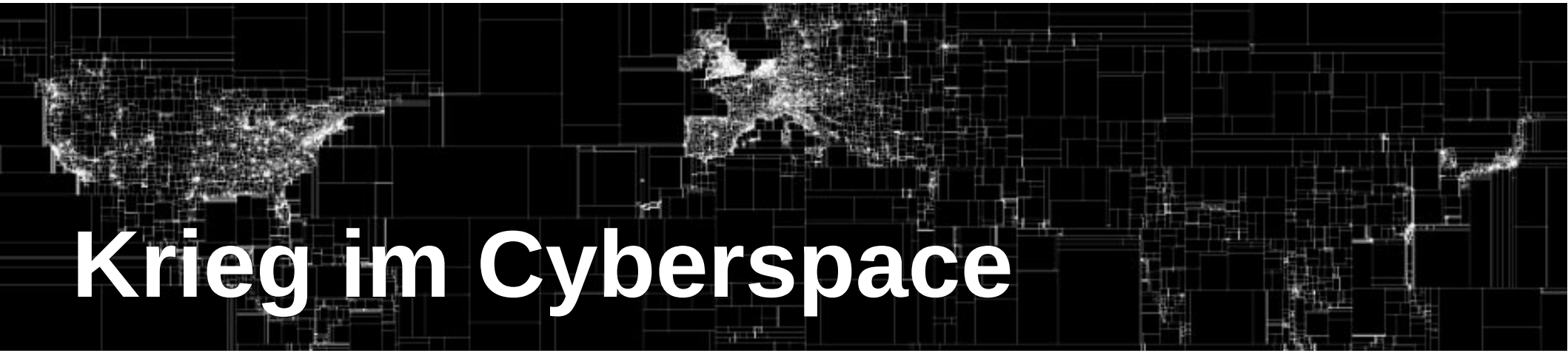


Krieg im Cyberspace

Technische und politische Aspekte der militärischen Aktivitäten im Internet

Thomas Reinhold – reinhold@ifsh.de – cyber-peace.org
IFSH - Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg

- Das IFSH
- Cyberspace, Cyberwar & Cybercrime
- Hintergründe
- Was seit Stuxnet geschah
- Probleme

Das IFSH

- Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg
- Stiftung der Stadt Hamburg 1971
- Wurzeln in nuklearer Abrüstung
- Sicherheitspolitische und naturwissenschaftliche Arbeitsbereiche
- Wissenschaftliche Forschung und Politikberatung

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

Cyberspace, Cybercrime & Cyberwar

- Cyberspace
  - Cyber Security Strategy UK (2011):

    “an interactive domain made up of digital networks that is used to store, modify and communicate information. It includes the Internet, but also the other information systems that support our businesses, infrastructure and services”
- Abgrenzung Krieg vs. Kriminalität
  - Cybercrime → Frage der internationalen Strafverfolgung
  - Cyberwar → Fragen der politischen Motivationen der Akteure
- Zentrales Problem
  - Wie unterscheidet man in dies einer konkreten Situation

Hintergründe

- Stuxnet 2010
- Politisches Nachspiel
  - Was kommt als nächstes
  - Gibt es Cyberwaffen
  - Eigene Verwundbarkeit
  - Konsequenzen für die internationale Sicherheit
- Urheber: Israel und USA*
- Belastung zwischen-staatlicher Beziehungen
  - Abschreckung
  - Rüstungswettläufe

* New York Times, 1.6.2012 „Obama Order Sped Up Wave of Cyberattacks Against Iran“

! Es geht um die **Erwartung** und **Bewertung** des Handelns von Staaten durch Staaten und um gemeinsame **Regeln**

Was seit Stuxnet geschah

- UN-Bericht zur Militarisierung des Cyberspace (UNIDIR* / CSIS*) 40 Staaten mit offensiven militärischen Cyberprogrammen
- Tallin Manual zur Anwendung des Völkerrechts im Cyberspace
- MADIANT Bericht zur chinesischen Militär-Hackereinheit PLA 61398

* UNIDIR - United Nations Institute for Disarmament Research
* CSIS - Center for Strategic and International Studies

Was seit Stuxnet geschah

- UN-Bericht zur Militarisierung des Cyberspace (UNIDIR* / CSIS*) 40 Staaten mit offensiven militärischen Cyberprogrammen
- Tallin Manual zur Anwendung des Völkerrechts im Cyberspace
- MADIANT Bericht zur chinesischen Militär-Hackereinheit PLA 61398
- Veröffentlichungen von E. Snowden zu den FIVE-Eyes und ihren Ressourcen
- Obamas Presidential Policy Directive PPD 20/2012

* UNIDIR - United Nations Institute for Disarmament Research
* CSIS - Center for Strategic and International Studies

Einige Erkenntnisse gewonnen,
viele neue Probleme aufgeworfen

Einige Erkenntnisse gewonnen, viele neue Probleme aufgeworfen

?

- Was kommt als nächstes
- Gibt es Cyberwaffen
- Die eigene Verwundbarkeit
- Konsequenzen für die internationale Sicherheit

Einige Erkenntnisse gewonnen,
viele neue **Probleme** aufgeworfen

?

Was kommt als nächstes

Gibt es Cyberwaffen

Die eigene Verwundbarkeit

Konsequenzen für die internationale Sicherheit

Geheimdienste und das Militär

- US Presidential Policy Directive PPD-20, Oktober 2012
  - Working Group aus Verteidigungsministerium und Geheimdiensten
  - "Offensive Cyber Effects Operations“ (OCEO) und Identifikation potentieller Ziele im Cyberspace „to advance US national objectives“
- General Michael Rogers (aktueller NSA-Direktor)
  - Direktor US Cyber Command mit explizit offensiver Ausrichtung
  - Direktor Central Security Service (CSS) „assistance to military crythologic community“
  - Direktor des Joint Functional Component Command – Network Warfare (JFCC-NW) → Koordination weltweiter „computer network operations“
- „Combat Mission Forces“ des US Cyber Command
  - Cyber als integraler Bestandteil aller zukünftigen Militäroperationen

Völkerrecht, Cyberattacken & Cyberwaffen

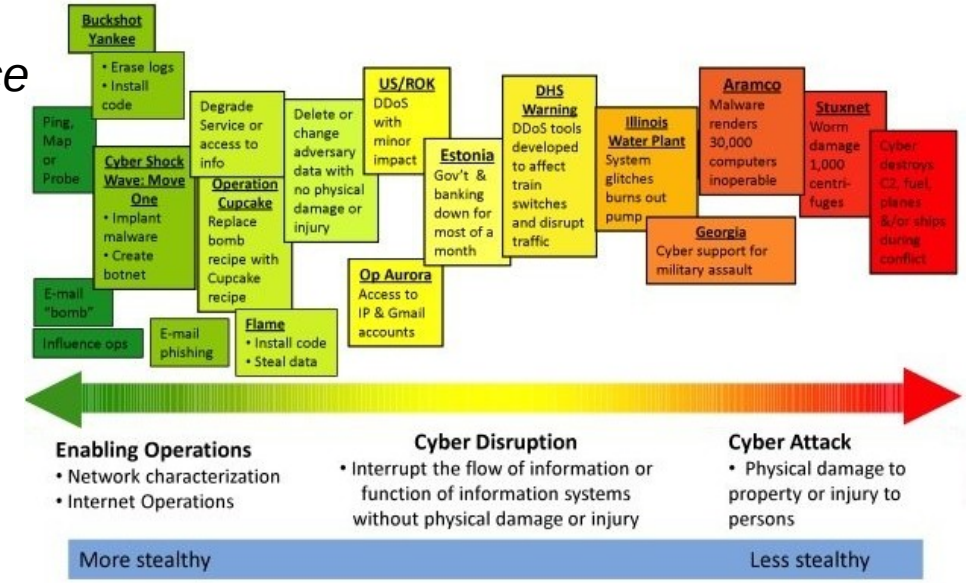
? Anwendbarkeit etablierter Normen des Völkerrechts

- Das Recht zum Krieg (ius ad bellum)
  - UN Charta Art. 2 (4) → Gewaltverzicht (“use of force”)
  - UN Charta Art. 51 → Recht zur Selbstverteidigung
- Das Recht im Krieg (ius in bello)
  - Genfer Konventionen
  - Prinzip der Proportionalität

Völkerrecht, Cyberattacken & Cyberwaffen

? Anwendbarkeit etablierter Normen des Völkerrechts

- Talin Manual (CCDCOE)
  - Analogien zu “kinetischen Wirkmitteln”
  - *Cyber activities that proximately result in death, injury, or significant destruction would likely be viewed as a use of force*
- Zur Definition von Cyberwaffen
  - OECD Studie “Reducing Systemic Cybersecurity Risk” (2010)
  - Kontinuums-Klassifikation nach Brown & Tullos



Rüstungskontrolle und Non-Proliferation

- Ausbreitung militärischer Cybermittel
  - regulieren
  - kontrollieren
  - unterbinden
- Dual-Use-Problematik
- Verifikationsmöglichkeiten oder “wie zählt man Malware”

Rüstungskontrolle und Non-Proliferation

- Ausbreitung militärischer Cybermittel
  - regulieren
  - kontrollieren
  - unterbinden
- Dual-Use-Problematik
- Verifikationsmöglichkeiten oder “wie zählt man Malware”

!

Es geht um die **Erwartung** und **Bewertung** des Handelns von Staaten durch Staaten und um gemeinsame **Regeln**

… und weitere politische Fragen

- Cyberattacken zwischenstaatlicher Akteure
- Internet Governance
  - Netzpolitik
  - Selbstregulation vs. Steuerung durch internationale Gremien (ITU)
- Freiheit vs. Kontrolle

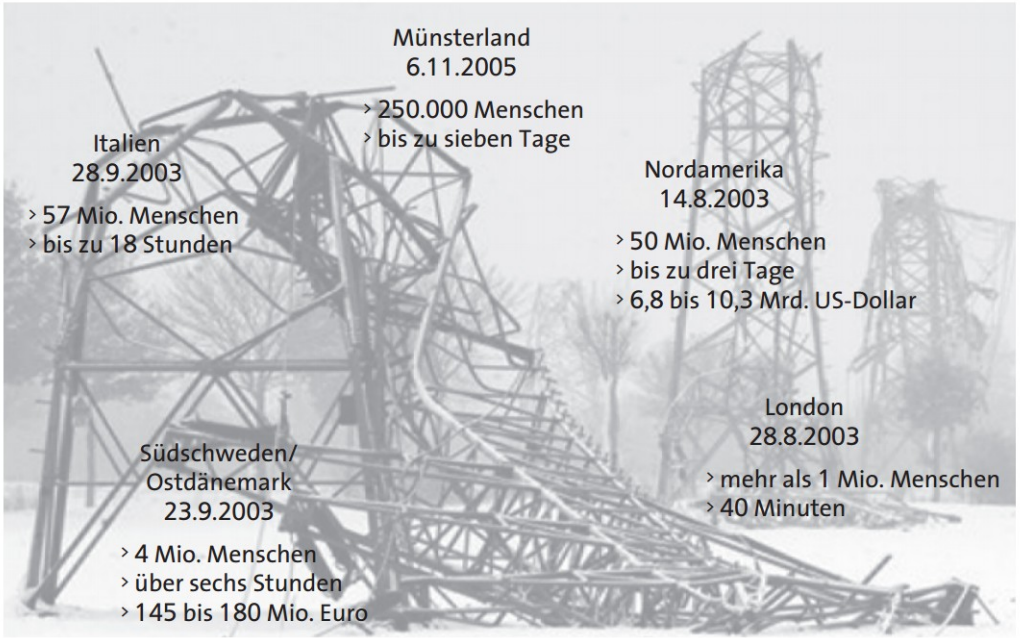
Technische Schwierigkeiten

- Das “Payload”-Problem
  - Abgrenzung zwischen Spionage und Sabotage eher eine Frage der Motivation des Akteurs als der angewandten technischen Mittel
- Attribution im Cyberspace
  - Maßgebliche Voraussetzung für Selbstverteidung UN Charta Ar.t 51
  - Möglichkeiten zur Verschleierung nur nachträglich forensisch durchschaubar
  - Madiant-Report (2013) und Abschlussbericht zu Stuxnet (2013) als Beispiele
- Einschätzung des Zerstörungspotentials von Cyberwaffen

Technische Schwierigkeiten II

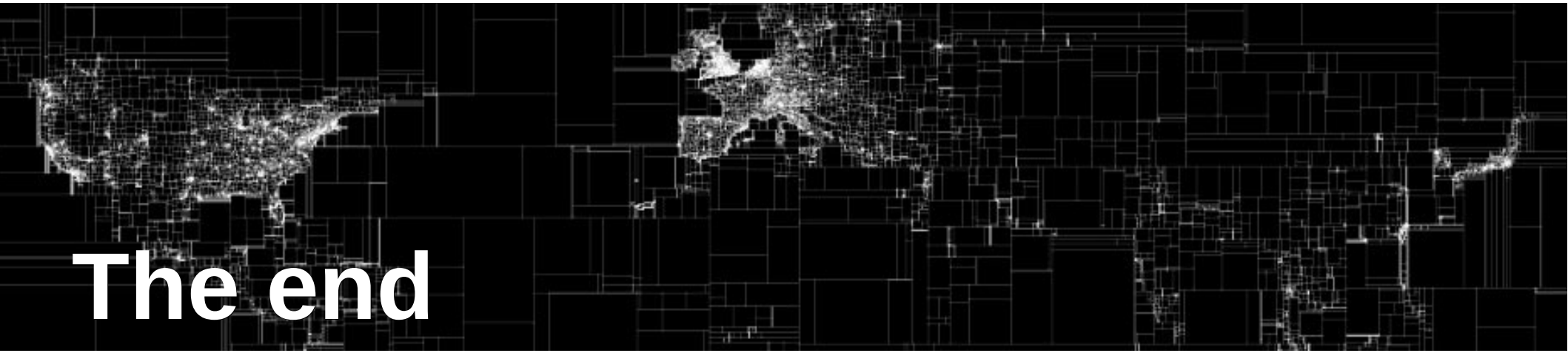
- Verwundbarkeiten
  - Embedded Systems
  - SCADA-Systeme
  - Unmittelbare und mittelbare Bedrohungen
  - Kritische Infrastrukturen
  - TAB-Studie 2011: fast keine systematischen Untersuchungen der einzelnen Bedrohungen und ihrer Auswirkungen*

ABB. 2 BEISPIELE FÜR GROSSE STROMAUSFÄLLE



Quelle: eigene Darstellung

* „Ein großräumiger und langandauernder Stromausfall: eine nationale Katastrophe“
Büro für Technikfolgenabschätzung beim deutschen Bundestag (TAB) 2011



The end

Thomas Reinhold
reinhold@ifsh.de
cyber-peace.org

Anhang: Aufwand einer militär. Cyberoperation

- Anforderungen für einen erfolgreiche Cyberattacke
  - Sehr klares und genaues Missionsziel und nötige Befugnisse
  - Spezifische Zielinformationen, i.a.R. Vorfeldaufklärung nötig
  - Unbekannte Sicherheitslücken (Zero day exploits)
  - Hochgradig professionelles Entwicklungs/Test/Angriffs-Team
  - Beständkeit des Angriffes in Qualität und Dauer
- Zeitpunkt des 1. Angriffs → Vorteil wandert zum Verteidiger
- ~ Lebensspanne einer entdeckten Lücke: 500 Stunden
- Entwicklungsaufwand eines militär. Angriffs ca. 2 bis 5 Jahre