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

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

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

Threat Library

Part 2/5

Techniques G–M

November 4, 2025

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

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

Threat Library

Part 1/5: About, Tactics, Techniques A–F
Part 2/5: Techniques G–M
Part 3/5: Techniques N–T
Part 4/5: Mitigations
Part 5/5: Repressive operations, Countries, Tutorial, Contribute

Original text in English

No Trace Project

notrace.how/threat-library

Case against Ruslan Siddiqi (#5): CCTV footage from factories near the train bombing site showed someone riding a bike shortly before and after the bombing, wearing camouflage clothing and carrying a backpack.[40] This supported the theory that the person who carried out the bombing traveled by bike.

Repression of the attack on Clarín's headquarters (#5): CCTV footage from multiple cameras showed one defendant leaving the attack site, being driven away on a motorcycle for a few blocks, and boarding a bus—the defendant was identified because he used his partner's electronic bus card to board the bus.[54]

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

CCTV footage from the hospital on the night of the arson showed:

- The license plate of the car that brought Louna to the hospital.
- The faces of the other people in the car.
- One of the people in the car carrying a watering jug. Investigators would later try to find this watering jug during a house raid.

CCTV footage from cameras in several towns was used to try to reconstruct the route of the car that brought Louna to the hospital, and the route Louna took when she left the hospital.[4]

Repression of the first Jane's Revenge arson (#5): CCTV footage helped identify a vehicle driven by the person, when they were seen entering a parking lot on foot after a demonstration, and the vehicle was seen leaving the same parking lot a few minutes later.[52]

Bure criminal association case (#5): Investigators used footage from the demonstrations, recorded by surveillance cameras and police forces, to:[4]

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

The three from the park bench (#5): On the evening leading up to the arrest, one of the people—while being followed by cops—stopped at a gas station and was seen by the station's video surveillance cameras buying gas and filling a gas can.[53] The cops obtained the CCTV footage the next morning.

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

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

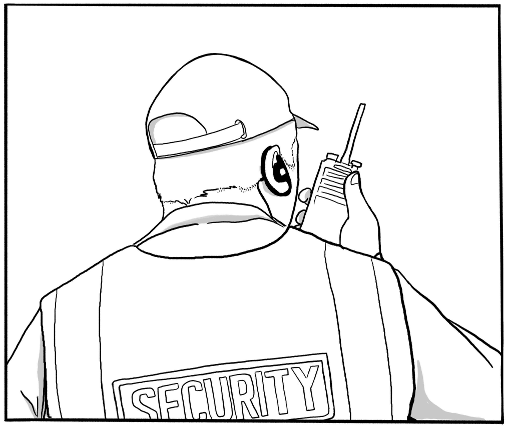
Contents

3. Techniques 3
3.10. Guards 3
3.11. House raid 4
3.12. ID checks 9
3.13. Increased police presence 10
3.14. Infiltrators 11
3.15. Informants 13
3.16. International cooperation 16
3.17. Interrogation techniques 17
3.18. Mass surveillance 19
3.18.1. Civilian snitches 19
3.18.2. Mass digital surveillance 22
3.18.3. Police files 23
3.18.4. Video surveillance 25

3. Techniques

3.10. Guards

Used in tactic: **Arrest**



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

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

Mitigations

Attack (#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,[1] tying them up[2] or shooting at them.[3]

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

transportation (buses, train stations, etc.), businesses, home surveillance systems, and municipal cameras, all within an extended perimeter of the action site.[48] In particular, footage of the interiors of buses appears to have helped identify people traveling to and from the action site.[49] Investigators also requested footage from highway toll booths, presumably to identify the occupants of known cars traveling on highways to or from the action site.

Prometeo (#5): Two of the people were allegedly seen on video surveillance leaving a store where investigators believe the envelopes used to prepare the parcel bombs were purchased.[50]

Arrest of Stecco (#5): Investigators analyzed CCTV footage from street cameras, train stations, highway toll booths, buses, and businesses to determine the movements of people under surveillance.[38]

2013 case against Mónica and Francisco (#5): Public CCTV footage was used by investigators to reconstruct the movements of Mónica and Francisco before and after the action.[8] This showed that they were near the action site shortly before the explosion of the device.

Case against Peppy and Krystal (#5): CCTV footage from a bus allowed investigators to identify the license plate of the motorcycle on which Peppy and Krystal arrived at and left the protest site.[51]

Case against Louna (#5): CCTV footage from the arson site showed two people setting fire to the excavator, and one of them burning themselves accidentally.[9]

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

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

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

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

Outdoor and device-free conversations (#4): You can conduct sensitive conversations away from surveillance cameras to prevent an adversary from recording those conversations with surveillance cameras equipped with microphones.

Reconnaissance (#4): Before an action, you can identify the location of surveillance cameras at an action site and make plans to avoid them if possible.

Transportation by bike (#4): You can use a bike instead of any other type of vehicle: compared to other vehicles, a bike is much harder to identify on CCTV footage, especially if its distinguishing features are minimized. For example, you can use a different stolen bike for each action you carry out.

Repressive operations

Case against Boris (#5): Soon after the April sabotage, investigators requested CCTV footage from businesses and municipal cameras, and lists of vehicles from automated license plate readers (ALPRs) and speed cameras, all within an extended perimeter of the sabotage site.[16]

2019-2020 case against Mónica and Francisco (#5): Public CCTV footage was extensively used by investigators to reconstruct the movements of Mónica and Francisco before and during the actions, despite the mitigations they took (taking taxis, changing clothes, wearing disguises).[37]

Repression against Zündlumpen (#5): Three weeks before an arson, a wildlife camera near the arson site captured a person walking, wearing an orange jacket.[29] After the arson, investigators obtained the camera footage and claimed that the jacket resembled one that M. had worn at some point.

Case against Revolutionära fronten (#5): CCTV footage from cameras near the scene of the Stockholm beating showed that some of the defendants were present during the beating.[4]

Repression of Lafarge factory sabotage (#5): Immediately after the action, investigators requested CCTV footage from public

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.[4]

3.11. House raid

Used in tactics: **Arrest, Incrimination**

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

When

An adversary can conduct a house raid:

- Most often, early in the morning when the occupants of the residence are asleep and taken by surprise.
- In some cases, during the day. This can be the case when one goal of the raid is to seize digital devices while they are turned on (and therefore their **encryption (#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.

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

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

[4] Private source.

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, printing equipment) with the goal of disrupting the organizational capacity of their targets.
- Arrest the occupants of the residence.
- Install **covert surveillance devices (#1)** 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

Analysis of CCTV footage can be performed:

- By humans.
- By automated systems such as automated license plate readers or **facial recognition systems (#1)**.

See also

- You Can't Catch What You Can't See: Against Video Surveillance.[44]
- The topics "Video surveillance"[45] and "Automated license plate readers".[46]

Mitigations

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

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

Attack (#4): You can disable[47] surveillance cameras.

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

- To prevent **gait recognition (#1)**, wear baggy clothing that hide your body shape, use an umbrella or other concealing objects, or drastically change your walking style by adopting a "funny walk".
- To prevent **facial recognition (#1)**, wear a mask to cover your facial features, and sunglasses or a hat with a low brim to cover your eyes.

[44] https://notrace.how/resources/#catch-see

[45] https://notrace.how/resources/#topic=video-surveillance

[46] https://notrace.how/resources/#topic=automated-license-plate-readers

[47] https://notrace.how/resources/#destroy-cameras

3.18.4. Video surveillance

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

Collection

Sources of CCTV footage include:

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

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

Storage

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

Analysis

An adversary can analyze CCTV footage:

- In real time if the cameras are integrated into a central network. Real-time analysis can take place either as part of routine surveillance or during exceptional events (e.g. demonstrations).
- Retroactively if the CCTV footage has been stored. Retroactive analysis can help identify a suspect by their **face (#1)**, **gait (#1)**, **voice (#1)**, etc.

a raid.[5]

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.[6]

Case against Revolutionära fronten (#5): During raids on the homes of some of the defendants, investigators found:[4]

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

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.[7]

2013 case against Mónica and Francisco (#5): During a raid on the home of Mónica and Francisco, investigators found:[8]

- 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.[4] They seized the car during the raid.

[5] 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

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

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

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

- 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.[9]

Case against Jeff Luers (#5): During the raid of the storage unit, investigators found:[10]

- 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:[4]

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

Operation 8 (#5): During the raids, investigators seized:[11]

[9] 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

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

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

time, and can be efficiently analyzed and cross-referenced using digital tools.

Notable examples of police files include:

- Databases of government-issued ID documents (ID cards, driving licenses, passports).
- Databases of biometric information (face photographs, fingerprints, DNA).
- Records of **ID checks (p. 9)**, fines, arrests, investigation proceedings, judicial proceedings, and convictions.

Mitigations

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

Repressive operations

Case against Boris (#5): Investigators found out that the DNA on the bottle cap belonged to Boris because his DNA was in France's national DNA database.[16]

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

2011-2013 case against Jeremy Hammond (#5): Under his online persona, Jeremy Hammond shared in online chats that he had been arrested at the 2004 Republican National Convention, had spent time in a federal prison and in a county jail, and was currently on probation.[27] Investigators were able to verify all of this using police files, which helped them to link Jeremy Hammond's online persona to his real life identity.

Bure criminal association case (#5): Investigators extensively used police files to establish links between people, including databases of driver's licenses and registered vehicles, as well as records of arrests, judicial proceedings and convictions.[4]

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

See the "Digital surveillance" topic.[42]

MITIGATIONS

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

Digital best practices (#4): You can follow digital best practices to make mass digital surveillance ineffective. For example, you can use Tor[43] to anonymize your Internet activity, and you can use security-oriented operating systems and applications that limit the data they store or collect about you.

Encryption (#4): You can encrypt "in-motion" data to prevent observers at certain points on the network from analyzing this data.

3.18.3. Police files

Police files are physical or digital records maintained by law enforcement agencies. Police files contain vast amounts of data about many things, are kept indefinitely or for long periods of

[42] https://notrace.how/resources/#topic=digital-surveillance

[43] https://torproject.org

- Electronic devices.
- Photos.
- Clothing items and camping gear, including tents, hiking boots, and tarps. The items were seized in an attempt to match them to similar items visible in footage of the "training camps."[12]
- Vehicles.
- Nine firearms.

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

Repression of the attack on Clarín's headquarters (#5): During raids, investigators found eight national identity cards and a debit card in the names of third parties.[13] In court, the cards were presented as evidence of the defendants' "strategy of concealment" and were used to justify keeping them in preventive detention.

Case against Direct Action (#5): In a raid on the house where four members of Direct Action lived, investigators found:[14]

- 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

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

[13] https://notrace.how/documentation/clarin-case-file.pdf

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

firearms and products that could be used to create explosives.[15]

3.12. ID checks

Used in tactics: **Arrest, Incrimination**

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

Complying with an ID check gives the State information about you, which can help them **map your network (#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.

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

which investigators used to create a composite sketch. Three weeks after the bombing, Ruslan Siddiqi encountered a local cop who compared him with the composite sketch and arrested him.

Case against Direct Action (#5): Several civilians helped investigators.[41] In particular:

- Journalists told investigators that they had noticed similarities between action claims published by Direct Action and articles in a local quarterly publication called Resistance.
- A hunter, presumably by chance, discovered two wooden structures where members of Direct Action stored the stolen explosives they used in bombings, and alerted the police to the discovery.[14]
- The landlords of the house where four members of Direct Action lived gave investigators the key to the house so they could enter and install hidden microphones.

3.18.2. Mass digital surveillance

The Utah Data Center (UDC), a giant data storage facility in Utah, United States, used for mass digital surveillance purposes by U.S. intelligence agencies.

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

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

a hospital. This seemingly led to Mbedzi's arrest at the hospital one hour later.

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

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

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

Belarusian anarcho-partisans (#5): While trying to cross the Belarusian-Ukrainian border, the people stopped at a shop about 10 kilometers from the border.[4] A shopkeeper called the border guards on them, which led directly to their arrest.

Case against Ruslan Siddiqi (#5): In the weeks following the train bombing, investigators interrogated many citizens in a large area surrounding the bombing site.[40]

In particular, investigators interrogated a shop clerk in a village. The clerk told investigators that, before the bombing, someone wearing a camouflage jacket and carrying a backpack had passed by the shop. The clerk provided a description of the person,

[40] https://theins.ru/en/society/280988

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.[16]

3.13. Increased police presence

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

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

Examples of increased police presence include:

- More frequent **police patrols (#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

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

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.[17]

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

3.14. Infiltrators

Used in tactic: **Incrimination**

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

Stop Hunting Sheep[18] describes five basic types of infiltrators:

1. Hang Around: Less active, attends meetings, events, collects documents, observes and listens.

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

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

Careful action planning (#4): Civilians can observe you during an action and report their observations to an adversary. To mitigate this, you can carry out actions at night or in areas with minimal foot traffic to minimize witnesses, and use a lookout to report the presence of any witnesses as soon as they are noticed. Beware of balconies and windows overlooking the action site.

Repressive operations

Fenix (#5): When Lukáš Borl was in clandestinity his photo and personal information were published on the national police website to encourage civilians to send information about him to the police.[36]

2019-2020 case against Mónica and Francisco (#5): The saleswoman of the cell phone store where Mónica bought a phone that was used as part of the 2020 action, when questioned by investigators, gave a description of a person that the investigators matched to Mónica.[37]

Arrest of Stecco (#5): After arresting Stecco, investigators showed his picture and asked questions to many people living around the arrest site, which allowed them to find the house where Stecco allegedly lived.[38]

Case against Amos Mbedzi (#5): When the explosive device exploded prematurely and severely wounded Mbedzi, a civilian was traveling by car on a nearby road.[39] The civilian stopped near the bombing site, saw another car stop, and saw Mbedzi shout "Hospital! Hospital!" and get into the other car. The civilian stayed at the site and informed the first cops who arrived that a man wounded in the explosion had gotten into a car towards

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

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

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

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

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:[15]

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

3.18. Mass surveillance

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

Mass surveillance is the large-scale surveillance of an entire or substantial portion of a population. It is the surveillance baseline of our society.

3.18.1. Civilian snitches

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

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

Mitigations

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

Attack (#4): If a civilian follows you after an action, you can scare them off with threats or pepper spray. If a civilian tries to call the police, you can destroy their phone.

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

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

See the "Infiltrators and informants" topic.[19]

Mitigations

Attack (#4): You can attack infiltrators when uncovered or years later[20] 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).

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

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

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.[21] During their infiltration, the two officers:

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

3.15. Informants

Used in tactic: **Incrimination**

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

An adversary can use different strategies to recruit an informant:

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

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

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.[16] For example, the investigators vaguely suspected that the people being interrogated had hosted Boris in April 2020 and wanted to confirm their suspicion, so they asked, "Our investigation revealed that you let [Boris] stay with you in April 2020. How long did he stay with you?"

Warsaw 3 (#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:[34]

- 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 train bombing.[35] 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

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

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

During the investigation Italian cops tried to target a person living in Germany.[31] 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 between Italian and French intelligence and police forces.[32]

Bure criminal association case (#5): Some of the people that were arrested had participated in demonstrations against the 2017 G20 summit in Hamburg, Germany.[4] Because of this, German investigators cooperated with French investigators, including by being present when the people were interrogated after their arrest.

3.17. Interrogation techniques

Used in tactic: **Incrimination**

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

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

See How the police interrogate and how to defend against it[33] (in French and German) for a comprehensive overview of police interrogation techniques.

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

[32] https://attaque.noblogs.org/post/2020/08/06/saint-etienne-arrestation-de-carla-recherchee-dans-le-cadre-de-loperation-scintilla

[33] https://notrace.how/resources/#police-interroge

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.[19]

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.

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.[22] Frank Ambrose became an informant after his arrest in 2007 (which was triggered by him throwing

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

incriminating material in a garbage can).[23] 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.[24]

2011-2013 case against Jeremy Hammond (#5): In June 2011, investigators recruited an associate of Jeremy Hammond, Sabu, as an informant.[25] 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.[26]

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:[27]

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

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

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

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

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

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

Operation 8 (#5): At least two informants were active as part of the operation.[28] In particular:

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

3.16. International cooperation

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

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

International cooperation can be used to:

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

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

Repressive operations

Repression against Zündlumpen (#5): House raids were conducted Austria, targeting people suspected of being close to N. and M.[29]

Bialystok (#5): In June 2020, people were arrested in Spain and France, thanks to cooperation between Italian, Spanish and French intelligence and police forces.[30]

[28] https://putatara.net/2015/10/05/informants

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

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