Informationssicherheit, Datenschutz und Bürgerrechte
– Eine kritsche Betrachtung –

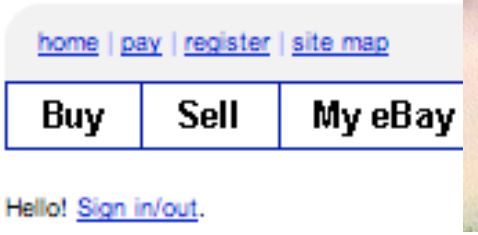
Prof. Dr. Hannes Federrath
Universität Regensburg
Lehrstuhl Management der Informationssicherheit

http://www-sec.uni-regensburg.de/

Neue Technik

- wird nicht nur zu legalen Zwecken eingesetzt, sondern kann auch von Kriminellen genutzt werden; Beispiele:
  - Verabredung von Straftaten, Terrorakten
  - Betrug (Kreditkarten-, Produktbetrug)
  - Verbreitung illegaler Inhalte (Kinderpornographie, Raubkopien)
  - ist selbst Ziel krimineller Handlungen (Viren, Würmer, trojanische Pferde)

- führt zunächst zu einer Ohnmachtserfahrung des Staates
  - „Das Internet ist kein rechtsfreier Raum."
  - Forderung nach besseren Überwachungsmöglichkeiten des Staates



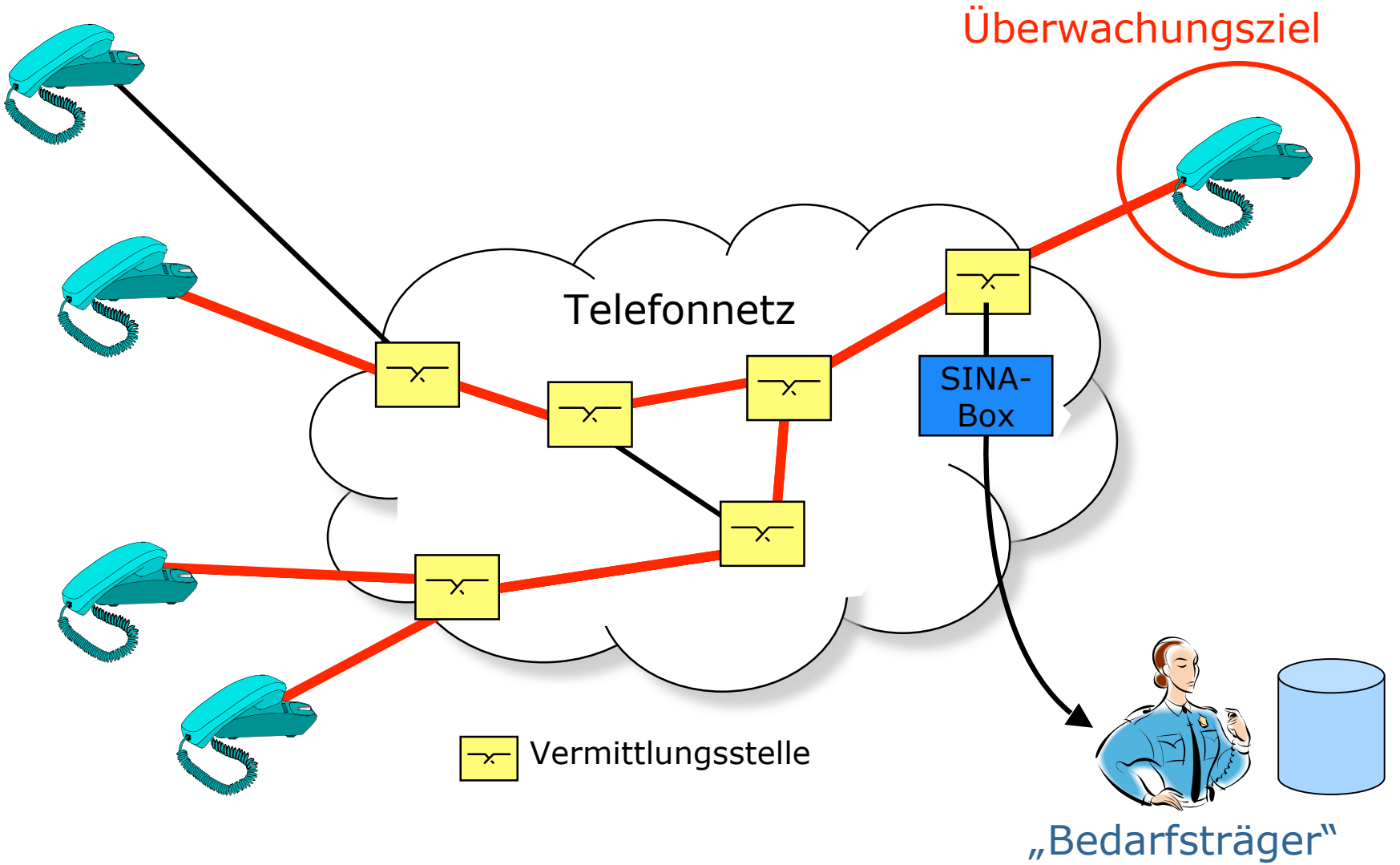
„Je mehr wir wissen, umso besser können wir Euch schützen“

- Beispiele für Techniken zur verbesserten Überwachung von

  Kritischen Infrastrukturen

1. Telefonnetz:
   - Telefonüberwachung
   - IMSI-Catcher
2. Verkehrsnetz:
   - Biometrische Reisepässe
   - Deutsches Mautsystem
3. Internet:
   - E-Mail-Überwachungssystem Carnivore
   - EU-Vorratsdatenspeicherungsrichtlinie

Telefonüberwachung



Telefonüberwachung

- Gesetzliche Grundlagen:
  - GG Art. 10 (Fernmeldegeheimnis)
  - G-10 Gesetz (Ermächtigung für Nachrichtendienste)
  - § 100 a, b StPO (besonders schwere Straftaten)
- Katalogstraftaten (§ 100 a StPO)
  - Hochverrat
  - Gefährdung des demokratischen Rechtsstaates
  - Geld- oder Wertpapierfälschung
  - schweren Menschenhandel
  - Mord
  - Bandendiebstahl
  - Raub
  - Erpressung
  - Geldwäsche
  - …

- Betroffene sind im Nachhinein von der Maßnahme zu informieren

Telefonüberwachung: Reale Zahlen

Quelle: ct, Heft 10, 2006, S.60

- Deutschland im Jahr 2002:
  - Studie Uni Bielefeld:
    - 21974 Anordnungen
    - mehr als 20 Millionen abgehörte Telefongespräche
    - ca. 1,5 Millionen betroffene Bundesbürger
  - Kriminologisches Institut der Uni Münster:
    - Hochrechnung für 2002:
      knapp 4 Millionen betroffene Bundesbürger
- USA im Jahr 2005:
  - Verwaltungsbüro der US-Gerichtshöfe
    - 1773 Anordnungen von Bundes- und Staatengerichten
      + 625 Anordnungen von Bundesbehörden
    - je Anordnung durchschnittlich betroffene US-Bürger: 107

22.000 ÜA · 100 Betroffene = 2.200.000 Betroffene

80 Mio. Bundesbürger / 2,2 Mio. Betroffene ≈ 40, d.h. jeder 40. Bürger ist betroffen

Telefonüberwachung

- Gesetzliche Grundlagen:
  - GG Art. 10 (Fernmeldegeheimnis)
  - G-10 Gesetz (Ermächtigung für Nachrichtendienste)
  - § 100 a, b StPO (besonders schwere Straftaten)
- Katalogstraftaten (§ 100 a StPO)
  - Hochverrat
  - Gefährdung des demokratischen Rechtsstaates
  - Geld- oder Wertpapierfälschung
  - schweren Menschenhandel
  - Mord
  - Bandendiebstahl
  - Raub
  - Erpressung
  - Geldwäsche
  - …

- Gutachten der Max-Planck-Instituts für ausländ. und int. Strafrecht:
  - nur ein Bruchteil der Betroffenen wird im Nachhinein informiert
  - Richtervorbehalt läuft ins Leere

„Je mehr wir wissen, umso besser können wir Euch schützen“

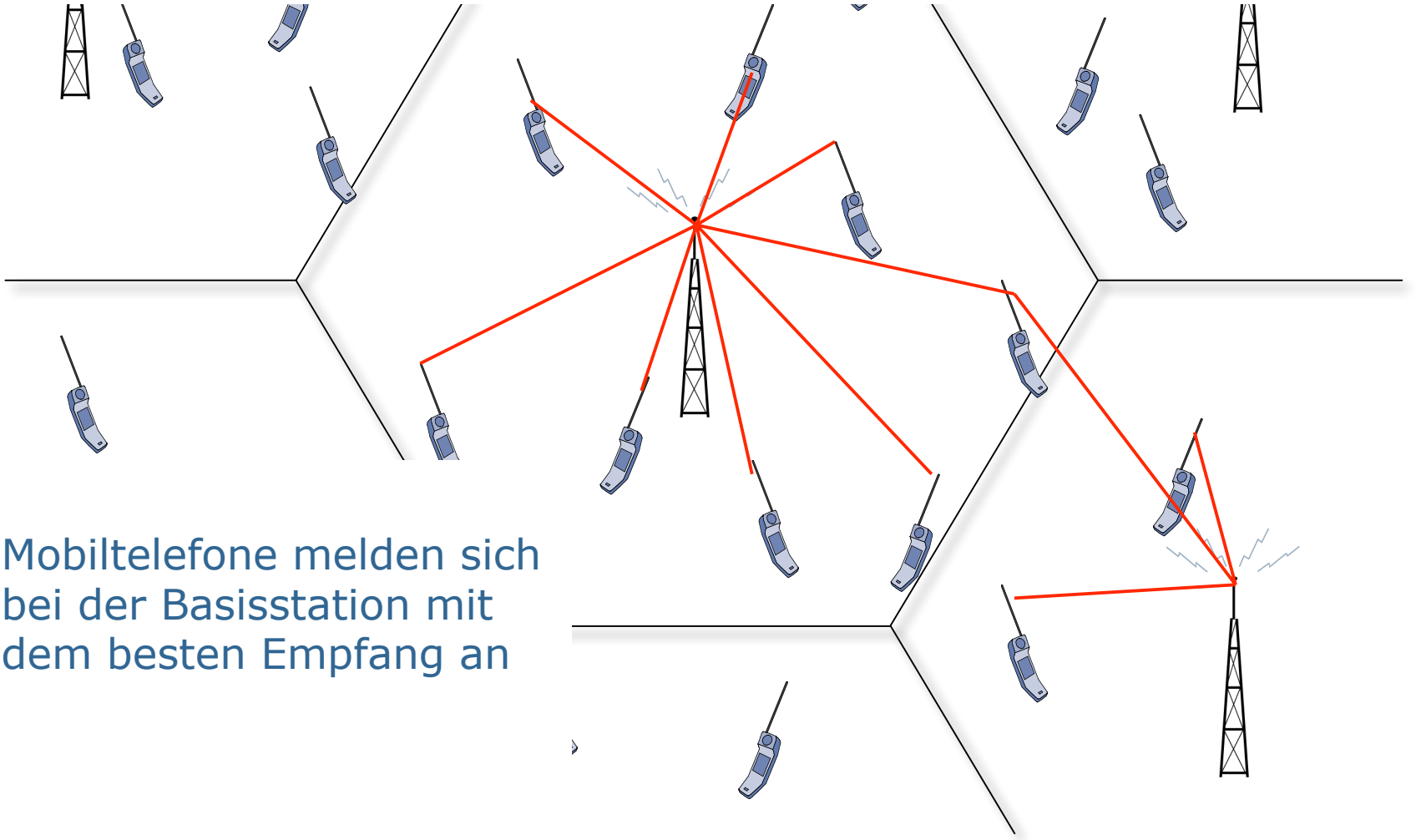
- Beispiele für Techniken zur verbesserten Überwachung von

  Kritischen Infrastrukturen

1. Telefonnetz:
   - Telefonüberwachung
   - IMSI-Catcher
2. Verkehrsnetz:
   - Biometrische Reisepässe
   - Deutsches Mautsystem
3. Internet:
   - E-Mail-Überwachungssystem Carnivore
   - EU-Vorratsdatenspeicherungsrichtlinie

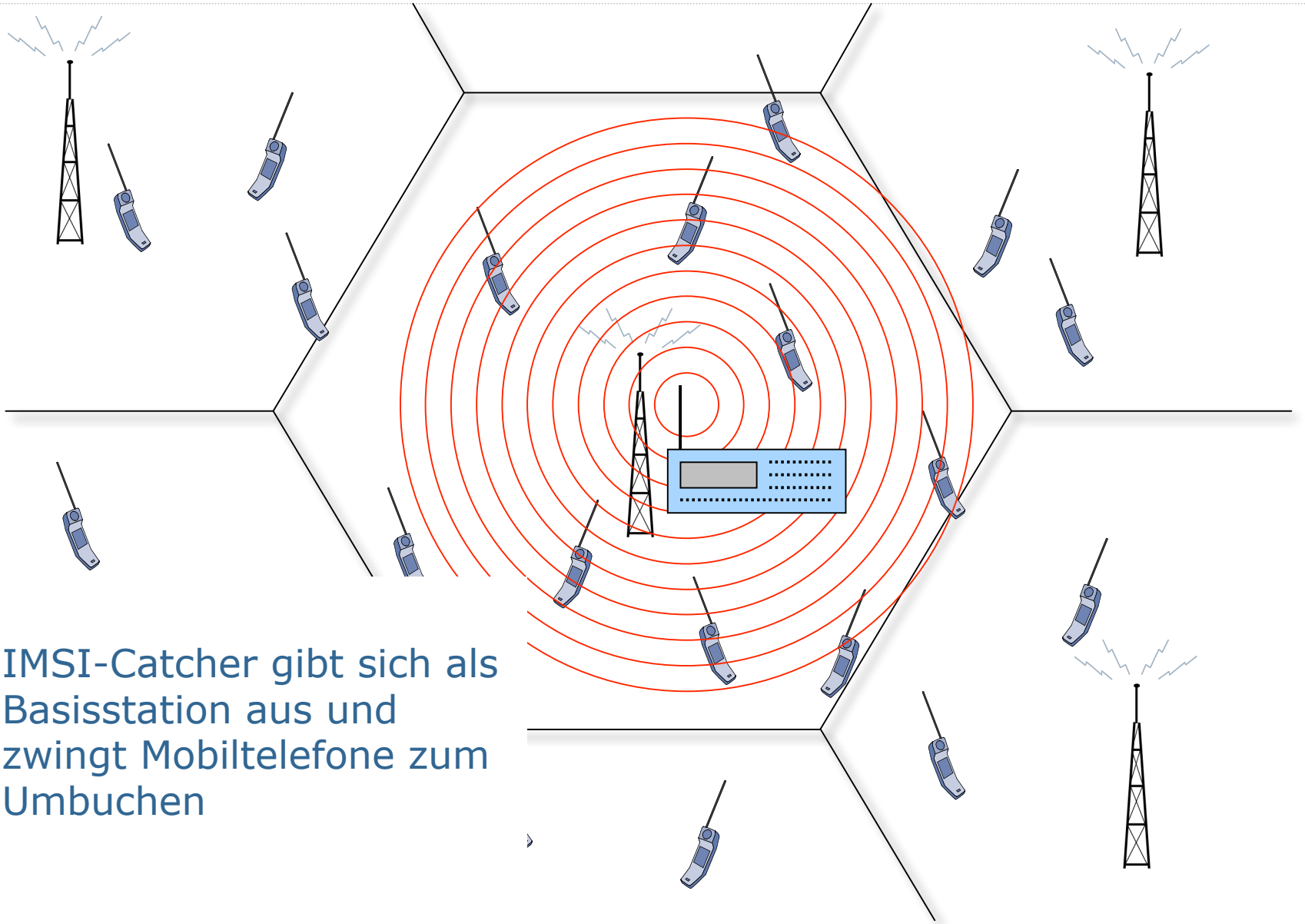
Mobilfunknetze

- IMSI-Catcher: Gerät zur Ortung von Mobilfunkteilnehmern
- IMSI: netzinterne Rufnummer eines Handys



- Mobiltelefone melden sich bei der Basisstation mit dem besten Empfang an

Mobilfunknetze: IMSI-Catcher



- IMSI-Catcher gibt sich als Basisstation aus und zwingt Mobiltelefone zum Umbuchen

Mobilfunknetze: IMSI-Catcher

- Es wird nicht nur der Betroffene geortet, sondern alle in einer Funkzelle befindlichen Mobiltelefone
- IMSI-Catcher wurde über mehrere Jahre ohne rechtliche Grundlage von Polizei und Geheimdiensten eingesetzt
  - „rechtfertigender Notstand"
  - Legalisierung durch Änderung der StPO § 100 i im Jahre 2002
- Einsatz kaum kontrollierbar, da nahezu „unbemerkt" einsetzbar
- momentan zwei Hersteller
  - MMI Research Inc.
  - Rhode & Schwarz

Quelle: Verfassungsschutz, http://www.datenschutz-und-datensicherheit.de/jhrg26/imsicatcher-fox-2002.pdf

„Je mehr wir wissen, umso besser können wir Euch schützen“

- Beispiele für Techniken zur verbesserten Überwachung von

  Kritischen Infrastrukturen

1. Telefonnetz:
   - Telefonüberwachung
   - IMSI-Catcher
2. Verkehrsnetz:
   - Biometrische Reisepässe
   - Deutsches Mautsystem
3. Internet:
   - E-Mail-Überwachungssystem Carnivore
   - EU-Vorratsdatenspeicherungsrichtlinie

Biometrische Reisepässe

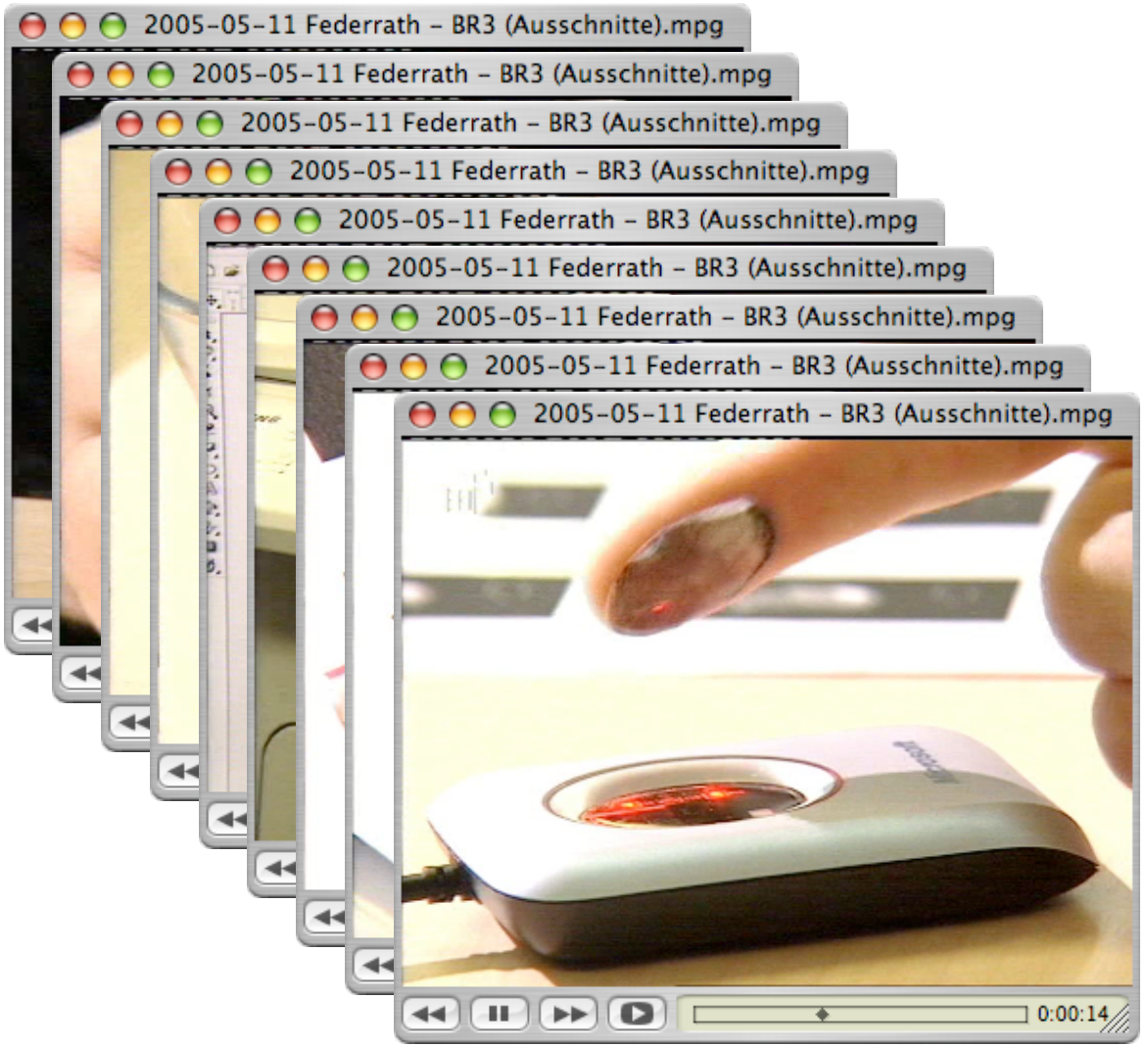
- Seit Herbst 2005 zur Verbesserung der inneren Sicherheit eingeführt

- Neue Funktionen:
  - Speicherung eines Fotos und zukünftig zusätzlich eines Fingerabdrucks des Passinhabers auf einem Chip
  - Kontaktloses Auslesen der biometrischen Merkmale aus dem Chip
- Probleme:
  - Biometrische Merkmale
    - erhöhen nicht die Zuverlässigkeit der Identifikation
    - geben möglicherweise Auskunft über weitere Eigenschaften der Person
  - Kontaktlose Chips
    - lassen sich unter bestimmten Umständen leicht von Jedermann auslesen

Fälschen eines Fingerabdrucks

- Vom Chaos Computer Club im Jahre 2005 praktisch demonstriert.

- Fingerabdruck sichtbar machen
- fotografieren
- nachbearbeiten
- ausdrucken
- Leim drauf
- warten
- abziehen



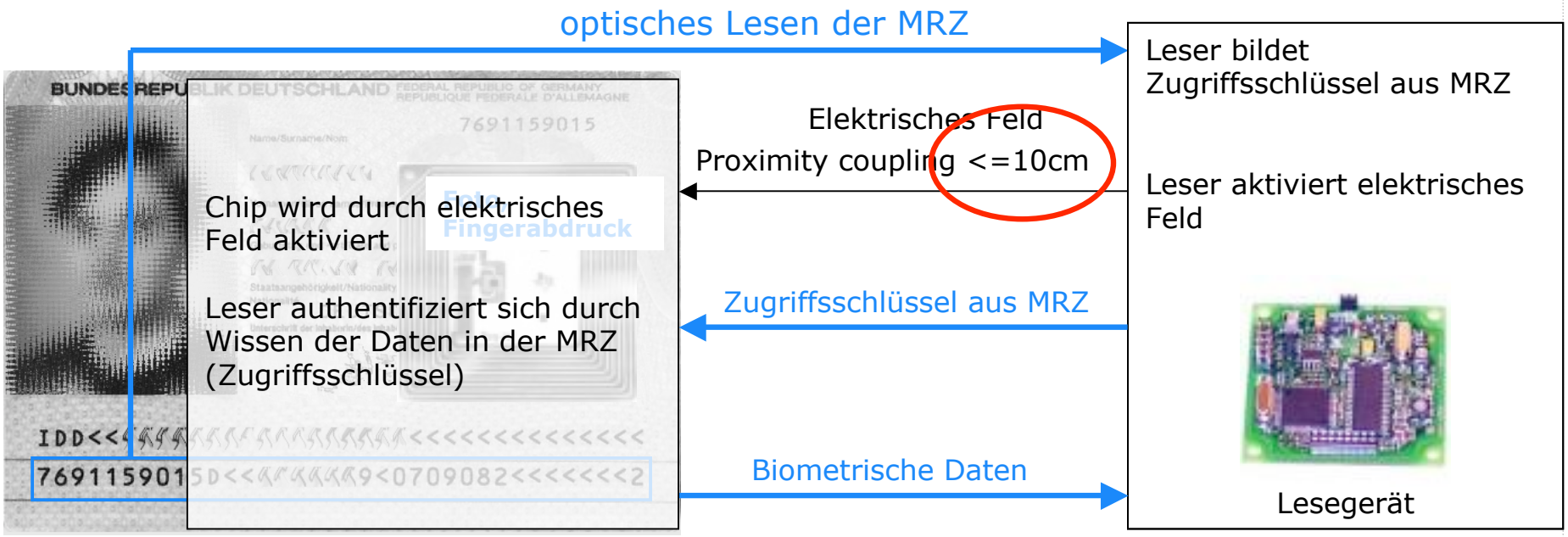
Biometrische Reisepässe

- Seit Herbst 2005 zur Verbesserung der inneren Sicherheit eingeführt

- Neue Funktionen:
  - Speicherung eines Fotos und zukünftig zusätzlich eines Fingerabdrucks des Passinhabers auf einem Chip
  - Kontaktloses Auslesen der biometrischen Merkmale aus dem Chip
- Probleme:
  - Biometrische Merkmale
    - erhöhen nicht die Zuverlässigkeit der Identifikation
    - geben möglicherweise Auskunft über weitere Eigenschaften der Person
  - Kontaktlose Chips
    - lassen sich unter bestimmten Umständen leicht von Jedermann auslesen

Biometrische Daten in Reisepässen

- Kontaktloses Auslesen der biometrischen Daten (vereinfacht)



Machine Readable Zone (MRZ):

```
P<D<<NAME<<VORNAMEN<<<<<<<<<<<<<<
123456789P<<JJMMDDP<JJMMDDP<<<<<<P
```

Passnummer Geburtsdatum Gültigkeitsdatum
jeweils mit Prüfziffer versehen

„Je mehr wir wissen, umso besser können wir Euch schützen“

- Beispiele für Techniken zur verbesserten Überwachung von

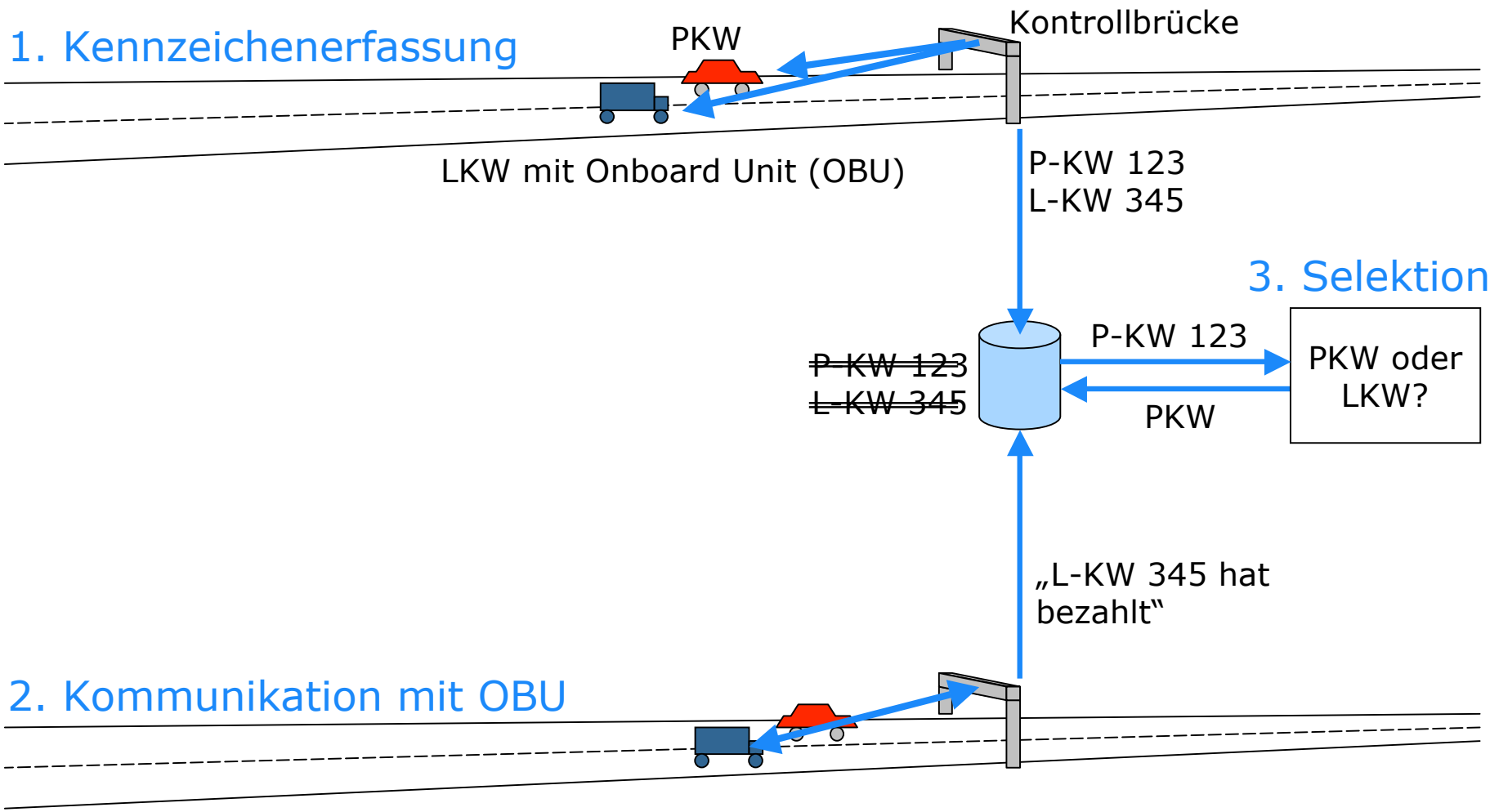
  Kritischen Infrastrukturen

1. Telefonnetz:
   - Telefonüberwachung
   - IMSI-Catcher
2. Verkehrsnetz:
   - Biometrische Reisepässe
   - Deutsches Mautsystem
3. Internet:
   - E-Mail-Überwachungssystem Carnivore
   - EU-Vorratsdatenspeicherungsrichtlinie

Deutsches Mautsystem

- dient der Erhebung von LKW-Straßenbenutzungsgebühren
- Kennzeichen aller durchfahrenden Fahrzeuge werden vorsorglich erfasst
  - PKW und LKW
- Fahrzeuge mit Onboard Unit tauschen Daten mit Kontrollbrücke aus
  - Prepaid System: Alle bezahlten Fahrzeuge werden sofort wieder aus Datenbank gelöscht

Deutsches Mautsystem



Deutsches Mautsystem

- Alle Fahrzeuge werden erfasst (PKW und LKW).
- Gesetzlich verankerte Zweckbindung der Datenerhebung:
  - nur zur Erhebung von Autobahnmaut (LKW)
- Generalbundesanwalt (a.D.) Nehm:
  - Daten sollen auch für Strafverfolgung zur Verfügung stehen (44. Deutscher Verkehrsgerichtstag, Januar 2006)
- Technisch problemlos möglich wären heute schon:
  - Automatische Geschwindigkeitskontrollen
  - Flächendeckende Bewegungsprofile
  - Einführung einer PKW-Maut
- Tollcollect hat für die technische Realisierung dieses perfekten Überwachungssystems den Big Brother Award 2002 erhalten.

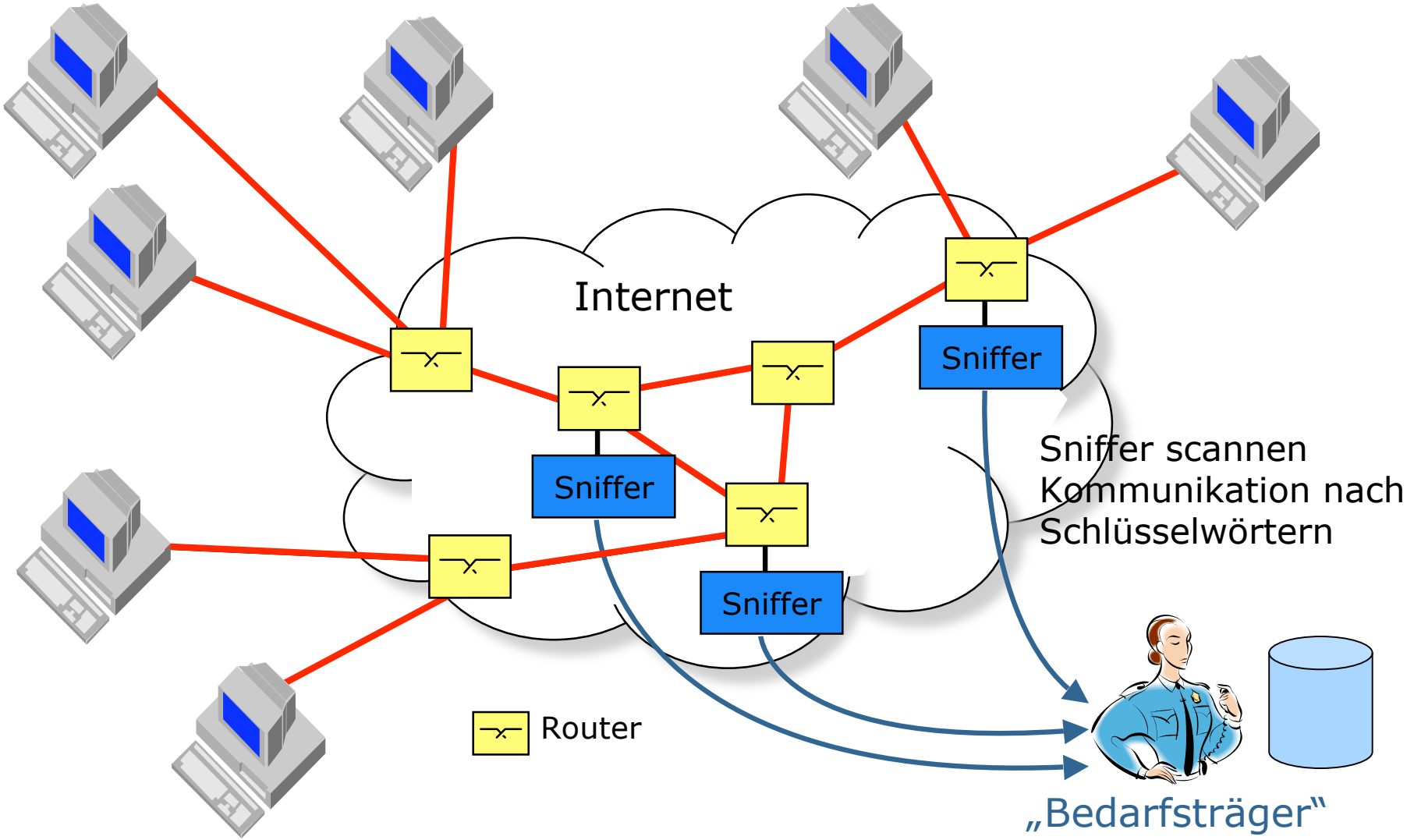
„Je mehr wir wissen, umso besser können wir Euch schützen“

- Beispiele für Techniken zur verbesserten Überwachung von

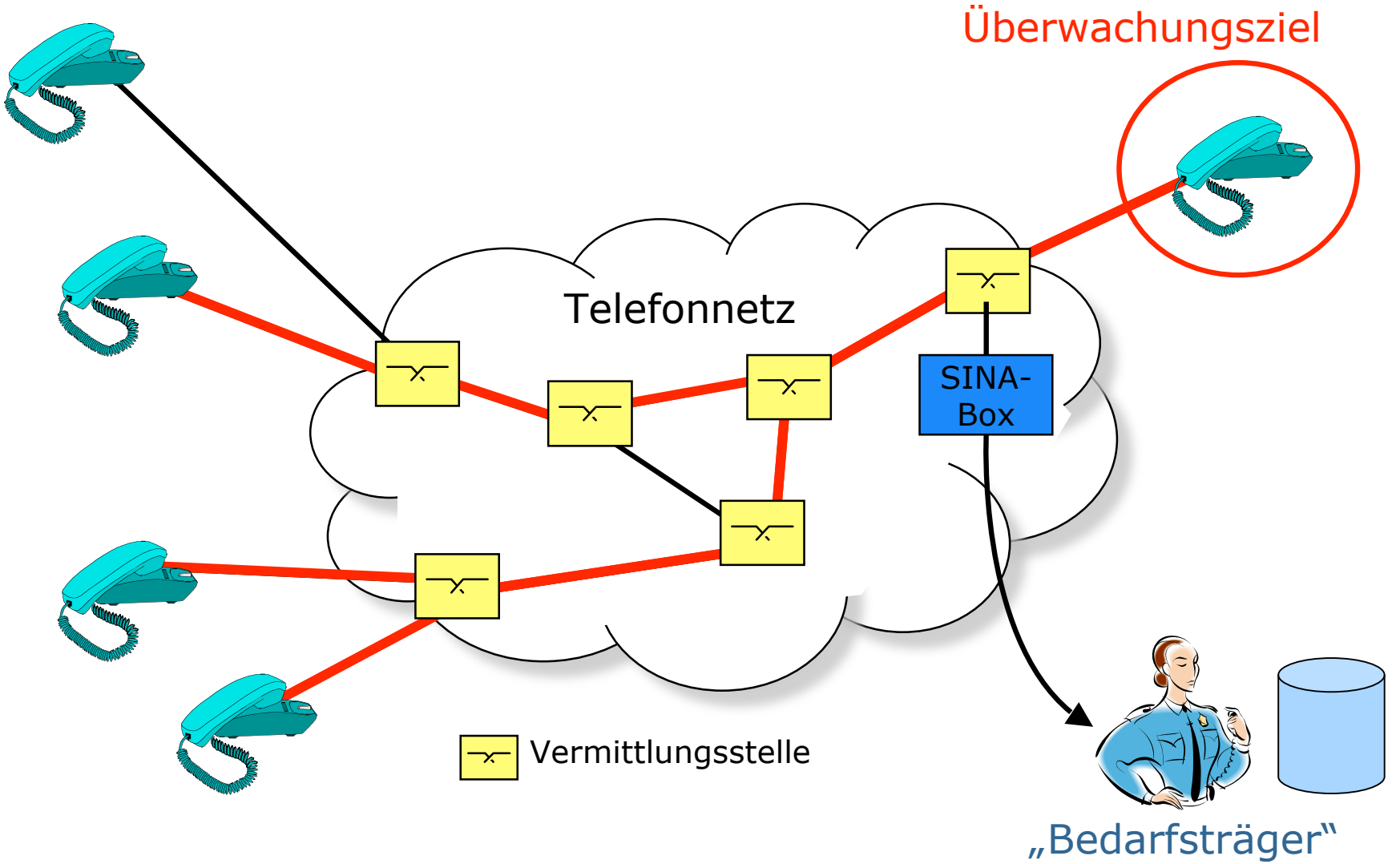
  Kritischen Infrastrukturen

1. Telefonnetz:
   - Telefonüberwachung
   - IMSI-Catcher
2. Verkehrsnetz:
   - Biometrische Reisepässe
   - Deutsches Mautsystem
3. Internet:
   - E-Mail-Überwachungssystem Carnivore
   - EU-Vorratsdatenspeicherungsrichtlinie

Internet: E-Mail-Überwachung: Carnivore



Telefonüberwachung



EU-Vorratsdatenspeicherungsrichtlinie

- Was bisher verdachtsabhängig gespeichert wurde, soll künftig verdachtsunabhängig überwacht werden.
  - Beschluss des Europ. Rates vom Februar 2006
  - Parlament hatte bereits im Dezember 2005 zugestimmt
  - Konkrete Ausgestaltung ist Sache der Nationalstaaten
- Speicherdauer 6 bis 24 Monate
  - Wer welche IP-Adresse zugewiesen bekommen hat,
  - Wer mit wem E-Mails austauscht,
  - Wer mit wem über Internet-Telefonie (VoIP) spricht,
  - Wer welche Webserver kontaktiert,
  - …
- Herausgabe der Daten bei „schweren Straftaten“
  - Hierzu zählen dann auch Urheberrechtsverletzungen.
  - Herausgabe nur an staatliche Stellen
- Aber: EU-Enforcementrichtlinie
  - zivilrechtlicher Auskunftsanspruch vorgesehen

Aufgabe des Staates: Schutz seiner Bürger

- Thomas Hobbes (1588-1679): Staat als Beschützer der Bürger
  - Der Staat hat das Leben seiner Bürger zu schützen, ebenso dessen Besitz und Freiheit.
  - Staat gibt Regeln für das Zusammenleben der Menschen vor.
  - Je stärker der Staat, umso besser kann er Eigentum und Freiheit schützen.
  - Die Bürger haben dem Staat das Monopol der legitimen Machtausübung gegeben.

nach: Hobbes: Leviathan (1651)

- Problem:
  - Hobbes‘ Staatsmodell ist auch „kompatibel“ mit dem Konzept eines Überwachungsstaates.
    - Recht auf informationelle Selbstbestimmung aufgegeben
  - Auch vom Staat gehen Gefahren aus:
    - Am Ende dient der Staat nur noch seiner Selbsterhaltung.

Nicht immer nur der Staat hat die Überwachungsmöglichkeiten

- Beispiele
  - Payback, Google Earth
- Situation von Geheimdiensten heute:
  - Aus der großen Menge (öffentlich) zugänglicher Daten die relevanten herausfinden
- Die Wirtschaft und private Organisationen sammeln heute mehr Daten denn je
  - freiwillige Preisgabe
  - Verbesserung des Service (Customer Relationship Management)
  - illegal (weil kaum nachweisbar und unauffällig) oder in rechtlicher Grauzone (z.B. international handelnde Unternehmen)
- Was kann der Einzelne tun?
  - Zurückhaltung, Skepsis bei Datenweitergabe, technische Schutzmöglichkeiten nutzen (z.B. Verschlüsselung, Anonymisierer)

Nicht immer nur der Staat hat die Überwachungsmöglichkeiten

- Beispiele
  - Payback, Google Earth