Measures Against Surveillance

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.

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"[22] (*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).

Measures Against Surveillance

Original text in German

Maßnahmen gegen Observation

Luchs / Michael Schmidt and Andrea Müller

2011

web.archive.org/web/20250615110730/https://militanz.blackblogs.org/massnahmen-gegen-observation

Translation and layout

No Trace Project

notrace.how/resources/#measures-surveillance

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

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,[21] 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.

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.

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

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

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

Note from the No Trace Project:

Although much of the Introduction and "Surveillance Basics" section is specific to the German context, we recommend reading both for the general concepts scattered throughout and as an example of a structural analysis. This analysis is relevant to other contexts where surveillance authorities might be organized in a similar way.

The "Countermeasures" section makes the claim that it is often impossible to detect surveillance, or only possible with the help of some friends who take counter-surveillance measures. We believe this is discouraging and simply not true: detecting surveillance is difficult but is a process that can be learned. Despite the limitations of this pessimism, and the correspondingly inadequate countermeasures presented, we believe that this publication is important for understanding how surveillance teams work.

Contents

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"[19] (*The Practices of State and Constitutional Protection Using the Example of Hamburg*, 1980) on the other hand "Enttarnung einer Observations-Wohnung des Bremer LfV" (*The unmasking of a surveillance apartment of the Bremen LfV*, 1981). 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"[20] (*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 work in the 1970s and 1980s. The way of thinking and the internal logics of surveillance units are represented very vividly and comprehensibly.

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

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

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 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 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.[18]

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.

[18] *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.

1. Preface

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. But sources are limited—neither journalists nor former members of surveillance units seem to have a particular interest in sharing information on the topic. In the media, it is mostly only the outcomes or the presence of surveillance that are mentioned, and only a few films or documentaries convey more than clichés and half-truths.

On the other hand, clandestine activities have always been captivating: spy movies and crime novels, political thrillers and police shows fill cinemas, bookstores and televisions. But how real are the depictions in "Tatort"[1] or by Bruce Willis in an action film? Is it really a single hero who uses luck, strength and technical miracles to hunt down gangsters, terrorists or corrupt politicians? Surveillance is neither the work of one or two detectives, nor wild manhunts ending in shoot-outs. In reality, there are large machines at work; teams and technical facilities where sole individuals do not play a major role.

In Berlin alone there are more than 300 bureaucrats on duty every day! Such a machine works day and night and is hardly controlled by political or "moral" authorities. Their work is often a banal, boring routine. It is not, however, without consequences. Hundreds of people, even thousands, get caught up in the machinery of State investigations and surveillance, and most of them never find out about it. Anyone who is "lucky" to have noticed their surveillance is often overwhelmed by the situation, makes mistakes or feels they are at the mercy of the surveillance authorities. For some, being surveilled even becomes a traumatic experience.

This text is intended to close information gaps. It is not a comprehensive overview of the security apparatus, but was compiled to specifically approach the topic of "surveillance". What is surveillance? Who is surveilling whom, why, and how? How can a surveillance operation be detected and how can those being targeted respond if necessary? The more general aspects that will remain relevant over time have been brought to the foreground. Of course, there are also particular details that continuously change, or which would be changed immediately in response to their publication, which is why mentioning them in a public text makes no sense.

First of all: the surveillance conditions in large cities are completely different from those in small towns or rural areas. This text is based on the situation in Berlin, which is also the surveillance capital of Germany. In principle, the big city significantly expands the scope of surveillance through special units, which can act anonymously and with more technology at their disposal. In the countryside, "social control" and open spaces set narrower boundaries for both pursuer and pursued and require different methods.

This text covers many surveillance practices, but there are certainly new techniques, special practices, and special cases that are not covered.

Considering the possible extent of surveillance can lead to paranoia… However, this text clearly has the opposite intention: to stimulate further discussion about the surveillance of society. State apparatuses already have a monstrous scope, but their potential is far from exhausted. If the political situation changes, the implications could be catastrophic.

Michael Schmidt and Andrea Müller, May 2011

[1] *No Trace Project (N.T.P.) note:* A German crime show.

2. Introduction

The police force and the Office for the Protection of the Constitution (BfV) belong to the "Authorities and Organizations with Security Tasks" (BOS). So it makes sense to mention both authorities in the same breath when it comes to surveillance. The separation between the "police" and the "intelligence service" has always been blurred and is often the subject of political and legal disputes. This so-called "mandate" of separation, which has haunted the security policy debate in this country, is less prominent in other countries. In Germany it was enforced by the Allies after 1945 to prevent a new Gestapo and to that extent, it is a unique result of a specific historical situation. Civil rights and liberal norms were less effective arguments for the necessity of maintaining this separation.

In the eyes of State security politicians and executive officers, to have an authority that both works as an intelligence service and has executive powers is so sensible and effective that it should be restored as a norm in Germany in the medium term. The role model for this is the FBI,[2] i.e. a police agency with intelligence resources rather than a regular secret service like the CIA.[3] Such a German FBI would also fit better into the post-Cold War global political landscape. Whereas up to 1989, comparably strong, highly armed State apparatuses faced off with each other, the "rogue States" of today are far weaker. Islamists or Kurdish guerrillas, let alone left-wing radical groups, have no safe haven or resources worth mentioning, and counter-espionage can only be carried out to a very limited extent. The western intelligence services and police are therefore much more confident, even arrogant, today than they were 20 years ago. These days they can reach and take out their opponents at will.

In addition, modern secret services tend to use fewer agents and less infiltration (in the technical jargon "HUMINT" for "human intelligence") and more technical surveillance methods (in the technical jargon "SIGINT" for "signal intelligence"). Possibly because one of the most important criteria for success is the head-start in information acquisition and analysis, and technical means and surveillance operations often work faster than dead drops[4] and conspiratorial meetings with informants. The job description of the secret agent, which haunts the media as the term "spook" repeated ad nauseam, has changed—there are fewer morally and ideologically motivated well-rounded specialists and more employees with niche specialized knowledge getting paid overtime.

The ideology of defending the constitution of the Federal Republic of Germany is quite similar between the police and intelligence services.

Both are only supposed to be law enforcement agencies with politically neutral officials, but they need politically educated and motivated people to fulfill their analytical tasks. For information analysis, young people are sought at universities, but in the area of information procurement, especially in the surveillance units, most employees come from the ranks of the police. Police officers are generally loyal to the State and have security clearance, and possess at least a basic knowledge of law enforcement and investigative activities, which is why they are obvious candidates for the intel-gathering departments of the intelligence services. Some police officers work for a limited time in the intel department of the Federal Office for the Protection of the Constitution (federal intelligence, referred to as the BfV) and then switch back to the police force—a welcome guarantee that they remain professionally involved and do not start disclosing inside information. Therefore, the surveillance operators of the BfV differ only insubstantially from the surveillance operators of the State Criminal Police Office. The only stupid thing is that the intel officials often only have limited political horizons and do not really understand much of what they are surveilling.

When it comes to surveillance, the different authorities act in a very similar way, because the methods of surveilling suspicious people are logically not that different. The police and the BfV differ almost only in terms of the number of personnel and the material equipment that is deployed.

[2] *N.T.P. note:* Federal Bureau of Investigation, the domestic intelligence and security service of the United States.

[3] *N.T.P. note:* Central Intelligence Agency, a foreign intelligence service of the United States.

[4] *N.T.P. note:* A dead drop or dead letter box is a method of espionage tradecraft used to pass items or information between two individuals using a secret location.

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.[17]

[17] *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 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.[a]

[a] https://notrace.how/resources/#surveillance-countermeasures

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 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

"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 tap-proof 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.

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.

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

Conclusion: the separation of police and intelligence services is (still) a sensitive topic in Germany at the political-administrative and management levels, but in practical work the borders have been blurring for many years.

2.1. Surveillance

When people think of "surveillance" today, they tend to think of more of technical things, i.e. postal and telephone monitoring, bugs and cameras, GPS or cell-phone tracking. The intelligence services are constantly developing new methods that give them an edge over opposing services, people under surveillance, and colleagues from other authorities. Most of it, however, will also be available to the police a few years later, at the latest. Isolated political stunts and lawsuits are effectively immaterial in this sense—think of the bizarre situation in which "online surveillance" was legally supposed to be available to the police, but not to the Office for the Protection of the Constitution.

Ultimately (from the authorities' perspective), there is often no way around in-person surveillance. What use is a tracking device on a car if you cannot see what the target is doing after they have parked the car? What use is telephone monitoring if the target does not speak on the phone but only at conspiratorial meetings?

Surveillance departments have long been a central component of the "operational forces" of police and intelligence services. They devour a lot of money and have considerable technical facilities. The civil servants employed by them are professionals and have been trained for this work. Some do nothing else, the surveillance of people is their everyday life, and the question of what the surveillance is actually about is secondary. They provide a lot of data—sometimes more than the authorities can analyze—but they can also become targets as, unlike the "technical means," they not only surveil, but can also be surveilled themselves. They communicate over the radio. They use vehicles that can attract attention, as can the operators themselves, which is called being "burned" in technical jargon. Their approach inevitably involves certain consistencies that the target can become aware of.

2.2. Squads and teams

A surveillance squad usually has between five and twenty members, although it is seldom possible to fill all the positions. Larger squads are difficult to coordinate and therefore rare. Several dozen surveillance teams work in Berlin every day, but not always at full capacity.

A brief explanation of terminology: in this text we use the term "squads" even though in everyday speech people use the phrase surveillance "teams." Strictly speaking, the "squad" refers to the most basic organizationally-defined unit, while "teams" are informally composed small groups within this unit. In surveillance practice, a "squad" is usually composed of several "teams".

The following information is only a snapshot, as the special departments in particular are constantly being restructured and regrouped.

Police surveillance is carried out either by the criminal police departments of the six local police departments or the FAO ("Search, Investigation, Observation") groups, the riot police, the specialist departments of the State Criminal Police (LKA) and the FAO groups located there, individual short-lived or even lengthy special commissions and "operational groups", the surveillance subdivision of the State Criminal Police (LKA 56) or, last but not least, the currently seven groups of the Mobile Operations Command (MEK) of the LKA division 6 (Operational Services), who process around 250 surveillance jobs a year.

The Berlin Office for the Protection of the Constitution (BfV) presumably has two active surveillance squads.

In addition, there are the Federal Police ("Mobile Search Unit", MFE), Customs Criminal Police Office, authorities in other federal States with guest appearances and finally the MEK of the Federal Criminal Police Office (BKA) and the surveillance department of the Federal Office for the Protection of the Constitution (BfV) with their surveillance squads. These two federal authorities are often active in Berlin with several teams at the same time.

Adding all this up, it is estimated that more than 300 officers from the "authorities and organizations with security tasks" are busy surveilling people every day in Berlin. This intensity is also due to the fact that there is an above-average number of targets there: 5 percent of the German population lives in Berlin, but it accounts for 20 percent of all political "extremists" (only right-wing extremists are probably more strongly represented elsewhere), with "organized crime" and espionage also above average.

A professional surveillance team handles 30–40 different surveillance assignments every year. The number of

people directly affected by surveillance each year is in the four-digit range in Berlin.

It should not be forgotten that surveillance activity has increased steadily over the past 40 years. The surveillance industry is booming.

Before the BKA was equipped to combat the RAF[5] in 1972, it did not have its own surveillance forces and had to borrow them from the BND (Federal Intelligence Service), which itself only had two surveillance teams. When the BfV observed RAF members Christian Klar and Adelheid Schulz during an extremely secret operation in Hamburg in 1978 and then lost sight of them, the on-site surveillance team was allegedly only eight people—a force that a local police surveillance unit could easily muster today.

The Berlin MEK was founded in 1969 as a small group of policemen who were eager to work towards de-escalating demonstrations, and had four surveillance squads in 1985. Fifteen years later there were seven, despite overall police downsizing.

Today's "surveillance density" has not always existed. On the contrary, even at the peak of the actual or supposed threat to the State at the end of the 1970s and the beginning of the 1980s, when a liberal public spoke of the "German autumn" and the "surveillance State", when protests were carried out against census and computer searches, the surveillance capacities of the security authorities were much lower than they are now.

2.3. Aim of this text

Our focus is on the surveillance methods of the true specialists, i.e. the teams from the BfV, BKA-MEK and LKA-MEK. They are all professionals, but have different material and financial resources. Federal authorities have more resources than State authorities and the BfV is less restricted by regulations and laws than the police.

Authorities below the LKA-MEK have a lower capacity for comprehensive surveillance. That sounds insignificant, but it is very important because if a surveillance operation is noticed, one of the most important questions is which authority is behind it and with how many resources available to them? From there it is possible to clarify questions such as the reason for the surveillance, its anticipated approach, possible consequences and sensible countermeasures. It is very important for those affected to be able to differentiate "worst case scenario" surveillance from less serious cases. By "less serious" we mean cases in which there are no consequences, such as imprisonment, for those directly or indirectly affected, where the intrusion into privacy remains limited, without long-term or intensive monitoring. Hypotheses and assessments play a central role in dealing with surveillance. The aim of this text is to help those affected deal with surveillance through discussing detailed questions and considering fundamental concepts.

Inevitably, reading this will teach you a lot about surveillance techniques. It can of course be assumed that the authorities are also reading along. This had to be accepted, especially because this audience already has training departments and more thorough internal textbooks than those available in stores. And, as the author of one of the few field reports aptly remarked from a surveillance operator's point of view: a tactic can be described as ideally executed if the other person, with full knowledge of the basic tactics, cannot escape its effect (quoted from "Joachim Kalz, Target Human —What you wanted to know about mobile police units", 1989).

[5] *N.T.P. note:* Red Army Faction, a West German far-left militant group founded in 1970.

"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 everyday 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. 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. 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

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 romantic 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. 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

3. Surveillance Basics

3.1. Terminology

The term "surveillance" is not as clear as it appears at first glance. From a legal point of view, "surveillance" encompasses much more than its common usage.

For the police, the Code of Criminal Procedure (StPO) and the General Security and Order Act (ASOG) form the legal basis for surveillance activities. Section 163f of the StPO permits "long-term surveillance" if the investigation is not possible or considerably more difficult by any other means. "Long-term surveillance" is usually accompanied by technical surveillance such as tapping phones, taking photos and filming outside apartments in accordance with Section 100 of the Code of Criminal Procedure. Measures under the Code of Criminal Procedure are not taken by the police at their own discretion, but are permitted to them for a certain period of time with permission from a judge. The police have two options. Either they need a general warrant, which are usually issued for three months and can be extended several times by the court, or they have a very specific time window in mind, e.g. a meeting between suspects, in which case a warrant is only requested for this date. Even if the actual surveillance only lasts two hours, it can be "long-term" in this sense. Usually, "long-term" means more than a day. The surveillance can also be resumed again and again with shorter or longer interruptions over a long period of time.

Surveillance, according to Section 100 of the Code of Criminal Procedure (§100 StPO), is usually implemented very quickly after the judicial decision. In particular, telecommunications surveillance (TCS), which includes telephone monitoring and all online activities such as email, internet, etc., can be set up without any difficulty. Most commercial providers only need a fax or, in the case of "imminent danger", a call from the investigating authority to fulfill their legal obligation to activate surveillance. Other areas of §100 StPO are tied to surveillance activities or the deployment of personnel on site, i.e. above all the use of video cameras, eavesdropping devices and GPS tracking devices and, in practice, mostly in connection with Section 163 measures.

In the case of a general warrant for three months of "long-term surveillance," it is by no means stated which measures will actually be carried out. This depends on various factors: when it appears appropriate to the investigating authorities, when resources are available, and when the necessary preparations have been completed. Sometimes surveillance is granted a permit but not carried out at all. The target would then be subject to "long-term surveillance" on paper, but would never actually be surveilled. In particular, the far greater numbers of personnel needed to commission a surveillance team has a limiting effect here—while TCS can be processed and analyzed by the investigating department itself.

The intelligence services work on different legal bases, but in principle function similarly. Active measures (beyond TCS) are regulated, for example, by the constitutional protection laws of the federal and State governments as well as in the G10 Act, which repeals the provisions of Article 10 of the Basic Law for postal and telecommunications privacy. Most of the measures for which the police need a judicial decision can be carried out by the Office for the Protection of the Constitution at their own discretion or with the consent of the respective interior ministry; authorization from a judge is needed for audio and visual monitoring only within "key private areas" i.e. an apartment. One problem for the Protection of the Constitution is the parliamentary control bodies such as the G10 commission of the Bundestag (German federal parliament) and the constitution protection committees in the federal States—not because they actually control much (they have too little insight) but because it is feared that despite the obligation to maintain secrecy, details of surveillance measures leak out.

In practice, the limitations of the intelligence services in surveillance are their own personnel, technical and financial resources.

As mentioned in the introduction, police and intelligence operations are similar. However, the Office for the Protection of the Constitution requires less bureaucratic preparatory work and has slightly better resources. Above all, they have somewhat larger teams and more quickly available technical means and data such as the

locations of cellphones or the data of targets registered with any authorities. In terms of professionalism, there has been no significant difference between the MEK police and the surveillance teams of the "operational" department at the Office for the Protection of the Constitution for years.

3.2. Other forms of surveillance

There are forms of surveillance that will feature less prominently in this text.

First, "open/blatant surveillance". It is used extremely rarely, at least much less often than is suspected in the circles of those who are potentially affected, and is almost never carried out by special units. Open surveillance is different from the personal "intimidation approach" at the beginning of demonstrations performed by State security or PMS ("politically motivated street violence" special unit at the Berlin LKA). Rather, it is carried out by several operators in order to put a target under pressure, and to instigate actions that give the operators information. For this, the operators have to reveal themselves, something that no member of a surveillance unit likes to do. In addition, the result is rather uncertain. Therefore, such "surveillance" is the absolute exception and should usually only be suspected if there's already proof of prior surveillance.

Secondly, preventive surveillance that is not directed against a specific target. During every major police operation, civil reconnaissance forces observe the environment and potential dangers of a demonstration or football game, etc., whereby individual "officially known" persons are also observed and sometimes followed for longer. Various departments cooperate here and communicate with special control centers, whose findings flow together through the management team. During large-scale operations such as May 1st in Berlin, more than 100 undercover vehicles from police departments to the riot police to the MEK can be used for surveillance. There is also preventive surveillance at police-defined "no-go-zones" where civil patrols look for indications of criminal activity such as drug trafficking. They use the General Security and Order Act (ASOG) as their legal framework and do not require a permit from a judge.

3.2.1. Non-openly investigating officers (NoeB)

This section concludes by exploring a certain grey area where police and intelligence actions meet. Special police units such as the LKA 64 (see below) have been placing comparatively high demands on the qualifications of their officers since the late 1980s: they should be familiar with the milieu of their target groups in order to be able to act inconspicuously if necessary and to quickly assess situations. As a practical exercise, this requires, for example, the occasional evening visit to trendy bars. The gap between such tactically camouflaged investigators and real "undercover investigators" (men and women with a false identity) appears here. "Non-openly investigating officers" (NoeB), occasionally also "non-openly investigating police officers" (NoeP), penetrate the milieu using the rudiments of a cover story, without consistently carrying this story forward. Such a procedure protects against exposure by suspicious opponents and at the same time circumvents the strict legal requirements for the use of an undercover. In 1994, two such NoeB of the MEK were exposed in the Berlin left milieu, who had covered each other and had repeatedly brought colleagues with them as "friends" to smuggle them into the milieu, all of whom had to be withdrawn after the exposure to be on the safe side. After that, the Berlin MEK became a little more cautious with such operations and increasingly relied on more offensive reconnaissance concepts such as the PMS, but this does not mean that there are no more NoeB.

With each of these police procedures, findings arise, including incidental ones, which are recorded in notes for the general picture of the situation. The political departments of the LKA and BKA keep internal files in which they update developments and findings on persons and groups who are not (yet) targets of an investigation. These "findings" can condense into thesis papers or even public prosecutor's "structural proceedings". For example, at the BKA, files have been kept for many years on the structure and alleged members of the left-wing underground magazine "radikal" without an official investigation.

In addition to the clearly-defined legal forms of surveillance described above, there is a diffuse area in which surveillance knowledge of all kinds is used by the police, but without qualified analysis apparatus such as an intelligence service. The collected findings are therefore not processed systematically, but remain in a

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,[16] 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 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.

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

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 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

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 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 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 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

department or in the memory of veteran officials for possible later use. If another department takes on a similar case, they may conduct the same investigation again. You could say that the police know more than what is legally authorized—but they themselves do not know exactly how much they know.

3.3. The various authorities

3.3.1. Police

The police are divided into the preventive police and the criminal police. Departments of the preventive police are only rarely involved in surveillance, and if so, mostly within the framework of the ASOG, e.g. as undercover scouts for the riot police during demonstrations. Individual members of the preventive police are, however, active in special units that formally belonged to the criminal police, such as the PMS. Surveillance is, however, typically carried out by the criminal police. This is divided into local sections and the State Criminal Police Office, which has investigative departments for certain offenses as well as special units.

At the lower end of the surveillance scale are the criminal police of the local police headquarters and smaller FAO units from various departments, including the riot police. Often only two or three vehicles are available to them, with which some officers carry out surveillance that cannot meet textbook requirements due to insufficient resources. The representations of surveillance in the media almost never go beyond this lowest level. Occasionally such forces work together in larger cases.

At the LKA there is more funding available for wanted persons or for independent LKA investigations such as narcotics and organized crime. In such cases 4–5 vehicles with 6–8 operators are normal. Five cars may not sound like a lot, but they are a difficult number to manage on the road! The same applies to the surveillance unit of the LKA 56 (State security), which is more likely to face the problem of its targets expecting police surveillance than other departments, thus requiring greater effort. LKA 56 has a total of around 40 vehicles and can easily deploy eight vehicles for larger surveillance operations.

3.3.2. Mobile Operations Command (MEK)

The upper end of the police scale is made up of the large special units, which in Berlin are grouped under LKA 6 "Operative Services": Mobile Operations Command (MEK), LKA 62, Special Operations Command (SEK) and Sniper Squad (PSK-LKA 63) as well as the LKA 64 combined reconnaissance groups (PMS and "Covert reconnaissance"). LKA 64 performs the tasks of "preventive surveillance" described above in the division of labor: PMS operates more or less openly and at the edge of the action, even if mostly in civilian clothes; whereas their colleagues from "Covert reconnaissance" operate well-camouflaged from inside demonstrations and from older, more inconspicuous vehicles. LKA 64 does not play a major role for surveillance in the narrower sense, but in the case of surveillance with a political element, competent officials from this department are occasionally involved. The SEK/PSK is only involved in "long-term surveillance" in exceptional cases, especially for the purpose of arrests.

In the area of surveillance, the "Covert reconnaissance" groups form the core of the MEK. There are currently seven "Mobile Task Forces" of the MEK with around 15 officers each, totalling around 100, who have a fleet of more than 80 vehicles at their disposal, plus a group for technical support and surveillance training.

Surveillance by the MEK generally has a force of approximately 6 and a maximum of 12 vehicles.

It should also be noted with regard to the LKA that there are regroupings every couple of years, especially in the area of special units, meaning the information given here may need to be checked to ensure that it is up to date. The Berlin MEK was originally founded in 1969 as an "intelligent" police department, whose officers should be able to debate with protesting students, similar to what is used today to try to pacify May Day demonstrations. But as early as 1971, the qualified officers were used for State security surveillance. Since then, this unit has grown with each regrouping.

In Berlin there are a total of around 2,300 police vehicles, of which around 200 are "camouflaged" surveillance vehicles with changing license plates and around 550 other "neutral" vehicles for civil patrols. The latter are usually only involved in smaller local surveillance.

3.3.3. Protection of the constitution (BfV) and federal authorities

The Federal Criminal Police Office (BKA) has its own MEK, which can be compared to the LKA-MEK in terms of size and equipment and is located, along with

several task forces, in the "Central Services" department (ZD 35) in Meckenheim near Bonn. Up to 15 vehicles are used for surveillance.

The Federal Police with its "Mobile Investigation Unit" (MFE) and the Customs Investigation Office have their own operational departments with limited capacities, which carry out surveillance in their areas of responsibility and support other criminal police.

For the police as a whole, it is customary to man surveillance vehicles with two officers.

Overall, the Federal Office for the Protection of the Constitution (BfV) is a much smaller apparatus than the police, although its surveillance departments as a sub-group of the "operational" area are relatively large in relation to the entire authority. The Berlin State Office for the Protection of the Constitution has a staff of around 180 civil servants, of which around 50 can be assigned to the operational area. During surveillance, 10 to a maximum of 20 vehicles can be expected.

The BfV, headquartered in Cologne, has several surveillance teams of 15–20 operators each. Here too, 10 to a maximum of 20 vehicles are used for surveillance. Contrary to the publicly maintained image of a "desk authority" that primarily analyzes sources and information from the State offices, the BfV is highly active in surveillance operations, even if the "analysis" department is significantly larger in relation to the "operational" department than at the State offices.

Surveillance vehicles for the BfV are usually manned by only one person.

Surveillance squads of the Protection of the Constitution are recruited predominantly from the middle service ("masters") of the police, especially from the riot police and the federal police. The salary level of the surveillance officers is in the border area between middle service and upper service, grades A7–A10, which makes the job financially unattractive for highly qualified officers despite the security clearance and training, not to mention the irregular working hours. Incidentally, in 2010 a court decision in Rhineland-Palatinate established that an officer for the BfV is entitled to a lower hazard allowance than an MEK police officer, since he does not have to make arrests.

Well-equipped special units, i.e. essentially those of the federal authorities and MEKs, try to achieve a ratio of around 1:1 between surveillance personnel and number of vehicles.

3.4. Differences between intelligence and police surveillance

Differences between intelligence and police surveillance are less noticeable in their processes than in their consequences. Intelligence service surveillance usually operates with more staff, with much more video surveillance from rented locations or camouflaged vehicles, and accompanying telecommunications surveillance (TCS) operations.

The main differences lie in the interests behind the investigations and the political and criminal dimensions of the cases that are being dealt with. Therefore, BKA surveillance often contains aspects of both types of authorities, since the BKA is both a police force and a political authority.

3.4.1. Police surveillance

The investigative interest of an authority is influenced by various factors: in addition to the immediate interests of the department responsible for the investigation, there are macro-structural influences within the authority as well as the influence of judicial authorities and interior ministries. The "political level" is probably anathema to most officials, but it cannot simply be ignored in investigations under the "terrorism" umbrella or investigations with international implications, e.g. organized crime, espionage, drug smuggling. Political interests do not aim to push police investigations to turn a blind eye to criminal offenses, but rather to justify conducting investigations despite insufficient evidence. Such investigations are "pushed" by the interior ministries or the BfV, often mediated by the general public prosecutor's office. The overriding motivation behind such investigations, i.e. publicly effective "executive measures", the intimidation or paralysis of a milieu, or the acquisition of information for completely different purposes such as to benefit the BfV but not the police, must then be linked to the police approach, which does not always go smoothly. The police can have a hard time exerting direct influence over such investigations, since the public prosecutor's office is involved. In addition, the "principle of legality" forces them to observe certain rules, such as largely obeying the law during investigations and intervening if it becomes apparent during the course of surveillance that serious crimes are being committed. On the other hand, the police are also quite

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 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 heavily 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.[15] 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

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

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.

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

ready to operate on the edge of legality. The phrase "for tactical reasons" is used to cover up all kinds of misleading and lies. "For tactical reasons", it is common practice when conducting political surveillance to give the impression that the person being investigated is a drug dealer when renting a surveillance post to make landlords more willing to cooperate.

Ultimately, the basic aim of police surveillance is the conviction of offenders and the conviction of the target by a court. If this seems improbable from the outset, tensions can arise between the authorities involved, which can negatively impact the motivation of the surveillance operators.

3.4.2. Intelligence service surveillance

Intelligence service surveillance has other investigative motivations, most of which are aimed at exposing the nature of structures and relationships. They are often based on earlier surveillance of certain people and result in later surveillance of other people, creating a network of information that has to be continuously analyzed and updated. Some targets are observed over and over again for a period of time. While the police are under strong pressure to succeed due to the expectations of the prosecution and courts as well as the constant presence of crime in the media, the success of intelligence operations is less precisely defined, and lots of surveillance has no measurable result at all. Some surveillance is only used to prepare for approaching a potential informant, comparable to the initial police surveillance for creating a movement profile of the target. This is followed by a BfV officer contacting the target—to recruit them as an informant or to provoke a reaction which provides the BfV with new knowledge, or as a tactic to plant information in a milieu, to make something public or to exert political influence.

As already mentioned, the BfV is relatively close to the police: its officers maintain the perspective of the police officers they once were and often do not possess the political horizons to judge their counterparts beyond the scope of criminal law. The ideology of the BfV is more that of a secret police than that of an intelligence service, because its hostile counterparts—public enemies, etc.—are considered to be more in the categories of regulatory and criminal law than in those of political conflict. Since the State and its officials are supposedly neutral, this is not seen as a problem.

While the police is moving closer to the intelligence service through technical and personnel upgrades of their special units, the intelligence service is moving closer to the police in their self-image.

As described in the introduction, with the end of the political East-West conflict, the work of the intelligence services has become internationally "police-ified". This development in Germany also includes the disappearance of the left-wing armed groups, whose high level of organization had forced all authorities involved to engage in very high level surveillance and occasionally to put intelligence logic before police logic. Currently, only individual organized cells of "left-wing extremism" are viewed by the police and intelligence services as opponents "on an equal footing" because of their motivation and sometimes high intellectual competence, along with well-organized crime due to their large financial and material resources.

3.4.3. Themes of surveillance

Police surveillance is not necessarily aimed at catching offenders in the act. It is often used to investigate criminal offenses, for example to collect information about suspects or to be able to arrest them in a "reliable manner."

Most surveillance activities are aimed at drug-related crime and property crimes, with a clear majority of the targets being non-German.

Political surveillance with the goal of criminal prosecution is almost always carried out as a result of investigations into Section 129/a/b of the German penal code (StGB) or related crimes, unless it is preventive surveillance, for example, because of publicly announced "days of action" by the left milieu that involve nightly arson attacks. There are three main focuses: Islamist groups, left-wing Turkish/Kurdish groups and German left-wing radicals. In Berlin, this surveillance is generally the responsibility of the LKA 56 or the MEK, and the more the Federal Public Prosecutor's Office is involved, the more often the BKA-MEK is also involved. In recent years there have been numerous collaborations between authorities. For example, the two major political proceedings from 2005 to 2007, the "militant campaign against the G8 summit" and the "militant group (mg)", were so staff-intensive that various authorities had to step in to provide support, from the federal to the local Berlin Offices for the Protection of the Constitution to the Saxony LKA.

Those who want to know who the BfV is surveilling can more or less find out in the annual Constitution

Protection report, which outlines the subject areas where the federal and State offices predominantly find their targets: Islamist groups, left-wing Turkish/Kurdish groups and German left-wing radicals. Of course, not all of the groups, currents and people mentioned can be monitored, and by no means are all of them surveilled. Right-wing extremist groups are more closely monitored by informants and TCS than by surveillance, which apart from a certain bias on the part of the authorities can also be explained by the fact that right-wing extremists usually have a low level of self-protection and so can be surveilled with relatively simple means.

For about ten years, the most important field of activity of the surveillance squads of the BfV has been Islamism. Islamists are an uncomfortable counterpart for German authorities, less because of their dangerousness or a high degree of organization (internally, most of them are considered to be amateurs) but more because of the confusion about this milieu and the cultural and linguistic barriers between officers and targets. In fact, the Islamists are not a great danger, their milieu is very closely monitored, and many personnel structures are known to the BfV and can be considered under control —if it were not for the great uncertainty about whether someone will suddenly go out and blow themselves up. The political sensitivity of this constellation forces the BfV as well as the State offices to invest a lot of time in their surveillance.

While the federal and local Berlin Offices for the Protection of the Constitution work closely together in the area of Islamism, there is a division of tasks in the area of left-wing extremism in Berlin. Larger cases from the field of terrorism, which include conspiratorial "autonomous groups", are processed by the BfV, while the State authority is more concerned with the local milieu and Turkish/Kurdish groups. Surveillance with the aim of recruiting informants or "tactical approaches" (for example, by manipulating the individual they contact by sharing specific information that they want to be spread) are carried out independently by the Federal and the Berlin Offices for the Protection of the Constitution.

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.

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.

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.[14]

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.

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

[14] *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.[a]

[a] https://notrace.how/resources/#surveillance-countermeasures

4. Surveillance Practices of the Security Authorities

4.1. How surveillance works

The following explanations do not make any particular distinction between the various services or authorities; the aim is to provide a picture of the surveillance process within special units that is as generic as possible.

4.1.1. The preliminary stages: from the desk of the administrative department...

In the lead-up to surveillance, the case is processed by the responsible clerk or the public prosecutor's office. Only when the paperwork has been dealt with do the surveillance units come into play.

Surveillance is done if other attempts at investigation and evidence gathering are foreseeably unsuccessful. This formula is part of every application for a judicial permit for "long-term surveillance", but it is more than just a formality, because surveillance costs time, personnel and money. After all, in order to control a single target, up to 20 people including their vehicles and technical equipment have to work for days. The surveillance units get many more inquiries than they can handle, so they can often only act when the clerk sees fit. In addition, there is the ever-present risk of "burning" the surveillance; that is, the target notices that they are being surveilled and thereby learns that they are under investigation. In addition, technical monitoring, i.e. above all, cellphone connection data, but also other telecommunications surveillance (TCS) and hidden video cameras, can often answer many of the investigators' questions about the movements of the target without costly surveillance.

When the judicial decision and the public prosecutor's order for enforcement are in place, the officer responsible for the case turns to the surveillance department and applies for an assignment. It usually takes a while before the surveillance actually starts because the department has many cases to process and it first has to plan the new assignment. Who is the target? Are there up-to-date photos? Is there only one target or several? What findings about the target are already available? Does a "conspiratorial apartment" (CA) have to be rented to monitor the target address? Telephone monitoring has most likely already taken place at this point in time, so some details about the target are known. However, it can take a few weeks before physical surveillance actually begins. A common procedure is to carry out a short surveillance operation with weak forces at the beginning in order to obtain the "movement pattern" of the target, i.e. to determine whether they are really at the assumed address, which means of transport they use and whether there are regularities. There is also second-tier surveillance, which involves only checking sporadically to see whether the target's car is in front of the door and only lingers there for a short time, hoping for chance discoveries.

4.1.2. ...to the desk of the surveillance team

MEK officers planning operations.

A surveillance team conducts team meetings every week. New cases are presented and the surveillance plan is developed. Who leads the surveillance squad on site, the squad leader or a subordinate official? How many people and cars are used for the case, which working hours and how many days are reserved, which technical means are used, who writes the surveillance report… etc. From now on, the person responsible for the case will be informed about the progress of the investigation but will not be on site himself. On the contrary, surveillance teams are reluctant to let their

colleagues from the administrative department disturb them at work.

By the way, surveillance operators are predominantly men—there are usually only two or three women in a squad.

The entire surveillance team is not always active on site. Particularly in the preliminary investigation, but also in uncomplicated cases, no more staff is used than necessary. Often four vehicles with 6–7 people are enough to keep a target under control, but sometimes the target needs to be observed around the clock, in which case several teams work alternating shifts. Such elaborate surveillance is seldom maintained for more than a week, and for a maximum of two weeks. But there is also surveillance that is only carried out on a certain day because of an expected meeting of several targets, with great effort and several surveillance teams. It has also happened that in particularly sensitive cases or with sensitive targets—for example armed groups—surveillance was conducted with deliberately irregular timing, but this is the absolute exception.

If a case is very important, different departments and even authorities take turns. Surveillance can be carried out by the MEK for a week, by the BfV for a further week, and then the LKA 56 takes over. "Administrative assistance" between the police and the BfV is not that common, but it is tried and tested and generally not a problem.

It is not really possible to describe a typical rhythm for surveillance because each situation and its environmental variables are too diverse. The best description of the average situation is surveillance that lasts eight hours a day for almost a week.

The surveillance team is assigned its own radio channel for work; using the TETRA[6] digital radio technology a "group" is assigned where no other forces are transmitting. The team works largely independently; a communications base is hardly required. Of course, the radio systems of the surveillance vehicles are hidden and have a hands-free facility and concealed call buttons, e.g. foot switches.

The principle of success for surveillance is the constant collection of knowledge. One can hardly hope to observe exactly what one is looking for very quickly. Instead, more and more data is gradually obtained that allows further conclusions. Even if surveillance does not bring a breakthrough for weeks, even if the target may be lost again and again, a mosaic is still created that helps to further the investigation. This approach leads to a certain routine with professional surveillance teams: they know that the constant repetition of the same unspectacular processes often leads to long-term success.

4.2. On the target property: "A-position" and "box"

If there are no particular reasons to do otherwise, surveillance will initially take place during normal working hours, i.e. from around 8:30 a.m. to around 4:30 p.m. If it turns out that the target has a completely different rhythm of life, this will of course be taken into account.

Surveillance always begins with the "A-position" on the target property. A-position is someone who sees the target immediately or will perceive them first when they appear. The target property can be their apartment and is usually called the "target address" (TA) but it could also be another location where the prospect of meeting the target is high. The "A-position" is usually, depending on local conditions, taken up from a vehicle, but also sometimes as an idle guest at a table in a café, a smoker on a park bench, or someone with binoculars through the window of a public building. Camouflaged vehicles are also used, in which someone is invisible from the outside, e.g. a minivan with tinted windows or curtains. The other operators first form a "box" around the target property. For this, all possible directions in which a target could leave or approach are covered as well as possible.

In professional surveillance, there is always at least one surveillance operator in the A-position. If not, the target is "out of control". Other operators report as "B-position", who can replace the A-position if necessary.

Only when it is absolutely impossible to take an inconspicuous A-position do authorities limit themselves to the formation of a box around the target and hope to discover them when they start moving through it. For example, the anticipated direction of travel would be covered at the next two intersections in order to receive the target there.

Most vehicles are on standby in the immediate vicinity and wait for reports from the A-position. In doing so, they position themselves in just the right location so that they can quickly cover the distance if the target moves. Usually, they are just around the corner or one

[6] *N.T.P. note:* Terrestrial Trunked Radio, a European standard for a trunked radio system used by many police forces in Europe.

gain certainty about whether you are a target, you have to move and force the operators to move with you.

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.

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

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 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

or two blocks away, if possible without a traffic light or a main road between them and the target property. The leader has a notebook so that they can enter interesting insights immediately. In addition to the squad leader, who controls the entire operation, the respective A-position has the right to give tactical instructions to the other operators: is the target clearly identified? If not, who can carry out an identification ("clarification")? If so, in which direction are they moving, how should the other operators behave, should they pause, follow, disperse?

In order not to miss anything even when things are hectic, radio communication is recorded centrally or, if necessary, recorded in individual cars with dictaphones.

After taking the first positions, there is often a long and uneventful waiting time. They doze off in the car, comfortable with the seat cranked back, listen to the radio and fall asleep. Every now and then they might get excited because someone thinks they have seen the target, but then realize it was just a false alarm. Once in a while, operators log out to get something to eat or to go to the toilet. The A-position is relieved at longer intervals, which is not only for inconspicuousness, but is also necessary because their concentration decreases considerably after a while. If the target is at home, they are usually replaced every hour, often every full or half hour. If the target is absent and the operation is waiting for them to arrive, the A-position sometimes stays on for several hours without being relieved.[7]

In order not to attract too much attention, the other vehicles also move from time to time. However, parking somewhere is inevitable—you cannot drive around in circles all day. Vigilant residents and pedestrians may notice what is going on after a while. However, this rarely results in disturbances to the surveillance. People see the operators and forget them, as they generally do not know what they're looking for. Experience has shown that almost no one remembers cars and their license plates or conspicuous people for more than a few minutes—not even the people who know that they are the target!

[7] *N.T.P. note:* Other sources disagree, stating that the A-position remains in place for long periods of time, usually changing only in the middle of the night to avoid detection by the target and third parties. If the A-Position is in a vehicle, the vehicle can be brought into position by a driver who then leaves while the surveillance operator remains in the back out of sight. Alternatively, the surveillance operator can drive themselves and then climb into the back. If they find a good spot, they'll stay there, have food prepared in advance, and shit in a bag.

If the surveillance is likely to last days or even weeks, the squad will look for a quiet place a little further away to meet in peace without chance observers being able to establish a connection to the actual target property. Well-suited locations for this are, for example, supermarket parking spaces, remote street sections or dead ends with many free parking spaces. "Mission meetings", mostly at the beginning or after the end of the day's shift, are also often held at such locations.

4.3. Mobile Surveillance

At some point the target shows up and there is "movement". At least one surveillance operator, usually several, have a digital camera and/or a camcorder with them and will try to make recordings of the target and of people with whom the target comes into contact ("contact persons", CP).

When the target shows up, it is important to start by describing them clearly to all operators so that they can be recognized from then on. This is done by the A-position, who then usually holds back a little because the target could have noticed them.

4.3.1. Movement by car

MEK officers on surveillance duty.

In every crime film we see a suspicious person driving away in a car and the policeman who is following them immediately pulling their car out ten meters behind to initiate the pursuit. In reality, this is, of course, completely impractical because the target could notice it. When the "target vehicle" (TV) starts to move, the vehicle in the A-position stops and waits while another vehicle from a greater distance follows. There is almost always enough time between the target getting into the car and driving off to bring another surveillance vehicle into position. Sometimes the vehicle even sits in front of the TV and allows the TV to overtake it once.

Tracking a car is a fairly safe and convenient form of surveillance. Radio communication is best and most

inconspicuously conducted in cars. Cars are severely restricted in their movement by traffic regulations and they can be clearly identified by their model, color and license plate, which makes tracking easier. Surveillance vehicles have a lot of horsepower and are driven by experienced people, so it is hard to shake them off by speeding. If necessary, they violate traffic rules, drive through red lights, on the sidewalk or against one-way streets in order to maintain contact. The authorities are allowed such rule violations under traffic regulations. In city traffic it is difficult to make up for a lost traffic light —not only because the TV can cover a kilometer in the passing minute and go beyond the field of view, but also because numerous cars push themselves in between, which then obstructs a pursuit. Therefore, at least a few surveillance vehicles will always try to maintain visual contact.

For some years now, the use of GPS tracking systems has been very widespread, the monitoring of which has switched from the control center to the surveillance vehicles, so that the position of the TV is visible at all times within an accuracy of several meters.

If the target drives a rental car, the operators will probably contact the rental company immediately or later in order to obtain further information: which name was the rental placed under, with which account number, how many kilometers were driven, etc. Many rental cars now have permanently installed tracking devices for theft protection or for fleet management.

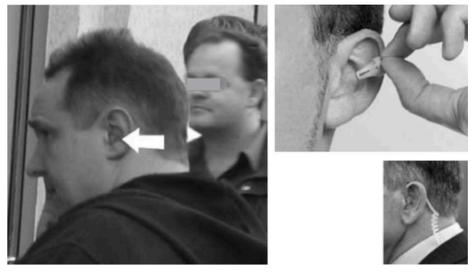
If the target is known to regularly use rental cars or car sharing, the operators may try to monitor frequently used vehicles.

4.3.2. Movement on foot

Surveilling a person on foot is a bit more strenuous. The pursuing operators, called "feet", have to be careful to send their radio messages inconspicuously—they mostly use larynx microphones in the collar of their jacket, sometimes on the wrist, sometimes hidden in a purse or in a backpack, which can be passed on to the colleagues who are relieving them. To receive radio, you have to have something in your ear—be it a Walkman headphone or a "Phonak", which is a wireless earpiece. Incidentally, such a "Phonak" is practical in itself, but it also has disadvantages: it is inconspicuous, but not invisible, and anyone seen with it is "burned". In addition, it is prone to interference, relatively quiet, quickly clogged with wax and can fall out of the ear at the wrong moment. In addition, a flat, elongated radio transmitter has to be hidden at a short distance (e.g. in the shoulder pad of the jacket or in the strap of a backpack). For all of these reasons, many operators prefer classic headphones.

All of this can be noticed by other pedestrians. That is why operators like to work on foot with cellphones. Reports can then only be heard by one colleague in order to then "translate" them over the radio for the other participants. By the way, cellphones have also allowed conference calls for years, allowing all other operators to listen when someone is speaking. However, these are expensive and cumbersome compared to radio and have therefore only been used sporadically for a long time. They are now more practical, but are no longer needed so urgently due to the introduction of digital TETRA radio.

If you are on foot, you can suddenly change direction, disappear into a house or change the means of transport, i.e. get on a bus, take a bike… Therefore, the "box" must be placed very tightly around the target, ideally with several "feet", who are on both sides of the street, so that when the target crosses the street, the A-position does not have to cross as well, which could be noticed. The target is also very slow on foot, which is why in the vast majority of cases it is possible to keep them under control, even if they make unforeseen movements.



Left: Policeman on duty with a "Phonak".

Top right: Inserting a "Phonak" into the ear.

Bottom right: This type of earphone with a transparent spiral cable is used by bodyguards but not during surveillance (too conspicuous).

4.3.3. Public transportation

If the target uses public transport, at least one operator will ride in the same vehicle. Often, in order to not attract attention, he will only get on at the next stop or, if the waiting time allows it and the direction of travel is clear, one stop earlier. An A-position is sought as far back as possible in the car in order to maintain view of all entrances and exits. The vehicles follow as best they

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

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

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 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

can. It is difficult to use a vehicle to keep up with the subway during rush hour traffic, so the vehicles try to drive ahead in the relevant directions while the target is still waiting on the platform. The target getting off is reported, whereby the surveillance operator stays on for one station further if possible and is picked up there by a vehicle. It is very rare that a target is really lost in this process.

The possibilities of shaking off operators in the subway and suburban train are overestimated in the specialist literature. targets tend to get lost due to communication problems of the surveillance operator, including confusion of platforms, and lack of information about the different lines and their directions of travel, which the concerned operators are not happy to admit.

And in the worst case scenario, the vast majority of targets now have cellphones with them, which can be located during phone calls or by "silent SMS",[8] which the surveillance teams make ample use of.

The video surveillance of platforms and vehicles cannot be effectively used for surveillance. When a target enters a subway station, it must be assumed that they will leave a minute later—during this time it is impossible to send an operator to the control center to check the screens there. In addition, the staff are primarily occupied with finding out which line(s) it is, when the departure times are, which transfer stations have to be covered and so on. There are also blind spots and the cameras have limited image quality. Even if the conditions are optimal, e.g. if the surveillance is for dealers who regularly act at certain train stations, the video monitoring via the control center will only take place in support of direct surveillance, as there are too many unanticipated movements for the target group to make that cannot be adequately controlled by the cameras.

[8] *N.T.P. note:* From GrapheneOS FAQ:[a]

> "Receiving a silent SMS is no longer a good indicator of being targeted by your cell carrier, police or government because anyone on the cell network can send them including yourself. Cellular triangulation is possible regardless of whether or not SMS texts are being sent or received by the phone. Even if an SMS did serve a useful purpose for tracking, a silent SMS would be little different than receiving unsolicited spam. In fact, sending spam would be stealthier since it wouldn't trigger alerts for silent SMS but rather would be ignored with the rest of the spam. Regardless, sending texts or other data is not required or particularly useful to track devices connected to a network for an adversary with the appropriate access."

[a] https://grapheneos.org/faq

4.3.4. Movement on two wheels

Surveilling a target on a bicycle or motorcycle can be very exhausting, as they do not move at the usual pace of road users. The bicycle is too slow for cars and too fast for "feet", and the motorcycle is usually too fast for all other means of transport. The surveillance forces must be prepared for this, which is to say, also use bicycles or motorcycles. This requires particular physical fitness and operational readiness, or a motorcycle license. In the case of special units, there are one or two motorcycles and/or scooters and a few bicycles per fleet; occasionally private bicycles are used.

Bicycles are more difficult to clearly identify, which can be an advantage for surveillance: the target will probably not recognize whether they have encountered any particular bicycle more than once a day. Usually, only one surveillance bike is used with a target who rides a bicycle, the driver of which changes their jacket from time to time or swaps it with a colleague. The cars try to keep in contact with the target as much as possible, while the operator surveilling by bike keeps a bit of a distance and approaches immediately if there are problems. The cars try to overtake the target as little as possible—this results in a noticeable jerky movement, because they have to keep pulling up to the right, then catch up again, then pulling up to the right again. This stop-and-go is a sure sign that a slow target is being pursued.

A motorcycle can outrun its pursuers by snaking forward at one or two traffic lights. But even during a motorcycle ride, only one, rarely two, surveillance motorcycles are used, the rest of the team tries to keep their cars in position as best they can. As with car pursuits, the relatively restricted network of traffic rules has an effect in favor of the operators, because in practice a motorcycle is also severely restricted in its freedom of movement in city traffic by red traffic lights, other vehicles and the road layout.

4.4. When the target gets "out of control"

Normally, the squad is not hell-bent on trying to keep contact. If the impression arises that the surveillance was recognized by the target, if the target's movements

are difficult to calculate, or if they move back and forth a lot in a very small area, the operators withdraw a little. If necessary, they give up the A-position, only to form a larger box around the area. They may even drop the target completely, "breaking off" in order to pick them up again at another location, such as at the home address.

If the target disappears, the area is searched. Other vehicles drive to known destination addresses and wait to see whether the target appears there.

If a target is judged to be particularly aware, they are sometimes left on a "long leash" and the team falls back a little, or the surveillance is carried out with breaks, only every two days or only every other week.

In only very few cases is a target lost because they consciously "shake off" the surveillance. It mostly happens through coincidence or inattention on the part of the operators. After all, they are the professionals and the target is an amateur, so they generally have a better understanding of how to shake off or avoid being shaken off.

If there is a possibility that the surveillance was recognized by the target, this does not necessarily mean that it will not be continued—depending on what information the operators want to obtain. Because the target also has an everyday life that they cannot easily change: work, social duties or other activities that they cannot easily end or postpone. Under certain circumstances, the operators will even accept that the target will remember a few cars and faces—and will probably soon forget them—in order to gain further knowledge.

4.5. End of the work shift

When the surveillance team has completed its daily workload, which is often almost exactly eight hours, a surveillance report is written. It contains the names of those involved, the vehicles used and of course, the observations and their associated times. In addition to the detailed surveillance report, which is entered in the unit's "diary", there is an abridged report for the investigation files. Sometimes this is used only by the clerks in the form of their own "reports".

In general, surveillance and arrest are two separate processes. There is indeed police surveillance with the specific aim of catching the target in the act. However, this does not happen very often, mainly when the surveillance supports the use of a liaison officer or similar, for example when buying drugs. The rule is that the surveillance is first analyzed and the responsible clerks decide what the procedure will be moving forward—so the arrest takes place later and by other forces.

4.6. Special case: "protective surveillance"

If the Office for the Protection of the Constitution (BfV) carries out "informant approaches," that is, attempts to recruit "sources," the target is observed beforehand with varying degrees of thoroughness so that the clerk is optimally prepared and can decide on the best time to make contact. This can take place on the street or as a home visit. This preliminary groundwork is usually carried out in only a few days, but in complicated cases it can take weeks.

On the day of contact, in the vast majority of cases, a surveillance squad is present to help the officer if the target reacts aggressively and to check the target's behavior after the contact. Do they make phone calls? After that, who do they go to first? If the contact is successful and an informant is recruited, later meetings are occasionally surveilled. For example, they are interested in whether the target spends the money they receive for cooperating immediately and for what, and whether they involve other people in the process.

In the case of a "tactical approach", which is to say, a contact that does not aim to recruit an informant, but is intended to manipulate the target, the surveillance can be limited to purely protective surveillance on the day of contact. The goal of such a contact can be to spread certain information, but also to provoke a reaction, which can be evaluated with other measures, such as TCS.

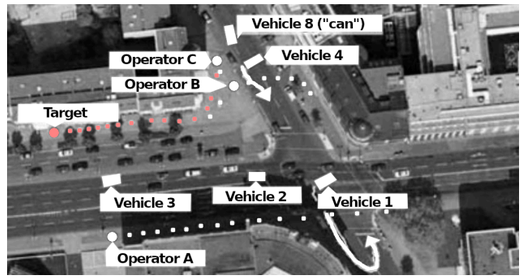


Fig. 8: The target surprisingly turns around and continues west on the main road

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.

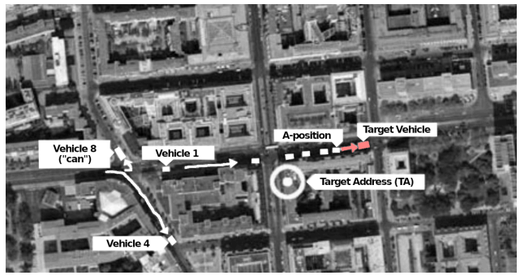


Fig. 5. Later, the target comes back from a drive in the vicinity of the TA

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.

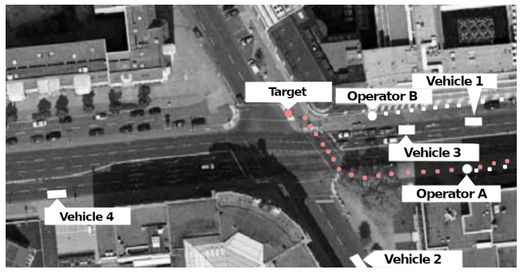


Fig. 6. The target again leaves the TA on foot

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.

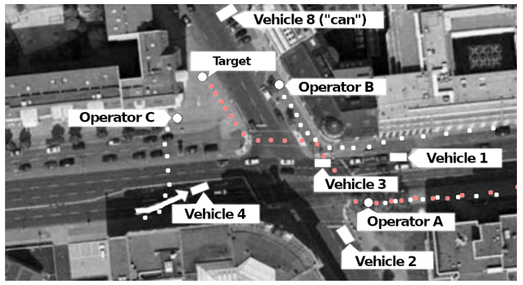


Fig. 7: The target crosses the cross street and turns to the right.

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.

5. Special Considerations

5.1. Radio

With the switch to the digital TETRA system from 2010 onwards, numerous considerations regarding radio communications will no longer apply. It will not be possible to intercept this digital encrypted radio in the foreseeable future.

5.1.1. Technology

TETRA antenna (very similar to cellphone antennas; three antennas are a characteristic feature).

Some facts about "Terrestrial Trunked Radio": TETRA is a digital radio process, created by an international consortium of companies based in Rome. With its takeover in Germany and other EU countries, TETRA will presumably establish itself as a Europe-wide digital standard.

TETRA radio itself is not yet secure against eavesdropping, but the Federal Office for Information Security (BSI) has developed an encryption system for German BOS radio that guarantees "end-to-end encryption" (all transmitted data is encrypted). This encryption is based on a built-in chip. Since every radio device has an ID number, every device that has been reported as lost can be blocked immediately, creating additional security against unwanted eavesdroppers.

BOS-TETRA radio is handled in the 380–395 MHz range ("70 cm frequency band"). There is a lower and upper band, as in the earlier analog duplex radio, in which mobile subscribers transmit on the lower channel ("Up-Link") and are received on the upper channel ("Down-Link"). The channel spacing is between "Up-Link" from 380 MHz and "Down-Link" from 390 MHz is 10 MHz. The channel spacing is 25 kHz. The transmission rate is relatively high due to the high frequency, but too low for the transmission of images. This problem is still being worked on.

5.1.2. Radio practice

The "radio discipline" that was taught to all operators during training is important in large radio circuits with many participants, regardless of whether they can be eavesdropped on by opponents, because otherwise communication will be ineffective: everyone has to be brief, only speak when permitted, use clear language, etc. This is less urgent for surveillance because the radio circuit is very manageable and the channel only belongs to a single team. In the past, radio discipline was more necessary for surveillance squads because of the risk of unauthorized interception. The textbook provided for people to be abbreviated as "P", the target being "P1", known contact persons then "P2" etc., vehicles as "F", properties as "O". Persons, vehicles and properties already known in the planning phase should be familiar to all operators and should only be referred to with their abbreviations in the course of the surveillance. Street names should, as far as possible, be abbreviated or circumscribed: for example, the street in which the target lives was then the "target street", other streets in the vicinity the "K-street", the "B-street", etc. That's the theory. In practice, this was and is hardly done as long as it is not about extremely sensitive cases with appropriate briefing at preliminary meetings. Even with good intention, unforeseen events occur, discipline deteriorates or the wrong word slips out in the excitement. When the target moves across several streets, it is almost impossible to speak in coded form—the colleagues simply cannot keep up. Instead, a typical jargon emerges within the units that avoids certain key words without strictly following the textbook.

Radio discipline is rather lax within special units. The official nickname of the unit is usually omitted because there is no need for it to address itself. The correct address is actually the two- or three-digit numbers that identify the vehicle (police) or the person (BfV), but

instead, often the first name is used, and they sometimes chat about trivial matters when nothing is going on. Quite a few operators also know each other privately and will chitchat. This is likely to increase with the introduction of TETRA and lead to excessive conversations during the quiet phases of the surveillance.

5.1.3. Science-fiction?

Another aspect of TETRA is that the common handheld radios from the manufacturers Motorola and Sepura look similar to cellphones (see photos) and can hardly be distinguished from professional radios. It is conceivable that devices disguised as cellphones will be developed. This could make it much easier to use in some areas, such as in foot pursuits. The reports of undercover agents in demonstrations, which had previously been sent to the control center by cellphone and forwarded from there to the rest of the squads with a time delay, in the future could possibly be fed into the radio circuit from the beginning. Telephoning with what appears to be a cellphone arouses much less suspicion than murmuring into the lapel of your jacket.[9]

TETRA devices currently in use: handheld device permanently installed in the car; MRI (base unit) from Motorola; HRT (hand-held) from Sepura.

5.2. Technical means

5.2.1. Telecommunications surveillance (TCS)

Strictly speaking, telecommunications surveillance measures, which include e-mail and the Internet, are usually part of contemporary surveillance. However, telephone calls are a particularly important part of surveillance practice. A distinction must be made between several areas of TCS: the collection of connection data, the location of cellphones, and the qualitative interception of conversation content.

Connection data

Connection data is constantly recorded by the telecom companies, stored for a certain period of time and passed on to authorities upon request, which companies are legally obliged to do, even if the duration of the storage is still controversial—the keyword here is "data retention". The legal threshold for obtaining this data is lower than the threshold for recording conversations, which is why connection data is routinely queried by surveillance personnel. This happens at the head office, where the responsible clerk then informs the management of the surveillance team whether the target's phone is currently being used, who is on the phone with whom, and, in the case of cellphones, whether it is turned on and connected. This data is therefore available to surveillance teams regularly and very promptly.

A few complex steps are still required to locate a cellphone to the exact meter, but this is usually not necessary—the registration of the phone in a certain cell tower already limits its possible location to such an extent that the surveillance squad has a good chance of finding the target or their phone with its prior knowledge of the target and their movements based on the connection data. For more precise location, the "triangulation method" can be used, in which the location of a cell phone can be determined to within a few meters by comparing the connection data of several neighboring cell towers. Many modern smartphones, iPhones and other devices with navigation and internet functions are already preset accordingly. If the signal from the GPS satellites is too weak for an exact location to be determined, e.g. in bad weather or in buildings, the triangulation method is automatically used. In order to locate a cellphone from the outside in this way, direct cooperation with the cellphone provider is required—the surveillance personnel cannot just call it up.

Not all connection data will be saved. When the cellphone is turned on and off, when changing from one coverage area to another, in the event of fluctuations in signal strength or during the regular automatic "Periodic Location Update" (PLU), the cellphone contacts the base station without this data being stored as connection data in the real-time monitoring of the device. However, it can in principle be localized in this way.

[9] *N.T.P. note:* Officers with good discipline would not talk into their jacket. Wireless microphones are very sensitive. Bluetooth headphones or smartphones are now so prevalent that it makes more sense for operators on foot to use these so they do not get spotted talking to themselves. Smartphones also provide a way for taking quick photos that seem casual.

6. Case Study

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

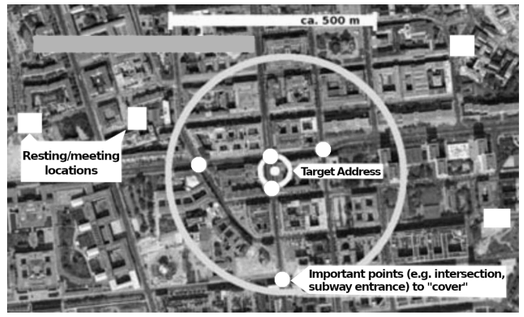


Fig. 1: Overview of the situation

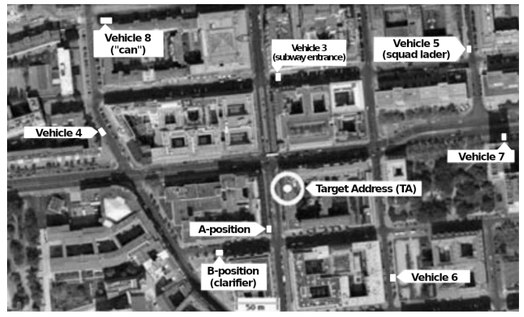


Fig. 2: Surveillance with 8 vehicles without a conspiratorial apartment

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).

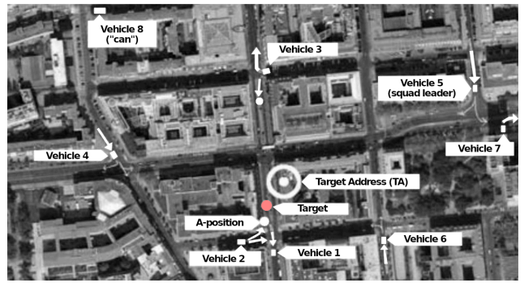


Fig. 3: The target leaves the TA and walks towards the subway station entrance

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.

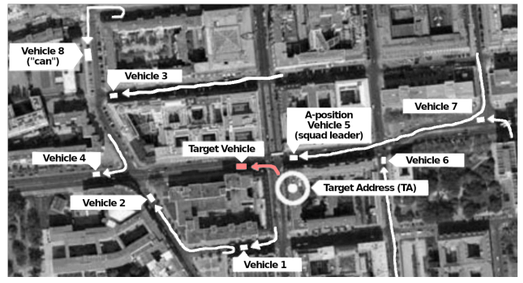


Fig. 4. The target moves away from the TA in a car

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.

evasively: "There must be a mix-up". Incidentally, such a "plausible deniability" is an important principle when camouflaging, including when choosing camouflage names and properties, etc.

Each surveillance vehicle has a set of interchangeable license plates in the trunk. During a surveillance operation, the license plates are usually not changed—unless they fear that the target noted it, which rarely happens. When the target vehicle leaves the city and appears to be embarking on a longer journey, license plates of the surrounding State or other large cities are installed as soon as possible. Changing the license plate number during surveillance is done by hand in an inconspicuous place like a supermarket parking lot—automatic license plate changing devices are still only available for James Bond.

5.5. People

The work in surveillance units is exhausting and is less well paid than a post as a senior criminal investigator or analyst. For most, it is not the end stage of their careers, but only an intermediate step. This work is particularly attractive for police officers of the "middle service" who are striving for the "higher service". After a few years the officers often lose their motivation to sit around for hours in the car at uncomfortable times of the day or to drive back and forth for whole weekends without success. Only a few officers are older than 40 years, most of whom are managers. Only the intelligence services of the surveillance squads are frequently manned by veteran, experienced and correspondingly "leisurely"-looking officers. The typical people are between 25 and 35 from the police force, so they meet the necessary conditions in terms of average body size and athleticism. You will not see people with physical disabilities, noticeably short or overweight people. Their posture is generally controlled and upright, facial expression attentive, and the gaze often concentrated. The feeling of belonging to an elite squad, of knowing secrets and being able to exercise invisible power as a group leads to a mostly calm, relaxed and dominant body language. Nervousness and a hectic pace only prevail during the first missions.

In the vast majority of surveillance, especially if they are not expecting to have to follow closely behind their target on foot, the operators' best disguise is their mediocrity. You look like thousands of others on the street. Sometimes it is claimed that in the past, plainclothes policemen could be recognized by their identical mustache, whereas today they are camouflaged with piercings and hair gel—in reality this only reflects the change in general social norms towards a greater variety of appearances. Subtle tattoos, earrings and daring haircuts can also be seen on riot police in uniform these days. Exaggerated aesthetics are not to be expected mainly because they do not match the personality profile of people who take up this profession. Active camouflage measures are only taken for a short time; BfV officers, special units in particular, sometimes take a wig with them. However, there are always some officials in the MEK's undercover reconnaissance who go to great lengths to blend in with the scene and get a punk mohawk haircut for a long time. In general, however, the officials also have a private life and do not want to be stared at in their free time by their bourgeois neighbors, especially not when they hide their status as BfV officers under the cover story of a boring work life.

Above all, their clothing should be inconspicuous and easy to move around in: they wear comfortable average clothing, "casual wear". Jackets are usually worn to hide the radio and footwear is almost exclusively sporty. Since you change or swap shoes less quickly and willingly than, say, jackets, and because you have to expect to be out and about for hours, the shoes have to be comfortable. Tight patent leather shoes, cowboy boots or pumps are ruled out. Women almost always wear trousers and do not dress conspicuously "feminine" because that attracts looks, makes them more conspicuous and is impractical for longer pursuits. Men usually do not wear ties and suits unless the target is moving in the appropriate environment. Of course, bright colors or similar irregularities are avoided. Sunglasses and baseball caps, on the other hand, are seen often.

In special cases, especially in the case of surveillance of the left milieu, more value is placed on camouflage; shaving is avoided for three days, a stained old jacket is thrown on or the haircut is changed. But only a few from the surveillance team camouflage themselves so well, since most surveillance takes place from surveillance vehicles, the appearance of which does not match the "scene" outfit operators might wear.

Connection data in the true sense of the word, which is stored centrally, is created during sending and receiving activity. This allows the cellphone to be located using "silent SMS" (in technical jargon: "pings"). Such an SMS from surveillance forces is not displayed on the cellphone, but generates connection data. Occasionally, "pings" are sent to a target phone at regular intervals, not only to locate it, but also to determine whether it is turned on—especially for targets who are believed to have intentionally turned off their cellphone as part of conspiratorial behavior. One can confidently assume that intelligence services in particular have been routinely and automatically using this method for a long time against numerous suspects, especially "terror suspects", to create movement profiles, for example in the form of hourly "ping" requests around the clock or at least from early in the morning until late in the evening. If several target phones can no longer be reached at the same time, the conclusion can be drawn that a conspiratorial meeting is taking place.

Monitoring of content

The qualitative tapping of phones, on the other hand, takes some work. The calls have to be listened to, often translated, and analyzed, which is very personnel-intensive. A real-time application of eavesdropping knowledge, i.e. its immediate forwarding to the active surveillance team, does not occur very often. For this, the case must already be very important—politically sensitive, or putting human lives in danger.

Incidentally, this also applies to the use of listening devices inside properties, whether apartments or vehicles. According to a study by the Federal Criminal Police Office in 2008, more than 30 police wiretapping measures were carried out in apartments in Germany in 2003, and after the restrictive ruling by the Federal Constitutional Court at the beginning of 2003 fewer than 10 police interception measures were carried out annually, around half of them in §129/129a proceedings. According to the study, "the personnel capacities for acoustic surveillance of living spaces are often only sufficient in the field of State security".

"IMSI catchers" are a technology which can be used at close range to identify and eavesdrop on cellphones that operators were not previously aware of. This technology is very expensive and complex to use, which is why it is normally only used in very high-profile cases or in cases in which the data is really needed urgently, e.g. in blackmail/kidnapping cases.[10] In order to record the cellphones in a certain area, for example as an aid to the identification of participants in a meeting, it is much easier and cheaper to request the corresponding connection data from the mobile network provider soon afterward. Both this and the other procedures require a court order.

This applies to all TCS measures that are carried out in the case of specific investigations, but not preventively and/or on a large scale as defined by the General Security and Order Act (ASOG). Both because the administrative effort would be too great, but above all because the effort to analyze such data is out of proportion to the benefit. The police will not monitor hundreds or thousands of cell phones during a large-scale demonstration in order to discover the plans of the "troublemakers" because this would not be possible in terms of personnel, and the tactical planning and management of surveillance operations is determined by active measures such as their own reconnaissance and on-site movement. On the other hand, it cannot be ruled out that individual cell phones that are considered relevant are monitored in this way.

5.2.2. Cameras

Cameras are essentially used for surveillance in two ways: for photographing or filming the target and their contact persons during active surveillance and for inconspicuous monitoring of house entrances or other important properties.

During the surveillance, several team vehicles always have cameras with them. Everything that the market has to offer is used, especially DSLR[11] cameras with powerful telephoto lenses and small digital cameras. These digital cameras usually have an image resolution that is too low to take effective portraits, but they can be used to record actions and movements and create mnemonic aids: which house did the person come from, which one did they enter? Entrance panels and mailbox labels can also be digitally documented quickly instead of standing suspiciously in front of them with a notepad.

When monitoring entrances etc. strong telephoto lenses are often used in order to reliably identify people. Such cameras have to be well camouflaged—despite

[10] *N.T.P. note:* More contemporary sources indicate the use of this technology is more widespread today.

[11] *N.T.P. note:* Digital single-lens reflex cameras, a type of digital cameras.

all the miniaturization, a good telephoto lens is still relatively large and noticeable today.

"Cans"

Official inside a camouflaged van (elevated position). The large window on the right is mirrored or heavily darkened.

Small trucks/vans are mostly used for camouflage. These have tinted or curtained side windows, especially when they are occupied by people. Such vehicles have the advantage of being very flexible: they can quickly change location in the course of the surveillance. The essential feature of almost all of these vehicles is that their interior cannot be seen even from close up, but they are not completely windowless. Either the panes are heavily tinted, often with additional curtains behind them which cannot be seen due to the tint. For the tinted effect, it is not the light that falls on the window from the front that is decisive, but the complete sealing of the interior against background lighting—the strength of a window tint is therefore best recognized by a bright light source behind the vehicle. Or the panes are covered by curtains or the like, which have a small gap, or "two-way mirrors" are used —surfaces mirrored on one side, which are usually not located directly on the pane so they are less noticeable. Small window hatches between the cargo area and the driver's compartment of a van are particularly suitable for this. The disadvantage of tinted windows is the loss of light, which is why cameras in such vehicles can only be used during the day in good lighting conditions and are usually removed when dusk falls.

Camouflaged cameras in vehicles and homes

MEK officers working in a conspiratorial apartment.

Cars with hidden/camouflaged cameras in an otherwise open interior are less conspicuous, but have the disadvantage that the camera has to be realigned to the target after each time the vehicle moves. Such cars are therefore used for recording the comings and goings at a fixed destination over a long period of time. The issue of storage capacities and battery power arises here, especially in the cold of winter, which is why such vehicles have to be regularly serviced. Usually, a stationary camera is positioned as close as possible to the target property in order to avoid any obstructions to the line of sight. Only when there is no alternative is a camera vehicle parked on the other side of the street, because traffic flows significantly obstruct the desired viewpoint and nobody is present to bridge gaps in surveillance.

If it seems worthwhile and/or no vehicle can be placed, a stationary camera is set up, usually in an apartment diagonally opposite the target property—a "conspiratorial apartment" (CA). Since empty apartments are not available on demand, it can take some time before a CA is available. If time is of the essence, contact is made with police-friendly tenants, who, as already mentioned, are gladly told that it is for the surveillance of drug traffickers, because this has the most widespread social acceptance. If possible, the CA should be on an upper floor, as the view is better here and the target does not look at it as regularly, but also not too high because of the obstructions from trees, awnings, signs, etc. For example, the camera can be camouflaged by plants, curtains or blinds, but it is almost even more important to ensure that, especially in the evening/at night, the windows are protected from outside by curtains or that there is no room light. A monitor in a dark room can also be recognized by its bluish reflection on walls or ceilings. Due to the high expenditure of personnel and costs involved, State authorities only use conspiratorial apartments in particularly important cases, while the well-equipped federal authorities such as the BfV often set up vehicles over longer periods of time, from which video surveillance is carried out for months or even years. A cheaper variant of the CA is the temporary use of commercial space that is provided by companies or owners, and the use of favorably located real estate in State or federal ownership, such as fire stations, police stations, and administrative buildings.

To monitor a rear exit, a small webcam can also be installed inconspicuously somewhere, the quality of the images being irrelevant. But that is the exception.

The remote control of computers and telephones and the associated acoustic and visual room monitoring still requires a great deal of technical know-how. But the more people become used to having their devices in constant background use and lose track of the technology beside them while being distracted by the colorful screens, the more attractive such surveillance becomes.

Older simple cellphones still have to be physically manipulated in order to turn them into eavesdropping devices. The new generations of cellphones already have so much software in use that most of them can be hacked and reprogrammed remotely like a computer. The same applies here as applies to the use of bugs: the analysis of the resulting data is personnel-intensive, so in the near future this type of monitoring will only be used against important individual targets.

5.4. Vehicles

Surveillance vehicles can be any type, from small cars to minibuses. A couple of motorbikes and bicycles are also possible. Most special units also have one or more taxis.

The vehicles must meet the following criteria: inconspicuousness in everyday traffic, usability in as many different environments as possible, usability by many different drivers, service and maintenance friendly, i.e. no exotic brands. Overall, they often appear impersonal and are easily mistaken for company or rental cars. Conspicuous and unusual paintwork is avoided.

The vehicles are usually clean, well-maintained and without special personal characteristics. For example, there is rarely anything hanging from the rearview mirror. They have a lot of horsepower, almost always with an automatic transmission, and only in very exceptional cases do they have diesel engines. They almost never have extra equipment, i.e. no wide tires, spoilers, special rims, leather seats… They almost always have four doors and often they will have a sunroof. Normally they also have an auxiliary heater, the control of which is integrated into the on-board computer in modern cars and can no longer be recognized. Inside the car there are sometimes telltale objects, e.g. a hand fire extinguisher, sometimes even a red and white police-issued trowel peeping out from under the passenger seat, or an additional interior mirror like in a driving school.

Bumper stickers are applied very sparingly and more temporarily. In general, camouflaging additions are rarely used, as they are double-edged: what makes the car inconspicuous at first glance becomes a problem during a second encounter, as it is memorized as a special feature and thus may have drawn attention to the vehicle. In particular, forged company labels with telephone numbers are avoided, since it is feared that someone will actually call the number.

The vehicles are equipped with a "silent alarm" and the alarm system is directly connected to the police.

5.4.1. Antennas

Antennas are not as clear a feature as they used to be, but they are still informative. Good radio still requires free-standing antennas. Even car models that can be found on the road without an antenna or only with very short stub antennas (GSM/GPS antennas for cellphones and navigation devices), such as Audi and BMW, are often equipped with longer antennas for surveillance use or upgraded with commercially available mobile magnetic base antennas.

TETRA radio is handled on the "70cm frequency band". The length of an antenna should ideally be a straight divisor of the wavelength (L, or "lambda"), which is why BOS vehicles have been equipped with 70cm antennas since 2009, an antenna length that is absolutely unusual in road traffic. These 70cm BOS antennas cannot only be seen on every patrol car, but also on numerous civilian vehicles. Since the responsible technicians have also noticed this, in the meantime, camouflaged civilian vehicles are gradually being retro-fitted with more inconspicuous antennas.

Camouflage antennas for special units are usually L/2 (35 cm) or L/4 (17 cm) in length. 35 cm antennas can best be used as commercially available radio roof antenna camouflages, as has been customary for a long time, since the previous "2m frequency band" also allowed such antennas. Usual radio roof antennas are 45 cm long. In contrast, 17 cm antennas are more like cellphone antennas, and many modern vehicles no longer have any visible radio antennas, but only GSM/GPS stub antennas.

5.4.2. License plates

The official license plates are also important. They are almost always clean and well-kept. The license plates of special units are specifically selected for the purpose of "plausible deniability"—there is always a double (a harmless "normal" car that has a very similar license plate) so that any inquiries can be answered

possible to transmit amounts of information by radio that seemed unimaginable a few years ago.

5.3.2. Future resources

Optical surveillance: Image and sound recordings consume a lot of storage space, and a corresponding amount of energy is used to send large amounts of data. In a few years this will no longer be an obstacle to placing cameras and listening systems in handy packages in target vehicles, similar to those used today. Nevertheless, this remains a technique for individual cases, because the analysis required is labor-intensive. Allegedly, intelligence services have been using mini cameras for years, for example to visually document the route of a target vehicle.

The optical monitoring of at least the area close to the apartment, e.g. the hallway, if not the apartment itself, is seen by the police as a desirable extension of their scope—pressure on legislation will grow in this direction in the coming years.

With the increase in **public video cameras** and the advancement of biometric software, it may become possible to track a person's movement through the streets of the city. The automated identification of people via video is theoretically well advanced, but in practice it is still prone to errors. In practice, this will only play a marginal role for surveillance in the foreseeable future, because the personnel effort required to analyze this data in real time is quite high. Such surveillance techniques are more likely to become more important for retrospective investigations.

Above all, the inconspicuous camera "domes" are becoming more and more common in the cityscape.

Various models of **optical scanners for license plates** are already being tested by the police, for example, in connection with toll systems—these could be used in the future for automated detection and recording video footage of vehicles. These readers look similar to mobile radar speed cameras and can occasionally be seen at the edge of highways.

Two license plate scanners in test use.

RFID (Radio Frequency Identification) technology could have a great future in surveillance technology. Today, RFID chips are already being used in billions of units, especially in inventory management and access control, but in some countries also for road toll systems. The classic passive RFID transponders are tiny and do not have their own power supply—they only react to the external signal from a scanner. However, their range is usually only centimeters to a few meters. Active and semi-active RFID transponders that have small batteries can reach ranges of several hundred meters. This means that in principle mini-tracking devices can be built with which not only cars, but also bicycles and people can be tracked.

Apart from that, passive RFID transponders are being built into more and more objects for everyday use and allow their identification and localization. Future mass applications include access controls for buildings, e-tickets or road toll registration using an "E-plate", and more license plate-RFID readers installed in more places. In the medium term, it is primarily a technical question of to what extent this can be used for surveillance purposes: the reading devices would have to be networked and large analysis capacities created, the standards of identification and data transmission would have to be adapted, the legal and technical requirements for the transfer of data analogous to the Telecommunications Surveillance Ordinance would have to be created—then it would be possible to track RFID fully automatically. With the general spread of this technology, sooner or later every person could carry chips with them on some card that is government-registered somewhere and therefore traceable. It will certainly be many years before this becomes routine. But the technicians of the intelligence services are definitely already researching its practical implementation.

IP identification: more and more electronic devices have their own Internet Protocol address (smartphones, ebook readers, etc.), and more will be added in the future, for example on-board computers in vehicles also have an IP. If such devices make contact with the Internet via a wireless connection, the dial-in area can be located in a similar way to how cell phones are located.

The camera recordings can be uploaded directly to the vehicles of the surveillance team.

In the case of surveillance in "terrorism" cases and/or the simultaneous use of eavesdropping equipment, video surveillance of the concerned house entrance can be assumed on principle.

5.2.3. Tracking devices

Due to technological progress, the monitoring of cars with tracking devices has become routine. The classic radio tracker has now largely been replaced by the GPS tracker.

With conventional radio tracking, a small transmitter is attached to the target vehicle. The range of its signals is small, only approximately 2 km in the city, and in order to use them the surveillance vehicles must have the appropriate technology on board: two receiving antennas. The strength of the signals indicates the distance of the TV and their compass direction. In spite of the tracking device, the pursuing vehicles must be relatively close to the TV and will often waste time searching.

GPS (Global Positioning System) requires a little more technology and larger transmitter units, but this is offset by their ease of use.

For example, a highly sensitive GPS antenna, a GPS module for data transfer, a GSM transmission unit, a technically adapted cell phone module, and a power source are required for GPS tracking. There are essentially two forms of application: the handy tracking module, also known as the "Quick-Pack", which can be attached to the target vehicle from the outside within seconds, and the "combined device for voice recording and tracking," which must be laboriously installed inside the target vehicle.

"Quick-Pack"

Depending on the size of the batteries, a tracking module is about the size of a thick paperback and is attached with strong magnets somewhere on the underside of the vehicle where it is not noticeable, is somewhat protected while driving, but is also quickly accessible and does not trigger an alarm system. Depending on the car model, the places that are best suited for this are the lower body frame around the wheels, the bumpers, and the empty spaces around the mudguard or the fuel tank. The engine compartment is looked into for maintenance too often to be suitable, and the area near the tailpipe is not an option either because of the heat. In principle, the metal of the body has a shielding effect, but it is so slight that it has to be accepted as long as the metal does not completely enclose the device. The tracker usually has high-capacity batteries that last for months and a vibration sensor that activates it as soon as the engine is started or the vehicle is moving. The tracker then continuously locates the movement, and the transmitter unit sends this data to the control center. This means that the movement of the TV can be tracked down to the meter from the office 24 hours a day. Most devices also store the data locally, so that even if the transmitter module fails, the data can be read later after the physical retrieval of the tracker.

Another possibility is to use external power sources on the vehicle, e.g. electrically adjustable exterior mirrors. This manipulation is less inconspicuous than placing it on the underside of the vehicle and takes a little longer, but removes the need for large batteries. The receiver and transmitter modules fit into a matchbox, so they also fit comfortably in the exterior mirrors of modern vehicles.

Permanently installed devices

In order to set up a combined device for voice recording and location tracking, with which not only the vehicle can be localized, but conversations in the interior can also be monitored, secure access to the target vehicle is necessary, if possible in an autoshop. Most of the time, the vehicle has to be "hijacked" for a few hours, which both requires considerable effort and risks discovery—and the same problem arises when the technology is recovered. The authorities can certainly come up with something to gain inconspicuous access to the vehicle. In the investigation against alleged members of the "Militante Gruppen" (mg), for example, the BKA went so far as to sabotage a parking gate so that the target vehicle could not be parked in a theft-proof way, and placed a similar vehicle into the parking space during the "kidnapping".

The installed device is by far harder to detect than the other trackers we discussed, even with precise searches. Modern cars have many cavities and difficult to identify components, and the electronics are so complex that it is almost impossible even with professional measuring devices to identify unwanted foreign electricity consumers. The positioning of the microphone(s) is problematic, since the interior of the vehicle is severely impaired by background noise. In practice, only pieces of the conversations in the vehicle can be reliably understood.

Simple GPS tracking via tracking modules are now used routinely by all special forces.

For the sake of completeness, it should be noted that there are also tracking devices of comparable size on the market based on cellphone connection data (see the "triangulation method" described above), for example, for monitoring vehicle fleets of trucking companies. As far as we know, however, these transmitters play no role in the surveillance process.

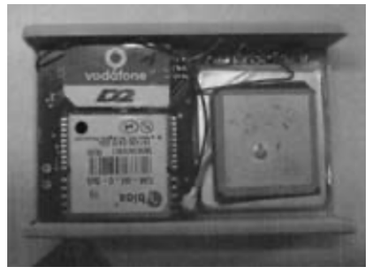
The devices described can be installed in all motor vehicles, and tracking modules in principle can also be placed in motorcycles, although this is a little more complex because there are only a few possible hiding spots. It is very difficult with bicycles because they can only be concealed in the frame, which is not very promising due to the shielding effect of the metal. Alternatives could be a permanently installed lighting system such as the dynamo (electrical generator for bicycles employed to power a bicycle's lights) and plastic parts with cavities such as reflectors and lighting. For a target, however, it is very possible to quickly examine a bicycle for foreign objects.

Left: GPS transmitter from the LKA Schleswig-Holstein (2007), GPS antenna and battery set separately.

Right: GPS transmitter from the BKA (2007), GPS antenna separately.

Four classic or commercially available GPS tracking modules from the years 2007–2009.

Top left: self-made with external GPS antenna; top right: Gmyrek; bottom left: Fugon; bottom right: Rettenegger.



Inside view of a GPS tracking module. At the top left the GSM card for transferring data via cellular network.

A GPS transmitter is placed, the technician is secured by two officers.

Installation of a GPS transmitter next to the rear wheel arch, in this case the GPS receiving antenna (at the very bottom) separate from the rest of the module.

Tracking module attached to the underside of the vehicle in a cavity. It is wrapped in plastic to protect it from splashing water. In winter, packaging also increases the service life of the battery (protection against discharge through cold).

5.3. Things to come

The three technical means of telephone connection data, video cameras and GPS tracking are today's standard of good surveillance units.

Other techniques, such as directional microphones, bugs, and eavesdropping on computer screens, are the exception and can be found in individual cases in operations by intelligence services or industrial spies. In the media, special methods are repeatedly presented as very easy to implement, be it recording signal radiation from computer screens (TEMPEST[12]) or listening to and identifying cellphones using an IMSI-catcher or even disrupting GPS signals ("GPS jammer"). Such reports are usually grossly exaggerated to add sensation and newsworthiness. The corresponding techniques look relatively simple in theory, but in practice they are time-consuming, prone to failure and can only be effectively used by experts with a high level of technical and financial commitment.

Basically, it should be noted: every surveillance technology is used (or not) according to a cost-benefit calculation. With large effort, large results must be obtained, and a large effort means a large personnel expenditure. If they get a lot of easy-to-process data with limited resources, as is the case with GPS bearings, the technology quickly becomes a routine resource. If, on the other hand, they have to spend a lot of time analyzing data, the vast majority of which is worthless, e.g. with acoustic room monitoring of a suspicious target who does not talk much, they will likely forego it. This explains why many of the highly developed technologies that the media describe are of little importance in everyday surveillance.

5.3.1. IMSI-catcher & Co.

As for the legendary IMSI-catchers, this technology is very expensive and specialized. A modern IMSI-catcher costs several hundred thousand euros and it can only be operated by highly paid specialists. In 2011, for example, the Berlin LKA budgeted 500,000 euros for the purchase of such a device. In order to use such an expensive device, there must be important reasons. This essentially applies to targets who work with several (sometimes unknown) cellphones or who are at least expected to do so, mostly in the fields of "international terrorism" and "organized crime". The BfV reports 10–15 deployments to the parliamentary control commission each year, with an upward trend; even if an unreported field is taken into account and other possible users such as the BKA and State authorities are included, "only" a double-digit number of deployments per year can be assumed. At least at this point in time, the worry of left activists that cellphones at demonstrations would be monitored by police IMSI catchers belongs to the realm of paranoia.[13]

The situation is similar with remote monitoring methods such as directional microphones and "Tempest". The technology is complex and prone to failure. It cannot be integrated into normal everyday surveillance because specialists have to be called in. In addition, detailed information about the target and their communication and movement behavior must be available and even bad weather can spoil all plans.

That is not to say that such techniques are irrelevant. Some specialty techniques will become routine in the next few years. This is mainly due to the fact that the transmission rates of digital data are increasing rapidly from year to year—so it is gradually becoming

[12] *N.T.P. note:* TEMPEST is a U.S. National Security Agency specification and a NATO certification referring to spying on information systems through leaking emanations, including reconstructing the image displayed on a computer screen from its unintentional signal radiation.

[13] *N.T.P. note:* Unfortunately, this is no longer true. In at least one recent case in Europe, cops used IMSI-catchers to monitor hundreds of cell phones during a demonstration. They then requested hundreds of corresponding names from phone providers, to try to establish links between those individuals.