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

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

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

Threat Library

Part 2/5

Techniques A–I

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

Original text in English

No Trace Project

notrace.how/threat-library

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

April 18, 2025

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

tion revealed that you let [Boris] stay with you in April 2020. How long did he stay with you?"

Warsaw 3 (#5): A few weeks into his detention, one person gave an "extensive" testimony to the police. He claimed this was partly because of two techniques used by one of his lawyers to push him to give this testimony:[81]

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

Case against Ruslan Siddiqi (#5): After his arrest, investigators were unsure of Ruslan Siddiqi's involvement in the bombing.[82] They interrogated him and deduced that he was hiding something. Ruslan Siddiqi recounts: "They started asking various questions about what I was doing on [the day of the bombing]. I made a couple of blunders in my answers, and [the person in civilian clothes] who asked the questions realized that I was hiding something."

December 8 case (#5): When interrogating defendants during custody, investigators:[4]

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

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

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

Contents

4. Techniques

4.1. Alarm systems

Used in tactic: **Arrest**

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

For physical infrastructure, modern alarm systems typically include sensors that detect unauthorized access to an area outside of normal operating hours. Such sensors include infrared motion detectors, sensors that detect the opening of doors, and many other types of sensors.[1] 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[2] 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.

[1] https://en.wikipedia.org/wiki/Security_alarm#Sensor_types
[2] https://en.wikipedia.org/wiki/Intrusion_detection_system

between Italian and French intelligence and police forces.[79]

Bure criminal association case (#5): Some of the people that were arrested had participated in demonstrations against the 2017 G20 summit in Hamburg, Germany.[12] Because of this, German investigators cooperated with French investigators, including by being present when the people were interrogated after their arrest.

4.17. Interrogation techniques

Used in tactic: **Incrimination**

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

Interrogation techniques can include lying, making threats, instilling guilt, shame, or pride, trying to appear friendly and helpful or, on the contrary, threatening and violent, etc. In some cases, they can include **physical violence (#3)**.

See How the police interrogate and how to defend against it[80] (in French and German) for a comprehensive overview of police interrogation techniques.

Mitigations

Avoiding self-incrimination (#4): You should not talk to an adversary under any circumstances: this is the best way to resist their interrogation techniques.

Repressive operations

Case against Boris (#5): When interrogating people close to Boris, investigators used elaborate lies to try to get information from them.[17] For example, the investigators vaguely suspected that the people being interrogated had hosted Boris in April 2020 and wanted to confirm their suspicion, so they asked, "Our investiga-

[79] https://attaque.noblogs.org/post/2020/08/06/saint-etienne-arrestation-de-carla-recherchee-dans-le-cadre-de-loperation-scintilla
[80] https://notrace.how/resources/#police-interroge

jail, and was currently on probation. Investigators were able to verify all of this using police files.

- Comrades of his had been arrested at a specific protest. Investigators were able to verify that an "associate" of Jeremy Hammond had attended the protest.
- He practiced dumpster-diving. Investigators saw him getting food from dumpsters during a physical surveillance operation.

4.16. International cooperation

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

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

International cooperation can be used to:

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

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

Repressive operations

Bialystok (#5): In June 2020, people were arrested in Spain and France, thanks to cooperation between Italian, Spanish and French intelligence and police forces.[77]

During the investigation Italian cops tried to target a person living in Germany.[78] They sent several requests to German police to extradite the person or have their house searched but the requests were rejected.

Scintilla (#5): Carla was arrested in France thanks to cooperation

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

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

Digital best practices (#4): When carrying out a cyber action, you can use digital evasion techniques[3] 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.

4.2. Biased interpretation of evidence

Used in tactic: **Incrimination**

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

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

Mitigations

Digital best practices (#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

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. Exam-

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

ples of this interpretation include:[4]

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

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

Prisoner support (#4): You can support prisoners from your networks: beyond the ethical imperative of this support, people are less likely to turn informant if they feel supported and connected to the movements for which they risked their freedom.

Repressive operations

Case against Marius Mason (#5): The main evidence against Marius Mason was provided to investigators by his former husband, Frank Ambrose, who had participated in some of the actions with him.[71] Frank Ambrose became an informant after his arrest in 2007 (which was triggered by him throwing incriminating material in a garbage can).[72] For several months, the snitch collaborated extensively with the Federal Bureau of Investigation (FBI), secretly recording 178 phone conversations and face-to-face meetings, and providing information on 15 people.[73]

2011-2013 case against Jeremy Hammond (#5): In June 2011, investigators recruited an associate of Jeremy Hammond, Sabu, as an informant.[74] For several months, Sabu helped investigators build a case against Jeremy Hammond. In exchange for their collaboration Sabu received a lenient sentence: after having spent 7 months in prison (for a bail violation), they were sentenced to time served.[75]

Sabu knew Jeremy Hammond's online persona but did not know his real life identity. To find out Jeremy Hammond's real life identity, investigators used information that he had shared with Sabu in online chats, including that:[76]

- He had been arrested at the 2004 Republican National Convention, had spent time in a federal prison and in a county

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

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

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

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

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

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

4.15. Informants

Used in tactic: **Incrimination**

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

An adversary can use different strategies to recruit an informant:

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

An adversary can use an informant to gather evidence or to **map a network (#3)**.

See the "Infiltrators and informants" topic.[68]

Mitigations

Attack (#4): You can attack informants when uncovered or years later to discourage others from becoming informants.

Background checks (#4): You can perform background checks to help ensure that someone in your network is not an informant.

Need-to-know principle (#4): You can apply the need-to-know principle to limit the information a potential informant can obtain about your involvement in actions (if an informant isn't involved in an action, they shouldn't know who is involved even if it's their own roommate).

Network map exercise (#4): You can conduct a network map exercise to help ensure your network does not place trust in people who could be or become informants.

4.3. Covert house visit

Used in tactic: **Incrimination**

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

An adversary can conduct a covert house visit to:

- Gather information.
- Install **covert surveillance devices (p. 7)** in the residence.
- Install **malware (#3)** on digital devices.

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

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

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

Mitigations

Clandestinity (#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.

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

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.[5]

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:[6]

- 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.

4.4. Covert surveillance devices

Used in tactic: **Incrimination**

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

Where

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

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

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

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

even a family as part of their undercover role. They will have a fake government-issued ID, employment and rental history, etc.

See the "Infiltrators and informants" topic.[68]

Mitigations

Attack (#4): You can attack infiltrators when uncovered or years later[69] to discourage the practice—police infiltrators are likely to be less enthusiastic if there is a local precedent of violence against them.

Background checks (#4): You can perform background checks to help ensure that someone in your network is not an infiltrator.

Need-to-know principle (#4): You can apply the need-to-know principle to limit the information a potential infiltrator can obtain about your involvement in actions (if an infiltrator isn't involved in an action, they shouldn't know who is involved even if it's their own roommate).

Network map exercise (#4): You can conduct a network map exercise to make your network more resilient to infiltration attempts.

Repressive operations

Fenix (#5): Two police officers infiltrated the network of the defendants for several months.[70] During their infiltration, the two officers:

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

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

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

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

- If you are planning to carry out arson, you can use an incendiary device with a delay so that the device is not activated until after you have left the action site.
- You can take advantage of the fact that an increased police presence in one place means the possibility of a decreased police presence elsewhere.

4.14. Infiltrators

Used in tactic: **Incrimination**

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

Stop Hunting Sheep[67] describes five basic types of infiltrators:

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

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

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

- 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.

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

See also

- Ears and Eyes.[7]

- The "Hidden devices" topic.[8]

4.4.1. Audio

A microphone found inside a neon ceiling light in Modena, Italy, in December 2015.[9]

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

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

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

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

Recorded conversations can be used as evidence in court if incriminating matters are discussed, or if they can be misconstrued to

[7]https://notrace.how/earsandeyes
[8]https://notrace.how/resources/#topic=hidden-devices
[9]https://notrace.how/earsandeyes/#modena-2015-12

4.13. Increased police presence

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

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

Examples of increased police presence include:

- More frequent **police patrols (#3)** in a particular area.
- The deployment of police officers and vehicles at a public demonstration. In the hours before a demonstration begins, police officers and vehicles can cluster on the streets around the demonstration or around its expected targets. This clustering can be an opportunity for them to conduct **overt surveillance (#3)** before, during, and after the demonstration.

Mitigations

Attack (#4): If you expect the police to increase their presence at a public demonstration, you can organize to make sure the crowd is large and fierce enough: decentralized and autonomous forces are more agile than the rigid chain of command that police agencies rely on for crowd control. For example, despite years of planning to militarize Hamburg, Germany, for the G20 summit, rioters were able to liberate a neighborhood from police occupation for an entire night.[66]

Careful action planning (#4): You can carefully plan an action to mitigate the risk of an increased police presence at the action site. For example:

- You can conduct a thorough **reconnaissance (#4)** of the action site and prepare a good escape plan.

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

check can be a pretext for questioning and pressuring, and can be followed by a search of the person's belongings.

Complying with an ID check gives the State information about you, which can help them **map your network (#3)**, and can lead to your arrest if you are wanted by them. The consequences of being unable or refusing to comply with an ID check are highly context-dependent, but may include having your biometric information taken by force or without your knowledge, being detained, and being deported out of the country.

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

Mitigations

Avoiding self-incrimination (#4): If possible, you can avoid answering questions or providing biometric information (face photograph, fingerprints, DNA) during an ID check.

Fake ID (#4): During an ID check, if providing your real identity could lead to your arrest or other negative consequences, you can present a fake ID (as long as the fake ID is not recognized as such by the State).

Repressive operations

Case against Boris (#5): Investigators obtained and analyzed records of ID checks made by local police shortly before and after the sabotages, in different perimeters around where the sabotages took place, presumably hoping to find the names of the saboteurs in those records.[17]

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[7] and the "Hidden devices" topic.[8]

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

Renata (#5): Six hidden microphones and a camera were found in a house after the operation.[10] The microphones were found in the living room, hallway, and bedrooms. The camera was found in the intercom system.

See the corresponding Ears and Eyes case.[11]

Case against Louna (#5): A hidden microphone was installed in a vehicle.[12]

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

[10] https://roundrobin.info/2019/03/trento-sei-microspie-e-una-telecamera-immagini-pesanti

[11] https://notrace.how/earsandeyes/#trento-2019-03

[12] Private source.

published.[13]

See the corresponding Ears and Eyes case.[14]

Case against Direct Action (#5): Investigators installed hidden microphones:[6]

- 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.[15] When the legal authorization for installing and using the microphone expired after two months, the microphone was remotely deactivated but not removed from the truck. It was removed several months later during the raids.

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

[13] https://macerie.org/index.php/2019/03/12/le-orecchie-della-pedrotta

[14] https://notrace.how/earsandeyes/#torino-2019-03

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

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

Case against Direct Action (#5): In a raid on the house where four members of Direct Action lived, investigators found:[65]

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

December 8 case (#5): During the raids, investigators found firearms and products that could be used to create explosives.[4]

4.12. ID checks

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

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

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

Repression of Lafarge factory sabotage (#5): Among the initial house raids, one was particularly thorough: cops searched under mattresses, behind sofa covers and in every drawer of every piece of furniture, inspected every book, notebook and piece of clothing as well as the dishes, and emptied packages of pasta and sealed jars.[63]

2013 case against Mónica and Francisco (#5): During a raid on the home of Mónica and Francisco, investigators found:[42]

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

Case against Louna (#5): Investigators raided:

- The home of the owner of the car that brought Louna to the hospital.[12] They seized the car during the raid.
- The home of a person suspected of being seen on the CCTV footage from the hospital carrying a watering jug, in the hope of finding the watering jug during the raid and confirming that the person was indeed at the hospital.[64]

Case against Jeff Luers (#5): During the raid of the storage unit, investigators found:[57]

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

Bure criminal association case (#5): During the raids, investigators found:[12]

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

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

4.4.2. Location

A GPS tracker found under a vehicle in Berlin, Germany, in August 2022.[16]

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.
- 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[7] and the "Hidden devices" topic.[8]

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

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.[17]

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

Case against Louna (#5): Several GPS trackers were installed on vehicles.[12]

Bure criminal association case (#5): Investigators installed a covert location tracker on a vehicle, where it remained for about a month.[12]

December 8 case (#5): A covert location tracker was installed on a vehicle used by Libre Flot.[15]

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

printing equipment) with the goal of disrupting the organizational capacity of their targets.

- Arrest the occupants of the residence.
- Install **covert surveillance devices (p. 7)** in the residence.

Additional considerations

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

Mitigations

Clandestinity (#4): If you enter clandestinity, an adversary cannot know where you live, and therefore cannot raid your home.

Preparing for house raids (#4): You can prepare for a house raid by minimizing the presence of materials that could be harmful in the event of a raid.

Preparing for repression (#4): You can prepare for repression to minimize the impact of house raids.

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

Scripta Manent (#5): One person was arrested after batteries and an electrician's manual were found in his home during a raid.[61]

Renata (#5): During a house raid, cops tried to get into the basement without waking up the people in the house, then privately complained that they were unable to hide what they wanted to hide.[62]

[61] https://web.archive.org/web/20170928080735/http://www.informa-azione.info/italia_repressione_5_nuovi_arresti_e_una_trentina_di_perquisizioni_per_attacchi_federazione_anarchica_informale

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

Reconnaissance (#4): Before an action, you can identify the presence of guards at the action site.

Repressive operations

Case against Louna (#5): In the days preceding the arson, a security guard saw suspicious vehicles driving near the arson site, took photos of them, and, after the arson, provided the photos to investigators.[12]

4.11. House raid

Used in tactics: **Arrest, Incrimination**

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

When

An adversary can conduct a house raid:

- Most often, early in the morning when the occupants of the residence are asleep and taken by surprise.
- In some cases, during the day. This can be the case when one goal of the raid is to seize digital devices while they are turned on (and therefore their **encryption (#4)** is not effective). In this case, the adversary can decide to conduct the house raid during the day because digital devices are more likely to be turned on when their users are awake, which is more likely to be during the day.

Why

An adversary can conduct a house raid to:

- Seize items to find evidence or to do **network mapping (#3)**. Commonly seized items include electronic devices, literature, materials that could be used in actions, and clothing. In some cases, the adversary seizes expensive items (e.g., computers,

4.4.3. Video

A camera found in the skylight of a public school in Berlin, Germany, in July 2011.[18]

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

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

- The living room of a target.
- The windows of a building close to the home of a target, with a line of sight on the entrance of the home.
- Close to **stash spots or safe houses (#4)** as has happened in Italy, where motion-activated cameras were installed to monitor a forest stash spot.[19]

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[7] and the "Hidden devices" topic.[8]

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

[19] 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

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.

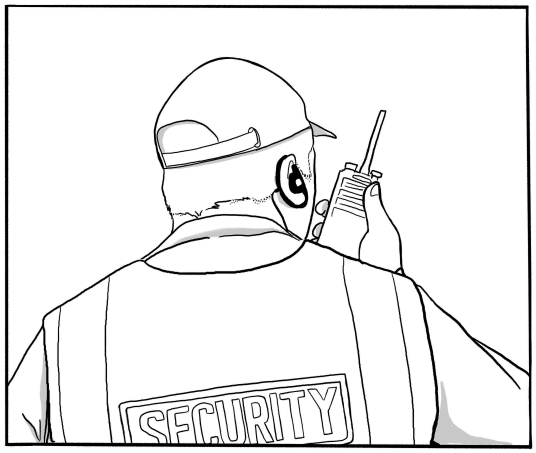
Physical intrusion detection (#4): An adversary often needs to covertly enter a space to install a covert video surveillance device in the space. You can use physical intrusion detection to detect such a covert entry.

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. 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.

4.10. Guards

Used in tactic: **Arrest**



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

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

Mitigations

Attack (#4): Before or during an action, you can incapacitate guards to prevent them from interfering with the action. For example, in their actions on logging companies machinery in so-called Chile, Mapuche people have neutralized guards by disarming them,[58] tying them up[59] or shooting at them.[60]

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

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

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

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.[57]

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.[4]

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

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.[17]

Case against Louna (#5): Cameras were installed to film the entrances of several places where people opposed to the highway project lived.[12]

December 8 case (#5): A camera was installed outside a small cabin used by some of the defendants, filming the cabin.[15] It was seemingly installed about 10 meters from the cabin, on a tree trunk.

4.5. Detection dogs

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

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

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

An odor is caused by volatile chemical compounds emitted by a substance. For example, the odor of an old book is caused by

chemical compounds released into the air by its pages, which are constantly decomposing.

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

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

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

Detecting substances

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

- At an action site or during a **house raid (p. 53)** or **covert house visit (p. 6)** to determine if a substance is present and locate it.
- During an **ID check (p. 56)** 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:

weeks apart, may produce shards that can be distinguished by analyzing their properties, including their refractive indices[55] and chemical elements.[56]
- 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,[44] 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. 23)**.

Other

Other types of trace evidence include:

- Human and animal hair. Hair can fall from a body at any time. Hair can reveal various information about its owner, including, in some cases, their **DNA (p. 25)**. See Handbook of Trace Evidence Analysis,[44] 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,[44] 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.

[55] https://en.wikipedia.org/wiki/Refractive_index
[56] https://en.wikipedia.org/wiki/Chemical_element

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,[54] section "Tool Traces" for a short discussion of tool marks.
- Color Atlas of Forensic Toolmark Identification[44] for a comprehensive overview of tool marks.

Glass

When glass breaks, it produces shards of various sizes.

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

- Two glass objects of different models, or manufactured in different factories, or manufactured in the same factory several

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

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

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

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

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

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

- The training of the dog and of its handler.
- Human activity on or near the trail.

- Wind. Air movement can displace the volatile chemical compounds that constitute a trail.
- Precipitations. Rain, snow or dew can dissolve some of the volatile chemical compounds that constitute a trail.

Scent lineups

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

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

Mitigations

Careful action planning (#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.[20]

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

- Compare two footprints to determine if they were left by the same foot.

See Examination and Interpretation of Bare Footprints in Forensic Investigations[53] for an overview of footprints.

Shoeprints

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

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

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

An adversary can:

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

See Footwear Impression Evidence: Detection, Recovery and Examination[44] for a comprehensive overview of shoeprints.

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

- 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,[44] 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. 34)**.
- On a soft surface such as sand, a foot may leave a very generic footprint that shows only a rough outline of the foot.

An adversary can:

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

Repression against Zündlumpen (#5): In some of the February 2025 raids, police used detection dogs to locate electronic devices.[21]

Bure criminal association case (#5): Detection dogs were used in one of the raids.[12]

4.6. Door knocks

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

Door knocks are when an adversary comes knocking where you live to intimidate you or get information. Door knocks aim to intimidate or create paranoia, to see who is willing to talk and possibly be recruited as an **informant (p. 61)**, 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 (p. 53)** because door knocks do not require a warrant or legal authorization.

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

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

Scintilla (#5): In May 2019, cops knocked on Boba's door under the pretext of giving a verbal notice to someone else.[22] Once inside, however, they revealed a warrant for Boba's arrest, arrested him, and searched the house.

4.7. Doxing

Used in tactic: **Deterrence**

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

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

Mitigations

Digital best practices (#4): You can follow digital best practices to make it harder for an adversary to dox you.

4.8. Evidence fabrication

Used in tactic: **Incrimination**

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

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

An adversary can use trace evidence to:

- Analyze a trace from an action site to obtain useful information. For example, they can analyze a shoeprint found at an action site to determine the size and model of the shoe that left it, and then search for people who possess shoes of that size and model.
- Link a trace from an action site to an object. For example, they can determine whether textile fibers found on a fence at an action site likely come from clothing that they seized from your home during a **house raid (p. 53)**.
- 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. 34)** and **DNA (p. 25)**, which are considered separate forensic disciplines.

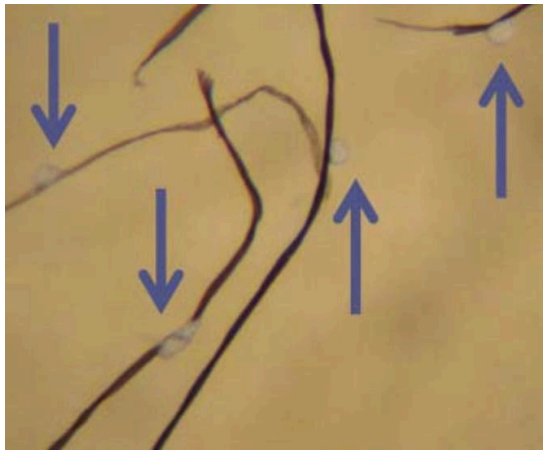
Fibers

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

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

- A worn wool sweater of an uncommon color, manufactured in an uncommon way, may leave a large amount of relatively unique fibers.

4.9.10. Trace evidence



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

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

Trace evidence can be:

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

Trace evidence can be transferred:

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

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

December 8 case (#5): Investigators mistranscribed or distorted conversations obtained through phone interception or hidden microphones to make them look suspicious.[4] 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.

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

4.9. Forensics

Used in tactic: **Incrimination**

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

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

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

4.9.1. Arson

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

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

Fire debris analysis focuses on ignitable liquid residues (ILRs) and aims to identify potential traces of accelerant and their chemical composition—these samples are often found by **dogs (p. 16)** at the scene.

Mitigations

Anonymous purchases (#4): An adversary can sometimes identify accelerants and trace them back to a gas station brand, and from

- Who is speaking on a tapped mobile phone or a recording made by a **hidden microphone (p. 9)**.
- Who called the authorities to make a bomb threat.

See also

On the topic of author identification:

- Counteracting Forensic Linguistics.[51]
- Who wrote that?[52]

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.

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.[50]

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.[30]

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.[6] 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)**.

[51] https://anonymousplanet.org/guide.html#appendix-a4-counteracting-forensic-linguistics

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

parcel bombs in an attempt to link the defendants to the attacks.[50]

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.[28] 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.[36]

4.9.9. Linguistics

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

Author identification

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

- Who wrote an anonymous action claim posted on the Internet or sent to a newspaper.
- Whether multiple anonymous action claims were likely written by the same person or group.
- Who wrote a plan describing illegal activities found during a **house raid (p. 53)**, a **covert house visit (p. 6)** or an arrest.

Voice identification

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

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

there to the identity of the person who purchased the accelerants. To mitigate this, you can purchase accelerants anonymously.

Careful action planning (#4): An adversary can tie actions together if accelerants from the same sources are used in all of them. To mitigate this, you can avoid reusing accelerants from the same source in different actions.

Repressive operations

Case against Louna (#5): A gas detector[24] was unsuccessfully used to detect traces of accelerant in the cab of the burned excavator.[12]

Traces of accelerant were collected:

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

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

Bure criminal association case (#5): Traces of accelerants were collected from items recovered after demonstrations and analyzed.[12]

4.9.2. Ballistics

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

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

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.

4.9.3. DNA

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

Collection

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

(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[44] 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.
  - 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

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

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

- Whether the baseline[49] 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

[49]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.

Analysis

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

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

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

DNA databases

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

See also

- Dna You Say? Burn Everything to Burn Longer: A Guide to Leaving No Traces[25] for a comprehensive overview of DNA forensics literature.
- The "DNA" topic.[26]

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.

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

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

DNA minimization protocols (#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 Cospito.[27]

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.[17]

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

[27] https://insuscettibiledіravvedimento.noblogs.org/post/2020/03/29/it-en-italia-su-una-sentenza-e-qualcosa-daltro-un-testo-di-marco-dal-carcere-di-alessandria

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

Factors of handwriting

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

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

Analysis

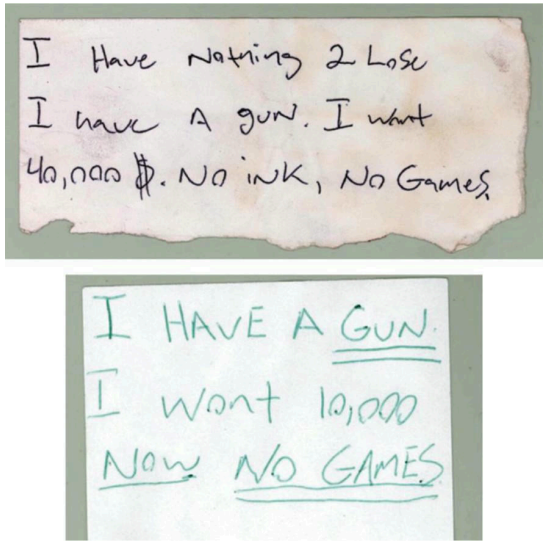
An adversary can analyze a writing sample to identify its characteristics, including:

- The layout of the text: margins, space between lines, and parallelism of lines. In the case of envelopes: the style, size, and position of the address on the envelope.

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.[46]

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.[47]

4.9.8. Handwriting analysis



Two robbery notes[48] showing similarities in the formation of the number "0".

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

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

[48]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.

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.[28]

Repression against Zündlumpen (#5): DNA traces were collected from a cigarette butt[29], zines,[30] 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.[31] Some time after the person's refusal, prison guards searched their cell and secretly replaced one comb with another, presumably to obtain the person's DNA from the hairs on the comb they took.

Repression of Lafarge factory sabotage (#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.[32] One person who refused to wear a mask had their underwear confiscated while in police custody, presumably for DNA collection.[33]

Prometeo (#5): DNA traces were used to convict the person accused of burning an ATM.[34]

Mauvaises intentions (#5): During police custody, DNA was collected from the people's clothing and from plastic cups.[35] In one case, only nine hours elapsed between the collection of a DNA trace in custody and the result of its comparison with another trace collected earlier.

The charges against one person were based on a match between their DNA and DNA collected at the scene of the attempted arson

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

[29]https://notrace.how/resources/#bavarian-christian

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

[31]https://roundrobin.info/2020/03/aggiornamenti-su-manu-stecco-juan-e-sasha

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

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

[34]https://roundrobin.info/2021/05/sentenza-beppe

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

of the electrical cabinet. DNA traces were collected both from a latex glove found nearby and from a bottle inside the cabinet—which did not catch fire because of a failed delay.

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

Case against Louna (#5): DNA traces of Louna were collected from:[12]

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

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

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

Unusable DNA traces were collected from:

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

Repression of the first Jane's Revenge arson (#5): In May 2022, DNA traces were collected from several items found by investigators at the action site, including a broken window, a glass jar, a lighter, and an intact Molotov cocktail.[36] In March 2023, police saw the person discard a bag containing a partially eaten burrito in

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

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. 14)**.
- 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[44] 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.

[44] Available on the Surveillance Archive.[45]

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

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

Analysis

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

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

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

a public trash can. DNA traces 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.[37]

Bure criminal association case (#5): DNA traces were collected from:[12]

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

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

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

Nea Filadelphia case (#5): The charges against several people were based on a match between their DNA, taken by force while in custody, and DNA traces found on "mobile objects" near the robberies.[38]

Panico (#5): DNA traces were the only evidence against one of the defendants.[39]

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

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

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

4.9.4. Digital

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

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

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

Mitigations

Avoiding self-incrimination (#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)**).

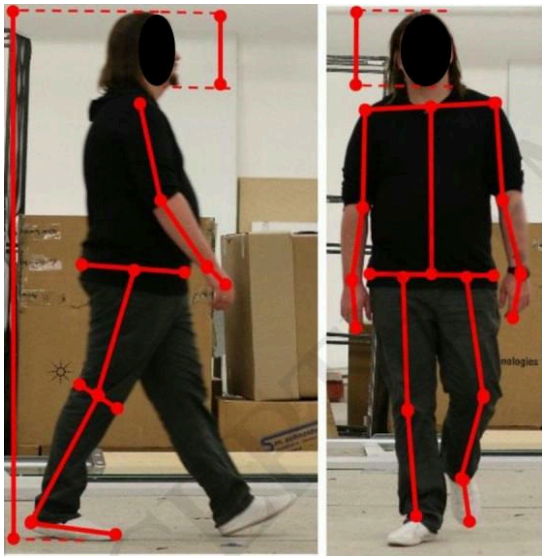
Digital best practices (#4): An adversary can use digital forensics to retrieve data from a digital device you have used. To mitigate this, you can follow digital best practices and, in particular, use

[40] https://tails.net

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.[12] The vast majority of the fingerprints collected did not match anyone. Some of the fingerprints collected matched individuals in the national fingerprint database.

4.9.7. Gait recognition



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

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

Factors of gait

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

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.[43]

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.

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

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

Tails,[40] an "amnesic" operating system designed to leave no trace on the computer it runs on.

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

- Use popular rather than custom tools.
- If you use a Virtual Private Server (VPS), **purchase it anonymously (#4)** and access it through Tails.[40]

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

Bure criminal association case (#5): Investigators analyzed storage devices by automatically extracting files containing the following keywords relevant to the investigation:[12]

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

4.9.5. Facial recognition

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

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

Modern facial recognition systems are capable of matching a face image against a large database of faces, even if the face in the image is masked, with only the eyes and eyebrows visible. Facial recognition systems coupled with **mass video surveillance (#3)** can be used to automate the tracking of individuals through a space.

See the "Facial recognition" topic.[41]

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.[28]

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

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

faces while they were in the subway, shortly before or after the action.[42]

4.9.6. 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.

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.

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