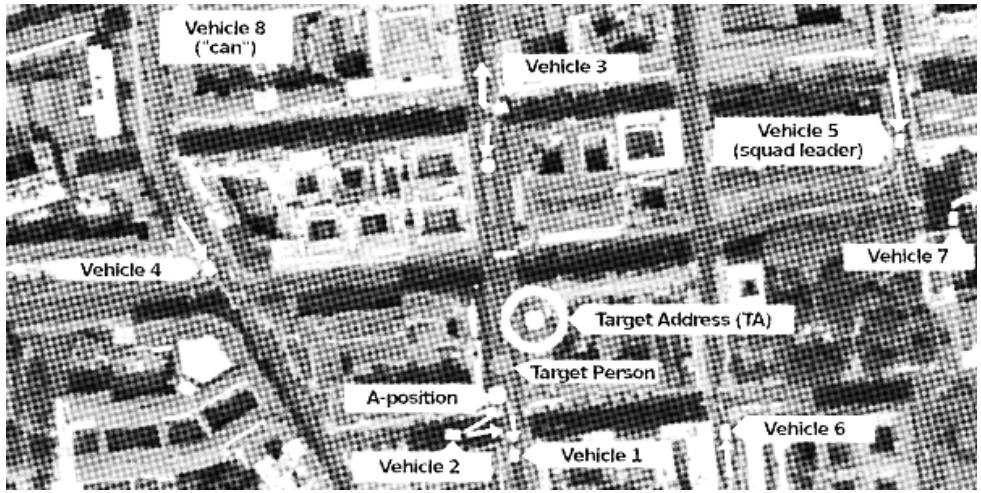
Surveillance and surveillance countermeasures: this text deals with options, risks and countermeasures. It is based on research, personal accounts and inside information, as well as a few publications on this subject.

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.

Measures Against Surveillance

Part 2/2



Measures Against Surveillance
Part 2/2

Original text in German

Maßnahmen gegen Observation

Luchs / Michael Schmidt and Andrea Müller

2011

militanz.blackblogs.org/massnahmen-gegen-observation

Translation and layout

No Trace Project

notrace.how/resources/#measures-surveillance

All in all, it is probably the most comprehensive and informative commercially available book on the subject.

8.3. Related topics

The range of texts on topics related to surveillance theory and practice is more extensive. On the one hand, there is an extensive debate on the political and scientific level with security authorities and State security policy, with a broad spectrum of radical left-wing activists from civil rights activists to constitutional lawyers and criminologists chiming in. Legal questions and aspects of technology-supported surveillance (e.g. the scandal of the "online search" or the surveillance of journalists) are discussed, sometimes through parliamentary inquiries, sometimes only indirectly, when denials or hints can be used to infer a real practice.

There is more "revelatory literature" about espionage and foreign intelligence services like the German BND than about the activities of the BfV and special police units. Such texts rather give an impression of the people who work in security authorities, of the internal structure of such authorities and of the technical and personal limits and conditions to which they are subject. They can help put into question the supposed omnipotence of the services, even if they are of little practical informational value. Other than this, these books, whether written by "experts" like Schmidt-Eenboom or by "insiders" like Juretzko, contain a lot of gossip from the office.

A very interesting publication is the "*Polizeibericht 2010*[10]" ("Police Report 2010") by Autonomen Gruppen, Berlin, which describes the structure of the Berlin police force in detail in around 100 pages. Even if the units of the Berlin police that are relevant for surveillance are only dealt with in passing, knowledge of the organizational structure and logistics of the entire authority is definitely helpful in order to be able to assess what is taking place (and what is not).

[10] https://notrace.how/documentation/polizeibericht-2010.pdf

In the book, each surveillance operation is meticulously prepared through preliminary observation, analyses, discussions, etc. In practice, the security authorities often do not have time for this. It is not uncommon for them to receive their orders on very short notice and the clerks receive more inquiries than can be processed anyways. Sometimes not even all members of a surveillance team have seen a photo of the target beforehand, let alone are familiar with the area. The briefing is held in just under half an hour in a supermarket parking lot instead of a Powerpoint presentation in the office. Usually the professional approach and the strength of the staff make up for such improvisations. The perfectionism that the book details is more relevant to "training" than as a "practical guide".

The statements on the "security behaviour of the target" are similarly impractical. In reality, only a few individuals have this "professional" behaviour and the countermeasures recommended in the book by the surveillance forces belong more to the area of counter-espionage than to everyday surveillance. The BfV occasionally takes into account possible counter-surveillance, even in the cases when their goal is intimidation. In most cases, however, this topic is only touched upon at the briefing. If the impression arises that the target would "shake", i.e. try to shake off possible pursuers, or "shine", i.e. observe possible pursuers, the surveillance is sometimes continued with a little more caution or a person experienced in surveillance admonishes their nervous young colleagues to simply calm down—in other cases the surveillance is interrupted at this point and resumed later on. Overall, the targets at this point in the book are presented as more powerful than they actually are.

Extensive discussions of conspiratorial hand signals in pursuit on foot are a holdover from earlier days when radio and telephone communications were less easily camouflaged. It can be assumed that most of the members of modern surveillance squads have just as little command of Morse Code as the list of various secret hand signals, but have reliable earphones and larynx microphones.

Contents

6. Case Study

The following case study provides an example of a surveillance operation in the arbitrarily selected Berlin city center.

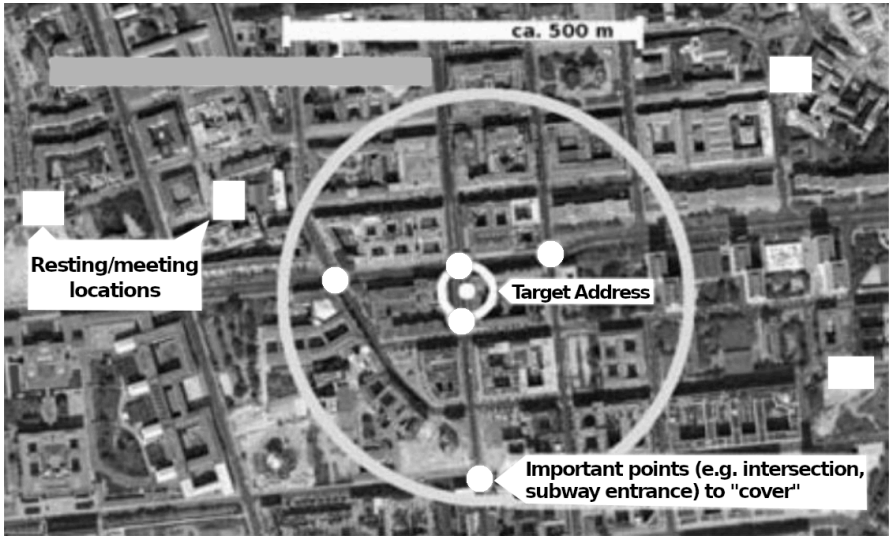


Fig. 1: Overview of the situation

work in the 1970s and 1980s. The way of thinking and the internal logics of surveillance units are represented very vividly and comprehensibly.

8.2. Glitza: "Practical Guide"

Another publication that is worth reading is the book "*Observation: Praxisleitfaden für private und behördliche Ermittlungen*" ("Surveillance: Practical Guide for Private and Official Investigations") by Klaus-Henning Glitza, Boorberg-Verlag 2009, 3rd edition[8], which should be discussed in more detail because it is the only thorough non-fiction book known from the surveillance operators' point of view. Apart from the quotes from "1000 Eyes", however, this book lacks the opposite perspective.

Over around 200 pages, the "Practical Guide" describes the procedure for surveillance for private detectives and State officers in detail. The revised edition from 2009 correctly presents surveillance as a whole. We do not recommend the first two editions, which use outdated sources.

The abundance of anecdotal information and the textbook format are problematic as they make it difficult to apply the information to an everyday practice. In addition, the treatment of all possible special individual cases obscures the view of the usual routine processes. Another weak point is the mixture of private, business and official surveillance. For example, the creative camouflage of the surveillance vehicles is very important for private detectives, since they only have a few and cannot change their license plates. Wearing disguises and changing rapidly is also more important for private detectives, especially since they may have to explain themselves to third parties, while members of the security authorities can simply pull out an ID card.

[8] *N.T.P. note*: The 4th edition is available here[9].

[9] https://notrace.how/resources/#observation-praxisleitfaden-fur-private-und-behordliche-ermittlungen

nung des Bremer LfV" (1981, "The unmasking of a surveillance apartment of the Bremen LfV"). In the following years, zines with text (excerpts) from police textbooks or leaflets that exposed civilian vehicles or undercover agents were published every now and then.

A very interesting disclosure book from circles on the left appeared in Nijmwegen in 1990: "*De Tragiek van een geheime Dienst*" extensively describes the Dutch intelligence services and police units and their methods, partly based on research and internal documents. Unfortunately, as far as is known, there is no German translation.

In 1995 the left-wing radical journals "Razz" from Hanover and "radikal" published the text "*1000 Augen*" ("1000 Eyes"), which dealt extensively with surveillance. Even after 15 years this text has lost little of its relevance. The weak point is that the surveillance apparatus is mainly described from the outside, as it is perceived by (possible) targets, while the internal processes of the security authorities are more likely to be assumed and interpreted. In order to understand surveillance and its logic, however, it makes sense, though it is not essential, to put the point of view of surveillance units and the perspective of the investigating clerk at the center of the analysis. The "1000 Eyes" text was nevertheless so convincing that it was included in the "Practical Guide" by K.H. Glitza (see below), quoted in detail as an expression "from the milieu"—in other words: the targets.

Since this text, too, could not prevent "radikal" activists from being surveilled intensively for a long time and arrested in 1995, another text followed a few years later in "radikal" which described how those affected dealt with the situation. We also recommend this.

One of the few authentic reports from real surveillance experience is the book "*Zielscheibe Mensch: Was Sie über Mobile Einsatzkommandos der Polizei niewissen wollten*" ("Target Man: What You Never Wanted to Know About Mobile Police Commandos") by Joachim Kalz from 1989, republished in 2008. Here a former criminal police officer, who was with the State security and MEK surveillance units, tells of his

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

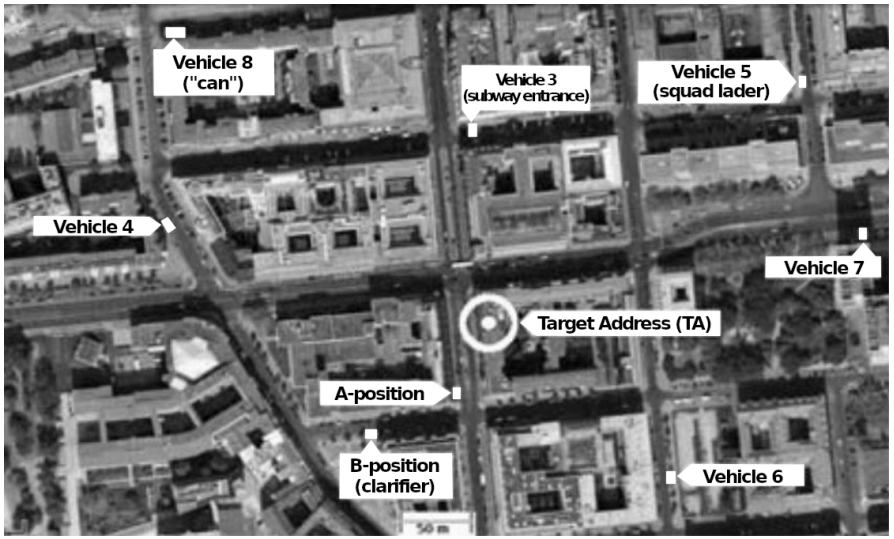


Fig. 2: Surveillance with 8 vehicles without a conspiratorial apartment

The "can" (vehicle 8) cannot be placed properly due to a lack of parking, but is on standby in the vicinity for any need. The A-position is vehicle 1, which is ready to drive away.

Around the corner, vehicle 2 is in B-position, ready to pull forward on a signal from vehicle 1 (or to drop off a "foot") if an interesting person needs to be examined more closely.

Vehicle 3 is near the subway entrance, for if the target enters the subway station directly opposite the TA (a transfer station with four directions!).

The remaining vehicles are conveniently distributed in the vicinity. In vehicle 5 (squad leader), the passenger is equipped with a laptop in order to record observations and, if necessary, to carry out online activities (e.g. internet research).

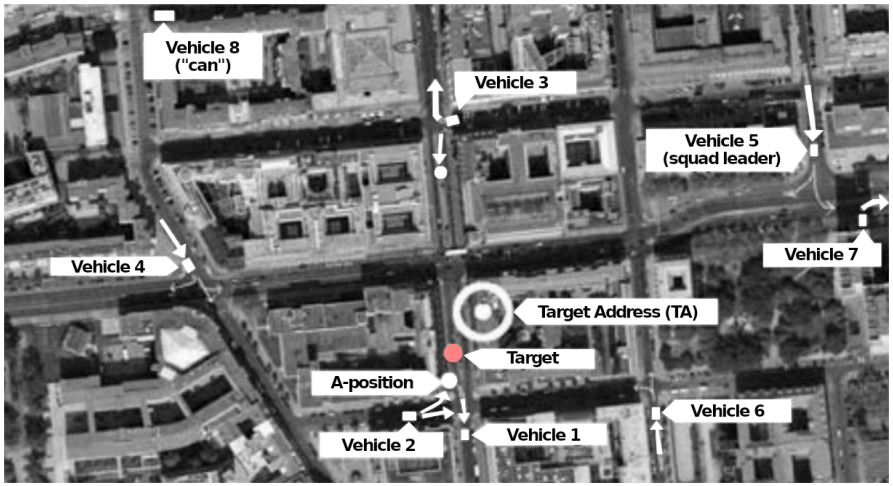


Fig. 3: The target leaves the TA and walks towards the subway station entrance

Vehicle 1 (A-position) moves away to be on the safe side in case the target passes the subway entrance.

Vehicle 2 drops off one "foot" (covered by the corner of the house) and slowly rolls towards the intersection to see what happens. The "foot" approaches the target; vehicle 2 and its foot take over the A-position.

Vehicle 3 also drops off a "foot" that goes to the subway station.

Vehicle 3 and the other vehicles start moving slowly. As long as the further movement of the target is unclear, they roll towards the four possible subway directions in order to "move forward" if necessary.

Vehicle 8 ("can") is still waiting.

8. Appendix: Literature on the Subject—a Few Tips

8.1. Surveillance in the strict sense

Apart from materials "for official use only", there are hardly any sources on the subject of surveillance in German-speaking countries.

There is a big gap between classic police films with a few main characters who have to do all the work, and agent thrillers, in which they pull out all the stops for surveillance involving all technical and personnel possibilities, including satellite use. The most informative are German TV documentaries, which often neglect the more interesting details in favor of show effects, but indirectly convey a few things about the way security authorities think and work, and US police thrillers are often relatively well researched, while German film directors rarely have expert advice.

In the written format there is also little more than the old clichés of "spooks" and crooks who "go to investigators"—almost only the legal and/or personal reasons and consequences of surveillance are discussed. The bourgeois press do not name a single source that would even begin to close this gap.

There are sporadic publications with a higher informative value in the left-wing radical milieu, but they are mostly unsystematic and oriented towards individual cases: two interesting texts were published in the early 1980s, on the one hand the Hamburg zine "*Die Praktiken von Staats und Verfassungsschutz am Beispiel Hamburg*[6]" (1980, "The Practices of State and Constitutional Protection Using the Example of Hamburg") on the other hand "*Enttarnung einer Observations-Woh-*

[6] https://notrace.how/documentation/die-praktiken-von-staats-und-verfassungsschutz-am-beispiel-hamburg.pdf

course of investigations and surveillance. This is especially true for by far the largest group of targets, namely young men between 18 and 25 years of age, whose urge to act and willingness to take risks far exceed their life experience. But even experienced people with years of practice in "conspiratorial" behaviour are, as mentioned, usually less prepared than the other side or than they themselves would believe. Even people who are in constant danger because they belong to illegal armed groups or work in espionage will try to protect themselves preventatively by constantly observing certain rules of behaviour in everyday life, but often cannot do much to counteract actual surveillance. That is also quite understandable, because who can or wants to take the time to deal intensively with surveillance and surveillance countermeasures in addition to all other everyday tasks?

And in the few cases in which the surveillance forces have to deal with "professional" protective behavior of the target, it mostly results in top-class surveillance, which is carried out with great expenditure of personnel, material and time, so that the surveillance provides the investigators with a lot of valuable insights through its intensity and duration alone, despite the advanced countermeasures[5].

We hope that this text will be help to throw a little sand into the gears of the surveillance machinery and to strengthen the awareness of those who may be affected so they can realize their own possibilities and responsibilities.

[5] *N.T.P. note:* We partially disagree with this claim. If a target implements "professional" surveillance countermeasures, they will prioritize covert countermeasures that the surveillance operators would ideally not notice. And if the operators do notice the countermeasures, it will only result in top-class surveillance *if the authorities are sufficiently motivated* and can mobilize the personnel, financial and material resources necessary to implement such top-class surveillance. Otherwise, the countermeasures will simply be effective.

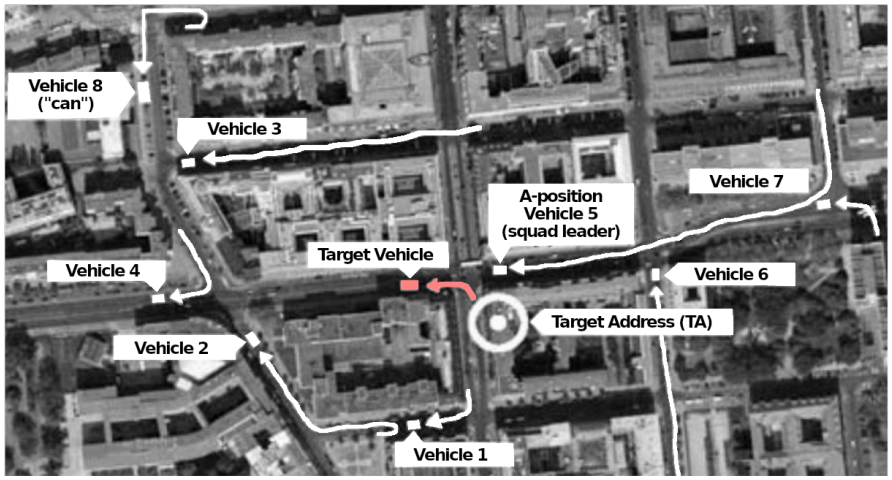


Fig. 4. The target moves away from the TA in a car

Vehicle 1 gives up the A-position and drives off to get into the rear position.

Vehicle 5 (squad leader) reacts quickly to the notification of departure and puts himself in a favorable position for "A".

Vehicle 4 positions itself in front of the target vehicle (TV) in order to be overtaken later.

The other vehicles quickly follow suit (also vehicle 8). Depending on the traffic light phase, vehicle 2 will also drive "in V" or line up behind vehicle 5 as the "B-position".

Vehicle 7 turns around in violation of traffic regulations in order to keep up.

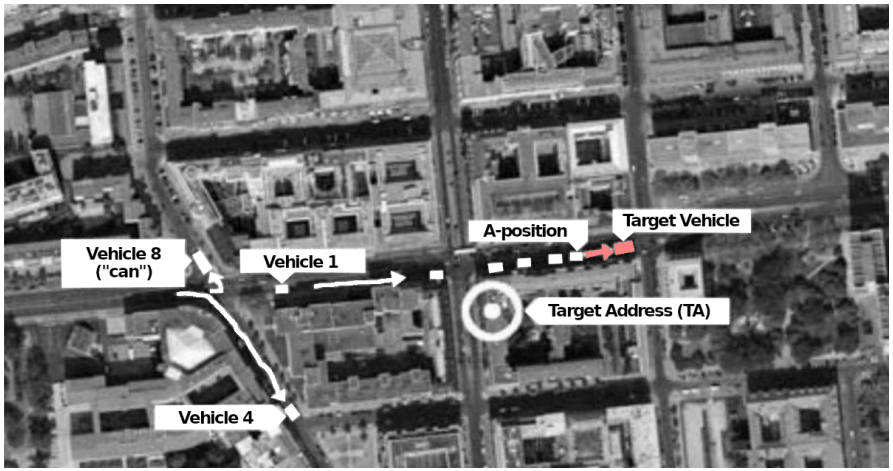


Fig. 5. Later, the target comes back from a drive in the vicinity of the TA

It is not yet clear whether the TV will drive past or park, but a return to the TA seems likely.

Most observation vehicles remain behind the TV in the flowing traffic.

Vehicle 4 pulls out and tries to find a good spot at the TA in order to be able to observe the arrival of the target.

Vehicle 1 dropped to the end of the column because the target could have noticed it earlier in the day.

Vehicle 8 ("can") speculates that the target wants to go home and drives to its previous parking space.

to change the means of transport to public transport, car or taxi without the parked bicycle being seen by the surveillance operators; or you have a safe place where you can wait a few hours for them to give up looking. Open public places are not safe. Anyone who goes through this procedure thoroughly will theoretically find that the important second part—what to do after shaking them off—is not simple at all and a spontaneous approach has little chance of success after recently identifying surveillance.

Anyone traveling by car can try to aggressively shake off their pursuers: keep a fast pace and run yellow or red traffic lights—you will break off the surveillance sooner or later and they will note that the target has behaved in a highly conspiratorial manner. As long as you could have a tracking device on the car, however, this maneuver is not enough, and the car must also be parked and left safely. At the very least, this can give you space for any urgently needed activities that you do not want to be observed by surveillance forces.

Basically, a change of means of transport is often necessary for successful "shaking", but on the other hand it is also an alarm signal for the surveillance forces, because hardly anyone normally does this. This change should therefore not be recognizable by the surveillance operators—for them the target should simply "disappear".

Furthermore, if you think you have to shake off surveillance forces for important reasons, you should also think beforehand about how you can verify that the maneuver was successful after your attempt!

7.7. Conclusion

As demonstrated, there are numerous ways to deal with suspected or detected surveillance. However, it must be emphasized once again that successful countermeasures are, in reality, the absolute exception. The vast majority of surveillance is not noticed by the targets. If it is noticed, those affected are often not able to adjust to it—they get excited or deny reality, follow incorrect advice or their own incorrect assumptions and assessments, or lack the background knowledge about the

still great uncertainties. In one case, someone on the way to a sensitive meeting spent half a day traversing the whole city, from the subway to a taxi and back to the bus, in order to remove any tails—and these tails meticulously recorded all of these movements. Of course, they became more and more excited about the meeting and the people there, who they were able to photograph and identify immediately.

In principle, at least in the city, it is possible to successfully shake off surveillance forces with much less effort. The key objective here is not simply to slip away from the A-position at a certain point and get "out of control", but rather to stay that way. This requires getting out of the area that is now being searched or surrounded by the surveillance team and getting to another place—which hopefully is not already under surveillance. If you want to shake off the forces of surveillance, you need an idea of how to get out of control and how to move afterwards. It is not enough to go up the escalator in a department store and then down again at the same time, because the surveillance operators are also at the exits. And if they cannot stand at all of them: how does the target know which ones they are not standing at? If you ride your bike into a cul-de-sac that leads to a footpath, you can ideally shake off the tailing cars—but you have to think about where you want to go afterwards. Otherwise you will unfortunately be picked back up at the subsequent intersections.

7.6.2. Tips to shake them off

A bicycle is actually the best way to shake off surveillance, because there are stretches in every city that cannot be controlled by pursuing cars or by operators jumping out quickly and pursuing on foot, and that are confusing enough that they cannot be visually followed. The area into which these routes lead must be really difficult to reach from the area that you're coming from or require a significant amount of time to get to. So you have to know in advance which way a car can drive around the obstacle and how long it will take to do so. For example, parks and areas with barriers to prevent unwanted traffic are suitable for this. When you have covered this distance, it is a good idea

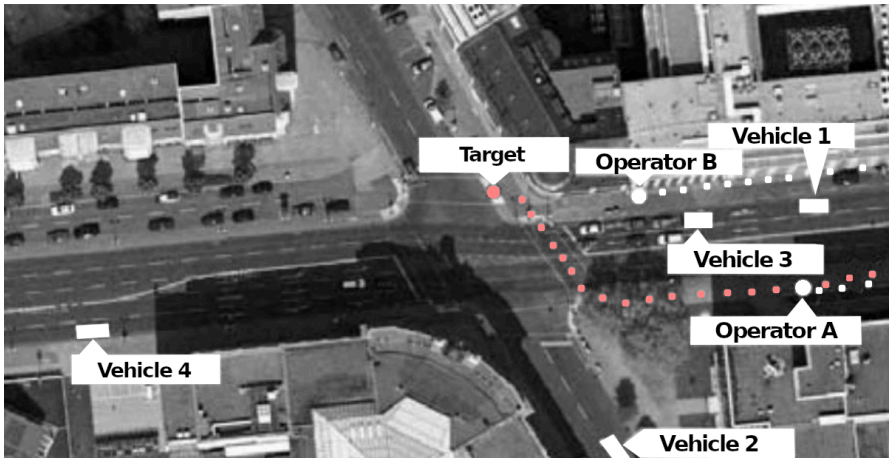


Fig. 6. The target again leaves the TA on foot

The target leaves the TA and is walking along the main road to the west (left in the picture).

Officer A follows on the same side of the main road, operator B on the opposite side. Officer A is in the A-position, but operator B also sends reports.

At the intersection, the target moves to the other side of the main road and is now at the traffic lights to go to the other side of the cross street. Officer B now takes over the A-position and closes up a bit. Officer A falls back a bit to be on the safe side, but remains on the move.

Vehicles 1 and 3 followed the target as slowly as possible, but are now driving in flowing traffic. Vehicle 2 approaches from the side street and reports a good view of the target.

Vehicle 4 is approaching from the west and also reports visibility of the target.

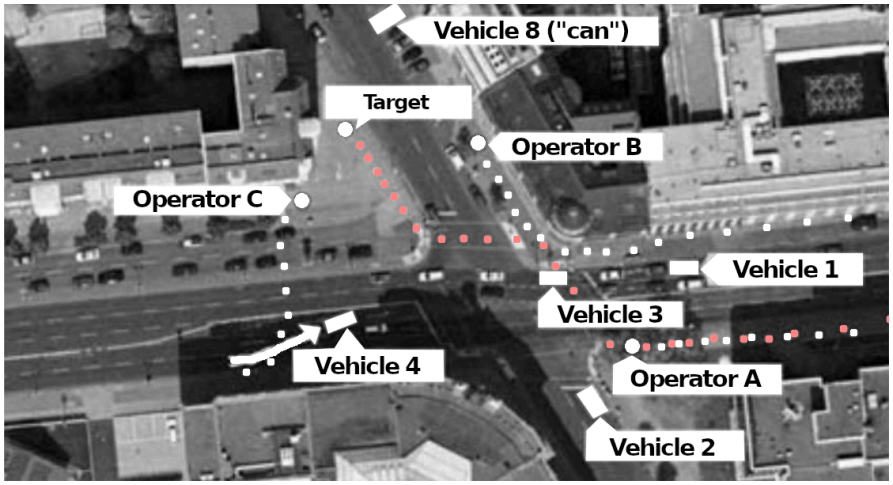


Fig. 7: The target crosses the cross street and turns to the right.

Officer B has stayed on the other side of the street and moves slightly backwards as an A-position.

Officer A is still on the main road to "cool off".

Officer C (from vehicle 4) got out with reasonably sufficient cover (by distance and the corner of a house) and hurried across the street to support operator B and relieve operator A.

Vehicle 4 pulls up to the intersection to turn into the cross street.

Vehicle 2 is still waiting at the traffic lights.

Vehicles 1 and 3 drive slowly over the intersection in flowing traffic, but as a precaution do not turn right.

Vehicle 8 ("can") has approached and parked in the cross street. When the target comes by, a good photo should be taken.

7.6.1. The difficulty in shaking them off

There are certain forms of "preventive" shaking off, which are often recommended and practiced, but are not without risk: very long journeys that sometimes take more than a day, sudden changes in mode of transport, routes through completely deserted areas, etc. This approach has several disadvantages. It is very costly because it requires precise planning, financial resources (e.g. for train rides), and a lot of time. Often the planning can only be carried out by third parties, e.g. checking unexpected transfer options for feasibility. After all, the "more is better" method is not particularly suitable for actually detecting surveillance—you simply assume there is surveillance and hope that your own countermeasures work. However, as long as you do not really know the resources and motivation of the other side, there are

---

or find you again. You should, however, try to shake off *potential* surveillance operators as part of a certain routine on your way to a "protected activity", after you have already made an effort to actively detect surveillance. Let us explain.

In everyday life, practice *passive surveillance detection* as a baseline. This involves being alert and developing an awareness for possible signs of surveillance in your environment.

On your way to a "protected activity"—such as preparing for an action, or the action itself—practice *active surveillance detection*. If you detect surveillance, don't proceed to the protected activity and have a quiet day.

If you do not detect surveillance, you should now take *anti-surveillance* measures ("shaking off" potential surveillance operators). Most anti-surveillance measures are designed to provoke one of two situations: either the surveillance operators expose themselves in a way that you can detect, or they lose you. If the operators expose themselves, you can detect them and not proceed to the protected activity. If the operators lose you, you are effectively unsurveilled during your protected activity.

To prevent a surveillance effort from re-establishing contact after the anti-surveillance measures and until the completion of your protected activity, it is critical that you completely avoid any places you regularly go, any people you regularly meet, any events that might be logical places for you to go that day (parties, demonstrations, etc.), and of course, that you don't use your regular car or bike, you don't have your phone with you, etc.

Passive surveillance detection, active surveillance detection, and anti-surveillance each have their own chapter in "*Surveillance Countermeasures: The Professional's Guide to Countering Hostile Surveillance Threats*" by Aden C. Magee.

7.5. Response of surveillance forces

All these active countermeasures can or will be noticed by the surveillance forces, which is not without consequence. Detected countermeasures affect the investigations and surveillance activities themselves. First of all, the surveillance operators feel confirmed in their assumption that the target is relevant, since from the point of view of the operators they are showing "conspiratorial behavior", though regular behavior can also be misidentified as countermeasures. So they find it all the more interesting when these measures can be identified without a doubt. This makes the continuation and extension of surveillance measures more likely. In very special exceptional cases, highly unconventional means have been used to observe particularly "sensitive" or aware targets, such as the use of private cars including the wives, children and dogs of the operators, which makes detection even more difficult.

In addition, the behaviour of the target is analyzed in connection with any observed countermeasures: have they changed their movement and communication behavior compared to before? Who did they contact shortly before and after the incident? Did they remove a tracking device, but not tell anyone or only a single trusted person, which could indicate a "sense of guilt" and possible accomplices? Are there any noticeable deviations between the target's "public" and private reactions?

7.6. Shaking off surveillance operators

It does not need to be reiterated in detail that the successful shaking off of surveillance forces is difficult and risky and should only be attempted when absolutely necessary[4].

[4] *N.T.P. note:* We want to clarify something here. As the authors say, if you know you are being followed you should not try to shake off the surveillance operators unless absolutely necessary (e.g. if you think you are going to be arrested). Instead, have a quiet day and don't do any activities that require you to be free from surveillance. It is too risky that the surveillance effort has managed to stay with you

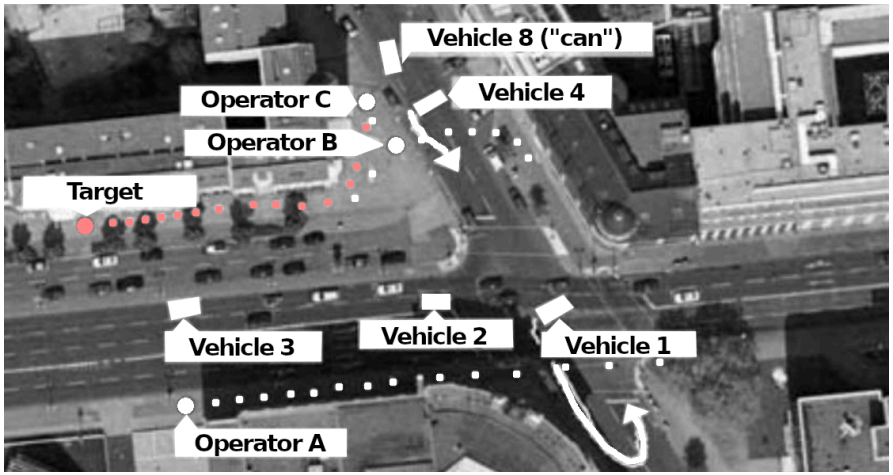


Fig. 8: The target surprisingly turns around and continues west on the main road

Officer C had to pass the target and walk a little further in order to not attract attention. He meets briefly with operator B, who has crossed the street, to discuss how to proceed.

Officer A caught up running and took over the A-position again from across the street. Vehicle 3 has the target in view and reports their movements, but must overtake them.

Vehicle 2 has now turned into the main road and is looking for an opportunity to keep inconspicuously to the right so as to not overtake the target.

Vehicle 4 turns around in the cross street; operators B and C get in if necessary.

Vehicle 8 ("can") could not take a photo and is now following the movement.

Vehicle 1 has turned left (a bit reserved as it was a former A-position at the TA) and quickly turns around in the cross street to keep up.

7. Countermeasures

7.1. General considerations

The "Countermeasures" section is about how to deal with surveillance. Possible responses in the legal or public sector would go beyond the scope of the text and should be discussed by those who are affected.

Possible ways of dealing with it all involve direct interaction with surveillance methods; in other words, people who are good at surveillance are also good at surveillance countermeasures and vice versa. This means that effective protective measures against surveillance are actually only promising if one has practical experience in this area, which only very rarely applies to the targets of surveillance. Those who can protect themselves best are either very motivated—be it for political reasons or because of their own high risk—or have good financial, technical or human resources. This applies above all to left-wing conspiratorial political groups, the leadership of organized crime, and trained agents.

Overall, however, the targets are very much at a disadvantage and usually have little hope of combatting the surveillance.

Even those who are of the opinion that they have a "nose" for it or have read the published texts on the subject mostly incorrectly assess the situation in the moment. This means, in most cases, thinking that the situation is less threatening than it is really is. Basically, general surveillance and its resulting individual risk are overestimated, whereas specific personal risk situations are underestimated. Many feel that they are being monitored by cameras in subway stations or the crackling of their phone calls, but cannot even recognize physical surveillance by the simplest police force. This can be explained psychologically, as direct personal concern is much more threatening than talking about general dangers and is therefore often suppressed or glossed over. Most of the targets assess their risk situation too positively, even

The permanently installed "combined device for voice recording and location tracking" can in principle also be found by searching. However, this requires autoshop equipment and time, just like it would to install the technology. In order to install the device, the car has to be in an autoshop for several hours, so it usually has to be "kidnapped" by surveillance forces. In practice, this is often difficult, greatly increases their risk of being discovered, and requires some creativity. Therefore this is only done in particularly important cases. Such manipulation can be made much more difficult by sensitive alarm systems, immobilizers, steering wheel claws, parking the vehicle in secure parking lots or directly in front of the front door, etc.—none of this prevents determined professionals from taking the vehicle with them, but it does make it much harder. In addition, you can think of ways of recognizing if your vehicle has been removed or moved by strangers afterwards —e.g. through hidden markings.

All areas that are in contact with the electrical system and that can be easily opened and closed again with a suitable tool must be searched. This includes above all interior lighting, the dashboard/center console, doors and side covers. Areas such as the roof and other high-up parts and the seats can only be opened relatively laboriously without leaving any traces, and are therefore unlikely to be used. It is not uncommon for the condition of screws and other locks to tell whether they have been opened in the recent past or not through the absence or presence of dirt, rust, or dust. Since the weak point of this monitoring technology is the intelligibility of conversation due to the high level of background noise, the microphones must be as close as possible to the driver's position or the presumed seated position of the main target, for example ventilation openings. It is also conceivable that microphones could be pushed into the sky light and the cables routed behind the edge seals of the door pillar. The installation of a tampered-with car radio is also conceivable.

On the other hand, the blocking of mobile communications also has a commercial interest, e.g. for sensitive hospital areas or prisons, and is offered in stores. The advantage of a disturbance of the GSM signal is that the transmission of GPS data, the tracking using the "triangulation method" and the location of the cell phone through "pings" are prevented at the same time. It is important that the range of such a blocker is large enough to interfere with the tracking device's signals, but not so great that the devices of other road users are impaired. The range of a standard mobile GSM blocker is approximately 5–10 m.

With the introduction of the digital "TETRA" radio, it is conceivable that data from tracking systems will no longer be transmitted via the GSM network, but within the "TETRA" network, making it tapproof and without additional costs for a SIM card. In the future, an optimal blockade of tracking systems would have to include a disruption of the "TETRA" band in the vicinity.

The side effect of such an approach is that it initially remains unclear to the surveillance forces why they are not receiving a signal. During data transmission, there are often disruptions and failures, so a break in the connection does not necessarily indicate active countermeasures. If contact is broken for longer than a day, at most, the surveillance forces might suspect an intentional disturbance.

7.4.2. Finding trackers

A GPS tracking device can also be actively searched for. As already described, it is mainly installed in two forms: as a battery-operated device in a cavity of the target vehicle or permanently mounted in the interior with power supply from the car's electricity. The tracker is attached without moving the target vehicle, which imposes tight physical limits—you might have to crawl under the car and force your arm into hollow spaces. During a thorough search on a car lifting platform, the chances of discovering such a tracker are very good; for example, contained in a matte black plastic case.

if they generally tend to be more worried about being surveilled. Since they have too little knowledge of the practical processes and usually no suitable personal experience, it is difficult for them to decide which of their own actions would endanger them—and others—and which would not. Letting yourself be guided by feelings of urgency can lead to significant misjudgments. It is, for example, a common tenet among police that an apartment search still makes sense even if the target has been forewarned, because they do not know the level of information that the other side possesses. Therefore, in many cases the target will overlook important details when "cleaning" their apartment.

The same applies to surveillance positions. Carelessness and paranoia are by no means mutually exclusive, but can unfortunately complement each other in the form of thoughtless actions driven by excitement and fear. The fear of being tailed does not give one any knowledge of what the surveillance operators see, know or do. Your own reactions are therefore strongly determined by your own ideas, fears and wishes about the course of the surveillance. The ostrich syndrome often plays a role: the wish that the situation may be less serious than it is. Quite a few people therefore judge their situation as being better than it actually is if they have already noticed the surveillance.

Often people are also more concerned with the possible future (not exclusively, but also legal) consequences of their actions than with their actual, real-time effects. They take care not to leave any traces behind in any action that could later be found, analyzed and used against them, but do not pay attention to their immediate surroundings and overlook the fact that they are already being surveilled.

It is difficult to give advice here. Of course, both recklessness and paranoia are inappropriate, but where is the right middle ground? Apart from practical experience—which should not be striven for—only general rules-of-thumb help here: go through the world with awareness and consciously perceive your own surroundings. Develop your own skills for critical analysis and observation, not allowing yourself to be hampered by schematic thinking and taboos. Improve your ability to think abstractly and see through the eyes of others. Stay calm and

breath easily. Do not be too hastily convinced of one point of view. Do not overestimate yourself…

Anyone who has had concrete experience with surveillance and its possible consequences will in a certain sense have learned from it, but will also find it difficult to generalize these experiences or adapt them to different situations. You remember specific incidents, faces or methods without knowing their system. The ability to learn from your experiences is therefore limited. In the few cases in which a target learns about the surveillance while it is still in progress, this is mostly due to external circumstances: mistakes by the surveillance operators, coincidences or observations by third parties. Since the operators try very hard to evade the perception of the target, they sometimes show conspicuous behavior in the outer area of the "box". Only exceptionally vigilant targets or those with a tendency to be more concerned about surveillance will recognize it for themselves.

The explanations in this section are of general use for "laypeople" as well as for "professionals" and they also show the possible weak points of the surveillance operators' own approach. It is imperative to warn against setting off with the "textbook" in your pocket and believing that surveillance can now be neutralized. It is not just the implementation of the practical tips that requires practice. The knowledge gained during this practical implementation should also be evaluated as thoroughly and objectively as possible. In order to be able to do counter-surveillance on special units, or to carry out observations yourself—even without the technical and financial means of such a unit—intensive (self-)training is required.

7.2. Detecting surveillance

There are different possibilities and situations where you can recognize surveillance yourself.

7.2.1. At the target property

Such data will not be generated if the battery is removed immediately. However, this method is not always desirable: on some cellphones, this deletes settings that have to be renewed later. Sometimes removing the battery is very time-consuming and/or not inconspicuous. In addition, when the cellphone is turned on again later, it logs into a cell tower, which in turn generates geo-location data that, in the worst case, could be monitored. A "Faraday cage" is used to temporarily shield a turned-on cellphone, which, due to the very short wavelength of the GSM frequency range, has to be very close-meshed in order not to let any signals through. Small cellphone pouches with integrated wire mesh are also available in stores, but these do not always close tightly and should be carefully checked for quality. It is important that the lid closes tightly and leaves no opening, however small. This is more difficult to implement in practice than one might think. A cellphone that is looking for network contact increases its transmission power considerably in the short term, and nowadays, even in elevators within reinforced concrete buildings, there is often no complete network shielding. In addition, it is difficult to check whether the shield is working because the cellphone has to be viewed and the shield must be opened for a short time. If you want to be sure that the shielding works reliably, you cannot avoid the need for thorough tests.

Another possible variant is the active jamming or blocking of a known or suspected tracker. To do this, there must be disruption either of the incoming signal from the GPS satellites or the data transmission from the device—usually via a GSM cellphone module—to the surveillance forces. Attacking the GPS signal is technically quite difficult, especially since GPS is a little more complex than you might imagine. Construction plans for "GPS jammers" are circulating on the Internet, but they are often incorrect or contain individual parts that are difficult to obtain. Since the GPS signal is extremely weak, the corresponding receiving antennas are very sensitive and able to obtain information from disturbed signals. In addition, there is no legal market for GPS jamming devices and with the increasing importance of satellite positioning in various areas of life, the criminalization of such jamming techniques will also tend to increase in the coming years.

day life to accommodate the unwanted companions could help. How this can look in individual cases depends on the respective personal and social circumstances and cannot be generally recommended here.

It can make sense to seek legal advice, but you should not expect too much from it. Lawyers know their way around criminal law and can tell you a lot about possible consequences such as house searches, seizures, DNA samples, identification services, criminal proceedings, etc. But they usually do not know much about surveillance. Surveillance logs do not play a prominent role in investigation files, are sometimes not included at all or only in abbreviated form, and they reveal next to nothing about the actual course of a surveillance operation. It is hardly discussed in criminal proceedings either. With regards to surveillance, legal advice can above all help to understand and better adapt to the perspective of the other side.

7.4. Protection against technical surveillance

Protection against technical monitoring devices can only be achieved within limits. The tried and true method of not having sensitive conversations in endangered rooms/vehicles and of covering the windows with curtains is still the best protection. Otherwise there are already some publications and a lively public discussion on the subject of surveillance of rooms, computers, etc., to which reference is made herein.

However, as mentioned, the audio or visual monitoring of rooms is far less common than the use of GPS trackers on vehicles and the location of cellphones via "pings", and there are defences against these methods.

7.4.1. Blocking cellphones and tracking devices

With a cellphone, of course, the battery can simply be removed, which is sometimes cumbersome, but does not harm the device. If the cellphone is turned off beforehand, it will send location data to the base station again at that moment, which can theoretically be analyzed.

The typical A-Position

A component of almost every surveillance operation is the surveillance of the place of residence—i.e. usually the house entrance of the target. There are three possibilities for this: an A-position with people, a camouflaged vehicle or the mostly video-supported surveillance from an adjacent property. These variants are not necessarily mutually exclusive. In the case of large surveillance operations in particular, both video surveillance and an A-position are used.

Surveillance forces must stay as close as possible to the target property in order to be able to reliably identify the target when entering or leaving the house and to minimize obstacles to the line of sight such as traffic, etc. On the other hand, however, they will endeavor not to be in the immediate vicinity of the target property in order to remain outside the field of vision of any surprise appearance of the possibly attentive target. Of course, they also have to adapt to existing conditions—if there is only one position directly next to the house entrance, the camouflage must be improved accordingly. A distance of approximately 30–50 m from the target property is ideal, this ensures that people can be recognized without being in their immediate field of vision. Good surveillance operators can also work with the rearview mirror.

The weak point of the A-position manned by a person is that it has to be filled over several hours if necessary. Even with frequent replacement, the unavoidable reality of the A-position is that an operator has to remain in close proximity to the target property for a long time—be it in a car, on a park bench, in a café… Whether the A-position is held alone or in pairs, at least one person has to keep the target in focus, which brings about a change in body language and significantly reduces attention for events outside of the target. The result is a tunnel vision that can be seen by outsiders. It is not "normal" for a person to just sit there for a long time and look in one direction. Every person has a reflex learned in early childhood to recognize human faces as such and to judge whether they are looking at him. It is well known that a circle with two points in the right place is sufficient to identify

an image as a "face." The arrangement of the eyes in relation to the face is subconsciously recognized in fractions of a second—if the eyes are centered on the face, we feel we are being looked at. And rightly so, because to focus your gaze you usually move your head and not just your eyes.

To alleviate these handicaps, the A-position may occasionally use their cellphone, lay a book or newspaper in front of them, or pretend to be asleep. In the car, they might put the seat as low as possible and slide down to make a less visible silhouette. With a normal cursory glance at our surroundings, we only perceive cars as "occupied" when a person's head covers the headrest or obscures the light background of the window. However, a target "only" needs to look out of the window twice every hour or to leave the house for brief errands to find out that the same occupied vehicle is unchanged or two occupied vehicles are alternating in the same place, or that a park bench diagonally opposite is permanently occupied. In order to be able to take a closer look at an occupied surveillance vehicle and its occupants inconspicuously, it is best to approach from behind at an angle in the blind spot, ideally on the sidewalk, because the blind spot of the rearview mirror is from around 5 m behind the parked vehicle up to the level of the rear side doors.

Camouflaged vehicles

If such an exposed A-position appears impossible or too dangerous, the surveillance team will use a camouflaged vehicle. All special observation units have such vehicles, it is often a minibus (such as a VW bus, Mercedes Vito, etc.) or a van (such as a Chrysler Voyager, Ford Galaxy, etc.) in which the rear windows are heavily tinted, sometimes with curtains. In daylight, the reflection of the windows makes it even more difficult to see into the interior. Tinting only works for cover if it is actually complete. As already mentioned, the background light is of decisive importance: the interior of a vehicle will be less visible to the outside viewer the less it is lit from the front, back or from the side. This complete blackout is not given to many normal civilian vehicles—they often only have individual tinted windows, or the tint

Surveillance operators view every action of the target with suspicion and endeavour to confirm their already existing suspicions. Any target who is not known to already photograph a lot will therefore immediately attract negative attention if they are seen with camera in hand. A cellphone camera is the most likely option, but this also requires some practice.

7.3.4. Personal conduct

The best and simplest reaction to detected surveillance is no reaction at all. Of course, it is advisable to refrain from certain actions during detected surveillance that could provide clues to the surveillance operators. However, this is made more difficult by the fact that in many cases the reason for the surveillance is unknown or is only suspected and the existing background knowledge of the surveillance operators can only be inferred to a very limited extent.

Normally, intensive surveillance does not last longer than two weeks, if only because of the limited resources of the other side. Since it always takes a certain amount of time until the surveillance is recognized, it can very well happen that one only experiences its final days and is amazed at its sudden end.

But that does not mean the end of the investigation. The surveillance can be resumed later, can be extended to other people in the social environment for the same matter, or it can be concentrated at specific times and special locations based on concrete evidence such as tapped phone calls.

In individual cases, above all surveillance against leftist and Islamist "terrorists", the surveillance can extend over many months, and in extreme cases even over several years. With such long periods of time, the advice "keep your head down" is hardly feasible, and the abundance of individual observations will inevitably give the surveillance operators a very comprehensive picture of the movements, contacts and social environment of the target(s). On the other hand, only a long vacation in the South Seas or a well-considered adaptation of every-

mantic partner or their parents. The more one deals with the situation, the more details become important that appeared unimportant at first —there is a reason why criminologists create an "investigation file" that often describes the most minute and apparently trivial details. For example, it is important to record precise dates and times in order to be able to meaningfully compare movements of the suspected target and the observed surveillance forces. All too often, statements like "I think it was Thursday or Friday during the day" and "It was noon and it was not on Wednesday" come into conflict, which is not very useful. The exact description of the surveillance operators is just as important. If "a black mid-range car drove behind me all the time" is sufficient the first time, it is no longer sufficient a day later when it is necessary to clarify whether the same car has attracted attention a second time: precise and accurate (!) information about the model, color and license plate are required. In practice, this is also more difficult than it sounds, but it has to be emphasized again because of its importance: cars are a central component of every surveillance activity and at the same time a good point of departure for response, as they can be identified precisely on the basis of make, model, colour and license plate and have restricted freedom of movement due to traffic regulations.

Recording observations promptly and discreetly is highly recommended, as short-term memory, especially in the span of everyday activities, often quickly erases important details.

Ideally, you would be able to photograph the surveillance operators without them knowing, but this will rarely be possible without jeopardizing your own safety. In particular, people are difficult to reliably compare based on mere descriptions, as long as they do not have any prominent characteristics, but are usually identifiable or comparable with sufficient certainty even in bad photos. However, it is practically impossible for the target to take pictures without being recognized. Even if you are of the opinion that you have recognized and gotten the surveillance operator in the "A-position" under control, you cannot be sure whether other operators have you in their field of vision.

is so weak that one can see through it from close up. Windows covered with tinting films are seen often on the road, but in most cases these stickers are faulty, there are folds, gaps, holes, air bubbles. Faulty stickers of this kind are hardly to be expected on surveillance vehicles, because, firstly, they make the vehicle more conspicuous and easier to recognize, and secondly, surveillance technicians are thorough Germans who, as a matter of principle, glue films accurately and also have the tools necessary to do so. Darkening foils can be firmly glued, but they can also be attached using static adhesion. A camouflaged surveillance vehicle will be tinted to such an extent that the interior cannot be seen from close up or from different directions. Since these vehicles are parked in normal streetscapes, but are anything but inconspicuous, they should not be located directly in front of the target property, but at the ideal distance of 30–50 m mentioned above.

Particularly well-equipped special units also use better camouflaged vehicles: vehicles with hidden cameras that transmit images to forces positioned a little further away. Identifying such vehicles is extremely difficult. Since the use of telephoto lenses is not necessary as long as the aim is to recognize a person leaving the target property and pick up physical surveillance, mini cameras with limited image resolution can be used which have lenses so small they are are barely visible, except upon very careful examination from close range, which the surveillance operators would of course notice. It could be a station wagon with a hold full of all sorts of things, with a small camera hidden somewhere; it could be a car that has a mini camera in the area of the sun visor or the rearview mirror bracket; it could be a scooter with a hidden camera in the top case. It is also possible to have a van with a completely closed cargo area, where filming can be done through the window between the cargo area and the driver's cab or through a ventilation opening. A BfV vehicle camouflaged in this way was unmasked by attentive participants on April 24, 2006 in Greifswald during the surveillance of a political meeting for the G8 summit in 2007. The vehicle had two options for video recording from the cargo area: from the front through the small window to the driver's cab, and

from the rear through a one-way mirror that was located behind a shelf full of electrician tools.

Modern vehicles of the upper middle class already have rain sensors on the interior mirror bracket as a standard, which cannot be distinguished from mini cameras. The use of mini front cameras in the same place, e.g. to detect dangerous traffic situations, will increase rapidly in the next few years and offers excellent camouflage.

From a property

Monitoring from a property, mostly from a "conspiratorial apartment" (CA), is also very difficult or impossible to detect. There are various ways of camouflaging a camera; using blinds, curtains, plants, shelves, and textiles. It is also common practice in Germany to obstruct the view of the outside of the apartment with visual obstacles of all kinds, part of the normal street scene. In addition, many more positions are possible: while there are usually only around 40 vehicle parking spaces in the ideal distance range on the street, there are several hundred windows in the same area in a normal urban street with apartment buildings. Finally, for monitoring from an apartment, you can work from greater distances of up to a few hundred meters, as long as trees etc. do not disturb the line of sight.

In most cases a CA is more likely to be recognized by spotting surveillance forces entering and leaving the property, if at all.

By recognizing a stationary A-position one has a clear indication of close-range surveillance, but still no information about who/what the target is. The surveillance can also apply to a neighboring house entrance, a neighbor or a parked vehicle or even the expected arrival of a target from a different direction. In order to gain certainty about whether you are a target, you have to move and force the operators to move with you.

other side can gain unwanted information, and you can find yourself under a dangerous impetus to act for and explain to third parties.

It makes sense to talk to a few selected people you trust and, if necessary, to maintain this group for an extended period of time. As a target, you are emotionally involved and incapable of assessing things as objectively as third parties. A thorough risk analysis includes the following points: What could be the reason for the surveillance? What could have made the target interesting to the security authorities in the recent past—their own actions, or contact with other people of interest? It should not be overlooked that the authorities are often completely wrong with their suspicions or at least draw incorrect conclusions based on faulty information, which makes it difficult to analyze their approach. What image do the investigative authorities have of the target? This image is based on their files and findings and may differ greatly from reality, as the target sees it! When did the surveillance presumably begin? What information can the surveillance forces have already gained, taking into account the assumption that telephone monitoring had already started well in advance? Where is there an objective need for immediate action, e.g. to avert harm to others? Which contact persons are possibly endangered? Which contacts with which people should be broken off, thinned out, given a cover story or, on the contrary, left unchanged? Who has the target been put on record with in recent years through joint arrests, investigations, registered addresses, etc., so that they can be considered as possibly affected?

7.3.3. (Counter-) analysis

It also makes sense to structure the known information and observations and to record them in writing, and of course keep these records safe, i.e. encrypted and/or not in the house of the target or their most important known contact persons. This is because when issuing search warrants, it is always taken into account whether there are other known places of residence or custody of the target where a search could be worthwhile, for example the home address of a ro-

easy as it sounds, because if you do not know how long the surveillance has been going on and what information the surveillance forces have, you also cannot know which behaviour they consider normal or, on the contrary, suspicious. Noticing surveillance can immediately trigger feeling threatened and a strong pressure to react in the target, which is difficult to suppress. Immediate reaction, however, may provide the operators with important information: on the one hand, how the surveillance was recognized, on the other hand, what actions, properties and people the target considers to be "relevant". An example of how the surveillance was recognized: the target receives a phone call and begins to behave conspicuously immediately afterwards—so they may have been warned by phone—so whoever they had talked to on the phone is now a "relevant" person for the operators. An example of what the target considers relevant: the target has often had contact with someone and suddenly breaks this off without any comprehensible reason, and he is now noticeably more attentive than before—this makes this "contact person" more interesting for the surveillance authority.

7.3.2. First measures

Anyone who recognizes surveillance and is not currently on their way to an illegal action can in most cases assume that an immediate arrest should not be expected, but that rather there is enough time to reflect, consult with others and draw conclusions. It is very likely that the initial spontaneous and emotional responses will have to be corrected on closer inspection and when further information is collected. It will not infrequently be the case that some reactions which seemed sensible and compelling initially were actually nonsensical or even definitively wrong.

It is therefore very important to conduct a risk assessment with a cool head, objectively and without prejudice, which one is often unable to do alone. However, that does not mean talking to as many people as possible, because this creates rumours and speculations in one's own social environment that ultimately do more harm than good. The

7.2.2. Movement

Movement by car

Driving in a car forces the surveillance operators to also use vehicles (the use of GPS tracking devices is left out here) and thus to make themselves recognizable. Movement in a car is the best way to detect surveillance without the surveillance operators noticing it. First off because, again, of the severely restricted movement possibilities for all involved, there are fewer variables and difficult-to-interpret movements that need to be taken into account. Secondly, because you enjoy a certain amount of privacy in the car. Anyone who moves on foot, on a bicycle or motorcycle is in the field of vision of the surveillance operators at all times, and often from a relatively short distance. They will notice if you look around, take notes, talk to yourself, or display unusual body language. Surveillance forces develop a feeling for "normal" body language, as they observe people throughout the day who believe they are not being observed.

The rearview mirror is a very valuable aid in the car. As a pedestrian or cyclist, in order to observe movements behind you, you have to find believable reasons to stop, to look around, to look into shop windows, etc. This can only be done a few times without attracting attention. By contrast, looking in the rearview mirror is routine in road traffic. It should, however, still be handled with care, as it can be recognizable by the operators who are behind you. Usually when you look into the rearview mirror of the car, your head involuntarily turns slightly to the top right. This movement is visible from behind and should only be made if it corresponds to the traffic situation, when changing lanes or turning. Otherwise, you should work "out of the corner of your eye", because as described above, eye movements and focusing are perceived very sensitively by attentive people. Sunglasses are also recommended because the mirror can inadvertently make eye contact with the driver in the vehicle behind it. In order to be able to recognize the faces of people in the vehicle behind you in the dark, it is best to stop at a traffic light—the brake light of your own car is usually sufficient to

illuminate the occupants in the car behind you. An indication of surveillance can be if someone is alone in the car behind you, but always speaks (lip movements!) when something happens in traffic: when the traffic light changes, the car starts moving, they turn on their blinkers, etc. Do not forget that surveillance vehicles can also drive next to and in front of you as "front row surveillance" and that the surveillance forces can choose to not drive directly behind the target vehicle, and use a random normal car in between to shield the A-position vehicle.

Should it be necessary to carry out minor detection maneuvers unobserved, it is more possible to do in the car than on foot. However, it should not be forgotten that there could be a surveillance vehicle next to you. In road traffic it is common to not pay any attention to the vehicles to your right and left, so a scrutinizing glance to the side while stopped at a traffic light, for example, could look conspicuous. In principle, there is more room for maneuvers when you are not alone in the vehicle—but the temptation to discuss the suspected surveillance also increases, although one must remember the possibility of listening devices in the vehicle.

During a test drive, routes that lead straight ahead for a long time and/or are normal routes for transit traffic or rush hour traffic should be avoided in order to exclude the possibility of a harmless car accompanying you over a long period of time. However, one should also avoid constant turning or unmotivated stopping, as it could be interpreted as attempts to "shake," which puts the operators on alert and could cause them to break off the surveillance at this point—which in turn would lead to not seeing any surveillance forces in the following period and wrongly assuming that you are not a target. Normally, the surveillance vehicle in the A-position would follow the target vehicle for a maximum of one or two turning maneuvers before being replaced. In the case of surveillance by large units with up to ten vehicles, it takes quite a while until it is the first vehicle's turn again to take up the A-position, and by then it may have changed its license plate. It is therefore an unreliable strategy to count on recognizing the same vehicle behind you twice to detect a surveillance operation.

windows, commercial use (i.e. labels with telephone number, though there have recently been rare exceptions here), unchangeable equipment such as fixed installations or extensions that hinder use for surveillance (e.g. missing seats, painted windows, advertising, permanent private design of the interior such as special seat covers, permanently attached lettering or accessories), an unkempt/dirty interior, significant damage to the interior, badly dented/dirty license plates, an expired TÜV certificate[3], conspicuous license plate combinations such as four identical numbers. Individual rare exceptions are possible, e.g. the BKA-MEK occasionally uses "sporty" vehicle models with special rims and coloured seat covers in individual cases.

Exclusion criteria for car occupants are: children and adolescents, seniors over 65 years of age, very obese people, especially overweight women, women with noticeably heavy make-up, very finely and expensively overdressed people, an appearance that is culturally very different from the German norm, e.g. beard, turban, face tattoo, heart-shaped sunglasses, purple wig.

7.3. Behaviour as a target and possible countermeasures

7.3.1. Dealing with surveillance

It is difficult for "laypeople" to develop appropriate responses and reactions to observed surveillance without the operators noticing it and being able to adapt. The classic mistake when recognizing surveillance is to try to "shake off" the operators immediately: there is a very high probability that this will not succeed, or at the very least be recognized by the operators.

The very first basic rule is therefore not to react immediately when surveillance is detected unless there is imminent danger. It's not as

[3] *N.T.P. note:* Informal name given in Germany to the certificate delivered after the periodic mandatory inspection of a vehicle.

fewer events and changing situations that need to be monitored, the easier and more reliable the subsequent evaluation will be.

The text also recommends “irregular stops at suitable places ('checkpoints'), where you stay for at least 15 to 20 minutes and observe for yourself.” If you do not already have an exceptionally good eye for surveillance operators, you will most likely not get anything during such a long stay, because the surveillance operators will line up at a safe distance in the vicinity and wait to see what happens next—at most a car will drive by now and then out of curiosity, but you should not expect the same one to appear multiple times.

7.2.5. Exclusion criteria

It is very important to distinguish features that mark vehicles, people or objects as irrelevant for surveillance. This negative catalog is neglected by most of those who deal with surveillance, but if you pay close attention it can help you to not lose track of things.

For surveillance vehicles in motion (i.e. not camouflaged video vehicles) the following applies: since they are generally relatively new, well-maintained, four-door, high-horsepower models with no particular abnormalities, various exclusion criteria can be described. Vehicles that are more than 20 years old are to be excluded. In 2011, this applies to Audi 80/100, BMW 3/5 series of the second series, Mercedes 124 series, Ford Escort/Sierra, Opel Kadett/Ascona/Rekord, VW Golf and Passat of series I and II, Trabant. This is all the more true as well-equipped surveillance units are increasingly renting vehicles, which helps their camouflage by allowing them to change cars more frequently, but makes old models even rarer. Special models such as convertibles and hardtops, pickups and two-seaters can be ruled out. Closed box vans are also not used, nor are very expensive brands like Porsche, Jaguar, Ferrari and imported brands.

Exclusion criteria for vehicle appearance include rust, old accident damage, neglected overall impression, lowered suspension, spoilers, low-profile tires, special rims, special paintwork, labels on paint or

The difficult task of memorizing multiple vehicles and comparing the traffic patterns in several places is unavoidable. This comparison takes place in two forms: specifically—based on individual cars; and generally—based on the volume of traffic. Roads with a passing lane are particularly suitable for this, but when traffic is sparse, making the numerous vehicles of the surveillance effort more noticeable. The surveillance staff may be familiar with isolated areas, e.g. low-traffic zones or dead ends, and not drive into areas with full force. If taking such a route, however, make sure to have a reason that appears logical to an outside observer: buy cigarettes at a kiosk, use a mailbox, throw something in a trash can, or, after the turning maneuver, drive a route that makes the maneuver logical, for example turn right onto a street which you could not enter from the other direction. It is important that there is no spontaneous stopping, evasive or turning maneuvers on the route leading there, which would allow the operators to wait at the roadside or to hide outside your field of vision. Highway exits that lead to intersections with different directional options are also advantageous because they force the operators to follow immediately instead of waiting on the highway shoulder to see what happens next. By stopping or turning, all operators should be made to drive past the target vehicle. Try to then answer the following questions: have I noticed these license plates or vehicles before? Do a conspicuous number of vehicles or their occupants correspond with the typical appearance of surveillance vehicles? Can I remove some or even all vehicles from the list of suspects (see “Exclusion criteria” below)? Did the traffic behind me look denser than in the following minutes on this street or just denser than usual?

As much as possible, this test drive should be carried out in areas and on routes that you know reasonably well, which also helps you avoid being distracted by difficult traffic situations. Ideally, it must be carried out more than once, because it is also conceivable that the surveillance

forces could lose the target vehicle shortly beforehand or that the surveillance was interrupted for other reasons[1].

Movement by bike

In principle, all of this can be done with a bicycle. As mentioned above, the bicycle has the significant disadvantage of not normally having a rearview mirror; in addition, observations are very difficult to write down or otherwise record without being noticed. But the bicycle is the most flexible means of transport in traffic; you can stop whenever you want, turn around wherever, ride back on the same side of the street on the sidewalk, etc. The speed and driving behavior of the surveillance operators can also be observed from a bike: if you ride in accordance with the rules and stop at red lights, you force them to overtake you or stop more frequently to mirror your slow pace, whereas biking through red traffic lights (which is widespread and therefore not necessarily noticeable) brings you closer to the average speed of car traffic and thus makes possible a more fluid observation from a car. When cycling, it is also advisable to stop at red lights, because this allows you to look around at the traffic behind you, including other cyclists—left turns using the pedestrian traffic lights are particularly useful for such observations.

Another advantage of the bicycle is the slightly raised seating position, which allows a better view of traffic than an average car.

[1] *N.T.P. note:* While this section does a good job of outlining various possible surveillance tactics and could give the reader some ideas about what to expect, it does not break down the State's tactics in a way that would help readers develop a systematic approach to detecting surveillance. The objective of the authors seems to be to illustrate how difficult it is to correctly identify surveillance, especially without alerting the enemy of your awareness. We believe that the authors exaggerate this difficulty, and that it is essential to have specific, planned-out procedures to detect surveillance. Adopting isolated maneuvers devoid of a systematic procedure, like driving down abandoned roads to see if anyone follows, is counterproductive and could lead to feeling overwhelmed and paranoid, creating a false sense of security, and showing our cards if anyone is watching. For more effective surveillance detection and anti-surveillance measures, see "*Surveillance Countermeasures: The Professional's Guide to Countering Hostile Surveillance Threats*" by Aden C. Magee.

after five minutes at the longest. Five minutes is a relatively long period of time in traffic!

If there actually was surveillance, it is very likely that it was immediately recognized at at least one of the surveillance points. If not, it helps to compare the vehicles on the list. It goes without saying that imprecise information such as "black small car, Berlin license plate" and "dark Fiat, rear with C 345" are not meaningfully comparable, so accuracy is a basic requirement for success. If uncertainties remain, it can be helpful to occupy the same observation points again the following day without the target driving the route. In this way, random observations can be checked and unjustifiably suspected vehicles can be screened out.

With such counter-surveillance, of course, conclusions can only be definitively drawn about that particular moment—the surveillance could also have coincidentally ended an hour before that day, or not started until an hour later. In this respect, only a positive finding is really meaningful and a useful starting point for further measures, e.g. searching around their house for camouflaged surveillance positions, searching the car and apartment for listening devices.

One more note: In a short text published in May 2011 from Bremen titled "*Wenn dir bei Tag und Nacht ein Schatten folgt*" ("If a shadow follows you by day and night")—which is worth reading—some tips on counter-surveillance are given which should be contradicted.

The text recommends that the selected route should contain "different traffic situations", including "for example empty streets, busy streets, a few stops on the tram, a department store or something like that", because this forces "possible surveillance operators to regroup again and again", which makes them easier to perceive. We strongly advise against such a procedure! In practice, the surveillance forces are much more experienced in rapid "regrouping" than the people doing counter-surveillance are in recognizing something like this. The more details and events that can be interpreted in different ways and have to be observed and evaluated, the more likely it is that the people doing counter-surveillance will be overwhelmed and confused. The

ily burdened with surveillance, i.e. hot spots or in streets where many possible targets such as leftists, Muslims and migrants live, in order to avoid confusion with other ongoing surveillance. It should not be a multi-lane road so that the people doing counter-surveillance do not lose track. The target drives this route punctually at the agreed time, calmly and without any actions that could arouse suspicion. Punctuality is especially important if the people doing counter-surveillance do not notice the appearance of the suspected target or if for other reasons they cannot see them directly as they drive past—they must be able to rely on the schedule to the minute!

The positions of the people doing counter-surveillance should not be too far apart, if possible, in order to ensure a quick exchange of information afterwards, so approximately 1–2 km. The people doing counter-surveillance should be at their positions a bit early in order to get an impression of the traffic there and to perceive any conspicuous vehicles that are not part of the surveillance. When the target passes the observation point, the people doing counter-surveillance note the vehicles behind the target with the time, model, color and license plate number, the most important criterion being that the license plate number is correctly read[2]. You have to consider the following options: in a classic surveillance scenario that runs according to plan, at least one vehicle will drive close behind the target, while the others will follow relatively quickly at a certain distance. In this case, after a minute or two, all surveillance vehicles have passed the surveillance point—there may be one or two stragglers who have lost touch. If, on the other hand, the A-position has lost contact with the target vehicle, one or more vehicles will follow relatively shortly after the target, but without visual contact, at a noticeably high speed. The third possibility is surveillance supported by a tracking device. In this case, the surveillance forces usually "loosely" drive on sight or leave a "long leash" and accept a brief break in visual contact. The surveillance vehicles will therefore only follow with an interval of a few seconds to a few minutes. In any case, the counter-surveillance can be ended

[2] *N.T.P. note:* A discreet or concealed video camera can help with this.

Movement on foot

Anyone who travels on foot has to struggle with the problem that it is absolutely unusual in normal pedestrian traffic to stop and look behind you. Such behavior is an immediate alarm for all surveillance operators. So you need reasons to explain the backwards glance. One possibility is to make a phone call with a cellphone, during which one can stop, walk back and forth and also look in other directions. But be careful: whether someone is just pretending to be on the phone can be checked later using telecommunications surveillance (TCS). In addition, surveillance operators know this trick because they use it all the time. Using other known means such as the reflection of a shop window or bending down to tie your shoes only allows very short snapshots and actually only make sense if you already have a concrete suspicion or a person in your sights who you want to take a closer look at. In that case, it can be even more sensible to simply slow down or stop in order to force the person to overtake you and then at least you can get a look at them more closely from behind: conspicuous behavior, nervousness, earphones, typical surveillance operator appearance? Entering a property, e.g. a shop, does not necessarily help. Firstly, you have to expect to be followed immediately, so you cannot just stand behind the window and keep an eye out because that would be noticed. Secondly, it is impossible to avoid further distractions: do I buy something, where do I turn, which products interest me, do I have to speak to salespeople, etc.—all of this steers away from the goal of recognizing the surveillance forces. Often you will not find a reason to stand still, finding that there is not much else left to do than turn around and recite "Oh, I forgot something" or "What, it's so late, I have to be quick…". Of course, this can only be done twice at most without arousing suspicion.

Those who are on foot are most likely to be able to recognize surveillance operators at night or in early morning deserted streets, or during the day in quiet areas such as side streets or parks. At night, surveillance operators have to follow relatively closely on foot so as not to lose sight of the target. During the day they are more likely to keep

their distance or even use the other side of the street from the start. If the target goes for a walk in a park and turns around to look for barking dogs, for example, they may see athletic men suddenly seek cover behind bushes instead of jogging…

Typical tell-tale mistakes made by surveillance operators are involuntary reactions to radio messages or to actions of the target. This includes, for example:

- Moving the hand towards the ear for better hearing or towards the microphone when speaking.
- A sudden change in the direction of gaze and/or movement.
- A visible discrepancy between the action and the line of sight, i.e. not concentrating on the traffic but on a distant destination when crossing a street.
- Incongruent body language like standing around casually, but at the same time appearing alert.
- Direct reaction to the target's movements, e.g. following the target with their gaze and associated head movement.
- Illogical behaviors like holding a hand in front of their mouth, suddenly stepping behind a tree, walking very quickly and then suddenly very slowly, "chance conversations" with other passers-by without a previous greeting…

By the way, some of these behaviors are also found in people with criminal intentions such as drug dealers or pickpockets. Of course, these classic mistakes are pointed out during training courses, but they still happen.

In general...

The following applies to all movement in public space: those who move "defensively" (i.e. at moderate speed and in compliance with traffic regulations) can observe more. This is especially true for bicycles and motorcycles, which require a great deal of focus on traffic to avoid accidents.

precisely and the presence of the concerned persons at the relevant location must be logical, e.g. as an appointment with a third party in a café or a shopping trip. Sometimes it can be useful for the counter-surveillance to be carried out by people who do not know the suspected target personally.

Anyone doing counter-surveillance needs nothing more than pen, paper and a good eye for observation. It is particularly beneficial if you can differentiate between car brands and models.

Under certain circumstances it can be helpful to use a different mode of transport than the target, especially if the counter-surveillance takes place in a small, clear area, since experience has shown that the concentration of the surveillance forces is influenced by the character of the target vehicle and they pay less attention to other means of transport. In general, people who drive a car pay more attention to other cars, and whoever walks looks more at pedestrians. Specifically, this means that if the target rides a bicycle, for example, the people doing counter-surveillance should not ride a bicycle during their work.

A route is established for the (suspected) target to travel in a vehicle at a designated time. As the surveillance forces will be in their cars, the target can also opt to use a bicycle. It goes without saying that the route has to fit somewhat into the typical movement pattern of the target in order not to attract attention. It does not have to be particularly long or complicated—ideally it is an everyday route that the target has already travelled. It should meet the following conditions: the route should avoid the coincidence of vehicles that happen to be driving in the same direction (so it should not be driven during rush hour and not remain within a single neighborhood), and it should pass through two clearly distinct traffic areas, such as crossing a river or a major road. It should not head for a specific destination with absolute clarity or offer opportunities for shortcuts and parallel routes in order to ensure that the surveillance vehicles really take the same route as the target and do not just go to the presumed destination or spread out along the way. Ideally, it should not take place in areas that are heav-

Clear readings can only be made under certain conditions, preferably outside the big city, where there are fewer signals. There should be no other cellphone within a radius of at least twenty meters. The monitoring device must be triggered to become active, e.g., to record sounds or movements. Then, after a certain period of time, transmission activity in the GSM area will start, which can be recorded. As long as it is not known at what intervals the transmission takes place, the test should be carried out for several hours. It should not be forgotten that a complex, permanently installed device can also be turned on and off remotely, i.e. it may be inactive at the time of the test for whatever reason.

GPS Trackers

Anyone who has already recognized surveillance can do a practical test to determine whether a GPS tracker has been planted on their own car, provided that the surveillance does not run around the clock: you wait until the surveillance operators have finished work or look for a time when they will probably not be there, for example, very early in the morning, and then drive to a completely different area where they have no reason to look for you and wait a long time there. Of course, do not take a cellphone with you. If they turn up there in the next few hours, they have targeted the car. If they do not appear, however, you are no more informed than before, because there can be a variety of reasons for this.

7.2.4. Counter-surveillance

Counter-surveillance should be organized with people who you trust. This requires at least two people who can be assumed to not be targets themselves. If they are part of the social scene of the target, however, it should be assumed that they are included as contact persons in the "photo folder" available to the surveillance forces, so they should be careful not to get into the field of view of the surveillance operators. If you cannot rule out the possibility that the people doing counter-surveillance are also targets, the whole process must be planned more

The procedure described here places high demands on memory, observation and comprehension. Accurate observation and its exact recording is of the utmost importance for both surveillance and surveillance countermeasures. Inaccurate observation, inaccurate memory and even inaccurate recording are unfortunately the norm, even for people with a lot of life experience and sensitivity to the topic. Anyone who reads police surveillance protocols may be initially surprised by the sometimes cumbersome, detailed and repetitive descriptions. However, these certainly serve their purpose of making what is observed understandable for others.

The danger that the surveillance operators will recognize or at least suspect what is going on when you engage in such maneuvers is relatively high. Independent surveillance countermeasures should therefore only be attempted if you consider the consequences of "burning" them to be calculable and not too bad. If, on the other hand, you want to be completely sure that any surveillance forces feel like they are masters of the situation and do not think they are burned, you should not try something like this, and instead seek help from other people (see "Counter-surveillance" below).

7.2.3. Technical means

Recognizing technical surveillance was already mentioned in this section, and an overview of "technical means" can be found in the "Surveillance Practices of the Security Authorities" section.

Telecommunications surveillance (TCS) cannot be easily recognized —the famous "crackling telephone line" is a thing of the past. Every now and then there are technical or administrative errors that lead to the discovery of TCS, for example it has happened that "forwarding to the police" was inadvertently listed on the phone bill of a target. In fact, there is only an indirect method of identifying TCS: anyone who has confirmed that they are the target of surveillance is certainly also the target of TCS.

Highly developed surveillance technology such as bugs and video cameras can theoretically be discovered either visually by searching or technically by using devices that emit signals. In practice, both methods require considerable effort and cannot realistically be implemented by the vast majority of those affected—let alone high-tech technology such as intercepting "compromising radiation" from computers, laser microphones on window panes, "structure-borne noise" analysis of wall and radiator vibrations, etc., which cannot be actively detected but whose risk can be accounted for.

Bug hunt

The search is further complicated when the surveillance technology is either outside of one's realm of access (as video cameras can be) or is very small and well camouflaged (as with bugs). There are a lot of hiding places in a house, especially for bugs that have an independent power supply. Outlets, light switches, telephones and other objects with direct power supply are "classic" hiding spots for bugs without their own battery. These can be checked relatively quickly, but this is where the first problems arise with modern electronic devices—the internal components are usually difficult to access and often not so precisely known that manipulated or foreign parts could be identified with certainty. It is all the more difficult with bugs with an independent power supply. People have often found small electronic devices or components that they thought were bugs, but which later turned out to be harmless. In addition, the exact aim of the TCS, when it started, and how long it will last is usually not known. Even with a very thorough search, in the end there's no way to be sure that you have checked every possible place, and to be on the safe side you should behave as if the apartment is being bugged.

It's not much better with emitted signals. Bugs which can be found with normal "frequency scanners" (and derived) devices that are widely available on the Internet are at the technical level of the 1980s. At least in large cities, there is a wide field of electromagnetic signals around the clock that cannot be easily identified, let alone evaluated in terms of content. Most are coded or encrypted in some way. In order

to be able to assess which technical standards one might be confronted with and how this can be recognized technically, expert knowledge and equipment is necessary. The technical equipment for professional bug hunting alone costs a few thousand euros and requires specialist knowledge to use it well, which is normally only available to security authorities or companies.

Cellphones

In principle, "tell-tale" signals are a possible point of defense for those affected, but only with cellphones. A manipulated cellphone or a GPS tracking device will in the vast majority of cases send signals at certain intervals over the normal GSM mobile network, and silent "pings" on a cellphone are of course also sent over this network. The good news is that these are the most common methods used in everyday surveillance.

There are various mobile radio detectors on the market, from simple key fobs for two euros to small scanners for a few hundred euros. These can be used to detect transmission activity in the dual band, i.e. the D and E networks, at close range. A cell phone in the vicinity of a maximum of approximately 1m from a loudspeaker produces interference noise when it is activated—the cheapest form of detector. However, there are numerous activities at all times in this network, the origin and occasions of which can rarely be clearly identified—they can come from your own cell phone, one in a neighboring apartment or a more distant, strong transmission source. Even if regular patterns can be traced, it cannot yet be determined with sufficient certainty whether they are automated "ping" queries or signals as part of "normal" cellular network activities. Every cellphone that is turned on regularly sends a sign of life to the base station, for example as a "Periodic Location Update" (PLU), although the intervals vary from provider to provider and are changed again and again. In 2010, the rhythm at Vodafone was one hour, at o2 was four hours and at D1-Telekom was six hours.