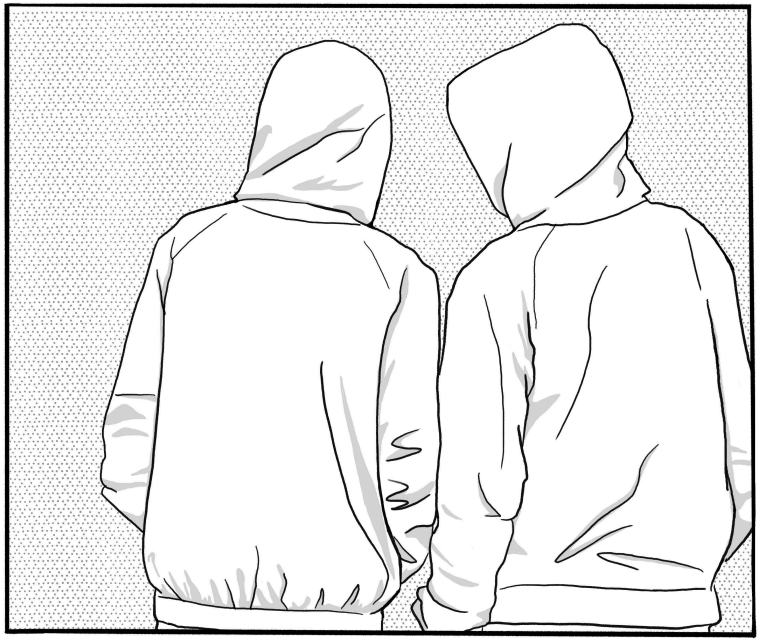
Threat Library

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.



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

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

November 4, 2025

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

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

Original text in English

No Trace Project

notrace.how/threat-library

Anonymous purchases (#4): 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 (#4): 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 (#4)**.
- 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 (#4): 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 (#5): 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 (#5): 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 (#5): During the raids, several objects (a stove, pans, gloves, spatulas) were analyzed for traces of products that could be used to create explosives.[8]

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

- Two glass objects of different models, or manufactured in different factories, or manufactured in the same factory several weeks apart, may produce shards that can be distinguished by analyzing their properties, including their refractive indices[71] 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. 30)**.

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. 38)**. 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 (#4): 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.

[71] https://en.wikipedia.org/wiki/Refractive_index
[72] https://en.wikipedia.org/wiki/Chemical_element

Contents

1. About the Threat Library

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

1.1. Threat modeling

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

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

1.2. The Threat Library

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

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

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:

[70] https://notrace.how/resources/#prisma

- 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.

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

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

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

1.3. Limitations

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

[2] In 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

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.

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. 49)**.
- 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:

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 (#2)**.
- 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. 49)** and **DNA (p. 38)**, which are considered separate forensic disciplines.

2. Tactics

2.1. Deterrence

Uses techniques:

Door knocks (p. 26)
Doxing (p. 27)
Increased police presence (#2)
Mass surveillance (#2)
Physical violence (#3)
Police patrols (#3)

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. 9)
Covert house visit (p. 11)
Covert surveillance devices (p. 12)
Detection dogs (p. 22)
Door knocks (p. 26)
Evidence fabrication (p. 28)
Forensics (p. 29)
House raid (#2)
ID checks (#2)
Infiltrators (#2)
Informants (#2)
International cooperation (#2)
Interrogation techniques (#2)

Mass surveillance (#2)
Network mapping (#3)
Open-source intelligence (#3)
Parallel construction (#3)
Physical surveillance (#3)
Physical violence (#3)
Police patrols (#3)
Roadblocks (#3)
Service provider collaboration (#3)
Targeted digital surveillance (#3)

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

2.3. Arrest

Uses techniques:

Alarm systems (p. 8)
Detection dogs (p. 22)
Guards (#2)
House raid (#2)
ID checks (#2)
Increased police presence (#2)
International cooperation (#2)
Police patrols (#3)
Roadblocks (#3)

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

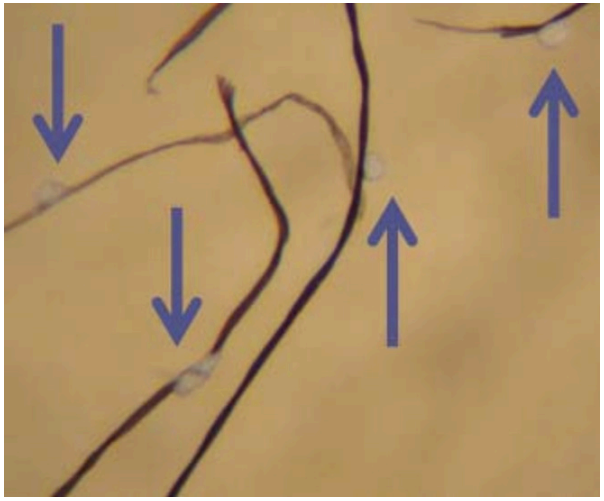
Repressive operations

Scripta Manent (#5): 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 (#5): 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 (#5): 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 (#3)**.

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

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 (#2)**, a **covert house visit (p. 11)** 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. 14)**.
- Who called the authorities to make a bomb threat.

See also

On the topic of author identification:

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

Mitigations

Biometric concealment (#4): You can hide the acoustic properties of your voice to mitigate voice identification.

Masking your writing style (#4): You can mask your writing style to mitigate author identification.

[67] https://anonymousplanet.org/guide/appendix-a4-counteracting-forensic-linguistics

[68] https://notrace.how/resources/#who-wrote

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 systems[4] 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 (#4): 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.

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

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

Digital best practices (#4): When carrying out a cyber action, you can use digital evasion techniques[5] to prevent intrusion detection systems from detecting the action.

Reconnaissance (#4): 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 (#4): 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 (#4): 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 (#5): 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:

[5]https://en.wikipedia.org/wiki/Intrusion_detection_system_evasion_techniques
[6]https://putatara.net/2013/11/25/operation-8-the-evidence

- 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 (#5): Handwriting samples of some of the defendants (including notes seized during raids and letters written from prison) were compared to handwritten addresses on unexploded parcel bombs in an attempt to link the defendants to the attacks.[66]

2019-2020 case against Mónica and Francisco (#5): 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 (#5): 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

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

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

- Whether the baseline[65] 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.

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 (#4): 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.

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

- Activities captured by hidden cameras at the "training camps"—training with firearms, learning military tactics, experimenting with Molotov cocktails—were intepreted 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 (#5): 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 intepreted as paramilitary trainings.
- Handwritten notes of one of the defendants contained terms and phrases such as "weapons", "recruitment", "cleaning DNA", "incendiary device" and "are we ready for a comrade to be wounded or killed?", which were interpreted as indicative that the defendant was preparing an attack in France (despite the defendant's claims that the notes were about either airsoft or Rojava).

[7] Private source.

[8] https://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. 12)** in the residence.
- Install **malware (#3)** 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 (#4): 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 (#4): You can use physical intrusion detection to detect a covert house visit.

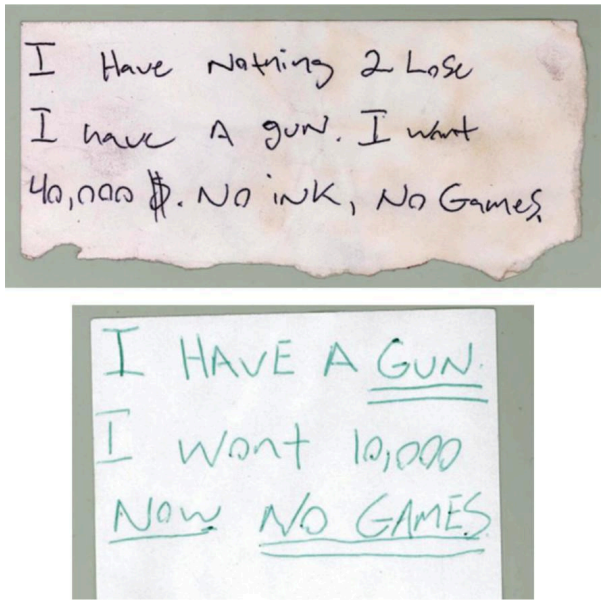
- Your writing level: whether you are learning to write or are an experienced writer.
- The writing instrument: pen, pencil, brush, spray paint can, etc.
- Where you hold the writing instrument: in your right hand, left hand, foot, mouth, prosthesis, etc.
- How you hold the writing instrument: for example,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

Analysis

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

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

3.9.8. Handwriting analysis



Two robbery notes[64] showing similarities in the formation of the number "0".

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

Factors of handwriting

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

- How you learned to write: how you learned to form letters and move the writing instrument.
- Your writing habits: how you personally form letters and move the writing instrument, which can be more or less similar to how you learned.

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

Preparing for house raids (#4): 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 (#4): 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 (#5): Investigators made a covert visit of the cabins where N. and M. lived in order to collect **scent samples (p. 22)**.[9]

Case against Peppy and Krystal (#5): 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 (#5): After overhearing (presumably during a **physical surveillance (#3)** 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.

[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

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 (#4)**) 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.

Bialystok (#5): 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 (#5): 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 (#5): 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 (#5): 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

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

See also

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

Mitigations

Anonymous dress (#4): You can wear baggy clothing to conceal your gait.

Biometric concealment (#4): 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 (#4): 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.

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]

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.

[12] https://notrace.how/earsandeyes
[13] https://notrace.how/resources/#topic=hidden-devices
[14] https://notrace.how/earsandeyes/#modena-2015-12

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 (#3)**.

See Ears and Eyes[12] and the "Hidden devices" topic.[13]

Mitigations

Bug search (#4): You can conduct a bug search to locate covert audio surveillance devices and eventually remove them.

Outdoor and device-free conversations (#4): You can conduct sensitive conversations outdoors and without electronic devices to prevent an adversary from recording those conversations with covert audio surveillance devices.

Physical intrusion detection (#4): 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 (#5): 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 (#5): 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.

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

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.

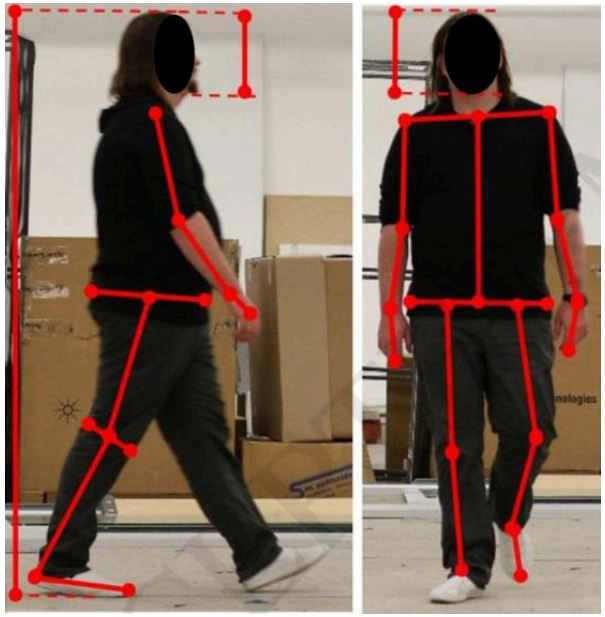
Gloves (#4): You can wear gloves to avoid leaving fingerprints on surfaces you touch.

Repressive operations

Bure criminal association case (#5): Fingerprints were collected from items found during raids, including a notebook, sheets of paper, gas masks, helmets, Molotov cocktails, and containers filled with gasoline or other substances.[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 (#5): 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.

See the corresponding Ears and Eyes case.[16]

Arrest of Stecco (#5): Microphones were installed in two homes, one collective space, and several cars.[17]

Case against Louna (#5): A hidden microphone was installed in a vehicle.[7]

Scintilla (#5): 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 (#5): Microphones were installed in several vehicles and homes.[6]

Case against Direct Action (#5): Investigators installed hidden microphones:[11]

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

One day, after overhearing (presumably during a **physical surveillance (#3)** 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 (#5): 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

[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
[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

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.

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.

[21] https://notrace.how/earsandeyes/#berlin-2022-08

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 (#4): 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.

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

2013 case against Mónica and Francisco (#5): 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 (#5): 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

- 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 (#3)**.

See Ears and Eyes[12] and the "Hidden devices" topic.[13]

Mitigations

Bug search (#4): You can conduct a bug search to locate covert location surveillance devices and eventually remove them.

Physical intrusion detection (#4): 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 (#4): You can use a bike instead of any other type of vehicle: unlike other vehicles, when you conduct a **bug search (#4)** 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 (#5): 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

Repression against Zündlumpen (#5): A GPS tracker was installed on N.'s car.[9]

Arrest of Stecco (#5): 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 (#5): Several GPS trackers were installed on vehicles.[7]

Bure criminal association case (#5): Investigators installed a covert location tracker on a vehicle, where it remained for about a month.[7]

December 8 case (#5): 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:

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

- "*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 (#2)** can be used to automate the tracking of individuals through a space.

See the "Facial recognition" topic.[58]

Mitigations

Anonymous dress (#4): You can wear a mask that adequately covers your face, including your eyebrows and up to the top of your nose.

Biometric concealment (#4): You can wear a mask to cover your facial features, and sunglasses or a hat with a low brim to cover your eyes.

Repressive operations

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

[58] https://notrace.how/resources/#topic=facial-recognition

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 (#4)** and access it through Tails.[57]

Encryption (#4): 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 (#4): 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 (#5): 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 (#5): 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.

- 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 (#4)** 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 about the targets of surveillance and help in **network mapping (#3)**.

See Ears and Eyes[12] and the "Hidden devices" topic.[13]

Mitigations

Bug search (#4): You can conduct a bug search to locate covert video surveillance devices and eventually remove them.

Digital best practices (#4): 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 (#4): 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 (#4): 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 (#4): 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.

[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

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

Repressive operations

Case against Boris (#5): 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 (#5): 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 (#5): 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 (#5): Cameras were installed to film the entrances of several places where people opposed to the highway project lived.[7]

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 (#4): An adversary can use digital forensics to retrieve self-incriminating information from a digital device. To mitigate this, you can avoid storing such information on digital devices except for very deliberate reasons (such as writing and sending an action claim while following **digital best practices (#4)**).

Digital best practices (#4): 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.

[57] https://tails.net

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 (#5): 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 (#5): 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 (#5): DNA traces were the only evidence against one of the defendants.[56]

[54]https://theins.ru/en/society/280988
[55]https://abcsolidaritycell.espivblogs.net/archives/130
[56]https://panicoanarchico.noblogs.org

Operation 8 (#5): 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 (#5): 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:

- At an action site or during a **house raid (#2)** or **covert house visit (p. 11)** to determine if a substance is present and locate it.
- During an **ID check (#2)** 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

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

DNA 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 (#5): 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.[39] 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 (#5): 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 (#5): 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.

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

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.

Repression of Lafarge factory sabotage (#5): 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 (#5): DNA traces were used to convict the person accused of burning an ATM.[51]

Mauvaises intentions (#5): 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 (#5): 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 (#5): DNA samples matching Louna's DNA were collected from:[7]

[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

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

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

Repressive operations

Fenix (#5): In one of the house raids, the police used detection dogs trained to detect explosives.[26]

[25] https://notrace.how/resources/#things-burning

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

Cospito.[44]

Case against Boris (#5): 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 (#5): 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 (#5): In some of the raids, DNA samples were collected from a cigarette butt,[46] zines,[47] books, doors, cups, and printing machines.

Renata (#5): 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 (#5): 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.

[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

See also

- Dna You Say? Burn Everything to Burn Longer: A Guide to Leaving No Traces[42] for an overview of DNA forensics.
- The No Trace Project DNA Literature Review[41] for a collection of useful details on DNA forensics, taken from academic literature.
- The "DNA" topic.[43]

Mitigations

Careful action planning (#4): 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 (#4)**.
- Ensure that nothing is accidentally left behind such as a bag, tool, or anything that could fall out of a pocket.

DNA minimization protocols (#4): 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 (#4): You can wear gloves to avoid leaving DNA on surfaces you touch.

Repressive operations

Scripta Manent (#5): DNA evidence was used to convict Alfredo

[42] https://notrace.how/resources/#dna-you-say
[43] https://notrace.how/resources/#topic=dna

Repression against Zündlumpen (#5): 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 firelighters, firelighter 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 (#5): Detection dogs were used in one of the raids.[7]

3.6. Door knocks

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

[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 (#2)**, 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 (#3)**.

In many countries, it is easier for the State to carry out door knocks than **house raids (#2)** because door knocks do not require a warrant or legal authorization.

Mitigations

Avoiding self-incrimination (#4): 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 (#4): 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 (#5): In 2025, agents from the Federal Bureau of Investigation (FBI) knocked on doors and asked for information about the person.[7]

Scintilla (#5): 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.

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

- 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.

- 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 Review[41] 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 Review[41] 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.
- 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:

[41] https://notrace.how/resources/#dna-review

Doxing often uses information obtained through **open-source intelligence (#3)**.

Mitigations

Digital best practices (#4): 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 (#4): 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 (#5): 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

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

in the investigation files as “prima o poi scoppierà” (“will, sooner or later, explode”).

December 8 case (#5): 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 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.

3.9.3. 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 cell[40] 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.

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.

[40] With the exception of red blood cells.

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 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 (#4): 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 (#4): 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.

3.9.1. 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 (#2)** 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. 22)** 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.

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 (#5): 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 (#5): A gas detector[38] 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 (#5): DNA samples were collected from an intact Molotov cocktail found by investigators at the action site.[39]

Bure criminal association case (#5): Traces of accelerants were collected from items recovered after demonstrations and analyzed.[7]

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

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

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

there to the identity of the person who purchased them. To mitigate this, you can purchase accelerants[36] and device components anonymously.

Careful action planning (#4): 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

[36] If 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.

- 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]
- 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

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

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

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.
- 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.

[33] A 2020 study from the Netherlands briefly mentions "a database of gasoline collected nationally."

- **DNA traces (p. 38)** and **fingerprints (p. 49)** left while handling the device components.
- **Tool marks (p. 60)** left when constructing the device.
- Identifiers visible on the device components such as serial numbers or barcodes.
- **Glass traces (p. 60)**, 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 (#4): An adversary can link accelerants and incendiary device components to where they were purchased, and from

[34] For more information see the "Degradation" section of the No Trace Project DNA Literature Review.[a]

[a] https://notrace.how/resources/#dna-review

[35] Available on the Surveillance Archive.[a]

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