in tactic: **Deterrence**

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

Doxing often uses information obtained through **open-source intelligence** (p. 44).

²⁹<https://macerie.org/index.php/2019/05/23/incendio-al-carcere-boba-arrestato>

REPRESSIVE OPERATIONS

Case against Boris (#2): For several weeks, investigators regularly staked out Boris's home and tailed him as he moved on foot, on bicycles, and in vehicles.²²

Repression against Zündlumpen (#2): Investigators followed N. for 15 days.⁴⁷

Search for a fugitive (#2): In 2022, a surveillance operator conducted, alone, covert physical surveillance of a residence.⁷ Three days prior, investigators had obtained the address of the residence through the collaboration of the Supplemental Nutrition Assistance Program,¹²² 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 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 (#2): Investigators learned through a hidden microphone installed in a home that someone under surveillance would be traveling by train the next day.¹⁷ 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 (#2): A week before the protest, investigators conducted covert physical surveillance at a local bookstore where they knew people planning the protest were organizing.¹⁰ They

¹²²Supplemental 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.

observed Peppy enter the bookstore and leave an hour and a half later.

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

2011-2013 case against Jeremy Hammond (#2): During a physical surveillance operation against Jeremy Hammond's home that lasted several days, investigators established a correlation between:⁹³

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

Case against Louna (#2): After the arson on the night of May 4 to May 5, 2024, investigators conducted several physical surveillance operations:⁷

- 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

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 (p. 11)** 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. 52)**.
- **Aerial surveillance (p. 45)**, such as a drone following the target from a distance.

Static

Static physical surveillance is the observation of a target when the target cannot move, or the surveil-

lance 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 Countermeasures¹¹⁹ about the principles and techniques of covert physical surveillance.
- Measures Against Surveillance¹²⁰ for insights into how police and intelligence agencies conduct covert physical surveillance.
- The “Physical surveillance” topic.¹²¹

MITIGATIONS

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

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

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

¹¹⁹<https://notrace.how/resources/#surveillance-countermeasures>

¹²⁰<https://notrace.how/resources/#measures-surveillance>

¹²¹<https://notrace.how/resources/#topic=physical-surveillance>

MITIGATIONS

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

3.8. Evidence fabrication

Used in tactic: **Incrimination**

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

Notable examples of evidence fabrication include:

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

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

MITIGATIONS

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

REPRESSIVE OPERATIONS

Prometeo (#2): Investigators distorted conversations obtained through phone interception to make them look suspicious.³⁰ For example, during a phone conversation involving one of the defendants, the phrase “tutta questa tensione sociale prima o poi scoppierà” (“all this social tension will, sooner or later, explode”) was said, which was only partially transcribed in the investigation files as “prima o poi scoppierà” (“will, sooner or later, explode”).

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

³⁰<https://ilrovescio.info/2020/08/23/uno-scritto-di-nataschia-dal-carcere-di-piacenza>

explosifs” (explosive vests) in a report by the prosecutors in charge of the case.

3.9. Forensics

Used in tactic: **Incrimination**

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

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

Forensic scientists often testify as “expert witnesses” at trials.

3.9.1. Arson



A fire investigator searching the scene of a fire.

Arson forensics (also known as *fire investigation*) is the application of science to the investigation of arson. Arson forensics aims to determine the origin and cause of a fire and, if it is suspected to be arson, to gather evidence that could help identify the potential arsonists.

An adversary can usually easily determine whether a fire was accidental or arson. It is difficult to carry out an arson and make it appear accidental to an adversary who is knowledgeable in arson forensics.

Fire scene investigation

Fire scene investigation is the inspection of the scene of a fire, looking for:

- The ignition source that started the fire and the fuel that source ignited. For example, in an accidental residential fire the ignition source may be a malfunctioning electrical outlet that overheats and the fuel may be a sofa positioned against the outlet. In an arson the ignition source may be a match and the fuel may be gasoline brought by the arsonist.
- Patterns left by the fire on walls, floors, ceilings, and objects. These patterns can indicate where the fire started and how it spread. For example, a fire that starts at the base of a wall may leave a distinctive V-shaped burn pattern on the wall.
- Eyewitness accounts and **video surveillance (p. 41)** footage of the scene of the fire before, during, and after the fire.

When a fire occurring inside a room reaches a high enough temperature—typically between 500°C and 600°C—it reaches the *flashover* point. During flashover, the room is so hot that all ignitable surfaces ignite more or less simultaneously and the fire spreads rapidly throughout the room. Once a fire has reached flashover it is usually significantly harder for the adversary to interpret the patterns it left on walls and other surfaces.

Fire debris analysis

Fire debris analysis is the collection and analysis of fire debris—objects that burned in a fire. An adversary can collect samples of fire debris at the scene of the fire and analyze them in a laboratory to find traces called ignitable liquid residues (ILRs), which are left when accelerants (also known as *ignitable liquids*) burn. An adversary can use **detection dogs (p. 13)** to locate ILRs at the scene of the fire, facilitating the collection of samples of fire debris that are likely to contain ILRs.

An adversary can analyze a sample of fire debris to determine:

- The presence of ILRs in the sample. This can indicate that the fire was arson rather than accidental and that the fire originated where the sample was collected.
- The type of accelerant that left the ILRs in the sample: gasoline, diesel fuel, kerosene, etc.

Accelerant comparison

An accelerant can have a more or less unique chemical composition depending on how it was produced, transported and stored. Let's take the example of gasoline, an accelerant made from refined crude oil. The chemical composition of gasoline sold at a gas station depends on:

- Where and how the crude oil was extracted.
- How the crude oil was refined.
- What chemicals were blended to make the gasoline.
- What additives were added to the gasoline. Additives can depend on the brand of gasoline, although a given brand can also use different additives depending on the region and the time of year.
- The chemical composition of the accelerant remaining at the bottom of the gas station's fuel tank when it was last refilled.³¹

An adversary can compare the chemical compositions of two samples of accelerant to determine the likelihood that they come from the same source. They can compare:

- An accelerant to an accelerant. This type of comparison is more precise. For example, they can compare a bottle of gasoline found unignited at the scene of a fire to gasoline found stored in a suspect's home.
- ILRs to an accelerant. This type of comparison is less precise. For example, they can compare ILRs from fire debris found at the scene of a fire to a sample of gasoline from a gas station.

If an adversary wants to know the source of a sample of accelerant—that we'll call the *questioned sample*—but does not have any particular leads, they have two options:

- They can collect a large number of potentially matching samples and compare them to the questioned sample. For example, they can collect gasoline samples from all gas stations in an area and compare them to a bottle of gasoline found unignited at the scene of a fire. State adversaries do not regularly do this.³²

³¹Gas station fuel tanks are typically refilled every few days, or every few weeks at stations with fewer customers.

³²According to a 2023 study from the United States, this is “not common practice in forensic casework.”

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. 50)** surveillance operation.
- Improving the chances of successfully following the target of surveillance during a **covert (p. 47)** 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 night¹¹¹).
- Locating suspects as part of routine **police patrols (p. 51)** 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,¹¹² with high-quality video at night.¹¹³

See the “Aerial surveillance” topic.¹¹⁴

MITIGATIONS

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

Anti-surveillance (#2): You can include in an anti-surveillance route locations that would prevent an aerial surveillance operation from following you: an

¹¹¹<https://actforfree.noblogs.org/post/2023/11/13/munich-germany-geothermal-energy-gets-hot-and-not-only>

¹¹²<https://theintercept.com/2020/04/09/baltimore-police-aerial-surveillance>

¹¹³<https://theintercept.com/document/2021/08/31/motion-to-suppress-aerial-surveillance-evidence-in-u-s-vs-muhammed-momtaz-alazhari>

¹¹⁴<https://notrace.how/resources/#topic=aerial-surveillance>

underground metro system, a shopping complex with many entrances, etc.

Attack (#2): During a demonstration, you can take down drones with fireworks, hack them, or blind them with lasers. See also 5 widely accessible ways to take down drones.¹¹⁵

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

REPRESSIVE OPERATIONS

Repression against Zündlumpen (#2): Drones were used to follow N. and M. in a forest during a covert physical surveillance operation.⁹

Berlin 2023 railway conspiracy case (#2): The arrested people were discovered at night by a helicopter on a routine surveillance flight, presumably equipped with night-vision equipment.¹¹⁶ A text¹¹⁷ 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 (#2): 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.⁸¹

Repression of the 2019 uprising in Chile (#2): Drones were used to track rioters leaving riots in order to facilitate their arrest.¹¹⁸

Case against Direct Action (#2): After investigators discovered the remote area where members of Direct Action hid the stolen explosives they used in bombings, they arranged for a helicopter to fly over the area daily for surveillance purposes.¹¹

¹¹⁵<https://notrace.how/resources/#5-ways>

¹¹⁶<https://notrace.how/resources/#conspiring>

¹¹⁷<https://kontrapolis.info/9821>

¹¹⁸<https://es-contrainfo.espiv.net/2019/11/06/chile-una-mirada-anarquica-al-contexto-de-revuelta-y-represion>

MITIGATIONS

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

REPRESSIVE OPERATIONS

2019–2020 case against Mónica and Francisco (#2): The photos used to identify Mónica and Francisco in public CCTV footage were found on social media.⁴⁵

Repression against Zündlumpen (#2): Investigators:⁹

- 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 (#2): Investigators analyzed the posts made by the person on the social media Instagram from 2019 to 2022 and found:⁷

- 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 (#2): 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 blurred¹¹⁰ in the video.⁷

Repression of Lafarge factory sabotage (#2): Investigators collected metadata from photos of the action posted online, including the name and serial number of a camera.⁵⁰ This helped them identify a person they accused of taking the photos.

Bure criminal association case (#2): Investigators visited a Facebook page associated with the struggle against Cigéo and then analyzed the Facebook profiles of everyone who had “liked” the page.⁷

¹¹⁰<https://aftonbladet.se/nyheter/a/WL8EEEd/atal-mot-va-nsterextremister-i-revolutionara-fronten>

Operation 8 (#2): Investigators obtained information on people from web searches and newspaper articles.⁶

Repression of the attack on Clarín's headquarters (#2): Investigators analyzed social media profiles to establish links between the defendants.⁶⁰ 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.

For example, an intelligence agency can collect incriminating digital evidence from a phone without a warrant, and then conduct a **house raid (p. 33)** 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

- If they have access to an *accelerant database*—a database of samples of accelerants collected regularly in a given region—they can compare the questioned sample to all the samples in the database. For example, if the questioned sample is a bottle of gasoline found unignited at the scene of a fire, they could identify the brand of gasoline (if samples are collected from refineries whenever a batch of gasoline is produced for a given brand) or the gas station where it was bought (if samples are collected from gas stations whenever their fuel tanks are refilled). It is unknown if any State adversaries have access to such databases.³³

Incendiary devices

An incendiary device is an arrangement of items or materials that is designed to be left at the scene of a fire in order to help start, accelerate, spread, or delay the fire. Incendiary devices range from simple Molotov cocktails to complex time-delay devices with electronic timers.

Since incendiary devices are designed to be left at the scene of a fire, an adversary can recover their burned remains and analyze them to find evidence that could help identify the arsonists. It is relatively common for incendiary devices to fail—whether they fail to ignite or ignite but burn significantly less than expected—in which case an adversary can recover the devices intact or partially intact and potentially find much more evidence than if the devices had not failed.

Incendiary devices can fail because of:

- An inherent flaw in the construction or use of the device. For example, Molotov cocktails typically have a high failure rate because they often either do not break upon contact with their target, or break but fail to sufficiently ignite their target.
- Rough handling of the device during construction, transport, or installation. This rough handling can be caused by stress, darkness, or inexperience.
- Weather conditions during storage of the device (between its construction and use), particularly if it includes moisture-sensitive components.

³³A 2020 study from the Netherlands briefly mentions “a database of gasoline collected nationally.”

- Weather conditions at the scene of the fire: wind, dew, fog, and rain.

When analyzing an incendiary device or its burned or partially burned remains, an adversary can analyze:

- Accelerants contained in the device, or ILRs left on the device.
- **DNA traces (p. 20)** and **fingerprints (p. 25)** left while handling the device components.
- **Tool marks (p. 30)** left when constructing the device.
- Identifiers visible on the device components such as serial numbers or barcodes.
- **Glass traces (p. 30)**, if the device includes glass components.
- Details of the device's construction, including the use of tape and glue and how components are wired, welded, or knotted together.

An adversary may successfully analyze a DNA trace left on an incendiary device even if the device ignited, depending on the type of trace, the temperature to which it was exposed, and the duration of the exposure.³⁴ For example:

- A saliva trace was left on the outside of a Molotov cocktail made from a glass bottle. The Molotov cocktail was thrown and broke but only produced a short-lived burst of flames without further damage. An adversary may successfully analyze the DNA in the saliva trace.
- Skin cells were left on the outside of an incendiary device. The device was activated and surrounding objects caught fire, resulting in a sustained fire that enveloped the device for several minutes. An adversary should not be able to successfully analyze the DNA in the skin cells.

See “Incendiary Devices: Investigation and Analysis,”³⁵ chapter “The Analysis of Incendiary Devices” for a detailed overview of the investigation of incendiary devices.

MITIGATIONS

Anonymous purchases (#2): An adversary can link accelerants and incendiary device components to

³⁴For more information see the “Degradation” section of the No Trace Project DNA Literature Review.^a

^a<https://notrace.how/resources/#dna-review>

³⁵Available on the Surveillance Archive.^a

^a<https://notrace.how/surveillance-archive.html>

where they were purchased, and from there to the identity of the person who purchased them. To mitigate this, you can purchase accelerants³⁶ and device components anonymously.

Careful action planning (#2): If you use an incendiary device in an action and the device fails, an adversary can recover the device intact or partially intact and potentially find much more evidence than if the device had not failed. To mitigate this, you can:

- Make and use several test devices similar to the “real” device you will use in the action. You should conduct the tests with good security precautions because conducting such tests can be incriminating. In particular, you can:
 - Construct test devices with components of the same brand and model as the components you will use for the real device.
 - Store test devices in the same conditions (e.g. humidity) as the real device, and for the same length of time.
 - Transport test devices in the same way as the real device.
 - Install test devices in the same conditions as the real device (weather, temperature, darkness, etc.)
- Ensure that you will be able to construct, transport, and install the device under the psychological conditions of the action (e.g. stress).

If you use accelerant in an action and an adversary goes through the effort of collecting accelerant samples for comparison (e.g. gasoline samples from gas stations), they could identify the source of the accelerant you used. To mitigate this, you can:

- Make the identification less likely to be effective by using a mix of accelerants of the same type coming from different sources (e.g. gasoline from different gas stations).
- Make the identification even less likely to be effective by using a mix of accelerants of the same type from sources located in different areas (so that the chemical compositions of the accelerants are more distinct) and let some time pass between when you obtain the accelerants and

when you use them (so that the adversary cannot retroactively obtain the samples they would need for comparison because the fuel tanks of the gas stations where you obtained the accelerants have been refilled).

REPRESSIVE OPERATIONS

Mauvaises intentions (#2): DNA samples were collected from a cigarette used as a delay for an incendiary device—the delay failed and the device was found intact under the police tow truck.³⁷

Case against Louna (#2): A gas detector³⁸ was unsuccessfully used to detect traces of accelerant in the cab of the burned excavator.⁷

Traces of accelerant were collected:

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

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

Repression of the first Jane's Revenge arson (#2): DNA samples were collected from an intact Molotov cocktail found by investigators at the action site.³⁹

Bure criminal association case (#2): Traces of accelerants were collected from items recovered after demonstrations and analyzed.⁷

3.9.2. Ballistics



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

Ballistic forensics (also known as *firearm examination*) is the application of science to the investigation of firearms and bullets. When a bullet is fired from a

³⁷<https://infokiosques.net/spip.php?article597>

³⁸https://en.wikipedia.org/wiki/Gas_detector

³⁹<https://notrace.how/documentation/first-jane-s-revenge-arson-investigation-files.pdf>

³⁶If it is too difficult to purchase accelerants anonymously in your context (e.g. because it is too suspicious to buy gasoline from a gas station without arriving in a car), you can prefer to purchase them non-anonymously, and mitigate this technique in other ways.

the bus.¹⁰⁹

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** (p. 37).

The State very frequently uses social media friends lists (a form of **open-source intelligence** (p. 44)) for network mapping because they do not require a warrant or legal authorization.

MITIGATIONS

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

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

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

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

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

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

Network map exercise (#2): An adversary can map a network by using infiltrators and informants to

¹⁰⁹https://web.archive.org/web/20211210123411/https://www.revolucionpopular.com/otras-noticias/la-policia-detuvo-a-otro-hombre-por-el-ataque-a-clarin_a61b34174d2f0a04884749d24

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 (#2): Investigators claimed that because N. and M. were partners, they likely committed arson together.⁹

Mauvaises intentions (#2): To prove that the defendants knew each other and were therefore likely accomplices, the investigators used several clues:³⁷

- 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 (#2): Before the raids, investigators spent several months establishing links between people by examining metadata from:⁶

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

Repression of the attack on Clarín's headquarters (#2): After identifying the first defendant, investigators identified the other defendants by establishing links between them. Investigators found that the defendants:⁶⁰

- 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 they took (taking taxis, changing clothes, wearing disguises).⁴⁵

Repression against Zündlumpen (#2): Three weeks before an arson, a wildlife camera near the arson site captured a person walking, wearing an orange jacket.⁹ After the arson, investigators obtained the camera footage and claimed that the jacket resembled one that M. had worn at some point.

Case against Revolutionära fronten (#2): CCTV footage from cameras near the scene of the Stockholm beating showed that some of the defendants were present during the beating.⁷

Repression of Lafarge factory sabotage (#2): Immediately after the action, investigators requested CCTV footage from public transportation (buses, train stations, etc.), businesses, home surveillance systems, and municipal cameras, all within an extended perimeter of the action site.⁵⁰ In particular, footage of the interiors of buses appears to have helped identify people traveling to and from the action site.⁴⁹ 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 (#2): Two of the people were allegedly seen on video surveillance leaving a store where investigators believe the envelopes used to prepare the parcel bombs were purchased.³⁰

Arrest of Stecco (#2): Investigators analyzed CCTV footage from street cameras, train stations, highway toll booths, buses, and businesses to determine the movements of people under surveillance.¹⁷

2013 case against Mónica and Francisco (#2): Public CCTV footage was used by investigators to reconstruct the movements of Mónica and Francisco before and after the action.⁵⁹ This showed that they were near the action site shortly before the explosion of the device.

Case against Peppy and Krystal (#2): CCTV footage from a bus allowed investigators to identify the license plate of the motorcycle on which Peppy and Krystal arrived at and left the protest site.¹⁰

Case against Louna (#2): CCTV footage from the arson site showed two people setting fire to the excavator, and one of them burning themselves accidentally.⁸⁰

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.⁷

Repression of the first Jane's Revenge arson (#2): CCTV footage helped identify a vehicle driven by the person, when they were seen entering a parking lot on foot after a demonstration, and the vehicle was seen leaving the same parking lot a few minutes later.³⁹

Bure criminal association case (#2): Investigators used footage from the demonstrations, recorded by surveillance cameras and police forces, to:⁷

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

The three from the park bench (#2): On the evening leading up to the arrest, one of the people—while being followed by cops—stopped at a gas station and was seen by the station's video surveillance cameras buying gas and filling a gas can.¹⁰⁸ The cops obtained the CCTV footage the next morning.

Case against Ruslan Siddiqi (#2): CCTV footage from factories near the train bombing site showed someone riding a bike shortly before and after the bombing, wearing camouflage clothing and carrying a backpack.⁵⁴ This supported the theory that the person who carried out the bombing traveled by bike.

Repression of the attack on Clarín's headquarters (#2): CCTV footage from multiple cameras showed one defendant leaving the attack site, being driven away on a motorcycle for a few blocks, and boarding a bus—the defendant was identified because he used his partner's electronic bus card to board

gun, the gun leaves microscopic marks on the bullet and cartridge case. These marks are like ballistic fingerprints.

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

MITIGATIONS

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

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

3.9.3. DNA



Collection of a DNA sample using a swab.

DNA forensics is the collection and analysis of DNA samples for the purpose of matching DNA samples to individuals.

DNA is the molecule that contains the genetic code of organisms. Every cell⁴⁰ in a human body has DNA. Each individual's DNA is unique, with the exception of identical twins. An adversary can compare an individual's DNA with a DNA sample collected from an item or location and, if they match, conclude that the individual was likely in contact with that item or location.

⁴⁰With the exception of red blood cells.

Transfer

Human body cells and the DNA they contain can directly transfer from the body to the environment. For example:

- When you sweat, urinate, defecate, or bleed, you leave sweat, urine, feces, or blood.
- When you breathe or speak, you emit respiratory droplets from your mouth and nose that contain saliva and mucus.
- When you touch a surface with your skin, skin cells transfer from your skin to the surface.
- Even when you're not doing anything, you are constantly shedding skin cells and hair.

Human body cells can also transfer indirectly. For example, if you touch the outside of a pair of gloves with your fingers, then put the gloves on and touch a door handle, your skin cells can transfer first from your fingers to the outside of the gloves and then from the outside of the gloves to the door handle.

See the “Transfer” section of the No Trace Project DNA Literature Review⁴¹ for more details on direct and indirect DNA transfer.

Degradation

DNA is very robust and does not easily degrade, but it can degrade under certain conditions, such as when exposed to high temperatures or sodium hypochlorite.

See the “Degradation” section of the No Trace Project DNA Literature Review⁴¹ on the conditions under which DNA can degrade.

Collection

An adversary can collect a DNA sample:

- From a surface known to contain DNA, such as a visible biological mark (e.g. saliva or blood).
- From a surface suspected of containing DNA, such as a door handle suspected to have been touched by a suspect at an action site.

An adversary can use techniques to facilitate DNA collection, such as:

- Soot removal techniques to collect DNA samples hidden beneath soot after a fire.

⁴¹<https://notrace.how/resources/#dna-review>

¹⁰⁸<https://notrace.how/resources/#parkbank>

- Luminol to locate blood samples invisible to the naked eye.

Analysis

An adversary can analyze a DNA sample to identify genetic markers of the DNA. Such an analysis is successful if:

- The sample contains enough DNA. For example, a drop of blood contains significantly more DNA than skin cells left through brief contact between skin and a surface.
- The DNA isn't too degraded.
- All or most of the DNA in the sample is from at most three individuals.

An adversary can compare *two* successfully analyzed DNA samples to:

- Determine whether they come from the same individual. For example, they can compare a DNA sample collected from the mouth of a suspect in custody to a DNA sample collected at an action site and, if they match, conclude that the suspect was likely present at the action site.
- Determine whether they come from individuals closely related genetically, such as parents and their children, siblings, or cousins.

An adversary can also use a *single* successfully analyzed DNA sample to:

- Determine the individual's genetic sex.
- Attempt to predict the individual's appearance using forensic DNA phenotyping. Currently, eye, hair, and skin color can be predicted with relatively high accuracy, and research is ongoing to attempt to predict other characteristics. This technique is not used in all contexts.

DNA databases

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

Countries can exchange DNA data with each other through:

- International DNA databases, such as the Interpol DNA database or the Europol Information System.

- Linked or networked national DNA databases. For example, European Union member states are required to maintain a DNA database that other member states can access.
- Request-based exchange of DNA data, typically in cases of serious crimes.

See also

- Dna You Say? Burn Everything to Burn Longer: A Guide to Leaving No Traces⁴² for an overview of DNA forensics.
- The No Trace Project DNA Literature Review⁴¹ for a collection of useful details on DNA forensics, taken from academic literature.
- The “DNA” topic.⁴³

MITIGATIONS

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

- Secure your hair under a hat.
- If you have to cut a fence, cut any fence holes large enough to pass through without touching the fence.
- Ensure that surfaces at the action site are not touched if they do not need to be, and that surfaces that need to be interacted with (such as a door handle) are touched by someone following **DNA minimization protocols (#2)**.
- Ensure that nothing is accidentally left behind such as a bag, tool, or anything that could fall out of a pocket.

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

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

⁴²<https://notrace.how/resources/#dna-you-say>

⁴³<https://notrace.how/resources/#topic=dna>

- 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 (p. 24)**, **gait (p. 26)**, **voice (p. 29)**, etc.

Analysis of CCTV footage can be performed:

- By humans.
- By automated systems such as automated license plate readers or **facial recognition systems (p. 24)**.

See also

- You Can't Catch What You Can't See: Against Video Surveillance.¹⁰⁴
- The topics “Video surveillance”¹⁰⁵ and “Automated license plate readers”.¹⁰⁶

¹⁰⁴<https://notrace.how/resources/#catch-see>

¹⁰⁵<https://notrace.how/resources/#topic=video-surveillance>

¹⁰⁶<https://notrace.how/resources/#topic=automated-license-plate-readers>

MITIGATIONS

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

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

Attack (#2): You can disable¹⁰⁷ surveillance cameras.

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

- To prevent **gait recognition (p. 26)**, wear baggy clothing that hide your body shape, use an umbrella or other concealing objects, or drastically change your walking style by adopting a “funny walk”.
- To prevent **facial recognition (p. 24)**, wear a mask to cover your facial features, and sunglasses or a hat with a low brim to cover your eyes.

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

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

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

REPRESSIVE OPERATIONS

Case against Boris (#2): Soon after the April sabotage, investigators requested CCTV footage from businesses and municipal cameras, and lists of vehicles from automated license plate readers (ALPRs) and speed cameras, all within an extended perimeter of the sabotage site.²²

2019–2020 case against Mónica and Francisco (#2): Public CCTV footage was extensively used by investigators to reconstruct the movements of Mónica and Francisco before and during the actions, despite the

¹⁰⁷<https://notrace.how/resources/#destroy-cameras>

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

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

See the “Digital surveillance” topic.¹⁰²

MITIGATIONS

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

Digital best practices (#2): You can follow digital best practices to make mass digital surveillance ineffective. For example, you can use Tor¹⁰³ to anonymize your Internet activity, and you can use security-oriented operating systems and applications that limit the data they store or collect about you.

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

3.18.3. 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).

¹⁰²<https://notrace.how/resources/#topic=digital-surveillance>

¹⁰³<https://torproject.org>

- Databases of biometric information (face photographs, fingerprints, DNA).
- Records of **ID checks (p. 35)**, fines, arrests, investigation proceedings, judicial proceedings, and convictions.

MITIGATIONS

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

REPRESSIVE OPERATIONS

Case against Boris (#2): Investigators found out that the DNA on the bottle cap belonged to Boris because his DNA was in France's national DNA database.²²

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

2011-2013 case against Jeremy Hammond (#2): Under his online persona, Jeremy Hammond shared in online chats that he had been arrested at the 2004 Republican National Convention, had spent time in a federal prison and in a county jail, and was currently on probation.⁹³ Investigators were able to verify all of this using police files, which helped them to link Jeremy Hammond's online persona to his real life identity.

Bure criminal association case (#2): Investigators extensively used police files to establish links between people, including databases of driver's licenses and registered vehicles, as well as records of arrests, judicial proceedings and convictions.⁷

3.18.4. Video surveillance

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

Collection

Sources of CCTV footage include:

REPRESSIVE OPERATIONS

Scripta Manent (#2): DNA evidence was used to convict Alfredo Cospito.⁴⁴

Case against Boris (#2): The only evidence against Boris was that his DNA was found on a bottle cap at the foot of one of the burnt antennas from the April sabotage.²²

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

2019-2020 case against Mónica and Francisco (#2): Francisco's DNA was found on the parcel bomb sent to the former Minister of the Interior, which was defused and didn't explode.⁴⁵

Repression against Zündlumpen (#2): In some of the raids, DNA samples were collected from a cigarette butt,⁴⁶ zines,⁴⁷ books, doors, cups, and printing machines.

Renata (#2): After their arrest and imprisonment, the person accused of the explosive attack on the Lega Nord headquarters in Treviso refused to have their DNA taken.⁴⁸ Some time after the person's refusal, prison guards searched their cell and secretly replaced one comb with another, presumably to obtain the person's DNA from the hairs on the comb they took.

Search for a fugitive (#2): Following the 2020 attack on the building, DNA samples were collected from broken glass, window blinds, the sidewalk outside the building, as well as on blood found on a bottle of lighter fluid and other items.⁷ It seems that at this point, the samples did not match anyone in DNA databases.

In 2023, the person was convicted in an unrelated case in a state other than Georgia. As part of the conviction, they were required to provide a DNA sample to the police, which matched the samples collected in 2020.

⁴⁴<https://insuscettibilediravvedimento.noblogs.org/post/2020/03/29/it-en-italia-su-una-sentenza-e-qualcosa-daltro-un-testo-di-marco-dal-carcere-di-alessandria>

⁴⁵<https://notrace.how/resources/#monica-francisco>

⁴⁶<https://notrace.how/resources/#bavarian-christian>

⁴⁷<https://notrace.how/resources/#cops-and-robbers>

⁴⁸<https://web.archive.org/web/20210518112509/https://roundrobin.info/2020/03/aggiornamenti-su-manu-stecco-juan-e-sasha>

Repression of Lafarge factory sabotage (#2): In one of the initial raids, police insisted that those arrested wear surgical masks to protect against Covid: the masks were later taken for DNA collection.⁴⁹ One person who refused to wear a mask had their underwear confiscated while in police custody, presumably for DNA collection.⁵⁰

Prometeo (#2): DNA traces were used to convict the person accused of burning an ATM.⁵¹

Mauvais intentions (#2): During police custody, DNA was collected from the people's clothing and from plastic cups.³⁷ In one case, only nine hours elapsed between the collection of a DNA sample in custody and the result of its comparison with another sample collected earlier.

The charges against one person were based on a match between their DNA and DNA collected at the scene of the attempted arson of the electrical cabinet. DNA samples were collected both from a latex glove found nearby and from a bottle inside the cabinet—which did not catch fire because of a failed delay.

The charges against other people were based on a match between their DNA and DNA collected from a cigarette used as a delay for an incendiary device—the delay failed and the device was found intact under the police tow truck.

Case against Amos Mbedzi (#2): Mbedzi's DNA was found on a cushion and a sun visor of the car used to transport the explosive device to the bombing site.⁵²

Case against Louna (#2): DNA samples matching Louna's DNA were collected from:⁷

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

⁴⁹<https://sansnom.noblogs.org/archives/16831>

⁵⁰<https://notrace.how/resources/#lafarge>

⁵¹<https://web.archive.org/web/20210612231740/https://roundrobin.info/2021/05/sentenza-beppe>

⁵²<https://notrace.how/documentation/case-against-amos-mbedzi-case-file.pdf>

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

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

Unusable DNA samples were collected from:

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

Repression of the first Jane's Revenge arson (#2):

In May 2022, DNA samples were collected from several items found by investigators at the action site, including a broken window, a glass jar, a lighter, and an intact Molotov cocktail.⁵³ In March 2023, police saw the person discard a bag containing a partially eaten burrito in a public trash can. DNA samples collected from the bag's contents matched those collected at the action site.

Scintilla (#2): The charge against Peppe was based on a match between DNA traces found inside the parcel bomb and his DNA collected from a cigarette butt during the investigation.⁵³

Bure criminal association case (#2): DNA samples were collected from:⁷

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

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

- A DNA sample collected from a Molotov cocktail found in a raid matched an individual in the national DNA database.
- A DNA sample collected from the lid of a jar containing materials that could be used to build

explosive devices, found in a raid, matched an individual in the national DNA database.

- A DNA sample collected from a lighter recovered after a demonstration matched another trace from an earlier, unrelated case, but did not match anyone in the national DNA database.

Case against Ruslan Siddiqi (#2): DNA samples were collected from people living in a large area surrounding the train bombing site, including from soldiers and Ukrainian citizens, presumably because they were deemed potential suspects.⁵⁴

Nea Filadelphia case (#2): The charges against several people were based on a match between their DNA, taken by force while in custody, and DNA samples collected from “mobile objects” near the robberies.⁵⁵

Panico (#2): DNA traces were the only evidence against one of the defendants.⁵⁶

3.9.4. Digital



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

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

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

MITIGATIONS

Avoiding self-incrimination (#2): An adversary can use digital forensics to retrieve self-incriminating information from a digital device. To mitigate this,

to send information about him to the police.¹⁰¹

2019–2020 case against Mónica and Francisco (#2): The saleswoman of the cell phone store where Mónica bought a phone that was used as part of the 2020 action, when questioned by investigators, gave a description of a person that the investigators matched to Mónica.⁴⁵

Arrest of Stecco (#2): After arresting Stecco, investigators showed his picture and asked questions to many people living around the arrest site, which allowed them to find the house where Stecco allegedly lived.¹⁷

Case against Amos Mbedzi (#2): When the explosive device exploded prematurely and severely wounded Mbedzi, a civilian was traveling by car on a nearby road.⁵² The civilian stopped near the bombing site, saw another car stop, and saw Mbedzi shout “Hospital! Hospital!” and get into the other car. The civilian stayed at the site and informed the first cops who arrived that a man wounded in the explosion had gotten into a car towards a hospital. This seemingly led to Mbedzi's arrest at the hospital one hour later.

Additionally, three civilians provided investigators with visual descriptions of Mbedzi: the aforementioned civilian, the driver of the car that took Mbedzi to the hospital, and the hospital security guard. This helped investigators reconstruct Mbedzi's movements and prove that he was at the bombing site.

Case against Louna (#2): Several civilians helped investigators. In particular:⁷

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

Belarusian anarcho-partisans (#2): While trying to cross the Belarusian-Ukrainian border, the people stopped at a shop about 10 kilometers from the border.⁷ A shopkeeper called the border guards on them, which led directly to their arrest.

Case against Ruslan Siddiqi (#2): In the weeks following the train bombing, investigators interrogated many citizens in a large area surrounding the bombing site.⁵⁴

In particular, investigators interrogated a shop clerk in a village. The clerk told investigators that, before the bombing, someone wearing a camouflage jacket and carrying a backpack had passed by the shop. The clerk provided a description of the person, which investigators used to create a composite sketch. Three weeks after the bombing, Ruslan Siddiqi encountered a local cop who compared him with the composite sketch and arrested him.

Case against Direct Action (#2): Several civilians helped investigators.¹¹ In particular:

- Journalists told investigators that they had noticed similarities between action claims published by Direct Action and articles in a local quarterly publication called Resistance.
- A hunter, presumably by chance, discovered two wooden structures where members of Direct Action stored the stolen explosives they used in bombings, and alerted the police to the discovery.⁸²
- 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.

3.18.2. 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.

⁵³<https://web.archive.org/web/20200918130026/https://roundrobin.info/2019/12/verona-una-perquisizione-e-un-arresto>

⁵⁴<https://theins.ru/en/society/280988>

⁵⁵<https://abcsolidaritycell.espivotblogs.net/archives/130>

⁵⁶<https://panicoanarchico.noblogs.org>

¹⁰¹<https://antifenix.noblogs.org/post/2016/03/11/confirmed-lukas-borl-under-police-investigation>

See How the police interrogate and how to defend against it⁹⁸ (in French and German) for a comprehensive overview of police interrogation techniques.

MITIGATIONS

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

REPRESSIVE OPERATIONS

Case against Boris (#2): When interrogating people close to Boris, investigators used elaborate lies to try to get information from them.²² For example, the investigators vaguely suspected that the people being interrogated had hosted Boris in April 2020 and wanted to confirm their suspicion, so they asked, “Our investigation revealed that you let [Boris] stay with you in April 2020. How long did he stay with you?”

Warsaw 3 (#2): A few weeks into his detention, one person gave an “extensive” testimony to the police. He claimed this was partly because of two techniques used by one of his lawyers to push him to give this testimony:⁹⁹

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

Case against Ruslan Siddiqi (#2): After his arrest, investigators were unsure of Ruslan Siddiqi’s involvement in the train bombing.¹⁰⁰ They interrogated him and deduced that he was hiding something. Ruslan Siddiqi recounts: “They started asking various questions about what I was doing on [the day of the bombing]. I made a couple of blunders in my answers, and [the person in civilian clothes] who asked the questions realized that I was hiding something.”

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

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

3.18. 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.

3.18.1. Civilian snitches

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

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

MITIGATIONS

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

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

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

REPRESSIVE OPERATIONS

Fenix (#2): When Lukáš Borl was in clandestinity his photo and personal information were published on the national police website to encourage civilians

you can avoid storing such information on digital devices except for very deliberate reasons (such as writing and sending an action claim while following **digital best practices (#2)**).

Digital best practices (#2): An adversary can use digital forensics to retrieve data from a digital device you have used. To mitigate this, you can follow digital best practices and, in particular, use Tails,⁵⁷ an “amnesic” operating system designed to leave no trace on the computer it runs on.

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

- Use popular rather than custom tools.
- If you use a Virtual Private Server (VPS), **purchase it anonymously (#2)** and access it through Tails.⁵⁷

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

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

REPRESSIVE OPERATIONS

Case against Revolutionära fronten (#2): Investigators analyzed the computer of one of the defendants, that was seized during a raid, and retrieved messages sent and received by the defendant on the messaging application MSN Messenger.⁷ The messages included:

- Detailed discussion of the Stockholm beating, including mentions of the names of some of the defendants as participants in the beating.
- Discussion of the nighttime visit to the fascist’s house, including mentions of the names of the occupants of the house and mentions of the

names of some of the defendants as participants in the visit.

Bure criminal association case (#2): Investigators analyzed storage devices by automatically extracting files containing the following keywords relevant to the investigation:⁷

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

3.9.5. Facial recognition

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

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

Modern facial recognition systems are capable of matching a face image against a large database of faces, even if the face in the image is masked, with only the eyes and eyebrows visible. Facial recognition systems coupled with **mass video surveillance (p. 41)** can be used to automate the tracking of individuals through a space.

See the “Facial recognition” topic.⁵⁸

MITIGATIONS

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

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

⁹⁹<https://wawa3.noblogs.org/post/2017/05/24/olsen-gang-replies-statements-of-warsaw-three-en>

¹⁰⁰<https://anarchistnews.org/content/you-could-call-me-partisan-ruslan-siddiqi-recounts-his-anti-war-actions>

⁵⁷<https://tails.net>

⁵⁸<https://notrace.how/resources/#topic=facial-recognition>

REPRESSIVE OPERATIONS

2019–2020 case against Mónica and Francisco (#2): In order to identify Mónica and Francisco on public CCTV footage, photos of both were compared to the footage, including a comparison of several facial features: eye distances, wrinkles, piercing scars, ear size, mouth and nose shape.⁴⁵

2013 case against Mónica and Francisco (#2): The main evidence against Mónica and Francisco was a comparison of photos of both of them with public CCTV footage that showed their uncovered faces while they were in the subway, shortly before or after the action.⁵⁹

Repression of the attack on Clarín's headquarters (#2): Investigators used facial recognition software to identify one of the defendants, using a photo of their face extracted from CCTV footage near the attack site.⁶⁰

3.9.6. Fingerprints



Ridges on a human finger.

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

Collection

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

⁵⁹<https://notrace.how/documentation/monica-and-francisco-2013-case-file.pdf>

⁶⁰<https://notrace.how/documentation/clarin-case-file.pdf>

Analysis

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

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

Fingerprint databases

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

Other types of prints

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

See also

See the “Fingerprints” topic.⁶¹

MITIGATIONS

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

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

REPRESSIVE OPERATIONS

Bure criminal association case (#2): Fingerprints were collected from items found during raids, including a notebook, sheets of paper, gas masks, helmets, Molotov cocktails, and containers filled with

⁶¹<https://notrace.how/resources/#topic=fingerprints>

collaboration Sabu received a lenient sentence: after having spent 7 months in prison (for a bail violation), they were sentenced to time served.⁹²

Sabu knew Jeremy Hammond's online persona but did not know his real life identity. To find out Jeremy Hammond's real life identity, investigators used information that he had shared with Sabu in online chats, including that:⁹³

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

Operation 8 (#2): At least two informants were active as part of the operation.⁹⁴ In particular:

- Informants provided investigators with background information on the defendants and the dates of the “training camps.”
- An informant offered to sell someone a shotgun, presumably so that person could later be charged with possessing the shotgun.

3.16. International cooperation

Used in tactics: **Arrest, Incrimination**

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

International cooperation can be used to:

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

⁹²<https://latimes.com/nation/nationnow/la-na-nn-hacker-sabu-sentenced-20140527-story.html>

⁹³<https://notrace.how/documentation/jeremy-hammond-affidavit.pdf>

⁹⁴<https://putatara.net/2015/10/05/informants>

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

REPRESSIVE OPERATIONS

Repression against Zündlumpen (#2): House raids were conducted Austria, targeting people suspected of being close to N. and M.⁹

Bialystok (#2): In June 2020, people were arrested in Spain and France, thanks to cooperation between Italian, Spanish and French intelligence and police forces.⁹⁵

During the investigation Italian cops tried to target a person living in Germany.⁹⁶ They sent several requests to German police to extradite the person or have their house searched but the requests were rejected.

Scintilla (#2): Carla was arrested in France thanks to cooperation between Italian and French intelligence and police forces.⁹⁷

Bure criminal association case (#2): Some of the people that were arrested had participated in demonstrations against the 2017 G20 summit in Hamburg, Germany.⁷ Because of this, German investigators cooperated with French investigators, including by being present when the people were interrogated after their arrest.

3.17. Interrogation techniques

Used in tactic: **Incrimination**

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

Interrogation techniques can include lying, making threats, instilling guilt, shame, or pride, trying to appear friendly and helpful or, on the contrary, threatening and violent, etc. In some cases, they can include **physical violence** (p. 50).

⁹⁵<https://malacoda.noblogs.org/anarchici-imprigionati>

⁹⁶<https://attaque.noblogs.org/post/2022/02/20/italie-alle-magne-de-rome-a-bialystok-en-passant-par-berlin>

⁹⁷<https://attaque.noblogs.org/post/2020/08/06/saint-etienne-arrestation-de-carla-recherchee-dans-le-cadre-de-loperation-scintilla>

⁹⁸<https://notrace.how/resources/#police-interroge>

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

REPRESSIVE OPERATIONS

Fenix (#2): Two police officers infiltrated the network of the defendants for several months.⁸⁷ During their infiltration, the two officers:

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

3.15. Informants

Used in tactic: **Incrimination**

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

An adversary can use different strategies to recruit an informant:

- Target people who are seen as more likely to become informants: people on the periphery of a network who are less committed, people who are no longer in a group or network and harbor feelings of resentment...
- Threaten someone with negative consequences if they don't become an informant: a longer prison sentence, deportation...
- Offer someone positive consequences if they become an informant: immunity or leniency in the judicial case in which they are asked to become an informant or in another case, money...

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

See the “Infiltrators and informants” topic.⁸⁵

⁸⁷<https://antifenix.noblogs.org/post/2015/07/01/the-czech-undercover-police-agents-reveald>

MITIGATIONS

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

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

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

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

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

REPRESSIVE OPERATIONS

Case against Marius Mason (#2): The main evidence against Marius Mason was provided to investigators by his former husband, Frank Ambrose, who had participated in some of the actions with him.⁸⁸ Frank Ambrose became an informant after his arrest in 2007 (which was triggered by him throwing incriminating material in a garbage can).⁸⁹ For several months, the snitch collaborated extensively with the Federal Bureau of Investigation (FBI), secretly recording 178 phone conversations and face-to-face meetings, and providing information on 15 people.⁹⁰

2011-2013 case against Jeremy Hammond (#2): In June 2011, investigators recruited an associate of Jeremy Hammond, Sabu, as an informant.⁹¹ For several months, Sabu helped investigators build a case against Jeremy Hammond. In exchange for their

⁸⁸<https://supportmariusmason.org/about-marius/about-the-case>

⁸⁹https://mlive.com/news/ann-arbor/2008/10/activist-turned_informant_sent.html

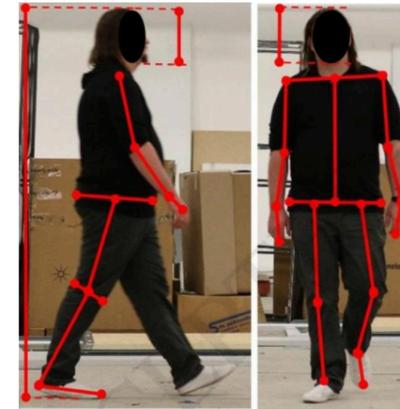
⁹⁰<https://animalliberationpressoffice.org/NAALPO/snitches>

⁹¹<https://rollingstone.com/culture/culture-news/the-rise-and-fall-of-jeremy-hammond-enemy-of-the-state-183599>

gasoline or other substances.⁷ The vast majority of the fingerprints collected did not match anyone. Some of the fingerprints collected matched individuals in the national fingerprint database.

Repression of the attack on Clarín's headquarters (#2): The fingerprints of one defendant were found on a Molotov cocktail that was used in the attack but did not break.⁶⁰

3.9.7. Gait recognition



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

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

Factors of gait

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

- Intrinsic factors: how you learned to walk, your anatomy and physiology, and any injuries or pathologies you may have.
- Extrinsic factors: your clothing and the terrain on which you move (flat or not, with or without obstacles...)

Analysis

An adversary watching you move can locate, measure, and categorize your body features (position of your ankles, knees, hips...) at various stages of movement and compare them to the body features of another

moving person. This comparison can allow the adversary to determine whether or not you could be that other person, but it usually doesn't allow the adversary to determine with certainty that you are that other person. This comparison is usually done by humans, sometimes assisted by specialized software.

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

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

Typical scenario

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

- A person is captured by CCTV carrying out an action. They are not recognizable because they are **dressed anonymously (#2)**. The adversary obtains the CCTV footage.
- Based on other evidence, the adversary suspects someone of having carried out the action. They obtain footage of this suspect moving, either through CCTV near their home, CCTV while they are in custody, or a **covert video surveillance device** (p. 12).
- The adversary compares the person's gait in the first footage to the suspect's gait in the second footage to determine whether or not they could be the same person, and the confidence in that determination.

See also

See *Forensic Gait Analysis: Principles and Practice*³⁵ for a comprehensive overview of gait recognition.

MITIGATIONS

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

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

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

REPRESSIVE OPERATIONS

Bialystok (#2): The main evidence against the person accused of an explosive attack on a police station was a comparison of his gait and the color of his coat with the corresponding characteristics of a person recorded by the surveillance cameras of the police station.⁶²

Scintilla (#2): Two of the people were accused of arson because their gait and body shapes were considered compatible with people recorded by video surveillance cameras placing a canister of flammable liquid in front of an Italian post office.⁶³

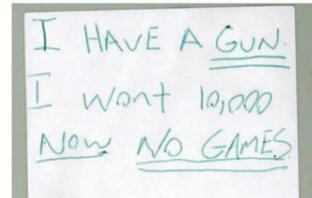
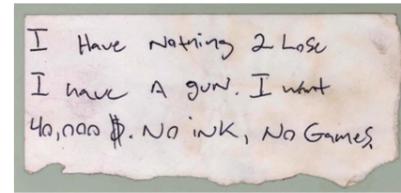
Operation 8 (#2): One person was identified in footage of the “training camps” based on their height, gait, and skin color.⁷

Repression of the attack on Clarín's headquarters (#2): One of the defendants was identified because their gait was considered compatible with that of a suspect visible in CCTV footage near the attack site.⁶⁰

⁶²<https://ilrovescio.info/2022/02/02/aggiornamento-sulle-misure-e-sul-processo-per-lop-byalistok>

⁶³<https://macerie.org/index.php/2019/04/17/ultime-da-carceri-e-tribunali>

3.9.8. Handwriting analysis



Two robbery notes⁶⁴ showing similarities in the formation of the number “0”.

Handwriting analysis (also known as *handwriting recognition*) is the analysis of handwriting samples, typically for the purpose of matching one sample to another.⁸³

Factors of handwriting

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

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

⁶⁴Some bank robberies are carried out by discreetly handing the teller a written note demanding money in order to draw as little attention as possible.

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

MITIGATIONS

Attack (#2): If you expect the police to increase their presence at a public demonstration, you can organize to make sure the crowd is large and fierce enough: decentralized and autonomous forces are more agile than the rigid chain of command that police agencies rely on for crowd control. For example, despite years of planning to militarize Hamburg, Germany, for the G20 summit, rioters were able to liberate a neighborhood from police occupation for an entire night.⁸³

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

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

3.14. Infiltrators

Used in tactic: **Incrimination**

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

⁸³<https://crimethinc.com/2017/08/07/total-policing-total-defiance-the-2017-g20-and-the-battle-of-hamburg-a-full-account-and-analysis>

Stop Hunting Sheep⁸⁴ describes five basic types of infiltrators:

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

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

See the “Infiltrators and informants” topic.⁸⁵

MITIGATIONS

Attack (#2): You can attack infiltrators when uncovered or years later⁸⁶ to discourage the practice—police infiltrators are likely to be less enthusiastic if there is a local precedent of violence against them.

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

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

⁸⁴<https://notrace.how/resources/#stop-hunting>

⁸⁵<https://notrace.how/resources/#topic=infiltrators-and-informants>

⁸⁶<https://actforfree.noblogs.org/post/2022/03/12/hamburgermanya-incendiary-attack-on-the-car-of-former-police-spy-astrid-oppermann>

- Clothing items and camping gear, including tents, hiking boots, and tarps. The items were seized in an attempt to match them to similar items visible in footage of the “training camps.”⁶
- Vehicles.
- Nine firearms.

Some of the raids were particularly thorough: cops searched freezers, garbage bins, and compost bins.

Repression of the attack on Clarín's headquarters (#2): During raids, investigators found eight national identity cards and a debit card in the names of third parties.⁶⁰ In court, the cards were presented as evidence of the defendants' “strategy of concealment” and were used to justify keeping them in preventive detention.

Case against Direct Action (#2): In a raid on the house where four members of Direct Action lived, investigators found:⁸²

- Related to the electrical substation bombing: plans of the action site, a copy of the action claim sent after the bombing, and newspaper clippings of articles about the bombing.
- Related to the Litton Industries bombing: photographs and plans of the action site, newspaper clippings of articles about the bombing, and a pocket knife taken by a member of Direct Action from the stolen van used in the bombing.

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

3.12. ID checks

Used in tactics: **Arrest, Incrimination**

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

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

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

MITIGATIONS

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

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

REPRESSIVE OPERATIONS

Case against Boris (#2): Investigators obtained and analyzed records of ID checks made by local police shortly before and after the sabotages, in different perimeters around where the sabotages took place, presumably hoping to find the names of the saboteurs in those records.²²

3.13. Increased police presence

Used in tactics: **Arrest, Deterrence**

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

Examples of increased police presence include:

- More frequent **police patrols** (p. 51) in a particular area.

- Your physical and mental state while writing: fatigue, stress, altered state due to alcohol, drugs or medication, etc.

Analysis

An adversary can analyze a writing sample to identify its characteristics, including:

- The layout of the text: margins, space between lines, and parallelism of lines. In the case of envelopes: the style, size, and position of the address on the envelope.
- The writing style: for example cursive or block letters.
- The space between characters and between words.
- Connections or separations between characters.
- The design and construction of characters: the shape of characters, whether a character is represented with one or more shapes throughout the sample, the order in which a shape is traced, whether and how a shape is affected by the particular shapes that precede and follow it, and the size of shapes.
- The strokes traced when the writing instrument reaches and leaves the writing surface, including their length, direction, path, and abruptness.
- The pressure exerted by the writing instrument on the writing surface.
- The position of the writing instrument relative to the writing surface.

In some languages that are written horizontally, such as English, an adversary can also identify the following characteristics:

- Whether the baseline⁶⁵ is straight or varies throughout the sample.
- The writing slant: the predominant inclination of characters relative to the baseline.

An adversary can compare the characteristics of a writing sample to the characteristics of another to determine whether or not the samples were written by the same person, and the confidence in that determination. This comparison can be done by humans or by specialized software.

⁶⁵The baseline is the horizontal line upon which the characters “sit”. For example, the “loop” of a lowercase “p” sits on the baseline, while its “tail” extends below the baseline.

Handwriting databases

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

See also

See also Huber and Headrick's *Handwriting Identification: Facts and Fundamentals*³⁵ for a comprehensive overview of handwriting analysis.

MITIGATIONS

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

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

REPRESSIVE OPERATIONS

Scripta Manent (#2): Handwriting samples of some of the defendants (including notes seized during raids and letters written from prison) were compared to handwritten addresses on unexploded parcel bombs

⁸²<https://web.archive.org/web/20100715145801/http://uniset.ca/other/cs5/27CCC3d142.html>

in an attempt to link the defendants to the attacks.⁶⁶ **2019–2020 case against Mónica and Francisco (#2):** The labels on the two parcel bombs remained intact—one because the parcel didn't explode, and one despite the explosion of the parcel.⁴⁵ The handwritten signatures on the labels were compared and positively matched. This showed that the parcels were sent by the same person.

Repression of the first Jane's Revenge arson (#2): A comparison between the cursive graffiti left at the action site and the same style of graffiti painted a few months later during a demonstration helped identify the person.³⁹

3.9.9. Linguistics

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

Author identification

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

- Who wrote an anonymous action claim posted on the Internet or sent to a newspaper.
- Whether multiple anonymous action claims were likely written by the same person or group.
- Who wrote a plan describing illegal activities found during a **house raid** (p. 33), a **covert house visit** (p. 8) or an arrest.

Voice identification

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

- Who is speaking on a tapped mobile phone or a recording made by a **hidden microphone** (p. 10).
- Who called the authorities to make a bomb threat.

⁶⁶<https://lib.anarhija.net/library/operation-scripta-manent-in-italy-2016-2019#toc15>

See also

On the topic of author identification:

- Counteracting Forensic Linguistics.⁶⁷
- Who wrote that?⁶⁸

MITIGATIONS

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

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

REPRESSIVE OPERATIONS

Scripta Manent (#2): Texts published by some of the defendants were compared with action claims by the Informal Anarchist Federation, with the aim of proving that the defendants had written these claims.⁶⁶

Repression against Zündlumpen (#2): Investigators compared texts from the newspaper Zündlumpen with private letters found in house raids, hoping to prove that people had written in the newspaper.⁴⁷

Case against Direct Action (#2): Investigators noticed linguistic similarities between action claims published by Direct Action and articles in a local quarterly publication called Resistance.¹¹ This led them to identify a contributor to Resistance, who was a friend of members of Direct Action, and place her under **physical surveillance** (p. 45).

⁶⁷<https://anonymousplanet.org/guide/appendix-a4-counteracting-forensic-linguistics>

⁶⁸<https://notrace.how/resources/#who-wrote>

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

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

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

REPRESSIVE OPERATIONS

Scripta Manent (#2): One person was arrested after batteries and an electrician's manual were found in his home during a raid.⁷⁷

Renata (#2): During a house raid, cops tried to get into the basement without waking up the people in the house, then privately complained that they were unable to hide what they wanted to hide.⁷⁸

Case against Revolutionära fronten (#2): During raids on the homes of some of the defendants, investigators found:⁷

- A computer containing incriminating messages sent and received on the messaging application MSN Messenger.
- Molotov cocktails.

Repression of Lafarge factory sabotage (#2): Among the initial house raids, one was particularly thorough: cops searched under mattresses, behind sofa covers and in every drawer of every piece of furniture, inspected every book, notebook and piece of clothing as well as the dishes, and emptied packages of pasta and sealed jars.⁷⁹

2013 case against Mónica and Francisco (#2): During a raid on the home of Mónica and Francisco, investigators found:⁵⁹

- Several pieces of clothing and other accessories that Mónica and Francisco had used during the action and that were visible on public CCTV footage.

⁷⁷https://web.archive.org/web/20170928080735/http://www.informa-azione.info/italia_repressione_5_nuovi_arresti_e_una_trentina_di_perquisizioni_per_attacchi_federazione_anarchica_informale

⁷⁸<https://infernourbano.altervista.org/che-si-sappia-comunicato-dal-trentino>

⁷⁹<https://sansnom.noblogs.org/archives/16978>

- Several unencrypted digital storage devices that contained suspicious documents.

Case against Louna (#2): Investigators raided:

- The home of the owner of the car that brought Louna to the hospital.⁷ They seized the car during the raid.
- The home of a person suspected of being seen on the CCTV footage from the hospital carrying a watering jug, in the hope of finding the watering jug during the raid and confirming that the person was indeed at the hospital.⁸⁰

Case against Jeff Luers (#2): During the raid of the storage unit, investigators found:⁷³

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

Bure criminal association case (#2): During the raids, investigators found:⁷

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

Operation 8 (#2): During the raids, investigators seized:⁸¹

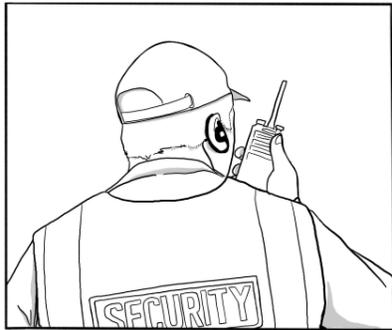
- Electronic devices.
- Photos.

⁸⁰<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>

⁸¹https://rebelpress.nz/wp-content/uploads/2021/03/Day_Raids_Came.pdf

3.10. Guards

Used in tactic: **Arrest**



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

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

MITIGATIONS

Attack (#2): Before or during an action, you can incapacitate guards to prevent them from interfering with the action. For example, in their actions on logging companies machinery in so-called Chile, Mapuche people have neutralized guards by disarming them,⁷⁴ tying them up⁷⁵ or shooting at them.⁷⁶

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

REPRESSIVE OPERATIONS

Case against Louna (#2): In the days preceding the arson, a security guard saw suspicious vehicles driving near the arson site, took photos of them, and, after the arson, provided the photos to investigators.⁷

⁷⁴<https://actforfree.noblogs.org/post/2022/08/04/chile-a-fiery-july-in-the-mapuche-territories>

⁷⁵<https://actforfree.noblogs.org/post/2022/02/28/chile-the-mapuche-struggle-continues-under-a-state-of-emergency>

⁷⁶<https://actforfree.noblogs.org/post/2021/07/21/chile-mapuche-zone-ignites-after-the-murder-of-pablo-marchant-update>

3.11. House raid

Used in tactics: **Arrest, Incrimination**

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

When

An adversary can conduct a house raid:

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

Why

An adversary can conduct a house raid to:

- Seize items to find evidence or to do **network mapping (p. 44)**. Commonly seized items include electronic devices, literature, materials that could be used in actions, and clothing. In some cases, the adversary seizes expensive items (e.g., computers, printing equipment) with the goal of disrupting the organizational capacity of their targets.
- Arrest the occupants of the residence.
- Install **covert surveillance devices (p. 9)** in the residence.

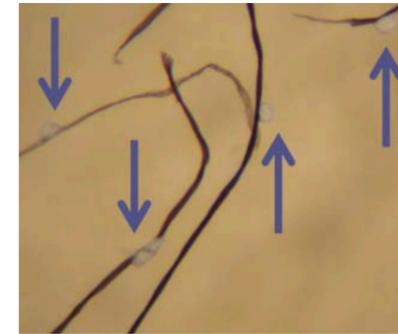
Additional considerations

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

MITIGATIONS

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

3.9.10. Trace evidence



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

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

Trace evidence can be:

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

Trace evidence can be transferred:

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

An adversary can use trace evidence to:

- Analyze a trace from an action site to obtain useful information. For example, they can analyze a shoeprint found at an action site to determine the size and model of the shoe that left it, and then search for people who possess shoes of that size and model.
- Link a trace from an action site to an object. For example, they can determine whether textile

fibers found on a fence at an action site likely come from clothing that they seized from your home during a **house raid (p. 33)**.

- Link a trace from an object to an action site. For example, they can determine whether shards of glass found on your clothing during your arrest likely come from a window that was recently broken nearby.
- Link traces from different action sites. For example, they can determine whether hammer marks found at different action sites were left by the same hammer, and therefore the actions were likely carried out by the same people.

Trace evidence does not include **fingerprints (p. 25)** and **DNA (p. 20)**, which are considered separate forensic disciplines.

Fibers

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

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

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

An adversary can:

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

See Handbook of Trace Evidence Analysis,³⁵ chapter “Fibers” for an overview of fibers.

Footprints

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

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

- On a hard, dusty surface, a foot may leave a very unique footprint that shows the ridges of the toes, which are as unique as **fingerprints (p. 25)**.
- On a soft surface such as sand, a foot may leave a very generic footprint that shows only a rough outline of the foot.

An adversary can:

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

See *Examination and Interpretation of Bare Footprints in Forensic Investigations*⁶⁹ for an overview of footprints.

Shoeprints

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

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

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

An adversary can:

- Analyze a shoeprint to determine the size and model of the shoe and to obtain information

about the person who left it, such as the size of their feet and an estimate of their height.

- Compare a shoeprint to a shoe in their possession to determine if the shoe left the shoeprint. To do this, they can use the shoe to make reference prints and compare them to the suspect shoeprint.
- Compare two shoeprints to determine if they were left by the same shoe.

See *Footwear Impression Evidence: Detection, Recovery and Examination*³⁵ for a comprehensive overview of shoeprints.

Tool marks

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

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

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

An adversary can:

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

See also:

- PRISMA,⁷⁰ section “Tool Traces” for a short discussion of tool marks.
- *Color Atlas of Forensic Toolmark Identification*³⁵ for a comprehensive overview of tool marks.

Glass

When glass breaks, it produces shards of various sizes.

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

- Two glass objects of different models, or manufactured in different factories, or manufactured in the same factory several weeks apart, may produce shards that can be distinguished by analyzing their properties, including their refractive indices⁷¹ and chemical elements.⁷²
- Two glass objects of the same model, manufactured in the same factory during the same week, may produce shards that are indistinguishable.

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

See *Handbook of Trace Evidence Analysis*,³⁵ chapter “Interpretation of Glass Evidence” for an overview of glass evidence.

Traces of accelerant

Traces of accelerant are covered in the technique **Forensics: Arson (p. 16)**.

Other

Other types of trace evidence include:

- Human and animal hair. Hair can fall from a body at any time. Hair can reveal various information about its owner, including, in some cases, their **DNA (p. 20)**. See *Handbook of Trace Evidence Analysis*,³⁵ chapter “Forensic Hair Microscopy” for an overview of hair.
- Paint. A painted object can leave traces of paint on a surface it touches. A trace of paint can reveal information about the object that left it. See *Handbook of Trace Evidence Analysis*,³⁵ chapter “Paints and Polymers” for an overview of paint.

MITIGATIONS

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

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

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

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

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

REPRESSIVE OPERATIONS

Case against Jeff Luers (#2): In the raid of the storage unit, the police found a bolt cutter matching the cuts in the fence surrounding the site of the May arson attempt.⁷³

Case against Ruslan Siddiqi (#2): Investigators found bicycle tire marks near the train bombing site.⁵⁴ This supported the theory that the person who carried out the bombing traveled by bike.

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

⁶⁹<https://notrace.how/documentation/examination-and-interpretation-of-bare-footprints-in-forensic-investigations.pdf>

⁷⁰<https://notrace.how/resources/#prisma>

⁷¹https://en.wikipedia.org/wiki/Refractive_index

⁷²https://en.wikipedia.org/wiki/Chemical_element

⁷³<https://courtlister.com/opinion/2627996/state-v-luers>