Lawful Interception

Überwachung der Telekommunikation

Herbert Paulis

Dieser Artikel gibt einen kurzen Einblick in die Funktionalität der Überwachung von Telekommunikationssystemen. Dabei wird hier bewusst nur wertneutral die technische Seite betrachtet, gesellschaftliche und politische Aspekte kommen an andere Stelle dieser Ausgabe ausführlich zur Sprache. Es macht aber durchaus Sinn, erst mal zu wissen, wie funktioniert das Ganze denn überhaupt, bevor man sich mit anderen Aspekten befasst. Damit lassen sich dann auch technische Peinlichkeiten vermeiden, wie etwa die Ansage, dass man mit IMSI-Catchern Lawinenopfer aufspüren kann…

Alle Betreiber von öffentlichen Telekommunikationsnetzen müssen für staatliche Behörden Funktionen vorhalten, die die Überwachung der angebotenen Dienste ermöglichen. Sie sind verpflichtet, bei der Überwachung mitzuwirken und entsprechende Abhöreinrichtungen in ihre Netze zu integrieren. Diese Überwachung wird international als *Lawful Interception* (LI) bezeichnet, in deutschsprachigen Ländern auch als Telekommunikationsüberwachung.

Den gesetzlichen Rahmen für diese Überwachung liefern nationale Gesetze, in Österreich zum Beispiel das Telekommunikationsgesetz 2003 in der Fassung vom 25.05.2011 im §94. Damit wird unter anderem auch die EU-Richtlinie 2006/24/EG vom 21. Dezember 2007 umgesetzt. Nationale Regulierungsbehörden legen außerdem technische Vorschriften und Durchführungsverordnungen fest, in denen die technischen und organisatorischen Details der Überwachung geregelt sind. Diese können in verschiedenen Ländern durchaus sehr unterschiedlich festgelegt sein. Internationale Standardisierungs- und Normierungsgremien wie die ETSI oder die 3GPP haben verschiedene technische Standards[1] entwickelt, die es den Herstellern und nationalen Regulierungsbehörden erleichtern, sinnvolle und durchführbare Regeln zu implementieren und vorzuschreiben.[2]

Die eigentliche Überwachung selbst gliedert sich in zwei Bereiche. Zum einen werden übertragene Sprache und Daten von Teilnehmern dupliziert, also quasi „abgehört“, und an die überwachende Behörde weitergeleitet, zum andern ist eine sehr wichtige Funktion das Erfassen und Weiterleiten der sogenannten Ruf- oder Metadaten. Dabei handelt es sich um eine Fülle von Informationen, die eine Sprach- oder Datenverbindung näher beschreiben. So wird etwa Zeit und Dauer eines Anrufes festgehalten, sowie die Rufnummern der beteiligten Gesprächspartner bzw. IP-Adressen, die an einer Datenübertragung beteiligt waren. Beim Mobilfunk kommen noch Informationen über die Standorte der Mobiltelefone dazu, mit deren Hilfe dann auch die sog. Bewegungsprofile erstellt werden können, um nachzuvollziehen, wo sich die überwachten Personen wann aufgehalten haben. Auch die Inanspruchnahme von TK-Zusatzdiensten wie etwa DTMF o.ä. wird protokolliert.

Einige Fachbegriffe aus der Telekommunikationsüberwachung:

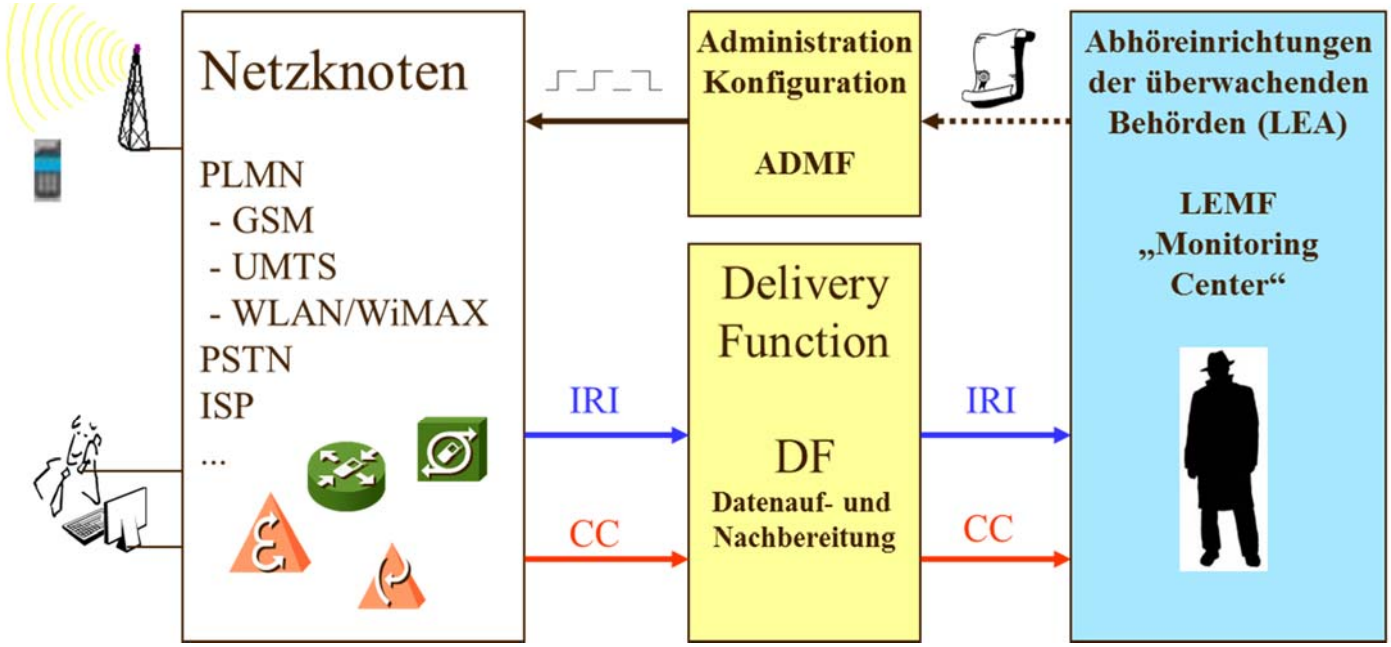
- Überwachte , die eine Überwachung veranlassen könTeilnehmer und Teilnehmerinnen werden als „Ziel“ bezeichnet (engl. *Target*).
- Staatliche Behördennen, nennt man „Bedarfsträger“ (engl. *Law Enforcement Agency*, abgk. LEA). Solche Bedarfsträger können u.a. sein (das ist in der Regel von Land zu Land unterschiedlich):
  - Polizei, Staatspolizei, Landeskriminalämter, Bundeskriminalamt
  - Geheimdienste
  - Zoll, Finanz
- Der international übliche Fachausdruck für die duplizierten Gespräche und Daten ist *Content of Communication*, abgek. *CC*, und für die gesammelten Rufdaten *Intercept Related Data*, abgek. *IRI*.

Die Überwachung muss etlichen strengen Kriterien genügen, die von Herstellern der Systeme, Netzbetreibern und Behörden penibel überwacht und überprüft werden:

- Privacy
  - Es dürfen nur bestimmte Ziele auf richterliche Anordnung hin überwacht werden.
  - Die zu überwachenden Ziele müssen eindeutig identifiziert sein.
- Geheimhaltung
  - Die überwachten Ziele dürfen nichts von der Überwachung bemerken.
  - Auch der jeweilige Netzbetreiber darf nicht bemerken, welche Kommunikation gerade überwacht wird.
  - Mehrere überwachende Bedarfsträger dürfen nichts voneinander bemerken.
- Security
  - CC und IRI müssen gesichert an die Bedarfsträger übertragen werden, zum Beispiel mit *Closed User Groups* für Sprache bzw. mittels IP Sec für Daten und IRI.
- Reliability
  - Es dürfen keine Daten auf dem Übertragungsweg verloren gehen.
  - Überwachte Ziele dürfen kein Möglichkeiten haben, sich der Überwachung zu entziehen.

Wie läuft jetzt die Überwachung technisch ab? **(siehe dazu auch Abbildung 1)** Es beginnt damit, dass ein Bedarfsträger den von einem Richter unterschriebenen Überwachungsauftrag (engl. *Warrant*) an den jeweiligen Netzbetreiber schickt. Dies geschieht zurzeit noch in Papierform, elektronische Schnittstellen sind aber bei den internationalen Standardisierungsgremien bereits in Ausarbeitung. Beim Netzbetreiber befindet sich ein System, das zur Administration und Konfiguration der Überwachung dient

Abbildung 1: Prinzip der Überwachung



(ADMF) und zu dem normalerweise nur spezielles sicherheitsüberprüftes Personal Zugang hat. Dieses gibt nun die entsprechenden Daten in das System ein, welches die Daten dann entsprechend aufbereitet an die jeweils zuständigen Netzknoten übermittelt. Das können Fest- und Mobilfunkvermittlungsstellen sein, Router, oder andere, je nach verwendeter Technologie.

Dabei werden sämtliche Tätigkeiten in gesicherten Logfiles aufgezeichnet, um später jederzeit nachverfolgen zu können, wer beim Netzbetreiber wann welche Eingaben und Abfragen im System getätigt hat. Damit soll auch einem eventuellen Missbrauch vorgebeugt werden.

Im Netzknoten werden nun alle anfallenden Kommunikationsdaten einer überwachten Verbindung dupliziert. Da heute alle solche Netzknoten digital arbeiten, ist der Vorgang des Duplizierens technisch völlig unproblematisch und beschränkt sich in der Regel auf das Duplizieren der zu übertragenden Datenbits. Diese werden über die entsprechend vorkonfigurierte Verbindung ausgeleitet, ebenso die in der vermittlungstechnischen Software gesammelten Rufdaten. Bevor aber CC und IRI an den oder die Bedarfsträger geschickt werden (ein Ziel kann auch gleichzeitig von mehreren Bedarfsträgern überwacht werden), werden sie allerdings noch an ein ebenfalls beim Netzbetreiber befindliches System geleitet, die sog. Delivery oder Mediation Function (DF). Hier werden herstellerspezifische Protokolle, Formatierungen und/oder Codecs in genormte Formate umgewandelt beziehungsweise auch länderspezifische Anpassungen vorgenommen.

Mit wenigen Sekunden Verzögerung, bedingt durch die beschriebene Nachbearbeitung, landen dann alle Informationen bei den Bedarfsträgern, in speziellen Auswerte- und Überwachungssystemen. Diese werden auch als Monitoring Center bezeichnet, engl. *Law Enforcement Monitoring Facility*, abgk. LEMF. Hier werden alle eingehenden Daten sicher abgespeichert, zusammengeführt und anschließend Analysten oder Auswertern zugewiesen. Die Analyse erfolgt heute auch intensiv softwareunterstützt. So werden etwa automatisch Benutzerprofile nach verschiedensten Kriterien erstellt, etwa Bewegungsprofile **(siehe Abbildung 2)**, Korrelationen mit Daten aus anderen Quellen ermittelt **(siehe Abbildung 3)** und Sprachanalysen durchgeführt.

Einige Besonderheiten gilt es noch im Bereich des Mobilfunks zu erwähnen. Sind von zu überwachenden Mobiltelefonen Daten wie die Rufnummer (MSISDN), die internationale Kennung (IMSI) oder die eindeutige Gerätenummer (IMEI) bekannt, so kann die Überwachung ohne weitere Probleme in der Mobilfunkvermittlungsstelle vorgenommen werden, egal, ob es sich dabei um GSM, UMTS, oder andere Mobilfunksysteme handelt.

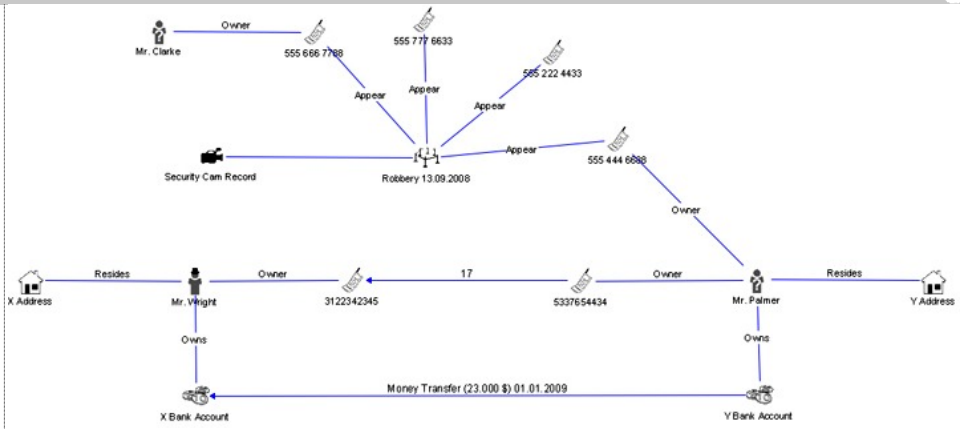


Abbildung 3: Beispiel einer Korrelationsanalyse (Quelle: [1])

Wird jedoch eine anonyme Wertkarte verwendet und alle oben beschriebenen Identitäten sind (vorerst) noch unbekannt (z.B. wegen neuem Mobiltelefon), so kommt ein spezielles Gerät zum Einsatz, der sog. IMSI-Catcher. Dieses Gerät nützt die Eigenschaft von GSM aus, dass sich zwar das Mobiltelefon gegenüber dem Netz authentifizieren muss, nicht aber das Netz gegenüber dem Mobiltelefon. Der IMSI-Catcher gaukelt nun dem zu überwachenden Mobiltelefon vor, eine Zelle im Netz zu sein, die die beste Empfangsqualität bietet, dem eigentlichen Mobilfunknetz präsentiert er sich als Mobiltelefon. Damit kann nun das im IMSI-Catcher unverschlüsselt vorliegende Gespräch überwacht werden, außerdem lassen sich so alle wichtigen Kenndaten (MSISDN, IMSI, IMEI) für eine reguläre Überwachung ermitteln.

Bei UMTS ist die Vorgangsweise etwas komplizierter, da sich hier erstmals auch das Netz gegenüber der Mobilstation identifizieren muss *(mutual entity authentication)*. Hier wird ein *Man-in-the-Middle*-Angriff durchgeführt, mit dessen Hilfe das Mobiltelefon anschließend in den GSM-Modus gezwungen wird, wonach genauso wie oben verfahren werden kann.

Der Betrieb eines IMSI-Catchers ist allerdings auch mit etlichen Problemen und Nachteilen verbunden, die hier kurz erwähnt werden sollen. So muss etwa der Netzanbieter des Ziels schon im Vorfeld ermittelt werden. Je nach Signalstärke des IMSI-Catchers befinden sich mehrere Mobiltelefone im Einzugsgebiet, die vom IMSI-Catcher zwar abgewiesen werden, aber dann trotzdem nicht auf das eigentliche Netz zugreifen können. Er verursacht daher eine lokale Störung im Mobilfunknetz, die (zumindest theoretisch) vom Netzbetreiber im Nachhinein festgestellt werden kann. Auch können nur ausgehende Anrufe mitgehört werden, außerdem scheint das abgehörte Gespräch nicht auf der Telefonrechnung des Teilnehmers auf. Die Überwachungsmaßnahme kann also von aufmerksamen Anwendern zumindest begründet vermutet werden. Abgesehen davon erklärt die Beschränkung auf ausgehende Anrufe auch, warum ein IMSI-Catcher nicht geeignet ist, um Lawinenopfer zu lokalisieren – die gesuchte Person ist in der Regel nicht mehr in der Lage, selbst einen Notruf abzusetzen!

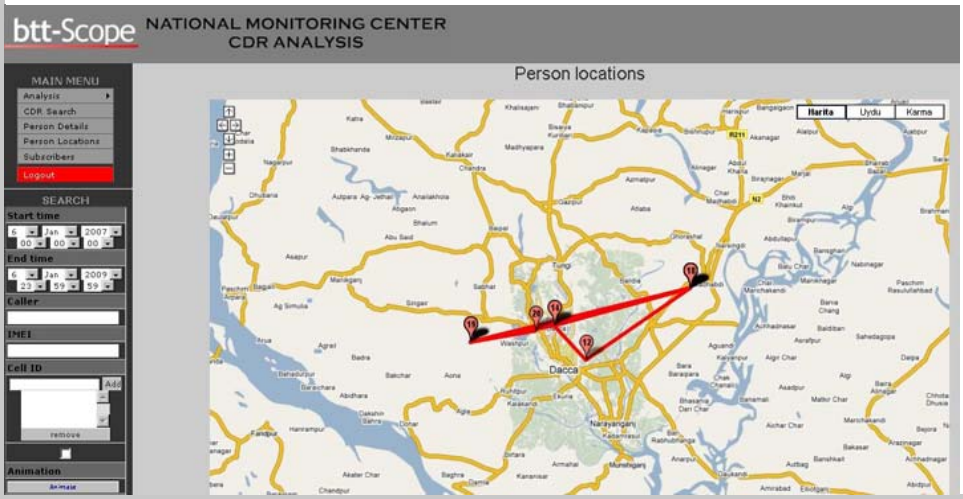
Auf eine detailliertere technische Beschreibung muss hier aus Platzgründen verzichtet werden, eine grundlegende Einführung in das Thema, wenngleich etwas veraltet, findet sich unter.[2] Eine exzellente Seminararbeit über die genaue Funktionsweise von IMSI-Catchern bei UMTS ist.[3] Die Beschreibung der Funktionsweise des IMSI-Catchers ist auch gut nachzulesen in Wikipedia.

Erwähnt werden soll hier auch noch die Vorratsdatenspeicherung (VDS), die aber mit Lawful Interception sowohl technisch als auch konzeptuell nur indirekt verwandt ist. So erfolgt LI nur bei begründetem Verdacht auf richterliche Anordnung, während die VDS präventiv durchgeführt wird. Da bei der VDS Rufdaten aller Teilnehmer und Teilnehmerinnen erfasst werden, kann das Sammeln dieser Daten nicht analog zu LI von der vermittlungstechnischen Software durchgeführt werden, da dies viel zu viel Aufwand bedeuten würde. Die sinnvolle LI-Überwachungskapazität einer Vermittlungsstelle liegt im niedrigen einstelligen Prozentbereich aller aktiven Verbindungen. Bei VDS werden bis auf wenige Ausnahmen (zum Beispiel E-Mail-Header) hauptsächlich Daten abgegriffen, die der Betreiber zu Abrechnungs- oder Dokumentationszwecken sowieso erstellen muss, und dann entsprechend ergänzt und abgespeichert. Außerdem findet bei VDS die Aufbewahrung der gesammelten Daten direkt beim Netzbetreiber statt und die Behörde greift auf diese nur bei Bedarf zu.

Dementsprechend groß ist auch das Speichervolumen, das die Netzbetreiber hier vorhalten müssen. Ein größerer Telekommunikationsanbieter etwa, der auch ein Mobilfunknetz betreibt und zugleich ISP ist, muss hier durchaus mit benötigten Kapazitäten rechnen, die ein Petabyte (1 PB = 1.000 TB = 1.000.000 GB = 10^{15} Byte) deutlich überschreiten können.

Wenn man über Überwachung der Telekommunikation spricht, so muss man auch fragen, wie es um dem Unterschied zwischen dem gesetzlich legitimiertem Abhören *(Lawful Interception)* und dem in letzte Zeit durch alle Medien geisternden großflächigem Abhören von Telekommunikation durch Geheimdienste (engl. *Signal Intelligence*) bestellt ist. Nun, formal existieren

Abbildung 2: Beispiel eines Bewegungsprofils (Quelle: [1])



diese Unterschiede natürlich, in der Praxis sind die Übergänge jedoch fließend. Auch geht dieser Artikel von einer theoretisch korrekten Vorgehensweise bei Telekommunikationsüberwachung aus, also nur auf richterliche Anordnung unter Beachtung aller einschlägigen Gesetze und Verordnungen, berücksichtigt also keinerlei Arten von potentiell natürlich möglichem Missbrauch *(„Aber wer überwacht die Wächter?“)*.[3]

Dennoch, bei oder besser vor allem wegen dem aktuellen Medienrummel zum Thema Überwachung durch diverse Geheimdienste sollte man doch die Kirche im Dorf lassen. Aussagen, dass diverse Verschlüsselungen laufend geknackt werden, sind stark übertrieben, siehe dazu auch.[4] Auch im Sinne einer effizienten Bedrohungs-und Risikoanalyse finde ich es wichtiger, meine Rechner vor allzu neugierigen Webservern, Cookie-Sammlern und nervigen Werbungen zu *schützen* als vor der NSA oder dem GCHQ.

Nicht unerwähnt soll auch bleiben, dass Verschlüsselung, zu der in diesem Zusammenhang immer wieder geraten wird, zwar ein passabler Schutz gegen das Abhören von Inhalten ist (so sie korrekt erfolgt), aber in keiner Weise gegen das Erfassen und Auswerten von Rufdaten schützt. Diese werden vielfach von Ermittlern sogar als wertvoller und wichtiger angesehen als die eigentlichen Gesprächsinhalte. Ein guter Artikel dazu findet sich unter [5], eine detaillierte technische Analyse mit Vorgangsweisen unter.[6]

Zusammenfassend kann man also sagen, dass die Überwachung der Telekommunikation eine zwar unangenehme Maßnahme ist und einen schweren Eingriff in das Persönlichkeitsrecht darstellt, aber in gerechtfertigten Fällen zur Verbrechensaufklärung absolut erforderlich ist. Das Motto dabei sollte aber immer sein, *„so viel LI wie nötig, aber so wenig als möglich“*.

Quellenangabe und weiterführende Links

[1] BTT Ltd., ein türkischer Hersteller von Überwachungsprodukten, www.btt.com.tr, die gezeigten Beispiele betreffen das Monitoring Center-Produkt BTT-Scope http://bttscope.com/bttscope.php#05

[2] *Der IMSI-Catcher*, Dirk Fox, DuD Datenschutz und Datensicherheit 26 (2002) 4, auffindbar z.B. bei http://www.secorvo.de/publikationen/imsicatcher-fox-2002.pdf

[3] *IMSI Catcher*, Daehyun Strobel, Ruhr-Universität Bochum 2007, auffindbar z.B. bei http://imperia.rz.rub.de:9085/imperia/md/content/seminare/itsss07/imsi_catcher.pdf

[4] *NSA hat Kryptografie nicht geknackt*, Erich Möchel, futurezone.at, http://futurezone.at/netzpolitik/nsa-hat-kryptografie-nicht-geknackt/26.870.159

[5] *Geheimdienste und Konkurrenten hören Telefongespräche mit*, Security Insider 2008 http://www.security-insider.de/themenbereiche/applikationssicherheit/kommunikations-sicherheit/articles/123429/

[6] *Mobile Security*, Bundesamt für Sicherheit in der Informationstechnik, https://www.bsi.bund.de/DE/Themen/weitereThemen/MobileSecurity/mobilsecurity.html

1 Im Gegensatz zu den LI-Standards der ETSI sind LI-Standards des Mobilfunks öffentlich auf der Website der 3GPP (www.3gpp.org -> „*Specifications*“) verfügbar. Sie tragen die Nummern 33.106, 33.107 und 33.108.

2 Eine solche nationale Verordnung als Beispiel in Deutschland trägt den etwas sperrigen Namen „Technische Richtlinie zur Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation und zum Auskunftersuchen für Verkehrsdaten (TR TKÜV)“

3 lat.: *“Sed quis custodiet ipsos custodes?”*, Juvenal (58 – 140), Satiren VI, 347f.
Ein Zitat, das heute gerne und oft im Zusammenhang mit Überwachung verwendet ist und auch ganz gut dort hineinpasst. Dennoch ist es stark aus dem Zusammenhang gerissen, denn Juvenal befasst sich im Band VI seiner Satiren mit den Frauen und der Ehe und an besagter Textstelle geht es darum, wie man sich der Treue seiner Frau sichern kann: Ein Freund schlägt vor, sie im Haus einzusperren und zu bewachen und der Dichter antwortet dann mit obigem Zitat.