Anti-Repression Talks #1

Preparing for Physical Surveillance

Anti-Repression Talks #1: Preparing for Physical Surveillance

No Trace Project

https://notrace.how/anti-repression-talks/preparing-for-physical-surveillance.html

January 18, 2025

Contents

Announcement

The No Trace Project is launching a new initiative, the Anti-Repression Talks, to encourage discussion of surveillance and security issues within and between informal anarchist networks, on an international level. We believe that many anti-repression practices are more powerful when they are carried out across a network, rather than only by specific affinity groups.

The Anti-Repression Talks will be a series of sessions, each on a different topic, and each lasting three months. During a session, participants are encouraged to form **local study groups** with people they trust to discuss the topic of the session—we provide resources and discussion points to help kickstart those discussions. At the end of a session, an **international online chat** takes place, where participants can anonymously meet to discuss their thoughts and findings. After a session, its findings are published on the No Trace Project website, including any materials contributed by study groups and a summary of the online chat.

The first session, **Anti-Repression Talks #1**, will address the topic of **preparing for physical surveillance** and will take place in **October, November, and December 2024**, with the online chat taking place on January 4, 2025.

Physical surveillance

In the past decades, the surveillance capabilities of State actors have greatly diversified, thanks in part to new technological developments such as video surveillance, mobile phones and DNA sampling. Despite this, physical surveillance—the direct observation of people or activities for the purpose of gathering information—is still widely used by State actors, in particular in cases where other surveillance techniques are not effective.

Our Threat Library references examples of the use of physical surveillance against anarchists[1].

We believe that the State is likely to use some degree of physical surveillance in contexts where high-impact anarchist direct actions are being investigated—for example in a city where an arson recently took place and the news of the arson has been posted on anarchist websites. We also believe that in many contexts, anarchists do not sufficiently prepare for the risk of physical surveillance. Preparing for physical surveillance isn't straight-forward, it requires developing a specific skill set, but it is possible, and **it is the only thing that will help you if cops are tailing you on the way to a sensitive meeting or action**.

Local study groups

We encourage participants to form local study groups to discuss the topic of the session, from October to December 2024. During the session, if they wish to do so, study groups can send us any materials that they deem relevant to the discussion. We will add such materials to the session findings where other groups will be able to see them.

We recommend that study groups read the following resources:

- The zine Measures Against Surveillance[2] for an overview of the physical surveillance techniques used by police in urban areas, with examples from Germany.
- The book The Theory of Covert Surveillance[3] for a more comprehensive overview of the physical surveillance techniques used by private investigators (and most police agencies), with examples from the United Kingdom.
- The book Surveillance Countermeasures[4] for a comprehensive overview of physical surveillance countermeasures: surveillance detection (including counter-surveillance) and anti-surveillance. Once you understand the logic of the enemy's physical surveillance tech-

[1] https://notrace.how/threat-library/techniques/physical-surveillance/covert.html#header-used-in-repressive-operations

niques, we highly recommend this book to start learning countermeasures that you can apply in your life and projects.
- Other resources can be found on our website[5].

And we suggest the following discussion points, which we encourage study groups to supplement with their own:

- From the recommended resources, what have you found difficult to understand or apply?
- How can we support each other in developing and practicing physical surveillance countermeasures?
- If you detect physical surveillance, which activities or projects would you want to continue and which would you want to put on pause? If you stop meeting with your friends to prevent the surveillance operation from mapping your social network, how can your network help you feel less isolated?
- If you detect physical surveillance, how can you communicate this to your network in a way that doesn't alert the surveillance operation that they have been detected? How can such communication happen in a way that doesn't bolster paranoia?

International online chat

An international online chat will take place on January 4, 2025. It will be open to anyone, so we ask that you do not share any identifying information or discuss anything that you wouldn't want to see published. It will be limited to text messages (no audio or video). Discussions will be held in English, with live translation available to and from French and Spanish —please get in touch if you are able to help with live translation in these languages or others.

For instructions on how to join the chat, see here[6].

---

[2]https://notrace.how/resources/#measures-surveillance
[3]https://notrace.how/resources/#theory-covert
[4]https://notrace.how/resources/#countermeasures
[5]https://notrace.how/resources/#topic=physical-surveillance
[6]https://notrace.how/anti-repression-talks/join-the-chat.html

Findings

Summary of the online chat

The session's online chat took place on January 4, 2025 in two moments. While only a couple of people came for the first moment, the second moment was more popular with about ten people in attendance. Here's a summary of what was discussed.

Learning, and when to start to act

About the tendency to want to master operational security practices before starting to carry out actions, and how this tendency can lead to not carrying out actions at all, the following ideas were shared:

- Mastering operational security practices is not possible as there is always room for improvement.
- It's very difficult to learn everything through theory, and operational security capacity should therefore be built up by carrying out actions. It makes sense to carry out low-risk actions for at least a year before escalating to actions that can lead to a decade in prison.
- It's possible to practice with low-risk actions while taking the same security precautions one would take for high-risk actions, for example carrying out a symbolic action like putting up a poster while being very careful about cameras, DNA, etc.
- To keep things in perspective, it's important to keep in mind that the vast majority of anarchist actions are never successfully prosecuted, even though perhaps many of them display "bad" operational security practices, such as leaving DNA traces at the action site, having their personal bike recorded by cameras near the action site, and so on.
- This tendency can be more difficult to address in countries where anarchists can face life sentences for actions that would have brought shorter sentences in other countries.

Long-range microphones

About the use of long-range microphones in physical surveillance operations to listen to sensitive meetings, the following ideas were shared:

- Sensitive meetings should not generally happen inside buildings because of the risk of hidden surveillance devices being present. Loud background noise is not sufficient to mitigate recording by hidden microphones as modern technology can filter out human voices despite the presence of loud background noise.
- Sensitive meetings of two or three people happening outside can be mobile: participants can walk while talking. Because they are mobile, such meetings are more difficult to record with long-range microphones.
- Sensitive meetings of more than three people happening outside are generally stationary, as it is difficult for more than three people to talk while walking. Because they are stationary, such meetings are more at risk of being recorded by long-range microphones.
- To successfully record, long-range microphones require a clear line of sight to what they're recording.

Long-range microphones can be mitigated by choosing appropriate meeting locations. On this, the following ideas were shared:

- A location can be chosen where no one else is present in a 200 meters radius.
- A location can be chosen where cars and people coming too close to the location can be seen. This is easier in the daytime.
- A different location should be chosen for each meeting.
- A cemetery can be a good location, although a meeting in a cemetery may look conspicuous. Another, less conspicuous location can be a region of a forest with very few people, for example at the end of a hike.

Audio jammers are devices that broadcast either audible white noise, or ultrasounds, or both, in order to interfere with recordings by microphones. About the use of audio jammers during sensitive meetings to interfere

with recordings by long-range microphones, the following ideas were shared:

- If a physical surveillance operation notices that a target is using an audio jammer, it will make the target appear as very "surveillance aware." This isn't good for the target, as projecting a lack of awareness for as long as possible is their best hope of being able to detect physical surveillance. However, though the use of an audio jammer can attract unwanted attention, a recording of the meeting would presumably attract even more unwanted attention. The audio jammer can be concealed so that a surveillance team only becomes aware of its presence if it tries to record the meeting with a long-range microphone.
- To prevent an audio jammer from being physically accessed by an adversary and turned into a bug, it can be stored in a tamper-evident way, as described in an AnarSec guide[7].

Drones

About the use of drones in physical surveillance operations, the following ideas were shared:

- In some contexts, the police are acquiring more and more drones. Countering drone surveillance can feel impossible. Detecting drones can feel impossible.
- It can be difficult for drones to follow someone through a forest at night, at least if the forest has a dense canopy. Forests could be integrated in surveillance detection[8] and anti-surveillance[9] routes for this reason. In an urban environment, large buildings such as malls could be used in the same way.
- Drones can make physical surveillance much easier. For example, a drone could be used to tail someone biking through a city over several hours, requiring only a drone operator rather than a large surveillance team. But drones don't seem to be frequently used against anarchists in this way yet.

[7] https://anarsec.guide/posts/tamper

- There is a need for a good text about drones and drone countermeasures, aimed at anarchists. Such a text could give advice on the types of drones that can be expected, on detecting drones, on when a drone can see people or not depending on its capabilities (night vision, etc.) and on technical countermeasures such as jamming, and in particular how to build a cheap jammer.

About existing resources on drones, the following was shared:

- "How to Shoot Down a Drone[10]" is a short text about shooting drones with firearms, which isn't a good solution in many cases.
- "How to Evade a First World Military Thermal Drone[11]" is a video about avoiding detection by drones equipped with thermal imaging in rural environments.
- "Countermeasures for Aerial Drones[12]" is a very technical book about drones and drone countermeasures, including detection and neutralization (e.g. through jamming). It is a good book but most of the solutions it suggests are too technical or expensive for most people.

To what extent should physical surveillance mitigations be implemented

About when and to what extent mitigations against physical surveillance —such as surveillance detection and anti-surveillance—should be implemented, the following ideas were shared:

- A line has to be drawn to determine what mitigations are "good enough" in a given context. This line is often drawn based on the gut feelings, comfort levels, risk tolerance, arbitrary ideas, and schedules of the people involved, rather than on a specific methodology.
- Mitigations can be implemented depending on the sensitivity of the activity. For example, a meeting could be considered as less sensitive

[8]https://notrace.how/threat-library/mitigations/surveillance-detection.html

[9]https://notrace.how/threat-library/mitigations/anti-surveillance.html

[10]https://notrace.how/resources/#shoot-drone

[11]https://youtube.com/watch?v=Pdy0uxaJl0E

[12]http://sx3kelhcum7aaemtp27n2p3x4figvaymt2vibcabjpftxupzuu5ifzyd.onion/#countermeasures-for-aerial-drones

than preparation for an action, which could be considered as less sensitive than the action itself. Depending on the context, preparation for the action and the action itself can be equally incriminating.

- A possible methodology to decide to which extent mitigations should be implemented is to think in terms of the amount of resources that an adversary would need to maintain a surveillance operation after the target of the operation has carried out a set of maneuvers. For example, after a given set of maneuvers, the target could be confident that a 5-person surveillance team wouldn't have been able to maintain the operation without being detected, but a 10-person team might have been able to. Thus, the target can carry out a set of maneuvers that is sufficiently robust that it's unlikely an adversary would have had enough resources to have been able to maintain a surveillance operation.
- The parameters of sensitive meetings—frequency, location, number of participants—can be chosen to find a compromise between having regular enough meetings while still being able to implement sufficient mitigations before the meetings. One approach is to frequently have mobile (i.e. less vulnerable to physical surveillance) meetings with three participants or less, and, less frequently, have stationary meetings with more participants. This approach can have detrimental effects on social dynamics among the participants. Another approach is to form affinity groups of only three people, so that mobile meetings are possible with all the group members.
- The parameters of sensitive purchases in physical stores can also be chosen to find a compromise between secure purchases—purchasing items in different stores, far away from one's home, etc.—and the ability to implement sufficient mitigations before going to the stores. One approach is to dedicate one day to shopping rather than going to a lot of different stores on a lot of different days. But this approach has limits: it might require a car, limit the ability to dress differently in different stores, and so on.
- Overall, security choices can place significant limits on what a group is able to accomplish. What risks are worth taking?

Reducing the cost of security practices

Security practices are time- and resource-intensive, and can become an obstacle to making progress on actions and projects. About how to reduce the "cost", in terms of time and resources, of security practices, the following ideas were shared:

- Evaluating the likelihood and extent of surveillance is important to decide what security practices are worth implementing. For example, people who haven't been previously arrested, who aren't visible in anarchist circles, and so on, are far less likely to be under intense physical surveillance.
- Informal organization between different groups can allow reusing resources and spreading out tasks to make them more efficient. For example, in the Revolutionäre Zellen[13], the people carrying out an action weren't necessarily the same people who handled a lot of the logistics that made the action possible. To be able to depend on other groups for logistical support, it's important to establish very specific baseline security practices between the different groups. Establishing baseline practices takes time initially, as the first few projects that implement the baseline are more time-intensive, but saves time in the medium-term, as people get more comfortable with the baseline.
- Items purchased to be used in actions can be stored in the long term, and reused for several actions. This long-term storage can be compartmentalized in different locations, so that any given storage location isn't too suspicious. For example, accelerant can be stored in a friend's garage, other materials with another friend's camping gear, and clothing at yet another friend's home. Such an infrastructural approach to logistics requires trust between more people, but is more time-efficient.

[13] *No Trace Project note:* The Revolutionäre Zellen (RZ, *Revolutionary Cells*) were a German far-left militant group active from 1973 to 1995.

Teaching security

About how to teach or talk about security practices, both within and outside anarchist circles, without making highly criminalized activity appear completely inaccessible, the following ideas were shared:

- In an expanding struggle or uprising, it can be desirable that actions spread faster than the speed at which security-related skills can be developed. As an uprising expands, it may not be desirable to spread zines in the streets advising people to first spend years developing skills before even thinking about highly criminalized activity. In the context of a riot, it can make sense to spread flyers that cover the most common ways people get caught—not wearing a mask, snitching on themselves on social media—rather than less common ways such as physical surveillance or DNA traces.
- Many actions are carried out by people who feel a strong sense of urgency, and whose desire to act quickly is stronger than their motivation to act as safely as possible. There is therefore a need to spread security practices that are "good enough" for the surveillance threats that people are most likely facing. It is always a question of "good enough"—"as safely as possible" is an ideal that can never be reached.

About how to teach or talk about physical surveillance, the following excerpt from the zine PRISMA[14] was shared:

> "We are aware that dealing with this topic in detail may stir up feelings of paranoia. Those reading this text should keep in mind that everything described here is an exceptional situation, perhaps comparable to airplane travel: before takeoff, instructions are given on the use of life jackets, and everyone should be familiar with how to use them, but they are only used in very few exceptional cases. And hardly anyone will think about life jackets throughout the entire flight."

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

Preparing for physical surveillance isn't straight-forward, it requires developing a specific skill set, but it is possible, and it is the only thing that will help you if cops are tailing you on the way to a sensitive meeting or action.

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.