Cybergeopolitik?

Das Internet als Staat?

Stefan Schumacher

PB Helmstedt
03.02.2017



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

- Pen-Testing (White Box/Black Box)
- 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

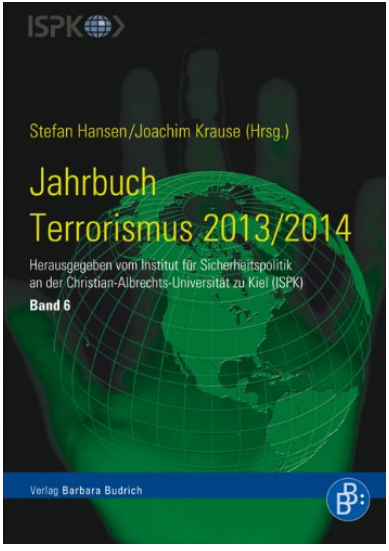
Sambleben, J. und Schumacher, S. (Herausgeber)



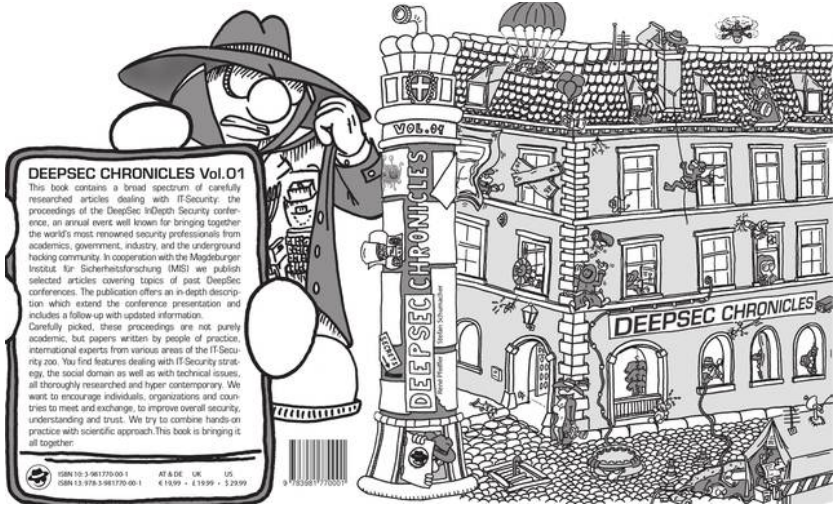
Sambleben, J. und Schumacher, S. (Herausgeber). (2012).
Informationstechnologie und Sicherheitspolitik:
Wird der dritte Weltkrieg im Internet ausgetragen?
Norderstedt: BoD, ISBN 9783848232703

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
Arnd Weber
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`



1 Staatentheorie

2 Sealand

3 Cyberspace

4 Cyber-Geo-Politik?



Völkerrechtssubjekt

- Rechtssubjekt im Völkerrecht
- Träger völkerrechtlicher Rechte und Pflichten
- überstaatliche, auch aus Prinzipien und Regeln bestehende Rechtsordnung
- Fehlen eines zentralen Gesetzgebungsorgans, einer umfassenden, hierarchisch strukturierten Gerichtsbarkeit und einer allzeit verfügbaren Exekutivgewalt zur gleichförmigen Durchsetzung völkerrechtlicher Grundsätze
- Friedensvölkerrecht und Kriegsvölkerrecht



Völkerrechtssubjekt

- originäre Völkerrechtssubjekte und derivative Völkerrechtssubjekte
- originäre staatliche Völkerrechtssubjekte: Staaten
- originäre nichtstaatliche Völkerrechtssubjekte: Internationales Komitee vom Roten Kreuz, Heiliger Stuhl und Souveräner Malteser-Ritterorden
- derivative Völkerrechtssubjekte: abgeleitet aus der Völkerrechtsfähigkeit ihrer Subjekte, internationale Organisationen wie EU und VN



Staat

- Im Staatsrecht existiert keine allgemein gültige Definition des Begriffs Staat
- Georg Jellinek: Drei-Elemente-Lehre
- Der Staat ist ein soziales Gebilde, dessen konstituierende Merkmale ein von Grenzen umgebenes Territorium (Staatsgebiet), eine darauf als Kernbevölkerung ansässige Gruppe von Menschen (Staatsvolk) sowie eine auf diesem Gebiet herrschende Staatsgewalt kennzeichnen.



Staat

- 1933: Konvention von Montevideo über Rechte und Pflichten der Staaten
- Seventh International Conference of American States
- regionales Völkervertragsrecht
- *Der Staat als Subjekt des internationalen Rechts sollte folgende Eigenschaften besitzen: (a) eine ständige Bevölkerung; (b) ein definiertes Staatsgebiet; (c) eine Regierung; und (d) die Fähigkeit, in Beziehung mit anderen Staaten zu treten.*
- *Die politische Existenz eines Staates ist unabhängig von seiner Anerkennung durch die anderen Staaten.*
- *Jeder Staat, ob international akzeptiert oder nicht, hat das Recht auf Verteidigung seines Territoriums, politischen Kontakt und innere Sicherheit.*



1 Staatentheorie

2 Sealand

3 Cyberspace

4 Cyber-Geo-Politik?



Principality of Sealand

- Maunsell-Seefestung *HM Fort Roughs* 10Km vor der Küste von Suffolk
- Gebaut im 2.WK als FlAk-Festung, danach verlassen
- Am 2. September 1967 durch Paddy Roy Bates besetzt
- Wollte eigentlich einen Piratensender betreiben
- proklamierte Sealand als eigenständigen Staat
- forderte die Staatengemeinschaft auf, Sealand als Staat anzuerkennen
- Verteidigte die Station juristisch und mit Waffengewalt
- Lehrbuchbeispiel einer Mikronation



Principality of Sealand

- Gerichtsurteile aus USA und DE entschieden dass Sealand nicht die nötigen Voraussetzungen für einen Staat erfüllt
- kein Völkerrechtssubjekt
- 1987 Ausdehnung britischer Gewässer auf eine 12-Meilen-Zone



1 Staatentheorie

2 Sealand

3 Cyberspace

4 Cyber-Geo-Politik?



Cyber War

Etymologie

- Cyber engl. für Kybernetik bzw. Steuerungstechnik
- Cyberspace: William Gibson prägt den Begriff Cyberspace (und Matrix)
- technische und soziale Dimension
- technisch: Hardware und Software, Protokolle und Dienste
- sozial: Kommunikationsplattformen wie Facebook, Second Life, Twitter, Cybermobbing, Ankündigung von Amokläufen (Leaking)



Völkerrecht

- Es gibt keinen internationalen Vertrag der »Cyber-Aggressivität« regelt
- Kriegsvölkerrecht (Humanitäres Völkerrecht) greift
- jus ad bellum: das Recht, in den Kriegszustand einzutreten
- jus in bello: das Recht im Kriege
- Analogiebildung: Rotes Kreuz, Waffenstillstand, Non-Kombatanten ...
- Gegenwärtig werden Cyber-Attacken *nicht* als kriegerischer Akt betrachtet
- Kriegerische Akte müssen von einem Staat (einer staatlichen Organisation) ausgehen
- Urheberschaft von Attacken *sehr* schwer festzustellen



Nonproliferation/Nichtverbreitung

- Nonproliferation von Cyber-»Waffen« ist in Diskussion
- Internationale Verträge notwendig
- Beispiel: Atomwaffensperrvertrag, Antarktisvertrag, §202c StGB
- Es ist ein technisches Problem
- Wie will man die Ausbreitung von »Wissen« kontrollieren?
- Was ist eine Cyberwaffe? Virenscanner? Kryptographie?
- Wie will man den Schmuggel von Micro-SD-Karten (11x15x0,7mm) unterbinden?
- Oder gar Netzwerkverkehr?



Verträge

Definition (Thomas Hobbes – Philosophie der Neuzeit)

Und Verträge sind ohne das Schwert leere Worte und vermögen in keiner Weise dem Menschen Sicherheit zu geben.

Wer soll welches Schwert wohin führen?



Cyberwar ./. Cybercrime

- juristische Definitionen von Cyberwar und Cybercrime sind notwendig
- ein internationaler Cybercrime-Vertrag ist notwendig
- eine internationale Cybercrime-Agentur auch
- Cybercrime ist gegenwärtig gefährlicher als Cyberwar (vgl. Iftach Amit: Cybercrime-Cyberwar)
- Cybercrime-Banden sind sehr kompetent, recht gut organisiert (ex-KGB)
- können zu »Söldnern« werden (Estland, Georgien)

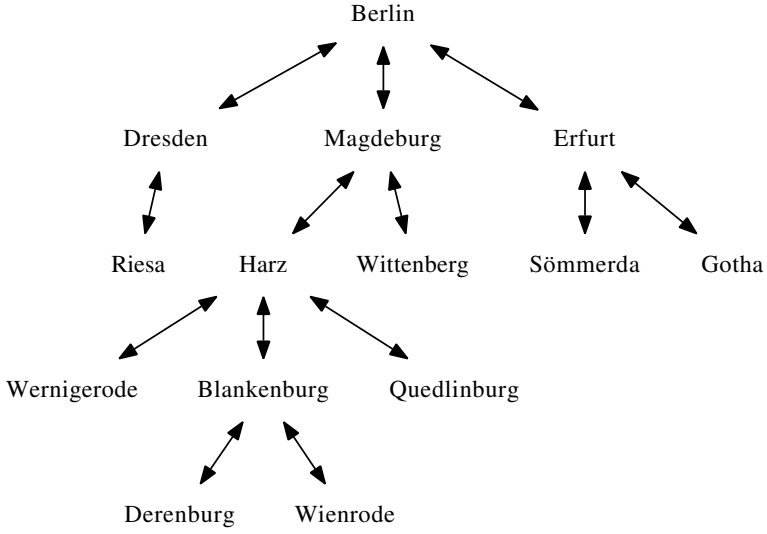


Routing

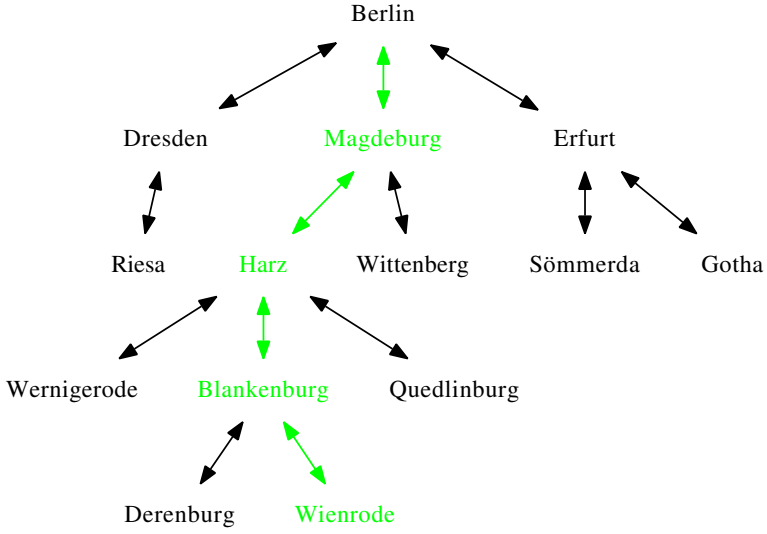
- 1962: ARPA will neues Kommunikations-Netz
- Graphentheorie en vogue $\rightsquigarrow$ Berechnung der Resilienz möglich
- Telefonnetze sind hierarchisch, Unterbäume fallen aus
- Arpanet ist paketvermittelnd, jedes Paket nimmt eigene Route
- Jeder Router vermittelt das Paket selbständig weiter
- große Teile des Netzes können ausfallen, Routing funktioniert trotzdem
- Quelle eines Angriffs schwer zu identifizieren



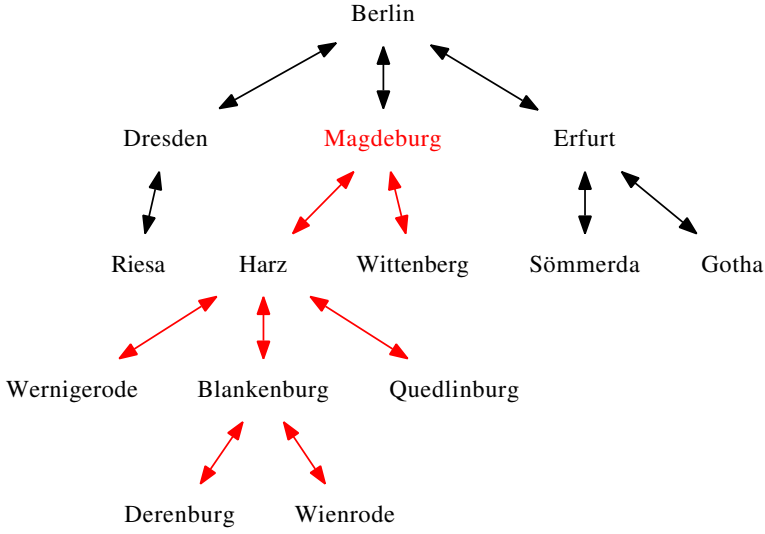
Hierarchie


Berlin
Dresden
Magdeburg
Erfurt
Riesa
Harz
Wittenberg
Sömmerda
Gotha
Wernigerode
Blankenburg
Quedlinburg
Derenburg
Wienrode

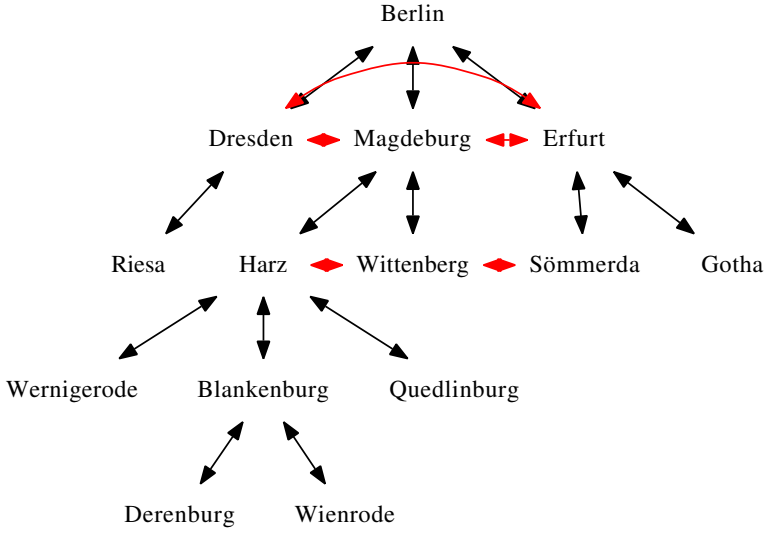
Hierarchie


Berlin
Dresden
Magdeburg
Erfurt
Riesa
Harz
Wittenberg
Sömmerda
Gotha
Wernigerode
Blankenburg
Quedlinburg
Derenburg
Wienrode

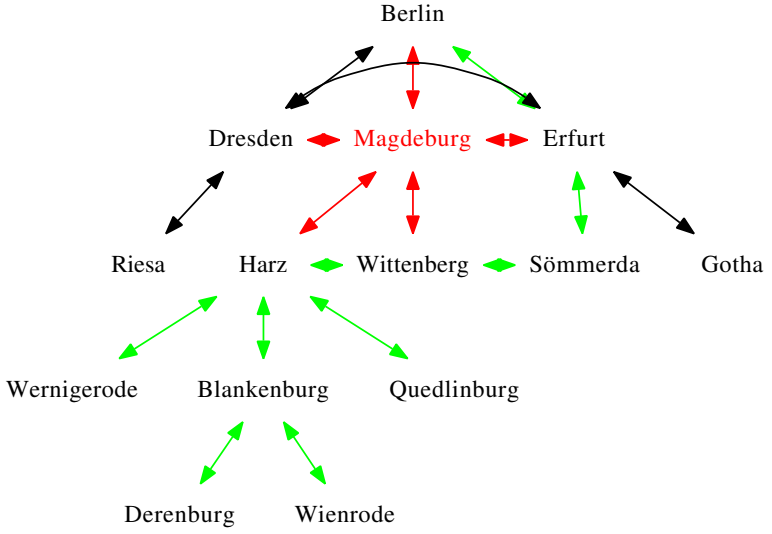
Hierarchie


Berlin
Dresden
Magdeburg
Erfurt
Riesa
Harz
Wittenberg
Sömmerda
Gotha
Wernigerode
Blankenburg
Quedlinburg
Derenburg
Wienrode

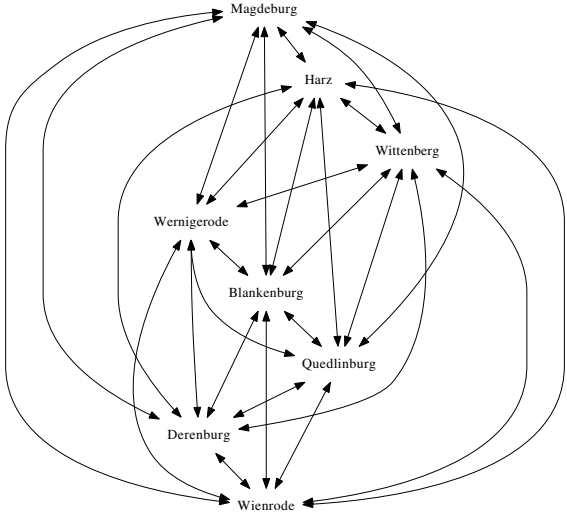
Hierarchie


Berlin
Dresden
Magdeburg
Erfurt
Riesa
Harz
Wittenberg
Sömmerda
Gotha
Wernigerode
Blankenburg
Quedlinburg
Derenburg
Wienrode

Hierarchie

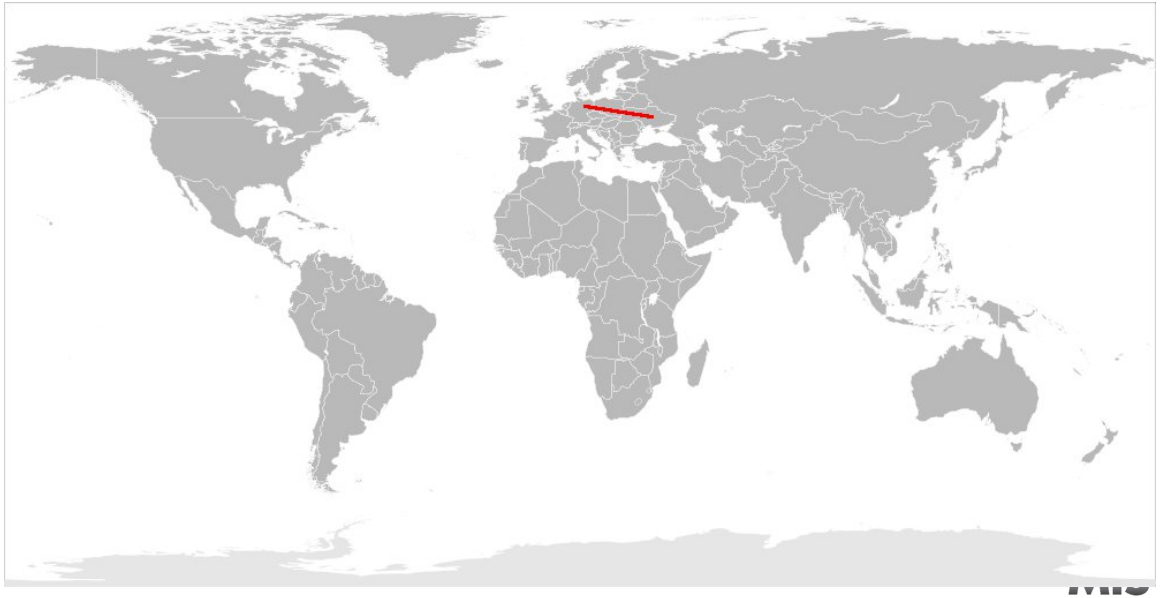

Berlin
Dresden
Magdeburg
Erfurt
Riesa
Harz
Wittenberg
Sömmerda
Gotha
Wernigerode
Blankenburg
Quedlinburg
Derenburg
Wienrode

Netz

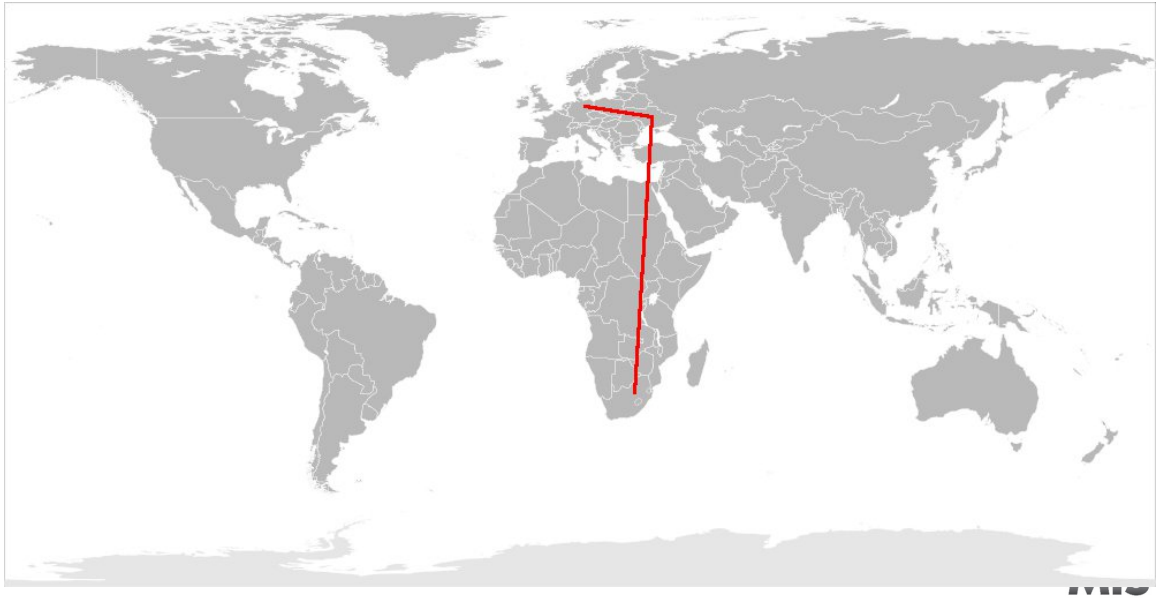


$n\frac{n-1}{2}$ Kanten je Netz == $8\frac{8-1}{2} = 28$ Kanten bei 8 Knoten

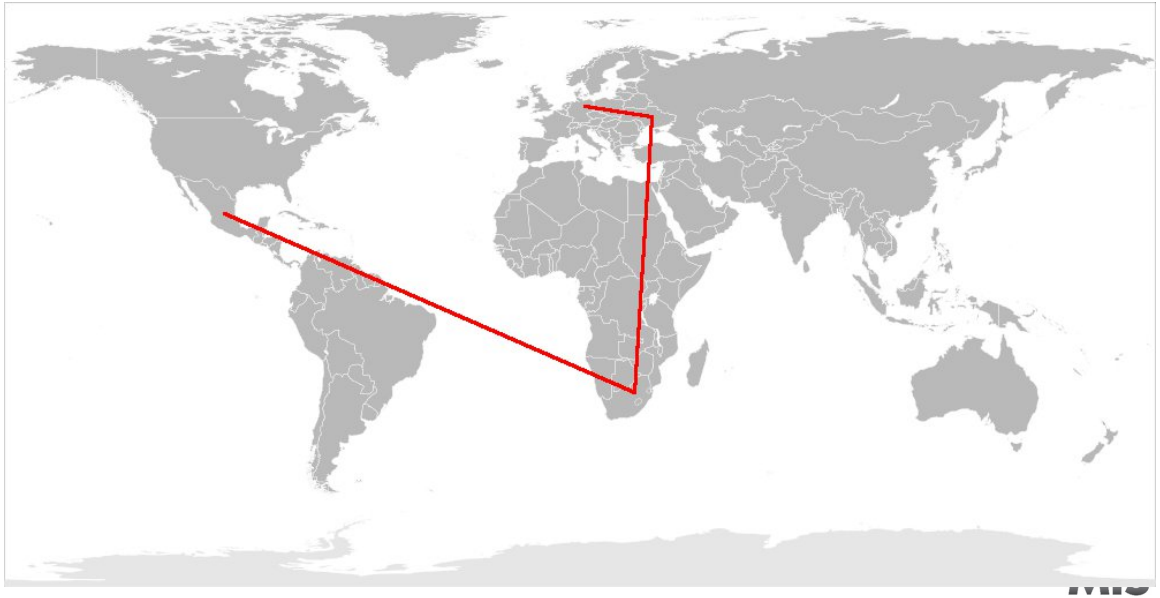
Zurückverfolgung



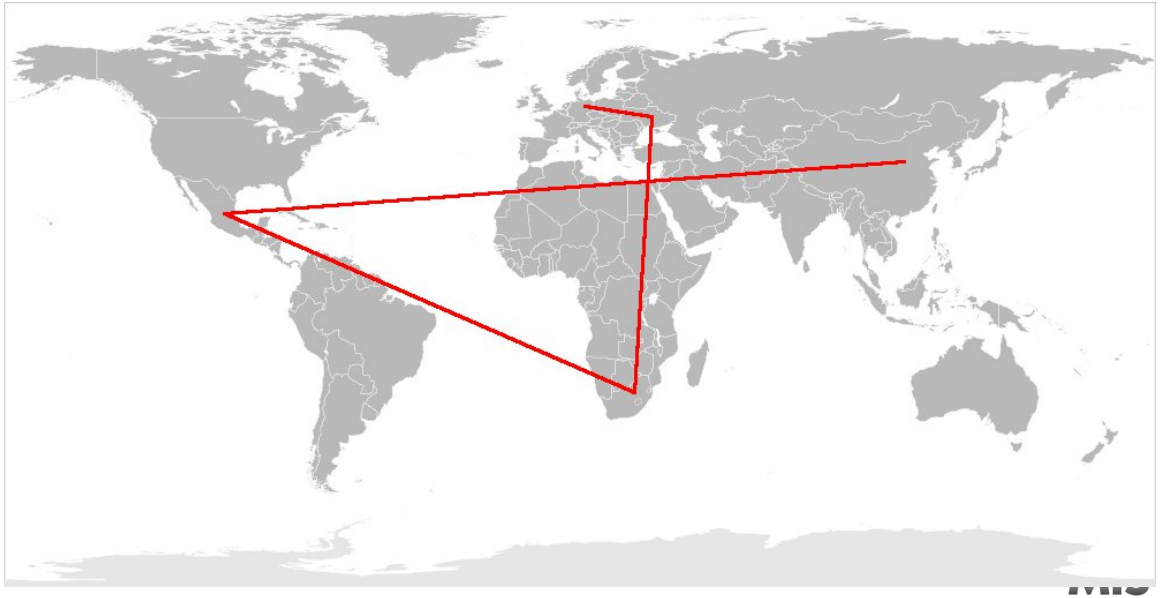
Zurückverfolgung



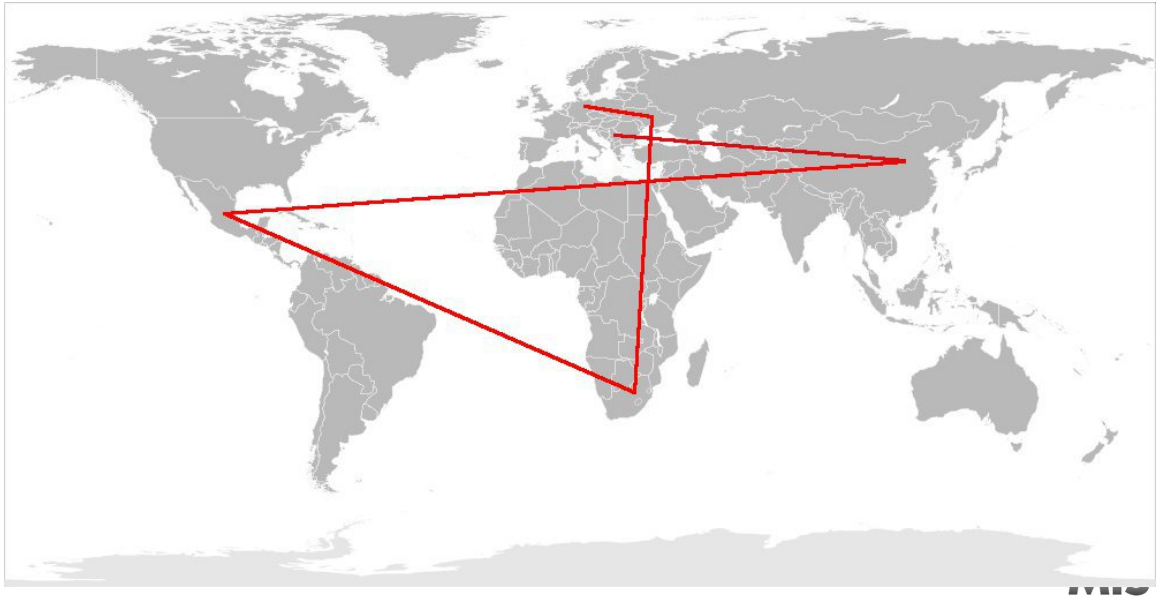
Zurückverfolgung



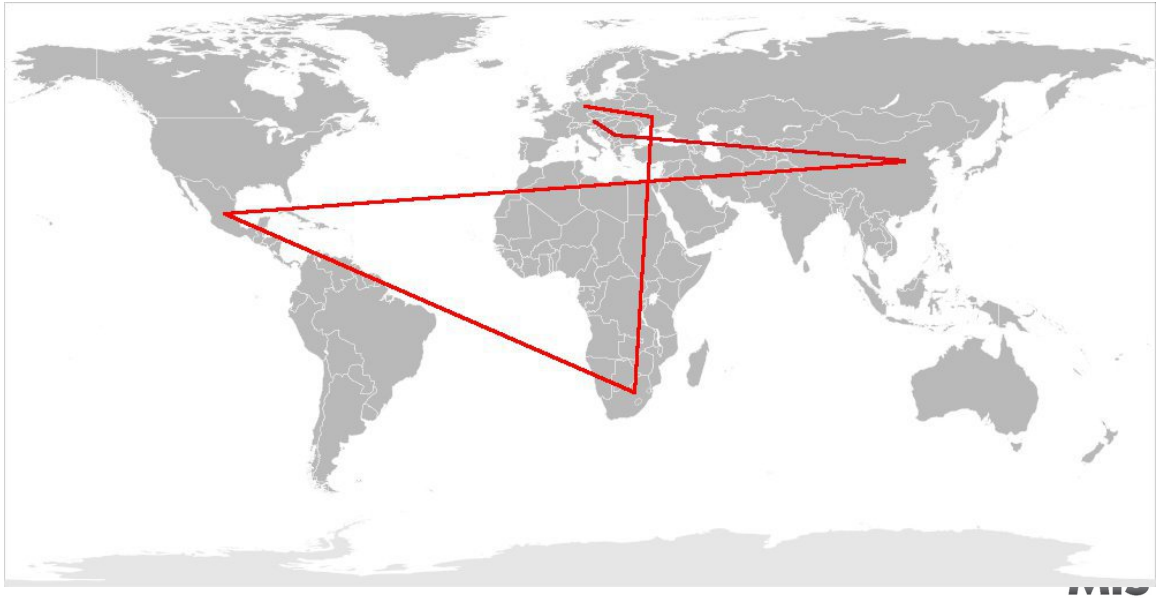
Zurückverfolgung



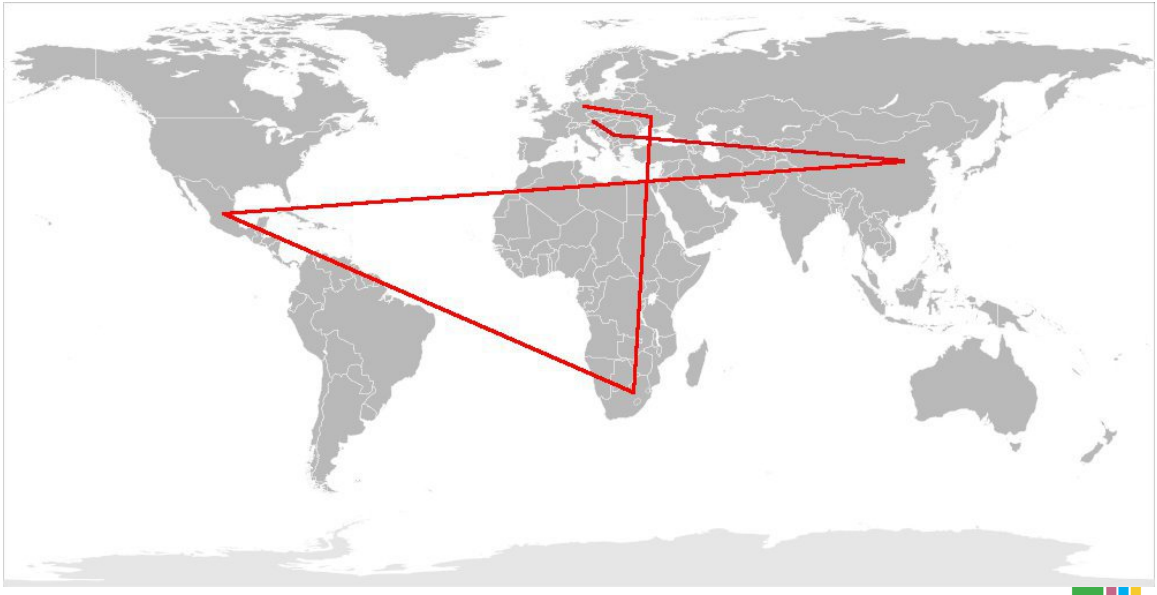
Zurückverfolgung



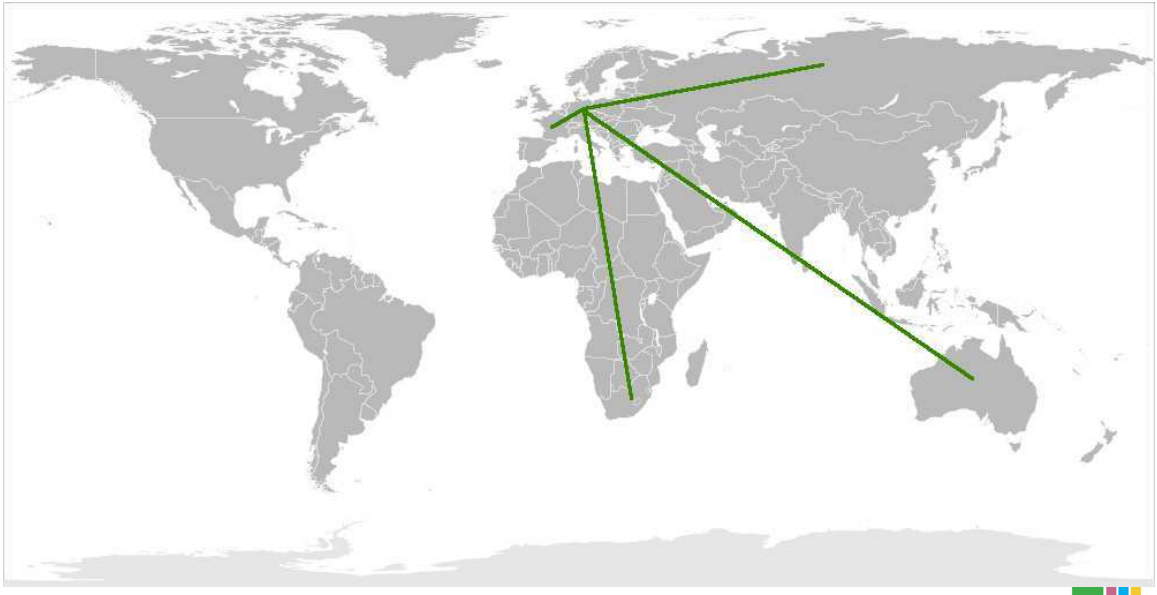
Zurückverfolgung



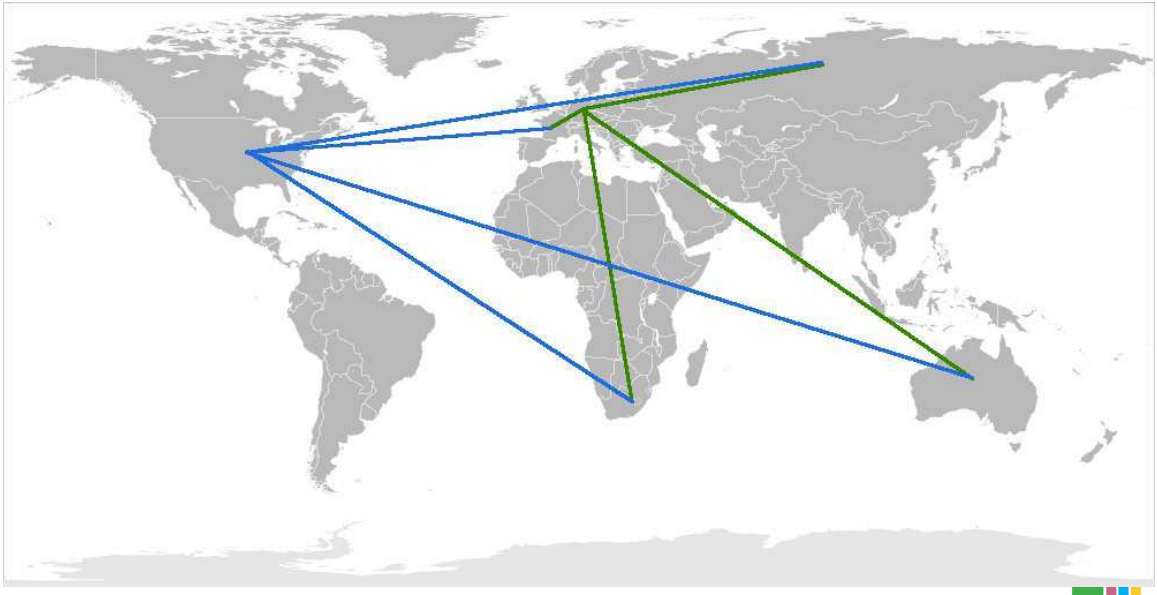
Zurückverfolgung



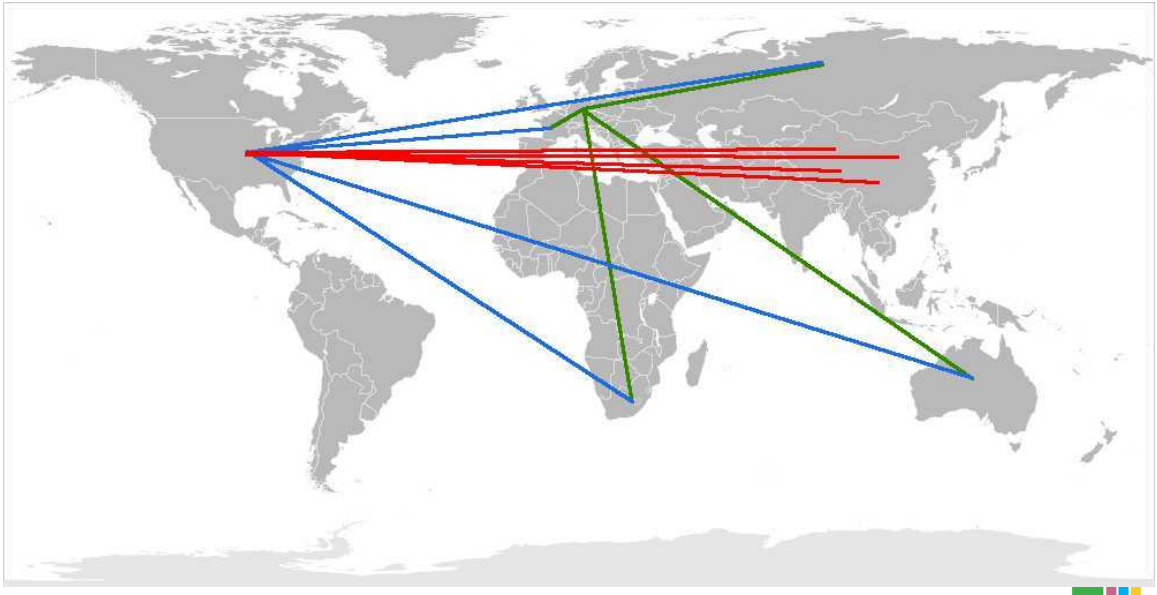
spoofed dDoS



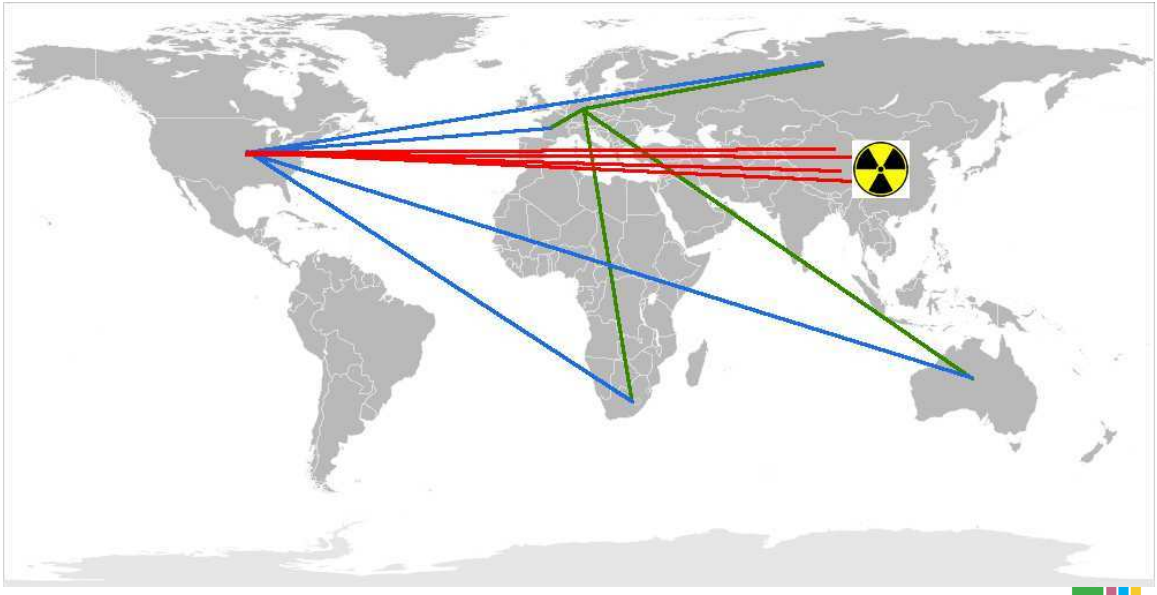
spoofed dDoS



spoofed dDoS



spoofed dDoS



Angriffsmöglichkeiten

- Virus/Wurm/Trojaner der bestimmte Rechner angreift: Wie identifiziere ich die Zielrechner? Eigene Rechner als Kollateralschäden?
- Konventionelle Attacken auf Infrastruktur: DE-CIX peert über 400 ISPs in 45 Ländern, 1815 GBit/s Peak, AMS-CIX 1300 GBit/s
- Elektromagnetischer Puls



1 Staatentheorie

2 Sealand

3 Cyberspace

4 Cyber-Geo-Politik?



Cyber-Geo-Politik

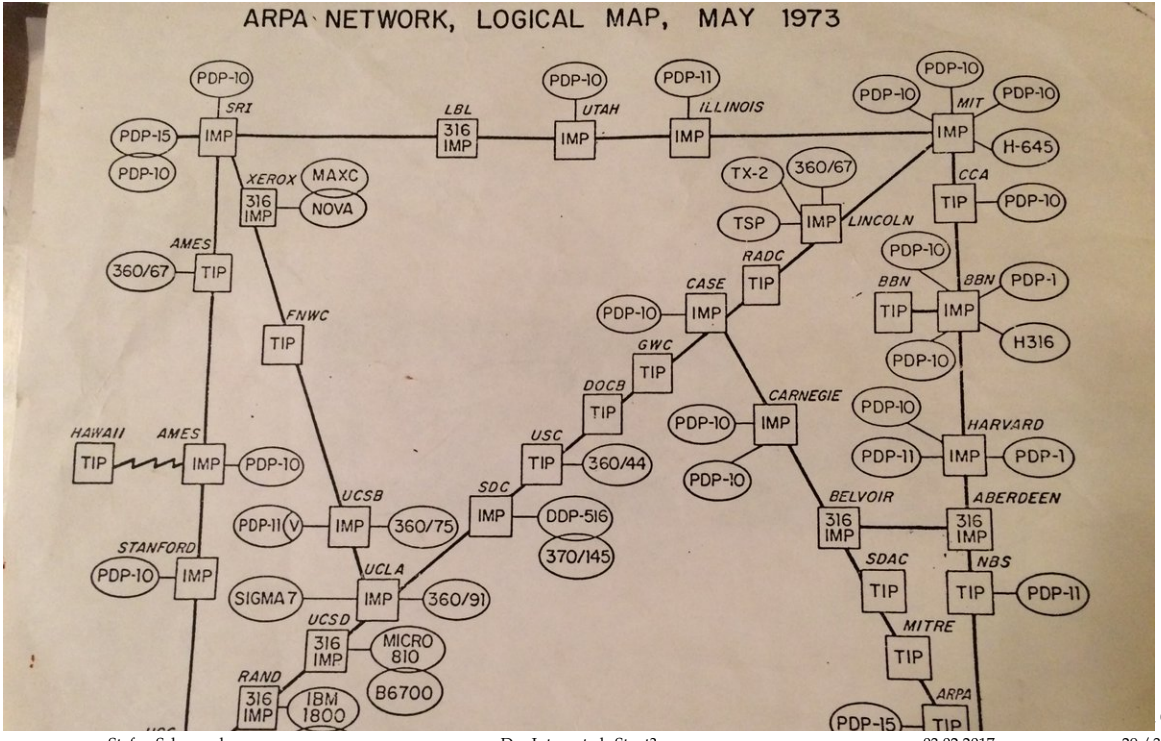
- Cybergeopolitik, Cyberaußenpolitik, Cybergeostrategie?
- Gibt es das?
- *Dänemark will mit „digitalem Botschafter“ Google und Facebook ins Land locken*
- Akkreditiert Facebook Botschafter? Ständige Vertretung Dänemarks bei Facebook?



Wem gehört das Internet?

- USA
- Al Gore
- US Chamber of Commerce
- Icann
- Deutsche Telekom?
- Innenminister NRW
- Otto Schily
- NSA




ARPA NETWORK, LOGICAL MAP, MAY 1973
PDP-10
SRI
IMP
PDP-15
PDP-10
LBL
316 IMP
PDP-10
UTAH
IMP
PDP-11
ILLINOIS
IMP
PDP-10
PDP-10
MIT
PDP-10
IMP
H-645
XEROX
316 IMP
MAXC
NOVA
TX-2
360/67
TSP
IMP
LINCOLN
CCA
TIP
PDP-10
AMES
360/67
TIP
RADC
TIP
PDP-10
BBN
TIP
BBN
IMP
PDP-1
H316
FNWC
TIP
CASE
IMP
PDP-10
GWC
TIP
PDP-10
DOCB
TIP
CARNEGIE
PDP-10
IMP
PDP-10
HAWAII
TIP
AMES
IMP
PDP-10
USC
TIP
360/44
HARVARD
PDP-10
PDP-11
IMP
PDP-1
UCSB
PDP-11
V
IMP
360/75
SDC
IMP
DDP-516
370/145
BELVOIR
316 IMP
ABERDEEN
316 IMP
STANFORD
PDP-10
IMP
UCLA
SIGMA7
IMP
360/91
SDAC
TIP
NBS
TIP
PDP-11
UCSD
316 IMP
MICRO 810
MITRE
TIP
RAND
316 IMP
IBM 1800
B6700
ARPA
PDP-15
TIP

DNS

- Domain Name Service
- wandelt IP-Adresse in Domain Namen um
- rechner.subdomain.subdomain.domain.ccTLD
- `sekretariat.geometrie.mathefakultaet.uni-wittenberg.dr`
- TLD/ccTLD als oberste Hierarchie, Verwaltung durch ICANN und lokale NICs
- 7 Rootserver
- 2001 .iq und .af "ausgefallen"
- ohne DNS geht kaum noch etwas



- 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

