Beobachtungsmöglichkeiten im Domain Name System

Angriffe auf die Privatspäre und
Techniken zum Selbstdatenschutz

Dr. Dominik Herrmann

Folien zum Download:
http://dhgo.to/dns-dagstuhl

Tracking ohne Cookies

Überwachung von Internetnutzern
anhand ihrer DNS-Anfragen

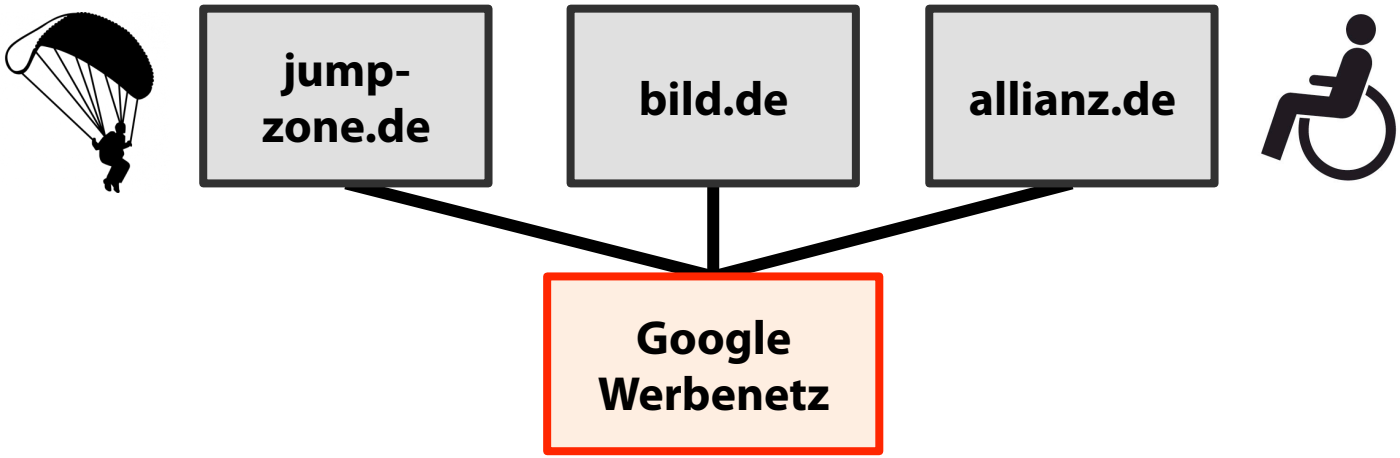
Tracking-Cookie

ID = 22e4970c0a0200bb…

Browser-Fingerprinting

How quickly daft jumping

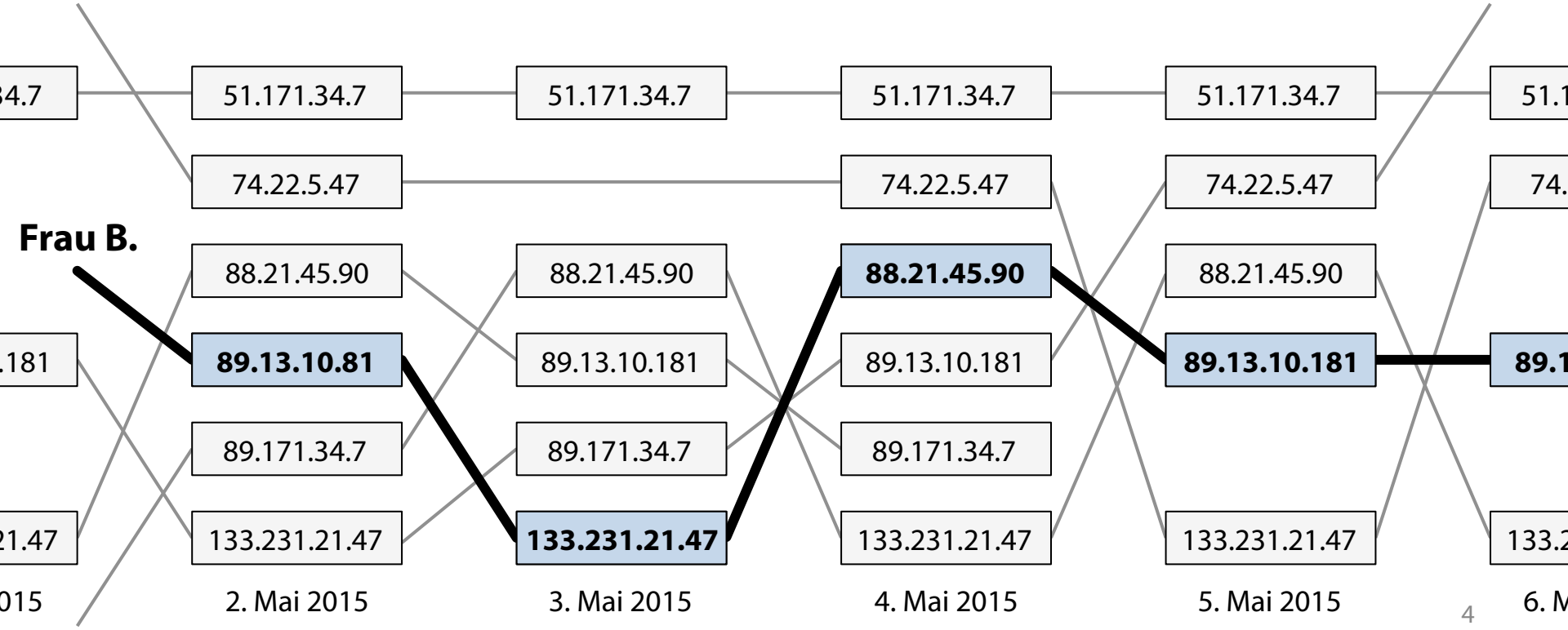
How quickly daft jumping



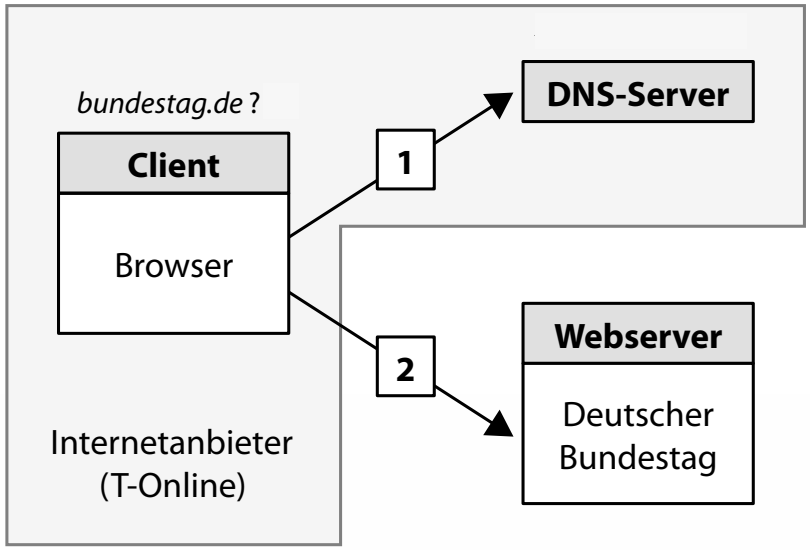
aktuelle Techniken unzuverlässig bzw. erkennbar

Neues Verfahren
Wiedererkennung anhand der beobachtbaren DNS-Anfragen

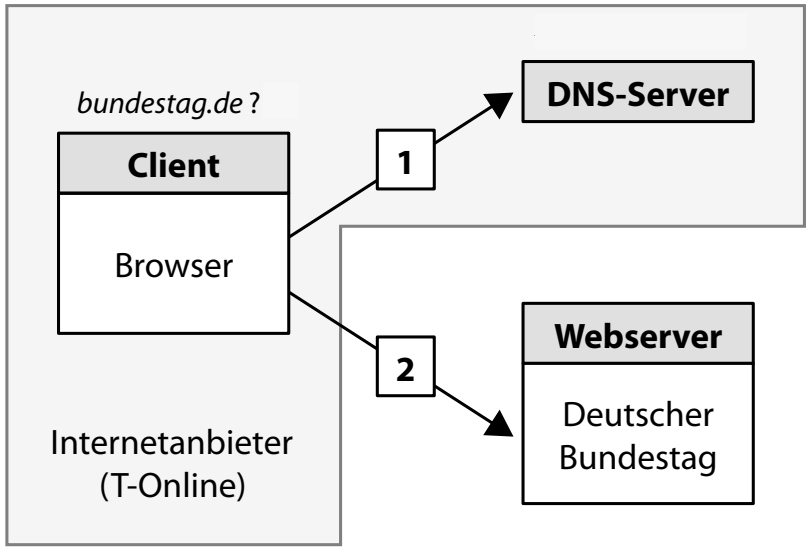
Herausforderung
Wiedererkennung von Nutzern trotz (meist täglich) wechselnder IP-Adressen



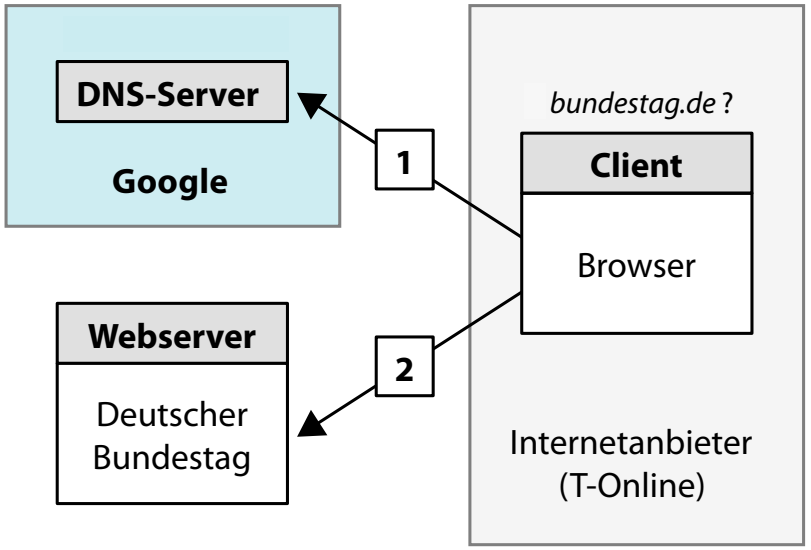
Das Domain Name System löst Domains in IP-Adressen auf.



Vertraulichkeit?
Brauchen wir nicht.



sicherer,
zuverlässiger



Google DNS-Server 8.8.8.8
>150 Mrd. Anfragen pro Tag (2013)

oder doch?

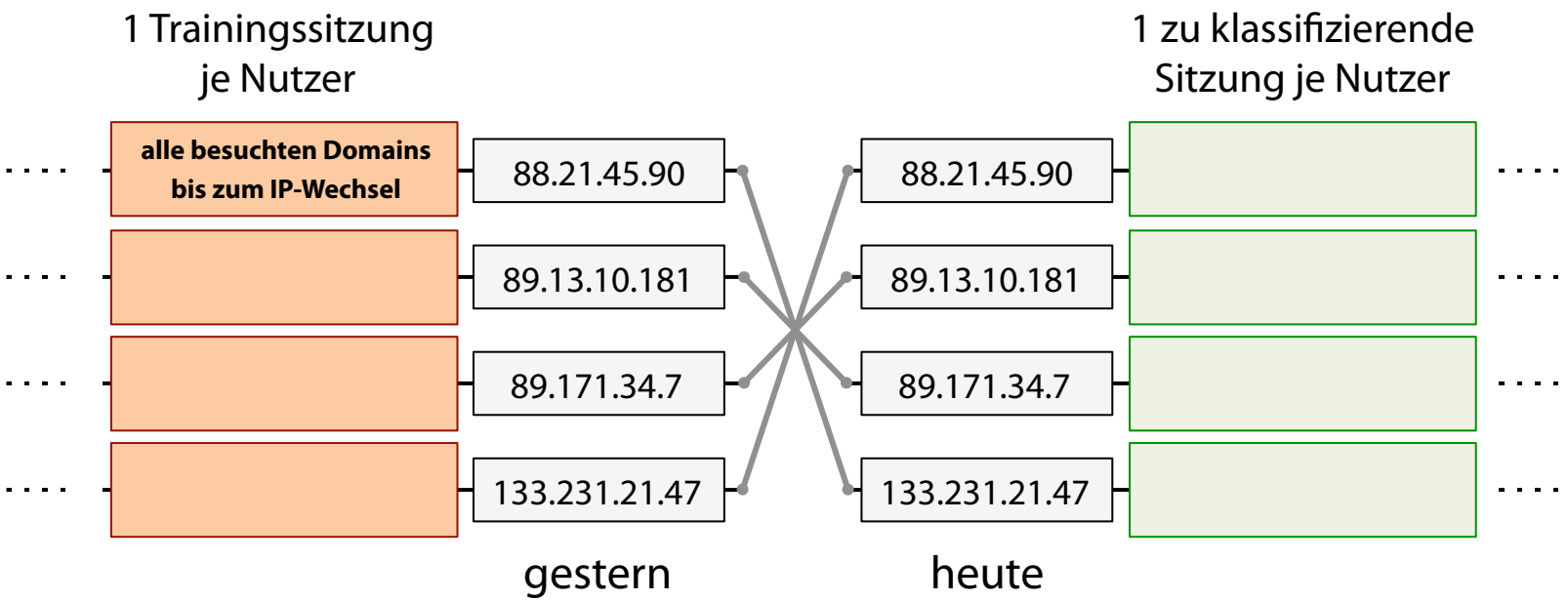
c't magazin

SPIEGEL ONLINE

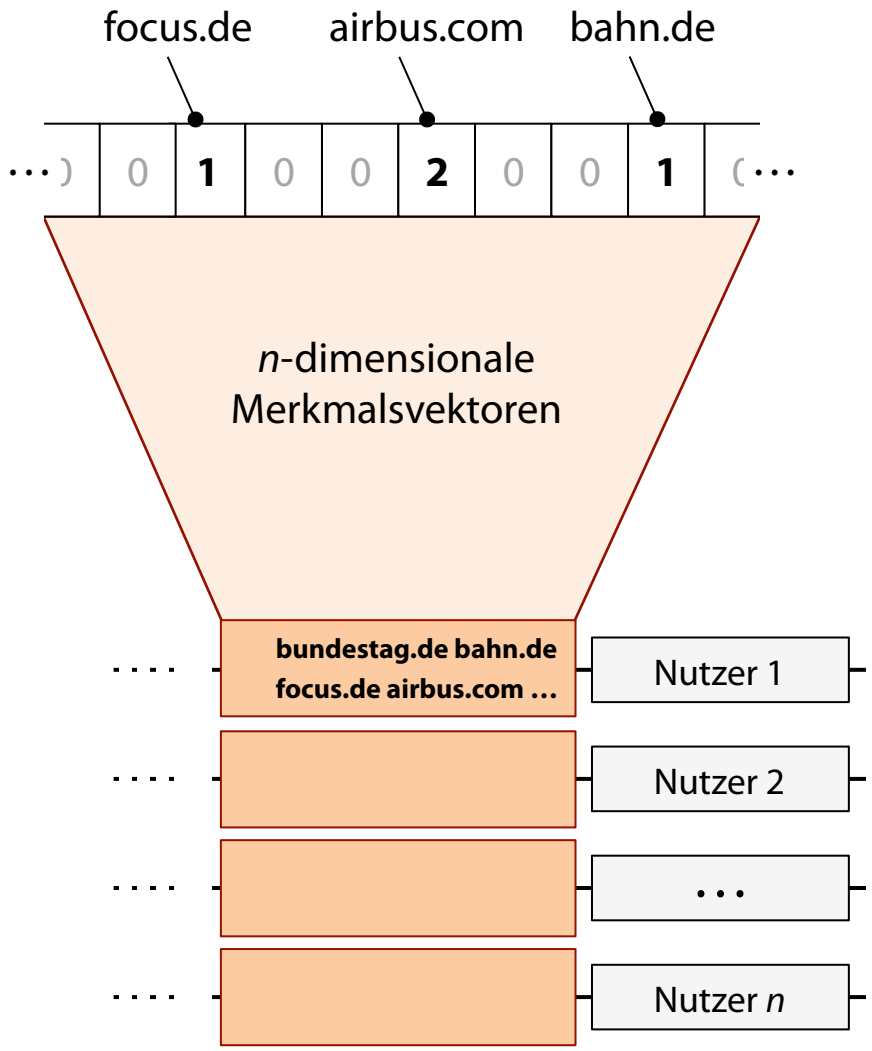
Hypothese

individuelle Vorlieben tägliche Routine

Verkettung durch überwachtes Lernen



Konstruktion des Verkettungsverfahrens



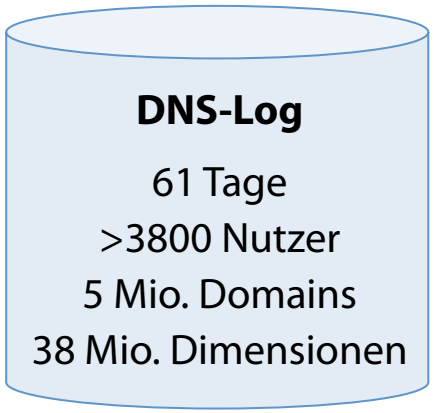
Logarithmierung der Häufigkeiten
Gewichtung mit IDF-Faktor
Normierung der Vektorlänge
Bildung von N-Grammen

1-Nearest-Neighbor-Klassifikator
Cosine-Similarity

Empirische Untersuchung 1/2

Forschungsfragen:

- Genauigkeit?

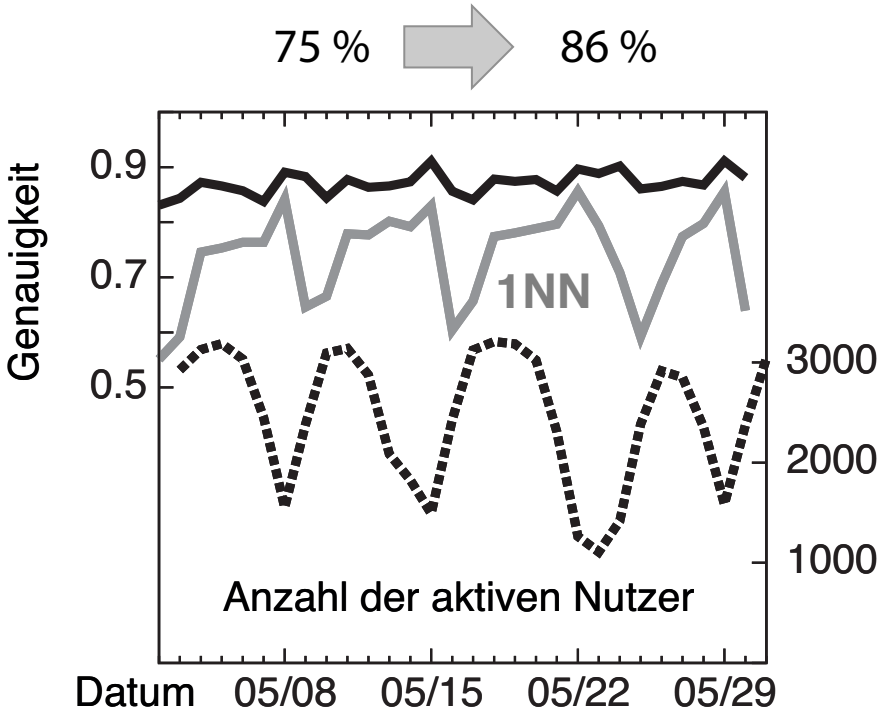


inkl. »ground truth«

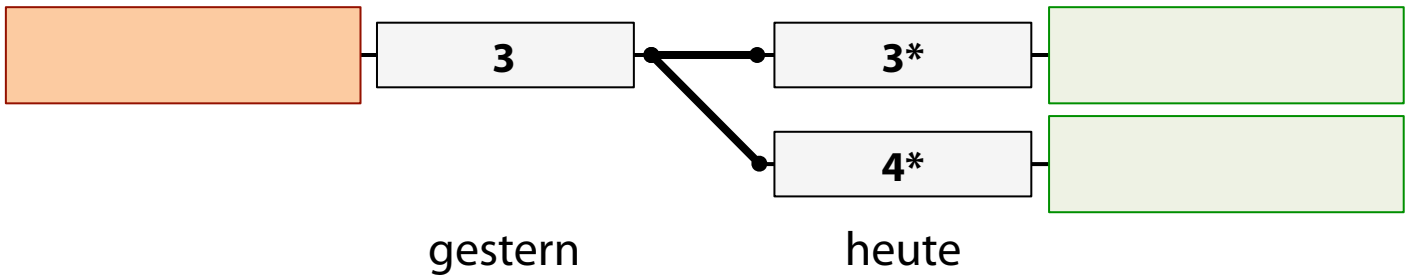
Empirische Untersuchung 1/2

Forschungsfragen:

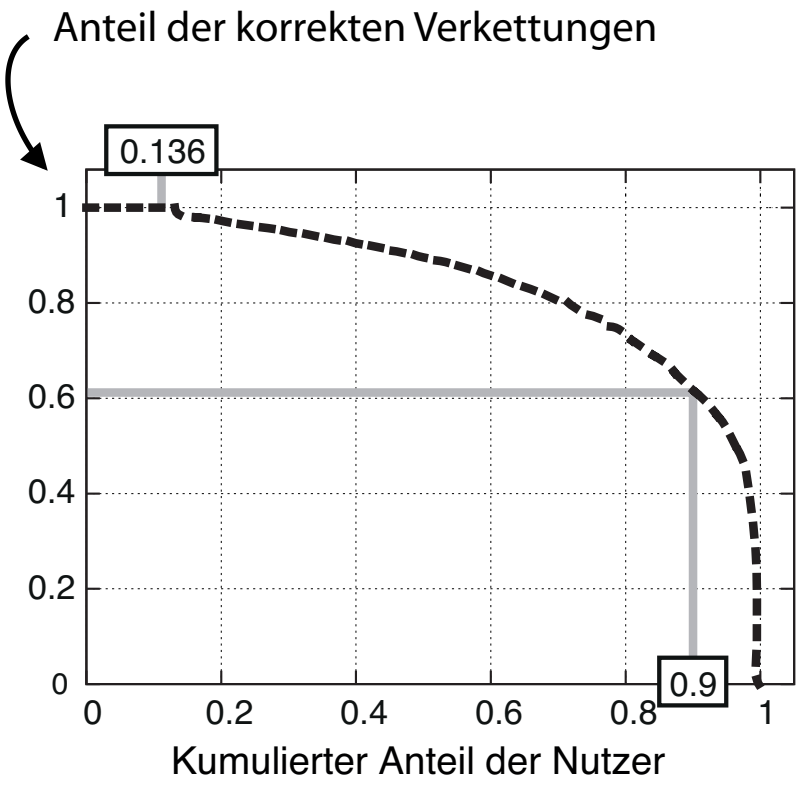
- Genauigkeit?
- Umgang mit Fluktuation?



Mehrdeutige Zuordnungen im **Open-World-Szenario**



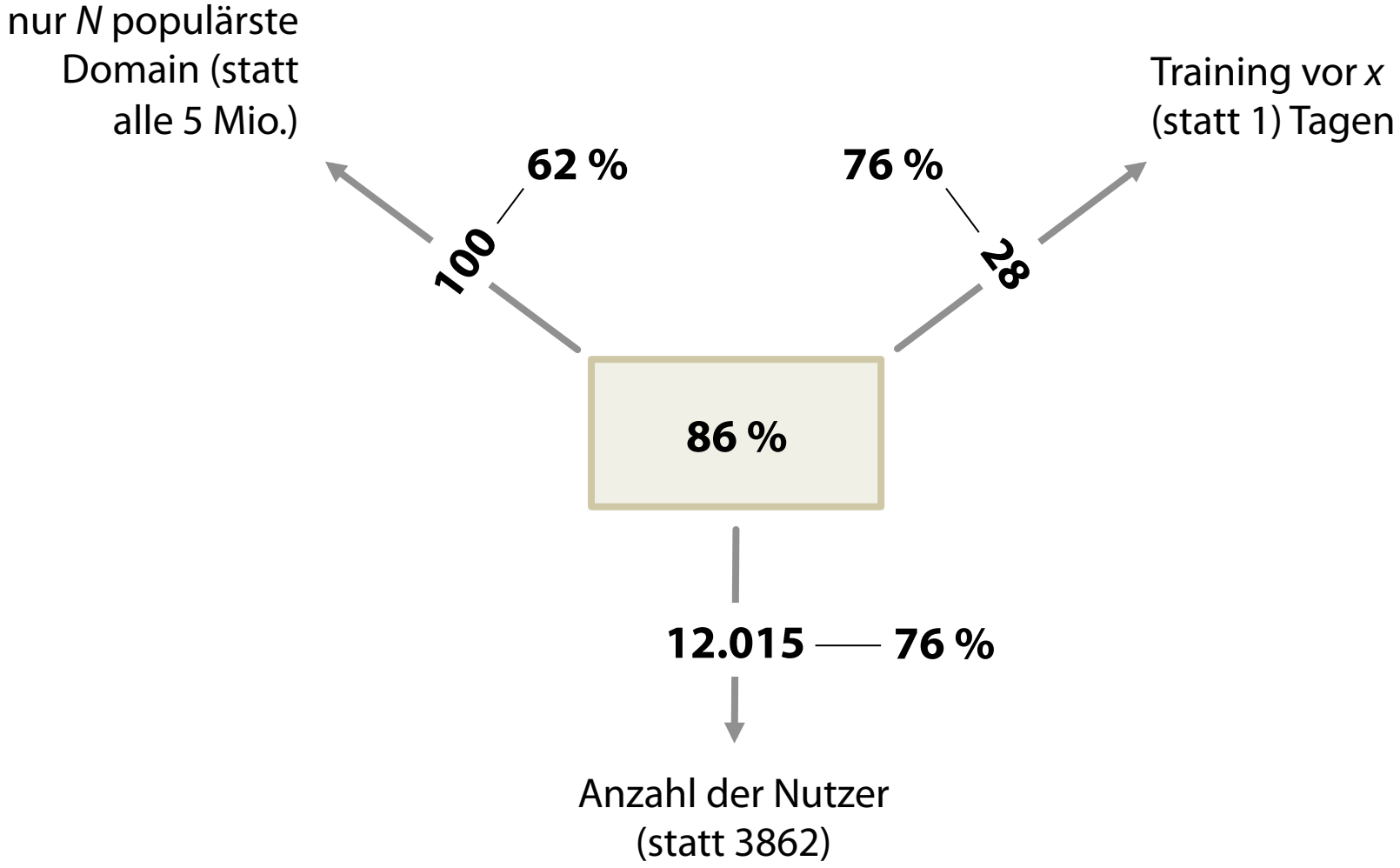
Empirische Untersuchung 2/2



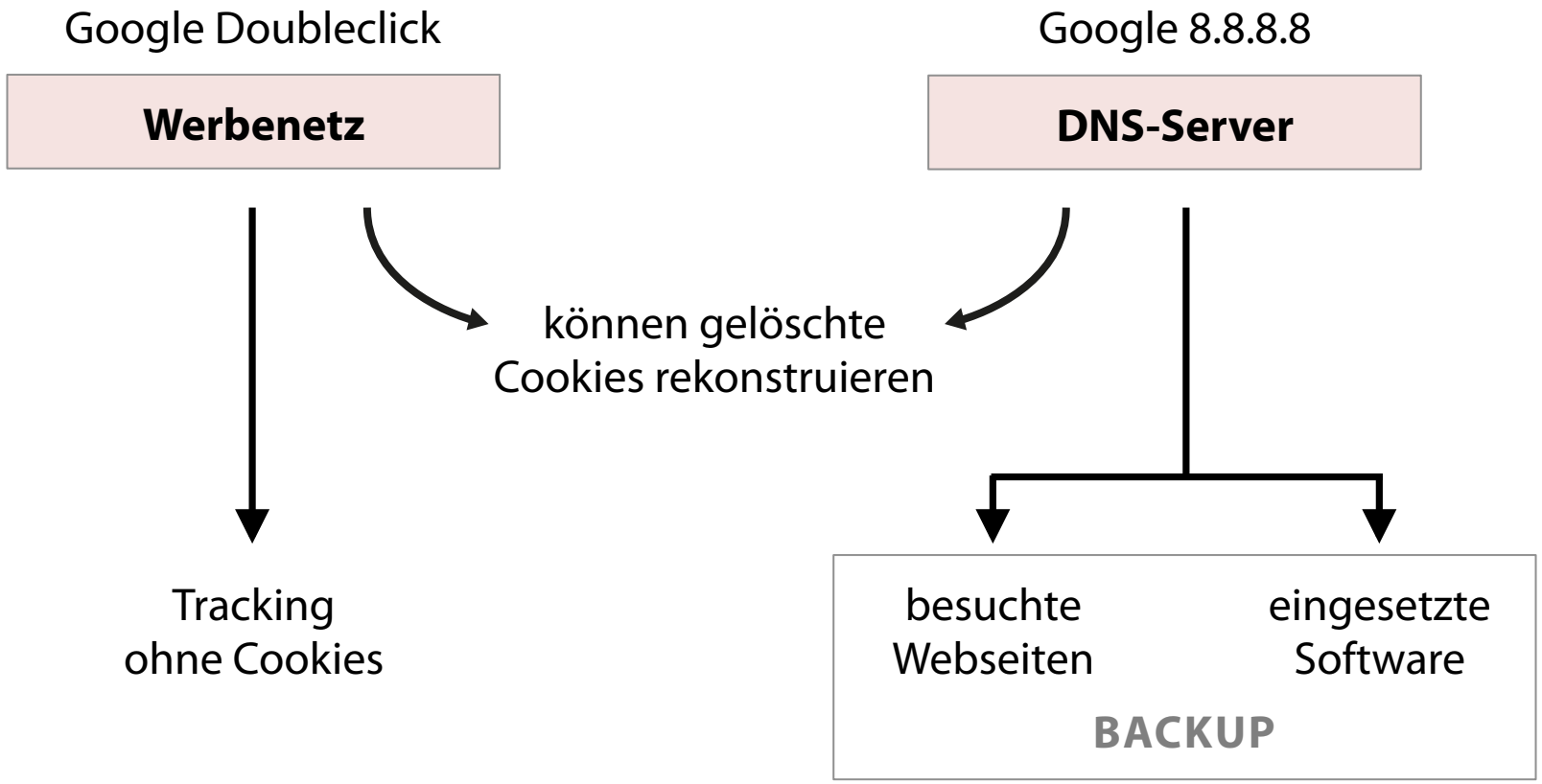
Einflussfaktoren (Spearman)

Stunden/Tag	**+0,32**
Intra-Ähnlichkeit	**+0,26**
Inter-Ähnlichkeit	**–0,46**

Verkettung gelingt auch unter erschwerten Bedingungen



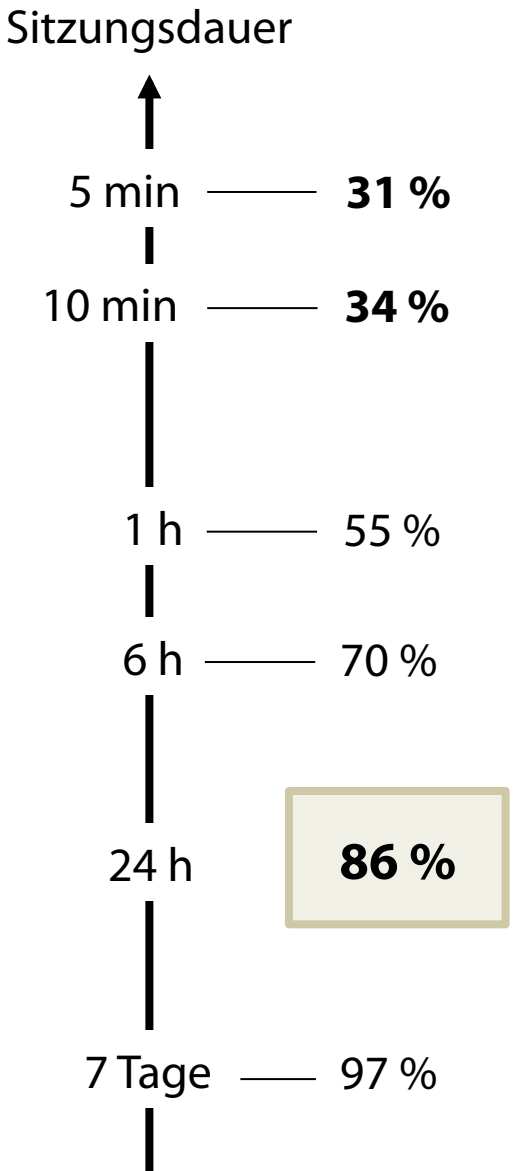
Ergebnis: neue Beobachtungsmöglichkeiten – nicht nur im DNS



rein passiv und
nicht erkennbar

Verlust der informationellen Selbstbestimmung

Praktikable Techniken zum Schutz vor Verkettung



IP-Adresse häufig wechseln

Chance

»Privacy by Default« mit IPv6

Bundesministerium
für Bildung
und Forschung

ANON/NG

Selbstdatenschutz mit DNSMIX

BACKUP

Beobachtungsmöglichkeiten im DNS

umfangreich, aber bislang vernachlässigt

(INFERENZ-)ANGRIFFE AUF DIE PRIVATSPHÄRE	TECHNIKEN ZUM SELBSTDATENSCHUTZ
Verhaltensbasiertes Tracking ohne Cookies	**Häufiger IP-Wechsel** längeres DNS-Caching
DNS-basiertes Website-Fingerprinting	Verschleierung Range Querys
Software-Identifizierung anhand DNS-Verhaltens	Unbeobachtbarkeit DNSMIX-Push-Dienst
Sensibilisierung – aber auch in der IT-Forensik anwendbar	Gestaltungsvorschläge für Forschung und Entwicklung