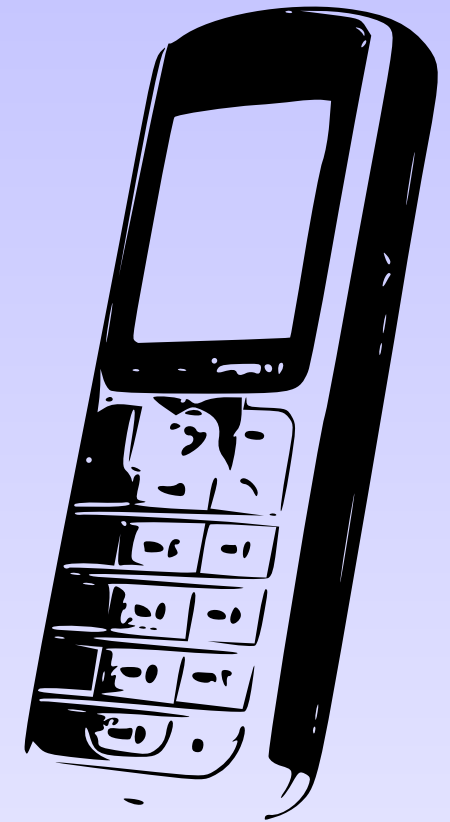


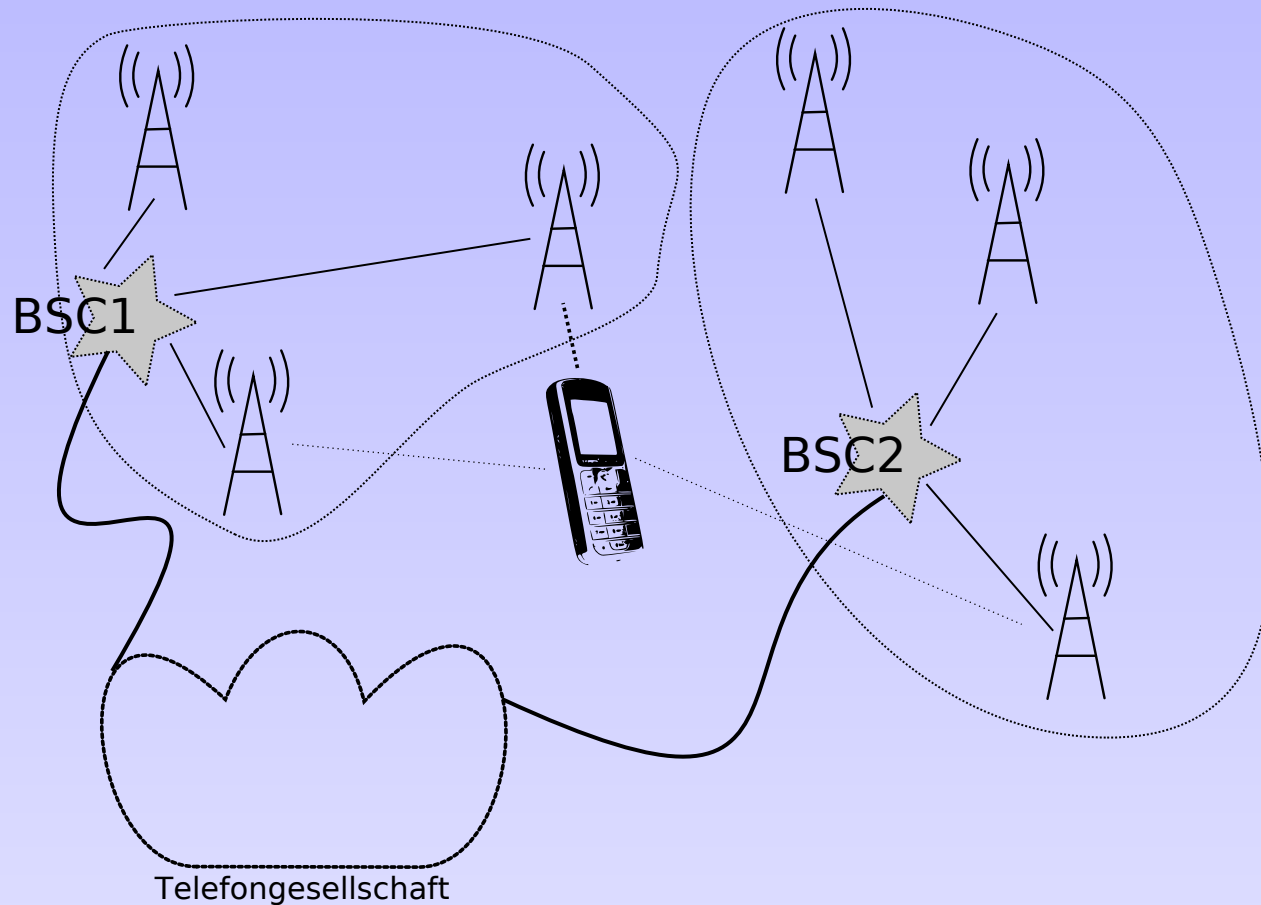
Der V-Mann in der Tasche

Seid vorsichtig, aber nicht paranoid

- GSM – ganz kurz
- Akkus raus? – Das Telefon als Wanze
- IMSI-Catcher und so
- Verkehrsdaten
- Fälle
- Was tun?



GSM – ganz kurz



SIM-Karte (IMSI)

Telefon (IMEI)

Netz

Provider

Ein Telefon kann (im Groben) aus, idle oder dedicated sein.

Vorneweg: Lauschangriff

Mobiltelefone können ihre Umgebung abhören:

1. Indem sie ohne klingeln abheben oder
2. indem sie die Umgebungsgeräusche aufzeichnen und später übertragen

Das Anschalten eines abgeschalteten Telefons durch „Fernbefehl“ ist *nicht* möglich und wird es nie sein.

Die Bundesregierung hat 2008 gesagt, das BKA habe sowas nicht eingesetzt.

Rechtsgrundlage wäre §100c StPO („großer Lauschangriff“) oder §23 PolG BaWü.

Lawful Interception

Die Daten auf dem Weg zwischen Antenne und Telefon sind verschlüsselt und normalerweise schwer zu knacken. Abhörschnittstelle ist daher das MSC; dort ist es einfach.

Allein die Polizeien in der BRD haben 2007 in 4800 Verfahren abgehört, davon vielleicht etwa 300 aus dem weiteren Politbereich. Schätzungen gehen von gegen 30000 betroffenen Anschlüssen, davon 20000 Mobiltelefonen, und in die Millionen gehenden Gesprächen aus, harte Zahlen sind nicht verfügbar.

Abhilfe: Mobiltelefone und Festnetz unterscheiden sich hier nicht – nichts Vertrauliches am Telefon.

Rechtsgrundlagen sind §100a/b StPO.

IMSI-Catcher

Der IMSI-Catcher simuliert für eine kleine Umgebung einen starken Funkmast eines Netzes. Die Telefone denken, sie hätten sich bewegt und versuchen einen Location Update. Daraufhin kann der Catcher dem Telefon IMSI und IMEI entlocken. Neuere IMSI-Catcher können auch *ein* Gespräch nach außen weitergeben und derweil abhören.

Zweck: (1) Sehen, ob ein Telefon in einem Haus ist, etwa zur Ergreifung von Flüchtlingen. (2) Bestimmung von IMEI und IMSI, die eine observierte Person mit sich führt.

Abhilfe: Telefon ausschalten.

Rechtsgrundlage: §100i StPO oder §23a (6) PolG BaWü

Verkehrsdaten

Verkehrsdaten sind in § 96 TKG definiert:

- Kennung der verbundenen Anschlüsse und ggf. weiterer beteiligter Anschlüsse
- IMEI und IMSI der beteiligten Geräte
- „Standortdaten“ (etwa Funkzellen)
- Anfang und Ende der Verbindung, Dienst, ggf. Datenmenge
- „sonstige zum Aufbau und zur Aufrechterhaltung der Telekommunikation sowie zur Entgeltabrechnung notwendige Verkehrsdaten“

Die Vorratsdatenspeicherung verlangte, diese Daten 6 Monate vorzuhalten.

Bestandsdaten

Das sind Name, Adresse, Telefonnummer, IMSI, IMEI usf., die zu einem „Anschluss“ gehören.

Verkehrsdaten kommen idR quasi pseudonymisiert, also mit Rufnummer oder IP-Adresse. Übersetzung in Namen nach §112/113 TKG.

Die Bundesnetzagentur kann in den Gesamtdaten auch mit Wildcards suchen und reicht die Fähigkeit an u.a. Polizei (zu Strafverfolgung und Gefahrenabwehr) durch.

Nach §113 TKG: u.a. Auskunft zu PUK für „Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung.“

Zugriff auf Verkehrsdaten

Die Polizei fordert Verkehrsdaten unter Angabe einer „räumlich und zeitlich hinreichend bestimmte[n] Bezeichnung“ an (§100g/h StPO, §23a PolG BaWü).

Damit kann die Polizei während der Speicherfrist und auch live:

- für 30 bis 180 Tage sehen, mit wem ihr telefoniert (habt)
- für 7 bis 92 Tage grob sehen, wo ihr seid (wart)

Voraussetzung: Verkehrsdaten müssen entstanden sein.

Nebenbei: §23a (7) PolG BaWü erlaubt der Polizei auch, eure Gespräche zu unterberechnen oder zu unterbinden.

Stille SMS

Verkehrsdaten lassen sich auch ohne Kommunikation von eurer Seite erzeugen. Zur Wartungs- und Diagnosezwecken kann der Provider einem Telefon ein SMS-Äquivalent schicken, das das Telefon kurz dedicated macht: „stille SMS“.

2009 hat die Polizei NRW 320000 davon verschickt.

Ausgeschaltete Telefone können nicht dedicated werden und sind daher immun gegen stille SMS.

Fälle

- Magedburg, Banküberfall, 2005.
- Oldenburg, Holzklotz-Fall, 2008.
- Rostock, Kupferdiebstahl, 2007.
- Stade, Raubüberfälle auf Privatwohnungen, 2005.
- Köln, Telefonkauf mit Falschgeld, 2003.
- Rottweil, Diebstahl, 2004.

Plus: Meist ignorierte Benachrichtigungspflichten bei Abhören, Observation, Verkehrsdatenabfrage, IMSI-Catchen.

Daher: Rechtsschutz ist normalerweise FDGO-Fiktion.

Zwei Verfahren in Dresden

(1) 129-Prozess des LKA: 5 FZAen rund um den 13. und 19.2., darunter eine über 48 Stunden und eine über 12 Stunden für die ganze Dresdener Südvorstadt. 923167 Verkehrs-Records und daraus 54782 Namen.

(2) Landfriedensbruch, „Soko 19/2“: 14 „Tatorte“ mit recht genauen Zeiten. 153266 Datensätze aus Verkehrsdaten, 445 aus Bestandsdaten.

Die Daten wurden auch für 45 Verfahren wg. Versammlungsgesetz verwendet. Das LKA hat dann noch seine Datensätze aus (1) an die Soko 19/2 gegeben.

Was tun?

Fazit: Das Mobiltelefon ist auch ohne weitere staatliche Intervention eine permanente Datenerfassungsmaschine.

„Wer sein Telefon einschaltet, braucht eigentlich die Batterie auch nicht rauszutun.“

Dennoch: Es ist keine schlechte Idee, Prepaid-Karten zu kaufen und dabei falsche Personalien anzugeben – vielfach geht das.

Aber: Letztlich ist das nur politisch anzugehen. Überwachungsparagraphen (z.B. §§100ff StPO) müssen weg, weitere Befugnisse der Polizei verhindert, Gesetze zur politischen Verfolgung (z.B. §§129ff StGB) abgeschafft werden.

Schafft Rote Hilfe (oder sowas ähnliches)