Drogenkartelle in Lateinamerika

Anonymous vs. Los Zetas

Stefan Schumacher

sicherheitsforschung-magdeburg.de

14.08.2015



Über Mich



Über Mich

- Geek, Nerd, Hacker seit mehr als 20 Jahren
- Berater für Finanzinstitute, Regierungen, Sicherheitsbehörden
- Direktor des Magdeburger Instituts für Sicherheitsforschung
  Forschungsprogramme zur Unternehmenssicherheit
- Herausgeber des Magdeburger Journals zur Sicherheitsforschung
- `www.Sicherheitsforschung-Magdeburg.de`



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



Informationstechnologie und Sicherheitspolitik

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



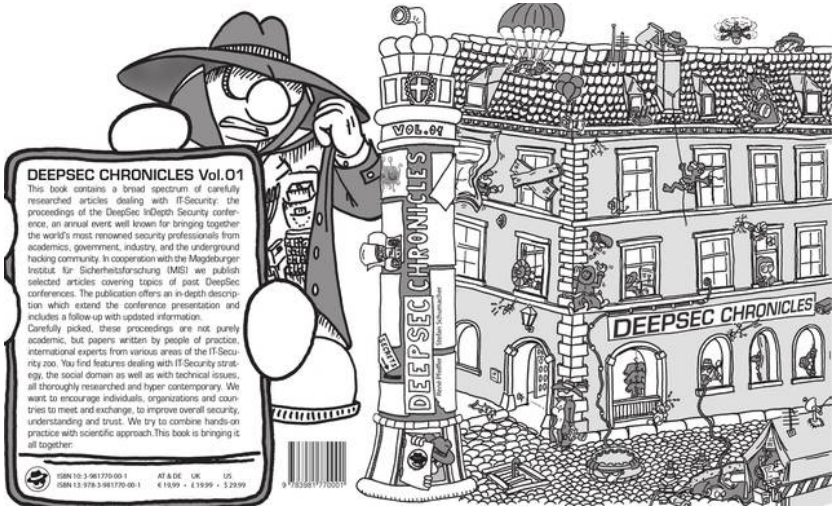
sicherheitsforschung-magdeburg.de/buecher.html

Jahrbuch Terrorismus 2013/2014

Hansen, S. und Krause, J. (Herausgeber, Institut für Sicherheitspolitik Kiel)



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 € 19,99 + UK £ 19.99 + US $ 29.99
9 783981 770001
Vol.01
DEEPSEC CHRONICLES
Stefan Schumacher
Bernd Fix
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`



Inhaltsverzeichnis

1 Drogenkartelle

2 Überwachung online

3 Darknet

4 Anonymisierung



War on Drugs

- 1972 von Richard Nixon geprägt
- 1973 Gründung der Drug Enforcement Administration (DEA)
- aggressive Anti-Drogenpolitik
- privatisiertes Gefängnissystem
- Polizeierfolg über Verhaftungen gemessen
- massive Inhaftierung von Schwarzen und Latinos, obwohl Drogen in allen Schichten gleich verteilt sind
- Verteilung von Drogen durch FBI an Bürgerrechtler währen COINTELPRO



War of Drugs

- Air America: CIA geführte Fluggesellschaft für verdeckte Operationen
- verdeckte Operationen in Indochina, Burma, Kambodscha, Thailand und Laos
- transportierten Opium und Heroin für Hmong
- finanzierten Ausrüstung und Waffen durch Drogenhandel



War of Drugs

- Iran Contra: Illegale Waffenverkäufe an den Iran (TOW und HAWK)
- Gewinne weitergeleitet an rechte Rebellen in Nicaragua (Contras)
- Contras schmuggelten jahrelang Kokain in die USA
- mit Wissen und eventuell Unterstützung durch die CIA
- teilweise mehr als die Hälfte des gesamten Kokains in den USA
- Crack-Welle in den 1980ern



Kartelle

- Medellín-Kartell (Kolumbien, nebeneinander unabhängiger Gruppen)
- Cali-Kartell (Kolumbien, nebeneinander unabhängiger Gruppen)
- Golf-Kartell (Mexiko, straff organisiert, absteigende Macht)
- Mara (Jugendbanden in El Salvador, Guatemala und Honduras)



Kartelle

- La Familia (Mexiko, abgespalten von Golf, inzwischen zerschlagen)
- Los Caballeros Templarios (Mexiko, Kämpfer für soziale Gerechtigkeit)
- Sinaloa-Kartell (Mexiko, gilt als mächtigstes Kartell weltweit)
- Los Zetas (Mexiko, gegründet von Elite-Soldaten und Polizisten, extrem gewalttätig, technisch sehr fortschrittlich)
- extreme Korruption in Polizeien, Staatsanwaltschaften, Politik, Militär



Technik

- Cali-Kartell ließ alle Telefonate von/nach Bogotá bis 1995 aufzeichnen
- israelische Technologie für abhörsichere Telefonate beschafft
- verschlüsselte Dateien auf Laptops, die nicht entschlüsselt werden konnten



Internet

- Propagandaplattform
- Facebook-Gruppen, Blogs, Webseiten
- Videos von Enthauptungen mit Äxten, Kettensägen, Messern, Hämmern (Los Zetas)
- Narco-Blogs: outet Kartellmitglieder (vertrauenswürdig?)
- False Flags im Krieg der Kartelle
- Blogger ermordert



Mobilfunk

- Los Zetas bauen eigenes Mobilfunknetzwerk auf
- mit sicherer Verschlüsselung
- Führungsebene nutzt verschlüsselte Internetkommunikation
- Mobilfunknetzwerk für Wachposten, Strassendealer und andere
- 167 Funkantennen und ein 90m Sendemast in Veracruz gefunden
- von 2008-2012 mindestens 36 Techniker entführt



Anonymous



Anonymous



Anonymous

- Hervorgegangen als Protest gegen Scientology in den USA
- Anonymisierung mit Guy-Fawkes-Masken (V wie Vendetta) zum Schutz vor Klagen
- Operation: Payback u.a. Angriffe auf Finanzdienstleister und Spiegelung der Cables
- keine Hierarchie, sondern Heterarchie
- Virtuelle Organisation
- jeder kann das Label Anonymous verwenden
- Radikalisierung im 4chan um Wikileaks,
- Organisation via IRC oder Webforen



Anonymous

- eine (oder mehrere Ideen), keine formale Struktur (e.V. o.ä.)
- schwer angreifbar, kaum ausschaltbar (vgl. Al-Kaida)
- entstehen spontan u.a. in Weißrussland, Ukraine, Russland, Ägypten, Syrien (Übernahme eines GSM Rechenzentrum)
- starke Diskussion auch in der Hacker-Szene über das Vorgehen



Anonymous vs. Los Zetas

- Proteste gegen Los Zetas in Veracruz
- angeblich 4 Anonymous Aktivisten entführt
- Anonymous droht mit der Veröffentlichung von Los Zetas Daten
- Los Zetas lassen entführte Aktivisten frei



Inhaltsverzeichnis

1 Drogenkartelle

2 Überwachung online

3 Darknet

4 Anonymisierung



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



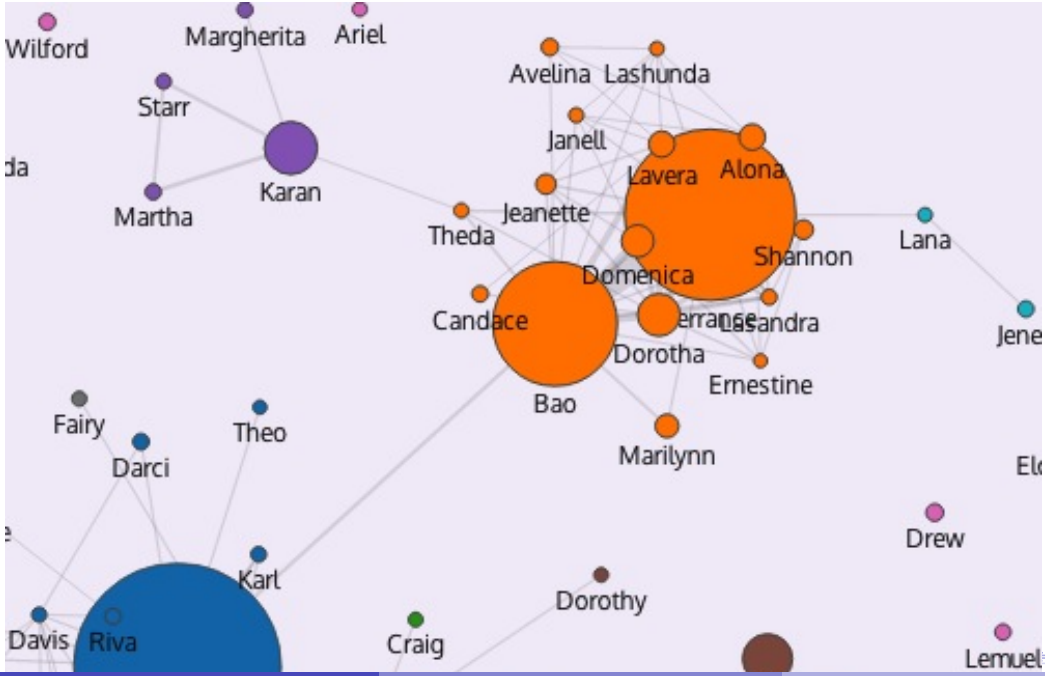
Bewegungsprofil Malte Spitz



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



Inhaltsverzeichnis

1 Drogenkartelle

2 Überwachung online

3 Darknet

4 Anonymisierung



Darknet

- Teile des Internets die nicht indiziert sind
- erste Indizierung durch Webkataloge mit Redakteuren
- 1995 AltaVista als Forschungsprojekt der DEC
- 1996 HotBot von Inktomi
- 1996/1998 Google
- agentenbasierte Indizierung – keine Redakteure mehr

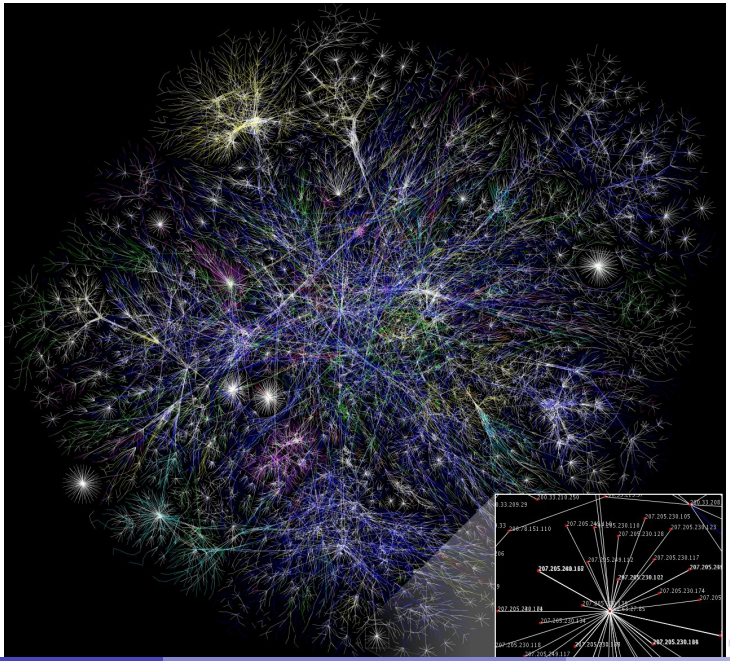


Suchmaschine

- finden nur Seiten die verlinkt werden
- Milliarden Seiten auf die nicht gelinkt wird
- nicht verlinkte Seiten werden nicht gefunden
- nicht indiziert
- `www.universitaet.de/~nutzerna`
- Seiten mit Bot-Verbot
- Seiten mit Passwörtern
- DeepWeb



Internet Map 2005



Inhaltsverzeichnis

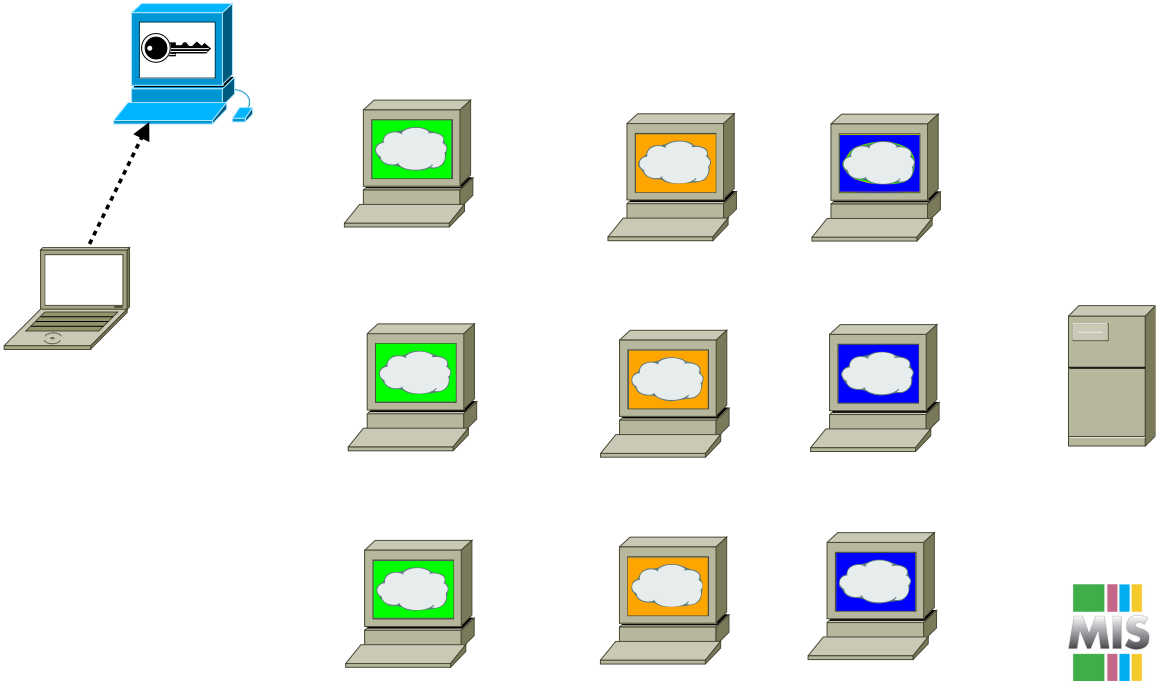
1. Drogenkartelle
2. Überwachung online
3. Darknet
4. Anonymisierung

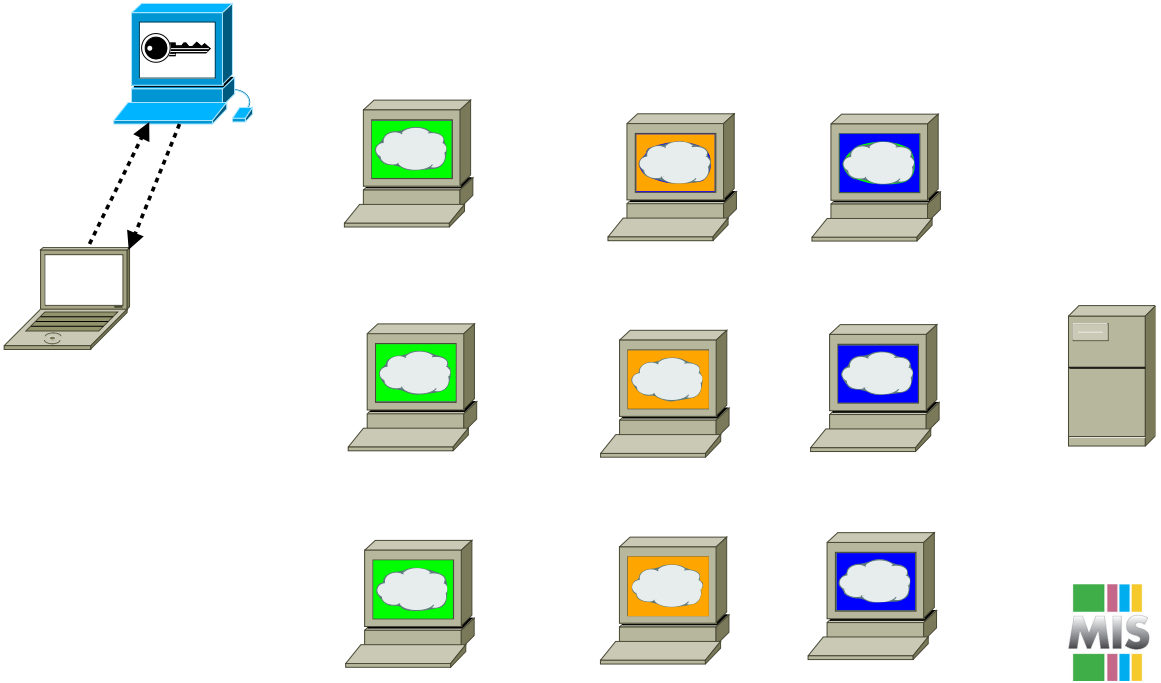


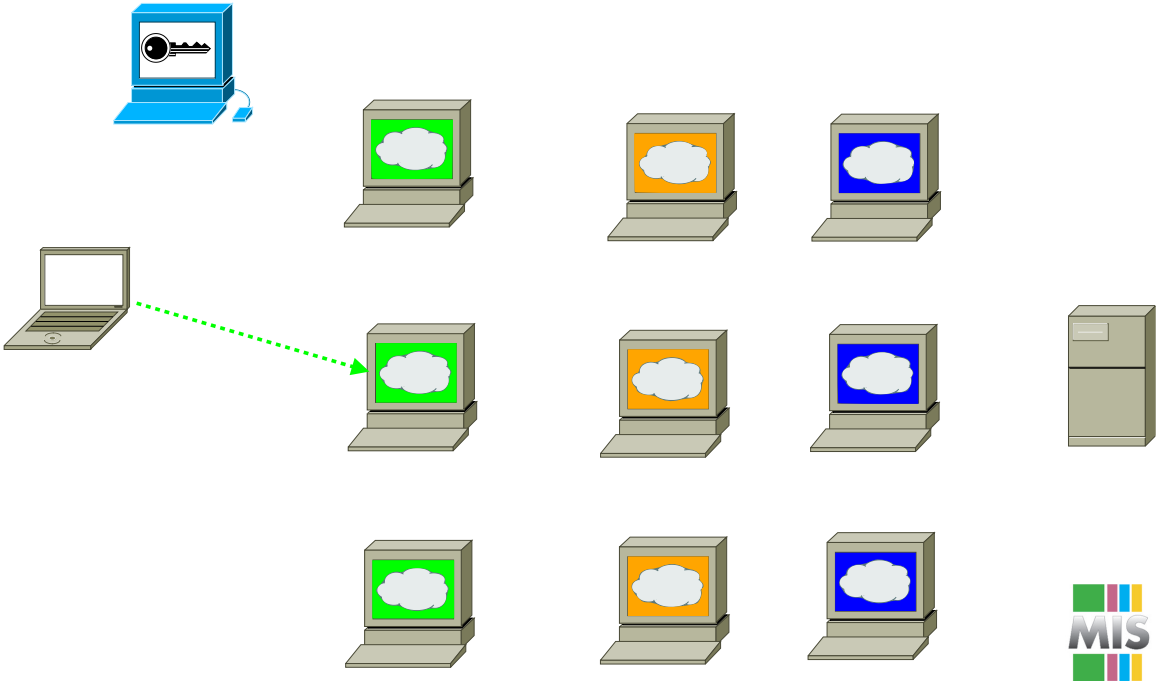
TOR

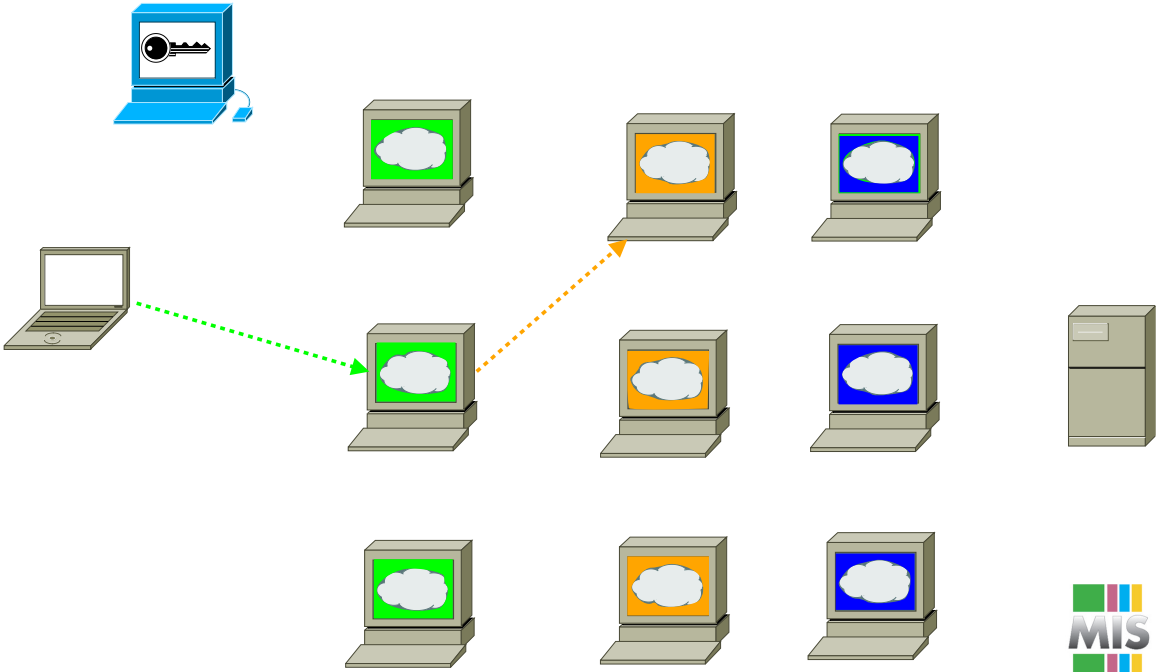
- Netzwerkverkehr wird großräumig überwacht
- Identifizierung über IP-Adresse und Nutzernamen möglich
- Anonymisierung durch Verschlüsselung und durchleiten durch mehrere Proxies (Kaskade)
- Zwiebelprinzip $\rightsquigarrow$ The Onion Router $\rightsquigarrow$ TOR
- Alle Verbindungen innerhalb TORs sind verschlüsselt
- Anonymisierter Zugriff auf Webseiten u.ä.

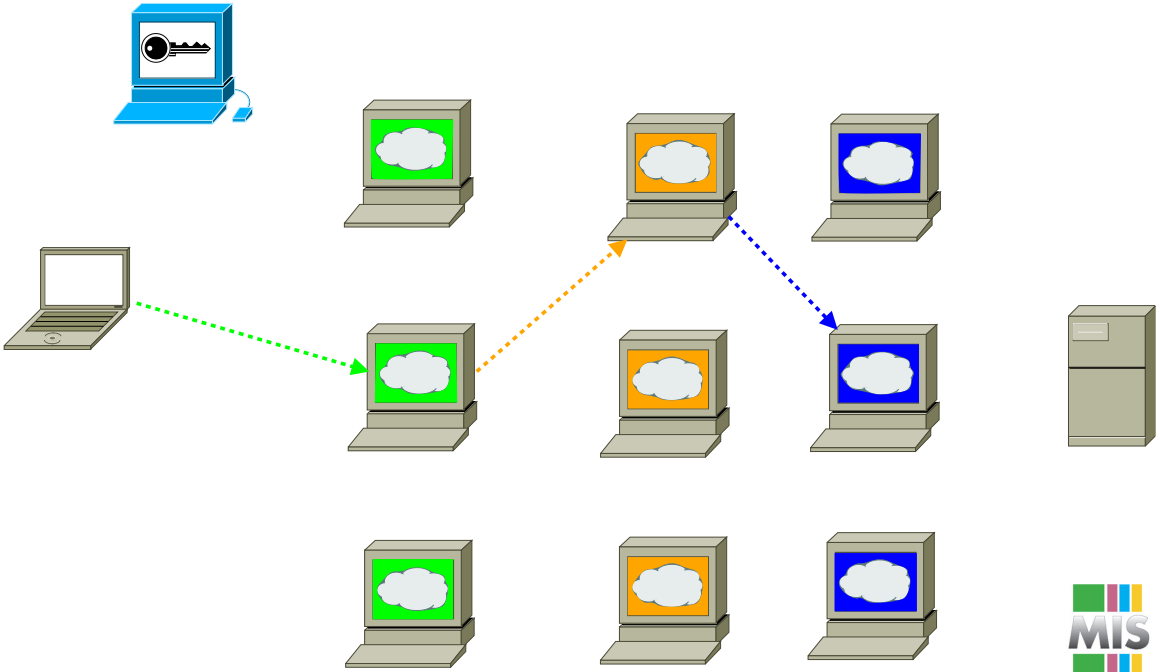


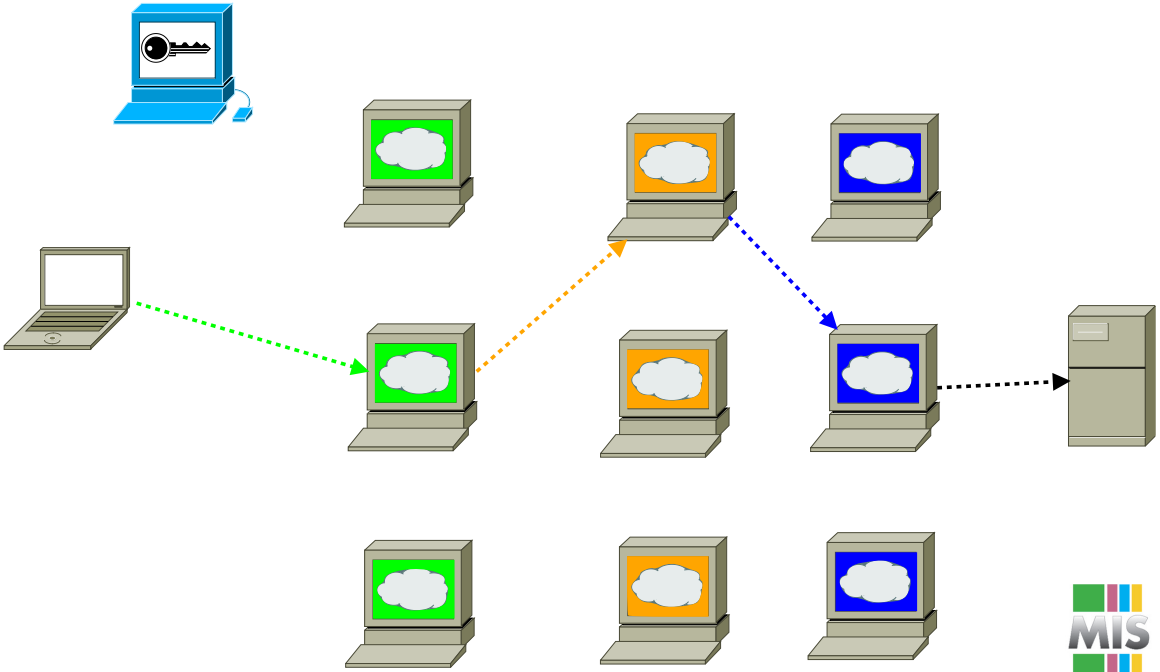


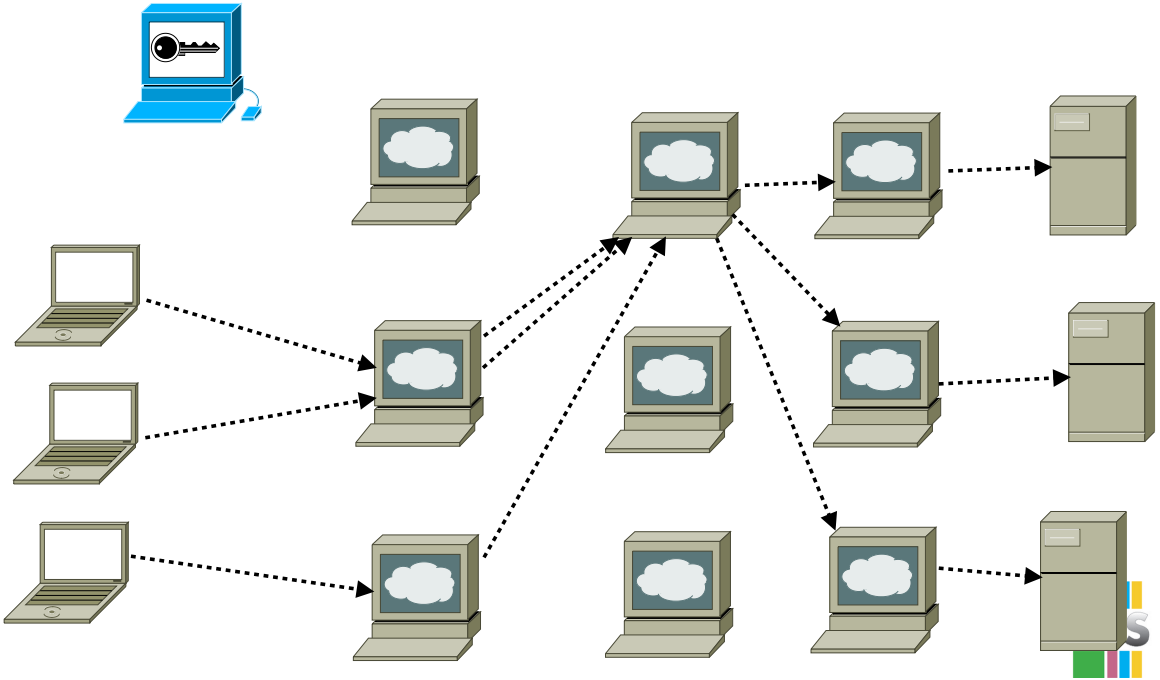








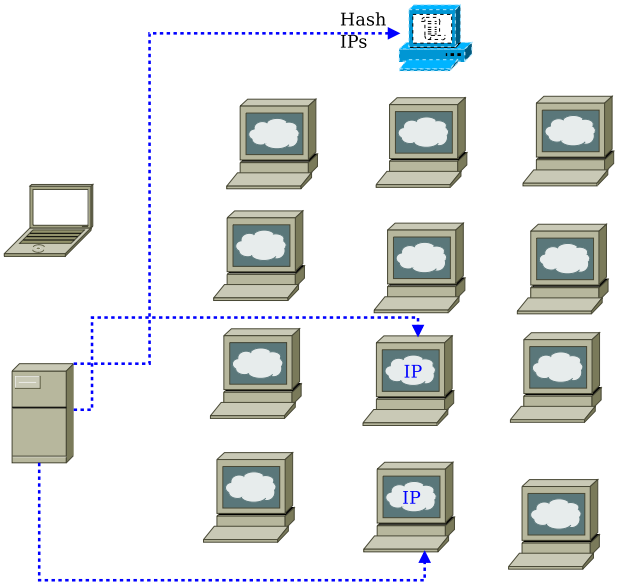


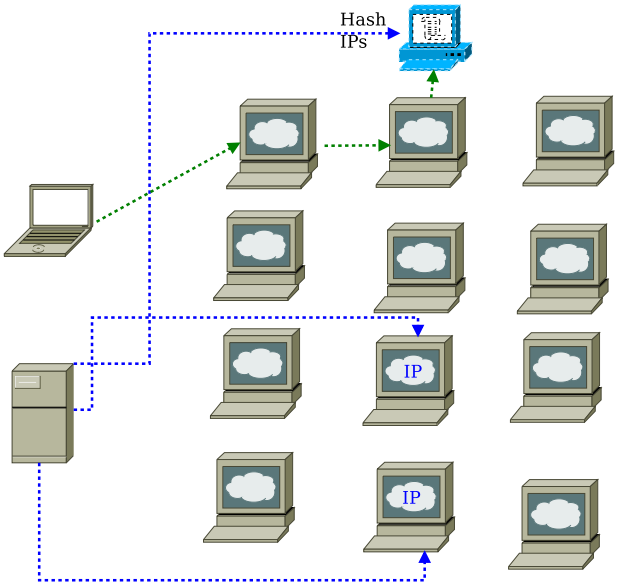


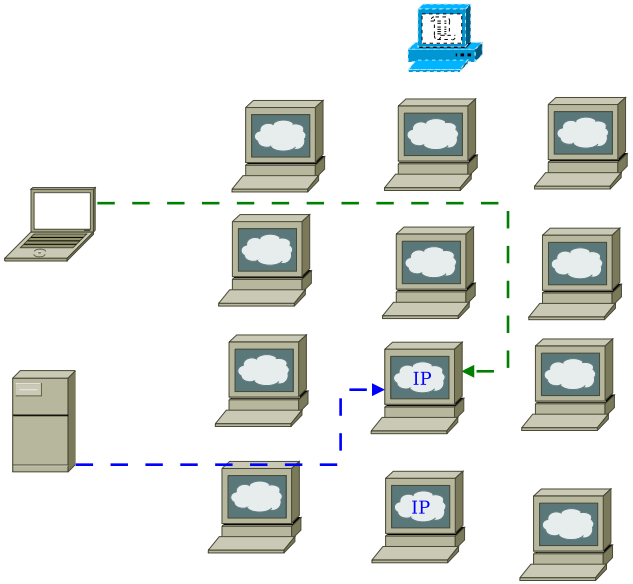
Tor Network

- Nur der Benutzer wird anonymisiert
- Zugriff erfolgt auf normale Webseiten im WWW
- Webserver nicht anonymisiert
- Hidden Services: anonymisiert Benutzer und Webserver
- beide Verbindungen durch Tor-Netzwerk geroutet




Hash
IPs
IP
IP


Hash
IPs
IP
IP


IP
IP

Tor

- Tor und Hidden Services sehr sicher
- Fehlkonfigurationen und gezielte Angriffe
- Logistik: Transport bzw. Übergabe von Waffen, Drogen etc.
- Versand in DE z.B. über gehackte Packstation-Daten
- Bezahlung über Bitcoins



- sicherheitsforschung-magdeburg.de
- sicherheitsforschung-magdeburg.de/publikationen/journal.html
- stefan.schumacher@sicherheitsforschung-magdeburg.de
- 9475 1687 4218 026F 6ACF 89EE 8B63 6058 D015 B8EF



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