Vertrauensbildung im Cyberspace
Möglichkeiten und Grenzen IT-basierter Ansätze

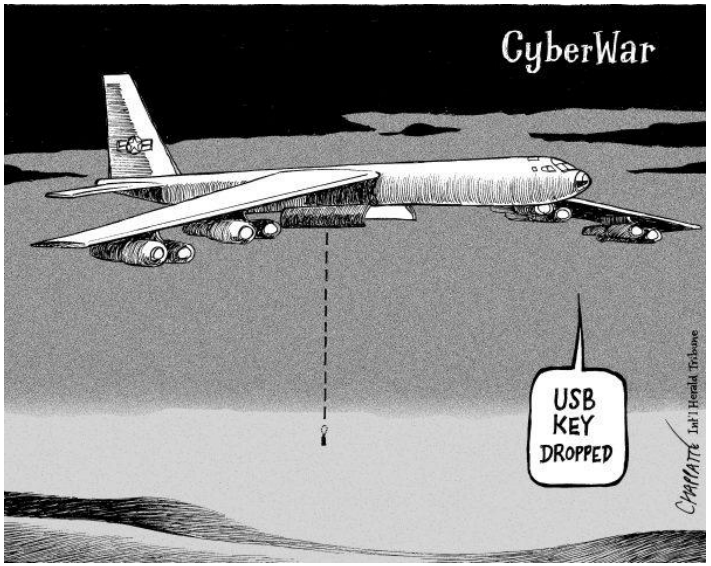
Thomas Reinhold - reinhold@ifsh.de - cyber-peace.org

Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg

Die Situation

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

- Militarisierung des Cyberspace
- Planungen für offensive Operationen
- Hacking-Back als Verteidigungsstrategie



- Beispiele
  - NATO 2016 Warschau
  - USA US Cybercommand mit ständigen "Field-Units"
  - BMVg 2016 Aufbau des Cyber-Organisationsbereiches

Das Problem

- Fehlendes international verbindliches Verständnis des Problembereiches
  - Was ist der Cyberspace
  - Was ist eine Cyberattacke
- Unklares Bedrohungspotential von "Cyberwaffen"
- Aufrüstungsspiralen und Abschreckungsdebatten

Erste internationale politische Ansätze ...

- Expertengruppen der UN und OSCE
- Tallinn-Manual des NATO Exzellenzzentrums CCDCOE*
  - Version 1.0 (2013) on the International Law Applicable to Cyber Warfare
  - Version 2.0 (2017) on the International Law Applicable to Cyber Operations
- Proposal einzelner Staaten für einen code of conduct

CCDCOE - Cooperative Cyber Defence Centre of Excellence

... und Schwierigkeiten dabei

- Spezifika des Cyberspace erschweren die Übertragung etablierter Regeln
- Abbildung nationaler Souveräntität im Cyberspace
- Das Attributionsproblem als "show stopper"
  - Zuweisung von Angriffen bestenfalls mit aufwändiger IT-Forensik möglich
  - Fehlzuweisungen und absichtlich falsche Fährten

=> Vertrauensbildende Maßnahmen als Werkzeug zur Risikoeingrenzung

=> Wie können vertrauensbildende Maßnahmen und Verifikation im Cyberspace gestaltet werden?

Die Ursachen...

- Spezifika des Cyberspace und von Software
  - Virtualität / Anonymität
  - Dezentralisierung
  - Fehlende physische Repräsentation
  - Quantifizierbarkeit
  - Duplizierbarkeit
  - Dual-Use-Charakter
- ABER: Der Cyberspace als vollständig gestaltbare Domäne

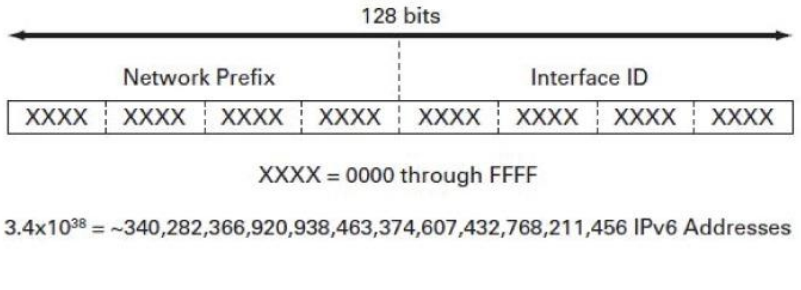
... Lösungsansätze ...

- Adaption von IT-Produkten und Verfahren für vertrauensbildende Maßnahmen und Verifikationsverfahren im Cyberspace
  - Identifikation der Kernprinzipien etablierter CBM
  - Analyse problematischer Funktionsprinzipien des Cyberspace
  - Identifikation neuer Ansätze und Verfahren auf Basis bestehender Technologien
  - Modellierung, Simulation und Evaluation im Sinne der CBM-Zielstellung

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

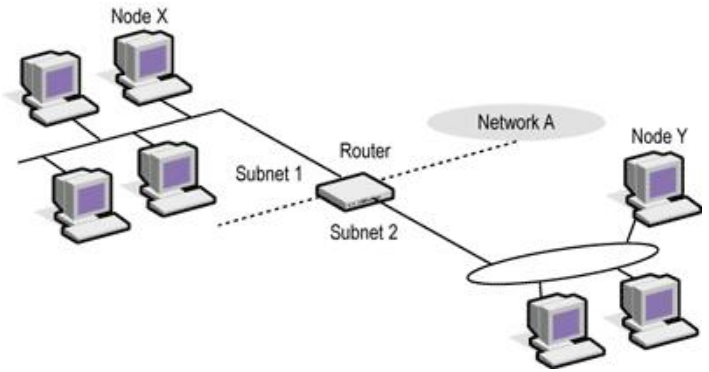
- Beispiele
  - Identifikation von Objekten: IPv6

    Eindeutige Addressierung jeglicher IT-Geräte im gesamten Internet



  - Quantifizierung und Limitierung: Kopierschutzverfahren
  - Verifikation und Kontrolle von Maßnahmen: Netzwerkdaten-Logging und Analyse

    Zugriffsmöglichkeiten für Kontrolle des Datenflusses, der Ziele und Datentypen



... und Hindernisse

- Fokus ist Gestaltungsbereich der staatliche Regulation
- Persönlichkeits- und Datenschutzrechtliche Aspekte
- Technische Voraussetzung und Betriebskosten
- Bewusstsein für Technikgestaltung in der Informatik

Ausblick

- Analoge Probleme für Verfahren der
  - Rüstungskontrolle
  - Proliferationskontrolle
  - Abrüstung
- Operationalisierung der Ergebnisse
- Publikation der konkreten Implementierungen als Best-Practice-Ansätzes