Vom Cyber-Kriege

Stefan Schumacher

www.sicherheitsforschung-magdeburg.de
Magdeburger Institut für Sicherheitsforschung

Mannheim, 10.05.



Über Mich

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



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

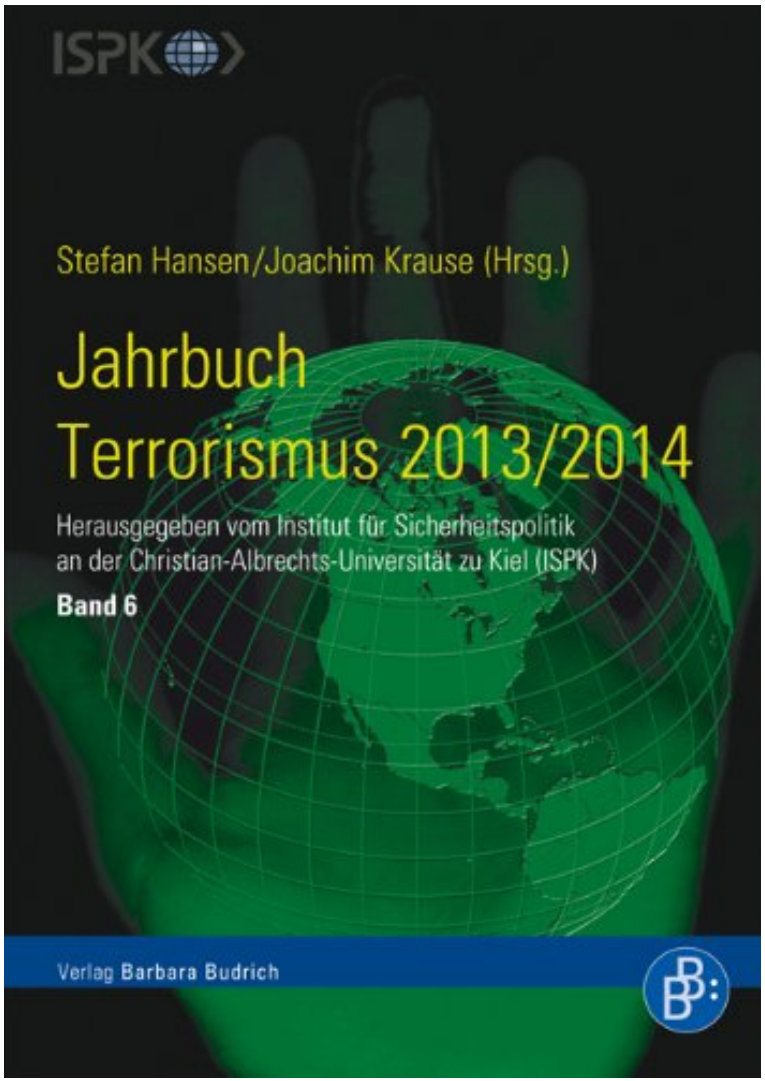
Sambleben, J. und Schumacher, S. (Herausgeber)



sicherheitsforschung-magdeburg.de/buecher.html

Jahrbuch Terrorismus 2013/2014

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



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

Inhaltsverzeichnis

1. Vom Kriege
2. Politik und Recht
3. Krieg im Internet? Geht das?
   - Angriffsvektoren



Warum das alles?

Cyberwar ist zur Zeit ein vieldiskutiertes Thema in

- den Medien
- der Hacker- und IT-Sicherheitsszene
- Militär
- Politik
- Politikwissenschaft

Stuxnet, Flame, »Chinesen« im Bundestag, Estland, Georgien, Backdoors in militärischen FPGAs …



Qualität der Diskussion

- Viele Diskussionsbeiträge ohne technische Grundlagen oder fehlerhaft
- technisches Problem
- technische Analyse
- Technikfolgeabschätzung
- Was ist ein Krieg? Kann dieser Krieg im Cyberspace geführt werden?

Inhaltsverzeichnis

1. Vom Kriege
2. Politik und Recht
3. Krieg im Internet? Geht das?

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)

Cyber War

Krieg

Definition (Clausewitz: Vom Kriege, Buch I, Kapitel 1, Abschnitt 2)

Der Krieg ist also ein Akt der Gewalt, um den Gegner zur Erfüllung unseres Willens zu zwingen.

- Krieg ist die Fortsetzung der Politik mit anderen Mitteln $\rightsquigarrow$ Strategie *über* dem Kriege
- Ziele des Krieges: begrenzte Ziele erreichen oder einen Gegner derart entwaffnen, dass er politisch hilflos und militärisch wehrlos ist



Inhaltsverzeichnis

1 Vom Kriege

2 Politik und Recht

3 Krieg im Internet? Geht das?



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



Vom Cyber-Kriege

- staatlicher Urheber
- Gegner wehrlos machen oder zwingen können
- Strategie notwendig
- Ziele notwendig

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)



Inhaltsverzeichnis

1 Vom Kriege

2 Politik und Recht

3 Krieg im Internet? Geht das?



Cyber-*Krieg*?

- Ziel: Gegner derart entwaffnen, dass er politisch hilflos und militärisch wehrlos ist
- Geht das im Cyberspace?
- Gefährdungsanalyse durchführen (Pen-Testing, Tiger-Teams)
- Problem: sensible Daten liegen nicht offen
- Beispiel-Assets: E-Werke/Stromnetze; Kom-Netze; Waffensysteme
- *Abhängigkeit* von den Assets: Was passiert bei Stromausfall?

Cyber-*Krieg*?

- Ziel: Gegner derart entwaffnen, dass er politisch hilflos und militärisch wehrlos ist
- Geht das im Cyberspace?
- Gefährdungsanalyse durchführen (Pen-Testing, Tiger-Teams)
- Problem: sensible Daten liegen nicht offen
- Beispiel-Assets: E-Werke/Stromnetze; Kom-Netze; Waffensysteme
- *Abhängigkeit* von den Assets: Was passiert bei Stromausfall?

Smartmeter

Ein neuer Angriffsvektor

- EU möchte »intelligente« Stromzähler in allen Haushalten
- messen Verbrauch und melden ihn an die Versorger
- können Stromversorgung für Haushalt abschalten
- IT-Sicherheit wird dort sehr stark vernachlässigt (E-Techniker)
- geringe Diversifikation + Sicherheitslücke im Smartmeter $\rightsquigarrow$ Massenepidemie
- Smart Grid erfordert Kommunikation zwischen Netzteilnehmern
- Europäisches Verbundnetz $\rightsquigarrow$ Europa ohne Strom
- 24.12.2017, 15 Uhr, -12° C und die Ukraine dreht die Gaspipeline zu ...



Stuxnet

Ein Blick auf die strategische Ebene

- Stuxnet war teuer, mehrere gute Programmierer + Projekmanagement
- Testgestellung inklusive SCADA (!) und Frequenzumrichter
- gut organisierte Gruppe, generalstabsmäßig geplant
- nutzte mehrere 0day Exploits (teuer)
- nutzte mehrere Agriffsvektoren
- physisch ausgerollte USB-Sticks in Kernkraftwerken wahrscheinlich über Konferenzen
- organisierter, strategisch geplanter Akt der »Gewalt«
- *aber* hat es den Gegner dazu gebracht, einen Willen zu erfüllen oder politische Ziele erreicht? Wer stellte denn Forderungen? Was sind denn die Ziele?



Stuxnet

Ein Blick auf die strategische Ebene

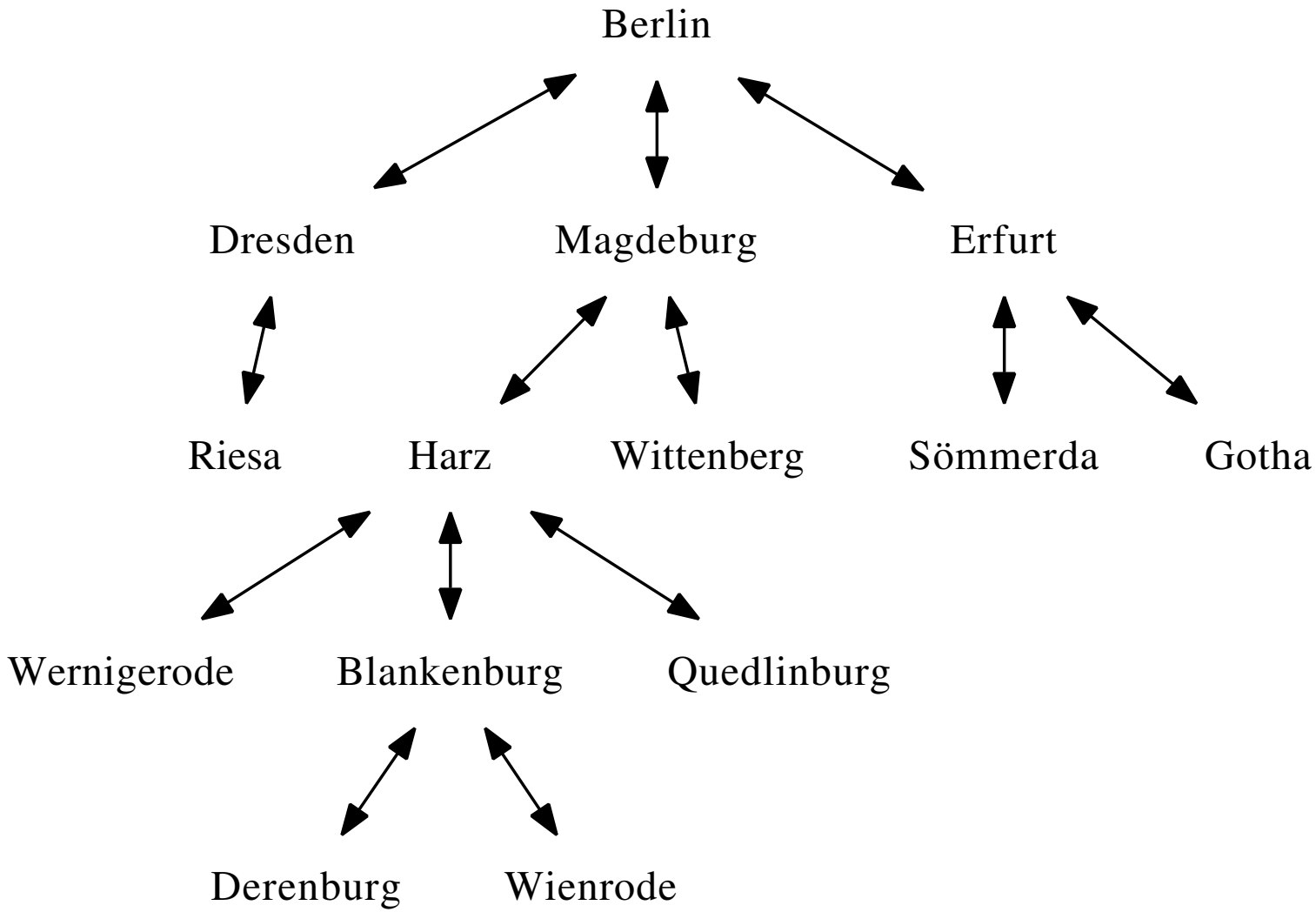
- Stuxnet war teuer, mehrere gute Programmierer + Projekmanagement
- Testgestellung inklusive SCADA (!) und Frequenzumrichter
- gut organisierte Gruppe, generalstabsmäßig geplant
- nutzte mehrere 0day Exploits (teuer)
- nutzte mehrere Agriffsvektoren
- physisch ausgerollte USB-Sticks in Kernkraftwerken wahrscheinlich über Konferenzen
- organisierter, strategisch geplanter Akt der »Gewalt«
- *aber* hat es den Gegner dazu gebracht, einen Willen zu erfüllen oder politische Ziele erreicht? Wer stellte denn Forderungen? Was sind denn die Ziele?



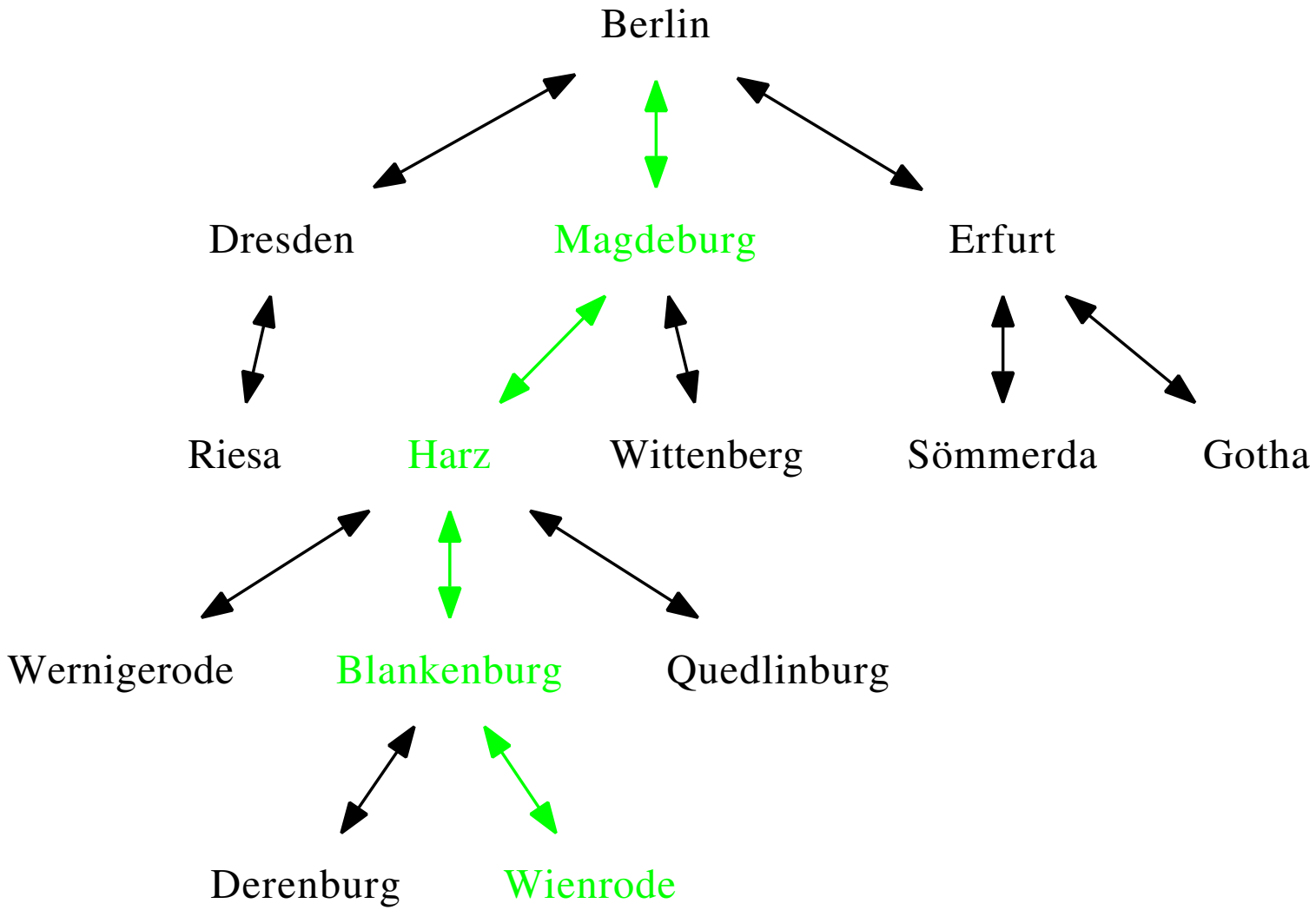
Routing

- 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

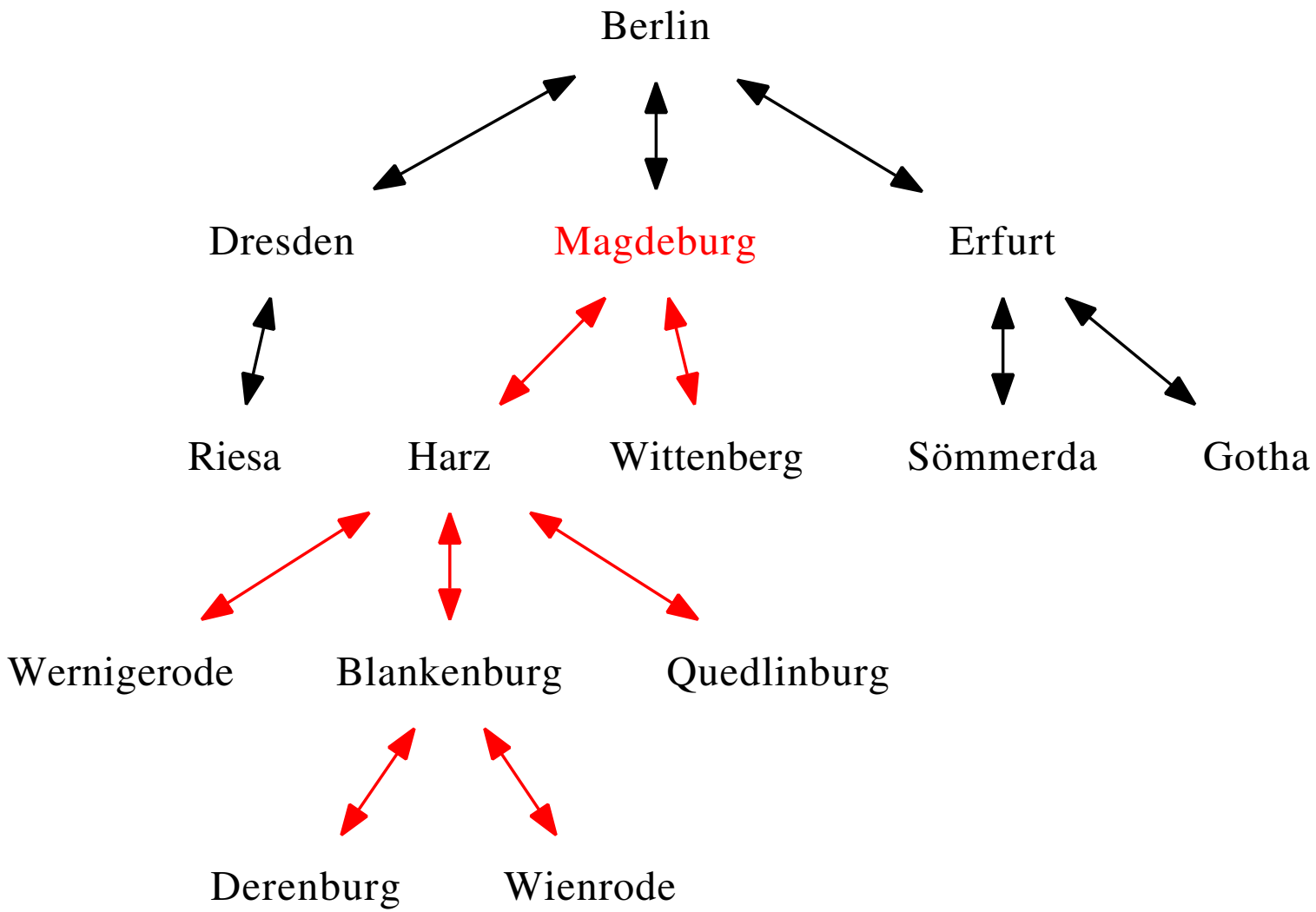
Hierarchie


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

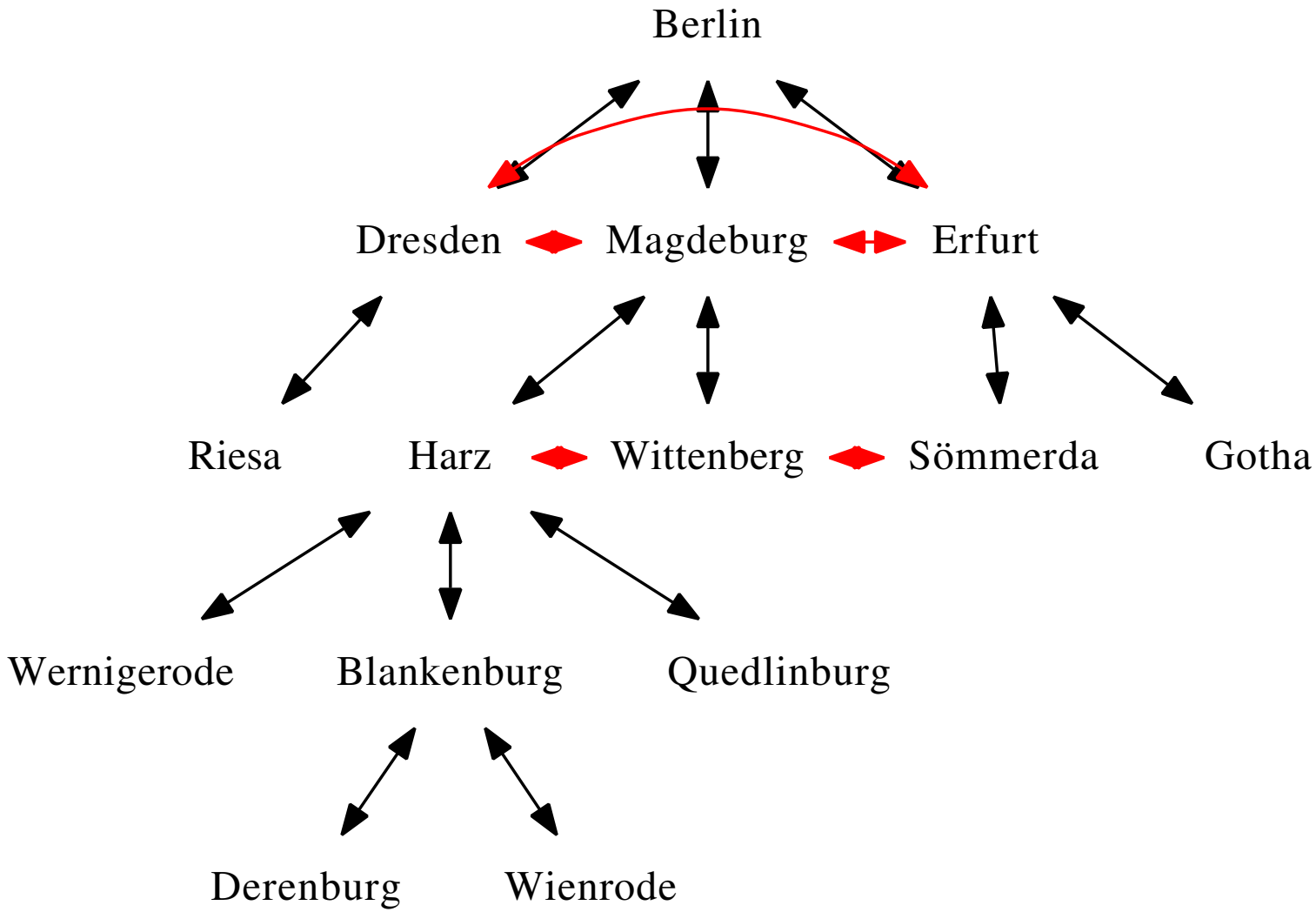
Hierarchie


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

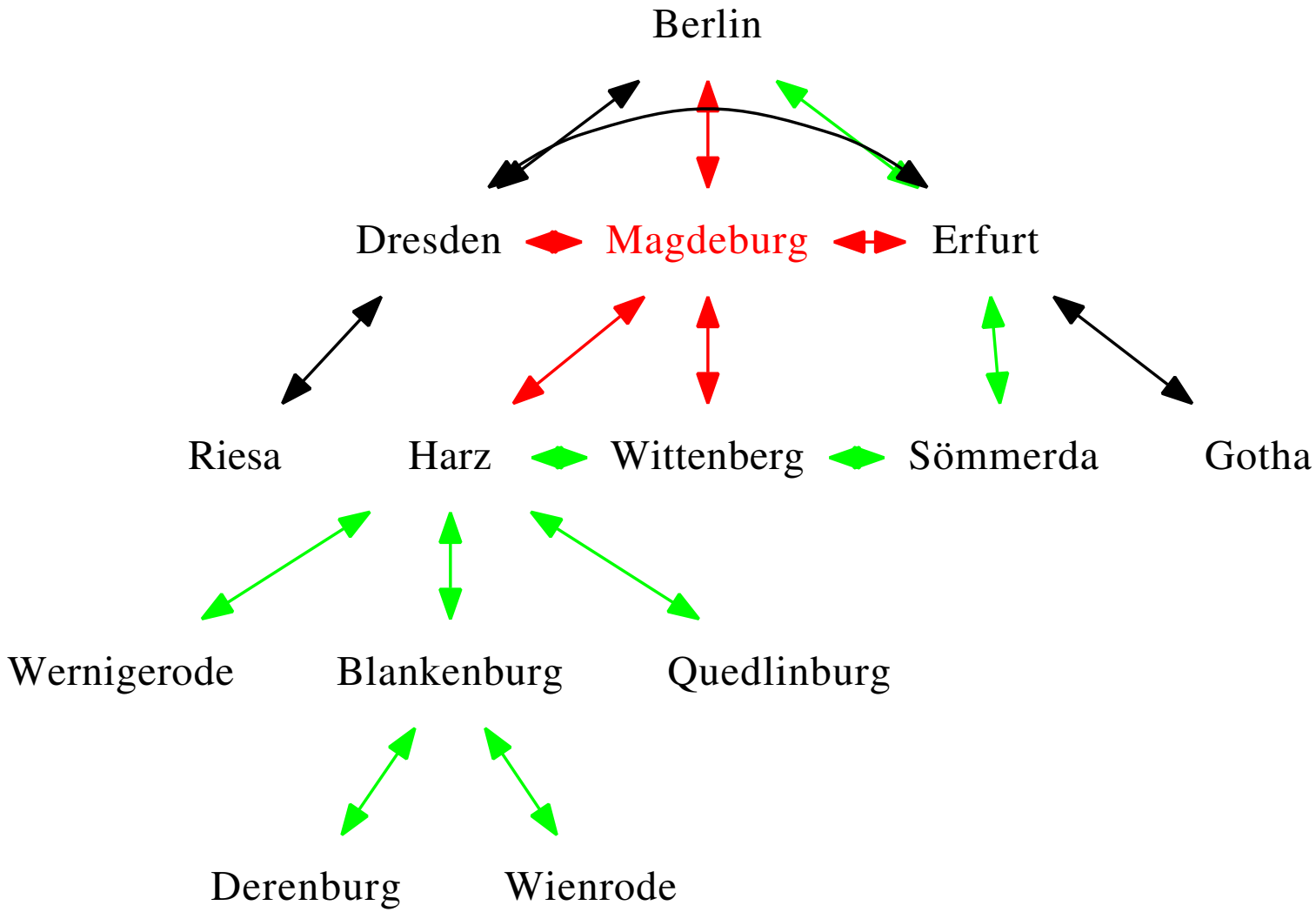
Hierarchie


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

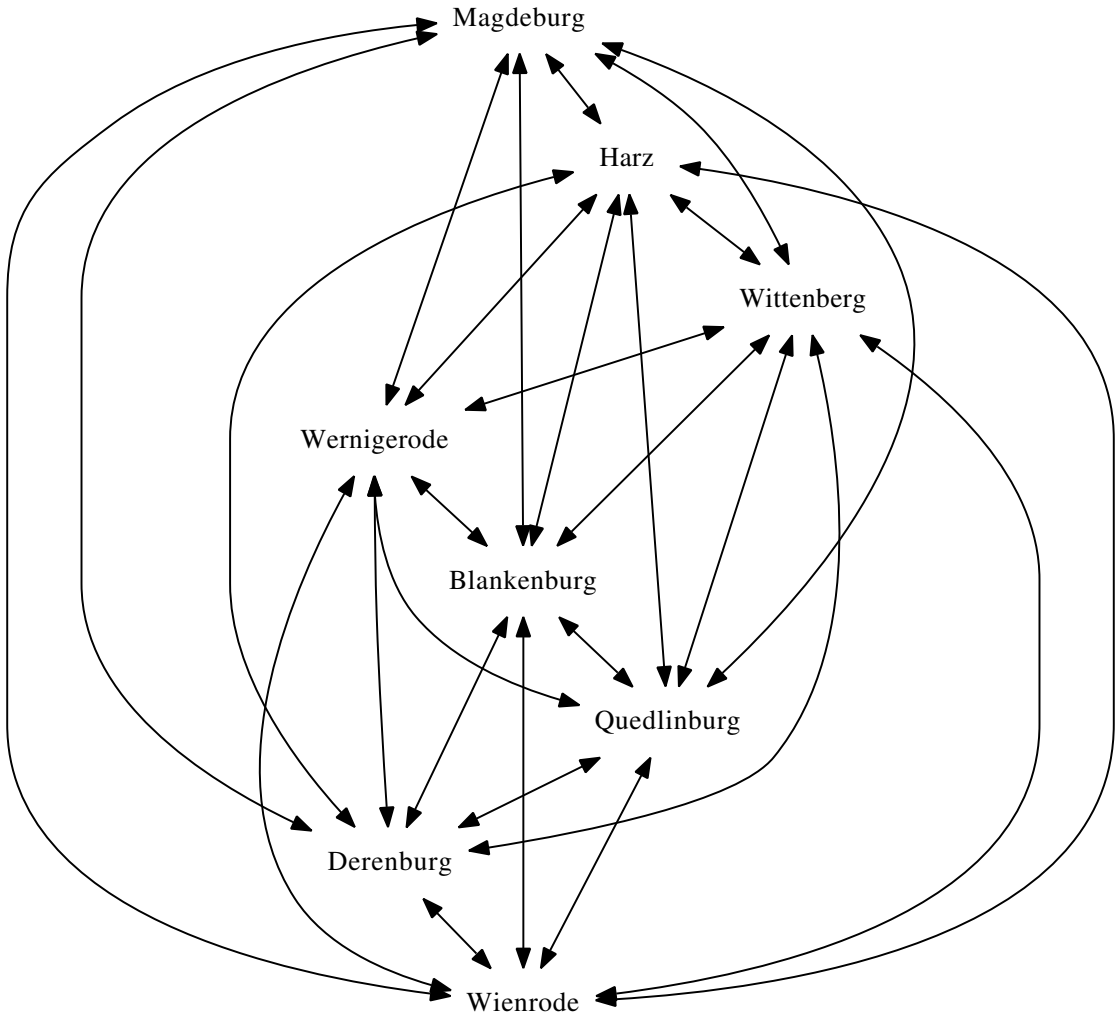
Hierarchie


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

distributed Denial of Service (dDoS)

- ein Angreifer schickt soviele Anfragen, dass der Server überlastet wird
- der Angreifer nutzt mehrere Rechner, sog. Botnetz
- erlangt durch Trojaner Kontrolle über »Zombies«, idR Microsoft Windows
- Zombies sind normale Privatrechner, keine Kombatanten oder Söldner
- können *jeden* Rechner lahmlegen, Verteidigung sehr schwer
- Botnetze können gemietet werden
- Bsp: Stacheldraht (2000), Estland (2007), Georgien (2008)
- 14-jähriges Skriptkiddie kann bspw. das Kommunikationsnetz der US Air Force lahmlegen

distributed Denial of Service (dDoS)

- ein Angreifer schickt soviele Anfragen, dass der Server überlastet wird
- der Angreifer nutzt mehrere Rechner, sog. Botnetz
- erlangt durch Trojaner Kontrolle über »Zombies«, idR Microsoft Windows
- Zombies sind normale Privatrechner, keine Kombatanten oder Söldner
- können *jeden* Rechner lahmlegen, Verteidigung sehr schwer
- Botnetze können gemietet werden
- Bsp: Stacheldraht (2000), Estland (2007), Georgien (2008)
- 14-jähriges Skriptkiddie kann bspw. das Kommunikationsnetz der US Air Force lahmlegen



Authentizität und Integrität

- Integrität: etwas wurde nicht verändert
- Authentizität: etwas stammt vom Urheber
- ist elektronisch definitiv nicht sicherzustellen
- außer mit Kryptographie (digitale Unterschrift)
  Problem: beide Seiten müssen wollen
- IP-Pakete können leicht gefälscht werden
- wenn ich »unsichtbar« bleiben will kann ich das
- erst recht als Geheimdienst/Armee

Authentizität und Integrität

- Integrität: etwas wurde nicht verändert
- Authentizität: etwas stammt vom Urheber
- ist elektronisch definitiv nicht sicherzustellen
- außer mit Kryptographie (digitale Unterschrift)
  Problem: beide Seiten müssen wollen
- IP-Pakete können leicht gefälscht werden
- wenn ich »unsichtbar« bleiben will kann ich das
- erst recht als Geheimdienst/Armee
- chinesische Superhacker im Bundestag?
- Trojaner und Zombies, oder: Wer hat die Befehlsgewalt über den Rechner? (Beispiel folgt)

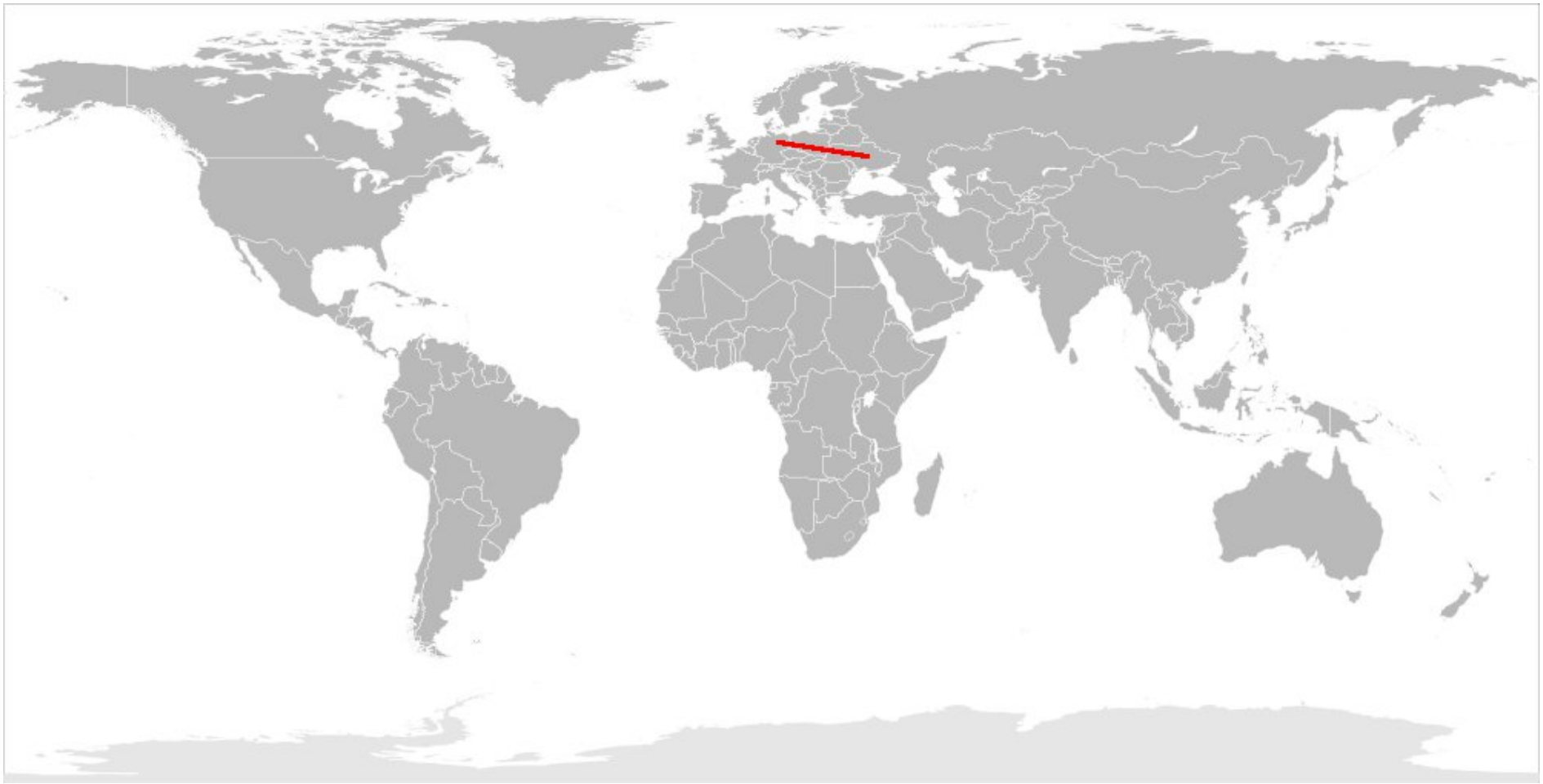


Authentizität und Integrität

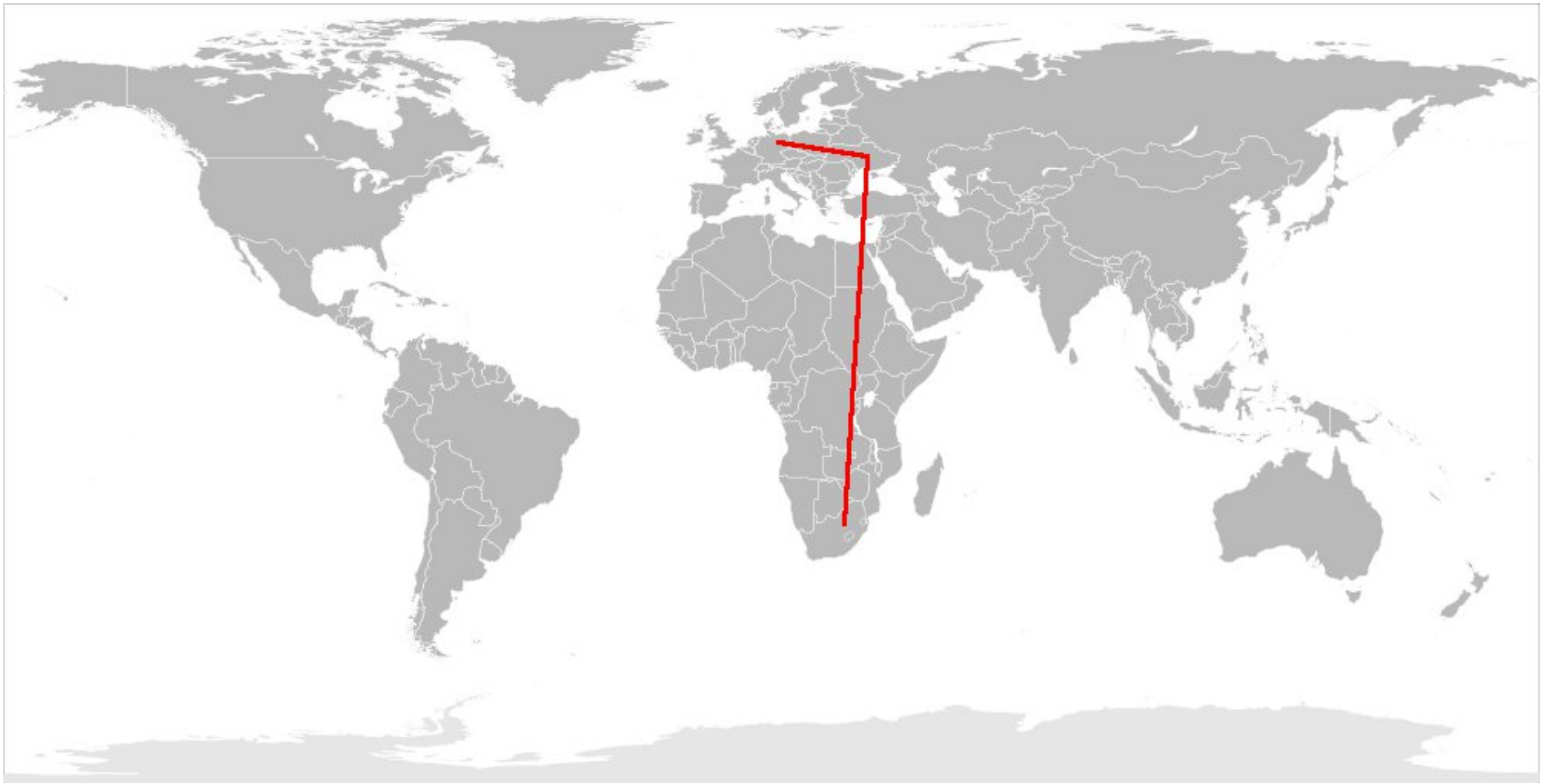
- Integrität: etwas wurde nicht verändert
- Authentizität: etwas stammt vom Urheber
- ist elektronisch definitiv nicht sicherzustellen
- außer mit Kryptographie (digitale Unterschrift)
  Problem: beide Seiten müssen wollen
- IP-Pakete können leicht gefälscht werden
- wenn ich »unsichtbar« bleiben will kann ich das
- erst recht als Geheimdienst/Armee
- chinesische Superhacker im Bundestag?
- Trojaner und Zombies, oder: Wer hat die Befehlsgewalt über den Rechner? (Beispiel folgt)



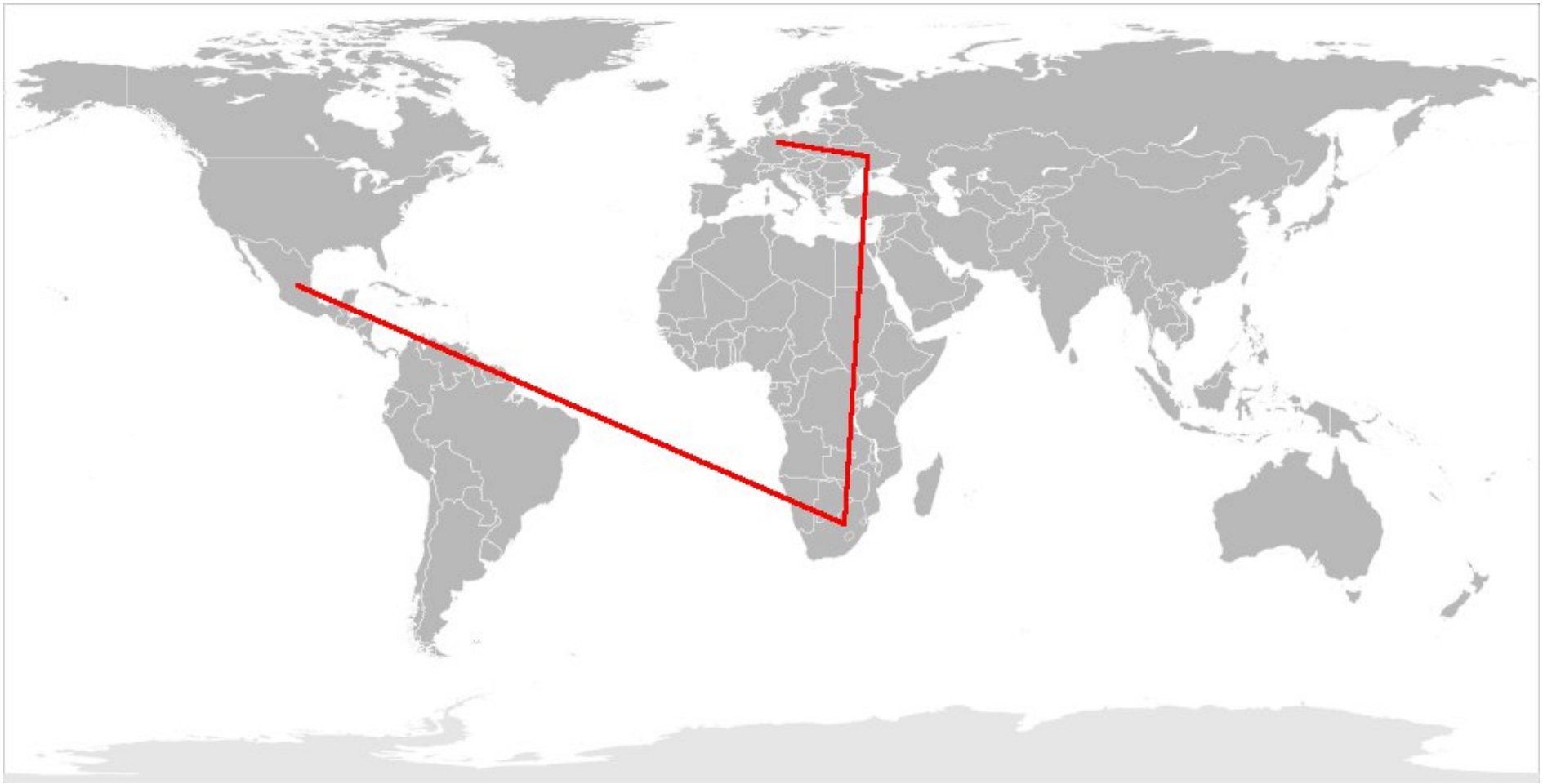
Zurückverfolgung



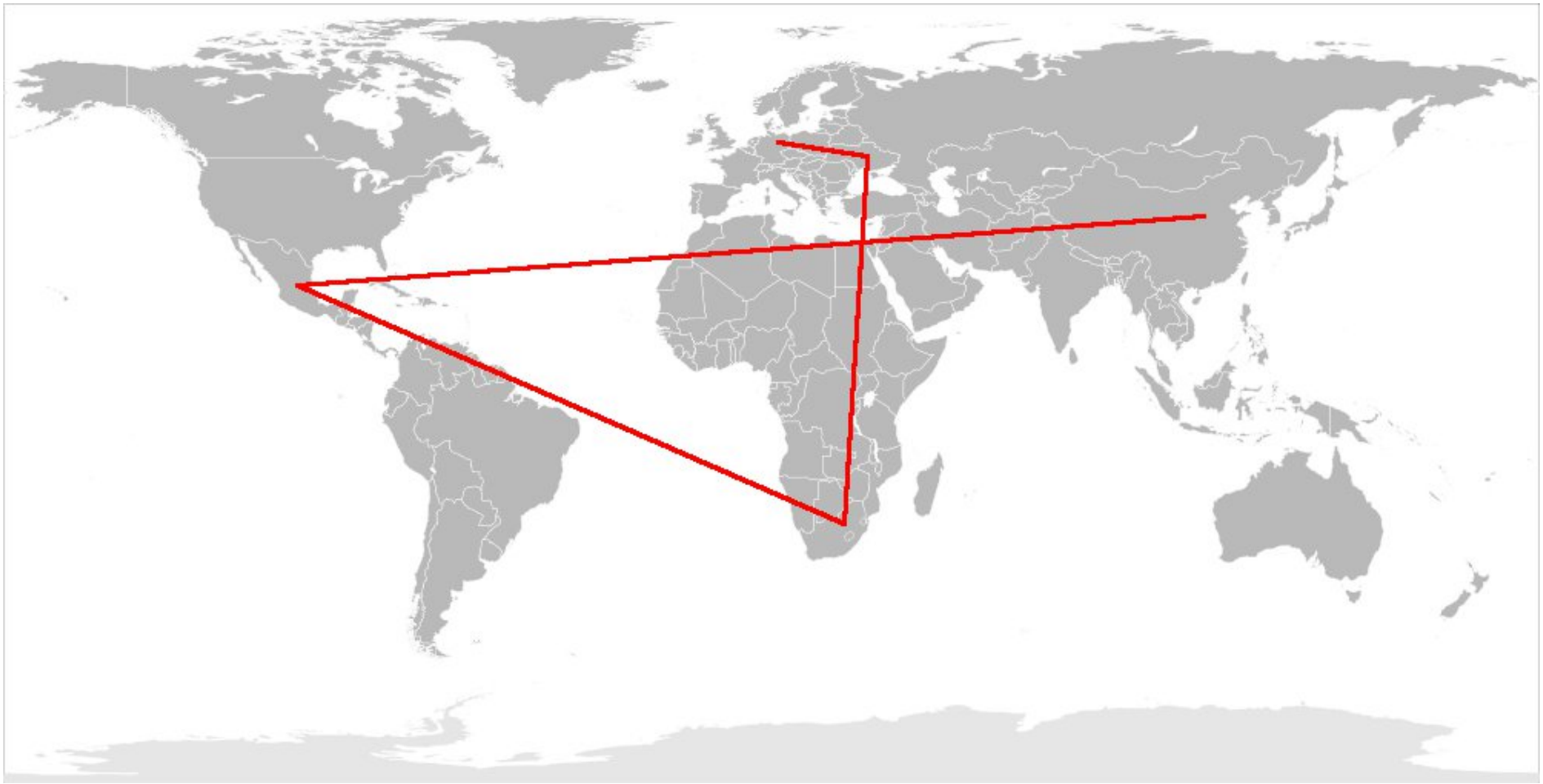
Zurückverfolgung



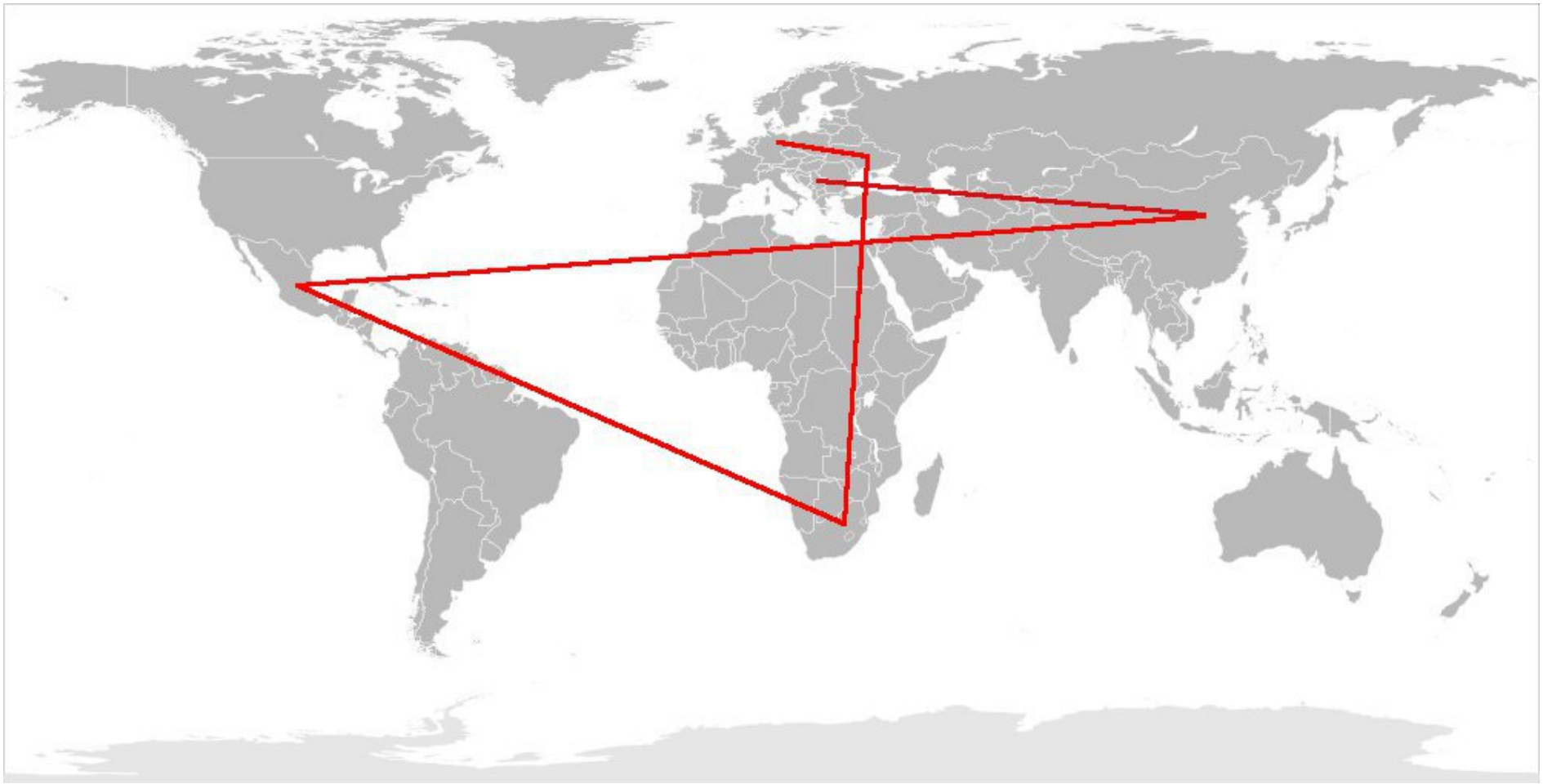
Zurückverfolgung



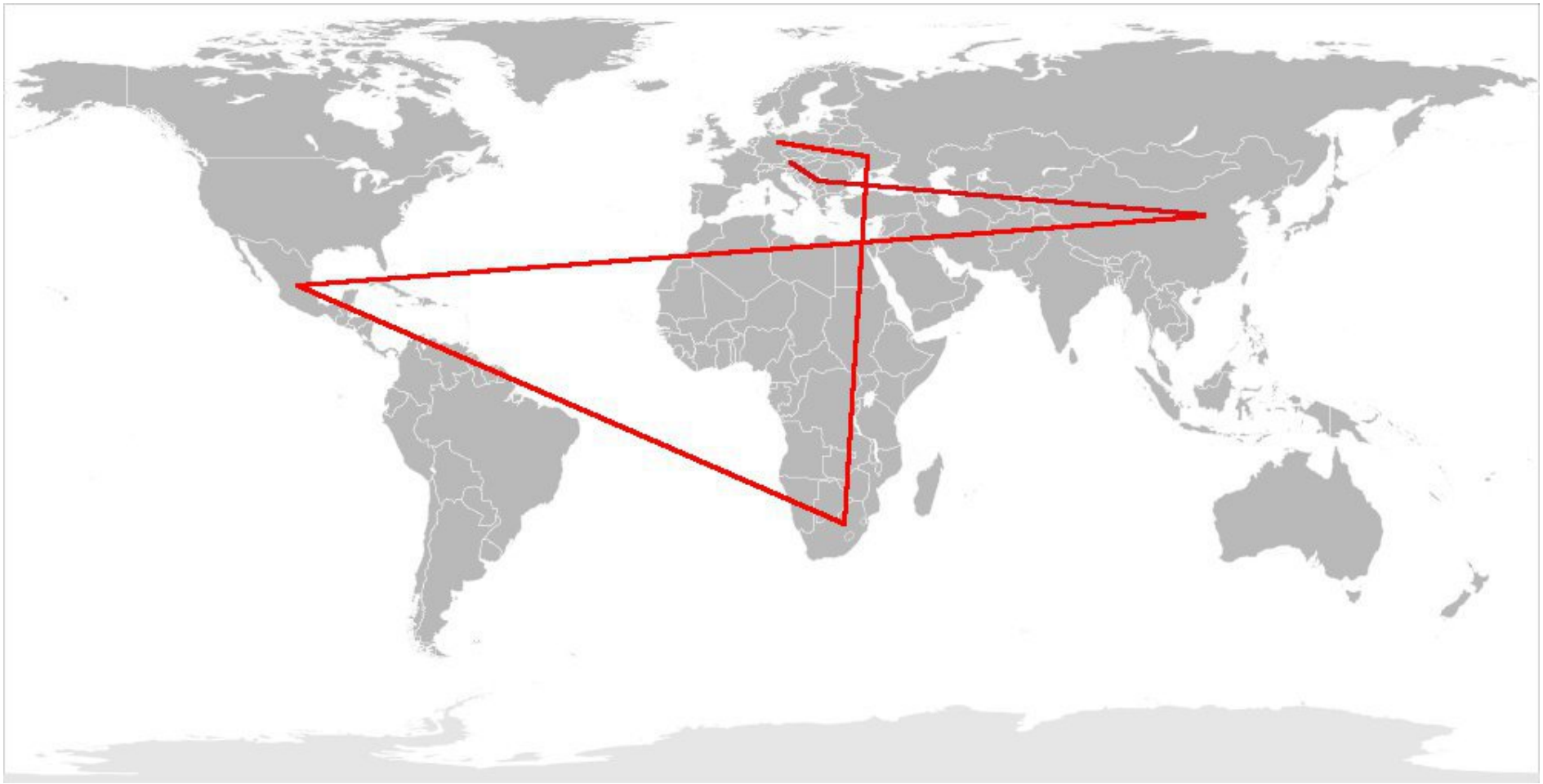
Zurückverfolgung



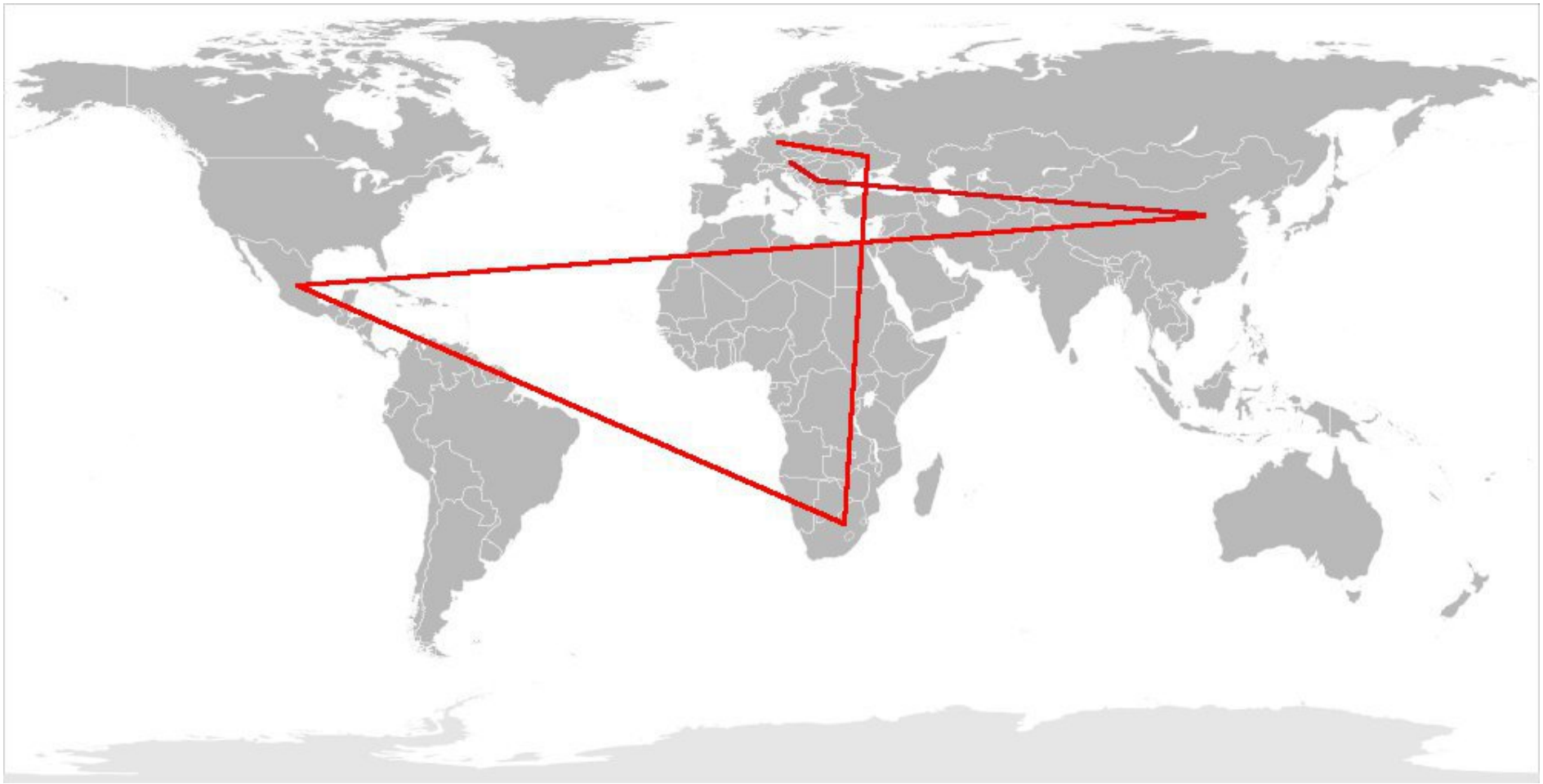
Zurückverfolgung



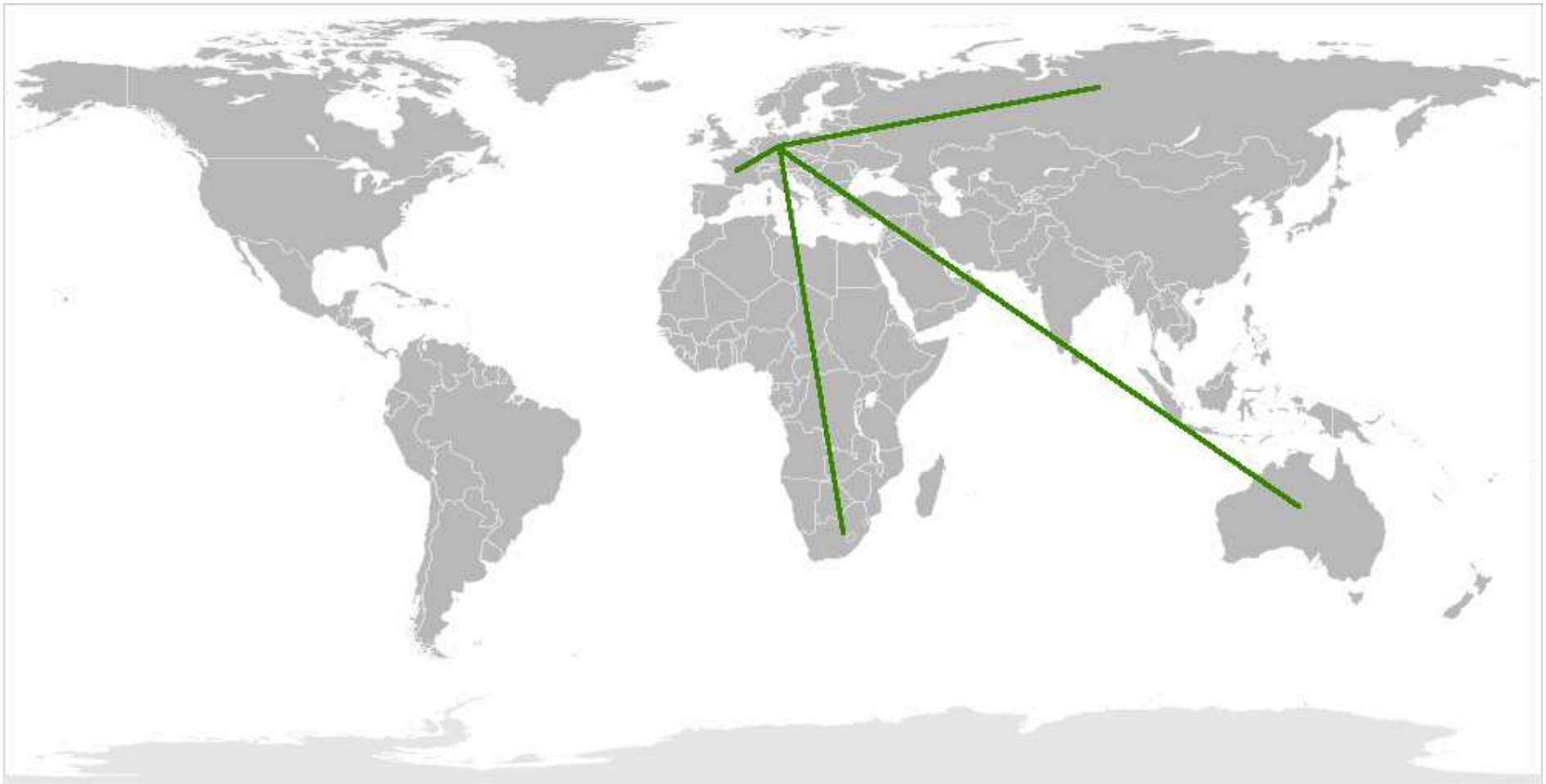
Zurückverfolgung



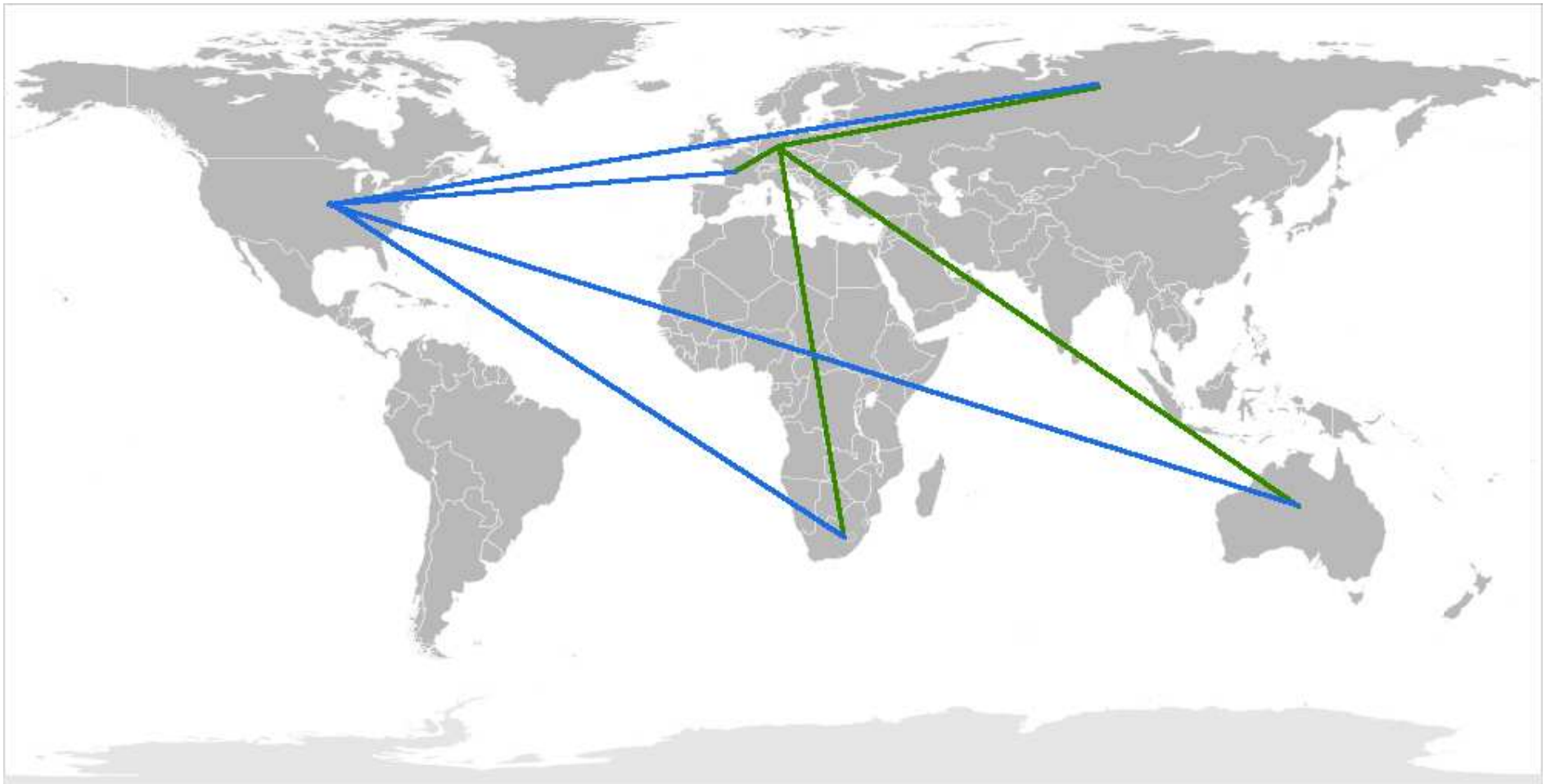
Zurückverfolgung



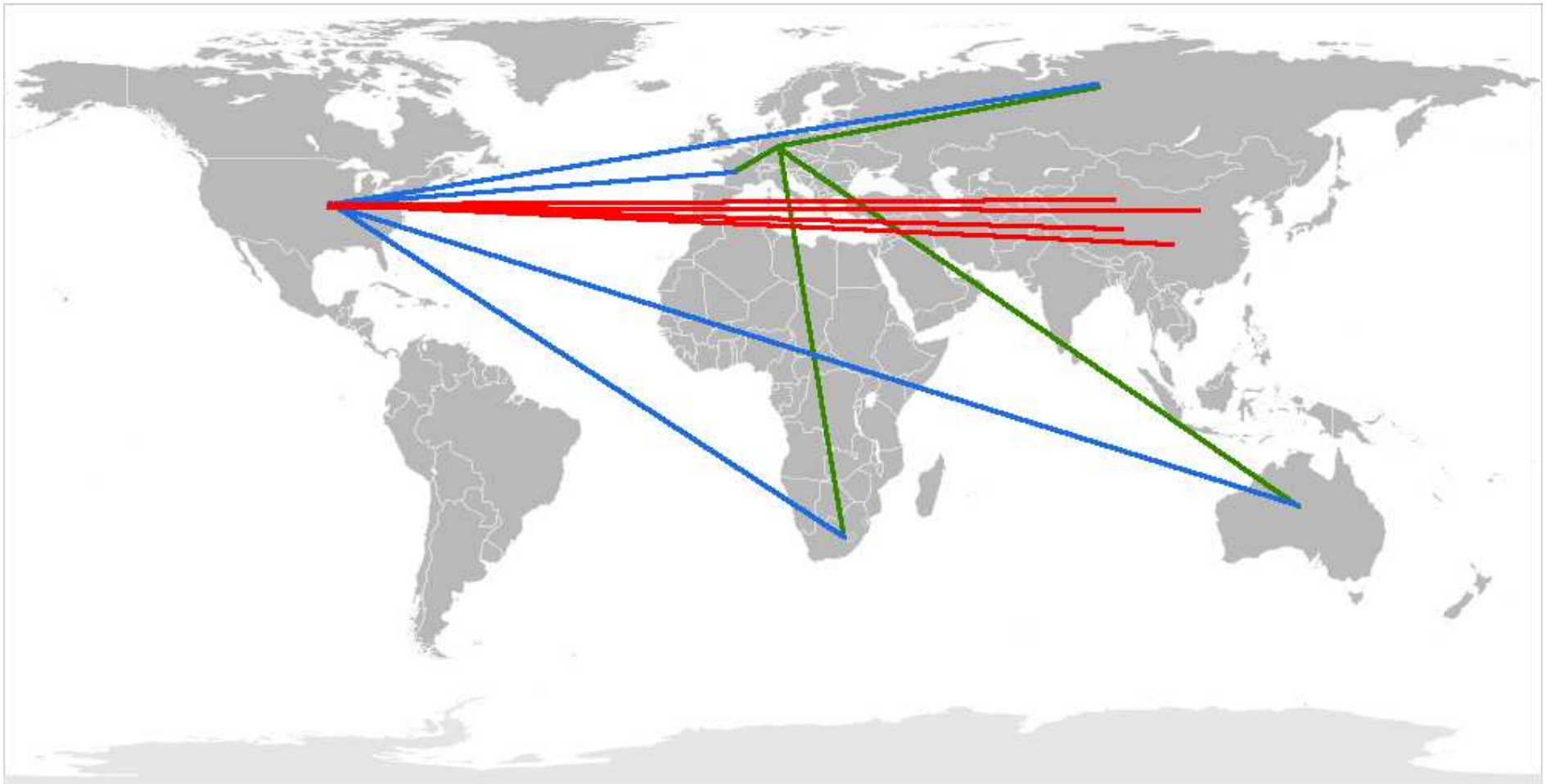
spoofed dDoS



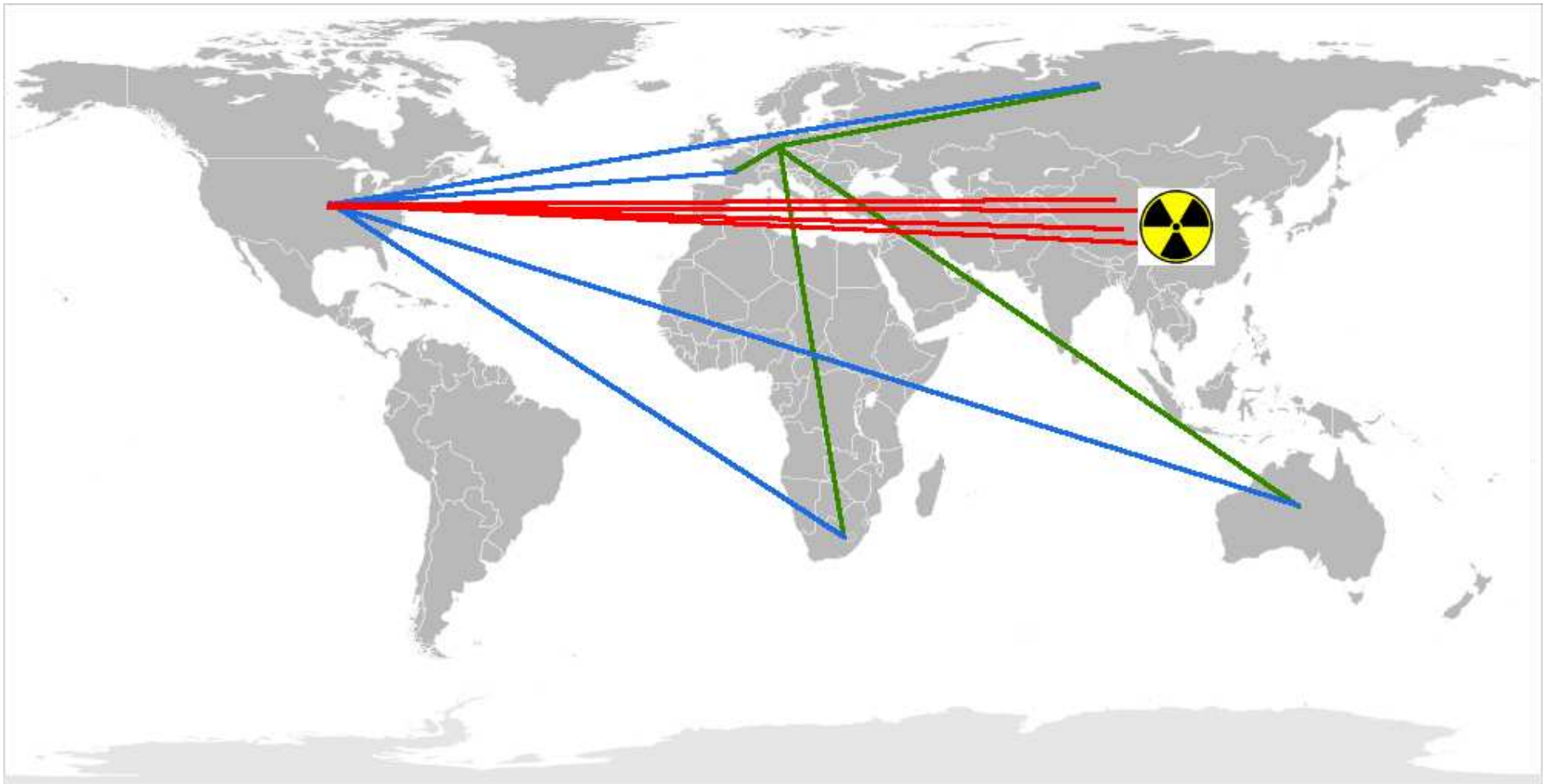
spoofed dDoS



spoofed dDoS



spoofed dDoS



Cyberwar und militärische Strategie

- Cyberwar kann ein fundamentales Paradigma ändern:
- *Es ist einfacher zu verteidigen als anzugreifen*
- Logistik, Geländekenntnisse, Nebel des Krieges
- der Verteidiger muss *alle* Systeme erfolgreich verteidigen, der Angreifer nur *eine einzige* Sicherheitslücke ausnutzen
- IT-Systeme sind zu komplex um wirklich überprüft zu werden
- NetBSD:ca. 163 000 Quelldateien, 57 228 442 LoC, 1 991 091 842 Zeichen
- Faust I: 4 600 Zeilen, 200 000 Zeichen



Die Nebel des Krieges

oder: aufblasbare Gummipanzer in Zeiten des Internets

- 1944: Alliierten ließen aufblasbare Gummipanzer in Dover aufstellen $\rightsquigarrow$ FHQ ging von D-Day-Landung in Calais aus
- Englandspiel 1942-44: Abwehr und SiPol infiltrieren holländischen Widerstand und drehen deren Funker um $\rightsquigarrow$ Abwehr steuert britischen SOE und MID

Die Nebel des Krieges

oder: aufblasbare Gummipanzer in Zeiten des Internets

- Honeypot und Honeynets: Programm, das auf einem Rechner läuft und nach außen einen anderen Rechner oder ein komplettes Netz vortäuscht
- dient ursprünglich als »Recorder« der Erforschung von Angriffen
- Deutschlandspiel 2015: Honeynet täuscht das Netzwerk des Bundestages vor, sämtliche Spionagetätigkeit darin wird aufgezeichnet

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



Lockheed Martin RQ-170 Sentinel

Beast of Kandahar



Lockheed Martin RQ-170 Sentinel

Beast of Kandahar

- Unbemanntes Flugobjekt (UAV)
- navigiert selbständig $\rightsquigarrow$ benötigt NAVSTAR GPS oder Trägheitsnavigation
- GPS ist genau aber angreifbar
- Trägheitsnavigation ist problematisch und ungenau über längere Zeiträume (Kopplung)
- Iran behauptet Hack bzw. GPS Jam, USA bestreiten den Einsatz von GPS



Navigational Satellite Timing and Ranging - Global Positioning System

- min. 24 Satelliten in 20 200 km mittlerer Bahnhöhe
- Positionsbestimmung über Triangulation gegenüber den Satelliten
- öffentliches Signal und verschlüsseltes militärisches Signal mit erhöhter Präzision
- Signalstärke -155 dBW $\rightsquigarrow$ leicht zu jammen
- Richtfunkantenne zum Satelliten
- `http://www.phrack.org/issues.html?issue=60&id=13#article`
- China fälscht/jammed systematisch GPS



Abhängigkeit/Auswirkung

- Wie abhängig sind wir vom angegriffenen System?
- Wir können es uns aussuchen!
- Die Kampfkraft einer Cyber-Waffe wird durch das angegriffene System bestimmt!



Abhängigkeit/Auswirkung

- Wie abhängig sind wir vom angegriffenen System?
- Wir können es uns aussuchen!
- Die Kampfkraft einer Cyber-Waffe wird durch das angegriffene System bestimmt!

NATO

- USA wollen konventionell gegen Cyberattacken agieren
- 14-jähriges pakistanisches Skriptkiddie kann die US Air Force mit einem Botnetz ausschalten
- dabei vorgeben ein Chinese zu sein

NATO

- USA wollen konventionell gegen Cyberattacken agieren
- 14-jähriges pakistanisches Skriptkiddie kann die US Air Force mit einem Botnetz ausschalten
- dabei vorgeben ein Chinese zu sein
- und konventionelle Gegenmaßnahmen provozieren

NATO

- USA wollen konventionell gegen Cyberattacken agieren
- 14-jähriges pakistanisches Skriptkiddie kann die US Air Force mit einem Botnetz ausschalten
- dabei vorgeben ein Chinese zu sein
- und konventionelle Gegenmaßnahmen provozieren
- von allen NATO-Mitgliedern?
- gegen China $\rightsquigarrow$ Weltkrieg?

NATO

- USA wollen konventionell gegen Cyberattacken agieren
- 14-jähriges pakistanisches Skriptkiddie kann die US Air Force mit einem Botnetz ausschalten
- dabei vorgeben ein Chinese zu sein
- und konventionelle Gegenmaßnahmen provozieren
- von allen NATO-Mitgliedern?
- gegen China $\rightsquigarrow$ Weltkrieg?



Fazit

- Cyber*war* ist übertrieben (Wirtschaftskrieg? Zickenkrieg?)
- Man kann gegenwärtig einen Gegner nicht via Internet bezwingen
- Clausewitz lesen ;-)
- Aber: unsere Gesellschaft macht sich immer mehr von IT abhängig
- Es gibt absolut keine (inter)-nationale Strategie für IT-Sicherheit
- Wir sind in einer Experimentierphase (Roter Oktober, Flame ...)

Termine

- 07.05. Bremervörde: Vom Cyber-Kriege
- 09.50. Mannheim: Vom Cyber-Kriege
- 14.05. Gold Coast/Australia: Security in a Post NSA world
- Juni: E-Businesslotsen Halle u.a. Industrie 4.0



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



- youtube.de/Sicherheitsforschung
- Twitter: 0xKaishakunin
- Xing: Stefan Schumacher