Projekt: Cyberattacks – eine neue Bedrohung für die internationale Sicherheit?

Politische und technische Möglichkeiten vertrauens-bildender Maßnahmen und der Rüstungskontrolle

Autoren: Thomas Reinhold, Götz Neuneck

Partner: UNIDIR, Auswärtiges Amt

Gliederung

- Kernfragen
- Zum Begriff „Cyberspace“
- Dimensionen der Debatte „Cyberspace“
- Motivation und Hintergrund des Forschungsprojekts
- Zentrale Fragestellungen und Ziele
- Bisherige Ergebnisse und Ausblick

Kern-Fragen

Welche **Aufrüstungmaßnahmen** im Cyberspace existieren oder sind geplant?

Welche **Bedrohungen und Konsequenzen** für die internationale Politik ergeben sich daraus?

Welche **Vorschläge zur Einhegung** künftiger Cybergefahren gibt es und wie sind sie zu bewerten?

Welche **gesellschaftlichen Akteure** können originäre Beiträge für mehr internationale Sicherheit im Cyberspace leisten?

Zum Begriff „Cyberspace“

- *EU Cybercrime Convention (2001):*

  By connecting to communication and information services users create a kind of common space, called "cyber-space"

- *Cyber Security Strategy UK (2011):*

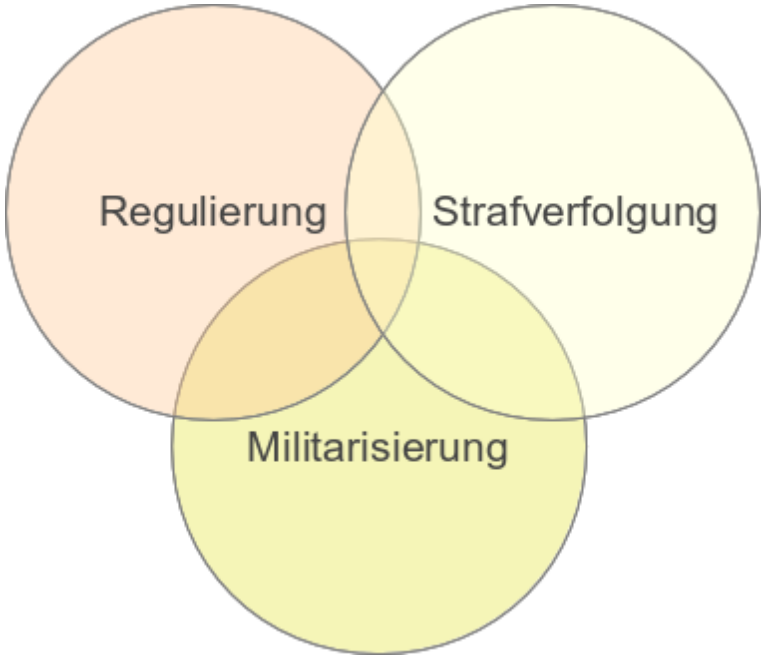
  “an interactive domain made up of digital networks that is used to store, modify and communicate information. It includes the Internet, but also the other information systems that support our businesses, infrastructure and services”

- Aus Sicht der Technik:
  - Alle vernetzungsfähigen Computer & deren Infrastrukturen
  - Alle Daten der Systeme, deren Austausch & Nutzeraktionen
  - Vom Smartphone über Server bis zum Industrierechner

Dimensionen der Debatte „Cyberspace“

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

- Regulierung: *Freiheit vs. Kontrolle*
- Strafverfolgung: *Cybercrime vs. Cyberwar*
- Militarisierung: *Aufrüstung und Bedrohungen*



Motivation und Hintergrund

- Tägliche Cyber-Attacken steigen
- Vorkommnisse mit vermutlich staatlichen Akteueren

Malware	Aktiv seit	Wirk-Ziel	Akteur
Stuxnet	06.2009	Schadwirkung iranische Atomanlagen	USA/Israel
Duqu	11.2010	gezielte Spionage IT-Strukturen	USA (?)
Flame	03.2010	„breite“ Spionage	USA
Gauss	09.2011	gezielte Spionage von Individuen	USA (?)
Rocra	05.2007	„High-target“ Spionage	Russland/China (?)

Motivation und Hintergrund II

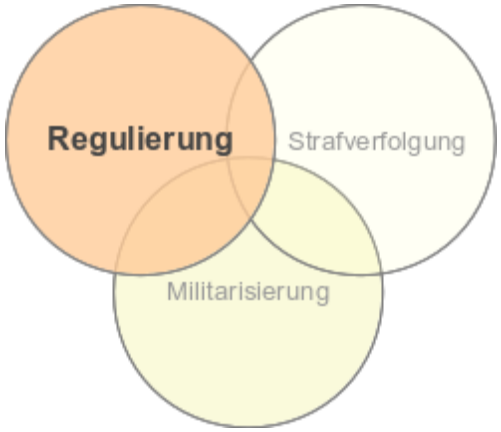
- 33 Staaten mit militärischen Cyber-Programmen in Sicherheits- und Militärdoktrinen

  (J. Lewis 2011: Cybersecurity and Cyberwarfare - Preliminary Assessment of National Doctrine and Organization)

  - USA: Department of Defence Cyber strategy (2011)
    handling the cyberspace as warfare domain (..) allows (DoD) to organize, train, and equip for cyberspace as we do in air, land, maritime, and space to support national security interests
  - Russland: Erneuerte Militärdoktrin (2010)
    (equipping the armed forces includes) "the development of the forces and means of information warfare"
  - China: White Paper on National Defence (2004)
    (*People's Liberation Army takes) „informationalization as its orientation and strategic focus"*

Fragestellungen und Ziele

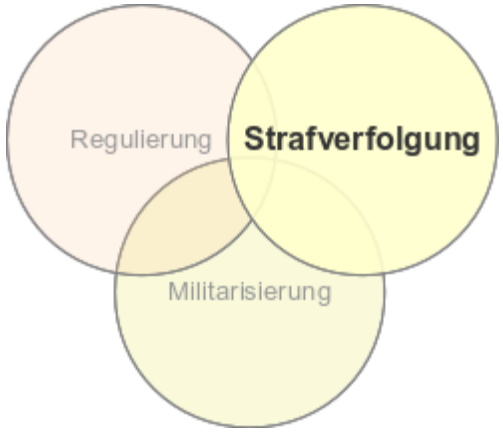
- Regulierung: *Freiheit vs. Kontrolle*
  - Analyse der (inter)nationalen Netzpolitik
  - Selbstregulation vs. Steuerung durch internationale Gremien (ITU)
  - Interviews relevanter politischer & gesellschaftlicher Akteure
    - NGOs
    - Regierungen
    - Parteien
    - Hacker
  - Workshops & Vernetzung



Fragestellungen und Ziele II

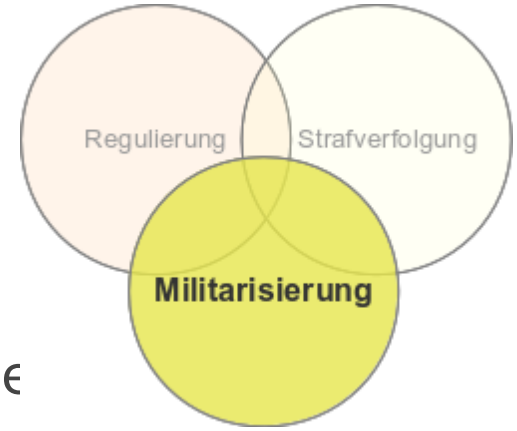
IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

- Strafverfolgung: *Cybercrime vs. Cyberwar*
  - Entwicklung von Abgrenzungen und Definitionen: Spionage, Sabotage, Attacke
  - Cyberattacken und das „Recht zum Krieg“
  - Verwundbarkeit kritischer Infrastrukturen
  - Staatliche Souveränität im Cyberspace
  - Akteure:
    - Staaten
    - ENISA
    - EUROPOL
    - UNODC



Fragestellungen und Ziele III

- Militarisierung: *Aufrüstung und Bedrohungen*
  - Analyse der Doktrinen & Vorkomnisse
  - Monitoring militärischer Programme und Folgen für die internationale Sicherheit
  - Ansätze für die Vertrauensbildung
  - Analyse spezifisch technologischer Aspekte
  - Möglichkeiten der Abrüstung & Rüstungskontrolle
  - Akteure:
    - Staaten
    - OSZE
    - NATO, weitere Verteidigungsbündnisse
    - EU



Bisherige Ergebnisse und Ausblick

- Workshops & Konferenzen
  - nationaler Kleinworkshop zu neuen Bedrohungen 2010
  - Mitorganisation „Challenges in Cyber Security – Risks, Strategies, and Confidence-Building“, Auswärtiges Amt 2011
  - Vorträge bei UNIDIR
- Berichte und Forschungspublikationen
  - Konferenzbericht zur Tagung im Auswärtigen Amt 2011
  - UNIDIR-Bericht „Cyber Warfare: Legal Frameworks and Constraints and Perspectives for Transparency and Confidence Building”
  - Friedensgutachten 2012
  - IFSH-Working Paper Nr. 18 „Like and Strike“

Bisherige Ergebnisse und Ausblick II

- Entwicklung eines Forschungsprogramms und Antragstellung bei der Gerda-Henkel-Stiftung
- Ausblick 2013
  - Working Paper „Bedrohungen, internationale Akteure und militärische Aktivitäten im Cyberspace“
  - Beitrag und Präsentation des UNIDIR Jahrbuch „Cyber Security Index“
  - Publikation „Technische Aspekte der Vertrauensbildung im Cyberspace“
  - Kleinere Veröffentlichungen und Masterarbeiten
  - Konferenz-Beiträge und Vernetzung
  - Beteiligung Ringvorlesung