



# Als die digitale Privatheit Laufen lernte

Prof. Dr. Hannes Federrath

Sicherheit in verteilten Systemen (SVS)

<http://svs.informatik.uni-hamburg.de>

# Als die digitale Privatheit Laufen lernte

- Ladenburger Kolleg «Sicherheit in der Kommunikationstechnik» 1993
- Schwerpunktprogramm «Sicherheit in der Informations- und Kommunikationstechnik» 1998



# Ladenburger Kolleg «Sicherheit in der Kommunikationstechnik»

- Interdisziplinärer Diskurs zwischen Juristen, Soziologen, Psychologen, Wirtschaftswissenschaftlern und Technikern (Informatiker, Elektrotechniker)

Welche Risiken bei der zunehmenden Vernetzung der kommen auf uns zu?  
Welche Konsequenzen hat die zunehmende Verschmelzung von Beruflichem und Privatem?

- Entwicklung von neuen Lösungen und Demonstratoren zum Schutz der Menschen vor Verlust ihrer informationellen Selbstbestimmung
  - These 1993: Mobilität wird in Zukunft bedeutsame Rolle spielen

Erstes GSM-Netz wurde 1992 in Deutschland in Betrieb genommen.

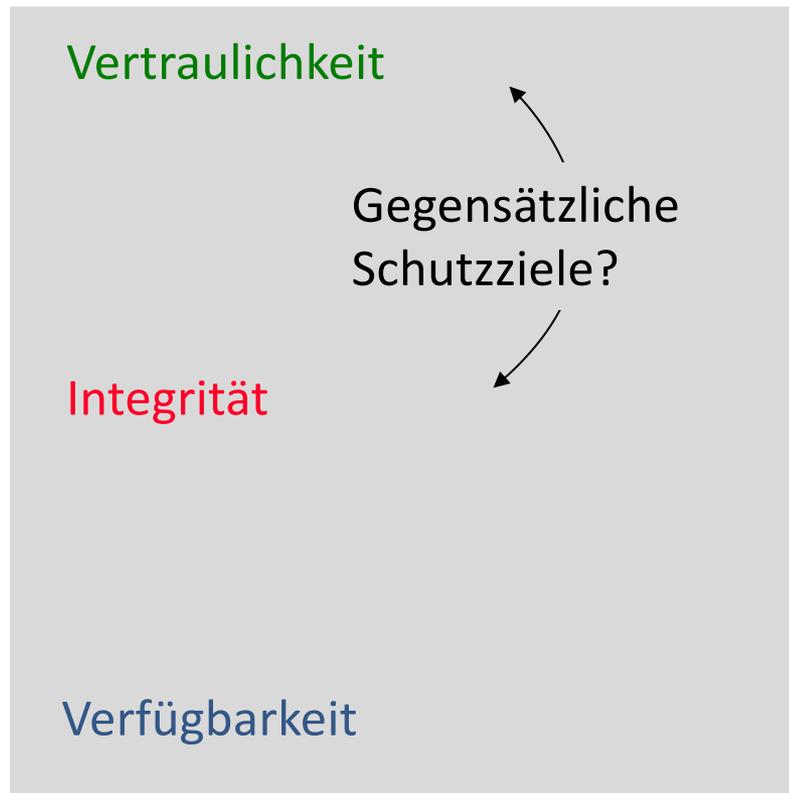
# Ladenburger Kolleg «Sicherheit in der Kommunikationstechnik»

- Entwicklung von neuen Lösungen und Demonstratoren zum Schutz der Menschen vor Verlust ihrer informationellen Selbstbestimmung
- Drei exemplarische Fallbeispiele
  - Konzept der mehrseitigen Sicherheit
  - Verfahren zum Schutz vor Lokalisierung in digitalen Mobilfunknetzen
  - Demonstrator für ein mobiles Erreichbarkeitsmanagement



Andreas Pfitzmann (1958-2010)

- Klassische IT-Sicherheit berücksichtigt im Wesentlichen Risiken, die durch *regelwidriges Verhalten* in IT-Systemen entstehen.

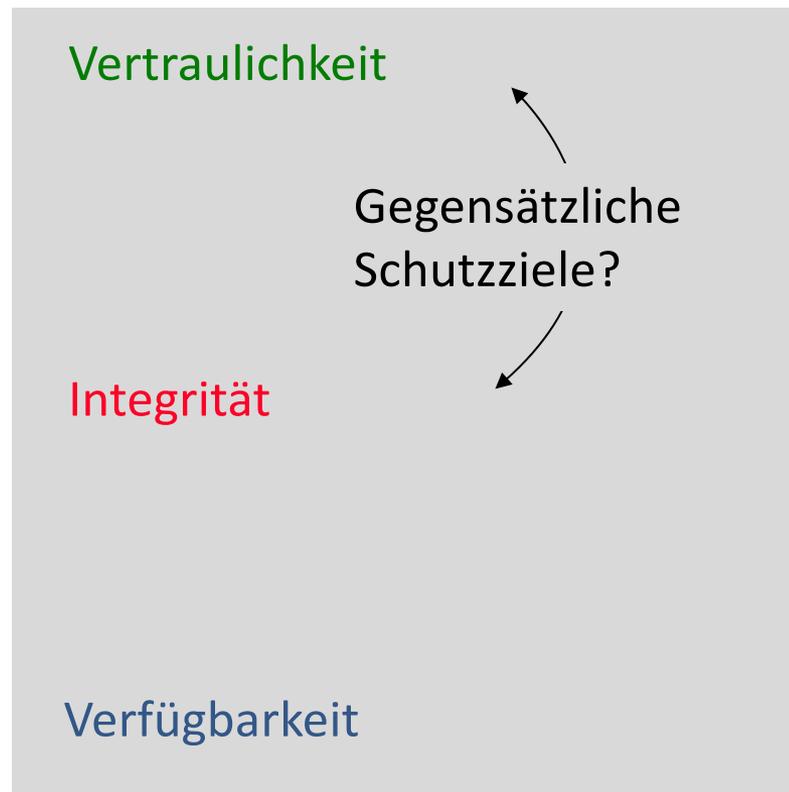


unbefugter Informationsgewinn

unbefugte Modifikation

unbefugte Beeinträchtigung der Funktionalität

- Mehrseitige Sicherheit bedeutet die Einbeziehung der Schutzinteressen aller Beteiligten sowie das Austragen daraus resultierender Schutzkonflikte.



- Voraussetzung
  - regelwidriges Verhalten hält Systeme und Nutzer schadlos
- Ziel
  - gegensätzliche Sicherheitsinteressen werden erkannt, Lösungen ausgehandelt und durchgesetzt

# Schutzziele der mehrseitigen Sicherheit

Kommunikationsgegenstand  
Was?, Worüber?  
Inhaltsdaten

Kommunikationsumstände  
Wann?, Wo?, Wer?  
Verkehrsdaten

Vertraulichkeit  
Verdecktheit

Inhalte

Anonymität  
Unbeobachtbarkeit

Sender

Ort

Empfänger

Integrität

Inhalte

Zurechenbarkeit  
Rechtsverbindlichkeit

Absender

Bezahlung

Empfänger

Verfügbarkeit

Inhalte

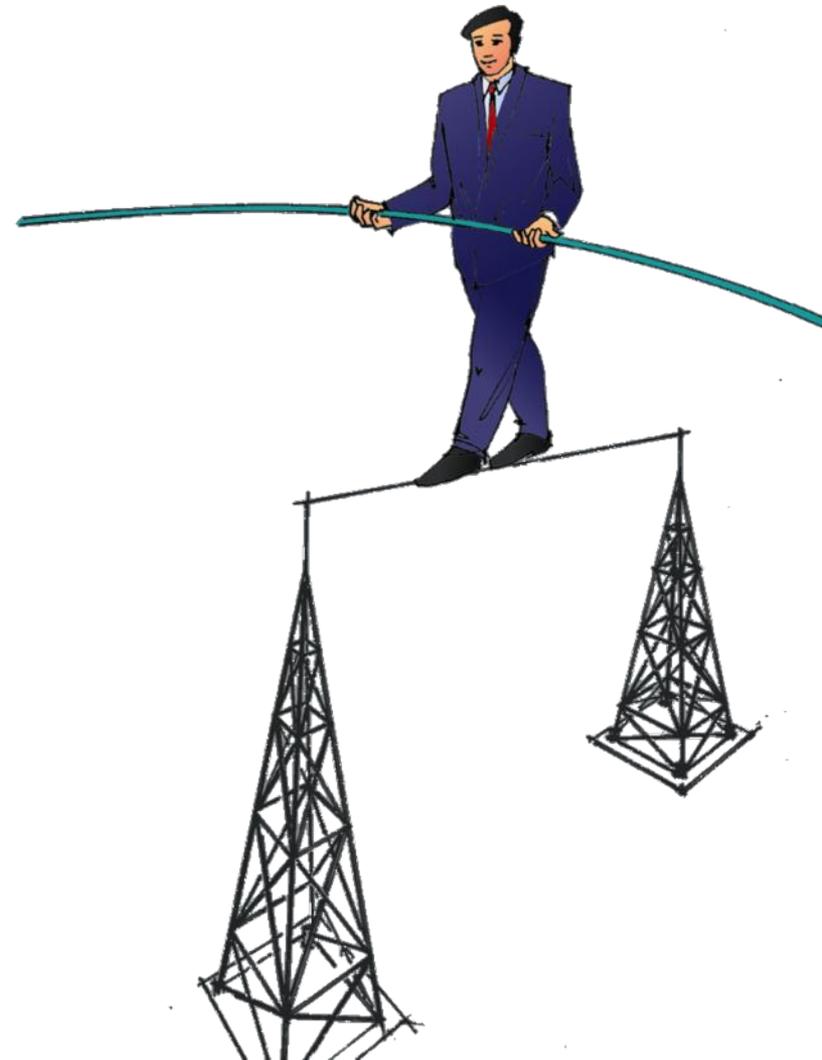
Erreichbarkeit

Nutzer

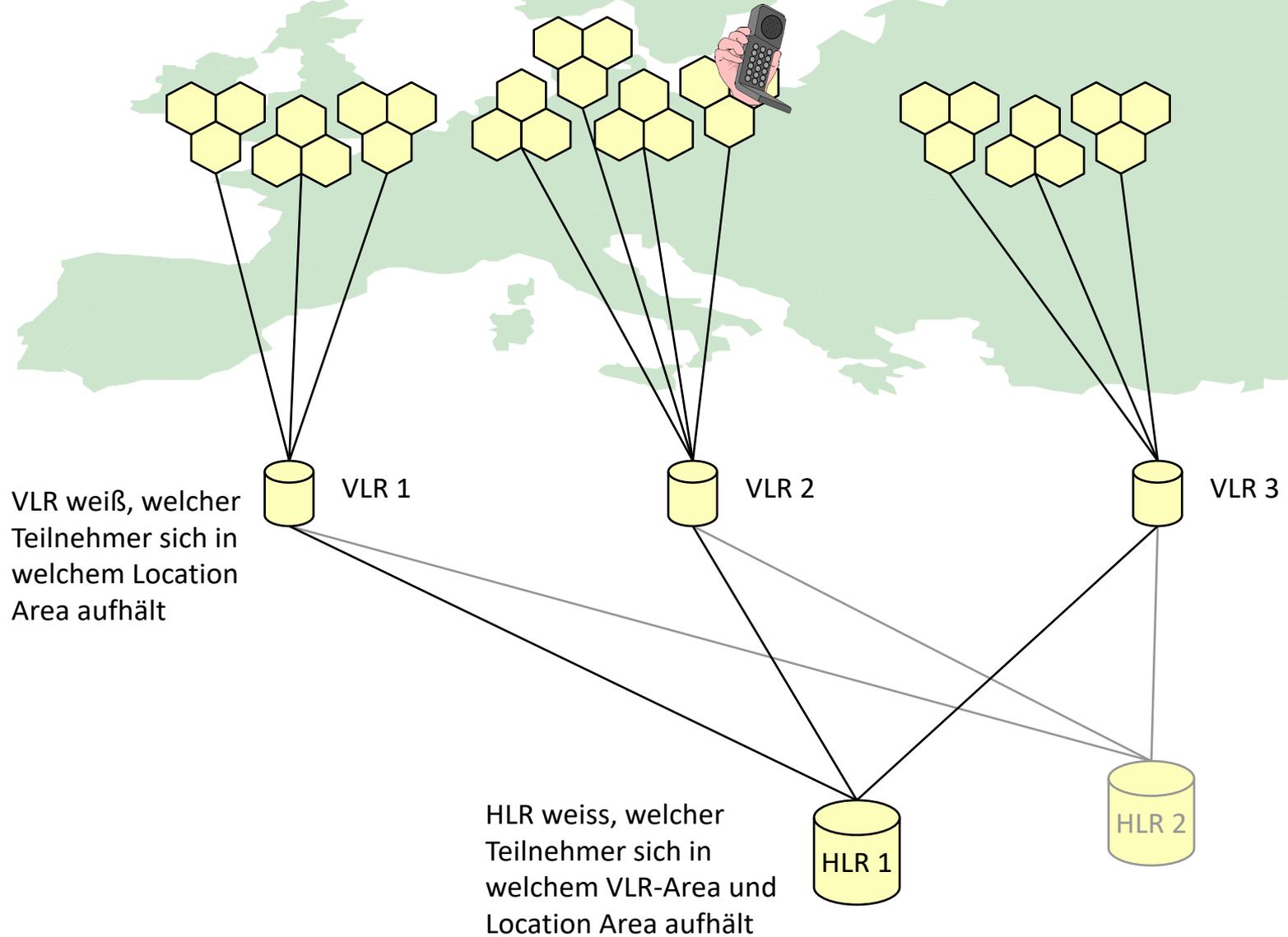
Rechner

# Ladenburger Kolleg «Sicherheit in der Kommunikationstechnik»

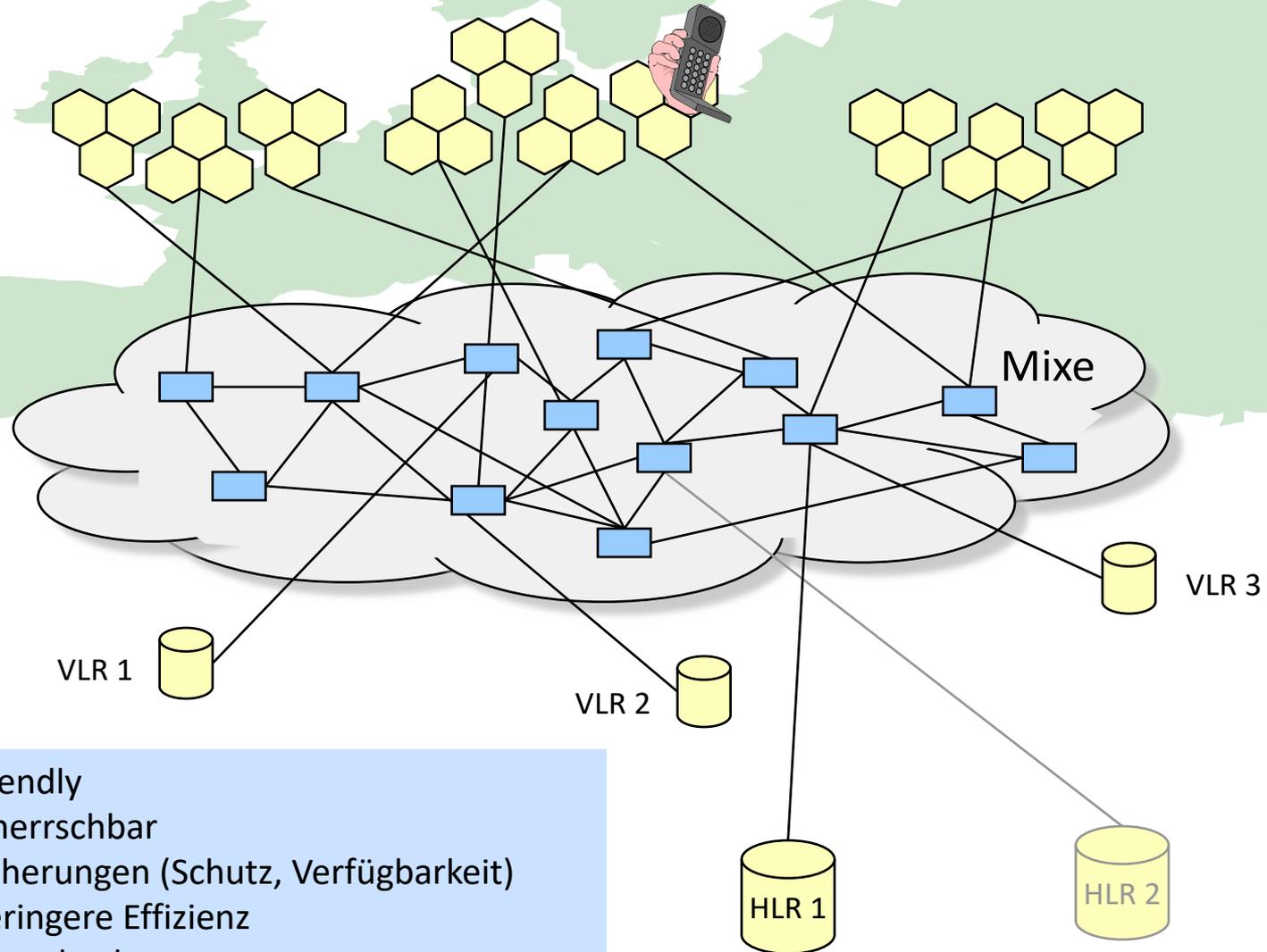
- Entwicklung von neuen Lösungen und Demonstratoren zum Schutz der Menschen vor Verlust ihrer informationellen Selbstbestimmung
- Drei exemplarische Fallbeispiele
  - Konzept der mehrseitigen Sicherheit
  - Verfahren zum Schutz vor Lokalisierung in digitalen Mobilfunknetzen
  - Demonstrator für ein mobiles Erreichbarkeitsmanagement



# Realisierung im GSM

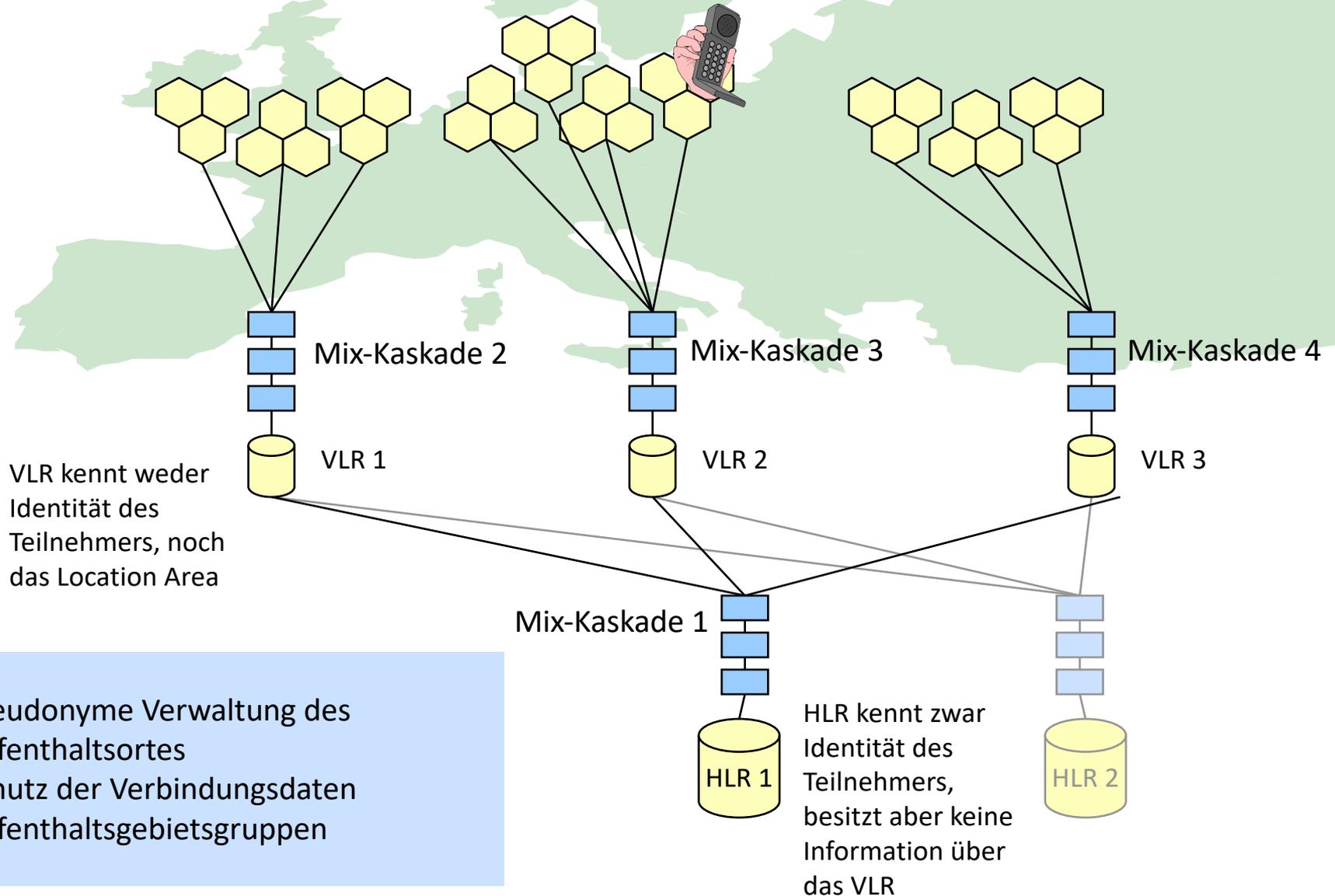


# Mobilkommunikationsmixe: Variante 1: Anonymes Netz



- Internet friendly
- Schwer beherrschbar
- Keine Zusicherungen (Schutz, Verfügbarkeit)
- Deutlich geringere Effizienz
- VLRs werden obsolet

# Mobilkommunikationsmixe: Var. 2: Dedizierte Kaskaden

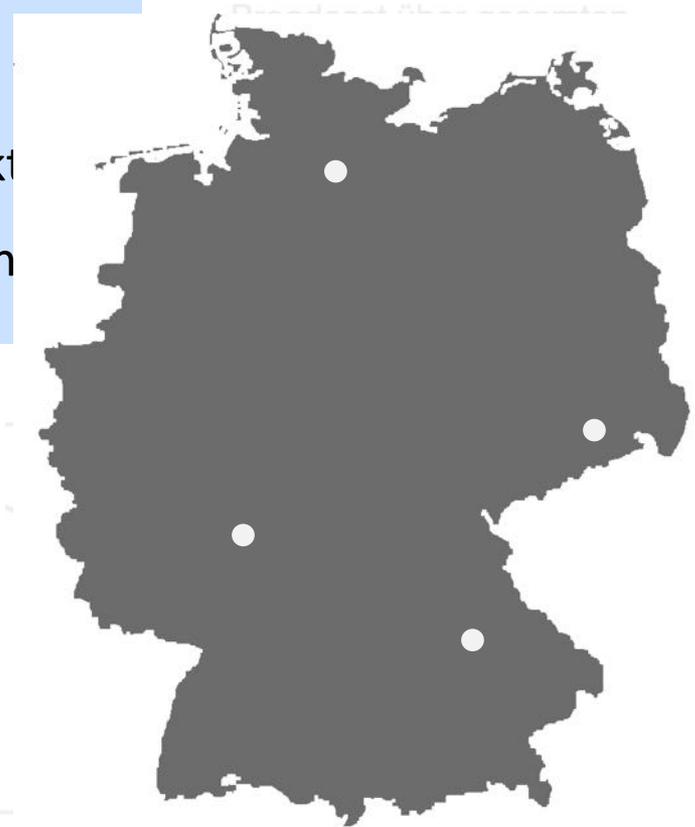




# Verfahren zum Schutz vor Lokalisierung in Mobilfunknetzen

- Vertrauenswürdige Speicherung im Heimbereich (Pfitzmann 1993)

Idee wird aktuell weiterentwickelt im  
Teilprojekt Datenschutz in 5G Netzwerken  
innerhalb des interdisziplinären BMBF-Projekt  
Anonymität Online der nächsten Generation



# Ladenburger Kolleg «Sicherheit in der Kommunikationstechnik»

- Entwicklung von neuen Lösungen und Demonstratoren zum Schutz der Menschen vor Verlust ihrer informationellen Selbstbestimmung
- Drei exemplarische Fallbeispiele
  - Konzept der mehrseitigen Sicherheit
  - Verfahren zum Schutz vor Lokalisierung in digitalen Mobilfunknetzen
  - Demonstrator für ein mobiles Erreichbarkeitsmanagement



Bild: Apple Newton 1993

# 2007 über 1997



The screenshot shows the top portion of a web article on the Stern website. At the top right, there are navigation links for 'NEON', 'NIDO', 'VIEW', and 'STERN TV'. Below these are social media icons for Facebook, Twitter, and Instagram. A search icon is also present. The main navigation bar includes categories like 'Panorama', 'Politik', 'Kultur', 'Lifestyle', 'Digital', 'Wirtschaft', 'Sport', 'Gesundheit', 'Genuss', 'Reise', 'Familie', and 'Auto'. The article title is 'Cebit 1997' with a sub-headline 'Staunen und träumen vor zehn Jahren'. The author is 'Von Sebastian Wieschowski' and the date is '12. März 2007 10:29 Uhr'. A URL box contains the link: <https://www.stern.de/digital/computer/cebit-1997-staunen-und-traeumen-vor-zehn-jahren-3359294.html>

Die Cebit 1997 war die letzte Messe, auf der Mannesmann (heute Vodafone), Viag Interkom (heute o2) und Co. keine erdrutschartigen Preissenkungen verkünden konnten. Mit Spannung wird der Fall des Telekom-Monopols erwartet. Das Mobiltelefon ist 1997 fast ausschließlich in Begleitung eines Geschäftsreisenden anzutreffen. Zwar stellt ePlus mit "free@easy" den ersten Prepaid-Tarif Deutschlands vor, Mobilfunk ist in der Bundesrepublik jedoch immer noch Luxus. Topmoderne Geräte wie das Siemens S6D wogen 190 Gramm und passten mit einer Länge von 19 Zentimetern nicht in jede Jackentasche.

Die Cebit 1997 war die letzte Messe, auf der Mannesmann (heute Vodafone), Viag Interkom (heute o2) und Co. keine erdrutschartigen Preissenkungen verkünden konnten. Mit Spannung wird der Fall des Telekom-Monopols erwartet. Das Mobiltelefon ist 1997 fast ausschließlich in Begleitung eines Geschäftsreisenden anzutreffen. Zwar stellt ePlus mit "free@easy" den ersten Prepaid-Tarif Deutschlands vor, Mobilfunk ist in der Bundesrepublik jedoch immer noch Luxus. Topmoderne Geräte wie das Siemens S6D wogen 190 Gramm und passten mit einer Länge von 19 Zentimetern nicht in jede Jackentasche.

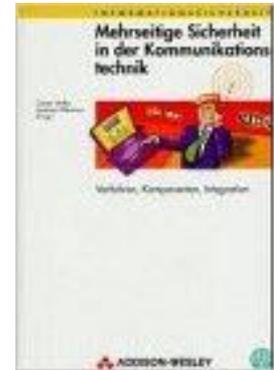
## **Das Internet - ein Megatrend**

Überall auf der Cebit 1997 war ein Wort zu lesen: "Internet". Messebesucher fühlen sich von den schier unendlichen Möglichkeiten des weltweiten Datennetzes angezogen. Trotzdem steckt das Internet 1997 in Deutschland noch in den Kinderschuhen. Onlinekosten von fünf Mark pro Stunde trieben dem Vater von Stefan Fössel Schweißperlen ins Gesicht. In Deutschland haben die drei größten Online-Dienste T-Online, AOL und Compuserve zusammen mehr als 2,6 Millionen Mitglieder.

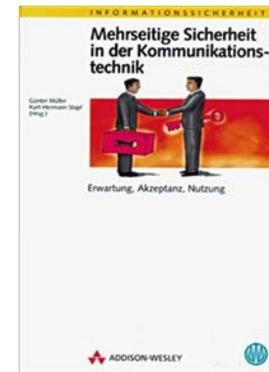
Die DeNic eG, gegründet zum Jahresbeginn, verwaltete lediglich 50.000 deutsche Internetadressen - heute sind es fast 11 Millionen. Domain und Mailadresse kosteten 29 Mark pro Monat - erst ein Jahr später starteten Billigheimer wie Strato oder Puretec mit Kampfpreisen und Web-Visitenkarten für eine Mark.

# Ladenburger Kolleg «Sicherheit in der Kommunikationstechnik»

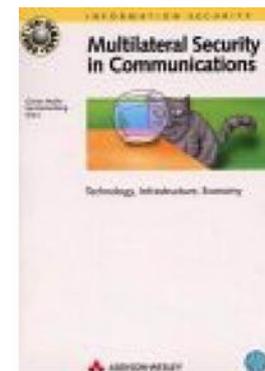
Günter Müller, Andreas Pfitzmann (Hrsg.)  
Mehrseitige Sicherheit in der Kommunikationstechnik,  
Bd.1, Verfahren, Komponenten, Integration  
Addison-Wesley, 1997



Günter Müller, Kurt-Herrmann Stapf (Hrsg.)  
Mehrseitige Sicherheit in der Kommunikationstechnik,  
Bd.2, Erwartung, Akzeptanz, Nutzung  
Addison-Wesley, 1999



Günter Müller, Kai Rannenber (Ed.)  
Multilateral Security in Communications  
Addison-Wesley-Longman, 1999



# DFG-Schwerpunktprogramm

## «Sicherheit in der Informations- und Kommunikationstechnik»

---

- Ausgangspunkt: Schutzziele für mehrseitige IT-Sicherheit
  
- Arbeiten zu den Bereichen
  - Mechanismen und Bausteine
  - Sichere Systeme
  - Methoden
  
- Nachweis der Leistungsfähigkeit anhand von Referenzszenarien

Systemübergreifende Betrachtung von Sicherheit stand im Mittelpunkt

# DFG-Schwerpunktprogramm

## «Sicherheit in der Informations- und Kommunikationstechnik»

**DFG SPP** Sicherheit

### Initiativgruppe:

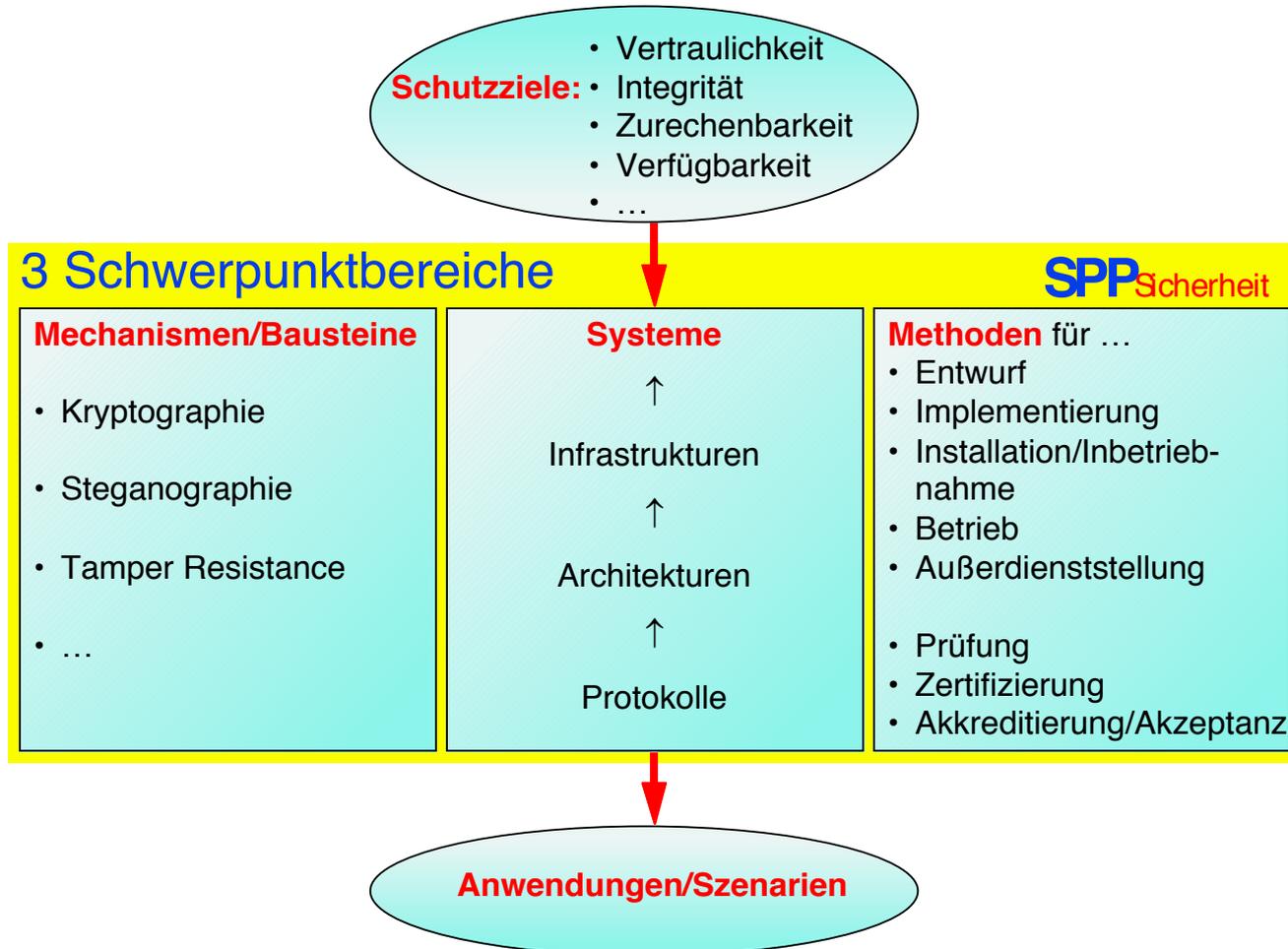
- Prof. Dr. J. Buchmann, Darmstadt
- Prof. Dr. P. Kühn, Stuttgart
- Prof. Dr. G. Müller, Freiburg (Sprecher)
- Prof. Dr. A. Pfitzmann, Dresden
- Prof. Dr. O. Spaniol, Aachen
- Prof. Dr. J. Swoboda, München



# DFG-Schwerpunktprogramm

## «Sicherheit in der Informations- und Kommunikationstechnik»

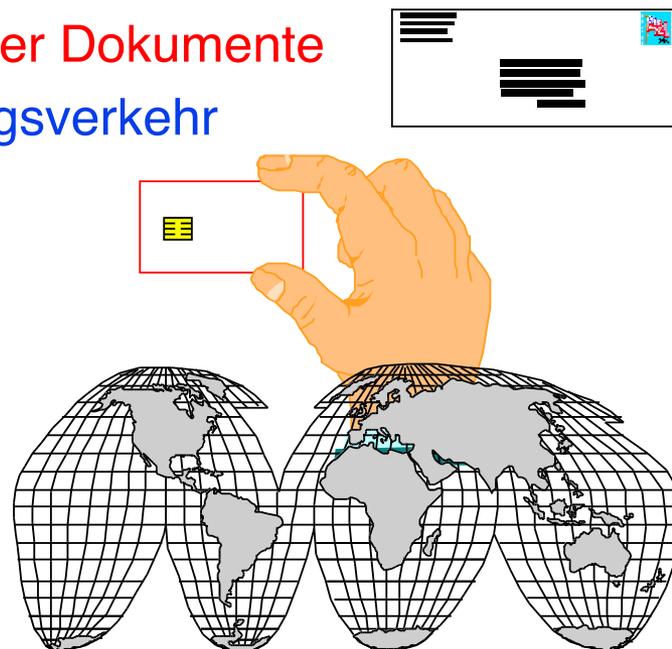
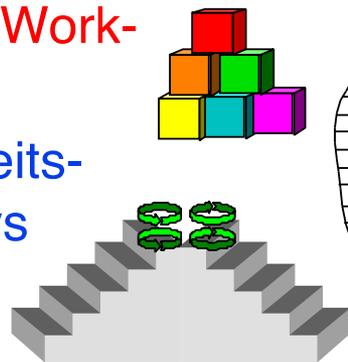
- Folie von 1998:



- Folie von 1998:

### Beispiele für Referenzszenarien **SPP** Sicherheit

- Signieren elektronischer Dokumente
- Elektronischer Zahlungsverkehr
- Digitale Brieftaschen
- Elektronische Marktplätze und Foren
- Sichere Workflows
- Sicherheitsgateways



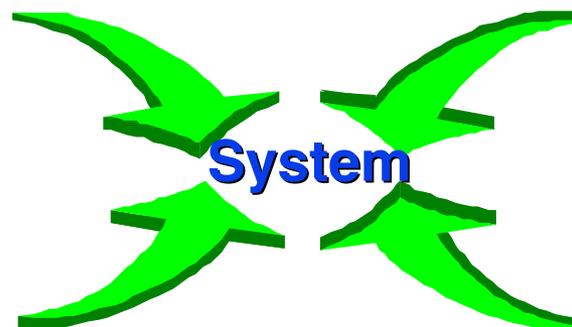
- Folie von 1998:

### Mögliche Arbeitsgegenstände

SPP Sicherheit

- Mechanismen und Bausteine:
  - alternative kryptographische Funktionen
  - Modularisierung von (Krypto)-Funktionen
  - Steganographie/Watermarking
  - Tamper Resistance
  - Fälschungssichere Protokollierung

... stets als Teil des Systems betrachten



## Wo stehen wir heute?

- Sicherheitsfunktionen werden als EU-weit gesetzlich verpflichtender Teil von Datenschutz gefordert
  - Privacy by Design
  - Privacy by Default
- EU-Datenschutzgrundverordnung tritt am 25. Mai 2018 in Kraft





Universität Hamburg Fachbereich  
Informatik Arbeitsbereich SVS Prof. Dr. Hannes  
Federrath  
Vogt-Kölln-Straße 30 D-22527 Hamburg

E-Mail [federrath@informatik.uni-hamburg.de](mailto:federrath@informatik.uni-hamburg.de)

Telefon +49 40 42883 2358

<https://svs.informatik.uni-hamburg.de>