Überwachungstechnik

<<TableOfContents>>

= Überwachungstechnik =

Der Schwerpunkt dieser Seiten liegt zwar auf Datenbanken und nicht auf der Akquise von Material, aber ganz ausblenden wollen wir das Thema der technischen Hilfsmittel nicht, zumal ja Datenbanken nicht unabhängig von den Methoden der Datensammlung bestehen.

Neben den hier diskutierten Hilfsmitteln zu Überwachung und Observation gibt es noch die klassischen Methoden verdeckter Informationsbeschaffung wie [[Observation]], [[Verdeckte Ermittler]] und [[V-Leute]]. Technisches zur Telekommunikationsüberwachung ist ausgegliedert nach LawfulInterception ("Abhören") bzw. [[TK-Verkehrsdaten]].

== Vorbemerkung ==

Vorsicht vor Paranoia: 99.99% der "komischen Dinge", die Computer oder Telefone so tun, haben nichts mit gezielter Überwachung zu tun. Dennoch ist ohne verlässliche Ende-zu-Ende-Verschüsselung mit gegenseitiger Authentifikation (z.B. PGP mit ordentlichem Schlüsselmanagement) nicht davon auszugehen, dass bei Telekommunikation Vertraulichkeit herrscht.

== Lawful Interception ==

Das Abhören von Telekommunikation läuft unter dem schönen Begriff LawfulInterception -- siehe dort.

Zu Vorratsdatenspeicherung, Funkzellenabfrage, stiller SMS und ähnlichem siehe [[TK-Verkehrsdaten]].

== Wohnraumüberwachung (Großer Lauschangriff) ==

Der "Große Lauschangriff" hat in der Repressionspraxis eine weitaus geringere Relevanz als die politische Aufmerksamkeit (verglichen mit anderen Repressionstechnologien) das vermuten lässt. [[http://www.bmj.de/files/-/1319/Bericht%20Wohnraumüberwachung_270906.pdf|Das BMJ berichtet]] für 2006 (nach dem etwas beschränkenden BVerfG-Beschluss) von 7 überwachten Objekten mit 27 Betroffenen. Bayern ist dabei effizient: 13 Tage abhören kostet dort 45.24, in NRW kosten 16 Tage rund 50000 Euro.

Zahlen von 2006/07 bietet [[http://dip21.bundestag.de/dip21/btd/16/103/1610300.pdf|BT-Drucksache 16/10300]].

Rechtsgrundlage im Strafrecht ist §100c StPO, der relativ hohe Hürden setzt; im Politbereich erlaubt wie immer das 129a-Konstrukt großzügige Eingriffe.
Wohl dank der Prosa über den Schutz des "Kernbereichs der persönlichen Lebensgestaltung", der bei den Maßnahmen geschützt bleiben muss, halten sich die Berhörden derzeit noch weitgehend zurück. Dies ist um so bemerkenswerter, als §100c auch die Rechtsgrundlage für die allseits befürchtete Raumüberwachung mit Mobiltelefonen wäre.

Auch diverse Landesgesetze erlauben den großen Lauschangriff zur "Gefahrenabwehr", so etwa §23 PolG Baden-Württemberg, das ihn zur "Abwehr einer unmittelbar bevorstehenden Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leben, Gesundheit oder Freiheit einer Person" erlaubt. Wie weit solche Befugnisse wirklich eingesetzt werden, ist nicht bekannt.

=== Wanzen ===

Zur Aufzeichnung von Geräuschen in Räumen werden verschiedene Geräte eingesetzt, im einfachsten Fall ein schlichtes Mikrofon mit Sender; da diese allerdings mit verschiedenen "Wanzendetektoren" relativ einfach zu lokalsieren sind, werden zunehmend Geräte eingesetzt, die die Signale zunächst aufzeichnen und dann komprimiert übertragen.

In Heidelberg wurde 2011 eine Art Handy-Wanze im dortigen Fachschaftenbüro (der Studivertretung) gefunden, welche dort vermutlich vom [[Verdeckte Ermittler|Verdeckten Ermittler]] Simon Bromma angebracht wurde (vgl. [[http://peter-nowak-journalist.de/2011/06/09/%C2%BBdu-fahrst-zu-oft-nach-heidelberg%C2%AB/|Du fährst zu oft nach Heidelberg]] von Peter Nowak). Dieser Einsatz allerdings dürfte sich nicht auf Regelungen zur Wohnraumüberwachung gesstützt haben, da der Raum eben kein Wohnraum war; im Strafverfahren wäre hier §100f StPO einschlägig gewesen, da Bromma zur Gefahrenabwehr eingesetzt war, wird sich die Polizei auf §22 (1) PolG berufen.

- [[http://www.expertenwissen.eu/bedienungsanleitungen/minisender.pdf|Beschreibung und Bedienungsanleitung eines Wanzendedektors der Firma alarm.de]]
- Zahlreiche Bauformen und Varianten von Wanzen finden sich im <<Doclink(2011-elaman-katalog.pdf,Elaman-Katalog von 2011)>>

=== Mobiltelefone als Wanzen ===

Da Mobilelefone bereits mit Mikrofon und Sender ausgestattet sind, können sie relativ leicht als Wanzen eingesetzt werden. Dies wird etwa im [[http://www.heise.de/newsticker/Polizei-nutzt-Handys-als-Wanzen--/meldung/92713|Heise-Newsticker 2007]] diskutiert. Zumindest die Polizeien des Bundes der BRD haben das aber nach [[http://dip.bundestag.de/btd/16/060/1606079.pdf|Bundestags-Drucksache 16/6079]] (2008) bisher nicht getan.

Ein Grund für die Zurückhaltung dürfte sein, dass der Teufel dabei im Detail liegt und in aller Regel die Software des Telefons in zum Teil nichttrivialer Weise manipuliert werden muss. Wenn allerdings Wohnraumüberwachung populärer wird, dürften entsprechende Lösungen von privater Seite wenigstens für verbreitere Telefone verfügbar werden. Insbesondere ist zu bedenken, dass

moderne Telefone Wochen und Monate von Umgebungsgeräuschen aufzeichnen und speichern und diese Daten ggf. auf Bestellung übermitteln können.

Aber nochmal: Es gibt keine Belege, dass sowas in der BRD überhaupt gemacht wurde, eine verbreitete Praxis ist es jedenfalls nicht.

- [[http://datenschmutz.de/gc/cellphones.pdf|Rote Hilfe Zeitung über die Überwachungsmöglichkeiten durch Handys]] (pdf)

== Akustische Überwachung außerhalb von Wohnungen ==

Außerhalb von Wohnungen erlaubt im Strafverfahren §100f die verdeckte Tonaufzeichnung grob unter den Bedingungen des Telefonabhörens. Nicht Beschuldigte dürfen im Rahmen einer Verhältnismäßigkeitsabwägung in Mitleidenschaft gezogen werden. Entsprechende Regelungen finden sich in vielen Polizeigesetzen zur Gefahrenabwehr (z.B. §22 PolG BaWü).

Ein besonders widerwärtiges Gerät zum Abhören in dieser Weise findet sich im <<Doclink(2011-elaman-katalog.pdf,2011 geleakten Spitzelkatalog von Elaman)>> auf PDF-Seite 19 ("Model 6309 Audio Scope System"); es erlaubt durch eine Art inverser Wellenfeldsynthese, auf einzelne Schallquellen zu "zoomen", ggf. auch im Nachhinein.

=== Direktes Abhören von GSM-Verbindungen ===

Die Verschlüsselung auf der Luftschnittstelle von GSM kann inzwischen als gebrochen angesehen werden. Bei legaler Überwachung dürfte das keine Rolle spielen, da die Sicherheitsbehörden problemlos eine Telefonüberwachung mittels [[LawfulInterception]] einleiten können.

Bei halblegalen bis illegalen Überwachungen allerdings schon. So tauchen inzwischen kommerzielle Lösungen auf, die -- wohl vor allem für Private oder Geheimdienste außerhalb ihrer Jurisdiktion -- das Abhören von GSM-Telefonaten über die Luftschnittstelle erlauben; Ein [[http://ftp.ccc.de/documentation/sigint/enfopol-2002/Telco_Surveillance_Systems/IMSi%20Catcher/GSM%20Abh%f6ranlage.pdf|Whitepaper zu einem solchen Gerät]] der Firma [[http://www.alarm.de|alarm.de]] wurde 2002 noch für 200000 Dollar verkauft. Inzwischen sind weit billigere Lösungen verfügbar.

== Stille SMS ==

Stille WikiPedia:SMS sind Kurzmitteilungen die vom Handy nicht angezeigt werden und so unbemerkt [[TK-Verkehrsdaten]] erzeugt werden, welche von der Polizei beim Mobilfunkprovider abgefragt werden können.

vgl [[TK-Verkehrsdaten#Stille_SMS]]

== GPS Peilsender == [[http://www.mini-gts-peilsender.de/|Mini Peilsender]] werden für jederman/frau verkauft, d.h. auch zum Überwachen von untreuen Lebenspartnern. Die Position wird per GPS bestimmt und per SMS mitgeteilt. Da das Senden von SMS nicht unbemerkt bleibt, lässt sich so etwas durch einen Wanzendetektor finden. Vgl.

[[http://howto.wired.com/wiki/Check_Your_Car_for_a_GPS_Tracker|Check Your Car for a GPS Tracker]]

Das Programm zur [[Observation]] mit Hilfe eines GPS-Peilsenders heißt [[Patras]] und wird von der [[Bundespolizei]], [[BKA]], [[Zoll]] und den [[LKA]]s der Länder verwendet. Zumindestens geht das aus einem Hack der [[http://dl.nn-crew.cc/|NoName Crew]] hervor, welche laut [[http://www.spiegel.de/netzwelt/web/0,1518,773189,00.html|Spiegel]] Juli 2011 den Server des Zolls für die Observation per GPS gehackt hatte. Danach laden sich das die Observierer (d.h. MEKs) der Polizei das Programm auf einem Laptop und mit Hilfe einer festen GPRS-Verbindung werden die Daten über einen zentralen Server übertragen. Die Peilsender selber senden die Daten mit Hilfe von SMS über ein [[PAIP]] (Police Applications Intercommunication Protocol), das PAIP wird auch bei Wanzen und ähnlichem zur Übertragung verwendet (vgl [[http://de.indymedia.org/2011/07/311418.shtml|Indymedia]])

== IMSI-Catcher ==

IMSI-Catcher imitieren eine Funkzelle mit starker Sendeleistung, so dass die Handys in der Nähe sich bei dieser Funkzelle melden. Der IMSI-Catcher kann so die IMSIs (d.h. die eindeutige Nummer der SIM-Karte) der sich in einem gewissen Umkreis zum IMSI-Catcher befindenen Handys ermitteln.

vgl [[IMSI-Catcher]]

== WLAN-Catcher ==

In <<BtDS(17/8544)>> erwähnt die Bundesregierung, das BKA habe zwischen 2007 und 2011 16 Mal einen "WLAN-Catcher" eingesetzt (die anderen Bundesbehörden haben sich sowas nicht aufschwatzen lassen). Zu dessen Zweck führt die Regierung aus:

{{{#!blockquote Ein WLAN-Catcher erfasst die über ein WLAN geführte Kommunikation einschließlich der anfallenden verbindungsbegleitenden Daten. [...] Für die Ermittlung des WLAN-Namens (Service Set Identifier -- SSID) für Zwecke der Strafverfolgung können die allgemeinen Befugnisregelungen der §§ 161 und 163 StPO heran- gezogen werden. }}}

Es ist nicht wirklich klar, was das BKA da gekauft hat. Vorstellbar wäre ein Gerät, das eine WLAN-Verbindung anbietet (vielleicht mit einer SSID "Free WLAN" oder so, wie sie von privatrechtlichen Bösewichtern gerne an Flughäfen eingesetzt werden) und hofft, ein Rechner würde sich automatisch damit assoziieren, um dann abzuhören, was die Maschine zu sagen hat. Dagegen würde aber die Prosa zur SSID sprechen.

Denkbar wäre auch, dass das BKA versucht, existierende Funkzellen zu überbrüllen, um Rechner auf ihren Access Point zu zwingen und so abzuhören, was die Maschine so kommuniziert. Das allerdings ist sehr wacklig, funktioniert mit verschlüsselten Netzwerken nur, wenn der Rechner sehr unvorsichtig konfiguriert ist und hat ohnehin wohl wenig Wert, weil ja entsprechende Daten in der Regel vom Provider abgegriffen werden können.

In Summe liegt die Vermutung nahe, dass jemand dem Staat stark überteuerte Mobilrechner andreht.

== Kameras am Arbeitsplatz == Die am Arbeitsplatz eingesetzten Kameras sind Mini-Kameras und senden ähnlich wie Wanzen per Funk ihre Aufzeichnungen. Sie lassen sich daher auch mit einem Wanzendetektor aufspüren. Kameras, die über eine interne Speicherkarte verfügen, lassen sich auf Grund der Reflektion des Objektivs der Kamera aufspüren (Allerdings nur für Geübte).

[[http://www.shop-alarm.de/ALONMA_Detector_und_Linsenfinder_zur_Ortung_versteckter_Kameras.html|Produktbeschreibung eines professionellen Kameradetektors]]

== Kameras vor der Haustür == Aus den Akten von etlichen [[129a Verfahren]] geht hervor, dass Kameras vor den Hauseingängen angebracht wurden. Inwieweit es sich dabei um Mini-Kameras oder um Kameras in benachbarten Wohnungen handelt, geht aus den Akten nicht hervor. Mini-Kameras lassen sich in der Regel auch durch Wanzendetektoren aufspüren. Desweiteren gibt es noch die Methode mit Hilfe eines Spiegel nach einem Objektiv zu suchen, da Kameras zumindestens ein Mini-Objektiv haben müssen. Im Juli 2011 haben laut [[http://de.indymedia.org/2011/07/311409.shtml|Indymedia]] (mit Fotos) Bewohner neben eines ehemaligen Besetzten Hauses in Berlin, welches vor kurzem geräumt wurde, Kameras in den Dachfenstern der gegenüberliegenden Schule entdeckt.

== Kameras in der Wohnung ==

Nach dem neuen [[BKA]]-Gesetz, darf das [[BKA]] auch Kameras in Wohnungen installieren. In [[Belgien]] ist das anscheinend schon länger erlaubt, denn die haben 2011 eine Kamera hinter der Lüftung in ihrer Küche gefunden. Auf [[http://ovl.indymedia.org/news/2011/05/31487.php|Indymedia Belgien]] wird beschrieben, wie sie aussieht und wo sie angebracht wurde.

== Hubschrauber mit Kameras ==

Laut dem [[http://linksunten.tachanka.org/de/system/files/data/2010/12/1693129053.pdf|Polizeibericht 2010]] können, die an den Aufklärungshubschraubern befestigten Kameras, schon aus mehreren 100 m Höhe Potrait-Aufnahmen anfertigen. Bei Dunkelheit werden Nachtsichtkameras oder Infrarotkameras verwendet. Letztere messen die Wärmestrahlung des Körpers, können daher nur Menschen mit einer gewissen Körperstatur identifizieren. Dafür können sie allerdings auch durch Büsche sehen. Nachtbildkameras verstärken dagegen das vorhandene Licht, bei wirklicher Dunkelheit sind sie daher nutzlos. In einer Stadt mit Straßenbeleuchtung sind sie dagegen recht wirkungsvoll. Allerdings sind Hubschrauber nicht unsichtbar, so dass es sinnvoll ist ab und zu nach oben zu schauen. Wenn dieses auch im Alltag gehäuft auftritt, könnte es sein, dass sie Dich auf dem Kieker haben.

== Observation mit Kleinflugzeugen == Laut einem [[http://www.lvz-online.de/nachrichten/mitteldeutschland/streit-um-geheimbericht-zu-neonazi-trio--verbindungen-zu-saechsischer-bloodhonour-sektion/r-mitteldeutschland-a-121683.html|Artikel in der Leipziger Volkszeitung]] hat das [[BfV]] ein Kleinflugzeug zum Auffinden von untergetauchten Neonazis eingesetzt. Es ist anzunehmen, dass der VS bei Linken schon bei geringerem Anlass Kleinflugzeuge

zur Unterstützung der Observation einsetzt. Das perfide ist das es auch genug Hobbyflieger gibt und die Flugzeuge somit erstmal nicht auffallen.

== Drohnen mit Kameras ==

Nach [[http://www.heise.de/tp/r4/artikel/34/34202/1.html|Telepolis]] benutzt die Polizei von [[Datenbanken Sachsen|Sachsen]] seit 2011 offiziell Drohnen mit Kameras zur Aufklärung ([[Neusprech]] für Überwachung). Mehrere Länder testen sie seit ein paar Jahren und auch in Berlin sind sie schon gesichtet worden. Sie schließen ein Lücke zwischen Hubschraubern und [[Observation|Observierern]] auf der Erde. Ende 2011 hat die Bundesregierung laut [[http://euro-police.noblogs.org/2011/12/bald-drohnen-uber-deutschen-dachern/|euro-police]] einen Gesetzesentwurf zur Änderung des Luftverkehrsgesetzes im Deutschen Bundestag vorgestellt, welche in Zukunft Drohnen zur Observation erlaubt.

== Staatstrojaner ==

<<Anchor(Bundestrojaner)>>Trojaner sind Programme, die gegen den Willen des/r Besitzer_in auf einem Rechner laufen.
Staatstrojaner (offiziell gerne durch Begriffe wie "Onlinedurchsuchung" oder "Quellen-TKÜ" kaschiert) sind Programme, die staatliche Stellen (die "Bedarfsträger" der LawfulInterception) auf den Rechner bringen, um diesen in gewissem Umfang zu kontrollieren.

vgl [[Staatstrojaner]]

== RFID Chips ==

Ein Mini-Sender von der Größe von ein paar Millimetern, zusammen mit dem Sender hat das Platz auf einer Chipkarte. Ein [[RFID]]-Chip besitzt keine eigene Energiequelle, sondern bezieht seine Energie aus dem Sender, der mit ihm in Kontakt tritt (Genau beschrieben wird das auf der [[http://www.foebud.org/rfid|Spezialseite des Foebuds]] zum [[RFID]]-Chip). Der [[E-Perso]] ist mit einem [[RFID]]-Chip ausgerüstet.

== Öffentliche Überwachungskameras ==

Die Polizei kann [[Videoüberwachung]] im öffentlichen und halböffentlichen Raum (wie Bahnhöfe, Züge, Straßenbahnen, Busse) zum Auswerten nach Straftaten, aber auch zum Finden und Verfolgen von Verdächtigen benutzen und zum Identifizieren von Nutzern von Prepaid-Handys.

vgl [[Videoüberwachung]]

== Einschreiben und Pakete == Ohne Kontrolle können die [[Geheimdienste]] ebenfalls auf die Datenbank der Post (siehe [[http://www.gesetze-im-internet.de/bverfschg/__8a.html|§ 8a BverfSchG]]zugreifen, wo gespeichert ist wann, wo und an wen ein Einschreiben oder Paket abgeschickt wird.

== Google-Datenbank ==

Google sammelt laut einem [[http://www.spiegel.de/netzwelt/netzpolitik/0,1518,665613,00.html|Spiegel-Artikel:]] mehr Informationen über Internetnutzer als jedes andere Unternehmen. Seit Dezember 2009 werden Suchergebnisse sogar ohne Zustimmung der User "personalisiert".

vgl [[Private Datenbanken#Anfragen_bei_google]]

== Daten der Deutsche Bahn ==

Die DB bietet den Sicherheitsbehörden etliche Überwachungsmöglichkeiten, vgl [[Private Datenbanken#Deutsche Bahn]].

== Vorratsdatenspeicherung ==

Nach einer [[EU]]-Richtlinie werden alle Telekommunikationsanbieter der EU verpflichtet sämtliche Verkehrsdaten 6 Monate bis 2 Jahre zu speichern.

vgl [[Vorratsdatenspeicherung]]

== Handy-Funkzellen Datenbanken ==

Bei der Funkzellenauswertung werden "örtlich und zeitlich hinreichend genau bestimmte" Daten der Mobilfunkanbieter an die Polizei übertragen. Die Rechtsgrundlage wurde gemeinsam mit der für die Vorratsdatenspeicherung geschaffen ([[[http://bundesrecht.juris.de/stpo/__100g.html|§100g]] (2) StPO). Für alle so eingegrenzten Verbindungen werden mindestens Kommunikationspartner, Anfang und Ende der Verbindung, verwendete Endgeräte und Funkzelle übertragen.

vgl [[TK-Verkehrsdaten#Funkzellenauswertung]]

== Weiterführende Links ==

- [[http://bundesrecht.juris.de/tk_v_2005/BJNR313600005.html| Telekommunikations-Überwachungsverordnung - TKÜV]] Gesetzliche Verordnung, wie die Telekomunikationsüberwachung auszusehen hat.
- [[http://www.gliif.org/LI_standards/TIIT-v1.0.0.0.pdf|Transport of Intercepted IP Traffic]], genaue Beschreibung, wie die Schnittstelle zur Überwachung von Mobilfunk und Internet für die Sicherheitsbehörden realisiert werden muss.
- [[http://www.nadir.org/nadir/archiv/Repression/abhoerratgeber/abhoerratgeber.html|Der kleine Abhörratgeber]], ein Buch aus den 90-zigern ein wenig veraltet, aber teilweise noch brauchbar
- [[http://www.datenspuren.de/2005/vortraege/GSM%20Abhoeren%20Datenspuren.pdf|Abhörvortrag]] Vortrag von Frank Rieger über Mobilfunküberwachung (pdf)
- [[http://einstellung.so36.net/files/glitza_observation_2002.pdf|Glitza, Klaus-Henning: Observation - Praxisleitfaden für private und behördliche Ermittlungen, Boorberg Verlag 2002 (16 MB)]] Leitfaden für klassische Überwachung (mit Hinweisen zum Testen ob mensch überwacht wird)

- [[http://www.heise.de/tr/artikel/Mein-Job-beim-Big-Brother-964053.html|Heise-Artikel: Mein Job bei Big Brother]] Ein Insider verrät, wie die Abhör-Industrie und ihre Auftraggeber im arabischen Raum ticken. *[[http://ftp.ccc.de/congress/2001/mp3/vortraege/tag2/saal2/28-s2-1300-IMSI-Catcher.mp3|CCC-Vortrag zu IMS-Catchern]], älterer Vortrag über IMSI-Catcher aus dem Jahre 2001 (mpeg3)
- [[http://www.shop-alarm.de|Alarm Shop]] Zum Stöbern was es sonst noch alles für fiese Sachen zur Überwachung gibt
- [[http://www.datenschutz.de/themen/?catchid=25100&score=1|Artikel zum Schlagwort Technologien]], zusammengestellt vom virtuellen Datenschutzbüro
- [[http://www.datenschutz.de/themen/?catchid=22115&score=1|Artikel zum Thema Telekommunikation]], zusammengestellt vom virtuellen Datenschutzbüro
- [[http://www.gipfelsoli.org/rcms_repos/Antirepression/COMPUTERSICHERHEIT-HANDBUCH-1.2.pdf|Handbuch der Computersicherheit]]
- [[http://datenspuren.c3d2.de/|Kongresswebseite "Datenspuren" des CCC]] mit Beschreibungen der Vorträge und Links zu den Audiomitschnitten
- [[http://mandalka.name/privatsphaere_im_internet/|Infos über die Privatsphäre im Internet]]
- [[http://www.gulli.com/news/bundestrojaner-ein-2009-09-22|gulli.com: Interview mit einem Programmierer von Trojanern für Repressionsbehörden]]
- [[http://www.selbstdatenschutz.info|www.selbstdatenschutz.info]]
- [[http://www.jungewelt.de/2011/12-24/036.php| Junge-Welt: Jahresrückblick 2011]], Heute: Überwachungstechnik. Trojaner, IMSI-Catcher und »stille SMS« helfen, den Widerstand klein zu halten. Deutsche Technologie wird weltweit eingesetzt

[[VeranstaltungsMaterial|Weiter Skripte zur Technik finden sich unter Veranstaltungsmaterial]]

Version #1
Erstellt: 2025-10-27 22:34:03 UTC von Datenschmutz Migration Bot
Zuletzt aktualisiert: 2025-10-27 22:34:03 UTC von Datenschmutz Migration Bot