4. Unsere eigene Sicherheit

Spuren

Etwas Wichtiges vorweg: Wir wollen in diesem Kapitel keine Panik verbreiten! Beschäftigt mensch sich mit dem Thema Spuren, kann schnell der Eindruck entstehen, dass eigentlich gar nichts mehr möglich ist, ohne Spuren zu hinterlassen. Die militante Praxis der letzten Jahre zeigt jedoch, dass eine Menge möglich ist und Ermittlungserfolge auf Seiten der Bullen eher selten sind. Also lasst euch nicht abschrecken und seid vorsichtig! Das Wissen um die Möglichkeiten der Gegenseite und entsprechendes Handeln oder Vorsicht sind die wichtigsten Tugenden, um sich einer Verfolgung durch Bullen und Justiz zu entziehen.

Eine Spur kann alles sein, wie winzig oder unauffällig auch immer. Jede Umweltveränderung hinterlässt Spuren. Keine Spuren zu verursachen ist unmöglich. Daher geht es darum, so wenig Spuren wie möglich zu hinterlassen. Und es geht darum, dafür zu sorgen, dass Spuren nicht zu euch zurückzuverfolgen sind. Daher sollte hier nicht an Kosten und Aufwand gespart werden. Handschuhe und andere Aktionsmittel sowie Werkzeuge sollten immer neu gekauft und nur einmal verwendet werden.

Spuren werden von den Bullen direkt am Aktionsort, an verdächtigen Personen und in den von diesen genutzten Räumen gesucht (Wohnung, Arbeitsplatz etc.). Es reicht also nicht aus, nur die Spuren am Ort eurer Aktion im Blick zu behalten. Ihr könnt Spuren nicht nur zurücklassen, sondern auch mitbringen. Ein Beispiel ist Sand oder Staub. Deren Zusammensetzung kann durch kriminaltechnische Labors ziemlich genau analysiert und zugeordnet werden. Wenn ihr also Schlamm von einem Feldweg an euren Sohlen mit zu euch nach Hause bringt, ist nachvollziehbar, dass ihr auf diesem Feldweg spazieren gegangen seid. Gerade solche feinen Spuren verwischen schnell. Durch einen Zufall kann aber genug von einer Spur übrig sein, um eine Verbindung zu euch zu rekonstruieren. Diese kann dann als Indiz für eure Beteiligung an einer Aktion ausgelegt werden. Leichter ist das noch mit Glas- oder DNA-Spuren, also allem, was nicht schnell verrottet. Wenn ihr etwas am Aktionsort absichtlich zurücklasst, könnt ihr sicher sein, dass dies besondere Aufmerksamkeit auf sich zieht. Gleiches gilt für Bekenner_innenschreiben oder Reste eures verwendeten Materials, wenn sie den Bullen in die Hände fallen.

Die Sicherung und Analyse von Spuren ist zeit- und kostenintensiv. Nicht in jedem Fall wird das ganze Repertoire an kriminaltechnischen Spielereien angewendet. Meistens gilt hier: Je größer der Schaden oder die Aufmerksamkeit, um so mehr wird darin investiert, euch zu finden.

Aber es gilt auch hier zu bedenken, dass kriminaltechnische Methoden stetig weiterentwickelt und bereits eingeführte Methoden standardisiert und vermehrt eingesetzt werden. Was wir heute an Vorsichtsmaßnahmen für übertrieben halten, kann in Zukunft vielleicht nicht mehr genug sein. Ein gutes Beispiel für eine solche Entwicklung ist die DNA-Analyse. Diese verhältnismäßig neue Ermittlungsmethode hat vor 30 Jahren noch kaum jemand vorausgesehen, wodurch natürlich auch nicht auf die Vermeidung von DNA-Spuren geachtet wurde. Wie sich aktuell am Beispiel des 1977 vom RAF-Kommando Ulrike Meinhof erschossenen Generalbundesanwalt Buback zeigt, können bei entsprechendem politischen Druck neuartige Analysemethoden dazu führen, einmal gefundene Spuren nach Jahrzehnten erneut zu untersuchen. Auf diese Weise zeigt der Staat, dass er nicht vergisst und versucht vielleicht auch heutige Aktivist_innen abzuschrecken.

Neben der Problematik, dass alte Spuren durch neue Methoden zu neuen Ermittlungen führen können, können auch neue Methoden durch Weiterentwicklung und Standardisierung immer preisgünstiger und häufiger angewandt werden. Die Hemmschwelle, DNA-Proben als angeblichen Beweis zu benutzen und in immer niedrigschwelligeren Bereichen der Kleinstkriminalität aufgrund vager Verdachtsmomente heranzuziehen, sinkt und auch die für Analysen notwendige Menge an gefundenem Erbmaterial hat sich bereits verringert.

Zusätzlich können rechtliche Rahmenbedingungen kippen, wie z.B. das Verbot, Rückschlüsse auf bestimmte körperliche Eigenschaften oder Krankheiten in den BKA- und LKA-Datenbanken zu speichern; erlauben sie doch heute schon eine Speicherung der biologischen Geschlechtszugehörigkeit.

Natürlich können wir hier nur versuchen, das Thema Spuren in Bezug auf heutige kriminaltechnische Methoden darzustellen. Wir finden es jedoch wichtig, die stetige Weiterentwicklung kriminaltechnischer Ermittlungsmethoden mitzudenken, wenn wir sie schon nicht voraussehen können. Technisch neuartige Methoden werden oft vor der faktischen Nutzung überlegt, diskutiert und ins Spiel gebracht. (Dass sie dann auch vor ihrer Legalisierung angewandt werden, steht auf einem anderen Blatt...) Insofern finden wir es wichtig, kriminaltechnische Entwicklungen im Blick zu behalten und sich gegenseitig darüber zu informieren, indem wir sie in unseren Medien thematisieren.

Ausgespart bleiben in diesem Kapitel Telefon und Internet. Hier nur ganz kurz: Für uns ist es selbstverständlich, dass keine Telefone bei Aktionen und ihrer Vorbereitung dabei sind. Mit ihnen können Bewegungsprofile erstellt werden und sie können als Wanzen benutzt werden. Außerdem stecken sie voller Informationen über euch und eure sozialen Kontakte. Jeder Klick im Internet hinterlässt mehrere Spuren auf dem Rechner, an dem ihr sitzt, auf dem Server, auf den ihr zugreift, und auf allen Servern danach und davor. Manche dieser Spuren lassen sich vermeiden oder kontrollieren, aber das ist ein Kapitel für sich.

Wir können hier keine vollständige Liste von möglichen Spuren geben. Deshalb ist es wichtig, dass ihr selbst alle Schritte durchdenkt und euch überlegt, wo ihr Spuren hinterlasst.

Dass es die 100%ige Sicherheit nicht gibt, wird von den Bullen genutzt, sich als allmächtig darzustellen. Die Funktion von Spurensicherung und kriminaltechnischer Ermittlung ist immer auch eine psychologische. Es geht darum, euch mit den Spurenfunden glauben zu machen, die Bullen hätten euch schon überführt. Damit erpressen sie Geständnisse. Oft sind selbst bei eindeutigen Spuren diese nur Indizien und noch keine Beweise für eure Beteiligung an einer Aktion. Für eine Verurteilung braucht es aber in der Regel mehr als nur Indizien. Also gerade auch, wenn die Bullen euch vorhalten, sie hätten genug gegen euch in der Hand, gilt: Anna und Arthur halten das Maul!

Fingerabdrücke

Fingerabdrücke sind der Klassiker der Kriminalistik. Sie sind die Spuren, die der dünne Film von Säure, Fett und Schmutz auf unseren Fingerkuppen auf Objekten hinterlässt. Erfasst werden von den Bullen auch die Abdrücke der gesamten Hand inklusive Handfläche. Sie gelten als individuelles Merkmal. Die Abnahme von Vergleichsproben gehört zum Standard jeder Erkennungsdienstlichen Behandlung (ED). Sie werden immer noch häufig mit Tinte und Papier erhoben. Scanner, die sie direkt digitalisieren und in die entsprechenden Datenbanken einspeisen, setzen sich aber zunehmend durch. Mittlerweile kommt hinzu, dass der Staat schon ein Auge auf das neue Verfahren zur Passerstellung geworfen hat. Dieses neue Verfahren macht die Abgabe eines Fingerabdrucks für den Erhalt eines Passes zwingend. Wie sich das auf die polizeiliche Praxis auswirkt, bleibt abzuwarten. Die Fingerabdrücke aus den ED-Behandlungen werden in Datenbanken wie AFIS (Automatisiertes Fingerabdruckidentifizierungssystem) gespeichert. Diese Datenbanken gleichen eingespeiste Spuren aus aktuellen und aus älteren Fällen ab.

Das beste Mittel gegen Fingerabdrücke ist, sie konsequent zu vermeiden. Dies bedeutet, alle Gegenstände, die den Bullen in die Hände fallen können, nicht mit bloßen Händen anzufassen und sich nicht nur auf die eigene Fähigkeit sie zu reinigen zu verlassen. Fingerabdrücke gehören zu den widerstandsfähigsten Spuren. Sie werden oft unbedacht hinterlassen und können jahrelang erhalten bleiben. Selbst an Gegenständen, die über Jahre im Wasser gelegen haben, können unter bestimmten Bedingungen Fingerabdruckspuren gesichert werden. Nahezu jedes Material kann Träger von Fingerabdrücken werden. Dies führt zu unterschiedlichen Gegenmaßnahmen. Immer zu empfehlen ist eine gründliche Reinigung mit Hilfe fettlösender Mittel (wie alkoholhaltigen Reinigungsmitteln). Am einfachsten zu reinigen sind Glas/Kunststoffoberflächen, hier reicht gründliches Abwaschen und intensives Abwischen der Oberflächen mit alkoholhaltigen Reinigungsmitteln oder, bei gründlicher Anwendung, auch Spülmittel. Zwingend wird der Einsatz von oberflächenverändernden Mitteln wie Stahlwolle (also Topfkratzer) beim Entfernen von Fingerabdruckspuren auf Metalloberflächen. Da die Abdrücke leicht säurehaltig sind, ätzen sie sich ins Metall. Es ist den Bullen möglich, je nach Aufwand, die Fingerabdrücke mit Hilfe von Laser wieder sichtbar zu machen. Dagegen ist das Zerkratzen der Oberflächen durch Stahlwolle oder Schleifpapier eine der besten Möglichkeiten. Für unlackiertes Holz gelten ähnliche Maßstäbe wie für Metall. Mit lackiertem Holz kann ähnlich wie mit Kunststoffoberflächen umgegangen werden. Stoffe sind zwar schlechte Träger für Fingerabdrücke, können jedoch auch Spuren aufweisen und tragen dafür umso besser DNA. Passt auf, was ihr am Ort des Geschehens zurücklasst!

Wenn ihr ein Papier mit euren Fingern berührt habt, dann solltet ihr es sauber kopieren und vernichten, denn es ist nicht möglich, es zu reinigen. Beim Kopieren von Texten solltet ihr immer darauf achten, dass ihr die Kopien niemals direkt mit euren Händen berührt. Da es oft unnötige Aufmerksamkeit erregt, mit Handschuhen im Kopierladen zu stehen, solltet ihr einfach ein paar Leerkopien vor und nach dem Text machen, den ihr sauber halten wollt. Den Papierstapel fasst ihr dann nur von außen an und legt ihn zum Beispiel in eine neue Mappe. Kopiert diese Texte nicht in einem Kopierladen, in dem ihr bekannt seid. Nutzt Verkleidungen, da es den Bullen möglich sein kann, zurückzuverfolgen, auf welchem Kopierer die Kopien entstanden sind (für Kopierer gilt das gleiche wie für Laserdrucker, siehe auch „Schriftspuren"). Kopierer verfügen mittlerweile über einen eigenen Arbeitsspeicher und dieser ist nicht nach ein paar weiteren Kopien schon überschrieben. Es gibt immer noch die Theorie, dass mehrfaches Vergrößern und Verkleinern auf verschiedenen Kopierern individuelle Kopiererspuren verwischt. Wir sind uns nicht sicher, ob dies eine wirklich sichere Methode ist. Sie kann aber auf jeden Fall der Spurensicherung die Arbeit erschweren. Viele Kopierläden zu betreten, birgt aber auch das Risiko, dass sich mehr Menschen an euch erinnern können und die Wahrscheinlichkeit steigt, von irgendeiner Überwachungskamera zum Beispiel im Kopierladen aufgenommen und gespeichert zu werden. Auch Werkzeuge wie Schreibmaschinen, auf denen für die Bullen interessante Texte getippt wurden, sollten nicht mit bloßen Händen angefasst werden, da darauf auch nach Jahren Fingerabdrücke auffindbar sind.

Das einfachste und sicherste Mittel zur Vermeidung von Fingerabdrücken sind Handschuhe. Doch auch hier ist einiges zu beachten: Gummihandschuhe reißen leicht und in ihrem Inneren, wie auch am Einschlupf bleiben Abdrücke zurück. Dünne Latexhandschuhe können die Fingerstrukturen durchdrücken. Eine Möglichkeit ist, zwei Paar übereinander anzuziehen oder Küchenhandschuhe mit Profil zu benutzen. Demgegenüber haben Stoffhandschuhe den

Vorteil, dass auf ihnen nur schwer Fingerabdrücke zurückbleiben. Grobmaschige Handschuhe können jedoch gerade bei intensiver Benutzung Löcher bekommen. Deshalb sollten keine gestrickten Handschuhe verwendet werden. Stoffhandschuhe nehmen auch wesentlich mehr Staub- und DNA-Spuren auf als Gummihandschuhe. Sie sind praktisch nicht mehr zu reinigen. Lederhandschuhe sind relativ teuer und müssen, wie andere Handschuharten auch, nach Aktionen entsorgt werden. Das ist in unseren Augen ein entscheidender Nachteil. Es sollte aber generell bedacht werden, dass in den Handschuhen, auch innen Spuren zurückbleiben. Handschuhe, die bei einer Aktion benutzt wurden, müssen unserer Meinung nach immer weggeworfen werden. Denn allgemein bleiben an den Handschuhen Spuren zurück, die oftmals auch einer bestimmten Aktion zugeordnet werden können. Außerdem hinterlassen Handschuhe am Aktionsort individuelle Spuren des Profils oder von kleineren Unregelmäßigkeiten durch Abnutzung (siehe Materialspuren). Bei Hausdurchsuchungen sind die Bullen oft besonders auf solches Material aus.

Es gibt weitere Mittel zur Vermeidung von Fingerabdrücken, gerade wenn nicht offensichtlich Handschuhe getragen werden können. Eines dieser Mittel ist das Auftragen und Trocknenlassen einer dicken Schicht Sprühpflaster auf die Finger. Ein weiteres Mittel ist sich normale Pflaster um oder auf die Fingerspitzen zu kleben. Beide Methoden halten wir für nicht hundertprozentig sicher und sehen in ihnen höchstens eine Möglichkeit, Spuren zu verringern.

Eine neuartige Methode, die zur Zeit in den USA erprobt wird, ermöglicht die Analyse der chemischen Zusammensetzung von Fingerabdrücken. Durch die Analyse lassen sich Drogen, Sprengstoff und bestimmte Stoffwechselprodukte bestimmen und nachweisen. Sie lassen Rückschlüsse auf mögliche „Täter_innen" zu. Das Analyseverfahren ist schnell und kann direkt vor Ort eingesetzt werden. Bisher wird es zwar noch nicht für die Spurenermittlung eingesetzt - dies ist jedoch nur eine Frage der Zeit.

DNA-Spuren

Ein in den letzten Jahren immer wichtiger gewordenes Thema in der Auseinandersetzung mit Repression sind DNA-Spuren. Die Repressionsorgane haben ein hohes Interesse daran, einerseits ihre Unvermeidbarkeit und andererseits ihre Eindeutigkeit zu betonen.

Sicher sind DNA-Spuren oft nur mit größerem Aufwand zu vermeiden und aufgrund ihrer häufigen annähernden Unsichtbarkeit für uns kaum zu entdecken. Andererseits werden DNA-Spuren am Ort des Geschehens oft als unumstößlicher Beweis angesehen. Wie diese Spuren an einen Ort kamen, wird dabei oft kaum berücksichtigt. So kann eine Decke, mit der Werkzeug zugedeckt war, die DNA Spuren einer Person übertragen, die vor Jahren darin geschlafen hat.

DNA-Spuren sind unmöglich zu vermeiden. Und sie verrotten einfach nicht. Es werden jetzt, Jahrzehnte später, noch Fälle anhand früher gesammelter DNA-Spuren neu aufgerollt. DNA-Spuren werden durch Blut, Haare, Spucke, Urin und Hautzellen hinterlassen. Also durch alles, was aus eurem Körper kommt und von ihm abfällt. Aber: Nicht jede Spur reicht schon für einen DNA-Vergleich. Für die Laboruntersuchung wird momentan noch eine gewisse Menge an DNA-Material gebraucht, am besten sind eine oder mehrere intakte Zellen. Hier wird die Technik aber immer mehr verfeinert.

DNA-Analysen sind teuer. Das heißt, sie werden nicht in jedem Fall angeordnet. Es gilt wohl auch hier meistens: Je größer der politische oder wirtschaftliche Schaden, um so mehr technischer Aufwand wird betrieben. Das kann sich aber in nächster Zeit durchaus ändern. Es wird an billigeren Tests geforscht, DNA-Analysen sollen als Standard durchgesetzt werden. Eine DNA-Datenbank wird seit Jahren gefüllt.

Relativ leicht kann durch DNA das Geschlecht zugeordnet werden. Um die Spur darüber hinaus auswerten zu können, brauchen die Bullen eine Vergleichsprobe von euch. Solche werden entweder bei einer Erkennungsdienstlichen Behandlung (ED) beschafft oder am Arbeitsplatz, bei Hausdurchsuchungen etc. von persönlichen Gegenständen wie Kämmen abgenommen. Es ist auch schon vorgekommen, dass die Bullen diese Proben Verwandten der Beschuldigten abpressen wollten, da deren DNA ähnlich sei. Proben solltet ihr nie freiwillig abgeben, gerade auch, wenn ihr unterwegs aufgegriffen werdet. Protestiert und legt Widerspruch ein, unterschreibt nichts! In einigen Fällen konnte die DNA-Abgabe mit Hilfe von Anwält_innen verhindert oder zumindest herausgezögert werden.

Da es schwer ist, DNA-Spuren zu vermeiden, geht es darum, sie zu minimieren. Das fängt damit an, dass ihr nicht in der Nähe eures Aktionsortes nochmal pissen geht oder eine Zigarette mit eurer Spucke dran liegen lasst. Am besten ist, ihr raucht einfach gar nicht bei einer Aktion.

Haarspuren vermeidet ihr durch Mützen und Sturmhauben. Lange Klamotten, auch im Sommer, verringern das Abfallen von Hautpartikeln und kleinen Haaren etwas. Ein Mundschutz hilft gegen Speichel und Nasenschleim.

Wenn ihr Werkzeug und Tragetaschen mitnehmt, die ihr vorher bei euch zu Hause hattet, achtet darauf, dass sie nicht nur frei von Fingerabdrücken, sondern auch von Haaren und Hautzellen bleiben. Sie können prima als DNA-Transporter funktionieren. Das kann auch für eure Kleidung und Schuhe gelten. Bewahrt alles, was ihr zur Aktion mitnehmt, am besten jeweils getrennt in sauberen Behältern auf, zum Beispiel in nicht benutzten Mülltüten. Ihr solltet grundsätzlich vermeiden, wichtige Aktionsmaterialien bei euch zu Hause zu lagern. Auch Haare von euren Haustieren können hinterher zugeordnet werden.

Gerade verschickte Bekenner_innenschreiben werden oft nach DNA-Spuren untersucht. Diese können sich am Papier, am Briefumschlag und an der Briefmarke befinden. Besonders gut lässt sich übrigens der Speichel an der Klebefläche von Briefumschlägen analysieren, weil er konserviert wird.

Bei der Herstellung von allen Dingen, die in die Hände der Bullen gelangen können, wie Briefe und Reste eures Aktionsmaterials, solltet ihr unbedingt das Risiko, DNA-Spuren zu hinterlassen, minimieren (siehe Mischkasten und Reinraum).

Möglichkeiten für die Schaffung eines sauberen Arbeitsplatzes

Für bestimmte Arbeiten ist es sinnvoll, einen weitgehend DNA-freien Reinraum einzurichten. Dieser Raum hat sowohl die Funktion, eure Spuren am Objekt zu verringern, als auch - soweit möglich - zu verhindern, dass eure Spuren im Raum der Aktionsvorbereitung zurückbleiben. Dies ist sicher aufwändig und nicht ganz billig, letzten Endes müsst ihr aber selber einschätzen, wie sicher ihr gehen wollt. Bedenkt bei der Abwägung der Sicherheitsvorkehrungen neben Aktionslevel, Ermittlungsdruck, drohender Repressalien und eurem eigenen Sicherheitsbedürfnis auch, mit welcher Wahrscheinlichkeit ein Arbeitsobjekt in die Hände der Behörden gelangt. So kann mensch z.B. sicher sein, dass bei der Presse eingehende Bekenner_innenschreiben früher oder später bei den Bullen landen.

Die nachfolgende Beschreibung mag vielen extrem erscheinen und sicherlich sind nicht für jede Arbeit alle nachfolgenden Sicherheitsvorkehrungen notwendig. Wir finden es jedoch angesichts der rasant fortschreitenden Entwicklung im Bereich der DNA-Analyse wichtig, sich der Probleme und Gefahren bewusst zu werden, die damit zusammenhängen. Sucht euch die Vorkehrungen raus, die euch für eure Aktion notwendig erscheinen und lasst euch nicht abschrecken!

Um einen solchen Raum einzurichten, müsst ihr euch vor dem ersten Betreten des Raumes mit Schutzkleidung ausstatten, die möglichst verhindert, dass DNA-Spuren in den Raum gelangen. Dazu könnt ihr originalverpackte(!) Overalls aus dem Baumarkt nehmen, die relativ günstig zu bekommen sind. Zieht sie an und setzt eine möglichst ungetragene Sturmhaube auf und zieht die Kapuze des Overalls darüber. Zur Bedeckung der Haare eignen sich auch Badekappen gut, da sie noch undurchlässiger sind und die Haare nicht einfach durchpiksen können. Als Nächstes steckt ihr jeden Fuß in einen Müllsack und klebt den Sack am Bein des Overalls dicht mit Klebeband fest. Dann zieht ihr euch Gummihandschuhe mit Profil an und klebt diese an den Ärmeln abschließend zu. Zieht euch eine Staubmaske aus dem Baumarkt möglichst vor den Mund, um Speicheltropfen auf dem Werkstück zu vermeiden und setzt euch eine Schutzbrille auf, die auch die Augenbrauen mit einschließt. Ihr solltet immer zu zweit arbeiten und gegenseitig darauf achten, dass keine freien Hautflächen zu sehen sind.

Als Arbeitsraum wählt möglichst einen Ort, an dem eure Haare und Hautzellen nicht ohnehin schon umher fliegen. Der Ort sollte auch frei von Haaren eines Hundes, einer Katze oder sonstiger tierischer Gesellen sein, die als euer Haustier zugeordnet werden könnten. Benutzt den Keller oder die Garage von Freund_innen (die nicht politisch aktiv sind). Oder mietet ein Zimmer in einem Hotel oder über die Mitwohnzentrale. Nun richtet euch einen sauberen Arbeitsplatz ein, am besten verwendet ihr eine Plane oder stellt, falls ihr ganz sichergehen wollt, ein unbenutztes Zelt im Raum auf. In diesem Zelt bleiben die Spuren eurer Arbeit zumindest weitgehend drin und ihr könnt es danach sicher entsorgen.

Bei der Arbeit solltet ihr verschiedene Müllsäcke parat haben und den Müll nach Gefährlichkeit für euch trennen (also z.B. Abfälle von Bauteilen in den einen, die Verpackung von Frischhaltebeuteln in den anderen etc.). Bei der Mülltrennung solltet ihr auch überlegen, welche Verpackungen z.B. eure Fingerabdrücke tragen und welche nicht. Selbstverständlich hat keiner dieser Säcke etwas in eurem Hausmüll verloren.

Seid euch bewusst darüber, dass die Arbeit in dieser Kleidung sowohl schweißtreibend als auch anstrengend ist und denkt falls nötig an Ablösung oder Arbeitsteilung, denn Arbeitsunterbrechungen bedeuten, sich nochmal neu einkleiden zu müssen. Denkt daran, euch nicht am Kopf oder Gesicht zu kratzen, während ihr Handschuhe anhabt. Eine sinnvolle Arbeitsteilung ist z.B., dass eine Gruppe den Reinraum vorbereitet und die andere ihn dann zum Arbeiten betritt. Bewahrt fertiggestellte Bauteile oder Objekte in Gefrierbeuteln oder neuen Tupperware-Behältern auf.

Beim Anziehen der Schutzkleidung sowie bei jedem Arbeitsschritt solltet ihr bedenken, an welchen Objekten eure DNA-Spuren eventuell haften. Wenn ihr z.B. alles in Verpackungen gekauft habt, habt ihr diese vermutlich ohne Handschuhe angefasst und ihnen haften nun vielleicht Hautzellen an. Fasst ihr die Verpackungen mit euren sauberen Handschuhen an, können die Spuren von der Verpackung auf eure Handschuhe und von dort auf eure Arbeitsobjekte gelangen. Um dies zu verhindern, ist ein sehr diszipliniertes Arbeiten und mehrmaliger Handschuhwechsel notwendig. Am besten zieht ihr dafür über die festgeklebten Handschuhe ein weiteres Paar.

Eine weitere Möglichkeit, um die Spurenproduktion zu verringern, ist die Anfertigung eines Mischkastens
(aus: RZ - Handbuch für den Widerstand)

Dafür könnt ihr einen großen Pappkarton nehmen, der nach oben offen ist. Aus der längeren Seite schneidet ihr zwei Löcher für eure Arme aus. Durch diese Löcher werden dann zwei lange Gummihandschuhe gesteckt und ihre Enden außen am Karton festgeklebt. Jetzt braucht ihr zwei große Plastikdosen mit Deckel, sägt deren Böden ab und klebt sie an diesen Stellen mit Isolierband zusammen. Diese Röhre, die an beiden Enden mit Deckeln verschlossen ist, schiebt ihr bis zur Hälfte durch ein Loch, welches ihr in die kürzere Seite des Kartons geschnitten habt. (...)

Ergänzung: Für unsere Zwecke kann der Kasten nun mit durchsichtiger Frischhaltefolie oben zugeklebt werden. Wichtig ist, dass ihr bei der Herstellung des Mischkastens möglichst ebenfalls darauf achtet, spurenfrei zu arbeiten. Auch Karton und Zutaten sollten spurenfrei sein. Der Vorteil des Mischkastens ist wie bei der Verwendung eines Zeltes, dass die Materialspuren, die am Arbeitsplatz hinterlassen werden, dadurch stark reduziert werden.

Künstliche DNA

Ein neueres Verfahren zur Abschreckung und Verfolgung von z.B. Dieben ist die künstliche DNA. Für linke Aktivist_innen ist sie zur Zeit vielleicht weniger bedeutsam, aber wer weiß, was die Zukunft bringt? Die künstliche DNA ist wie die menschliche DNA einmalig und eindeutig zu identifizieren. Sie wird zusammen mit ebenfalls unverwechselbaren Mikroplättchen in eine klebstoffhaltige Trägerflüssigkeit gegeben, die unter UV-Licht violett leuchtet. Mit der Substanz können Wertgegenstände mit einem Pinsel bestrichen oder Gebäude mit sog. DNA-Duschen ausgestattet werden. Die Markierung von Gegenständen ist dauerhaft und gegen normales Putzen unempfindlich. Kommst du mit der Substanz in Berührung, bleibt sie für ca. sechs Wochen an dir haften. Das relativ neue Verfahren wurde Ende 2009 in Bremer Schulen, in zwei Wohnvierteln und an einigen Tankstellen als Pilotprojekt eingeführt. In Großbritannien und den Niederlanden wird das Verfahren schon länger angewandt.

Geruchsspuren

Eine neuere Entwicklung ist die Abnahme von Geruchsproben, wie z.B. bei den Razzien gegen mutmaßliche militante Gegner_innen des G8-Gipfels in Heiligendamm 2007. Zwar sind diese selbst laut BAW eher zweifelhaft, könnten aber einen Beitrag zur „Gesamtwürdigung" leisten. Vor allem aber sind sie einfacher zu erhalten als DNA-Proben.

Jeder Mensch verfügt nach wissenschaftlichen Erkenntnissen über einen einmaligen und unverwechselbaren Eigengeruch. Diese Geruchsspur, im Fachjargon als „odrologische Spur" bezeichnet, kann auch durch größte Reinlichkeit und Hygiene nicht vermieden werden.

Sie setzt sich aus verschiedenen Bestandteilen zusammen, hauptsächlich jedoch aus zersetzten Hautschuppen. Diese verliert der Mensch in jeder Sekunde, egal ob er irgendwo sitzt, geht oder steht. Bei der Zersetzung der Hautschuppen durch Bakterien entstehen Gase, welche eingesetzte Spürhunde durch ihre hochsensiblen Nasen wahrnehmen können. So sollen Körpergerüche mit am Tatort zurückgelassenen Duftmarken abgeglichen werden.

Schuhabdrücke

Ein oft unterschätztes Gefahrenpotenzial bieten Schuhabdrücke. Sie sind genauso individuell wie Fingerabdrücke und von ihnen können Rückschlüsse auf Größe, Gewicht, Gangart etc. der verursachenden Person gemacht werden. Wird der Spuren verursachende Schuh bei einer Hausdurchsuchung gefunden, kann er, je nach Qualität der Spuren, relativ sicher identifiziert werden. Am Schuh zurückgebliebene Erdspuren oder Pflanzenreste tun ihr Übriges. Daher ist es empfehlenswert, die Schuhe nach einer Aktion zu entsorgen, besonders wenn über Schnee, Erde etc. gegangen wurde.

Aber nicht nur die Marke des Schuhs hinterlässt Spuren, sondern auch die Art, wie Schuhe abgelaufen worden sind, ist individuell. Alle von einer Person getragenen Schuhe weisen die gleiche Art von Abnutzung auf. Wenn Fußabdrücke in der Erde oder im Schnee hinterlassen wurden, fertigen die Bullen einen Gipsabdruck an. Mit Hilfe dieses Abdrucks sind sie oft nicht nur in der Lage, den Schuh zu identifizieren, der diesen Abdruck produziert hat, sondern auch anhand der Art, wie sich die Abnutzung des Schuhs im Abdruck widerspiegelt, andere Schuhe des_der Verdächtigen diesem Abdruck zuzuordnen. Benutzt also besonders bei Aktionen, bei denen ihr über weiche Oberflächen gehen müsst, keine alten abgetragenen Schuhe von euch.

Kauft euch kurz vor einer Aktion Billigschuhe und werft sie danach weg, wenn ihr wirklich sicher gehen wollt. In von euch benutzten Schuhen befinden sich aber mit Sicherheit DNA-Spuren. Deshalb entsorgt diese auf keinen Fall in der Nähe des Aktionsortes.

Ein weiteres Mittel, den Bullen die Arbeit zumindest etwas schwerer zu machen, ist, sich Socken über die Schuhe zu ziehen. Dies verschleiert die Marke und das Profil des Schuhs und kann auch als Schutz bei Kameraüberwachung dienen. Probiert aber vorher mal aus, wie ihr damit laufen und rennen könnt.

Fahrzeugspuren

Die Wahl des passenden Fahrzeugs sollte gut durchdacht sein. Überlegt, ob ein Auto wirklich notwendig ist, weil es viele Risiken birgt.

Die Spuren, die Fahrzeuge hinterlassen, bestehen einerseits aus den Abdrücken von Autoreifen und andererseits, bei Unfällen, aus dem Lack des Autos. Spuren (besonders Lackspuren) eines Unfalls können sowohl am Auto als auch an der Unfallstelle gefunden werden. Sowohl aus den Reifenspuren, als auch aus Lacksplittern lässt sich der Typ des Autos ermitteln. Falls das Auto vorhanden ist, lässt es sich auch individuell identifizieren. Durch einen Reifenwechsel, möglichst vor und nach der Aktion, kann die Zuordnung der Reifenspuren erschwert werden. Alleine nach der Aktion die Reifen zu wechseln reicht nicht, da die Bullen die am Aktionsort aufgefundenen Reifenspuren evtl. mit Reifenspuren vor eurer Wohnung oder in eurer Garage abgleichen können. Achtet bei der Benutzung eines Autos auch auf auslaufendes Öl oder Wasser.

Das wichtigste individuelle Merkmal eines Autos ist jedoch bekanntlich das Nummernschild. Um wenigstens eine Kennzeichenabfrage ohne Kontrolle zu überstehen, können z.B. die Nummernschilder ausgetauscht werden. Da die meisten von uns nicht in der Lage sind, Dubletten von Nummernschildern anzufertigen, ist es sinnvoll, diese kurz vor der Aktion zu klauen. Wichtig ist, dass das Auto den gleichen Typ und die gleiche Farbe wie das bei der Aktion verwendete hat, denn normalerweise fragen die Bullen standardmäßig die Nummer eines Autos ab und bekommen dann von der Zentrale zurück, ob das Auto gestohlen ge-

meldet ist, die Farbe und den Typ. Wenn das alles übereinstimmt, sinkt die Wahrscheinlichkeit einer Kontrolle etwas. Einer richtigen Fahrzeugkontrolle werden diese geklauten Nummernschilder aber natürlich nicht standhalten.

Um für den Fall einer Kontrolle vorbereitet zu sein, solltet ihr Aktionsmittel gut verstecken und wenn möglich nicht im Kofferraum aufbewahren. Achtet auf die Verkehrssicherheit des Fahrzeugs. Warndreieck und Verbandskasten nicht vergessen.

Oft reicht es, die Nummernschilder mit einem Schraubenzieher herauszuhebeln oder, je nach Marke, die Schrauben zu lösen, um sie zu entfernen. Probiert es an einem ruhigen Ort erstmal entspannt aus. Die Nummernschilder könnt ihr dann z.B. mit doppelseitigem Klebeband (bei Regen aufpassen) an eurem Auto anbringen. So könnt ihr sie nach einer Aktion schnell wieder verschwinden lassen. Gerade bei Motorrädern kann auch das Verschmieren oder Abkleben von Nummernschildern helfen. Das geht allerdings zu Lasten der Unauffälligkeit. Diese Maßnahmen sind auch wegen der zunehmenden Überwachung durch Maut- und Verkehrsleitsysteme sinnvoll. Das Mautsystem wird teilweise zur automatischen Kennzeichenabfrage bei Fahndungen genutzt. Achtet auch darauf, welche Spuren sich in eurem Auto befinden könnten und versucht sie zu vermeiden, z.B. durch gute Verpackung der Aktionsmittel. Kaum zu vermeiden ist es unserer Meinung nach, dass DNA-Spuren von euch im benutzten Auto zurückbleiben. Das Auto ist nicht nur ein guter Spurenträger, sondern durch eventuell unter dem Auto angebrachte Peilsender auch leicht zu verfolgen. Deshalb sollte die Nutzung möglichst vermieden werden.

Eine gute Alternative können Fahrräder sein. Auch sie hinterlassen individuelle Reifenspuren, was oft vergessen wird. Es ist deshalb sinnvoll, das Fahrrad nicht in direkter Umgebung des Aktionsortes zu parken. Je nach Untergrund kann ein Mantelwechsel vor und nach der Aktion sinnvoll sein. Individuelle Merkmale wie Firmenaufkleber können einfach abgeklebt werden. Sicherlich kann ein auffällig gefärbtes Fahrrad auch leicht zum Blickfang werden. Wie bei Autos ist bei Fahrrädern außerdem, gerade wenn ihr nachts unterwegs seid, auf die Verkehrssicherheit zu achten.

Werkzeugspuren

Werkzeugspuren sind sehr vielfältig und für jedes Werkzeug unterschiedlich. Deshalb können wir hier nur ein paar grundsätzliche Dinge zu dem Thema schreiben. Als Werkzeugspuren definieren wir hier individuelle Spuren sowohl auf dem Werkzeug als auch auf dem „Werkstück".

Jedes Werkzeug ist durch kleine Unregelmäßigkeiten in der Produktion und durch Abnutzung im Gebrauch ein Unikat und lässt sich als solches identifizieren. Daraus folgt, dass jedes dieser Unikate einmalige Spuren auf einem bearbeiteten Gegenstand hinterlässt. Einem zerschnittenen Blatt Papier kann genau eine bestimmte Schere (die aber natürlich den Bullen vorliegen muss) zugeordnet werden. Liegt sie den Bullen nicht vor, kann bei mechanischen Werkzeugen, die in direkten Kontakt mit dem Werkstück kommen, meist nur der Typ bestimmt werden.

Das bedeutet für den sicheren Umgang, den Bolzenschneider, Schraubenzieher oder was auch immer nach einer Aktion zu entsorgen. Lasst alles verschwinden, was direkt mit dem Werkstück in Berührung kam. Leider reicht das allein noch nicht. Denn, um bei dem Beispiel von der Schere und dem Blatt zu bleiben, die Bullen können nicht nur ein Blatt einer bestimmten Schere zuordnen, sondern auch feststellen, ob zwei Blätter mit der gleichen Schere zerschnitten wurden. Wenn ihr also den Bolzenschneider, mit dem ihr einen Zaun aufgemacht habt, auch dafür verwendet, euer Hochbett zu bauen, dann können die Bullen das feststellen, selbst wenn das Werkzeug längst verschwunden ist.

Darum ist es nötig, das Werkzeug für eine Aktion neu zu kaufen, um sicher zu arbeiten. Es muss ja nicht immer das Beste und Teuerste sein.

Verbrauchsmaterial wie Klebeband, Seile, Kabel und deren Bruchstücke an Schnittstellen können einander zugeordnet werden. Ein kleines Bruchstück eines Kabels in eurer Wohnung, das zu einem Kabel im Besitz der Bullen passt, kann euch als starkes Indiz eine Menge Ärger einbringen.

Beim Arbeiten mit Klebeband oder Klebstoff müsst ihr ganz besonders auf Sauberkeit achten, denn Kleber fixiert Staub und DNA-Spuren.

Individuelle Spuren können aber auch an selbst hergestellten Werkzeugen, wie z.B. Brandsätzen, zu finden sein. Diese Spuren müssen nicht DNA oder Fingerabdrücke sein. Um zum Beispiel festzustellen, ob die gleiche Person einen Brandsatz hergestellt hat, reicht oft die Untersuchung von individuellen Merkmalen in der Art und Weise des Aufbaus. Jede_r interpretiert eine allgemeine, einfache Bastelanleitung unterschiedlich und setzt sie anders um. D.h. jede_r macht Knoten auf eine bestimmte Weise oder klebt etwas anders ab, benutzt eine andere Bauweise etc.. Diese Liste ist damit noch nicht abgeschlossen und individuelle Merkmale lassen sich sicher nicht ganz vermeiden, aber durch bewussten Umgang reduzieren. Schon ein Abwechseln innerhalb der Gruppe beim Bau von Aktionsmitteln macht es den Bullen schwerer, gerade bei nicht gezündeten Brandsätzen, diese einer Gruppe oder Person zuzuordnen und beugt außerdem der Spezialisierung Einzelner vor.

Das K.O.M.I.T.E.E. schrieb in seiner selbstkritischen Auflösungserklärung Ende 1995, dass die Bullen ihnen manche ihrer Aktionen nur deshalb so schnell zuordnen konnten, weil sie kontinuierlich den gleichen Zündertyp verwendeten. Deshalb ist die Entscheidung für oder gegen entsprechende Variationen eine Entscheidung, die von Zusammenhängen bewusst getroffen werden muss. Dies gilt auch für mögliche

Variationen in den für eine Aktion benutzten Chemikalien und, soweit es geht, deren Mischungsverhältnissen. Ebenso sollten nicht immer die gleichen Marken oder Bauteiltypen benutzt werden. Zu Zündertypen kann grundsätzlich gesagt werden, dass umso weniger Spuren zurückbleiben, je einfacher sie sind. Ein Molli ist am leichtesten sauber zu halten und ein chemischer Zeitzünder hinterlässt weniger Spuren als ein mechanischer oder elektrischer. Gerade bei elektrischen Zündertypen können auch Seriennummern auf Bauteilen zum Problem werden. Ingrid Strobl wurde Mitte der 80er Jahre ein Wecker zugeordnet, der bei einer Aktion der RZ verwendet wurde. Das passierte mit einer groß angelegten Aktion des BKA in Kaufhäusern. Da, laut BKA, die RZ immer denselben Weckertyp verwendeten, wurde dieser mit einer Seriennummer versehen und jede Person, die ihn kaufte, gefilmt. Dieses Verfahren bescherte zwei Menschen längere Untersuchungshaft und in einem 129a-Verfahren wurden linke Bewegungen eingehend durchleuchtet.

Deshalb ist auch bei der Auswahl der entsprechenden Mittel, wie etwa Wecker, Variation angebracht. Seriennummern von Weckern zu entfernen ist schwer, da sie oft unter fest verbauten Teilen liegen. Prägungen in Metall können zwar herausgefräst werden, sind aber dann von den Bullen wiederherstellbar, da der Prägestempel auch das darunter liegende Metall verformt. Prägespuren können nachhaltig nur durch Überprägen oder Ausmeißeln entfernt werden, da dabei wie beim ersten Prägevorgang die Struktur des ganzen Werkstücks verändert wird.

Brandspuren

Unabhängig davon, dass ihr immer damit rechnen müsst, dass ein Brandsatz nicht angeht und Spuren bleiben, solltet ihr beachten: Brände vernichten Spuren nicht vollständig. Sie hinterlassen präzise Hinweise über das verwendete Material, die Zündart und die Stelle, an der der Brand angefangen hat. Die Bullen können aus Rußspuren, den Gasen in der Luft an einem Brandort und auf welche Art und wie stark etwas verkohlt ist, eine ganze Menge rekonstruieren. Wichtig ist auch hier: Variation und möglichst einfache Mittel. Die Verwendung von zum Beispiel dem immer gleichen Gemisch Brandbeschleuniger oder der gleichen Zündart ist wie das Hinterlassen eines Autogramms.

Schriftspuren

Handschriften sind sehr individuell und gut zuzuordnen. Das geschieht anhand der Linienführung, den Punkten beim Auf- oder Absetzen des Stiftes und dem Druck auf das Schreibgerät. Kalender, Tagebücher, handschriftliche Briefe und selbst Einkaufslisten können als Schriftvergleichsproben verwendet werden. Auch die Farbe und Tinte des Schreibgerätes oder die Zusammensetzung der Bleistiftmine kann eine Spur sein.

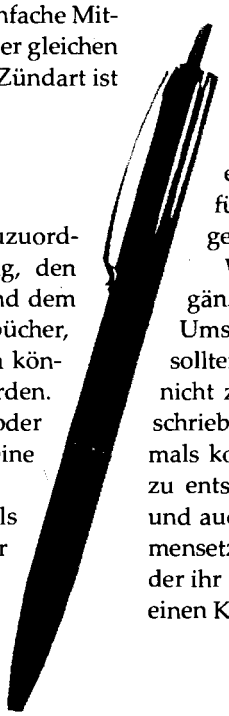
Blockschrift gilt als schlechter identifizierbar als Schreibschrift, da viele Eigentümlichkeiten in der Linienführung hier entfallen. Filz- und Fasermaler hinterlassen zwar auch individuelle Schreibmerkmale, wie die Handstellung oder den ausgeübten Druck, aber weniger als z.B. Kugelschreiber oder Füllfederhalter.

Denkt daran, immer auf festen Unterlagen zu schreiben. Die Schrift drückt auf das darunter liegende Material durch. Auf einem Block hinterlasst ihr nicht nur auf dem nächsten, sondern auch auf den nachfolgenden Blättern Spuren. Am besten eignen sich Glas oder Metall als Unterlage. Es versteht sich von selbst, dass mensch nichts Handgeschriebenes hinterlassen oder veröffentlichen sollte. Die Hinweise zur Handschrift sind aber vielleicht hilfreich für Mitteilungen untereinander oder ähnliches.

Grammatik, Rechtschreibung, Wortschatz, regionale Eigenarten und Dialekt können heute mit Hilfe von Computerprogrammen verglichen werden. Diese Untersuchungen sind nicht so eindeutig wie die Handschriftenanalyse. Aber sie werden immer mehr verfeinert. Das BKA hat eine Datenbank für Erpresser_innenbriefe und Anschlagserklärungen eingerichtet, die von den Bullen für den Vergleich genutzt wird. In einem Erpressungsfall wollten die Täter_innen durch Grammatikfehler verschleiern, dass sie muttersprachlich deutsch sprechen. Die Bullen konnten das jedoch dadurch rekonstruieren, dass schwierige Wörter richtig geschrieben waren.

Schreibt einfache Sätze, benutzt keine unnötigen Fremdwörter oder Spezialbegriffe aus eurem Berufsfeld. Variiert die Schreibweise von Jahreszahlen, Abkürzungen und ähnlich markanten Hinweisen. Entscheidet euch bewusst, ob ihr groß oder klein schreibt. Die Ermittlungen gegen angebliche mg-Mitglieder haben auch gezeigt, dass die Bullen inhaltliche Vergleiche zwischen Bekenner_innenschreiben anstellen. Schlagworte und selbst Parolen, die in anderen – sogar in öffentlich unterschriebenen – Texten auftauchen, dienen ihnen als Ermittlungsansatz, um in bestimmten Strukturen zu schnüffeln.

Lest eure Texte in der Gruppe gegen und wechselt euch beim Schreiben ab. Das verhindert nicht nur eine feste Arbeitsteilung, sondern dient auch eurem Schutz, denn jede_r hat ihren individuellen Schreibstil. Damit können die Texte im besten Fall nicht einer Person direkt zugeordnet werden.



Schreibt nur das Nötigste. Je kürzer, um so weniger Material liefert ihr den Bullen.

Auch das Papier ist eine Spur. Es kann verglichen und anderen Blättern aus demselben Block oder von derselben Papiersorte zugeordnet werden, ebenso wie ein verwendeter Klebstoff. Das gilt auch für Briefumschläge. Hebt nicht verwendete Umschläge nicht für das nächste Mal auf. Kauft lieber neue!

Wenn ihr Texte zu euren Aktionen verschickt, ergänzt zum Beispiel einen falschen Absender auf dem Umschlag. Das macht den Brief unauffälliger. Adressen sollten auf einem Drucker ausgedruckt werden, der euch nicht zugeordnet werden kann, mit Schreibmaschine geschrieben oder mit Stempel erstellt und am besten mehrmals kopiert werden. Denkt daran, alles hinterher sauber zu entsorgen. Briefmarken nicht mit Spucke (eure DNA) und auch nicht mit Leitungswasser aufkleben. Die Zusammensetzung des Leitungswassers kann auf die Region, aus der ihr kommt, Hinweise geben. Benutzt gekauftes Wasser, einen Klebstift oder am besten selbstklebende Briefmarken.

Erstellt immer mehrere Exemplare, falls eines verloren geht. Verwendet verschiedene Briefkästen, die weit voneinander entfernt liegen.

Viele benutzen als Alternative zum relativ unberechenbar speichernden Computer immer noch eine Schreibmaschine zum Verfassen ihrer Texte. Aber auch Schreibmaschinen hinterlassen Spuren auf dem Papier und so können auch nach dem Kopieren Texte einer bestimmten Schreibmaschine zugeordnet werden. Aus dem Farbband ist oft der geschriebene Text reproduzierbar und auch auf der Walze können Spuren der letzten geschriebenen Seiten gefunden werden. Die Typen einer Schreibmaschine sind so eindeutig wie jedes andere Werkzeug. Die Identität von Schrift und Schreibmaschine lässt sich ohne größeren Aufwand feststellen. Also benutzt keine Schreibmaschine, auf der ihr vorher einen Brief an Oma geschrieben habt.

Das Risiko der Wiedererkennung der Schrift kann auch hier durch Größer- und Kleinerkopieren minimiert werden. Darunter leidet aber oft auch die Druckqualität. Für Schreibmaschinen gilt das gleiche wie für alle anderen Werkzeuge: kaufen, verwenden und wegwerfen. Das kann auf Dauer relativ teuer werden, minimieren lassen sich die Kosten durch den Kauf gebrauchter Schreibmaschinen (nicht aus linken Zusammenhängen!). Um Spuren einzuschränken, können auch elektrische Schreibmaschinen mit wechselbarem Typenrad verwendet werden, allerdings bleiben Spuren auch auf anderen Teilen einer Schreibmaschine zurück.

Zunehmend werden Computer ohne Festplatte z.B. mit dem auf Linux basierenden Betriebssystem Knoppix verwendet. Hier soll aber kurz auf Probleme mit dem Ausdrucken eingegangen werden. Drucker hinterlassen Spuren, euer Drucker zu Hause scheidet für solche Arbeiten also aus. Zumindest bei Farblaserdruckern ist bekannt, dass sie ihre Seriennummer im ausgedruckten Text verstecken. Ob dieses Problem auch Kopierer betrifft, wissen wir zwar nicht, es sollte jedoch damit gerechnet werden. Habt das im Kopf, wenn ihr irgendwo etwas ausdruckt! Das gleiche Problem besteht auch bei CD- und DVD-Brennern. Sie brennen die Seriennummer des Gerätes, also ein eindeutiges Merkmal, mit auf die CD. (Ausführliche Informationen findet ihr im 5. Kapitel „Sicher schreiben lernen am Computer".)

Materialspuren

Wir meinen mit Materialspuren alle Spuren, die unbeabsichtigt an euch, eurer Kleidung oder in genutzten Räumlichkeiten zurückbleiben. Auch hier kann es für uns keine hundertprozentige Sicherheit geben, aber wir können den Bullen zumindest die Arbeit erschweren.

Anfangen wollen wir hier mit den Spuren, die an eurer Kleidung haften. Auch wenn ihr sie nicht sehen könnt, trägt eure Kleidung viele Spuren mit sich, die nicht unbedingt durch Waschen zu entfernen sind. Je nach Art der Aktion sind diese für die Bullen unterschiedlich verwertbar. Wenn ihr sprühen geht, könnt ihr euch sicher sein, dass, auch wenn ihr es nicht seht, feinste Farbpartikel an eurer Kleidung, besonders an Hose und Schuhen zu finden sind. Die Bullen können diese Partikel mit einer Speziallampe zum Leuchten bringen. Diese Lampe ist keine Spezialtechnik, die nur dem BKA zugänglich ist, sondern ist auf jeder Wache vorhanden. Sicherlich verlieren diese Farbspuren oft mit zunehmender zeitlicher Entfernung zur Aktion ihre Relevanz, entfernen lassen sie sich jedoch nicht mehr.

Ebenso wenig lassen sich die feinen Glaspartikel entfernen, die beim Einschlagen einer Scheibe entstehen. Diese Partikel können leider auch noch einer bestimmten Scheibe nach Art des Bruchs zugeordnet werden. Auch hier hilft das Waschen der Kleidung wenig. Blutflecken sind kaum oder nur schwer zu entfernen und hinterlassen Rückstände in Stofffasern. Sie bleiben nachweisbar. Das Entsorgen eurer Aktionskleidung ist oft der einzige Weg, möglichst spurenfrei zu bleiben. Abhilfe kann ein einfacher günstiger Overall aus dem Baumarkt schaffen. Den könnt ihr nach der Aktion schnell ausziehen und unter ihm unauffällige Kleidung tragen. Übt aber auf jeden Fall das Ausziehen vorher und schneidet, falls nötig, die unteren Enden der Hosenbeine etwas auf, damit ihr ihn über die Schuhe bekommt. Entsorgt ihn auf keinen Fall in der Nähe des Aktionsortes, da er mit Sicherheit zumindest DNA-Spuren von euch trägt. Zum Thema Schuhe und Bodenspuren haben wir weiter oben schon einiges gesagt.

Alle Kleidung, die ihr tragt, hinterlässt Spuren an euch. Das ist besonders wichtig, wenn ihr Handschuhe tragt, da die Bullen anhand von Faserspuren, zum Beispiel unter euren Fingernägeln, feststellen können, dass ihr Handschuhe getragen habt und welche.

Verkleidungen wie Bärte und Perücken hinterlassen ebenfalls entsprechende Spuren. Zu verhindern ist das kaum, es sollte euch nur bewusst sein, dass ihr auch nach Umziehen und in Entfernung vom Aktionsort nicht völlig frei von Spuren seid und auch dort möglicherweise Gewebeabdrücke oder gar Kleidungsfetzen hinterlassen habt.

Es ist wichtig, vor einer Aktion möglichst alles zu Hause zu lassen, was leicht von der Kleidung abfallen kann. Also nichts mit Knöpfen, die verloren gehen können, anziehen und auch auf lange Schals oder Kleidung mit Fransen verzichten. Die behindern euch nicht nur bei einer etwaigen Flucht, es können auch leicht Fetzen am Aktionsort zurückbleiben.

Wenn ihr bei der Aktion oder beim Bauen mit Benzin in Berührung kommt, sollte euch bewusst sein, dass der Geruch kaum zu entfernen ist und bei einer Kontrolle gefährlich für euch werden kann. Passt beim Molliwerfen auf, dass kein Benzin auf eure Haut und Kleidung tropft. Das Problem dabei ist die eigene Wahrnehmung. Denn die Nase entwickelt eine gewisse Toleranz gegen den Geruch, wenn sie ihm länger ausgesetzt ist und ihr merkt es nicht mehr, wenn ihr wie eine kleine Tankstelle riecht.

In solchen Fällen, wie auch bei Aktionen mit Feuer, pflegen die Bullen eure Hände in Plastikbeutel zu stecken, um später analysieren zu können, was für Spuren daran zu finden sind. Dies trifft insbesondere auf Schmauchspuren zu, die z.B. beim Abschuss von Waffen entstehen. Untersuchungen auf Schmauchspuren werden mittlerweile auch auf Demos angewandt, um feststellen zu können, ob die festgenommene Person einen Pyro abgeschossen hat oder bei Menschen, die von den Bullen beschuldigt wurden mit Kaminanzündern Autos abgefackelt zu haben. Hier können Handschuhe helfen, die rechtzeitig entsorgt werden, denn

Schmauchspuren bleiben oft auch noch nach dem Waschen erhalten.

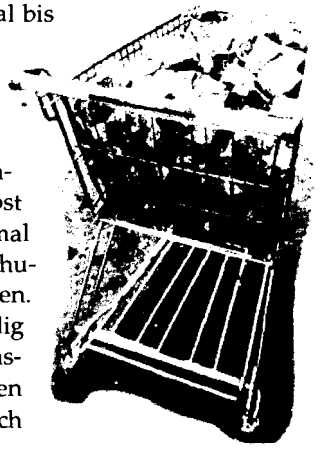
Spuren können aber auch bei der Herstellung von Aktionsmitteln entstehen. Wenn ihr mit pulverförmigen Substanzen arbeitet, müsst ihr davon ausgehen, dass sowohl euer Arbeitsplatz, als auch die benutzte Kleidung voll davon sind. Einen Arbeitsplatz wieder komplett zu reinigen, so dass auch chemische Verfahren der Spurensicherung nicht anschlagen, ist unseres Wissens nach unmöglich. Eure Wohnung sollte also, wenn ihr sicher gehen wollt, auch aus diesem Grund für solche Arbeiten ausfallen. Möglich sind sie in Räumlichkeiten, in denen es euch sicher erscheint und die nicht auf euch zurückzuführen sind (hier sind keine linken Projekte gemeint!), eine Möglichkeit sind z.B. leerstehende Häuser. Ihr solltet auch dort keine Fingerabdrücke und möglichst keine DNA-Spuren hinterlassen. Auch bei allen anderen Arbeiten solltet ihr darauf achten, keine noch so kleinen Splitter oder Drahtstückchen bei euch herumliegen zu lassen.

Einkaufen

Auch beim Einkaufen solltet ihr besonders vorsichtig vorgehen. Kauft immer nur eine Sache in einem Geschäft. Bezahlt bar, nicht mit Kredit- oder EC-Karte. Vernichtet eure Kassenbons. Überlegt euch vorher in Ruhe, was ihr wo einkauft und testet den Laden eventuell mit etwas Unauffälligem, damit ihr euch sicher fühlt.

Große Läden mit viel Publikum ermöglichen eine gewisse Anonymität. Sie haben aber meistens Kameras. Manchmal werden Videoaufzeichnungen nach 48 Stunden gelöscht. Nutzt dies und berücksichtigt es in eurer Zeitplanung, aber verlasst euch nicht darauf. Es ist immer besser, mit einem gewissen Abstand zur Aktion einzukaufen. Dann kommt ihr nicht in Bedrängnis und werdet unvorsichtig, wenn es etwas nicht gibt. Kleine Läden haben den Vorteil, dass sie oft keine Kamera haben. Dafür können sich die Verkäufer_innen oft sehr gut daran erinnern, an wen sie was wann verkauft haben.

Gegen das Wiedererkennen könnt ihr oft schon mit kleinen Verkleidungen große Wirkung erzielen. Von der Fensterglasbrille über den falschen Bart bis zu Perücke, farbigen Kontaktlinsen und Haartönungen, vom Anzug bis zur Joggingjacke sind hier der Fantasie keine Grenzen gesetzt. Selbst Theaterschminke oder Latexmasken können helfen. Allerdings solltet ihr euch in eurer Verkleidung wohl fühlen und normal bis unauffällig wirken.



Kauft, wenn möglich, alles immer in Verpackungen. Bittet um eine Tüte, oft packen die Verkäufer_innen dann euren Einkauf selbst ein. Im Winter ist es manchmal sogar unauffällig, mit Handschuhen (unbenutzt!) einzukaufen. Wenn Handschuhe zu auffällig sind, könnt ihr mit Heftpflasterspray Fingerabdruckspuren etwas verringern (siehe auch Abschnitt zu Fingerabdrücke), aber nicht sicher vermeiden. Gegen DNA-Spuren helfen sie nicht.

Fahrt nicht mit eurem Auto oder Motorrad einkaufen. Auch das Handy bleibt selbstverständlich zu Hause. Hier gelten die gleichen Vorsichtsmaßnahmen wie beim Auschecken des Aktionsortes. Wenn ihr öfter Aktionen macht, wechselt die Läden und die Marken. Variiert Zeiträume und Tage, an denen ihr bestimmte Sachen einkauft. Manchmal lohnt es sich auch, lieber etwas weiter weg oder sogar in die nächste Stadt zu fahren. Auf jeden Fall sollte aus euren Einkäufen nicht auf euren Wohnort geschlossen werden können.

Für Spezialteile denkt euch eine Geschichte aus, die erklärt, warum ihr sie ganz legal braucht. Recherchiert dafür vorher gründlich. Legt euch für alle Fälle auch eine Geschichte für den Smalltalk mit den Verkäufer_innen zurecht. Bei einigen Chemikalien müsst ihr den Zweck der Verwendung mit eurer Unterschrift bestätigen. Übt dafür eine falsche Unterschrift und verwendet für Formulare Druckbuchstaben. Bringt einen Filzstift mit (siehe auch Abschnitt zu Schriftspuren).

Ein paar Tipps zur Recherche

Bei der Vorbereitung einer Aktion hinterlasst ihr nicht nur materielle, sondern auch virtuelle Spuren. Wir wollen hier nur ein paar grundsätzliche Vorgehensweisen bei der Recherche zur Aktionsvorbereitung darstellen.

Die Bücher, die ihr in einer Bibliothek bestellt oder ausleiht, sind auf euch zurückzuführen und die Bullen überprüfen die Bibliotheksaccounts von Verdächtigen. Vermeidet dies deshalb unbedingt. Bibliotheken werden zum Teil auch videoüberwacht. Das gleiche gilt, wenn ihr euch von öffentlichen Computern aus mit eurem Account einloggt. Bei einer Internet-Recherche ist es wichtig, dass ihr nicht an eurem eigenen Rechner surft, dass ihr an einem Ort nur ein Thema und am besten nur einen Aspekt recherchiert. Ihr solltet euch, wenn ihr über ein Thema recherchiert, nicht gleichzeitig das konkrete Ziel auf dem Stadtplan anschauen oder gar praktische Anleitungen anzeigen lassen. Macht NICHTS Privates auf dem Rechner, keine E-Mail und auch sonst kein Surfen, denn gerade in Zeiten der Vorratsdatenspeicherung (alle Seiten, die ein Computer aufruft, werden gespeichert) stellt das eine große Gefahr dar. Lasst eure Handys zu Hause, wenn ihr zum Recherchieren geht.

Denkt daran, dass in Internet-Cafés oft Kameras hängen und versucht diese zu meiden. Auch solltet ihr darauf achten, dass ihr auf der Tastatur keine Spuren hinterlasst, vor allem wenn ihr eure Texte über das Internet verschicken wollt. Ladet sie direkt vom Datenträger hoch, wenn ihr es so machen wollt. Es ist für die Bullen leicht festzustellen, von welchem Rechner aus ein Text verschickt wurde. Deshalb solltet ihr immer beachten, dass es auch in Cafés ohne Kamera Menschen gibt, die euch eventuell identifizieren können. Versucht, mit Verkleidungen zu arbeiten und so unauffällig wie möglich zu bleiben. Denkt daran, dass auch auf Geldstücken eure Fingerabdrücke zumindest kurzfristig zu finden sind. (Buchtipp: Zum Thema Computersicherheit findet ihr viel in der neuen Ausgabe von „Wege durch die Wüste".)

Überwachungstechniken

Mit welchen technischen Mitteln wird überwacht? Und wie können wir damit umgehen?

(aus: Repression und Widerstand, mit kleinen Ergänzungen)

Wir kennen sie alle aus Spionagefilmen: Die Wanzen in Nachttischlampen und Kameras hinter lichtdurchlässigen Spiegeln aus den 60er-Jahre-Thrillern. Oder auch die modernen Einsatzzentralen der neueren Filme, die in Sekunden jedes Telefongespräch mithören und jede Spaziergängerin per Satelliten-Überwachung verfolgen können.

Die Realität liegt irgendwo dazwischen. Noch lange nicht jede Polizeistelle kann dabei auf die gleiche technische Ausrüstung (und geschultes Personal) zurückgreifen und wird diese nur dann anfordern, wenn sie die damit verbundenen Kosten mit einem entsprechenden Bedrohungsszenario oder durch ein bereits begangenes schwerwiegendes „Verbrechen" begründen kann.

Trotzdem sollten das Verfolgungs- und Kriminalisierungsinteresse des Staates nicht unterschätzt werden. Polizei und Geheimdienste werden zudem versuchen, den Erwerb und die Bereithaltung der teuren Gerätschaften durch deren möglichst häufigen Einsatz zu rechtfertigen.

Im Folgenden werden die derzeitigen technischen Instrumente der Geheimdienste und der Polizei grob erläutert (Stand: Herbst 2006). Die wirksamsten Gegenmittel sind sehr simpel und ohne technische Detailkenntnisse umzusetzen: Sich an Orten treffen, deren Überwachung höchst unwahrscheinlich ist, und riskante Kommunikationsmittel (Telefon, Post) für politische oder Szene-Zwecke nicht benutzen.

I. Abhören geschlossener Räume

Alle für die Überwachung geschlossener Räume zur Verfügung stehenden Instrumente haben zwei entscheidende Nachteile: Ihr Einsatz muss einige Zeit im Vorfeld vorbereitet werden und er ist relativ teuer.

1) Wanzen

Wanzen liefern von allen hier beschriebenen Abhörmethoden die beste Tonqualität. Je nach Einsatzgebiet sind sie sehr klein (2-3 Millimeter dick), können jedoch auch die Größe eines Würfelzuckers oder gar einer Streichholzschachtel erreichen. Sie sind kaum von anderen elektronischen Bausteinen zu unterscheiden und werden zum Teil getarnt, also fest eingebaut in andere Gegenstände, in den Raum oder das Fahrzeug gebracht.

Bevorzugte Orte für den Einbau von Wanzen sind Steckdosen, Lichtschalter, Telefone und andere, durchgängig mit Strom versorgte elektrische Geräte. Zur Not werden auch Löcher in Möbel gebohrt, um Mikrofone möglichst nah an den sprechenden Personen zu platzieren.

Wanzen können Gespräche im Umkreis von ca. 10 Metern abhören. Eine Wanze reicht aus, um einen etwa 100 Quadratmeter großen Raum zu überwachen. Je nach Batterie beträgt die Einsatzdauer zwischen mehreren Wochen (Knopfzelle) und einigen Monaten (9-Volt-Block). An das Stromnetz oder ein Telefonkabel angeschlossene Wanzen „leben" selbstverständlich länger.

Wanzen mit integrierten Funk-Sendern gehören zu den größeren Varianten und erreichen Funkreichweiten von mehreren hundert Metern, je nach Bebauung auch von bis zu 2 Kilometern.

Zur Übertragung der abgehörten Gespräche können auch Strom- und Telefonleitungen verwendet werden.

Spezielle in Telefonen oder deren Anschlussbuchsen versteckte Mikrofone lassen sich per Telefon von außen anwählen und abhören.

Gegenmaßnahmen

Selbstverständlich kann jede_r selber nach Wanzen suchen. Spezielle Wanzensuchgeräte werden in verschiedenen Preislagen angeboten und können auch gemietet werden. Professionelle Wanzensucher_innen verlangen viel Geld. Zudem haben sie im Regelfall eine Geschichte als Geheimdienstler_innen, Militärs oder Polizist_innen und werden sich daher vor Nestbeschmutzung hüten.

Gefundene Wanzen beweisen zwar, dass eine Abhörmaßnahme stattgefunden hat, eine Garantie, dass nicht noch weitere Mikrofone versteckt liegen, kann aber nie gegeben werden.

Das Abspielen von Musik, Tonbändern mit anderen Gesprächen oder Radio hilft nicht gegen Abhörversuche. Mit Hilfe moderner Technik können einzelne Stimmen ohne größere Probleme herausgefiltert werden.

Abhilfe schaffen hier spezielle Rauschgeneratoren. Das von ihnen erzeugte Geräusch wirkt für das menschliche Ohr kaum störend, verhindert aber eine Aufzeichnung und Übertragung der Gespräche. Rauschgeneratoren helfen ebenfalls gegen die weiter unten beschriebenen Abhörmöglichkeiten und sind ab ca. 500 Euro erhältlich.

Wer wirklich sicher gehen will, sollte generell auf die Aussprache von wichtigen Daten, Orten und Handlungen verzichten und dafür lieber Stift und Papier verwenden und das Geschriebene anschließend wirkungsvoll vernichten.

Es soll auch eine Art Tapete geben, die im Grunde aus Kohlenstoff besteht, und einen Raum, der rundum damit tapeziert ist, abhörsicher macht. Sie heißt „Multifunktionsbelag aus flexiblem Faservlies, elektrisch leitfähig bedruckt" und hat 1998 bei der „Marburger Tapetenfabrik" 16,40 DM gekostet. Gesundheitsschädlicher Elektrosmog soll damit geschluckt werden. (aus: taz, 17.6.98)

2) Stethoskope

Räume können von außen mit Hilfe von elektronischen Stethoskopen abgehört werden. Mit diesen Geräten lassen sich kleinste Schallwellen, die durch Wände, Türen und Wasserleitungen dringen, bis zu 40.000-fach verstärken und abhören. Auch das verhindern Rauschgeneratoren mit speziellen Kontaktresonatoren.

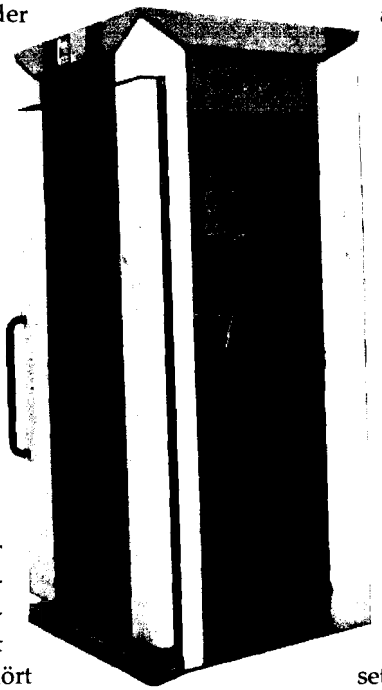
3) Reflexion der Fensterscheiben

Die in einem Raum entstehenden Geräusche lassen die Fensterscheiben ganz leicht mitschwingen. Mit Hilfe eines unsichtbaren Infrarotlasers können diese Schwingungen auf eine Entfernung von bis zu 200 Metern gemessen und wieder in Schallwellen zurück gewandelt werden. Komplettsysteme mit als Foto-Kameras getarnten Sendern und Empfängern, Verstärkern und Geräuschfiltern sind für unter 10.000 Euro erhältlich und dürften deshalb relativ häufig zum Einsatz kommen.

Die Nachteile dieser Technik: Eine Sichtverbindung zu einem Fenster des abzuhörenden Raumes muss vorhanden sein und bei doppelt verglasten Fenstern werden die Resultate ziemlich schlecht.

4) Videoüberwachung

Videokameras mit integrierten Funk-Sendern gibt es etwa ab der Größe einer Streichholzschachtel. Die Linsen dieser Kameras sind jedoch kaum größer als Stecknadelköpfe und können sehr wirkungsvoll getarnt werden. Sie lassen sich z.B. hinter Aufklebern verstecken oder als Kreuzschlitzschrauben tarnen. Auch vollständig getarnte Systeme in Form von Rauchmeldern, Schreibtischlampen und anderen Alltagsgegenständen werden angeboten.



Die von diesen Spezialkameras aufgenommenen Bilder sind qualitativ sehr hochwertig. Ihre Betriebsdauer und Funkreichweite sind vergleichbar mit denjenigen akustischer Wanzen.

Kameras können – soweit sie mit Funk-Sendern ausgestattet sind – mit Wanzensuchgeräten gefunden werden.

II. Telefonüberwachung

Im Jahr 2004 wurden in Deutschland über 30.000 Anordnungen zu Telefonüberwachungen erlassen, um Straftaten zu verfolgen. Dabei wurden in über 60 Prozent der Fälle Gespräche Unbeteiligter abgehört und nur in knapp 40 Prozent die Gespräche von Tatverdächtigen. Abhörmaßnahmen durch Geheimdienste und präventivpolizeiliche Maßnahmen sind in diesen Zahlen nicht enthalten.

Im internationalen Vergleich gilt Deutschland als Abhörweltmeister mit jährlich steigenden Zahlen. Die neue Bundesregierung hat im Dezember 2005 angekündigt, die gesetzlichen Regelungen bis Mitte 2007 zu überarbeiten (dies auf Druck des Bundesverfassungsgerichts).

Laut Gesetz müssen in der Regel alle Personen, deren Telefon überwacht wurde, nach Abschluss der Ermittlungen darüber informiert werden. Das geschieht aber höchst selten.

Die hohe Zahl der Telefonüberwachungen resultiert daraus, dass dies eine der am einfachsten durchzuführenden Überwachungsmaßnahmen ist: Richterliche Erlaubnis einholen und die betreffende Telefongesellschaft benachrichtigen. Schon werden alle Gespräche der gewünschten Anschlüsse an eine andere Nummer oder Sprachbox weitergeleitet und können abgehört werden. Aufgrund der durchgängig verwendeten digitalen Schaltanlagen ist garantiert kein verräterisches Knacken oder Rauschen zu hören.

Die Telefongesellschaften speichern ohne richterlichen Beschluss keine Gespräche. Festgehalten werden jedoch alle Verbindungsdaten – nämlich die genauen Angaben, wann mit welchen Anschlüssen wie lange telefoniert wurde. Diese Daten können für die Polizei bei der Aufklärung bereits begangener Taten von entscheidender Bedeutung sein. Sie bilden z.B. eine Grundlage zur Erkennung von Szene-Zusammenhängen oder helfen bei der Konstruktion krimineller Vereinigungen.

Verfassungsschutz und ausländische Geheimdienste hören permanent möglichst viele Telefonleitungen nach verräterischen Schlüsselwörtern ab. Diese Überwachung erfolgt vollautomatisch mit Hilfe von sehr weit entwickelter Spracherkennungssoftware. Diese ist in der Lage, Informationen miteinander zu verbinden und damit Bedeutungsmuster zu erstellen. Auffällige Gespräche werden gespeichert und anschließend manuell ausgewertet. Höchstwahrscheinlich ist mittels Stimmerkennung auch eine Zuordnung von Gesprächen zu den beteiligten Personen möglich.

Alle grenzübergreifenden Gespräche werden abgehört. Geheimdienste hören mit ziemlicher Sicherheit alle Gespräche ab, die über Satelliten übertragen werden (2-3 % der internationalen Gespräche in Europa und 60 % der interkontinentalen Gespräche).

Das am weitesten entwickelte Abhörsystem dieser Art wird von den englischsprachigen Geheimdiensten unter dem Namen „Echelon" betrieben. Die US-Behörde NSA setzt alleine dafür rund 28.000 Personen ein und ist in der Lage, ein Großteil der Internet-Kommunikation zu erfassen und auszuwerten.

Die Zusammenarbeit der Nachrichtendienste untereinander ist relativ eng – insbesondere dann, wenn aufgrund von Gesetzen das eigene Land nur schlecht beobachtet werden kann.

Festnetz-Telefone und Faxgeräte

Festnetztelefone können auch ohne Mithilfe von Telefongesellschaften direkt abgehört werden. Durch Wanzen im Telefongerät, in der Buchse, dem Schaltkasten im Haus oder dem Verteilerkasten an der Straße sind Abhörmaßnahmen relativ einfach zu bewerkstelligen.

Fax-Verbindungen werden auf die gleiche Weise ausgelesen und durch die Verwendung von Funktelefonen wird die Arbeit der Schnüffler_innen weiter erleichtert. Deren Signale können außerhalb des Hauses aufgefangen und entschlüsselt werden.

Öffentliche Telefonzellen und Telefonkarten

Es ist auch möglich, alle Telefonate, die mit einer Telefonkarte aus öffentlichen Telefonzellen geführt werden, zu überwachen. Hierzu wird der_die Betreiber_in der Zelle

von den Bullen zur sofortigen Übermittlung aller Verbindungsdaten dieser speziellen Telefonkartennummer verpflichtet. (aus: Interim 688)

Mobiltelefone

Mobiltelefone werden ebenfalls mit Hilfe der Telefongesellschaften abgehört. Für die Ermittlungsbehörden bieten sie jedoch zusätzliche Angriffspunkte: Sie ermöglichen die Positionsbestimmung der Verwender_innen, können zusätzlich über Funk abgehört werden und lassen sich zu Wanzen umfunktionieren.

Die meisten Handys speichern Verbindungsdaten und enthalten Adressverzeichnisse. Beide Datensätze sind für die Polizei von großem Wert und sollten deshalb regelmäßig überprüft und gelöscht werden.

Positionsbestimmung

GMS und UMTS-Mobilfunknetze sind in so genannte „Location Areas" unterteilt. Diese geografischen Gebiete haben im Schnitt etwa die Größe eines Landkreises (in Städten sind sie kleiner) und enthalten mehrere Funkzellen (Antennen). Jedes eingeschaltete Handy meldet sich bei seiner Location Area an und wartet anschließend „passiv" auf Nachrichten (sendet selber nicht). Im eingeschalteten Zustand ohne Verbindung kann das Endgerät deshalb nicht innerhalb dieser relativ großen Location Area lokalisiert werden (die Area ist allerdings bekannt).

Sobald jedoch eine Verbindung aufgebaut wird (Telefongespräch, SMS, ...) misst ein Mobiltelefon die Signalstärke der aktuellen (nächsten) Zelle sowie die Feldstärke der Nachbarzelle. Diese Daten werden jede halbe Sekunde an den Netz-Controller gesendet und ermöglichen eine relativ genaue Ortsbestimmung: In GSM-Netzen mit etwa 50 Metern Genauigkeit, in UMTS-Netzen mit etwa 15 Metern.

Positionsbestimmungen sind mit Hilfe der von den Telefongesellschaften gespeicherten Verbindungen auch nachträglich möglich. Liegen solche Daten vor, können Polizei und Geheimdienste sehr einfach feststellen, wo sich jemand zu einem bestimmten Zeitpunkt ungefähr aufgehalten hat.

In dringenderen Fällen – um herauszufinden, wo sich eine Person gerade aktuell aufhält - verwendet die Polizei so genannte „Silent SMS" (auch „Stealth Ping" genannt). Dabei wird eine von der_dem Empfänger_in nicht erkennbare SMS versendet. Anschließend werden die dadurch generierten Positionsdaten automatisch ausgewertet. Dafür muss die Handynummer der beobachteten Person bekannt sein.

Der Einsatz dieser „Silent SMS" ist gesetzlich kaum geregelt und dürfte unverhältnismäßig häufig erfolgen. Es ist davon auszugehen, dass verdächtige Personen mit Hilfe regelmäßiger „Silent SMS" vom Schreibtisch aus „beschattet" werden.

Abhören der Funksignale

Der Handy-Funkverkehr kann relativ einfach abgehört werden. Die Gespräche werden zwar verschlüsselt, können jedoch innerhalb von Sekundenbruchteilen wieder entschlüsselt werden. Die hierfür erhältlichen Geräte erfassen alle Gespräche der näheren Umgebung (bis mehrere Kilometer Umkreis) und können zum Teil auch den Richtfunk zwischen Zellen abhören (solange diese nicht durch Kabel verbunden sind). Da die Preise für entsprechendes Equipment stetig fallen, fürchtet sich mittlerweile sogar die Polizei vor Abhör-Angriffen aus dem organisiert kriminellen Milieu.

Um herauszufinden, welche Mobiltelefone sich in der näheren Umgebung befinden, kann ein „IMSI-Catcher" eingesetzt werden. Dieses Gerät tritt als eigene Funkzelle auf und erfasst auch Geräte, die gerade nicht senden. Dafür unterbricht ein einmal ausgesendetes Störsignal alle Mobilfunkverbindungen und bringt die Telefone anschließend dazu, sich bei der IMSI-Zelle anzumelden. Alle diese Handys sind zwar jetzt nicht mehr telefonisch erreichbar, je nach Ausrüstung des IMSI-Catchers können jedoch mehrere Telefone gleichzeitig nach „außen" telefonieren (und werden dabei abgehört).

IMSI-Catcher werden z.B. bei Hausbesetzungen eingesetzt, um einen schnellen Überblick über die im Haus befindlichen Mobiltelefone zu erreichen. Anschließend können dann deren Besitzer_innen ermittelt werden. Auch bei kleinen Demonstrationen und allen eher stationären politischen Aktionen lässt sich so sehr einfach die Anwesenheit bestimmter Personen erkennen, ohne Ausweiskontrollen durchzuführen. Dabei wird nicht nur die SIM-Karte identifiziert, sondern auch das Mobiltelefon. Ein einfacher Kartenwechsel schützt deshalb nicht vor der Verfolgung mit einem IMSI-Catcher.

Handys als Wanzen

Praktisch alle Handys können durch die Einstellungen „Stummschaltung" (kein Klingelton) und „Automatische Rufannahme" als einfache Wanzen eingesetzt werden. Dafür muss eine eingeweihte Person („Spitzel") das Telefon in den abzuhörenden Raum bringen und eingeschaltet lassen. Das Handy kann jetzt unbemerkt angerufen und abgehört werden.

Durch Aufspielen einer veränderten Handy-Software (im Internet erhältlich) bleibt das Handy beim Ausschalten im Lauschmodus (automatische Rufannahme) aktiv, ohne dass der_die Handynutzer_in dies bemerkt: Display und Alarm bleiben ausgeschaltet. Übertragungswege für derartige Software können Speicherkarten, Bluetooth-Verbindungen oder „Service-SMS" sein.

Bluetooth

Bei eingeschaltetem Bluetooth kann ein Handy über große Entfernungen von außen angegriffen werden. So lassen sich bei einigen Handy-Modellen z.B. Adress- und Kalenderdaten auslesen, ohne dass dies vom Telefon angezeigt wird.

Dauerhafter Bluetooth-Einsatz frisst also nicht nur unnötig Strom, sondern ist auch ziemlich riskant.

Gegenmaßnahmen

Gegen die Überwachung von Festnetz- und Mobiltelefonen kann nicht allzu viel unternommen werden. Möglich wäre allenfalls die Verwendung von Tarnbegriffen beim Telefonieren. Sicherer ist jedoch, bei sensiblen Inhalten ganz auf Telefongespräche zu verzichten, also auch Verabredungen zu Treffen und Demos nicht telefonisch auszumachen.

Auf Demos und zu anderen politischen Aktionen sollte am besten gar kein Handy mitgenommen werden. Wer den-

noch auf ein Telefon angewiesen ist, besorgt sich am besten ein zweites Gerät, mit leerem Telefonbuch, leerem Anrufeverzeichnis und leerer SIM-Karte, das ausschließlich in solchen „unsicheren" Situationen verwendet wird.

Mobiltelefone sollten bereits ausgeschaltet werden, bevor sich jemand auf den Weg zu einem Treffen oder einer Aktion macht. Vor allem dann, wenn diese in eher ungewöhnlicher Umgebung stattfinden. Wer absolut sicher gehen will, nicht über das Mobiltelefon abgehört zu werden, sollte den Akku entfernen. Handys enthalten zwar noch eine zweite Batterie, diese ist aber zu schwach für die Übertragung von Gesprächen.

Die Rufnummern-Unterdrückung ist übrigens im Umgang mit der Polizei immer wirkungslos.

III. Briefpost

Briefe können durchleuchtet werden. Das macht die Entscheidung der Schnüffler_innen leichter, ob es sich überhaupt lohnt, die Post zu öffnen. Gegen Durchleuchten hilft das Einwickeln der Post in Alufolie – was dann den Inhalt vielleicht erst richtig spannend macht.

Briefe können zudem mit Wasserdampf geöffnet werden. Auch in komplett neue Umschläge verpackte Briefe sind schwer als solche zu erkennen.

IV. Fahrzeuge

Mit Hilfe des Global Positioning Systems (GPS) ist eine Positionsbestimmung mit wenigen Metern Genauigkeit möglich. Das von den US-Militärs betriebene System besteht seit Anfang der neunziger Jahre und umfasst momentan 28 Satelliten, von denen jederzeit 4 empfangen werden können. Im Jahr 2000 wurde die für zivile Empfänger_innen eingeführte künstliche Ungenauigkeit abgeschaltet. Seitdem wird GPS z.B. in Autonavigationssystemen eingesetzt und wird von Polizei und Geheimdiensten zur Überwachung von Fahrzeugen verwendet.

GPS-Empfänger für den Überwachungseinsatz sind kleiner als Streichholzschachteln und ermitteln etwa alle 10 Sekunden ihre exakte Position. Diese Daten werden je nach Ausführung bis zu einem Jahr gespeichert oder per Funk (i.d.R. GSM-Mobilfunk/SMS) zu den überwachenden Stellen gesendet. Dort werden sie automatisch ausgewertet und können z.B. Hausnummer-genau in Stadtplänen und Landkarten dargestellt werden.

GPS-Empfänger lassen sich sehr einfach mit Magneten oder Klebstoff an der Unterseite von Autos befestigen. GSM-Sender können sich bei eingeschaltetem Autoradio durch das typische „Handy-Knattern" bemerkbar machen.

Kleinere Funk-Peilsender (15 x 35 mm mit 15 cm Antenne) werden ebenfalls eingesetzt und benötigen deutlich weniger Strom. Aufgrund ihrer geringen Größe können diese Sender in Fahrrädern und kleinere tragbare Gegenstände eingebaut werden. Peilsender senden jedoch keine Positionsdaten. Mit einem Empfänger kann lediglich erkannt werden, aus welcher Richtung das Signal kommt. Dadurch wird z.B. die Verfolgung von Personen erleichtert.

Alle in Gebäuden einsetzbaren Wanzen können selbstverständlich auch in Fahrzeugen benutzt werden. Bevorzugte Orte für den Einbau dieser Geräte sind die seitlichen Innenverkleidungen und der Dachhimmel des Autos. Durch die in die Decke eingebauten Lampen ist hier ein Stromanschluss vorhanden.

Auch in Deutschland werden die Forderungen nach einem obligatorischen Einbau so genannter Unfalldatenschreiber (UDS) immer lauter. Diese „Black Boxen" speichern alle wichtigen Daten, insbesondere Geschwindigkeiten und Entfernungen. Diese Daten sollen z.B. für die Rekonstruktion von Unfällen eingesetzt werden, sind aber selbstverständlich in Ermittlungsverfahren für die Polizei von besonderem Wert.

„Black Boxen" werden in den US-amerikanischen Autos serienmäßig eingebaut. In Europa werden sie in Mietwagen eingesetzt und sind in einigen Saabs zu finden.

V. Öffentlicher Raum

Mit Hilfe moderner Überwachungstechnik sind Polizei und Geheimdienste in der Öffentlichkeit oft näher am Geschehen, als den jeweils beobachteten Personen lieb ist. Mit Hilfe von Ferngläsern, Nachtsichtgeräten und Richtmikrofonen lassen sich Gespräche über größere Distanzen abhören, fotografieren und filmen. Treffen im Freien sollten also mindestens genau so sorgfältig vorbereitet und abgehalten werden wie in geschlossenen Räumen.

Richtmikrofone

Sie sind klein und handlich und können – je nach Ausführung und bei freiem Sichtfeld – Gespräche auf eine Distanz von 50 bis 200 Metern abhören. Sie verstärken ausschließlich den von der menschlichen Stimme abgedeckten Frequenzbereich und sind daher auch in lärmiger Umgebung und z.B. in Kneipen einsetzbar.

Das Abhören geschlossener Räume (durch Fensterscheiben oder Mauern hindurch) ist mit Richtmikrofonen nicht möglich (mit anderen Techniken wie Stethoskopen ist dies jedoch sehr wohl möglich).

Ferngläser

Mit tragbaren Ferngläsern können Gesichter bis auf eine Entfernung von etwa einem Kilometer eindeutig identifiziert werden. Mit an diese Ferngläser angeschlossenen Kameras lassen sich Foto- und Filmaufnahmen erstellen.

Nachtsichtgeräte

Restlichtverstärker ermöglichen das Sehen in teilweiser Dunkelheit, indem sie das vorhandene schwache Licht verstärken.

„Echte" Nachtsichtgeräte funktionieren auch bei absoluter Dunkelheit, indem eine Infrarotlampe die Umgebung ausleuchtet. Dieses Licht ist für das menschliche Auge nicht erkennbar und wird durch das Nachtsichtgerät als Schwarzweißbild sichtbar gemacht. Da Infrarotstrahlung Nebel besser durchdringt als Licht, werden diese Geräte auch bei solchen Bedingungen eingesetzt. Weiter entwickelte Nachtsichtgeräte verwenden Millimeterstrahlung anstelle der Infrarotlampen und können damit auch dünne Wände durchleuchten.

Wärmebildgeräte funktionieren ohne Restlicht oder Infrarotquelle. Sie stellen die von den beobachteten Objekten ausgehende Wärme grafisch dar und werden z.B. verwendet, um Isolierungen von Häusern zu überprüfen. Während der Castor-Transporte wurden diese Kameras aus der Luft eingesetzt, um im Gelände und in Wäldern versteckte Personen ausfindig zu machen. Auch frische Veränderungen im Erdreich können auf diese Weise sichtbar gemacht werden. An ihre Grenze stoßen die Geräte allerdings bei starkem Regen, Nebel oder Schneetreiben.

Festinstallierte Überwachungskameras

Mit dem Argument, die Sicherheit in Straßen und auf Plätzen und in öffentlichen Verkehrsmitteln zu erhöhen, wird in Deutschland ein immer dichteres Netz an fest installierten Kameras aufgebaut. Vor allem in Bahnhöfen und Flughäfen wird beinahe jeder Quadratmeter durch Videoüberwachung abgedeckt. Auch die Zahl der in U-Bahnen und Bussen installierten Kameras wächst.

Die Bilder von Überwachungskameras werden meist live auf Monitoren (z.B. in Kontrollzentren) angezeigt und zusätzlich zur späteren Begutachtung gespeichert. Sowohl Farb- als auch Schwarzweißkameras werden eingesetzt, wobei Schwarzweißkameras lichtempfindlicher sind und sich sehr einfach mit Infrarot-Systemen kombinieren lassen.

Im Bereich der Videoüberwachung lassen sich zwei Tendenzen erkennen:

- Die automatische Auto-Kennzeichen-Erkennung funktioniert praktisch fehlerfrei und wird heute bereits in LKW-Mautsystemen (Toll Collect) eingesetzt. Diese Systeme erfassen auch die Kennzeichen der nicht Maut-pflichtigen PKWs. Diese so erhobenen Daten werden nach Angaben der Betreiber_innen sofort wieder gelöscht. Dabei wird nicht nur das Kennzeichen, sondern auch der_die Fahrer_in fotografiert. Wenn ein Umfahren der Mautkameras nicht möglich ist, sollte daher darauf geachtet werden, dass zumindest die Insass_innen auf den eventuell doch nicht gelöschten Fotos nicht erkennbar sind. Z.B. kann mensch hierzu die Sonnenblenden herunter klappen und bei der jeweiligen Mautstelle mit dem Gesicht möglichst nah an diese herangehen.
- Sehr viel weitreichender gehen da die Planungen verschiedener deutscher Großstädte. Diese wollen ähnliche Systeme einsetzen, die gezielt nach gesuchten Kennzeichen fahnden. Hamburg hat sein Polizeigesetz diesbezüglich bereits angepasst und setzt zu diesen Zwecken mobile Kameras ein.

RFID-Chips

Radio Frequency Identification- (RFID-) Chips werden beispielsweise in Autoschlüsseln, Bibliotheksbüchern, den Tickets für die Fußball-WM 2006 und zur Identifikation von Tieren eingesetzt. Nicht unbedenklich ist die Integration der Chips in Kredit- und Kundenkarten und in die neuen Reisepässe. Als weiteres Einsatzgebiet sind KFZ-Kennzeichen mit RFID-Chips derzeit in der Diskussion.

In Supermärkten sollen diese RFID-Chips in absehbarer Zukunft die heutigen (Strichcode-)Preisschilder ersetzen. An der Kasse werden alle mitgeführten Waren automatisch per Funk erkannt und müssen bezahlt werden. Die RFID-Chips werden anschließend als „bezahlt" markiert, bleiben aber weiterhin auslesbar.

RFID-Chips werden berührungslos über Radiowellen angesprochen und senden die vom „Reader" abgefragten Daten zurück. Auf diese Weise können sie auch mehrfach mit zusätzlichen Daten beschrieben werden.

Die üblicherweise verwendeten „passiven" RFID-Chips kommen ohne eigene Stromversorgung aus. Sie beziehen die nötige Energie aus den empfangenen Funkwellen und sind dafür mit längeren, meist spiralförmigen Antennen verbunden. Die Reichweite der meisten dieser Chips liegt zwischen einigen Zentimetern und mehreren Metern.

Die Problematik der RFID-Chips liegt vor allem in der Tatsache, dass die Besitzer_innen keinen Einfluss darauf haben, welche Informationen über diese Chips abgefragt und gesendet werden und wann und von welchen „Reader" aus dies geschieht.

Je nach Ausgestaltung der Chips könnte die Polizei die Identität einer Person jederzeit per Funk feststellen, ohne dass diese das merkt oder verhindern kann. Gleichzeitig würde sichtbar, welche EC-Karte sie besitzt und dass sie soeben bestimmte Produkte eingekauft hat (oder Produkte dabei hat, die nicht als „bezahlt" markiert wurden). Horrorszenarien wie das „Ausscannen" ganzer Demos oder „sensibler" Orte sind ebenfalls denkbar.

Gegen diese Art der Bespitzelung gibt es glücklicherweise einfache und wirksame Gegenmaßnahmen: Bereits in Alufolie eingewickelte RFID-Chips sind absolut wirkungslos. Werden die nur Millimeter großen Chips von ihren wesentlich größeren Antennen abgetrennt, werden sie ebenfalls unbrauchbar.

Geräte zum Auffinden von RFID-Chips und -Readern werden beispielsweise vom FoeBuD (http://www.foebud.org) angeboten. Dort finden sich auch weiterführende Informationen zu dieser Thematik.

VI. Datenbanken

Praktisch alle Unternehmen haben ein sehr großes Interesse daran, möglichst viele Informationen über ihre Kund_innen zu sammeln. Auf diese Sammlungen haben Kund_innen nur begrenzten Einfluss und selbst wenn recht enge gesetzliche Bestimmungen bestehen – überprüft werden diese praktisch nicht. Durch Unterschrift können die Datenschutzbestimmungen zudem aufgehoben werden.

Nicht nur alle Transaktionen (Einkäufe, Bestellungen) und die Daten der Reklamationen, angeforderten Informationen usw. werden gespeichert. Mit Hilfe entsprechender Software werden aus „Wohngegend", „Anzahl Telefonanschlüsse pro Haus" und ähnlichen öffentlich zugänglichen Daten einigermaßen präzise Kund_innenprofile erstellt. Diese geben beim nächsten Anruf bei einer Hotline evtl. den Ausschlag, ob jemand sofort durchgestellt wird oder in der Warteschleife stecken bleibt.

Außerdem bieten verschiedene „Adress-Dealer" Daten zum Verkauf, an die sie auf legalem Weg nicht hätten gelangen können.

Selbst wenn die wenigsten dieser Firmen-Datensammlungen direkt von Überwachungsbehörden „angezapft" werden, ist die Gefahr vorhanden, dass solche Daten z.B.

durch Hacker_innen gestohlen und evtl. daraufhin im Rahmen eines Ermittlungsverfahrens bei der Polizei landen.

Deutlich erhöhtes Interesse haben Polizei und Geheimdienste in der Regel an folgenden Kund_innen-Daten:

- Bank- und Kreditkartenkonten: Sie geben Auskunft über Geldbewegungen – beim Einsatz von EC- und Kreditkarten auch über Transaktionen inkl. genauem Zeitpunkt und Ort.
- Bibliotheken und Buch-Versandhandel: Diese Daten geben evtl. Auskunft über die politischen Interessen der Personen und sind deshalb bei Rasterfahndungen von großer Bedeutung. Amazon wurde von US-Behörden bereits genötigt, seine Benutzer_innendaten herauszurücken.
- Von ähnlicher Bedeutung sind die Anbieter_innen von DVDs- und Tonträgern bzw. Musik-Downloads von den Nutzern halblegaler Tauschbörsen. Nur hinterlassen hier die Nutzer_innen in der Regel keine Personendaten (aber ihre IP-Adressen).
- Mitglieder-Verzeichnisse von politischen und religiösen Gemeinschaften und Kampfsportschulen/-vereinen.
- Flug- und Bahnreisen: Die Namen aller Passagiere auf Flügen in die USA werden an US-Behörden übermittelt. Je nach potenzieller Bedrohung durch solche Passagiere wurden schon verschiedene Flugzeuge zur Umkehr oder Landung in Kanada gezwungen. Je nach „Bedrohungslage" und Regierung ist ein solches Vorgehen auch bei deutschen und anderen europäischen Behörden möglich – mit dem Resultat, dass die Überwachungsorgane Einblick in die Reisetätigkeiten dieser Personen erhalten.

Sicherheitsmaßnahmen sind hier nicht ganz einfach. Natürlich haben wir alle Bankkonten und müssen von Zeit zu Zeit Geld von Automaten beziehen. Wer aber nicht allzu deutliche Spuren hinterlassen möchte, ist erstens äußerst sparsam bei der Abgabe persönlicher Daten und verzichtet möglichst darauf, Waren zu bestellen oder per Karte zu bezahlen. Barzahlung hinterlässt die wenigsten Spuren.

VII. Biometrie

Biometrie ist ein Wissenschaftszweig, welcher sich mit der Erfassung und Auswertung der körperlichen und verhaltenstypischen Eigenschaften von Lebewesen beschäftigt. Das Hauptaugenmerk bei der Anwendung auf den Menschen liegt in der computergestützten Identifizierung („Wer ist diese Person?") und Authentifizierung („Ist diese Person die, für die sie sich ausgibt?"). In der Praxis soll dies z.B. ausschließen, dass Unberechtigte durch den Diebstahl oder anderweitigen Erwerb von z.B. PINs oder Passwörtern Zugang zu ihnen ansonsten verwehrten Räumen oder Systemen erhalten. Hierbei verwendete Merkmale sind z.B. Körpergröße, Iris- und Netzhaut, Fingerabdrücke, Gesichtsgeometrie, Handschrift, DNA, Stimme, Gang oder auch Tippverhalten auf Tastaturen.

Die meisten Verfahren befinden sich noch in Testphasen, die von ihnen gelieferten Ergebnisse sind entweder zu ungenau oder die praktische Handhabbarkeit ist zu umständlich. Genutzt werden zur Zeit vor allem Systeme zur Iris-, Netzhaut- und Fingerabdruckerkennung sowie zur Gesichtserkennung. Im öffentlichen Bereich gibt es bisher recht wenige solcher Systeme, Beispiele sind der Zoo in Hannover, in dem der Zugang für Besucher_innen mit Jahreskarte über eine Gesichtserkennungsanlage erfolgt oder der Frankfurter Flughafen, an dem Reisende die Grenzkontrolle mittels Irisscan (in Verbindung mit ihrem Reisepass) passieren können.

Gesichtserkennungssysteme vermessen die relativen Abstände von Augen, Nase und Mund, wobei meistens von den Augen ausgegangen wird. Um einwandfrei identifiziert zu werden, muss sich eine Person frontal, ruhig und sehr nahe vor einer Kamera aufhalten (und ihr Gesicht muss zuvor einmal frontal gefilmt/fotografiert, ausgemessen und in das betreffende System aufgenommen worden sein). Es gibt auch bereits Versuche zur 3D-Erkennung, also der Möglichkeit, Gesichter aus jedem beliebigen Blickwinkel zu erkennen, praxistauglich sind diese aber noch nicht.

Neben den Zugangskontrollen ist die automatische Identifikation gesuchter Personen mit Hilfe öffentlich installierter Kameras ein angestrebtes und angepriesenes Ziel.

Allerdings sind bisher alle Versuche in diese Richtung gescheitert, die Fehlalarme waren einfach zu groß. Wie lange es allerdings tatsächlich noch dauert, bis gesuchte Personen auf diese Art in Echtzeit automatisch identifiziert werden können, lässt sich nicht wirklich einschätzen. Es ist zudem sehr wohl möglich, z.B. auf Demo-Fotos abgebildete Gesichter manuell „auszuschneiden" und dann automatisch überprüfen zu lassen.

Ein relativ einfacher Trick dies (bzw. ungewollte Gesichtserkennung überhaupt) zu verhindern besteht im Tragen von Sonnenbrillen oder tief sitzenden Baseball-Caps.

VIII. E-Pass

Seit November 2005 enthalten die Reisepässe in Deutschland einem Beschluss der EU folgend neben den bisherigen auch biometrische Daten. Momentan ist dies das Foto, ab November 2007 folgten zwei Fingerabdrücke. Diese Daten (sowie die meisten anderen Passdaten) werden verschlüsselt auf einem, ebenfalls neu eingeführten, RFID-Chip gespeichert. Welche Daten gespeichert werden, kann mensch sich bei den Passbehörden anzeigen lassen.

Angepriesen wird der neue Pass als enorm fälschungssicher. Wie bei allen RFID-Chips besteht auch hier die Gefahr des unbemerkten Auslesens. Um dies zu verhindern, sendet der Chip nur dann, wenn vorher das „normale" Datenblatt des aufgeschlagenen Passes erfasst und ausgelesen wurde. Das Lesegerät sendet an den Chip, dass es diese Daten kennt, woraufhin der Chip dann seine Daten ausspuckt.

Klingt zwar erstmal nicht schlecht, zumindest wenn mensch Vertrauen in vom Staat geschaffene Sicherheitstechnik und die Einhaltung der gesetzlichen Grundlagen hat. Sollte dieses Vertrauen fehlen, gibt es die Möglichkeit, den Chip abzuschirmen (durch Alufolie oder durch eine bereits erhältliche Schutzhülle). Prinzipiell kann der Chip auch zerstört werden, z.B. in der Mikrowelle. Pass rein, niedrigste Stufe, ganz kurz (kürzer als kurz) anschalten, Chip ist im

Der Pass bleibt auch gültig, wenn der Chip zerstört/unbrauchbar ist (aber eben nur der Chip – Brandlöcher im Deckel sind natürlich schlecht).

Die im Chip gespeicherten biometrischen Daten dürfen laut Passgesetz nicht in einer zentralen Datei gespeichert werden. Auch hier also – Papa Staat passt schon auf, dass alles mit rechten Dingen abläuft...

Ab November 2010 sollen dann auch die Personalausweise mit Chips und biometrischen Daten ausgestattet werden. Dann soll mensch sich noch aussuchen können, ob neben dem Foto auch die Fingerabdrücke darauf gespeichert werden. Spätestens danach wird das ganze aber unumgänglich. Achtung: Die Verschlüsselung von Pässen ist bereits teilweise umgesetzt!

Sicherheit und Handys

„Dieser Teilnehmer ist zur Zeit nicht zu erreichen..."
Einige nützliche Informationen zum Umgang mit Mobiltelefonen.

(aus: radikal 158/2005)

Eimer. Allerdings ist dies ein relativ riskantes Verfahren, der Chip kann anfangen zu brennen!

Das von Traditionsdogmatiker_innen unter den Autonomen lange Zeit verteufelte Handy hat mittlerweile nicht nur bei hippen Pop-Antifas Einzug gehalten, es ist für nahezu jede_n Polit-Aktivisten_in zum unverzichtbaren Bestandteil der Kommunikation geworden. Oft mischen sich der private, persönliche Gebrauch mit Polit-Kontakten. Das ist praktisch und eröffnet viele neue Möglichkeiten, etwa bei Nazi-Aufmärschen politische Aktionen zu koordinieren. Wie bei nahezu allen technischen Neuerungen haben auch Handys eine Schattenseite. Na und um die soll es an dieser Stelle gehen. Wir wollen dabei nicht grundsätzlich über die Zwiespältigkeit der Technik diskutieren. In erster Linie wollen wir einen Praxis-Leitfaden an die Hand geben, der euch im Umgang mit Handys sensibilisieren und euch aufzeigen soll, was die dunkle Seite der Macht mittlerweile alles kann.

Die Überwachung von Telefonen ist für die Bullen zum meistgenutzten Repressionsmittel überhaupt geworden. Es ermöglicht (mit einer richterlichen Anordnung) Gespräche zu belauschen, und versetzt die Bullen auch in die Lage, euch zu orten, wenn ihr ein eingeschaltetes Handy dabei habt. Zum Standardprogramm bei Festnahmen gehört klar auch die Auswertung eurer eingespeicherten Nummern, die ein mehr oder weniger vollständiges Kontaktbild eures Umfeldes liefern. Damit ist das Handy für den Repressionsapparat viel interessanter, als es früher ein normales Telefon in einer Wohnung war. In der Szene werden die Gefahren, die von der unbedachten Benutzung von Mobiltelefonen ausgehen, unserer Meinung nach deutlich unterschätzt. Viele Politaktivist_innen sprechen beispielsweise grundsätzlich kein Wort über klandestine Fragen in den eigenen vier Wänden (was sicherlich sinnvoll ist!). Dabei wird der große Lauschangriff, also das Verwanzen von Polit-WGs, jedes Jahr nur ein paar Mal angewandt (meistens bei Mordermittlungen und bei Drogenprozessen). Telefone wurden 2004 dagegen in fast 46.000 Fällen abgehört, die Ortung über Handys dabei nicht mitgezählt. Fast alle abgehörten Telefone waren Handys. Das Telefon ist also das Einfallstor Nummer 1, um Erkenntnisse über Kontakte, Aufenthaltsorte und Gespräche von Aktivist_innen zu erhalten. Das solltet ihr euch immer bewusst machen. Wir unterstellen dabei, dass ihr nichts am Telefon selbst besprecht, was irgendwelche Polit-Referenz hat - dass sensible politische Sachen nichts am Telefon zu suchen haben, ist ja wohl eh klar! Prinzipiell ist es auch möglich, bei Telefonen über die Software das Mikrofon unbemerkt zu aktivieren und damit unbemerkt Gesprächen zu lauschen. Allerdings spielt diese Methode in der Praxis nach unserem Wissen keine große Rolle. Dennoch solltet ihr euer Handy nicht angeschaltet lassen, und vorsichtshalber den Akku entfernen, wenn ihr sensible Gespräche führt.

(!) Aber Vorsicht: Akkus können verwanzt werden, dann nützt auch ausbauen nichts.

Wie funktioniert ein Handy?

Grundsätzlich hinterlässt dein Handy bei der Benutzung zwei digitale „Fingerabdrücke". Die IMSI-Nummer und die IMEI-Nummer. Die IMSI-Nummer (IMSI steht für International Mobile Subscriber Identity) ist der individuelle Code deiner SIM-Karte, die meist 15-stellig ist. Mit der IMSI-Kennung lässt sich anhand der ersten 3 Ziffern feststellen, aus welchem Land deine Karte ist. Die nächsten beiden Zahlen sagen, welche Mobilfunkfirma deine Karte ausgegeben hat (D1, D2, E-Plus...). Danach kommt eine individuelle Seriennummer. Der Verkaufsweg der IMSI-Nummer ist relativ simpel über die Register der

Mobilfunkfirmen nachvollziehbar. Die IMSI wird bei jedem Gespräch übermittelt. Die IMEI-Nummer (IMEI steht für International Mobil Equipment Identity) ist immer 15-stellig und findet sich innen im Gerät. Sie identifiziert dein individuelles Telefon. Anhand der IMEI lässt sich auch zurück verfolgen, aus welchem Land dein Telefon stammt. Die ersten beiden Stellen geben Aufschluss über das Land, deutsche IMEIs beginnen dann mit 49. Die drei Zahlen, die dann kommen, bezeichnen den Hersteller (also Siemens, Nokia...). Die nächsten beiden Ziffern sagen, in welchem Land das Gerät produziert wurde. Erst dann kommt die aktuelle Seriennummer. Der Verkaufsweg der IMEI-Nummer ist nachvollziehbar, was aber für die Bullen zeitaufwändig und mühselig ist. Auch die IMEI wird bei Nutzung des Telefons übermittelt. Wenn du also in deinem Gerät die Karte wechselst, benutzt du eine neue IMSI, aber weiter die alte IMEI. Wegen des mehr werdenden Diebstahls von Handys haben die Mobilfunkhersteller auf Druck des Staates in England mittlerweile ein zentrales IMEI-Register angelegt, in dem sämtliche Geräte mit ihrer IMEI registriert sind. Das Ziel ist, bei Diebstahl nicht nur die Karte (also die IMSI-Nummer) sperren zu können, sondern auch das Gerät selbst (über die IMEI). Damit würde ein gestohlenes Handy wertlos - ganz nebenbei eröffnen sich aber auch neue Überwachungsmöglichkeiten, weil die Identifizierung eines Gerätes, des Kaufortes und -datums etc. sehr unproblematisch wird. In Deutschland sind die Bullen noch nicht so weit, nach unserem letzten Stand hat allerdings Vodafone freiwillig mit dem Aufbau eines solchen Registers begonnen. Übrigens gibt es auch dagegen Gegenmittel: Im Internet gibt es Programme, mit denen sich elektronisch die IMEI eines Programms manipulieren lässt. Weil das auch die Bullen wissen, steht die Manipulation der Gerätenummer in England mittlerweile unter Strafe. Soweit unser kleiner Ausflug in die Welt der IMEI.

Prinzipiell funktionieren Handys so: Wenn du dein Gerät einschaltest, meldet es sich im Telefonnetz mit seiner IMSI-Nummer und der IMEI an, wobei für die Firmen nur die IMSI wichtig ist. Der Mobilfunkbetreiber, bei dem du dich eingeloggt hast (also beispielsweise E-Plus), registriert deine Daten in einem Besucher_innenregister und fragt anschließend bei deiner Mobilfunkfirma nach, ob deine Daten korrekt sind. Anschließend ist deine Anmeldung gespeichert und du darfst telefonieren. Allerdings ist damit noch nicht dein Aufenthaltsort bekannt - jedenfalls nicht genau. Die Mobilfunknetze sind nach dem Schachtelprinzip aufgebaut: Die kleinste Einheit sind die Antennen, die meist auf Dächern aufgebaut sind. Um die Antennen verwalten zu können, sind mehrere Antennen zu einer größeren Einheit zusammen gefasst, der sogenannten BSS (Base Station Subsystem). Mehrere dieser BSS ergeben wiederum eine Local Area, kurz LA genannt. Was wie technisch uninteressantes Kauderwelsch klingt, hat praktische Folgen. Denn die Mobilfunkfirmen wissen nicht automatisch, wo ihr euch befindet. Angemeldet seid ihr erst einmal nur in einer Local Area, die je nach Netzabdeckung ganz schön groß sein können - bis zu einigen hundert Quadratkilometern. Auf diese Weise reduzieren die Mobilfunkfirmen die Datenmengen. Es ist ja schließlich nicht entscheidend, mehr über euch zu wissen, als dass ihr euch in der oder dieser Region eingeloggt habt. Auch wenn ein Handy innerhalb einer Local Area den Ort wechselt, ohne dass das Telefon benutzt wird, findet ein Update in der Regel nicht statt. Erst wenn du dein Handy aktiv benutzt, wird präzise der genaue Standort gespeichert (also von welcher Antenne aus welcher BSS dein Signal kommt). Das gleiche geschieht nach einer längeren Phase der Inaktivität (zwischen einer halben Stunde und mehreren Stunden). Die Ortung von Handys schwankt also zwischen vielen Quadratkilometern, wenn du inaktiv in einer LA registriert bist, und einem bis unter 50 Meter genauem Ort, wenn du telefonierst. Die genauen Entfernungen hängen von der Dichte der Antennen ab. Logischerweise ist das in einer Großstadt präziser als auf dem Land.

Stille SMS

Weil dein genauer Aufenthaltsort gar nicht bekannt ist, wenn du das Telefon zwar an hast, aber nicht telefonierst (jedenfalls nicht so genau, dass ein Observationsteam dich in einer Großstadt findet), haben die Bullen ein trickreiches Mittel erfunden: Die stille SMS. Sie wird gerne eingesetzt, um dich zu orten, wenn dein Handy eine zeitlang inaktiv war und du nicht in eine spezielle Funkzelle, sondern nur allgemein in die „Local Area" eingeloggt bist. Die Bullen machen sich dabei eine Technik zunutze, die eigentlich von den Mobilfunkfirmen entwickelt wurde, um die Funktionsfähigkeit von Geräten zu testen, ohne dass dabei „offizielle" Kommunikation entsteht, denn die „stille SMS" wird von Handys nicht angezeigt. Mit eigens dafür entwickelten Programmen wie „Stealth Ping" oder „SMS Blaster" schicken die Bullen dabei eine SMS auf dein Handy, die so programmiert ist, dass dein Handy zwar ein kurzes Antwortsignal sendet, den ganzen Vorgang aber nicht anzeigt. Dieses Antwortsignal erzeugt die nötigen Daten: wann du dich wo befunden hast. Rechtlich betrachtet gilt das als Telefonverkehr, bei dem die Mobilfunkfirmen verpflichtet sind, sie der Polizei mitzuteilen. Auf diese Weise erhalten die Bullen genaue Angaben über deinen Aufenthaltsort, selbst wenn du denkst, dass du dein Handy gar nicht benutzt hast. Allerdings funktioniert die stille SMS natürlich nur, wenn du das Telefon eingeschaltet hast. Für die Bullen ist die stille SMS nicht nur eine gute Fahndungsmöglichkeit, sondern auch ein Trick, um die rechtlichen Hürden zu umgehen. Das Abhören von Handys ist nur bei schweren Straftaten möglich, wofür die Bullen eine richterliche Anordnung brauchen. Die Verbindungsdaten dürfen die Bullen aber seit einiger Zeit bereits bei Straftaten von „erheblicher Bedeutung" nutzen - also bei einer niedrigeren Schwelle. Die „stille SMS" ist so mittlerweile zu einem Standardwerkzeug der Bullen geworden.

IMSI-Catcher

Seit einigen Jahren gibt es den sogenannten IMSI-Catcher, ein neuartiges Instrument, das den Bullen hilft, im Handy-Zeitalter durchzublicken und das ein effektives Werkzeug zum Identifizieren von anonymen Handys ist. Der IMSI-Catcher ist ein kofferraumgroßes Gerät, das die Bullen bei Observationen dabei haben, wenn sie wissen wollen, mit welchen Handys du so telefonierst. Handys, die auf deinen

Namen angemeldet sind, sind schnell identifiziert, indem die Bullen in die Kund_innendateien der Telefonfirmen schauen. Anschließend beantragen sie bei der_dem Richter_in eine Abhörgenehmigung und sind ab da in der Leitung. Aber was tun bei anonymen Handys oder von Freund_innen geliehenen? In diesen Fällen observieren die Bullen dich mit einem IMSI-Catcher ein paar Tage lang, um herauszufinden, wie du kommunizierst. Immer, wenn sie dich telefonieren sehen, schalten sie den IMSI-Catcher ein. Technisch funktioniert das Gerät so, dass es eine Funkzelle der Handy-Betreiber simuliert. Das heißt, dein Telefon loggt sich nicht beim nächstbesten Telekom-Funkmast ein, sondern beim IMSI-Catcher - ohne es zu merken! Der IMSI-Catcher zieht sozusagen magnetisch die Signale aller Telefone im Umkreis von einigen 100 Metern an. Weil die Handys denken, sie würden mit einem normalen Funkmast kommunizieren, identifizieren sie sich artig mit ihrer IMSI und ihrer IMEI - und schon wissen die Bullen, mit welchem Gerät ihr telefoniert. Zum IMSI-Catcher gehört ein Computerbildschirm, auf dem alle Telefonnummern im Umkreis erscheinen. Das können vor der Flora im Schanzenviertel schon mal ein paar Dutzend oder Hundert Handys sein. Deshalb folgen euch die Bullen eine Weile und machen an verschiedenen Orten den Catcher an. So reduziert sich der Kreis der möglichen Handys, die an allen Orten eingeloggt sind, immer weiter, bis nur noch eine Nummer über bleibt. Rechtlich ist es so, dass der IMSI-Catcher schon seit Jahren eingesetzt wird, aber erst seit 2002 erlaubt ist. Allerdings dürfen die Bullen auf diese Weise nur deine Nummer herausfinden und dich noch nicht abhören. Deshalb gehen sie, wenn sie dein Handy identifiziert haben, anschließend zum_r Richter_in und beantragen eine Abhörgenehmigung, um möglichst bald in der Leitung zu sein. Technisch ist es heute allerdings bereits möglich, mit dem IMSI-Catcher nicht nur die Nummern zu erkennen, sondern auch mitzuhören. Entscheide selbst, wie hoch die Wahrscheinlichkeit ist, dass die Observateure nicht ab und zu mal reinhören, was da so gesprochen wird...

Was heißt das? Ein Beispiel

Wie ausgeführt, sind über das Handy verschiedene Dinge möglich, nicht nur das Belauschen von Gesprächen. Die eigentlichen Telefonate haben heute gar keine so große Bedeutung mehr. Viel wichtiger sind die Abfalldaten: Wer telefoniert mit welcher? Welche Bewegungsprofile entstehen? Welche benutzt welche, nicht auf sie angemeldete Handys? Und welche Namen und Nummern sind im Adressbuch gespeichert? Ihr solltet euch vor allem verdeutlichen, dass eure Geräte fette Datenabdrücke hinterlassen, die im Zeitalter des Computers natürlich noch lange danach nachzuverfolgen sind. Anhand eines fiktiven Szenarios wollen wir mal verdeutlichen, was das Handy so alles anrichten kann, wenn ihr es unachtsam gebraucht.

Die Polit-Aktivistin Anna (die in diesem Beispiel zwar das Maul am Telefon hält, aber leider unvorsichtig mit ihrem Gerät umgeht), ist ins Visier der Bullen geraten. Sie war einigermaßen clever und hat ein Telefon, das auf ihre Mutter angemeldet ist. Deshalb läuft eine Anfrage der Bullen bei T-Mobile, O2, E-Plus und Vodafone ins Leere. Weil Anna aber als Kontaktperson einer untergetauchten Freundin unter Beobachtung steht, folgt ihr ein paar Tage lang ein Observationsteam des Staatsschutzes, um rauszufinden, wie interessant Anna ist. Die Bullen haben einen IMSI-Catcher dabei, den sie einmal vor der Flora, einmal an der Alster und einmal am Hafen anmachen. Zwei Nummern erscheinen bei allen drei IMSI-Attacken auf dem Bildschirm: Die von Annas Mutter, die ab sofort abgehört wird, und eine zweite, unbekannte, die als Prepaid-Karte nicht registriert ist. Auch sie wird von diesem Zeitpunkt an abgehört. Am Telefon selbst ist Anna sehr vorsichtig und bespricht nichts politisch Relevantes. So kommen die Bullen also nicht weiter. Weil die Bullen aber überprüfen wollen, ob Anna an der Aktion einer militanten Gruppe teilgenommen hat, wegen der ihre Freundin gesucht wird, beantragen sie rückwirkend die Verbindungsdaten des Gerätes: Mit wem ist von diesem Handy aus gesprochen worden? Die Mobilfunkfirma liefert jetzt nicht nur die Verbindungsdaten, sondern auch die Logfiles, mit denen sich mit einiger Mühe ein ziemlich genaues Bewegungsprofil erstellen lässt. Ganz nebenbei (siehe oben) können die Bullen anhand der IMEI auch ablesen, ob Anna ihr Telefon beispielsweise aus Holland hat. Die Bullen waren gründlich und haben (über Anfragen bei den Mobilfunkfirmen und den IMSI-Catcher) nicht nur rausgefunden, welche Handys Anna benutzt. Sie haben auch rückwirkend bei der Mobilfunkfirma die Daten einer bestimmten BSS und der zugehörigen Antennen beantragt, die ganz in der Nähe eines vor einem halben Jahr abgefackelten Autos einer Schweinefirma liegen. Da die Aktion nachts um 4 Uhr stattfand, sind kaum Daten gespeichert. Allerdings war zum Zeitpunkt der Aktion das Prepaid-Handy von Anna eingeloggt, das nicht registriert war und zu dem die Bullen deshalb keinen Nutzer zuordnen können. Dank des IMSI-Catchers wissen sie jetzt, dass das Handy von Anna genutzt wird. Aus den Daten der Mobilfunkfirma wissen die Bullen auch, dass das Gerät in der betreffenden Nacht nur zwei Mal kurz genutzt wurde, ohne dass ein Gespräch zustande kam. Da aber auch Anwahlversuche gespeichert werden, wissen die Bullen immerhin, mit welcher anderen Nummer Anna nachts telefonieren wollte. Sie vermuten, dass die zweite Person ebenfalls an der Aktion beteiligt war und das Anklingeln ohne zu reden ein verabredetes Signal war. Durch die rückwirkend gelieferten Daten sehen die Bullen auch, dass das auf Annas Mutter registrierte Handy an einem Samstagabend vor vier Wochen in Berlin in der Nähe eines Szenecafés eingeloggt war. Dort fand eine Veranstaltung zu den Castortransporten statt, an der Anna offenbar teilgenommen hat. Erst am Montag darauf war sie wieder in Hamburg. Auf Grund der neu gewonnenen Erkenntnisse wird Anna observiert. Anna bemerkt die unauffälligen Herren in ebenso unauffälligen Opel Astras und schlägt ein paar Haken in der U-Bahn und bei Saturn, bis sie sicher ist, allein zu sein. Die Observateure schicken, nachdem sie Anna verloren haben, eine stille SMS an die Nummer. Siehe da: Anna hat das Handy ihrer Mutter eingeschaltet gelassen! Auf dem Display sehen die Observateure deshalb, in welcher Funkzelle das Handy eingeloggt ist. Ein paar Minuten später haben sie Anna wiedergefunden. Um nicht erneut aufzufallen, bleiben die Observateure ab sofort außer Sichtkontakt, überprüfen aber regelmäßig mittels stiller SMS den Aufenthaltsort des Handys. Bei einer Antifa-Aktion gegen

Weil die Bullen aber bei der anschließenden Hausdurchsuchung die PIN-Nummer ihres Telefons finden, kopieren sie als erstes das gesamte Handy-Adressbuch und werten es anschließend aus. Auf diese Weise haben sie nicht nur ein umfassendes Bewegungsprofil von Anna erhalten, sondern können auch präzise sehen, mit wem Anna wie oft Kontakt hält. Theoretisch könnten sie das gleiche jetzt mit allen so erlangten Nummern machen - was in der Praxis natürlich nur in ausgewählten Fällen gemacht wird.

Das Beispiel ist konstruiert und klingt krass. Es soll aber vor Augen führen, was theoretisch alles geht (und praktisch oft auch gemacht wird). Haltet euch immer vor Augen, dass neben dem Inhalt von abgehörten Gesprächen auch ein breites Bewegungsprofil von euch entsteht, wenn ihr Handys nutzt - aktuell, aber auch rückwirkend!

Zusammengefasst gilt:

- Bei heiklen Polit-Aktionen solltet ihr generell kein Handy dabei haben.
- Macht das Telefon bei sensiblen Gesprächen aus und entfernt den Akku!
- Rückt nie freiwillig die PIN raus!
- Macht eure Handys nicht nur während eines Polit-Treffens aus, sondern deutlich vorher und nachher, so dass euer Aufenthaltsort nicht rekonstruierbar wird! Achtet drauf, dass ihr den Bullen über das An- und Ausschalten eurer Handys keine Ansatzpunkte gebt, wann ihr zu interessanten Treffen geht!
- Wenn ihr Handys bei heiklen Polit-Aktionen einsetzen wollt, bleibt nur ein sicherer Weg: Ganz neue Mobiltelefone und SIM-Karten zu nehmen, die weder vorher noch nachher benutzt wurden oder werden.

Kameras

einen NPD-Stand, an der Anna teilnimmt, nehmen die Bullen sie schließlich im Umfeld hoch. Anna ist nichts nachzuweisen, weil sie (natürlich!) vermummt war.

Für unseren eigenen Schutz beim Auschecken, beim klandestin Agieren und beim Entfernen vom Aktionsort müssen wir darauf achten, dass uns keine Kamera registriert. Manchmal sind sie sehr versteckt angebracht und klein, manchmal offensichtlich und groß oder zur Abschreckung angebracht. Sie müssen leicht erkennbar für die Öffentlichkeit auf Schildern angezeigt sein. Das ist aber leider nicht immer der Fall, sowieso nicht da, wo sie von Polizei und Geheimdiensten zum Zweck der Überwachung postiert sind. Ihre Anzahl hat in den letzten Jahren zugenommen und wird noch weiter zunehmen. Doch wir sollten uns davon nicht abschrecken lassen, zu tun, was zu tun ist, sondern unsere Kenntnisse vergrößern - über ihre Verbreitung, ihre technischen Finessen und wie wir sie unschädlich machen können.

Wo sind sie zu finden?

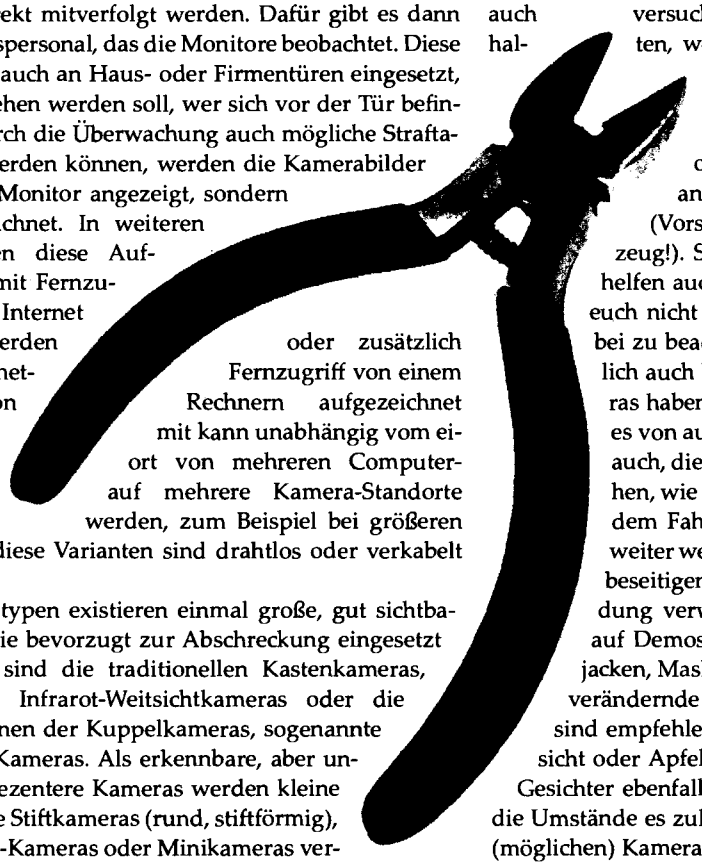
(Fast) immer an für den Staat sensiblen Stellen wie Banken, Botschaften, Ministerien, Kaufhäusern, Wohnorten hoher Persönlichkeiten, Firmensitzen. Oft und zunehmend auf Bahnhöfen, in Zügen und Bussen, vor Garagen, Einfahrten, Parkplätzen und in Geschäftseingängen, wo sie zum Teil auch die Gehwege mit erfassen. Oft sind Internetcafés, manchmal auch Copyshops kameraüberwacht. Gezielte Kameraüberwachung von öffentlichen Plätzen ist noch sehr umstritten und gibt es deshalb nur vereinzelt und unter medialer Aufmerksamkeit, z.B. in Leipzig-Connewitz oder auf Sylt. Hauseingänge von bekannten linken WGs, Autonomen Zentren oder Hausprojekten werden, falls überhaupt, auf jeden Fall möglichst unauffällig und meist nicht durchgehend überwacht. Einzelne Fälle von durchgehender, jahrelanger Kameraüberwachung sind aber aus politischen Strafverfahren bekannt geworden. Es lohnt sich bestimmt, mal die den Eingängen gegenüber liegenden Fenster (auch

in sehr schrägem Winkel) zu beobachten. Der Verfassungsschutz mietet manchmal für diese Zwecke Wohnungen an. Es wurden aber auch schon normale Mieter_innen gedrängt, ihre Fenster dafür zur Verfügung zu stellen. Ein zweiter Aus- und Eingang, über Höfe oder Dächer, kann deshalb interessant für euch sein. Es ist aber natürlich möglich, dass dort ebenfalls Kameras angebracht wurden.

Handyaufnahmen stellen zunehmend eine weitere Gefahrenquelle dar. Damit kann auch abseits von Gebäuden gefilmt oder fotografiert werden. Zu vergessen sind auch nicht die ständigen Filmaufnahmen von Bullen auf Demos. Auch Journalist_innen- oder Privataufnahmen können dort von Polizist_innen abgegriffen und dokumentiert werden.

Was können sie und wie sind sie zu erkennen?

Mit Kameratypen, Aufzeichnungsarten und Anwendungsbereichen ließen sich mehrere technische Fachbücher füllen, an dieser Stelle genügt aber ein grober Überblick. Überwachungskameras verfügen je nach Anwendungsbereich über verschiedene Aufzeichnungsarten. Zur Abschreckung werden manchmal auch nur Attrappen oder Schilder „Vorsicht Kamera" angebracht, ohne dass ein Gerät vorhanden ist. Dienen die Kameras der Beobachtung, wird gar nicht aufgezeichnet, sondern die Bilder der Kamera können nur am Bildschirm direkt mitverfolgt werden. Dafür gibt es dann z.B. Sicherheitspersonal, das die Monitore beobachtet. Diese Variante wird auch an Haus- oder Firmentüren eingesetzt, wenn nur gesehen werden soll, wer sich vor der Tür befindet. Sollen durch die Überwachung auch mögliche Straftaten verfolgt werden können, werden die Kamerabilder nicht nur am Monitor angezeigt, sondern auch aufgezeichnet. In weiteren Stufen können diese Aufzeichnungen mit Fernzugriff über das Internet angesehen werden oder zusätzlich über den Internet-Fernzugriff von einem Netzwerk von Rechnern aufgezeichnet werden. Dabei kann unabhängig vom eigenen Standort von mehreren Computer-Standorten auf mehrere Kamera-Standorte zugegriffen werden, zum Beispiel bei größeren Firmen. Alle diese Varianten sind drahtlos oder verkabelt möglich.



An Kameratypen existieren einmal große, gut sichtbare Kameras, die bevorzugt zur Abschreckung eingesetzt werden. Das sind die traditionellen Kastenkameras, kastenförmige Infrarot-Weitsichtkameras oder die großen Versionen der Kuppelkameras, sogenannte Speed-Dome-Kameras. Als erkennbare, aber unauffälligere, dezentere Kameras werden kleine bis mittelgroße Stiftkameras (rund, stiftförmig), Kuppel/Dome-Kameras oder Minikameras verwendet. Darüber hinaus gibt es natürlich verdeckte Kameras, sehr kleine Minikameras, z.B. in Klingelanlagen, an Haustüren oder Toren fast unbemerkt integriert und komplett getarnte Kameras in Uhren, hinter verspiegelten Scheiben, in Bewegungsmeldern oder Rauchmeldern.

Alle Kameratypen können mit verschiedenen Funktionen ausgestattet sein: Zoom, schwenken und drehen, extra breiter Radius, Nachtsichtmöglichkeit. Sie variieren in der Lichtempfindlichkeit, im variablen oder fixen Bildfokus, der Bildauflösung und Bildgenauigkeit. Bei hoher Bildgenauigkeit können Menschen oder Autokennzeichen erkannt und identifiziert werden. Sogenannte „intelligente Kameras", die vorher eingespeicherte Merkmale von Personen, wie Augen-Mund-Nase-Abstände, Iris-Scan oder Gangarten wieder erkennen und dann Alarm schlagen, werden, soweit wir wissen, in der BRD bisher nicht eingesetzt. Generell gilt: Nicht überall wird die neueste Technik eingesetzt, sie wird aber tendenziell besser und billiger. Die Kameratypen und ihre Fähigkeiten sind von außen nicht oder nur grob zu erkennen. Wichtig ist also auch eure Einschätzung des Ortes und welche Überwachungsstufe ihr dort für wahrscheinlich haltet.

Was können wir dagegen tun?

Wir können zum einen unsere Wege und Aktionsorte so wählen, dass keine Kamera uns erfasst. Aber wir können auch versuchen, sie zu überlisten: Etwas davor halten, wenn sie nicht zu hoch angebracht ist, z.B. Regenschirme oder Pappen oder eine Tüte darüber stülpen. Die Linse besprühen oder Farbe mit Farbeiern oder Farbspritzen auftragen, Aufkleber anbringen oder die Kabel durchtrennen (Vorsicht, immer nur mit isoliertem Werkzeug!). Steine oder Schläge mit dem Hammer helfen auch, wenn ihr gut vermummt seid oder euch nicht im erfassbaren Winkel aufhaltet. Wobei zu beachten ist, dass mensch sich diesbezüglich auch leicht irren kann, denn manche Kameras haben ein weiteres Erfassungsspektrum, als es von außen erkennbar ist. Manchmal reicht es auch, die Statur verdeckende Kleidung anzuziehen, wie einen Müllsack oder ein Regencape auf dem Fahrrad, zum Beispiel wenn die Kamera weiter weg ist. Hinterher solltet ihr die Kleidung beseitigen und natürlich nicht eure Alltagskleidung verwenden, mit der ihr womöglich auch auf Demos aufgenommen worden seid. Wendejacken, Masken, Regenschirme oder Körperformen verändernde Polster und Kissen unter der Kleidung sind empfehlenswert. Bärte, Perücken, Farbe im Gesicht oder Apfelstückchen in den Backen können eure Gesichter ebenfalls verändern. Wägt aber immer ab, ob die Umstände es zulassen, ein bisschen nachlässig mit den (möglichen) Kameras umzugehen! Im Zweifelsfall lasst die Aktion lieber sein, als euch unnötig zu gefährden!

Observationen

Tausend Augen
Observation - und was du dagegen tun kannst

(aus: radikal 153, Teil 2, 1995)

[Dieser Text ist schon etwas älter, aber immer noch ganz gut. Dass sich z.B. die Handytechnik in Bezug auf Headsets weiterentwickelt hat, wird jeder_m klar sein, der eine belebte Straße entlanggelaufen ist...]

Aus Fenstern starren dir sonnenbebrillte Augen nach, wohin du auch gehst... Autos rollen langsam an dir vorbei, drin sitzen zwei junge Typen und visieren dich aus dem Augenwinkel... vor deiner Haustür parkt seit Tagen ein Auto... im Telefon knistert es plötzlich nicht mehr wie früher, oder jetzt gerade... im Haus gegenüber ist seit neuestem eine Satelliten-Antenne angebracht, die genau auf dich zielt...über deiner Straße knattert in diesen Tagen oft ein Hubschrauber... jemand hat nach dir gefragt... jenseits des blauen Sommerhimmels zieht ein Spionagesatellit seine Bahn und fotografiert dich fünfzigmal in der Sekunde, während du durch menschenleere Straßen gehst...

Die Jahreszeit heißt PARANOIA.

Alle, die wir uns mit staatsfeindlichen Gedanken und hoffentlich auch Taten beschäftigen, kennen diese Jahreszeit. Viele von uns haben in den Jahren ihrer politischen Aktivität verschiedene Arten von Repression erlebt: Bullenprügel auf Demos, Ermittlungsverfahren, Prozesse, Durchsuchungen, Knast. Obwohl diese direkt erlebbaren Formen der Repression sich im Laufe der Jahre einigermaßen durchschauen lassen, ist es immer wieder erschreckend, wie wenig kollektiv aus diesen Erfahrungen gelernt wird. So sind immer wieder neue Kampagnen zur Aussageverweigerung nötig und immer wieder stehen Leute hilflos vor oder schon im Dornengestrüpp der Justiz und des Knastapparates, immer wieder scheinen Leute die alten Fehler wiederholen zu müssen. Zwar gibt es stapelweise Papiere zu allen möglichen Formen der Repression, aber es ist eben doch ein großer Unterschied, ob du selbst etwas erlebt oder nur darüber gelesen hast.

Was für die direkten, offen liegenden Erfahrungen mit Repression gilt, gilt erst recht für die geheimeren Formen. Die Linksradikalen wissen vieles über die Apparate ihrer Feinde oder verfügen zumindest über das theoretische Wissen, in der Praxis allerdings wird damit meist eher ungenau umgegangen.

Entweder ist es das subjektive Gefühl der Bedrohung, das das eigene Handeln bestimmt: Wird schon nix passieren – was können die schon wollen – ich pass ja auf – ich bin ja noch nicht ED-behandelt – wer interessiert sich schon für mich – aber auch: ich bin umzingelt, nichts geht mehr – besser, ich fasse gar nix mehr an – es wird eh alles beobachtet – Orwells „1984" ist längst überholt.

Oder aber es wird versucht, über allgemein aufgestellte Prinzipien die genaue Beurteilung der jeweiligen Situation überflüssig zu machen. Grundsätzlich wird nicht mehr in den eigenen Räumen geredet, über Telefon schon gar nicht, Schriftliches wird nicht mehr aufgehoben usw.

Dieser Text soll dazu beitragen, etwas Licht ins Dunkel der Observation zu bringen. Er hat vor allem zwei Anliegen:

Erstens: Die Methoden des Gegners kennen(lernen), heißt, sie bekämpfen zu können!

Zweitens: Nieder mit der Paranoia!

Uns ist dabei klar, dass durch die ausführliche Beschäftigung mit dieser Thematik Paranoia auch erst geschürt werden kann. Die, die diesen Text lesen, sollten sich deshalb stets vor Augen führen, dass alles, was hier beschrieben wird, eine Ausnahmesituation ist, zu vergleichen vielleicht mit der Situation in einem Flugzeug: Dort werden vor dem Start Hinweise für die Benutzung der Schwimmwesten gegeben und alle sollten mit dem Umgang damit vertraut sein, aber benutzt werden sie denn doch nur in ganz wenigen Ausnahmefällen. Und kaum jemand wird den ganzen Flug über andauernd an Schwimmwesten denken.

Wenn wir im Folgenden von Observation schreiben, meinen wir damit gezielte Beobachtungen von Personen; nicht näher gehen wir auf die alltägliche Schnüffelei ein, die eine Szene ganz allgemein betrifft, wie z.B. Szenezeitungen besorgen, Plakate registrieren, sich in einschlägigen Kneipen und auf Versammlungen rumtreiben.

Zuerst ein paar Grundregeln in Sachen Observation:

Eine Observation ist eine planmäßige, organisierte Überwachung; sie erfordert einigen Aufwand, wenn sie etwas taugen soll: Vorbereitung, Personal, Fahrzeuge, technische Hilfsmittel, Koordinierung. Die meisten Observationen haben keinen politischen Hintergrund, sondern werden in Bereichen wie organisierte Kriminalität, Einbruch, Raub etc. durchgeführt.

Es gibt verschiedene Formen der Observation. Sie lassen sich wie folgt unterteilen (die Namen sind von uns gewählt): Standortobservation, Objektobservation, Personenobservation, Bereichsobservation.

Bei der Standortobservation sitzen die Observant_innen selbst irgendwo fest in einem Objekt (Haus, Auto o.ä.). Sie bewegen sich von dort nicht weg. Es kann bspw. sein, dass sie sich nur dafür interessieren, wer ein bestimmtes Gebäude betritt oder ob irgendwo etwas im Gebüsch versteckt wird. Eine solche Observation ist nur sehr schwer oder gar nicht zu bemerken.

Die Objektobservation ist eine Abwandlung der ersten Form. Bei ihr geht es darum, an einem bestimmten Objekt dranzubleiben, z.B. einem Auto oder einem Geldpaket. Dazu müssen sich die Observationskräfte bewegen.

Bei der Personenobservation können die ersten beiden Formen durchaus integriert werden, indem z.B. die Wohnung der Zielperson kameraüberwacht wird (Standortobservation), aber ansonsten die Person selbst verfolgt wird, d.h. der Zielperson wird meist hinterhergeschlichen. In einzelnen Fällen kann es auch vorkommen, dass Peilsender eingesetzt werden oder die Observant_innen sich an festen Positionen aufstellen, an denen die Zielperson vorbeikommen muss. Eine Observation kann mit einer Festnahme enden oder aber sie hat erst einmal gar keine wahrnehmbaren Folgen, mal abgesehen davon, dass die Sicherheitsbehörden nichts löschen, was sie einmal gespeichert haben.

Anlass für die ersten drei Formen der Observation ist normalerweise ein Ermittlungsverfahren (bei den Bullen) oder etwas Entsprechendes bei den Geheimdiensten/Verfassungsschutz (wahrscheinlich ein „Vorgang" o.ä.). Ein Aspekt bei der Verschärfung der Sicherheitsgesetze ist, den Bullen zu ermöglichen, dich auch ohne Ermittlungsverfahren beobachten zu dürfen.

Bei der Bereichsobservation geht es darum, ein Gebiet zu beobachten, um darüber Erkenntnisse über Bewegungen verschiedener Personen zu gewinnen. Im politischen Bereich dient eine solche Observation als Versuch, Bewegungsbilder der Szene zu erstellen. Dies wird vor allem im Vorfeld wichtiger politischer Ereignisse gemacht. Ein konkretes Ermittlungsverfahren muss dem nicht zugrunde liegen.

Alle Formen der Observation lassen sich auch als offene Observation durchführen. Diese hat den Zweck, entweder die Zielpersonen nervös zu machen, um zu sehen, wie sie reagieren oder um überhaupt erstmal eine Zielperson ausfindig zu machen, indem geguckt wird, wer sich wie verhält. Eine offene Observation ist unmissverständlich als solche zu erkennen. In einem solchen Fall müssen sie dann eigentlich bei dir direkt vor der Haustür stehen, oder sie rufen dich sogar an und sagen, dass sie da sind. Aber beachte: Wenn du eine Observation bemerkst, dann ist damit noch lange nicht gesagt, dass es sich um eine offene Observation handelt! Denn nicht immer sind die Observant_innen so gut, wie wir es ihnen in der Regel unterstellen..

Eine Person zu observieren, die von nichts eine Ahnung hat, ist sehr leicht. Eine Person zu observieren, die mit der Beobachtung rechnet, ist sehr schwierig.

Der Aufwand, der für eine Observation betrieben wird, hängt von vielen verschiedenen Faktoren ab: Es müssen Prioritäten gesetzt werden: Was ist gerade mehr oder weniger erfolgversprechend? Was ist politisch gewollt, ob von den Regierenden, von der Innenbehörde oder den eigenen Machtfraktionen des Apparats? Was ist überhaupt durchführbar?

Zwischen den Behörden gibt es Konkurrenz darüber, wer was machen soll oder kann. Wenn eine Behörde sich von einer anderen irgendwie gestört fühlt, kann das eine Verminderung des Einsatzwillens zur Folge haben. Geldkürzungen und Personalengpässe treffen zwar Bullen und VS viel weniger als andere Bereiche, aber auch sie ein bisschen. Eine Rolle spielt auch, was für andere wichtige Fälle gerade am Laufen sind, die nicht einfach mal so hinten angestellt werden sollen oder können.

Der Apparat ist ein träges Beamt_innensystem, in dem viele Leute sitzen, die sich für ihren Job erst einmal kein Bein ausreißen. Oft werden Erfolge dort nicht durch spitzfindige Ideen oder besonders engagierte Arbeitsweisen erzielt, sondern durch die hundertfache Routine, also das immer gleiche Durchziehen der immer gleichen Abläufe.

Von Bedeutung ist auch, was der oder den Zielpersonen zugetraut wird an Gefährlichkeit und Aufmerksamkeit.

Um eine gründliche Observation durchzuführen, bedarf es einer gewissen Vorbereitungszeit, die durchaus einige Wochen betragen kann. Wer also bei irgendeiner Sache festgenommen wurde und nun befürchtet, deswegen observiert zu werden, braucht sich nicht zu wundern, wenn eine Observation erst lange danach beginnt, wenn die eigene Wachsamkeit schon wieder nachlässt.

Nicht alles, was geht, wird auch gemacht

Es gibt zahlreiche Broschüren und Bücher dazu, was heutzutage an Überwachungen technisch möglich ist. Sie beschreiben Wanzen, die staubkorngroß in Ritzen stecken und die ferngesteuert abgefragt werden können oder Kameraobjektive, die stecknadelkopfgroß irgendwo auf der Lauer liegen. Es gibt sogar schon Objektive, die überhaupt nicht mehr mit Linsen arbeiten, sondern mit beliebig tarnbaren lichtempfindlichen Mikrobauteilen. Es gibt Peilsender zu kaufen, die über Sateliten zu orten sind und den Observationseinheiten eine Lokalisierung ihres Opfers erlauben, ohne dass sie ihr Büro dafür verlassen müssen. Telefone können angerufen werden, ohne dass sie klingeln oder sich sonstwie bemerkbar machen. Über Laserstrahlen können Räume aus großer Entfernung abgehört werden. Computerbildschirme können ebenfalls abgehört werden. Frei verkäufliche Computerverschlüsselungsprogramme werden von Geheimdiensten in kürzester Zeit geknackt. Digitale

Telefonnetze wie das „D-Netz" können selbstverständlich auch abgehört werden (das Gejammer der geheimen Behörden über die angebliche Nichtabhörbarkeit betrifft mehr die Frage, wie aufwändig bzw. teuer dieses Abhören ist). Über schlüsselwortgesteuerte Computer können tausende von Telefongesprächen abgehört werden.

Eine Schwäche dieser Texte ist, dass sie denen, die sie lesen, meist nichts darüber sagen können, welche Mittel wann und von wem eingesetzt werden. Viele der erwähnten Techniken sind sehr teuer. Manche sind zwar technisch machbar, aber in ihrer Entwicklung noch nicht genügend ausgereift und noch in der Erprobungsphase. Andere werden zwar angewandt, aber „nur" von Geheimdiensten. Und was der Geheimdienst hat, haben die Bullen noch lange nicht – schon allein deswegen, weil der Geheimdienst ja Wert drauf legt, etwas Besseres zu sein als die Bullen. Außerdem gibt es noch Prioritäten: Heutzutage gibt es eben doch noch Einiges, was für Staat und Kapital bedrohlicher ist als gerade die linksradikale Opposition und/oder was über die herkömmlichen Methoden der Überwachung schwerer zu kontrollieren ist. In diesen Bereich fällt vor allem die staatliche Spionage und Gegenspionage und die Wirtschaftsspionage. Die aufwändigen, fiesen technischen Mittel werden im wesentlichen in diesen zwei Bereichen eingesetzt sowie natürlich im militärischen Bereich.

Selbstverständlich sind alle technisch möglichen Überwachungsformen für uns eine potenzielle Bedrohung. Alles was einmal irgendwo benutzt wird, wird auch wieder eingesetzt werden. Je billiger und je vertrauter die Behörden damit werden, desto breitgestreuter wird ihr Einsatz.

Dabei ist auch zu beachten, in welchem Verhältnis der Einsatz eines technischen Mittels zum Erfolg steht. Wanzen sind dafür ein gutes Beispiel: Eine Wanze einzusetzen macht dann einen Sinn, wenn die Observationskräfte eine relativ klare Vorstellung davon haben, was wo besprochen wird oder zumindest davon ausgehen, den Ort zu kennen, an dem interessante Gespräche geführt werden. Immerhin müssen sie das Ding erst einmal gut deponieren und sich dann auch weiterhin darum kümmern, z.B. Stromversorgung, Aufzeichnung, Auswertung, spätere Entfernung. Wenn sie davon ausgehen, dass die Zielperson sowieso zu Hause nicht oder wenig quatscht oder in einem Haus mit 20 Zimmern lebt, die weit auseinander liegen, werden sie sich zweimal überlegen, ob sie sich die Arbeit mit der Wanze machen.

Wenn irgendwo eine Kamera platziert werden soll, ist vorher abzuklären: Ist die freie Sicht garantiert? Wie gut sind die Aufnahmen? Wenn es darum geht, Leute zu porträtieren, muss ein Teleobjektiv verwendet werden. Damit scheiden dann die winzigen, getarnten Objektive schon mal aus, es muss also eine richtige Kamera irgendwie in der Nähe verborgen werden. Aber ein Kameraobjektiv, dass ein Gesicht erfassen soll, kann ja andererseits auch von der Person gesehen werden. Wenn es hingegen so weit entfernt installiert ist, dass es nicht mehr so einfach entdeckt werden kann, besteht die Gefahr, dass andere Dinge im Weg sind wie z.B. Bäume, Autos etc..

Es ist darum sicher realistisch, von zwei wahrscheinlichen Möglichkeiten auszugehen: Zum einen wird es einige wenige Observationen mit Einsatz aufwendiger technischer Mittel geben. Das dürfte in den letzten Jahren im wesentlichen RAF und RZ/Rote Zora betroffen haben.

Zum anderen wird es die Massen der politischen Observationen geben, die mit „konventionellen" Methoden arbeiten, also Beschatten der Zielperson, Abhören des Telefons, Postüberwachung, evtl. Überwachen des Hauseingangs mit einer Kamera.

Vieles von dem, was gemacht wird, kannst du bemerken

Ein wesentlicher Bestandteil einer Observation ist im „Normalfall" herauszubekommen, wer wann wohin geht und wen trifft. Aber alles, was mit Bewegung zu tun hat, ist ein Schwachpunkt bei Observationen. Zum einen müssen die Observationskräfte sich mit der Zielperson bewegen, zum anderen müssen sie Kontakt untereinander halten. Auch wenn die Zielperson das selbst nicht mitbekommt, ist die Wahrscheinlichkeit groß, dass andere, außenstehende Personen die Observation bemerken. Sie werden sehen, wie Autos plötzlich ohne erkennbaren Grund losrasen oder wie in parkenden Autos welche sitzen und sich ganz tief in den Sitz drücken oder ihnen wird auffallen, wie jemand plötzlich in den Jackenaufschlag hineinmurmelt oder wie jemand längere Zeit in einem Hauseingang lümmelt. All dies sind unvermeidliche Verhaltensweisen bei einer Personen- oder Bewegungsobservation.

Wenn du also Gründe hast, mit einer Observation rechnen zu müssen, hast du auch gute Chancen sie mitzukriegen – manches davon selbst, wenn du mit offenen Augen durch die Gegend läufst, manches durch die Hilfe anderer Leute.

Du bist nicht die_der Einzige, die gemeint sein könnte

Das bedeutet zumindest in größeren Städten, speziell in bestimmten Stadtteilen, wohnen hunderte, vielleicht tausende von Menschen, die potenziell Betroffene von Observationen sein können, bei dir um die Ecke oder in deinem Haus. Es wird wegen aller möglichen Delikte observiert: Hehlerei, Betrug, Diebstahl, Raub, Mord, Drogen etc. Im politischen Bereich ist auch allerlei denkbar. „Terrorismus", Antifa, autonome Kleingruppen, PKK, DevSol, vielleicht auch Nazis. Dazu kommt noch Spionage, islamische Fundamentalist_innen, Hilfsdienste für ausländische Behörden, Ausländerpolizei, Fahndung nach gesuchten Personen.

Wenn bei dir in der Gegend observiert wird und du dir so deine Gedanken machst, dass dies dir gelten könnte, dann bedenke also, dass ringsum dich noch viele andere Personen sind, bei denen ebenfalls Gründe für eine Observation vorliegen könnten.

Dein Wissen ist nicht das Wissen deiner Feinde

Du wunderst dich vielleicht, dass du noch nie beschattet wurdest. Oder du wirst beschattet und wunderst dich, wieso sie da stehen und nicht dort und dort. Z.B. stellst du fest, dass die Bullen tagelang vor deiner Meldeadresse rumste-

hen, obwohl du eigentlich dachtest, dass die doch längst wissen müssten, wo du wirklich wohnst. Aber vielleicht ist es ja so, dass das nur der VS weiß, es aber den Bullen nicht gesagt hat.

Du musst immer damit rechnen, dass du, wenn es passiert, nicht in der Art und Weise observiert wirst, wie du es an deren Stelle selbst machen würdest. Sie wissen vieles nicht, was du weißt. Aber sie wissen auch Dinge, die du nicht weißt. Oder sie können sich auch irren und an einem ganz falschen Punkt ansetzen, z.B. ordnen sie dir Menschen zu, mit denen du gar nichts zu tun hast. Eine andere Möglichkeit ist, dass sie an einem Konstrukt basteln, das von ihnen politisch gewollt ist, aber nicht viel mit der Realität zu tun hat. Also solltest du nicht davon ausgehen, dass die Observationen sich an dem orientieren, was du als Realität kennst oder annimmst. Deine Gegner_innen gehen von dem aus, was sie in ihren Akten stehen haben und das kann auch einiger Mist sein.

Wenn du automatisch davon ausgehst, dass sie wissen, was du weißt, kann es passieren, dass du ihnen durch dein Verhalten dieses Wissen erst verschaffst. Wenn du, durch die Observation nervös geworden, plötzlich anfängst, Kisten aus der Wohnung zu schaffen, teilst du ihnen evtl. damit erst mit, dass es tatsächlich Dinge gibt, die du verbergen willst.

Natürlich ist die erste Frage bei einer Observation immer, worum es denen eigentlich geht. Rechne nicht damit, dass du es herausfindest! Wenn du weißt, dass es „gute" Gründe gibt, dich im Visier zu haben, dann gehe davon aus, dass es deswegen ist. Aber du musst auch damit rechnen, dass es Gründe gibt, auf die du nie kommen würdest. Z.B.: Du hast unwissentlich dein Auto an jemanden verkauft, der wegen organisiertem Autoschmuggel observiert wird. Oder: Bei der Festnahme einer wegen RAF-Mitgliedschaft beschuldigten Person wurde ein Zettel gefunden, auf dem eine Zahl steht, die das BKA irrtümlich für deine Telefonnummer hält. Oder: Ein Spitzel hat dich fälschlicherweise bezichtigt, du hättest Kontakte zu einer klandestin organisierten militanten Gruppe. Das alles sind Sachen, die dir wahrscheinlich nie jemand mitteilen wird, die du also auch gar nicht einschätzen kannst.

Es gibt natürlich auch Hinweise, anhand derer du feststellen kannst, wieviel die Bullen wissen, z.B. anhand der Feststellung, welche Freund_innen von dir mitbetroffen sind oder zu welchen Uhrzeiten du beobachtet wirst. Wenn sie immer am Abend kommen, werden sie dich wahrscheinlich nicht wegen organisiertem Klauen im Supermarkt beobachten.

Paranoia nährt sich aus sich selbst heraus

Wenn du erst einmal Anzeichen für eine Observation um dich herum wahrgenommen hast, fängst du vielleicht an, das Gras wachsen zu hören. Plötzlich vermutest du überall Bullen, alles ist verdächtig. Das ist völlig normal, kommt und geht phasenweise und ist auch von deiner jeweiligen Stimmung abhängig. Versuche, dich nicht davon verrückt machen zu lassen. Solange du mit dieser Situation noch nicht so „vertraut" bist, musst du damit rechnen, dass du selbst den wesentlichen Teil einer Observation, die dich selbst betrifft, nicht mitbekommen wirst, ganz einfach, weil sie darauf achten, sich von dir fernzuhalten. Wenn du also ganz sicher bist, dass überall Bullen rumschwirren, kann das durchaus ein Zeichen dafür sein, dass du selbst nicht betroffen bist.

Was kannst du konkret tun

Wir kommen jetzt zum praktischen Teil, der drei Unterpunkte umfasst:

1. Allgemeine Vorsicht
2. Wie stelle ich eine Observation fest
3. Was tue ich, wenn ich eine Observation bemerkt habe

1. Allgemeine Vorsicht

Wenn du selbst links und politisch aktiv bist oder mit Menschen zu tun hast, die es sind, kann es nicht schaden, etwas wachsam durchs Leben zu gehen. Du musst dabei deine eigenen Grenzen überprüfen: Wo fängt auf der einen Seite Leichtsinn an, wo beginnt auf der anderen Seite Paranoia? Manche Leute haben einen Riecher für Bullen, andere bemerken sie nicht einmal, wenn neben ihnen das Funkgerät piepst. Solche Dinge musst du für dich rauskriegen. Deine Wachsamkeit muss für dich in deinen Alltag passen, in deine Blickweise auf die Umgebung. Wenn du mit dem ganzen Repressionsbereich überhaupt nicht umgehen kannst, wenn du ihn nur von dir weghalten willst, dann solltest du dich erst fragen, in welchem Verhältnis dieses Gefühl zu deiner politischen Tätigkeit steht, ob du dir so eine Herangehensweise bei deiner Arbeit leisten kannst oder nicht. Wenn ja, super, wenn nein, musst du dir überlegen, wie du einen erträglichen Umgang damit finden kannst und inwieweit andere dir dabei helfen können.

Bullen und Geheimdienste sind in irgendeiner Form immer präsent, ohne dass daraus unbedingt direkt etwas folgen muss. Nicht umsonst wird immer darauf hingewiesen, dass bei jeder Versammlung mit Spitzeln zu rechnen ist, dass Telefone abgehört werden usw.. Faktisch ist dadurch linksradikale Politik nie verhindert worden.

Der Sicherheitsapparat ist trotz seiner Regeln und Gesetze nicht völlig kalkulierbar und sicher auch oft etwas chaotisch. Oft wissen sie vielleicht selbst gar nicht, was bei ihnen gerade läuft auf den verschiedenen Ebenen.

Allgemeine Wachsamkeit bedeutet, sich über die Präsenz der Bullen im Klaren zu sein und sich davon nicht abhalten zu lassen, etwas zu tun. Schließlich ist es ein wesentliches Moment der „präventiven Repression", über das allgemeine Bewusstsein der ständigen Bullenpräsenz eine Lähmung zu erzeugen. Eine Steigerung erfährt dies durch polizeiliche Beschäftigungsspiele. Scheinbar sinnlose oder ungezielte Schläge des Repressionsapparates dienen manchmal dazu, Leute einfach nur zu beschäftigen, damit sie keine Zeit finden für andere Dinge. Die Initiative liegt damit bei den Bullen. Die sind offensiv und wir rennen den Ereignissen hinterher. Dieser politische Aspekt der Repression ist in anderen Texten vielfach ausführlich behandelt worden.

Allgemeine Wachsamkeit bedeutet, darauf zu achten, wie Bullen sich verhalten. Manchmal kann es nützlich sein, sich vorzustellen, wie und an was sie denken: Wie der Streifen-

bulle denkt und wie die Observationskräfte, wie die Staatsschutzbullen, wie die Führungskräfte. Sie denken sicher nicht nur an uns und unsere „Missetaten", sondern auch an den Feierabend, an die Ratenzahlungen, an den Chef, an die politischen Folgen, an die Karriere, an die Gewerkschaft, an etwas zu trinken, an die arroganten auswärtigen Behörden. Wie sie sich, geprägt durch bürgerliche Medien, vorurteilsgetrübte Spitzelberichte, schwer verständliche Szenetexte und Vorträge von „Szenekenner_innen", dich und deinen Alltag vorstellen. Was ihre moralischen Werte sind, wo sie ihre Berechtigung für ihre Arbeit hernehmen. Wenn du wegkommst von den oft parolenhaften Vorstellungen der Bullen als völlig willenlose Befehlsempfänger_innen oder als fanatische Recht-und-Ordnung-Kämpfer_innen, wird dich manches nicht mehr wundern, was du dir vielleicht sonst nicht erklären kannst, es sei denn durch enorme Verschwörungstheorien (...sie haben nicht eingegriffen, damit wir glauben, sie wissen von nichts... oder... sie haben gerade jetzt zugeschlagen, weil sie alles schon vorher wussten... Das kommt auch schon mal vor, aber meistens ist es banaler.)

Versuche also die Gegner_innen kennenzulernen. Nicht nur wie eben beschreiben ihre (Un-)Logik, sondern auch ganz direkt: Wie sehen sie aus, wie treten sie auf. Die Zeiten, in denen Zivis zu 95% Männer mit kurzen Haaren und Schnauzbärten waren, sind lange vorbei. Heute gibt es viele Frauen dabei. Frauen wie Männer tragen szene-typische Klamotten, die Männer haben oft längere/lange Haare, Ohrringe.

Wie sitzen sie im Auto? Wieso guckt ein Zivi anders aus dem Autofenster als andere Leute? Er oder sie hält Ausschau nach etwas. Allerdings sind Zivis leicht zu verwechseln mit Leuten, die sich in der Gegend nicht auskennen und deswegen sehr aufmerksam sind. Die Aufmerksamkeit der meisten Leute, die Auto fahren, ist eher nach innen gerichtet, zumal, wenn sie nicht alleine im Auto sind. Zivis hingegen achten meist stark auf die äußere Umgebung und unterhalten sich oft kaum mit den anderen im Auto.

Sinnvoll ist es auf jeden Fall für alle, die politisch organisiert arbeiten, sich zu überlegen, inwieweit es notwendig ist, sich auf Repression einzustellen, sich vertrauter zu machen mit den möglichen Bedrohungen durch Observationen etc.. Verlasst euch nicht darauf, dass ab und zu irgendwo irgendwelche Kennzeichen von Ziviautos veröffentlicht werden. Die Listen können Fehler enthalten, die Kennzeichen werden gewechselt. Der beste Schutz ist es, den „Riecher" für Bullen und Spitzel zu entwickeln, und den entwickelst du durch Aufmerksamkeit und Erfahrung.

2. Wie stelle ich eine Observation fest

Angenommen, du hast etwas vor und siehst dich deswegen in der Gegend um. Oder du hast gerade nichts zu tun und gehst aufmerksam spazieren. Wie kannst du bemerken, ob eine Observation in der Ecke läuft:

Am auffälligsten sind die Autos. In diesem einen Fall können wir mal über die Auto-Gesellschaft froh sein, in der wir leben. Autos sind gut zu identifizieren und lassen sich unmissverständlich beschreiben durch das Modell, die Farbe und das Kennzeichen. Fast alle Observationen laufen mit Autos, die Zivis, die zu Fuß unterwegs sind, sind meist ausgestiegene Beifahrer_innen. Das Auto hat für die Bullen diverse Vorteile: Sie können ihre Funkgeräte und sonstiges Material (Fotoapparat, Wechselklamotten) gut verstecken. Sie können laut sprechen und Funksprüche hören, ohne dass es Außenstehenden auffällt. Sie können schnell mal den Ort wechseln. Sie sitzen bequem, können vielleicht sogar mal ein Nickerchen machen, wenn eine Observation sich hinzieht, ohne dass viel passiert. Natürlich gibt es Observationen zu Fuß, mit dem Fahrrad, mit Motorrädern, die sind dann auch meistens schwerer zu erkennen.

In der Regel sind die Observationsfahrzeuge sauber und gepflegt. Es sind alle möglichen Automodelle in allen möglichen Farben, meist PS-starke Versionen, aber keine aufgemotzten oder sonstwie auffälligen Typen. Rechne nicht damit, dass du irgendwelche technischen Besonderheiten siehst, wie Funkgerät, Funkantenne oder so etwas. Die Zeiten, in denen so etwas die Zivi-Autos verraten hat, sind vorbei. Selbst bei „Derrick" haben heutzutage die Autos „Freisprech"-Anlagen, bei denen die Meldung von einem versteckten Raummikrofon aufgenommen wird und das Funkgerät z.B. im Handschuhfach versteckt ist.

Wenn du nun also spazieren gehst, kommst du vielleicht an einem Auto vorbei, das dir auffällt. Du guckst aus dem Augenwinkel genauer hin und siehst: Der Wagen ist sauber, hat eine Antenne, es sitzt jemand drin und liest ein Buch. Ansonsten sieht der Wagen ganz normal aus. Oder es sitzen zwei Leute drin, haben die Sitzlehnen halb heruntergekurbelt und dösen vielleicht vor sich hin. Oder es sitzt jemand drin und blickt konzentriert in eine bestimmte Richtung. Vielleicht siehst du aber auch nur einen Mann oder eine Frau mit Walkman-Kopfhörern, der_die unmotiviert an einer Ecke steht. Kurz darauf rollt langsam ein Auto an dir vorbei, in dem zwei junge Typen sitzen und interessiert aus dem Fenster sehen. Dann zwei Ecken weiter stehen zwei Autos nebeneinander, daneben stehen zwei Pärchen rauchen und quatschen, Wahrscheinlich haben sie normale,

sportliche Freizeitklamotten, ebensolche Schuhe. Weder haben sie „Bullengesichter", noch sehen sie besonders kräftig aus. Aber vielleicht piepst es gerade aus dem einen Auto, wenn du vorbeigehst.

Jetzt hast du möglicherweise schon die zwei wesentlichen Punkte der Observation gesehen: Zum einen die Beobachtungsposition für den Zielort bzw. die Zielperson, zum anderen die Observationskräfte, die sich für eine Verfolgung der Zielperson bereit halten.

Die Beobachtungsposition ist von zentraler Wichtigkeit für die Observation. Deswegen muss diese auch besonders unauffällig sein. Wird diese von Leuten in einem Auto besetzt, werden die Insass_innen vielleicht die Sitzlehnen herunterkurbeln, damit sie bequemer sitzen und von weitem nicht so gut gesehen werden können. Oder sie beschäftigen sich zur Tarnung mit etwas, z.B. Zeitung lesen. Die Beobachtungsposition kann auch zu Fuß gemacht werden. Dann sitzt vielleicht jemand in einem Café mit Blick auf die Haustür der Zielperson und meldet nur kurz, wenn die betreffende Person das Haus verlässt.

Wenn du ein Auto siehst, in dem ein oder zwei Leute sitzen, die konzentriert in eine Richtung gucken, kannst du schon relativ sicher sein, die Beobachtungsposition gefunden zu haben. Diese Position wird, wenn sie nicht gut getarnt ist, normalerweise in einer Entfernung von ihrem Ziel stehen, von der aus sie selbst das Ziel ganz gut im Blick hat, aber selbst außerhalb des unmittelbaren Blickfeldes der Zielperson ist. Das sind i.d.R. 40-80 Meter.

In gewisser Entfernung halten sich die anderen Observant_innen auf. Sie müssen aber doch noch so nah dran sein, dass sie schnell am Start sind, wenn es notwendig wird. Sie werden also darauf achten, dass sie verkehrstechnisch gut angebunden sind und mögliche Fahrtwege der Zielperson schnell erreicht werden können. Vermutlich stehen sie um ein, zwei Ecken, etwa 200-400 Meter entfernt. Wenn sie die Sache lockerer angehen, versammeln sie sich auch mal mit mehreren Autos, steigen aus, quatschen. Es kann aber auch sein, dass sie sich getrennt voneinander aufstellen und einen Ring um das Ziel bilden. Wichtig sind auch Plätze, wo sie sich ungestört treffen und bequatschen können, z.B. Sackgassen oder Parkplätze.

Von Zeit zu Zeit werden die Autos ihre Position ändern. Dann fährt das Auto, das zuerst die Beobachtungsposition hatte, zu den anderen in Bereitschaft stehenden Wagen und ein anderes Auto nimmt die erste Position ein. Ist die Parkplatzsuche schwierig, wartet das erste Auto, bis das es ablösende Auto kommt und überlässt ihm dann den Parkplatz.

Folgende Punkte sind ein Hinweis darauf, dass eine Observation am Laufen sein kann:

- Hast du Personen gesehen, die einen festen Ort fixieren?
- Hast du Personen mit Kopfhörern gesehen?
- Hast du Autos gesehen, die über mehrere Minuten unverändert mit Insass_innen parken?
- Hast du fahrende oder parkende Autos gesehen, die du für Ziviwagen hältst?
- Hast du aus Autos Funksprüche gehört?

Wenn du davon ausgehst, eine Observation entdeckt zu haben, ist der zweite Schritt herauszufinden, wo das Zielobjekt der Observation ist. Um die Beobachtungsposition herauszubekommen, kannst du sie entweder direkt suchen, also nach jemandem Ausschau halten, der_die konzentriert einen Ort ansieht oder du überlegst, welche Orte sich in der Umgebung befinden, die observiert werden könnten und suchst in der Nähe dieser Orte. Wenn du das Objekt der Begierde nicht herausfindest, kannst du nicht viel mehr machen, als in der nächsten Zeit aufmerksam durch die Gegend zu laufen. Ohne Identifizierung des Ziels ist eine Observation ein unkalkulierbares Ereignis für dich. Dementsprechend solltest du dich darauf beschränken sicherzustellen, dass es nicht um dich oder dir bekannte mögliche Zielpersonen/-objekte geht.

Kannst du die Beobachtungsposition ausfindig machen, versuche als nächstes, die Blickrichtung zu erkennen. Zwar weißt du, dass das Ziel sich in einer gewissen Entfernung befinden muss, du weißt aber nicht, ob es sich um ein Haus, ein Auto oder noch etwas anderes handelt. So kann es sich z.B. um ein Auto handeln, dass 100 Meter weit entfernt geparkt ist, aber auch noch aus der Entfernung gut gesehen werden kann, wenn es losfährt. Du kannst zuerst versuchen, mögliche Ziele auszuschließen. Dazu gehören alle Objekte in unmittelbarer Nähe der Beobachtungsposition, also die zwei bis drei Hauseingänge, Kneipen oder Läden direkt bei der Beobachtungsposition. Bedenke aber dabei, dass von einem Auto aus auch über Rück- und Außenspiegel gearbeitet werden kann. Trotz dieser Anhaltspunkte ist die Chance, das genaue Zielobjekt herauszufinden, sehr gering. Zumindest kannst du es aber örtlich einigermaßen eingrenzen und vor allem kannst du einschätzen, ob deine eigene Haustür, dein Auto oder Fahrrad oder das deiner Genoss_innen betroffen sein könnten.

Kommst du zu der Einschätzung, dass dein eigener Hauseingang im Bereich des Blickfelds liegt, wird dein Adrenalinspiegel wahrscheinlich erst einmal nach oben jagen. Trotzdem: Bleib ruhig. Bisher sind es nur Vermutungen. Es gibt viele andere Möglichkeiten neben der, dass es um dich persönlich geht. Allerdings ist es sinnvoll, wenn eine Observation deiner Haustür nicht auszuschließen ist, gewisse Vorsichtsmaßnahmen zu treffen. Z.B.: Gibt es Leute, die beim Betreten des Hauses besser nicht von Zivis gesehen werden sollten?

Lagern Sachen bei dir zu Hause, die dir in so einer Situation unangenehm werden? Möchtest du selber lieber nicht als Anwohner_in des Hauses identifiziert werden? Du musst also anfangen zu überlegen, wie du dich weiter verhalten sollst: Die Gefahr ignorieren, Leute warnen, Gegenmaßnahmen ergreifen? Darum geht es im dritten Teil.

3. Was tun, wenn ich eine Observation bemerkt habe

Wenn du sicher bist, eine Observation bemerkt zu haben, willst du natürlich wissen, ob sie etwas mit dir zu tun hat. Gibt es dafür weder Anhaltspunkte noch Gegenbeweise, kannst du mit einer Gegenobservation versuchen, Genaueres herauszubekommen. Dazu brauchst du ein paar Leute, denen du vertraust und die über eine gute Beobachtungsgabe verfügen. Dann arbeitest du einen Weg aus, den du zu einer bestimmten Zeit zurücklegen wirst. Dieser Weg sollte so gestaltet sein, dass er sich gut in deinen Alltag einfügt, damit etwaige Observant_innen nicht merken, wie der Hase läuft. Der Weg sollte außerdem ein paar Biegen haben, damit ausgeschlossen werden kann, dass z.B. ein Auto nur zufällig hinter dir dieselbe Strecke fährt. Die Strecke muss nicht besonders lang sein. Sie sollte nicht dauernd Hauptverkehrsrouten folgen, aber auch nicht zu sehr um sich selbst kreisen, da es sonst passieren kann, dass die Observationsgruppe einfach einen Ring drumherum bildet. Es können kurze Stopps eingebaut werden, durch die dann auch plötzliche Richtungswechsel plausibel werden. Z.B. bewegst du dich erst zu einem Copyshop und kopierst dort etwas, dann biegst du ab quer zur bisherigen Richtung und fährst zu einem Briefkasten, in den du etwas einwirfst. Dann kannst du wieder die Richtung wechseln und kaufst in einem Laden eine Zeitung. Am besten ist es, die Strecke in einem Auto zurückzulegen, denn dann wirst du auch von Fahrzeugen verfolgt und nicht zu Fuß. Die Fahrzeuge sind leichter und genauer zu beschreiben als Personen. Da du ja herausbekommen willst, ob jemand hinter dir her ist, macht es natürlich keinen Sinn zu versuchen, mögliche Verfolger_innen abzuhängen. Auch solltest du vermeiden, selbst zu checken, das machen ja andere für dich. Deine Verfolger_innen sollen sich möglichst sicher fühlen.

Die festgelegte Route hast du deinen Genoss_innen vorher mitgeteilt. Wenn es dir zu gefährlich erscheint, dich direkt mit ihnen zu treffen, musst du einen anderen Weg der Übermittlung finden. Am einfachsten ist es aber, den Weg mit Leuten abzuklären, mit denen du problemlos und unverdächtig zusammenkommen kannst und die mit großer Wahrscheinlichkeit selbst nicht observiert werden. Deine Freund_innen postieren sich dann möglichst unauffällig zum gegebenen Zeitpunkt entlang der von dir zurückzulegenden Strecke. Sie notieren genau, wann du vorbeikommst und was sich hinter dir alles bewegt: Autos mit Uhrzeit, Kennzeichen, Farbe, Modell. Hinterher werden die Beobachtungen zusammengetragen. Wirst du wirklich observiert, müsste sich das daran zeigen, dass an den verschiedenen Stellen die gleichen Personen oder Autos gesehen worden sind. Wahrscheinlicher ist aber, dass deine Freund_innen die Observant_innen unmittelbar erkannt haben, denn um an dir dranzubleiben, müssen sie manchmal mit hohem Tempo und unter Missachtung der Straßenverkehrsordnung durch die Straßen jagen. Für sie ist das wichtigste an dir dranzubleiben, dabei aber nicht von dir gesehen zu werden. Da bleibt wenig Raum für Rücksichtnahme auf andere Verkehrsteilnehmer_innen.

Natürlich bleibt eine Restunsicherheit. Es könnte sein, dass du einen Peilsender am Auto hast und die Observierenden deswegen einen größeren Abstand gehalten haben (aber hinterherkommen tun sie trotzdem!). Oder aber sie waren erst an dir dran, haben dich dann aber verloren. Oder sie haben wenige Minuten, bevor du die Route abgefahren bist, Feierabend oder Mittagspause gemacht. Deswegen kannst du über eine Gegenobservation immer nur darüber Gewissheit erlangen, ob sie an dem speziellen Zeitpunkt an dir drangehangen haben. Trotzdem hast du gute Chancen, wenn du Zeit und Ort gut wählst, dadurch eine ausreichende Gewissheit für deine unmittelbaren aktuellen Vorhaben zu bekommen.

Du kannst auch, wenn du alleine bist, versuchen etwas herauszubekommen. Dann fahre mit dem Auto oder mit dem Fahrrad eine vorher überlegte Route, die dir folgende Möglichkeiten bieten sollte: Du solltest überraschende Wendemanöver machen können – möglichst mit einer plausiblen Erklärung, z.B. eine fehlende Linksabbiegemöglichkeit. Oder du wählst eine lange, gerade Strecke ohne Abbiegemöglichkeit aus, auf der du dann plötzlich am Straßenrand anhältst. In beiden Fällen sind deine Verfolger_innen gezwungen, an dir vorbeizufahren, wenn sie dir nicht auffallen wollen. Du kannst dir dann Autos, Kennzeichen, Gesichter versuchen einzuprägen und den ganzen Vorgang an anderer Stelle noch einmal wiederholen, um zu sehen, ob es irgendwelche Übereinstimmungen bei den vorbeifahrenden Fahrzeugen gibt. Um diese Form der Gegenobservation durchzuführen, musst du allerdings in der Lage sein, dich so zu verhalten, dass die Bullen nicht merken, was du gerade mit ihnen machst. Das erfordert vor allem die Fähigkeit, auch in einer für dich angespannten Situation ruhig zu bleiben. Außerdem musst du schon einen „Riecher" für Bullenautos haben, denn du kannst dir meist unmöglich die Kennzeichen aller vorbeifahrenden Fahrzeuge merken.

Wenn du herausgefunden hast, dass die Observation tatsächlich dir gilt, musst du deine nächsten Schritte in Ruhe überlegen. Das solltest du nicht alleine tun, sondern mit einigen wenigen, dir vertrauten Menschen.

Wer und was ist gefährdet?

Unabhängig davon, warum sie an dir dranhängen, ist zu überlegen, ob es irgendwelche Leute gibt, die in Mitleidenschaft gezogen werden könnten. Denen muss Bescheid gesagt werden, aber vielleicht besser nicht von dir persönlich.

Gibt es bei dir zu Hause, in deinem Auto oder an Orten, wo du dich öfters aufhältst, Sachen, die gefährlich sein könnten, sollten diese diskret woanders hingebracht werden.

Du solltest erst einmal nicht mehr Leute informieren, als unbedingt notwendig ist. Entstehen erst einmal Gerüchte über Observationen, führt dies vor allem zu Panik, Nervosität, auffälligem Verhalten von Leuten und zu Gerede über mögliche Hintergründe der Observation. Das kann dir alles eher schaden als nützen.

Was kann der Grund für die Observation sein?

Um sich dieser Frage zumindest zu nähern, tragt möglichst alle Beobachtungen zusammen: Daten, Zeiten, Fahrzeuge, wann du wo warst. Vermutungen sind von sicheren Beobachtungen zu trennen. Versucht dann, zu einer Einschätzung zu gelangen, was die Observant_innen schon alles mitbekommen haben (könnten). Überlegt, was es alles für Gründe für ihre Aktivitäten geben könnte. Denkt dabei nicht nur an deine realen Tätigkeiten und Konflikte, sondern auch daran, was aufgrund von Zufällen oder unbeabsichtigten Konstellationen denkbar wäre. Z.B. wenn du mit jemandem polizeilich erfasst worden bist, etwa bei einer früheren Festnahme. In was für einem Fahrzeug bist du festgestellt worden? Wann und wo hast du die Dinge getan, die irrtümlich als konspirativ angesehen werden könnten?

Was kann in Zukunft drohen?

Ausgehend von der Arbeitshypothese, um was es bei der Observation geht, könnt ihr überlegen, wie die Sicherheitsbehörden weiter vorgehen werden. Eine unbekannte Größe ist dabei natürlich die Frage, ob es die Bullen sind oder ein Geheimdienst, die dich im Visier haben. Sind es die Bullen, läuft mit großer Wahrscheinlichkeit ein Ermittlungsverfahren gegen dich, dabei wird es dann meist in einem Zusammenhang mit §129, §129a (kriminelle/terroristische Vereinigung) stehen. In diesem Zusammenhang ist kurz zu erwähnen, dass diese beiden Paragraphen vor allem Ermittlungsparagraphen sind, die benutzt werden, um den Repressionsapparat rundlaufen zu lassen. Die wenigsten 129a-Verfahren führen zu Prozessen und Verurteilungen. Meistens werden sie genutzt, um eine Observation überhaupt zu legitimieren. Daher muss nicht zwangsläufig einer §129a-Observation eine Durchsuchung und/oder Festnahme folgen. Und wenn doch, heisst das noch lange nicht, dass es auch tatsächlich zu einem Prozess kommt. Du solltest dich zwar besser mit diesem Gedanken vertraut machen, aber es kann sein, dass die Observation irgendwann endet und für dich weiter nichts Erkennbares daraus folgt, mal abgesehen davon, dass deine Akte beim Staatsschutz oder VS wieder etwas dicker geworden ist.

Geheimdienste unterliegen nicht formal dem Legalitätsprinzip, d.h. sie können dich „bei Bedarf" observieren, wie sie wollen. Ob dann etwas Weiteres daraus folgt, hängt davon ab, ob der Geheimdienst die Bullen aktiviert.

Wenn eine Observation – was passieren kann – monatelang dauert, kannst du nicht die ganze Zeit mit gepackten Koffern leben, ob nun zum Abhauen oder für den Knast. Du musst irgendwann in dieser Situation einen Alltag für dich finden, sonst drehst du ab. Das heißt du musst entweder auf Dauer auf bestimmte Sachen verzichten oder du musst sie so regeln, dass du sie trotz der laufenden Observation durchführen kannst.

Manche Leute haben jahrelang unter der ständigen Bedrohung durch Observationen gelebt und auch politisch gearbeitet. Sie werden vermutlich viele ihrer Erfahrungen, die sie in dieser Zeit gemacht haben, nicht veröffentlichen, um den Bullen keine Hinweise dafür zu liefern, wie sie es angestellt haben, die Observation ins Leere laufen zu lassen. Wer betroffen ist, muss sich deshalb ziemlich viel selbst einarbeiten oder direkt den Austausch mit in dieser Hinsicht erfahrenen Genoss_innen suchen. Vor allem musst du aber mit deinen eigenen Leuten herausbekommen, was für dich/euch geht und was nicht.

Was kannst du selber tun?

Es gibt verschiedene Möglichkeiten, wie du dich verhalten kannst: Du kannst weiterleben wie bisher und ggf. auf gefährliche Sachen verzichten. Dabei nimmst du aber in Kauf, dass die Gegenseite einiges über dich und deine sozialen Kontakte und deine politischen Zusammenhänge in Erfahrung bringt. Der Vorteil dieser Umgangsweise ist, dass du die Observation weitgehend ignorieren kannst. Um andere zu schützen, musst du aber bedenken, wohin du die Zivis vielleicht mitschleppst und auf wen sie dabei aufmerksam werden könnten.

Eine andere Umgangsweise ist, dein politisches Leben auf Sparflamme zu drehen, du gehst sozusagen in Deckung und wartest, bis der Gegenseite die Observation langweilig oder sinnlos geworden ist, weil sie einfach nichts Interessantes zu sehen bekommen. Allerdings musst du bei diesem Verhalten bedenken, dass sie vielleicht schon länger an dir dran sind, als du es weißt und es ihnen von daher auffallen könnte, wenn sich dein Lebenswandel plötzlich verändert.

Oder aber du gehst offensiv mit der Geschichte um. Du lässt die Observant_innen „verbrennen", indem du sie offen ansprichst, fotografierst o.ä.. Vielleicht kannst du das politisch gegen sie wenden, wenn das entsprechende Klima und eine Öffentlichkeit dafür vorhanden sind.

Aber du riskierst auch, dass sie sich jetzt erst recht um dich kümmern, vielleicht etwas abwarten und dann eine bessere Truppe gegen dich einsetzen, die du dann nicht mehr so leicht bemerkst. Insofern solltest du dich mit anderen beraten, sofern du dich für diese Umgangsweise entscheidest. Die Verlockung ist groß, den Zivis zu zeigen, dass du sie erkannt hast und sie dich sonstwas können. Aber du tauschst vielleicht gegen dieses kurzfristige Erfolgserlebnis den langfristigen Verlust einer möglichen Kontrolle über die Observation.

Es kann in jedem Fall sinnvoll sein, eine_n Anwält_in einzuschalten. Auch hier musst du überlegen, was du ihm_ihr sagst und was besser nicht. Anwält_innen können natürlich keine Wunder vollbringen und in der Regel kennen sie sich zwar mit Justizangelegenheiten gut aus, nicht aber unbedingt mit Bullen/VS.

Grundsätzlich solltest du auffälliges Verhalten vermeiden: Dich also nicht dauernd auf der Straße umdrehen oder oft aus dem Fenster spähen. Im Bereich deines von außen einsehbaren Fensters solltest du keine „konspirativen" Handlungen begehen. Und unternehme keine halbherzigen Versuche, deine Verfolger_innen abzuschütteln. Letzteres solltest du überhaupt nur tun, wenn es unbedingt notwendig ist und das Gelingen auch einigermaßen gesichert ist, mit Unterstützung von anderen Leuten. Denn alles, was die Observant_innen „konspirativ" finden könnten, macht dich nur interessanter.

Bist du öffentlich politisch organisiert, musst du dir zusammen mit deinen Vertrauten überlegen, inwieweit du deine Gruppe einweihst. Es müssen nicht unbedingt alle Bescheid wissen, je nachdem, wie die Gruppenstruktur ist. Gerade wenn unerfahrene oder wenig belastbare Leute in deiner Gruppe sind, solltest du einen sehr genauen Umgang mit der Lage entwickeln. Manchmal ist es leider so, dass Warnungen mehr Schaden als Nutzen bringen können, dann kann verantwortungsbewusstes Umgehen besser sein als verbale Warnungen.

Vielleicht machst du lieber eine Weile Urlaub oder ziehst dich zumindest aus Teilen der Gruppenarbeit zurück.

Wenn du klandestin organisiert bist, ist die Situation natürlich eine völlig andere. Du musst dann sehr genau diskutieren, inwieweit diese Arbeit durch deine Observation bereits gefährdet sein könnte und ob du teilweise oder ganz die Finger davon lassen solltest! Umgekehrt kann aber auch ein plötzlicher Abbruch bestimmter Kontakte gerade auffällig erscheinen. Klar ist, dass die anderen, mit denen du in so einer Form organisiert bist, über die Situation informiert sein müssen. Diese Form der Organisierung bedeutet aber nicht automatisch, dass alle dieser Situation auch gewachsen sind. Leichtsinn, Selbstüberschätzung (gerade bei Männern), Unsicherheit, Paranoia, Schwatzhaftigkeit, Ungenauigkeit – all dies gibt es auch in klandestinen Strukturen.

Hast du festgestellt, dass die von dir beobachtete Observation NICHT dir gilt, gibt es keinen Anlass herumzulaufen und allen zu erzählen, was abgeht. Das sollte stets das letzte Mittel der Informationsvermittlung sein, wenn du überhaupt keine Idee hast, wem die Observation gilt und wem du Bescheid sagen könntest. Ansonsten wird so oft Panik erzeugt, indem Halbwissen oder Vermutungen mit Beobachtungen vermischt werden und Leute, die sich wichtig machen wollen, herumlaufen und Räuberpistolen erzählen. Besser ist es allemal, einzelnen Leuten Bescheid zu geben, von denen du annehmen kannst, dass sie ruhig bleiben und die notwendigen Infos an die richtigen Stellen weitergeben. Vielleicht könnt ihr ja rausfinden, um wen es bei der Observation geht. Wenn die Sache so läuft, sollte der Fall damit für dich beendet sein. Zwar mag es interessant sein, auf dem Laufenden zu sein, wer wo beobachtet wird, aber das ist den Betroffenen sicher nicht recht. Deswegen solltest du dich an das halten, was auch für militante Aktionen gilt: Bescheid weiß, wer damit zu tun hat, alle anderen halten sich an Anna und Arthur.

Wenn du observiert wirst...

...ist es sinnvoll sich an folgende Grundregeln zu halten:

Eine Observation bedeutet nicht das Ende aller Möglichkeiten.

- Eine Observation geht normalerweise nicht über längere Zeit rund um die Uhr, denn das ist personell nicht durchzuhalten. Nach einer längeren Phase der intensiven Observation kann es sein, dass eine längere Ruhepause folgt. D.h. zum einen, dass Observationen nicht für immer und ewig dauern, zum anderen aber auch, dass sie irgendwann wieder fortgeführt werden können. So eine Pause kann wochen- oder sogar monatelang dauern.
- Oder aber am Ende einer Observation steht eine Durchsuchung, eine Vorladung oder sogar eine Verhaftung.
- Bleib ruhig und gelassen. Hektik nutzt nur den Observant_innen.
- Versuche, zuverlässige Freund_innen einzubinden, um dich zu schützen und um Aufgaben zu übernehmen, die du selbst momentan nicht machen kannst. Rede mit ihnen, aber wirklich auch nur mit ihnen und das nicht nur technisch, sondern auch über Ängste und Unsicherheiten.
- Überlege dir, eine_n Anwält_in einzuschalten, damit du zumindest im Fall einer plötzlichen Festnahme schon weißt, an wen du dich wenden kannst.
- Rechne sicherheitshalber mit dem Schlimmsten. D.h.: Rechne mit einer technischen Überwachung deiner Wohnung und deines Autos. Das beinhaltet sowohl Kameraüberwachung als auch Wanzen (wenn auch unwahrscheinlicher), als auch Peilsender. Bezüglich der Überwachung deines Telefons und deiner Post kannst du sicher sein! Rechne damit, dass es nicht nur um dich, sondern auch um andere Leute geht. Rechne damit, dass du irgendwann festgenommen oder sogar verhaftet wirst.
- Säubere die Orte, die durchsucht werden könnten: Wohnung, Dachboden, Keller, Auto, Garage etc.
- Überlege dir, wo du in deiner Wohnung nicht kontrolliert werden kannst, wie du evtl. unbeobachtet das Haus verlassen kannst oder wie du dich ansonsten unauffällig der Observation entziehen kannst, falls es notwendig ist/wird.
- Vermeide jedes „konspirativ" erscheinende Verhalten.
- Versuche, einen Alltag in dieser Bedrohungssituation für dich zu entwickeln.
- Schreibe dir deine Beobachtungen auf und werte sie mit deinen Freund_innen aus.
- Entwickle eine These für den Grund der Observation, mit der du umgehen kannst. Überlege dir Perspektiven für dein zukünftiges Handeln.

Der schlimmste Fall für die Observant_innen ist die Zielperson, die den Spieß umgedreht hat und ihrerseits die Observierenden unter Kontrolle hat!

Der schlimmste Fall für dich ist Leichtsinn und Kopf-in-den-Sand-stecken! Aber der zweitschlimmste Fall ist Panik und Lähmung!

All denen, die gesucht oder observiert werden, wünschen wir alle nötige Kraft – lasst euch nicht verhärten in dieser harten Zeit!

Setzen wir Wissen gegen Paranoia!