Informationstechnologie und Sicherheitspolitik

Das Internet als Waffe

Stefan Schumacher

www.sicherheitsforschung-magdeburg.de
Magdeburger Institut für Sicherheitsforschung

Politische Bildungsstätte Helmstedt



Über Mich



Über Mich

- 20+ Jahre Hacker, einige Jahre NetBSD-Entwickler
- Berater für Unternehmenssicherheit `www.Kaishakunin.com`
- Berater für Finanzinstitute, Regierungen, Sicherheitsbehörden
- Direktor des Magdeburger Instituts für Sicherheitsforschung
- Herausgeber des Magdeburger Journals zur Sicherheitsforschung
- `www.Sicherheitsforschung-Magdeburg.de`
- Lehrbeauftragter

Forschungsprogramme des MIS

- Psychologie der Sicherheit
  - Social Engineering
  - Security Awareness, Sicherheit in Organisationen
  - Didaktik der Sicherheit
  - Didaktik der Kryptographie
- Lehrerfortbildung
  - Lernfelder: Fachinformatiker IT-Sicherheit
  - Lernfelder: IT-Sicherheit für Kaufleute
  - Lernfelder: IT-Sicherheit für Elektroberufe
- IT-Sicherheit in KMU
  - empirische Grundlagenforschung
  - didaktische Aufbereitung
  - Schulungen

Schulungs- und Beratungsangebote

- Sicher unterwegs in Internet
- Security Awareness Kampagnen konzipieren
- Die psychologischen Grundlagen des Social Engineerings
- Anonymität und Überwachung im Internet
- Der digitale Untergrund: zur aktuellen Bedrohungslage im Internet
- Kryptographie - Konzepte, Methoden und Anwendungen
- Strategien im Wirtschaftskrieg
- Selbstschutz in Krisengebieten
- Netzwerke absichern

Informationstechnologie und Sicherheitspolitik

Sambleben, J. und Schumacher, S. (Herausgeber)

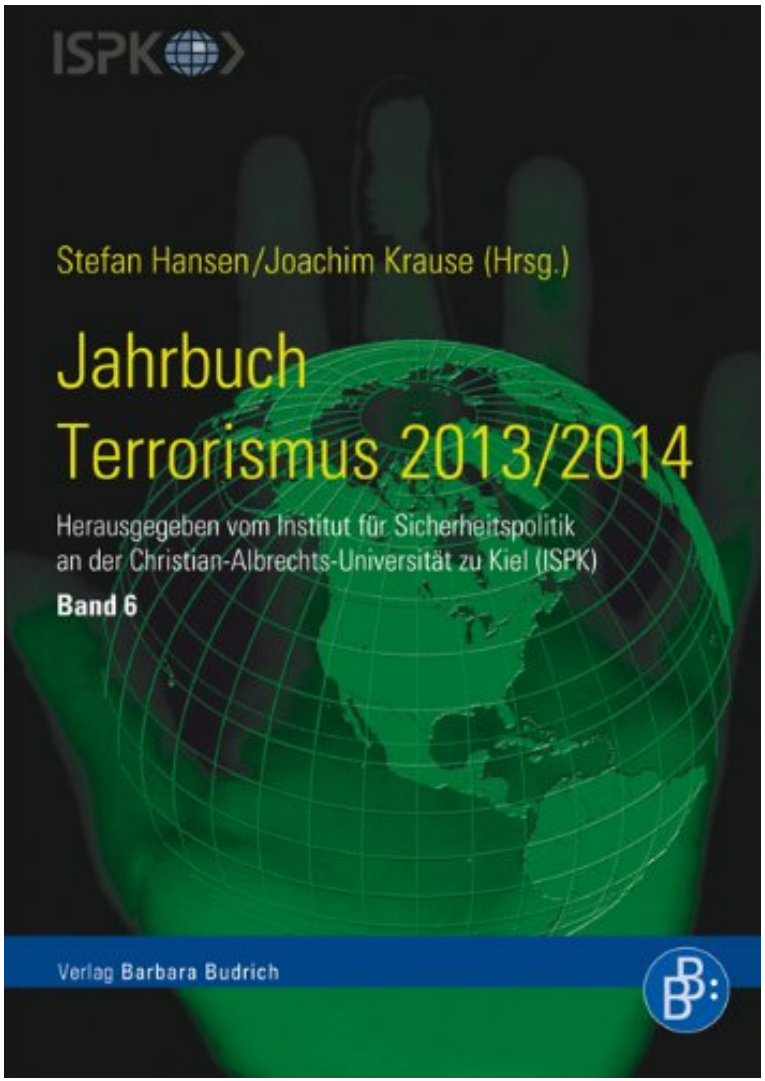


sicherheitsforschung-magdeburg.de/buecher.html

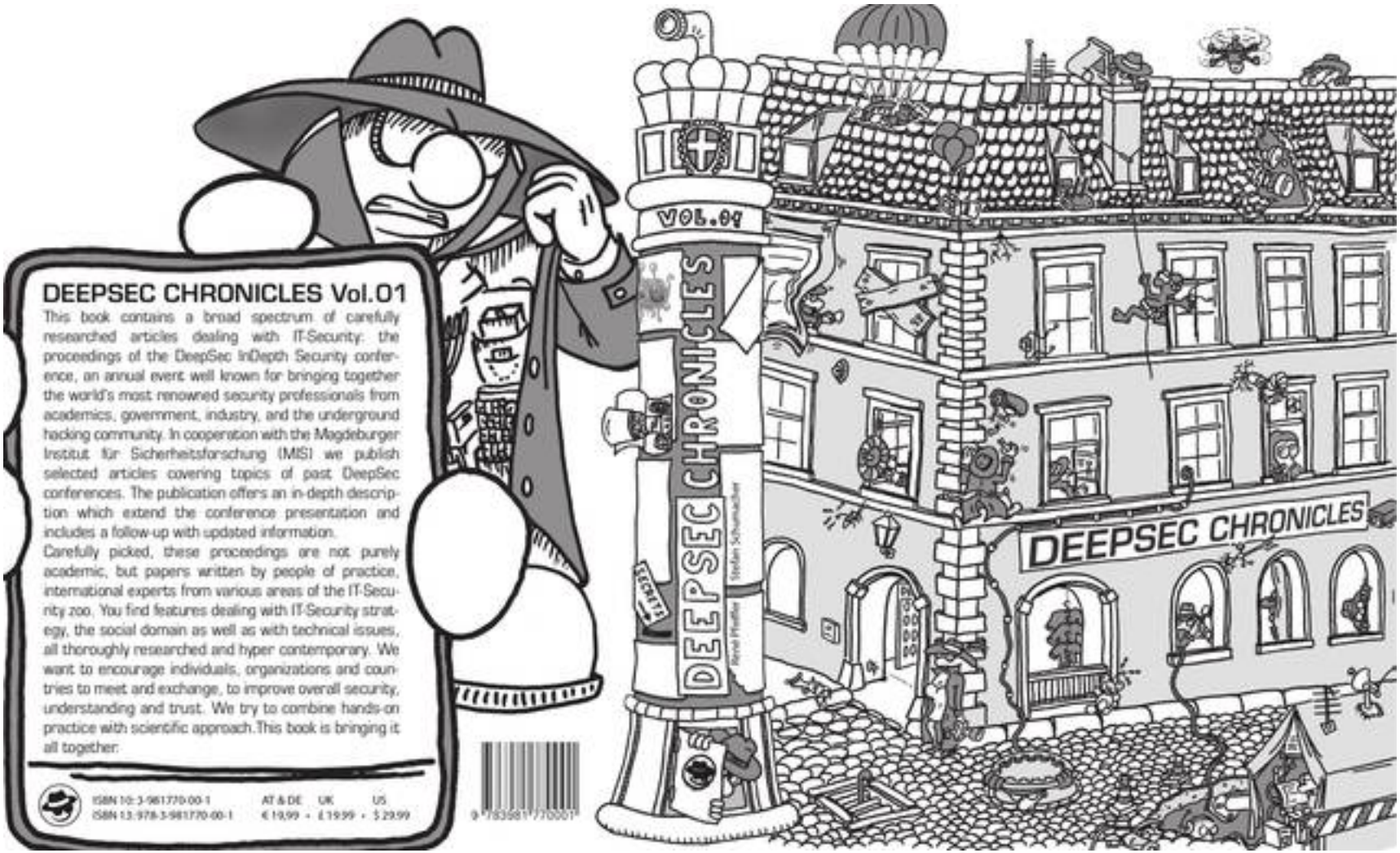


Jahrbuch Terrorismus 2013/2014

Hansen, S. und Krause, J. (Herausgeber)



Stefan Schumacher:
Cyber-Terrorismus:
Reale Bedrohung oder Mythos?
S. 159 – 180


DEEPSEC CHRONICLES Vol.01
This book contains a broad spectrum of carefully researched articles dealing with IT-Security: the proceedings of the DeepSec InDepth Security conference, an annual event well known for bringing together the world's most renowned security professionals from academics, government, industry, and the underground hacking community. In cooperation with the Magdeburger Institut für Sicherheitsforschung (MIS) we publish selected articles covering topics of past DeepSec conferences. The publication offers an in-depth description which extend the conference presentation and includes a follow-up with updated information.
Carefully picked, these proceedings are not purely academic, but papers written by people of practice, international experts from various areas of the IT-Security zoo. You find features dealing with IT-Security strategy, the social domain as well as with technical issues, all thoroughly researched and hyper contemporary. We want to encourage individuals, organizations and countries to meet and exchange, to improve overall security, understanding and trust. We try to combine hands-on practice with scientific approach. This book is bringing it all together.
ISBN 10: 3-981770-00-1
ISBN 13: 978-3-981770-00-1
AT & DE UK US
€ 19.99 £ 19.99 $ 29.99
Vol.01
DEEPSEC CHRONICLES
DEEPSEC CHRONICLES

- Stefan Schumacher and René Pfeiffer (editors)
- In Depth Security – Proceedings of the DeepSec Conference
- 360 Pages
- Magdeburger Institut für Sicherheitsforschung
- 978-3981770001
- `http://www.amazon.de/Depth-Security-Stefan-Schumacher/dp/3981770005/ref=sr_1_1?ie=UTF8&qid=1448888706`



Teil I

Soziale Netze



Geschichte der Sozialen Netze

- 1981: Usenet beginnt
- Server synchronisieren Text-Dateien im Arpa-Net
- thematische Diskussionsgruppen entstehen (rec.food.equipment, alt.sysadmin.recovery, de.alt.fan.aldi)
- Zugang über Unis, viele technische Listen
- dutzende Server
- Eternal September dank AOL
- Spam und Massenwerbung
- Filterung obszöner Worte (Brust, Brustkrebs)

Mailinglisten

- Leser melden sich auf der Liste an
- Mail an eine spezielle Adresse wird an alle Abonnenten weitergeleitet
- thematische Sortierung
- beliebt bei Entwicklern

BBS/Mailboxen

- entstanden Anfang der 1980er
- PC/Amiga/Atari-Szene
- Server mit Mailbox-Software und Modem
- DFÜ teuer, asynchrones Senden in der Baumstruktur
- geringere Verbreitung in DE dank Deutscher Bundespest

WWW und Internet

- World Wide Web: 1989 am CERN entwickelt
- unidirektionaler Hyperlink eingeführt
- ermöglicht Verlinkung von 2 Seiten
- ursprünglich für wissenschaftliche Artikel gedacht
- 1993: Mosaic Browser
- Mitte 1990er: schnelle Internetzugänge werden verfügbar
- explosionsartiges Wachstum



soziale Netze

- 2003 LinkedIn
- 2003 MySpace
- 2003 Second Life
- 2004 Orkut, Xing, Facebook
- 2005 StudiVZ

Inhaltsverzeichnis

1. Big Brother, Anonymität und Überwachung
2. NSA
3. PIP
4. Manipulation
5. Fazit



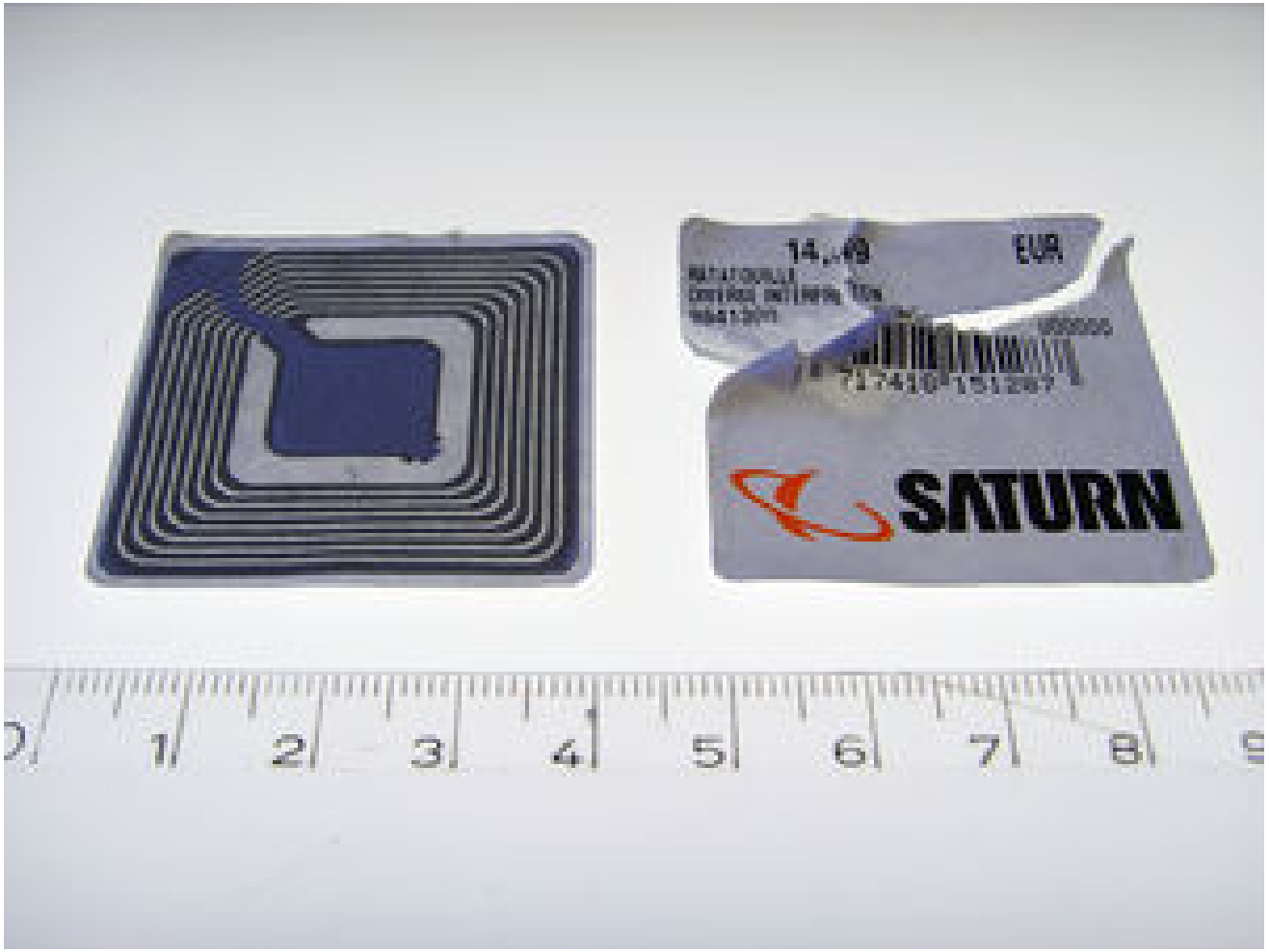
Hintergrund

1. Überwachung, Datenschutz und Anonymität werden stark diskutiert
2. soziale Dienste sammeln soziale Daten
3. Big Brother Awards als Auszeichnung für Datenkraken
4. Debatte schon älter: 12. September 1981 Gründung des Chaos Computer Clubs in Berlin auf Grund der damaligen Volkszählungsdebatte
5. automatisierte Auswertung der Daten durch EDV
6. Rasterfahndung (RAF, 9/11)
7. Echelon (1999 offiziell bestätigt)
8. Snowden: Prism, Tempora

Daten heute

- massive Ausbreitung des Internets in den letzten 20 Jahren
- massive Ausbreitung der IT in viele Lebensbereich (Smart Meter, Smart Home, Iphones, KFZ ...)
- Internet der Dinge dank RFID
- Bewegungsprofile im GSM/GPS
- massive Ausweitung der anfallenden Daten
- Sammlung und Auswertung der Daten um politische und wirtschaftliche Ziele umzusetzen

RFID



Daten - Information - Wissen

- Was ist das: 230580S71323?
- Daten: 27.04.2011, 2011-04-27, 04/27/2011
- Information: Daten müssen gelesen und interpretiert werden
- Computer kann schnell interpretieren, *wenn* ein Interpretationsrahmen vorgegeben ist



Daten - Information - Wissen

- Was ist das: 230580S71323?
- Daten: 27.04.2011, 2011-04-27, 04/27/2011
- Information: Daten müssen gelesen und interpretiert werden
- Computer kann schnell interpretieren, *wenn* ein Interpretationsrahmen vorgegeben ist

Beispiel Rasterfahndung

- Alle muslimischen, männlichen Studenten zwischen 20 und 30 Jahren, die Ingenieur- oder Naturwissenschaften studieren und im letzten Jahr in Afghanistan oder Pakistan waren, sind Terroristen.
- Payback erfasst Einkaufszettel: Gib mir alle schwangeren Frauen/Mütter mit Säuglingen in Magdeburg, die Grüne wählen und in Zahlungsschwierigkeiten sind.
- Facebook: Gib mir alle ungeouteten, latent homosexuellen, konservativen Studenten.



Knowledge Discovery in Databases

- Computer können Rechnen, mehr nicht. Sie sind stumpfsinnig.
- maschinelles Lernen: Generierung von Wissen aus Erfahrung, erkennt Gesetzmäßigkeiten in den Lerndaten (Handschriftenerkennung, Bilderkennung)
- Data Mining: neue Muster in großem Datenbestand erkennen (Rasterfahndung, Fraud Detection)
- Online Analytical Processing: Hypothesen als Anfragen (Business Intelligence)
- Hardware und Software wird besser und billiger



Problematisch: IP-Adresse

- IP-Adresse: »Hausnummer des Rechners« im Internet
- z.B. 141.44.1.1; 192.168.1.1, 127.0.0.1, www.Kaishakunin.com
- identifiziert ein Gerät im Internet, wird **immer** übertragen
- ISP (T-Online, Alice, AOL, Kabel Deutschland) kann die IP einer Person (Vertragspartner) zuordnen $\rightsquigarrow$ Identifizierbarkeit
- IP taucht auf in jeder E-Mail, in Weblogs, FTP-Logs etc.pp.
- Gateways und Proxies (VPN-Client, anyone)
- Protokollierung und Zusammenführung $\rightsquigarrow$ Profil
- Probleme: IP-NAT, UMTS, Gerichtsverwertbarkeit



Problematisch: Einbettung in HTML (Web-Bug)

- Teile einer Webseite können auf anderen Servern liegen
- die können mitloggen
- Bilder in E-Mails (öffnen reicht)
- IDs in Spam-URLs (böse-domain.de/newsletter-abbestellen.php?id=0xDEADBEEF)



Problematisch: Sessions und Cookies

- HTML ist Zustandslos
- Sessions oder Cookies
- RFC 2109 und RFC 2965
- Cookies sind kleine Textdateien, die den Nutzer identifizierbar machen können
- viele Webseiten gehen nicht mehr ohne
- Beim Browser beenden löschen



Problematisch: Zusammenführung

- Zusammenführung der Daten: Facebook + Payback + Amazon + GSM + Ebay
- Personalisierung der Daten, d.h. Zuordnung auf eine Person
- Daten werden verkauft
- validierte E-Mail-Adresse von Wissenschaftlern: 1-2$, Datensätze von Patienten bis zu 5.000$
- Ziehen von (falschen) Schlüssen
- Identitätsdiebstahl (vorrangig in den USA dank SSN)
- Umgehung nationaler Gesetze durch Kooperationen (NSA-UK, GCHQ-USA)

Bsp: Facebook

- Facebook hat Zugriff auf *alle* Daten in Facebook
- Facebook hat Zugriff auf Daten *außerhalb* von Facebook
- Facebook dataminet die Daten und verkauft die Ergebnisse
- Konzerne personalisieren Werbung
- Wenn etwas umsonst ist, dann sind die Nutzer das Produkt!

Bsp: Facebook

- Facebook hat Zugriff auf *alle* Daten in Facebook
- Facebook hat Zugriff auf Daten *außerhalb* von Facebook
- Facebook dataminet die Daten und verkauft die Ergebnisse
- Konzerne personalisieren Werbung
- Wenn etwas umsonst ist, dann sind die Nutzer das Produkt!



Inhaltsverzeichnis

1. Big Brother, Anonymität und Überwachung
2. NSA
3. PIP
4. Manipulation
5. Fazit



Was ist die NSA

- No Such Agency National Security Agency
- Vorläufer im 2. WK, vgl. Bletcheley Park
- 1952: Gründung der NSA
- Auftrag: Abhören ausländischer Nachrichtenverbindungen
- 2012: 40.000 Mitarbeiter, 10 Milliarden $, 409 GWh/a 409.000.000 KWh, Stadtverwaltung Münster: 40.000.000 KWh
- Kooperationen mit UK, Kanada, Australien, Niederlande seit 2.WK

Was ist die NSA

- No Such Agency National Security Agency
- Vorläufer im 2. WK, vgl. Bletcheley Park
- 1952: Gründung der NSA
- Auftrag: Abhören ausländischer Nachrichtenverbindungen
- 2012: 40.000 Mitarbeiter, 10 Milliarden $, 409 GWh/a 409.000.000 KWh, Stadtverwaltung Münster: 40.000.000 KWh
- Kooperationen mit UK, Kanada, Australien, Niederlande seit 2.WK

Auftrag

- Kommunikation mitschneiden
- speichern
- ggf. entschlüsseln
- automatisiert analysieren
- ggf. menschlich analysieren

Fähigkeiten

- Überwachung aller elektronischer Kommunikation in den USA
- Überwachung nahezu aller elektronischer Kommunikation außerhalb der USA
- E-Mail, Web, Usenet, FTP, Fax, Telefon, GSM, Satellitentelefon, Glasfaserkabel, Kupferkabel ...
- DE-CIX: 500 Organisationen, 2,4 TBit/s
- Spracherkennung und Umwandlung (Telefonat in Text, vgl. Siri)
- Suche nach Schlagwörtern und Semantik
- Handy: Anzapfen, als Wanze aktivieren, Orten, Bewegungsprofile
- Kernaufgabe: Zusammenführen der Daten

USS Jimmy Carter (SSN-23)

- Seawolf-Klasse Atom-Uboot
- Ausgerüstet um Unterseekabel anzuzapfen
- Daten werden gespeichert oder direkt an Bord analysiert
- bis zu 50 Mission Specialists an Bord
- `http://www.submarinecablemap.com/`

Datensammlung und -auswertung

- Data Warehousing (Wirtschaftsinformatik, SAP anyone?)
- riesige Datenbanken
- durchsuchen und analysieren der Datenbanken
- automatisierte Systeme
- Maschinelles Lernen
- Knowledge Discovery in Databases

Datensammlung und -auswertung

- gib mir alle Kontakte
- gib mir alle Kontakte der Kontakte



Datensammlung und -auswertung

- gib mir alle Kontakte
- gib mir alle Kontakte der Kontakte
- gib mir alle Kontakte der Kontakte der Kontakte



Datensammlung und -auswertung

- gib mir alle Kontakte
- gib mir alle Kontakte der Kontakte
- gib mir alle Kontakte der Kontakte der Kontakte
- gib mir alle E-Mails der Kontakte der Kontakte der Kontakte

Datensammlung und -auswertung

- gib mir alle Kontakte
- gib mir alle Kontakte der Kontakte
- gib mir alle Kontakte der Kontakte der Kontakte
- gib mir alle E-Mails der Kontakte der Kontakte der Kontakte
- gib mir alle E-Mails der Kontakte der Kontakte der Kontakte die Dihydrogenmonoxid enthalten und kleiner als 5kb sind

Datensammlung und -auswertung

- gib mir alle Kontakte
- gib mir alle Kontakte der Kontakte
- gib mir alle Kontakte der Kontakte der Kontakte
- gib mir alle E-Mails der Kontakte der Kontakte der Kontakte
- gib mir alle E-Mails der Kontakte der Kontakte der Kontakte die Dihydrogenmonoxid enthalten und kleiner als 5kb sind
- gib mir alle Handies die am 24.12. in der selben Funkzelle waren

Datensammlung und -auswertung

- gib mir alle Kontakte
- gib mir alle Kontakte der Kontakte
- gib mir alle Kontakte der Kontakte der Kontakte
- gib mir alle E-Mails der Kontakte der Kontakte der Kontakte
- gib mir alle E-Mails der Kontakte der Kontakte der Kontakte die Dihydrogenmonoxid enthalten und kleiner als 5kb sind
- gib mir alle Handies die am 24.12. in der selben Funkzelle waren
- gib mir alle Handynummern aller E-Mailkontakte

Datensammlung und -auswertung

- gib mir alle Kontakte
- gib mir alle Kontakte der Kontakte
- gib mir alle Kontakte der Kontakte der Kontakte
- gib mir alle E-Mails der Kontakte der Kontakte der Kontakte
- gib mir alle E-Mails der Kontakte der Kontakte der Kontakte die Dihydrogenmonoxid enthalten und kleiner als 5kb sind
- gib mir alle Handies die am 24.12. in der selben Funkzelle waren
- gib mir alle Handynummern aller E-Mailkontakte
- gib mir alle schwangeren Single-Frauen aus Hamburg die FDP wählen und Coldplay mögen sowie eine Katze haben

Datensammlung und -auswertung

- gib mir alle Kontakte
- gib mir alle Kontakte der Kontakte
- gib mir alle Kontakte der Kontakte der Kontakte
- gib mir alle E-Mails der Kontakte der Kontakte der Kontakte
- gib mir alle E-Mails der Kontakte der Kontakte der Kontakte die Dihydrogenmonoxid enthalten und kleiner als 5kb sind
- gib mir alle Handies die am 24.12. in der selben Funkzelle waren
- gib mir alle Handynummern aller E-Mailkontakte
- gib mir alle schwangeren Single-Frauen aus Hamburg die FDP wählen und Coldplay mögen sowie eine Katze haben

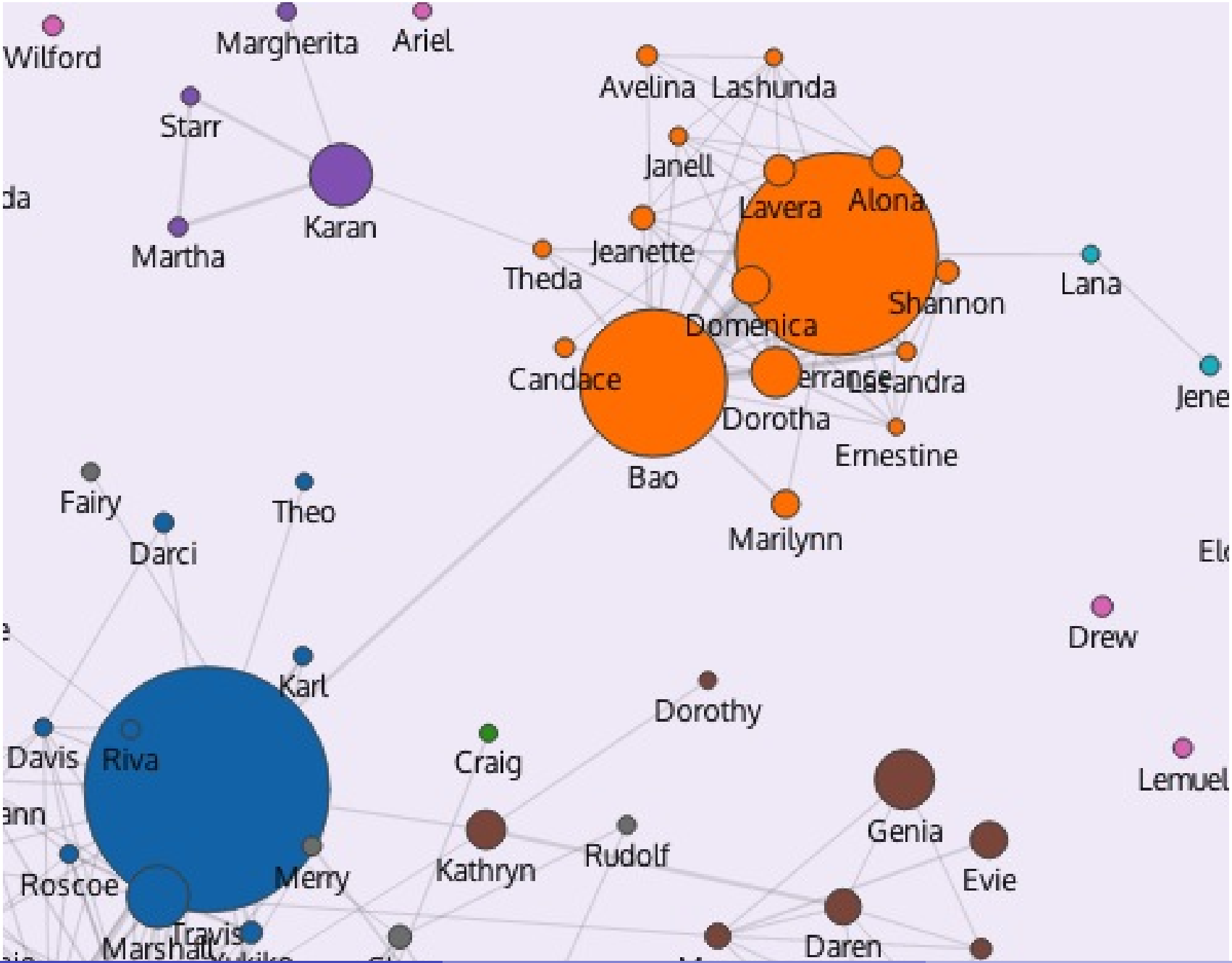
Bewegungsprofil Malte Spitz



Bewegungsprofil Malte Spitz



Kommunikationsnetz TechCrunch



Aufklärung

- großflächige Überwachung sozialer Netzwerke
- Erkennung von sich entwickelnden Revolutionen
- Kommunikationsaufkommen steigt massiv an
- Metadaten zur Analyse der Situation
- Braut sich was zusammen?



Daten verschneiden

- Kommunikationsdaten (Wer mailt/telefoniert mit wem?)
- Bewegungsdaten Handy
- Bewegungsdaten Bahn, Flugverkehr
- Zahlungsverkehr (SWIFT)
- gezielte Angriffe (Trojaner, etc.)
- Kombination zum Lagebild

Gefecht der verbundenen Waffen

Bestandteile

- Feuer
- Bewegung
- Sperren
- Elektronischer Kampf
- Kräfte
- Raum
- Zeit
- Information

Network Centric Warfare

- Entscheidungsunterstützungsysteme: Für operative und strategische Aufgaben relevante Informationen ermitteln, aufbereiten, übersichtlich zusammenstellen und bei der Auswertung helfen. Dazu gehören Funktionen zur Sortierung und Filterung von Daten, ihre flexible Darstellung sowie Auswertungsmöglichkeiten wie Summen oder Durchschnittsberechnungen, Vergleiche etc. Weiter gehende Funktionen erlauben die Ausführung von Modellrechnungen (Szenarien, Prognosen) und die Verknüpfung der Daten mit Optimierungsalgorithmen.
- NWC: Erhebung aller möglichen Daten und deren automatisierte Auswertung

Targeted Killings

- Ermordung von Personen aufgrund der Überwachungsergebnisse
- Tracking und Targeting über Datenbanken
- Daten an Drohnen oder Satelliten verfüttern
- Predator o.ä. für gezielte Schläge einsetzen
- Spezialeinheiten einschleusen für gezielt Mordaktionen



Inhaltsverzeichnis

1. Big Brother, Anonymität und Überwachung
2. NSA
3. PIP
4. Manipulation
5. Fazit



Kooperationen

- NSA kooperiert mit anderen Geheimdiensten
- u.a. BND
- BND führt in HUMINT im arabischen Raum
- BND darf keine Daten von Deutschen analysieren, außer G10-Kommision stimmt zu.
- Was wissen die schon?
- BND nutzt NSA-Software
- siehe auch: Gladio, Daniele Ganser

PIP

- In-Q-Tel - Joint Venture Capital Firm der CIA
- VC für HiTech-Firmen, Silicon Valley
- 2005: In-Q-Tel verkauft 5.636 Google Aktien
- Swap für Keyhole jetzt bekannt als Google Earth
- Silicon Valley geht stark auf die NSA, CIA zurück
- Enge verquickung von Wirtschaft und Geheimdiensten
- gezielte Angriffe auf Enercon 1998



PIP

- In-Q-Tel - Joint Venture Capital Firm der CIA
- VC für HiTech-Firmen, Silicon Valley
- 2005: In-Q-Tel verkauft 5.636 Google Aktien
- Swap für Keyhole jetzt bekannt als Google Earth
- Silicon Valley geht stark auf die NSA, CIA zurück
- Enge verquickung von Wirtschaft und Geheimdiensten
- gezielte Angriffe auf Enercon 1998

Angriffe auf Kryptographie

- verschlüsselte Daten werden gespeichert und ggf. später angegriffen
- Angriffe auf kryptographische Implementierungen (Intel PRNG)
- Angriffe auf Lavabit: Herausgabe der privaten SSL-Schlüssel
- Gegenmaßnahme: Ende-zu-Ende-Verschlüsselung (GnuPG etc.)

Inhaltsverzeichnis

1. Big Brother, Anonymität und Überwachung
2. NSA
3. PIP
4. Manipulation
5. Fazit



Shills

- Marketingunternehmen spezialisiert auf Soziale Medien
- Bots – Computerprogramme liken automatisch
- Likes werden gehandelt
- Filterbubble und Algorithmen

Inhaltsverzeichnis

1. Big Brother, Anonymität und Überwachung
2. NSA
3. PIP
4. Manipulation
5. Fazit



Werbung?

- bleibt es bei der Werbung?
- Was ist mit Krankenkassen und Lebensversicherungen? Payback sortiert alle raus die rauchen oder zuviel trinken? Facebook alle Homosexuellen wegen HIV?
- Fehlschlüsse? Wer ist Stefan E. Schumacher? Stefan A. Schumacher?
- Welche Daten sind überhaupt korrekt? (Verleumdung, Mobbying)

Daten kontrollieren

- angefallene Daten lassen sich nicht kontrollieren oder sicher löschen
- wir liefern unsere Daten freiwillig ab (Facebook)
- wir liefern unsere Daten freiwillig aus (Apple, Google, DRM)

Gegenmaßnahmen

- Kryptographie nutzen
- SSL/TLS: https://www
- E-Mails verschlüsseln
- Anonymisierungsdienste wie Tor nutzen
- starke Passwörter ausdenken



- sicherheitsforschung-magdeburg.de
- stefan.schumacher@sicherheitsforschung-magdeburg.de
- sicherheitsforschung-magdeburg.de/publikationen/journal.html



- youtube.de/Sicherheitsforschung
- Twitter: 0xKaishakunin
- Xing: Stefan Schumacher
- ZRTP: 0xKaishakunin@ostel.co