
Lawful Interception
FH CAMPUS WIEN
1. Version September 2006
Update August 2013
Dipl.-Ing. Herbert Paulis
Herbert.paulis@fh-campuswien.ac.at

Links zum Thema:

http://en.wikipedia.org/wiki/Lawful_interception
(Link in englische Version. Die deutsche Fassung ist sehr schwach.)

https://berlin.ccc.de/index.php?title=Telekommunikations%C3%BCberwachung&redirect=no

Gelegentlich wird die Abkürzung „LI" auch als „Legal Interception" gedeutet, in allen relevanten Unterlagen (z.B. Standardisierung) wird nur der Begriff „Lawful Interception" verwendet. Im Deutschen ist auch der Begriff „Telekommunikationsüberwachung" (TÜ oder TKÜ) gebräuchlich. In den USA wird die Bezeichnung „Communications Assistance for Law Enforcement Act" verwendet, abgekürzt CALEA.

Eine gute Auflistung mit Links der wichtigsten Dokumente und Standards findet man unter http://www.brookson.com/wap/li.htm.

Auszug aus einem LI-Standard (3GPP TS 33.106 V6.2.0):

“5.2.1.3 Security of processes

The intercept function shall only be accessible by authorized personnel.

To be effective, interception must take place without the knowledge of either party to the communication. Therefore, decryption must also take place without either party being aware that it is happening.

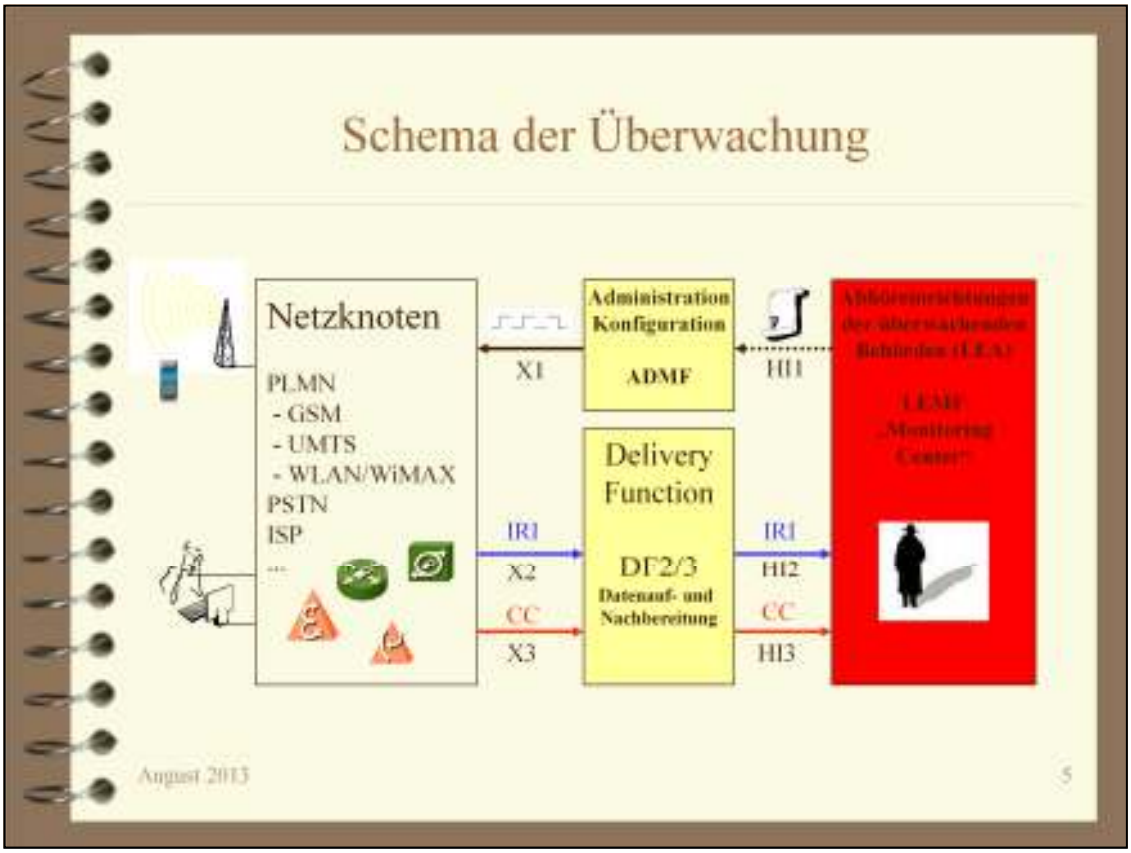
No indication shall be given to any person except authorized personnel that the intercept function has been activated on a target. Authentication, encryption, audits, log files and other mechanisms may be used to maintain security in the system. Audit procedures should be capable of keeping accurate logs of administration commands.”

Quelle: www.3gpp.org

Wie kann man zu überwachende Teilnehmer identifizieren? In der Regel an Hand von eindeutig zuordenbaren Kriterien, etwa (Mobil)Rufnummer, IP-Adresse, E-Mailadresse, usw. Manchmal wird aber auch nach anderen Kriterien abgehört, etwa alle Personen, die sich innerhalb eines gewissen Aufenthaltsbereiches befinden (Location Based Interception) oder alle Rufnummern, die mit einer bestimmten Vorwahl beginnen.

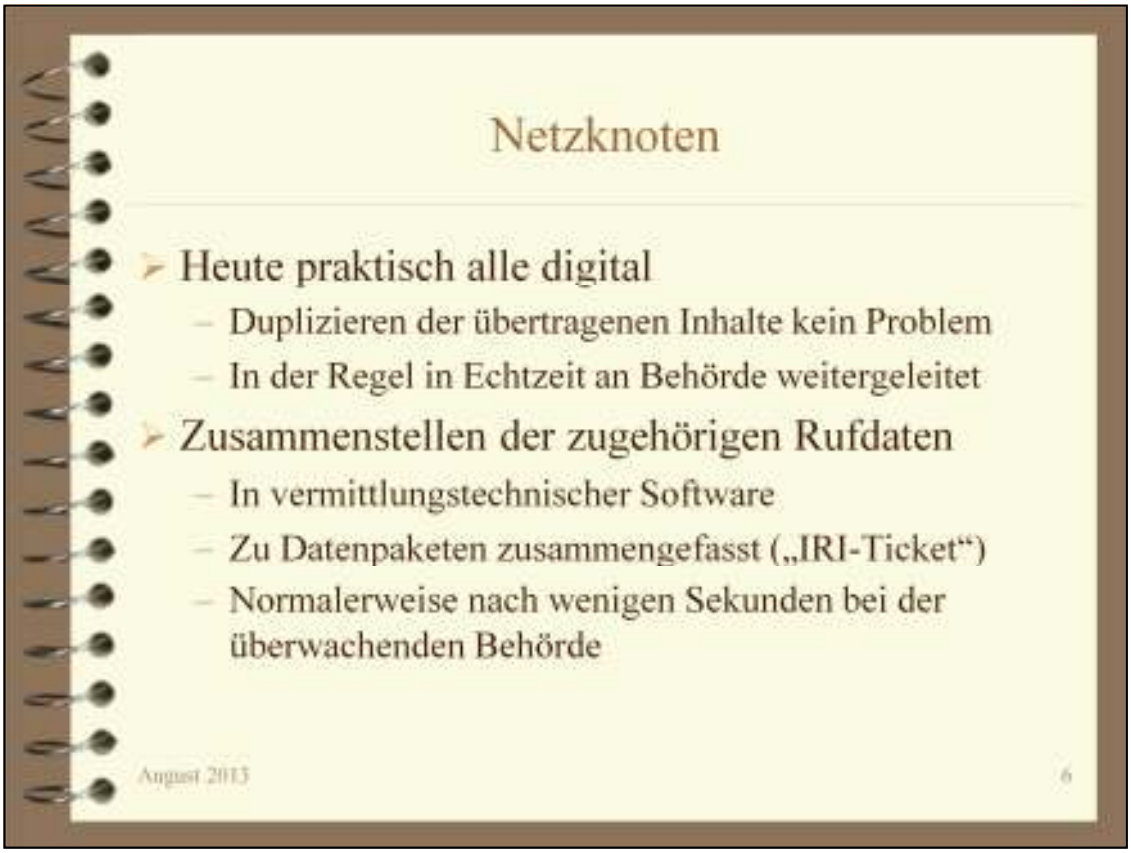
Im Zuge der richterlichen Anordnung werden auch Zeitpunkte für den Beginn und das Ende einer Überwachungsmaßnahme gesetzt, diese müssen strikt eingehalten werden.

In manchen Ländern ist auch gesetzlich vorgeschrieben, dass nach dem Ende von Überwachungsmaßnahmen die überwachten Teilnehmer von diesen Maßnahmen in Kenntnis gesetzt werden müssen, jedoch wird diese Bestimmung von den Behörden oftmals ignoriert.



Abkürzungen und Begriffe:

PLMN	Public Land Mobile Network Öffentliches Landmobilfunknetz z.B:: GSM, UMTS, WLAN, ...
PSTN	Public Switching Telephone Network Öffentliches Festnetz
ISP	Internet Service Provider
LEA	Law Enforcement Agency Polizeibehörde, usw. („Bedarfsträger“)
LEMF	Law Enforcement Monitoring Facility Abhöreinrichtung der Behörde
IRI	Intercept Related Information, „Call Data“ Rufdaten
CC	Content of Communication Abgehörte Gespräche bzw. Daten
Xn	Schnittstellen zwischen Knoten und Mediation (DF/ADMF)
HIn	Handover Interface Schnittstellen zwischen Mediation und Behörde



Auszug aus einem LI-Standard (3GPP TS 33.108 V7.2.0):

“5.2.1 Definition of Intercept Related Information

Intercept Related Information will in principle be available in the following phases of a call (successful or not):

1) At call initiation when the target identity becomes active, at which time call destination information may or may not be available (set up phase of a call, target may be the originating or terminating party, or be involved indirectly by a supplementary service).
2) At the end of a call, when the target identity becomes inactive (release phase of call).
3) At certain times between the above phases, when relevant information becomes available (active phase of call).

In addition, information on non-call related actions of a target constitutes IRI and is sent via HI2, e.g. information on subscriber controlled input.

The Intercept Related Information (IRI) may be subdivided into the following categories:

1) Control information for HI2 (e.g. correlation information).
2) Basic call information, for standard calls between two parties.
3) Information related to supplementary services, which have been invoked during a call.
4) Information on non-call related target actions.”

Quelle: www.3gpp.org

Informationen zu LI Administration und Verwaltung bei einem ADMF- und Mediation Device-Hersteller unter:

http://www.utimaco.de/

Ein anderer Hersteller von ADMF- und Mediation Devices:
http://www.verint.com/communications_interception/index.cfm

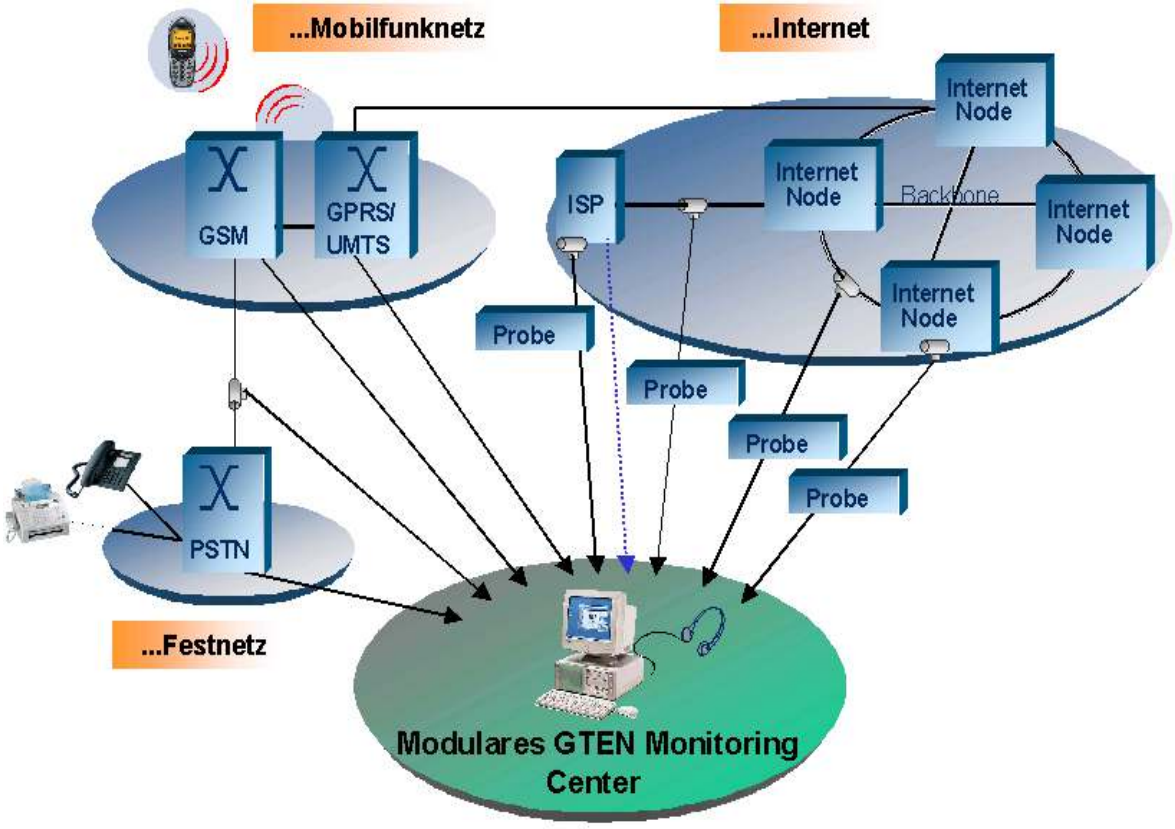
Beide vorgestellten Anbieter haben sowohl ADMF als auch Mediation Devices (DF2, DF3) in ihren Lieferprogrammen, die sie auch selbst entwickeln und produzieren.

Monitoring Center

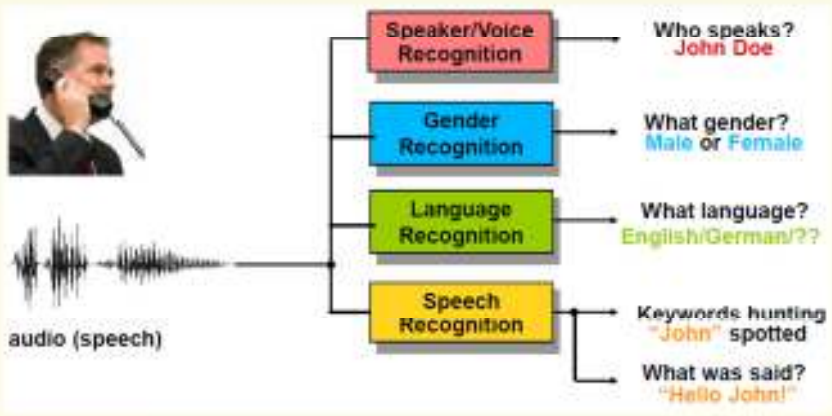
- Überwachungs- und Auswertungssystem der Behörde
- Sicheres Abspeichern aller eingehenden Daten
- Korrelation zwischen CC und zugehörigen IRI
- Zuweisen der Überwachungsfälle an Auswerter/Analysten
- Softwareunterstützte Datenauswertung
  - Benutzerprofile
    - Örtlich bzw. nach Kontakten
  - Korrelation mit anderen Daten und Informationen
    - Aus anderen Systemen bzw. Bereichen (z.B. Bankdaten)
  - Sprachanalysen, usw.

August 2013 9

Zum Themenkreis Monitoring Center bei Quintessenz.at:
http://www.quintessenz.at/cgi-bin/index%3ffunktion=view%26id=000100002077



Monitoring Center



Sprachanalyse - Aus einem MC-Werbeprospekt

Monitoring Center

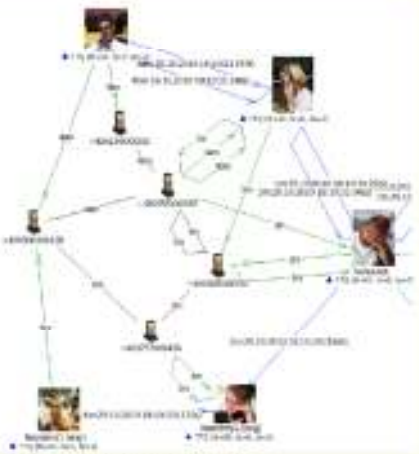
Detects person even if he/she use several phones.

⇒ Link analysis tools

Usage:

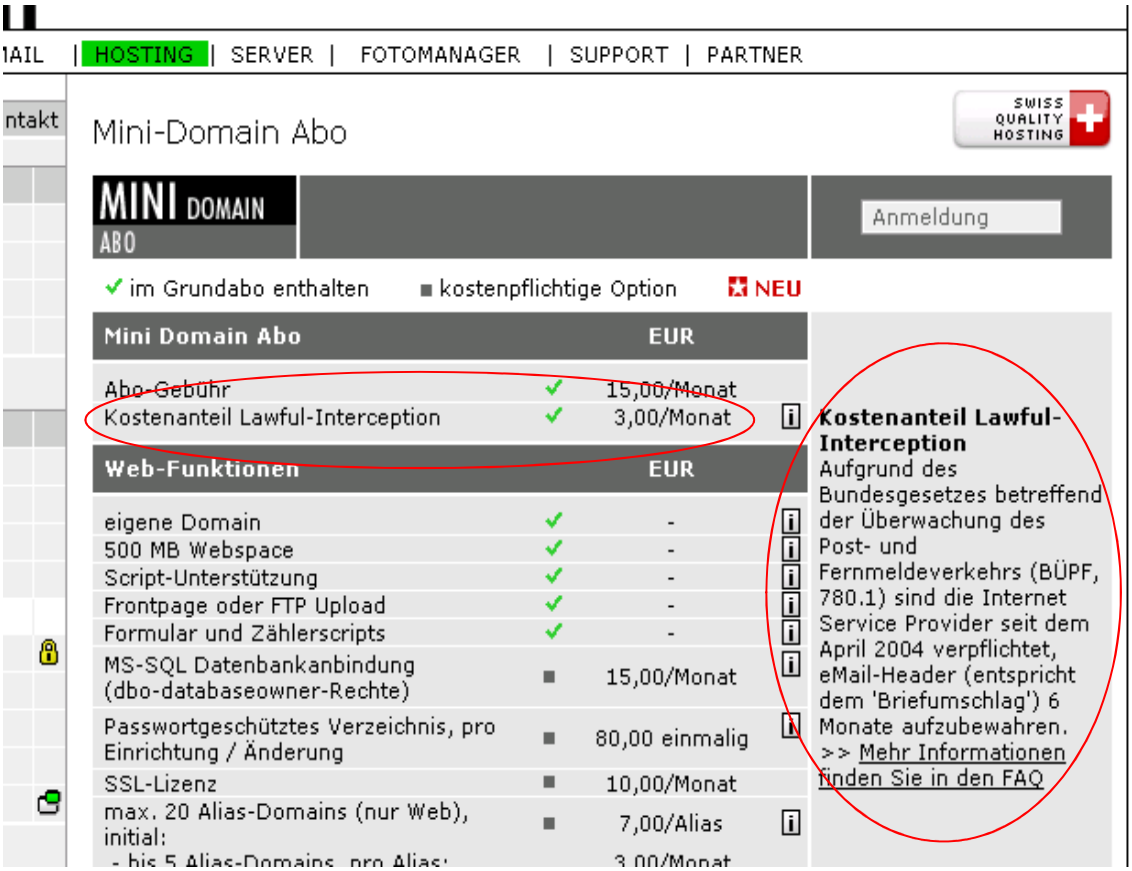
- Search for patterns
- Time analysis
- Frequency of calls proceeded by specific people

(i2 Analyst's Notebook, Tovek)



Linkanalyse - Aus einem MC-Werbeprospekt

Bei Einigen verschwimmen die Unterschiede allerdings:
(http://www.green.ch/, die Seite ist aber längst nicht mehr online)



Eine sehr gute detaillierte Beschreibung der Funktionsweise des IMSI-Catchers ist nachzulesen unter http://de.wikipedia.org/wiki/IMSI-Catcher.

Eine andere Erläuterung aus der Sicht von T-Mobile, die auch auf rechtliche und funktechnische Probleme des IMSI-Catchers eingeht, finden man unter http://www.datenschutz-berlin.de/jahresbe/01/anl/11d9.htm.

IMSI-Catcher können auch zum direkten Abhören von Gesprächen verwendet werden, allerdings mit großen Einschränkungen (nur abgehende Gespräche, all anderen Mobiltelefone in der Umgebung sind gestört). Außerdem scheint das abgehörte Gespräch nicht auf der Telefonrechnung des Teilnehmers auf, die Maßnahme kann also von aufmerksamen Anwendern zumindest begründet vermutet werden.

Daher werden in der Regel IMSI-Catcher nur verwendet, um die IMSI eines zu überwachenden Teilnehmers zu ermitteln. Anschließend wird auf der Basis dieser IMSI eine normale Überwachung im Mobilfunknetz über die Netzknoten aktiviert. Bei UMTS ist die Verwendung von IMSI-Catchern nicht mehr so einfach möglich (gegenseitige Authentifizierung von Mobilstation und Netz).

Einer der ersten IMSI-Catcher

IMSI-Catcher des deutschen Verfassungsschutzes (DuD 4/2002)

Eine gute Dokumentation über die Arbeit von IMSI-Catchern lässt sich im Internet leicht mit jeder Suchmaschine finden:

Die Seminararbeit „IMSI Catcher“ von Daehyun Strobel an der Ruhr-Universität Bochum.

Probleme und Bedenken

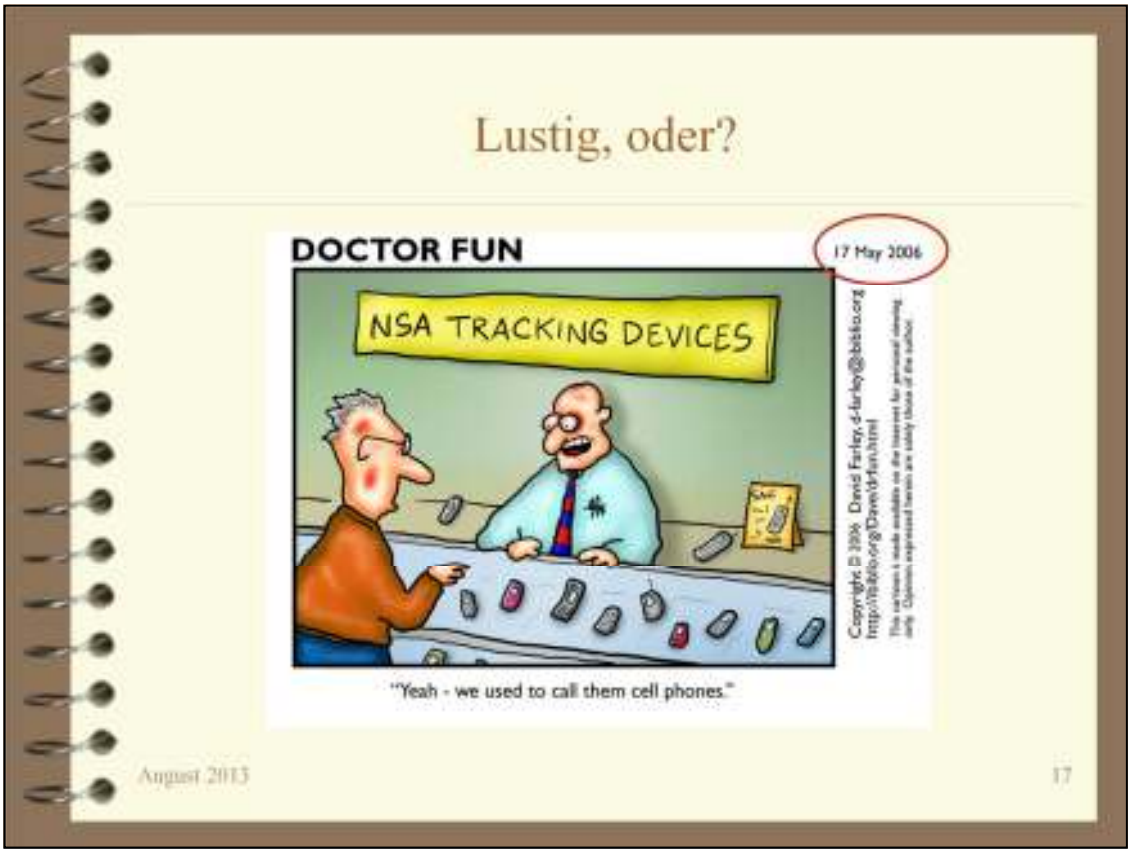
- Unterschied zwischen gesetzlich legitimiertem Abhören (*lawful interception*) und großflächigem Abhören von Telekommunikation durch Geheimdienste (*signal intelligence*)?
  - Existiert formal
  - In der Praxis oft fließende Übergänge

- Wachsender Verlust der Privatsphäre der Anwender
- Von totalitären Staaten oft zur Unterdrückung von Opposition und Andersdenkenden benutzt
- „Sed quis custodiet ipsos custodes?“

August 2013 16

lat.: Aber wer überwacht die Wächter?
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.



Man beachte das Datum des Cartoons! 2006 konnte man darüber noch lachen…

Betrifft mich das überhaupt?

- Viele Menschen reagieren in „Vogel-Strauß-Manier“
  - „Ich habe ja sowieso nichts zu verbergen!“
  - „Man kann ja eh nix machen dagegen…“
  - Kein echtes Problembewusstsein, solange man nicht selbst betroffen ist
    - Falsches bzw. irrtümliches Abhören kommt aber immer wieder vor

- Starke Kryptographie, wann immer möglich
  - Hilft aber nicht gegen Erfassung von Metadaten (IRI)!
- Aktives Problembewusstsein
  - „LI so viel wie nötig, aber so wenig wie möglich“

Michael V. Hayden war von 1999 bis 2005 Direktor der NSA und wurde am 30. Mai 2006 Direktor der CIA.

http://de.wikipedia.org/wiki/National_Security_Agency


Fragen?
August 2013
20