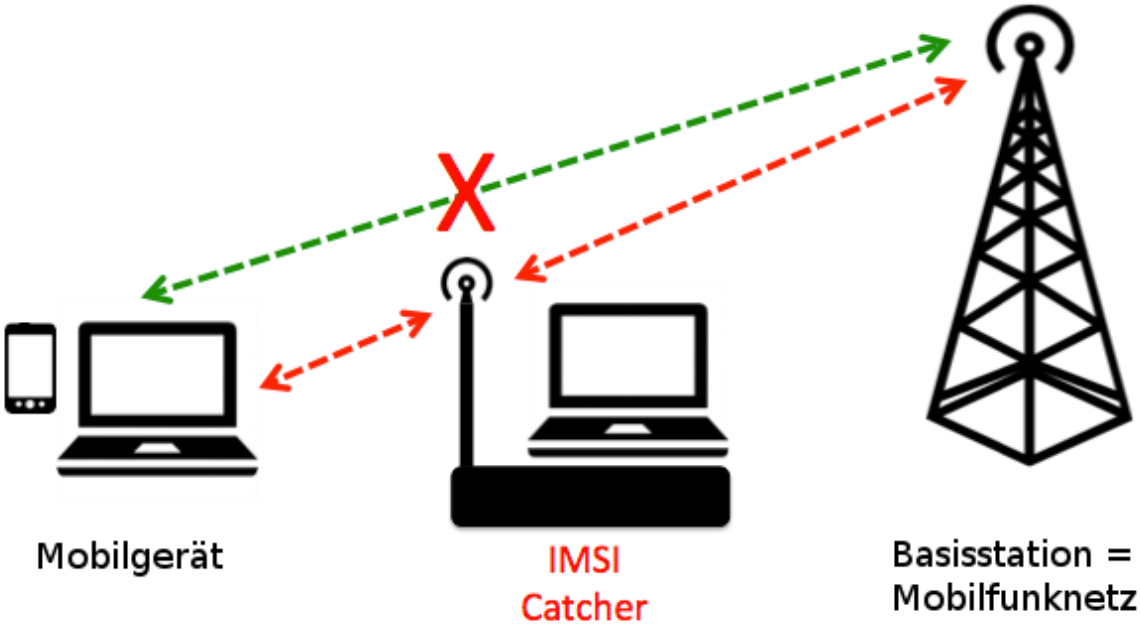
https://tarnkappe.info

Jedes Mobiltelefon (IMEI) und jede SIM-Karte (IMSI) haben eine eindeutige Nummer, die beim Benutzen des Telefonetzes mit den Mobilfunkstationen ausgetauscht werden. Diese eindeutigen Nummern wollen die Behörden mit Hilfe des IMSI Catchers ermitteln. Dabei wird eine Mobilfunkbasisstation vorgetäuscht, wie jene in die sich Mobiltelefone normalerweise einwählen. Er dient den Behörden zur Identifizierung, Lokalisierung und Überwachung von Mobilfunkgeräten und ihren Nutzer*innen. Dabei können Telefongespräche und Nachrichteninhalten mitgehört bzw. gelesen sowie die Position ermittelt und verfolgt werden.



https://causa-finita.com

Die IMEI-Nummer ist eine vom Hersteller des Mobiltelefons festgelegte eindeutige Nummer, die quasi im Gerät fest eingeschrieben ist und im Inneren meißt auf einem kleinen Aufkleber steht. Sie ist auch mit der Kombination *#06# auslesbar. Der IMSI Catcher kann diese Hardware-Nummer auch auslesen, weswegen es nichts nützt eine andere SIM-Karte (zB. eine „anonyme“) auf zB. einer Demonstration zu benutzen.

Die IMSI-Nummer der SIM-Karte setzt sich wie folgt zusammen:

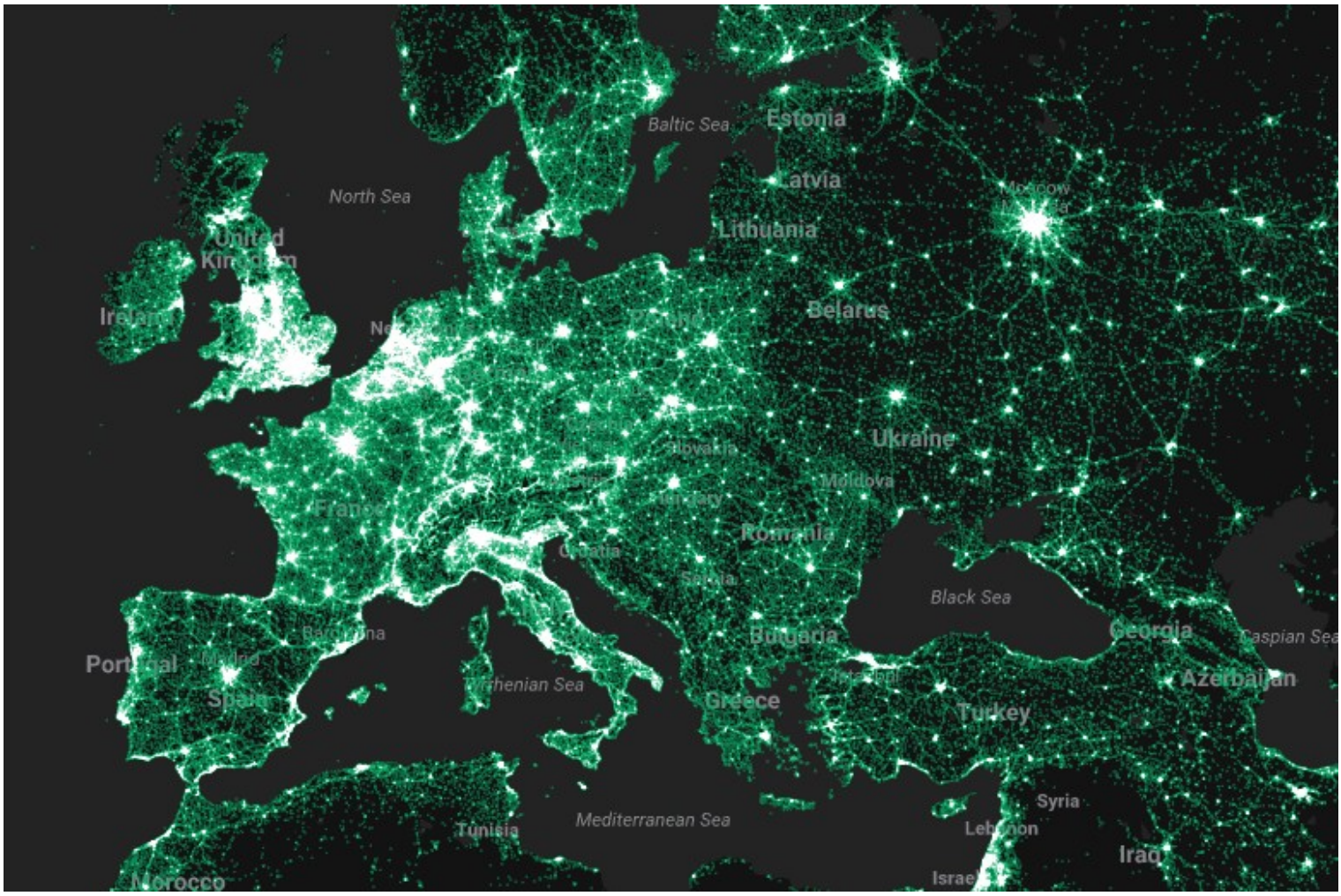
262 – 01 - 4219842350
MCC – MNC - MSIN

MCC = Ländercode (262 = Deutschland)
MNC = Netzcode des Anbieters
MSIN = Teilnehmer-Identifizierungsnummer

IMSI-Block	Nutzer
262 01	Deutsche Telekom Mobilnet GmbH (T-Mobile)
262 02	Mannesmann Mobilfunk GmbH (jetzt Vodafone)
262 03	E-Plus Mobilfunk GmbH (jetzt Telefonica)
262 04	Mannesmann Mobilfunk GmbH (jetzt Vodafone)
262 05	E-Plus Mobilfunk GmbH (jetzt Telefonica)
262 06	Deutsche Telekom Mobilnet GmbH
262 07	Telefonica Germany GmbH & Co OHG (o2)
262 08	Telefonica Germany GmbH & Co OHG (o2)
262 09	Mannesmann Mobilfunk GmbH (jetzt Vodafone)
262 10	Mannesmann Arcor (für GSM-R) (später DB Telematik, jetzt DB Netz)
262 11	Telefonica Germany GmbH & Co OHG (o2)
262 22	sipgate Wireless GmbH
262 16	vistream GmbH
262 42	Chaos Computer Club e. V. (CCC Event)
262 43	Lycamobile
262 77	E-Plus Mobilfunk GmbH (jetzt Telefonica)

https://de.wikipedia.org/wiki/International_Mobile_Subscriber_Identity#Situation_in_Deutschland

Das Mobilfunknetz (wie auch jedes andere Funknetzwerk) besteht aus mehreren Basistationen die in Abhängigkeit zu ihrer Sendeleistung und der Umgebung einen gewissen Bereich abdecken. Jede Basistation bildet also eine räumliche Funkzelle. Alle Mobilfunkzellen tauschen mit ihren Nachbarzellen Informationen über Nachbarzellen und sich selbst aus. Damit ist eine reibungslose Abdeckung des Netzes beim Bewegen durch mehrere Zellen gewährleistet.



https://opencellid.org

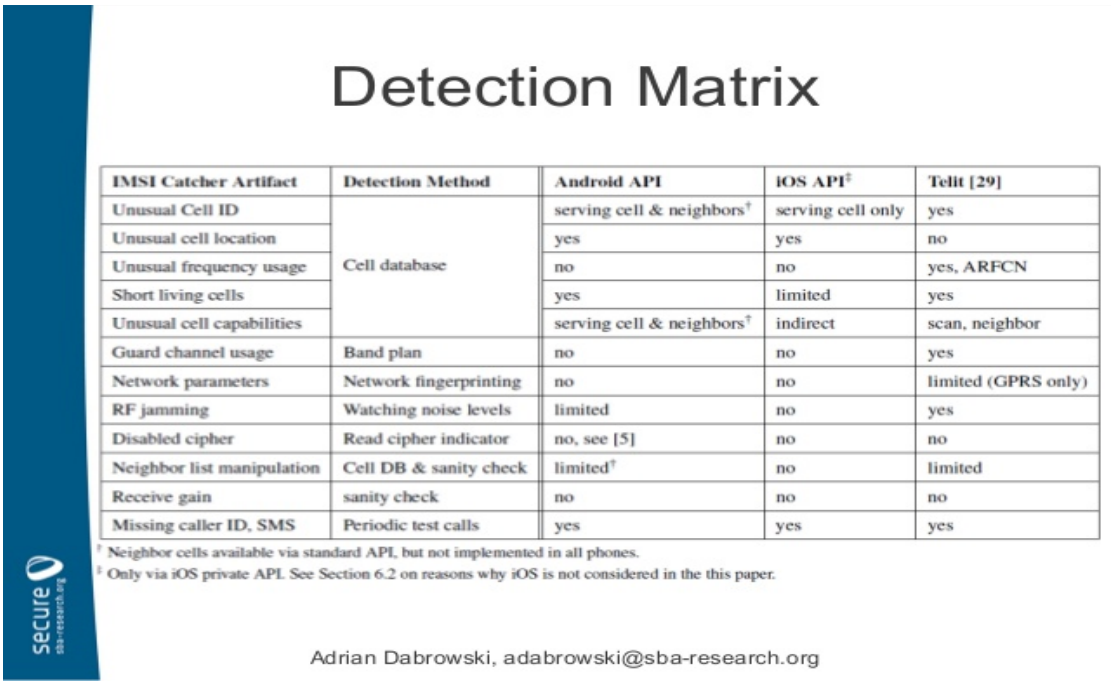
Der IMSI Catcher versucht das Mobiltelefone sich in sein künstlich geschaffenes Mobilfunknetz einwählen indem entweder die anderen Mobilfunknetze „gejammt“ werden (nur das IMSI-Catcher-Netz bleibt zum Einwählen übrig) oder rein durch eine stärkere Sendeleistung. Mobiltelefone wählen sich meißtens automatisch in die Basisstation mit der besten Sendeleistung, in dem Fall dann der IMSI Catcher.

Nb IMSI	TMSI-1	TMSI-2	IMSI	country	brand	operator	MCC	MNC	LAC	CellId
1			260 01 1101449281	Poland	Plus	Polkomtel Sp. z o.o.				
2			262 02 4740009619	Germany	Vodafone	Vodafone D2 GmbH				
3			262 02 1308296166	Germany	Vodafone	Vodafone D2 GmbH				
4	0xf62150e9	0x2c398754	262 43 0011112244	Germany	Lycamobile	Lycamobile	262	02	350	8683
5			262 02 6523731010	Germany	Vodafone	Vodafone D2 GmbH	262	02	350	8683
	0x6634a01c		262 02 1308296166	Germany	Vodafone	Vodafone D2 GmbH	262	02	350	8683
	0xfe1860e1		262 02 6523731010	Germany	Vodafone	Vodafone D2 GmbH	262	02	350	8683
6	0x69368a34	0x153f7667	262 02 1506631062	Germany	Vodafone	Vodafone D2 GmbH	262	02	350	8683
7	0xdd413b05	0x8f369a5c	262 02 9924978985	Germany	Vodafone	Vodafone D2 GmbH	262	02	350	8683
8			262 02 1409026104	Germany	Vodafone	Vodafone D2 GmbH	262	02	350	8683
9			262 02 9916189969	Germany	Vodafone	Vodafone D2 GmbH	262	02	350	8683
	0xf93a36a2		262 02 9916189969	Germany	Vodafone	Vodafone D2 GmbH	262	02	350	8683
	0xd5393441	0x63436e3c	262 43 0011112244	Germany	Lycamobile	Lycamobile	262	02	350	8683
10	0xc1192e2f	0x9137057c	262 02 1804821326	Germany	Vodafone	Vodafone D2 GmbH	262	02	350	8683
	0xcd1ba039		262 02 4740009619	Germany	Vodafone	Vodafone D2 GmbH	262	02	350	8683
	0x63436e3c	0xe342b449	262 43 0011112244	Germany	Lycamobile	Lycamobile	262	02	350	8683
	0x303ad78c		262 02 6523731010	Germany	Vodafone	Vodafone D2 GmbH	262	02	350	8683
11			262 02 1817040135	Germany	Vodafone	Vodafone D2 GmbH	262	02	350	8683
12	0xd0216661	0xf1222249	262 02 6140310100	Germany	Vodafone	Vodafone D2 GmbH	262	02	350	8683
13	0x74350b24	0x8f37c594	262 02 1819223515	Germany	Vodafone	Vodafone D2 GmbH	262	02	350	8683
14			262 02 1707512699	Germany	Vodafone	Vodafone D2 GmbH	262	02	350	8683
15			262 02 9905616558	Germany	Vodafone	Vodafone D2 GmbH	262	02	350	8683
	0x2d3883dc		262 02 1817040135	Germany	Vodafone	Vodafone D2 GmbH	262	02	350	8683
16			262 02 1707558625	Germany	Vodafone	Vodafone D2 GmbH	262	02	350	8683
17			262 02 7020246034	Germany	Vodafone	Vodafone D2 GmbH	262	02	350	8683
	0x6c34205c		262 02 1819223515	Germany	Vodafone	Vodafone D2 GmbH	262	02	350	8683
18			262 02 1707526867	Germany	Vodafone	Vodafone D2 GmbH	262	02	350	8683
	0xb33e7917		262 02 6140310100	Germany	Vodafone	Vodafone D2 GmbH	262	02	350	8683
19	0xe4429320		262 02 1605462891	Germany	Vodafone	Vodafone D2 GmbH	262	02	350	8683
	0x303b040c	0x6e35de64	262 02 6140310100	Germany	Vodafone	Vodafone D2 GmbH	262	02	350	8683
	0xc538400f		262 02 9905616558	Germany	Vodafone	Vodafone D2 GmbH	262	02	350	8683
	0xdf41c29b	0xc2204c3f	262 02 7020246034	Germany	Vodafone	Vodafone D2 GmbH	262	02	350	8683

Simple IMSI Catcher https://github.com/Oros42/IMSI-catcher

TIMSI – temporäre IMSI (soll vor Lokalisierung schützen)
IMSI – SIM-Kartennummer (MCC-MNC-ID)
MCC – Ländercode
MNC - Netzcode
LAC – Location Area Code (Kennzeichnung für ein Gebiet mehrerer Funkzellen)
CELLId – Identifikationsnummer der Funkzellen

Mit entsprechender Hardware (low-level ab ~20€, medium 200-400€, expert ab 1500€) kann sich JEDE*R einen IMSI Catcher selber bauen.



Detection Matrix

IMSI Catcher Artifact	Detection Method	Android API	iOS API‡	Telit [29]
Unusual Cell ID	Cell database	serving cell & neighbors†	serving cell only	yes
Unusual cell location		yes	yes	no
Unusual frequency usage		no	no	yes, ARFCN
Short living cells		yes	limited	yes
Unusual cell capabilities		serving cell & neighbors†	indirect	scan, neighbor
Guard channel usage	Band plan	no	no	yes
Network parameters	Network fingerprinting	no	no	limited (GPRS only)
RF jamming	Watching noise levels	limited	no	yes
Disabled cipher	Read cipher indicator	no, see [5]	no	no
Neighbor list manipulation	Cell DB & sanity check	limited†	no	limited
Receive gain	sanity check	no	no	no
Missing caller ID, SMS	Periodic test calls	yes	yes	yes

† Neighbor cells available via standard API, but not implemented in all phones.
‡ Only via iOS private API. See Section 6.2 on reasons why iOS is not considered in the this paper.

Adrian Dabrowski, adabrowski@sba-research.org

IMSI Catcher verraten sich durch folgende Punkte:

- **andere Netze sind nicht erreichbar**
- **Netzempfang wird angezeigt aber kein Signal**
- **Netzdowngrade (zB. auf GSM) des Mobiltelefons**
- **Verschlüsselungsdowngrade (mache Handys können das anzeigen)**

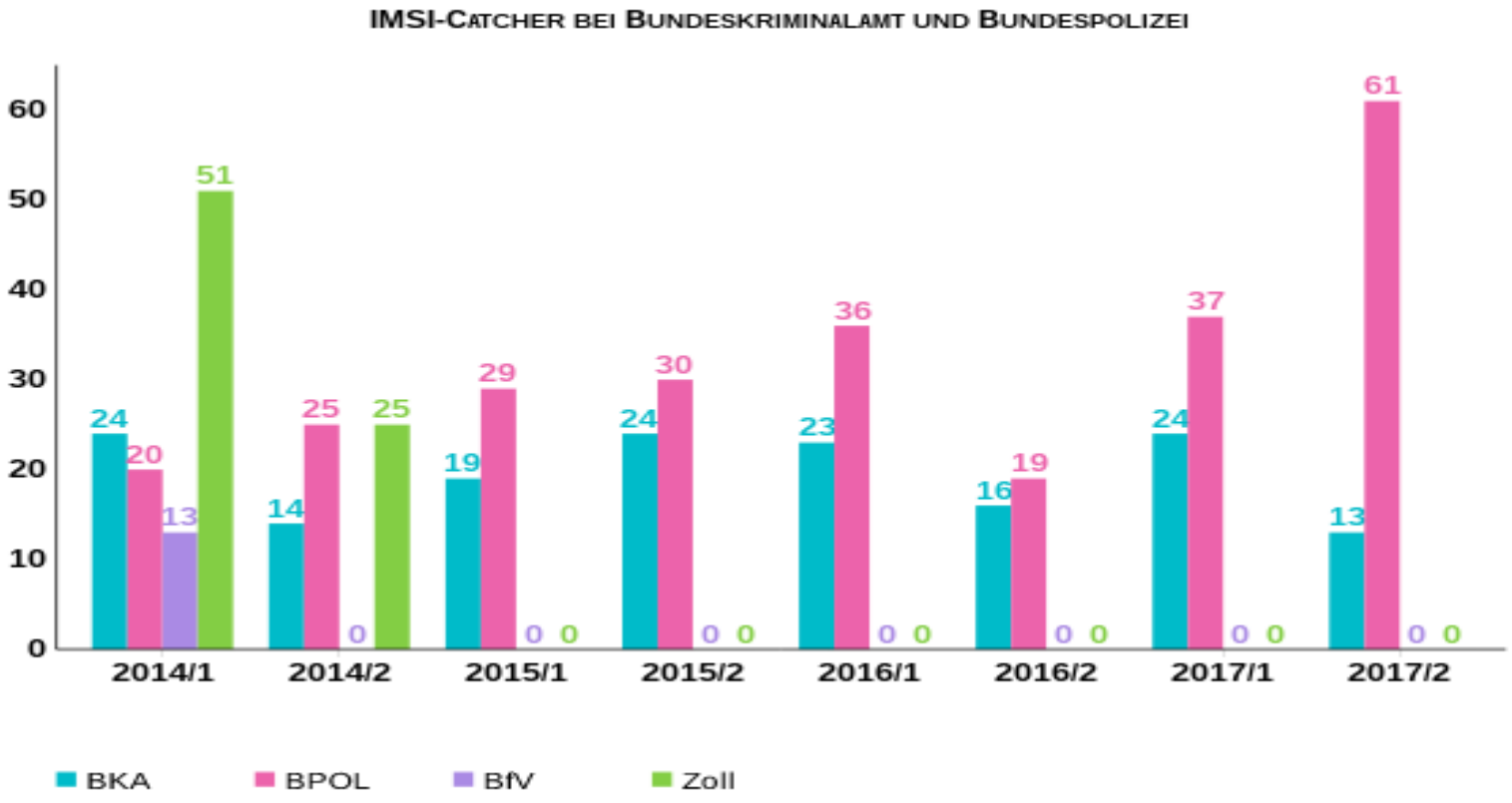
Nur mit technischen Hilfsmitteln (SDR) bemerkbar:

- **Zellen-ID**
- **Frequenz**
- **starke Sendeleistung**
- **liefern falsche oder keine Nachbarschaftsliste aus**
- **Zellen-ID steht nicht in den Nachbarschaftslisten der anderen Stationen**
- **Zellen-ID taucht doppelt in der Nachbarschaftsliste auf**
- **Verschlüsselung wird runtergebrochen oder abgestellt**

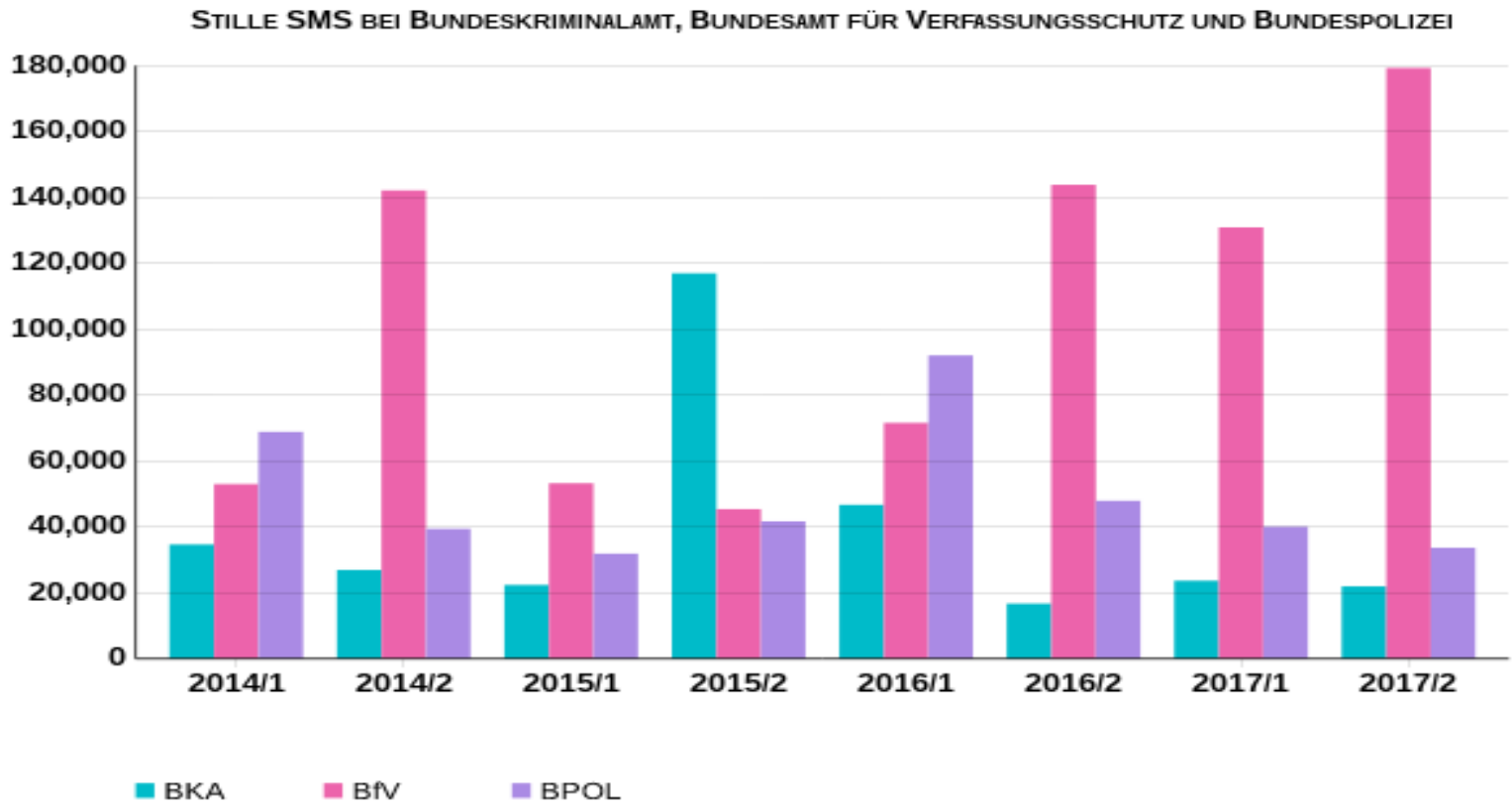
IMSI-Catcher & Stille SMS Detektoren für Android:

- **AIMSICD (F-Droid)**
- **SnoopSnitch (F-Droid/GooglePlayStore) – braucht ROOT & Qualcom Chip**
- **darshak (Github/GooglePlayStore) – braucht ROOT & Samsung Galaxy S3**

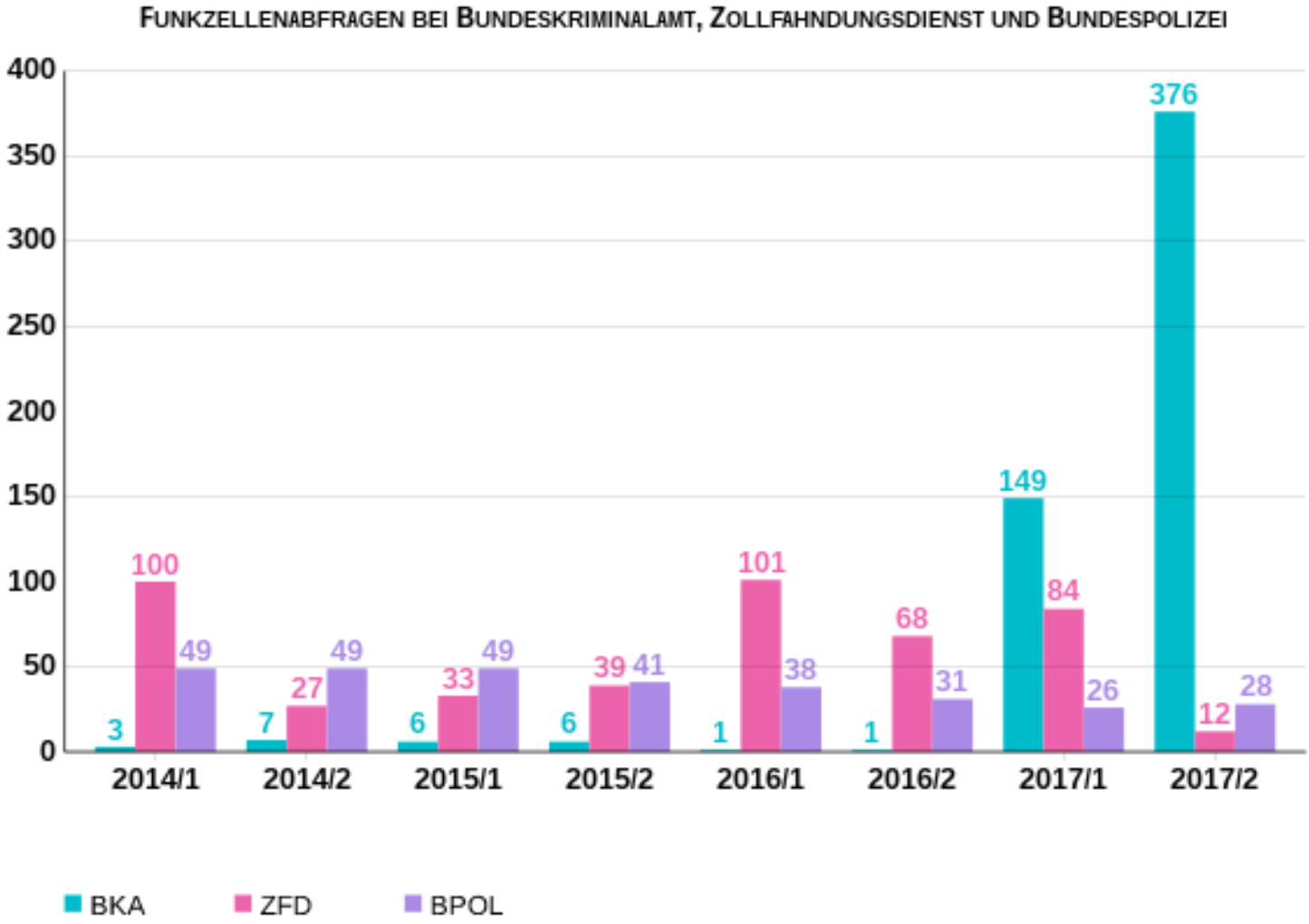
Noch ein paar aktuelle Zahlen (Stand 02/2018) von Netzpolitik.org zum Einsatz von IMSI Catchern:



Das war´s aber noch nicht leider! Denn da sind noch:



Der genaue Standort eines Mobiltelefons in einem GSM-Netz lässt sich nur bei aktiven Verbindungen (Telefonate/SMS) ermitteln. Stille SMS werden von den Behörden versendet und sollen eine aktive Verbindungen auslösen um den aktuellen Standpunkt zu übermitteln. Damit können Bewegungsprofile erstellt werden.



Funkzellenabfragen werden durch die Behörden über den Netzbetreiber betrieben und liefern sogenannte Verkehrsdaten (Ort, Zeit, ID, ...) über die Nutzer*innen. Ebenfalls auch zur Erstellung von Bewegungsprofilen einsetzbar.

Informationen zusammengetragen von: *www.futureshit.tk*