Möglichkeiten und Grenzen technischer Maßnahmen zur Sicherheits- und Vertrauensbildung im Cyberspace

Thomas Reinhold
reinhold@ifsh.de

Logo: FIfF

IFSH - Institut für Friedensforschung
und Sicherheitspolitik an der Universität Hamburg

Gliederung

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

- Zum Hintergrund und Ziel des Vortrags
- Einführung zu vertrauensbildenden Maßnahmen
- Vertrauensbildende Maßnahmen im Cyberspace
- Technische Möglichkeiten und Ansätze der Vertrauensbildung
- Grenzen technischer Ansätze
- Diskussion

Hintergrund und Ziel des Vortrags

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

- Militärische Aufrüstung im Cyberspace
- Verankerung des Cyberspace in Militärdoktrinen
- Unklare Bedrohungen
  - Verwundbarkeit kritischer Infrastrukturen
  - Zerstörungspotential von Cyberwaffen
  - Aufrüstungsumfang

→ Vertrauensbildende Maßnahmen sind wichtig

→ Technische Möglichkeiten sondieren

→ Impulsvortrag und Diskussion

CBM - Vertrauensbildende Maßnahmen

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

- Confidence building measures - CBM
  - Konzept in den 70'er Jahren im Rahmen der KSZE entwickelt
  - Glaubhaft die Abwesenheit von Bedrohungen demonstrieren
  - Unsicherheiten über Absichten der gegenerischen Seite verringern
  - die Möglichkeiten eingrenzen, in Krisensituationen Druck durch militärische Aktivitäten auszuüben
  - Kommunikation in Krisenzeiten verbessern
  - allgemeine Transparenz bzgl. Aufgaben, Strategien, Stärke und Doktrinen der Streitkräfte herstellen

CBM - Vertrauensbildende Maßnahmen

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

- UN Disarmament Commission guidelines for CBMs:

*"to **reduce** and even **eliminate** the causes of **mistrust, fear, misunderstanding and miscalculations** with regard to relevant military activities and intentions of other States" (..)*

*"to help to **prevent military confrontation** as well as covert preparations for the commencement of a war, to reduce the **risk of surprise attacks and of the outbreak of war by accident**."*

General Assembly, Special Report of the Disarmament Commission to the General Assembly at its Third Special Session Devoted to Disarmament, UN document A/S-15/3, 28 May 1988, pp. 28–33.

CBM – Typen und Kategorien

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

- Einteilung nach Akteuren und Verhandlungsebenen (Staaten, Militär, Zivilgesellschaft ...)
- Einteilung nach Art der Maßnahme

Kategorie	Maßnahme
Geografisch	Demilitarisierte Zonen
Strukturell	Defensive Orientierung von Streitkräften
Operationell	Begrenzung militärischer Übungen & Manöver
Deklaratorisch	Verzicht auf den „First use“ von Waffen
Informatorisch	Seminar zu Doktrinen, Informationsaustausch, Etablierung von Kommunikationskanälen
Verfikation	Überwachung per Sensoren, Inspektionen

CBM im Cyberspace – Warum?

- *It makes sense "to take this on right now (..) Other countries are preparing for a cyberwar. If we're not pushing the envelope in cyber, somebody else will."* Richard M. George, former NSA cyber defense official
- 33 Staaten mit offensive militärischen Cyber-Programmen in Sicherheits- und Militärdoktrinen (J. Lewis 2011: Preliminary Assessment of National Doctrine and Organization, UNIDIR)
- Cyberspace als weitere militärisch relevante Domäne
- Aufrüstungsprogramme
  - Plan X (DARPA) 1.54 Mrd. $ von 2013 bis 2017 für „cyber-offense"
  - US Cyber Command: 4000 zusätzliche Mitarbeiter
  - ...

CBM im Cyberspace – Analogien

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

- CBM nach Kategorien:

Kategorie	Maßnahme
Geografisch	…
Strukturell	Defensive Orientierung von Streitkräften
Operationell	Begrenzung militärischer Übungen & Manöver
Deklaratorisch	Verzicht auf den „First use“ von Waffen
Informatorisch	Seminar zu Doktrinen, Informationsaustausch, Etablierung von Kommunikationskanälen
Verfikation	…

CBM im Cyberspace – Ansätze I

- Erste „Best practise“ Maßnahmen
  - Seminare und Workshops zu Cyberdoktrinen und Definitionen
  - Gemeinsame (militärische) Übungen: Cyber europe 2010/2012, China-US-Wargames 2012
  - Aufbau von Datenaustauschknoten auf internationalem Level
  - Capacity Building
- Deklaratorische Ansätze: NATO CCDCOE Tallinn Manual ...
- Etablierung von nationalen Meldepflichten zu Cybervorfällen

CBM im Cyberspace – Ansätze II

- Technische Maßnahmen
  - Cyberspace vollständig “man made domain”
  - Technische Funktionen und Bedingungen definiert von:
    IRTF - Internet Research Task Force
    IETF - Internet Engineering Task Force
    ICANN - Internet Corporation for Assigned Names and Numbers
    IANA - Internet Assigned Numbers Authority
  - RFCs und Protokolle als Regelwerke des Cyberspace

CBM im Cyberspace – Ansätze III

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

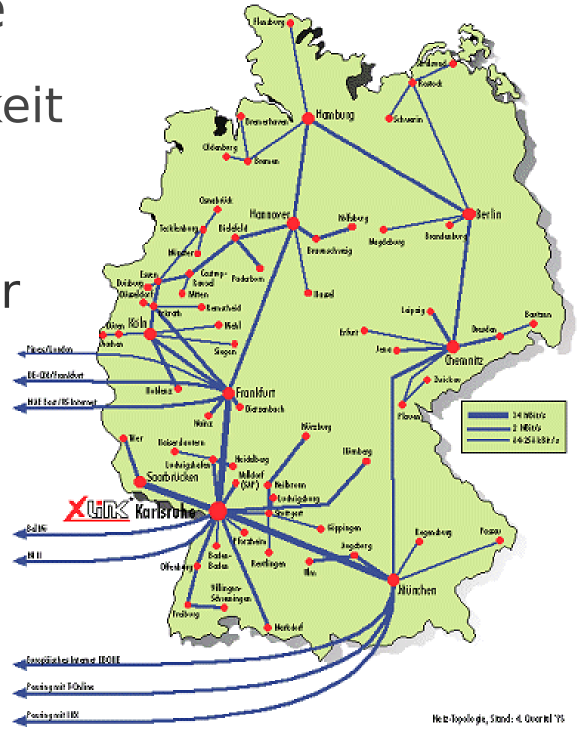
- Nebenbedingungen
  - Datenschutz & Menschenrechte
  - Netzpolitische Fragen
  - Individuell politische Interessen
- Unterschiedliche Verhandlungsebenen
  - unilateral
  - bilateral
  - Bündnisse
  - Internationale Abkommen

Technische Ansätze - Staatsgrenzen

- Nationalstaatliche Grenzen im Cyberspace
  - Staatliche Souveränität und Verantwortlichkeit
- Internet: ein Netz aus Netzen
  - Betreiber meist privatwirtschaftliche Anbieter
  - „Border-Router“ an der Verbindungs-punkten zwischen Netzen
  - Jeder Rechner hat eine geographischen Ort

→ Ansatzpunkt für Grenzen im Cyberspace

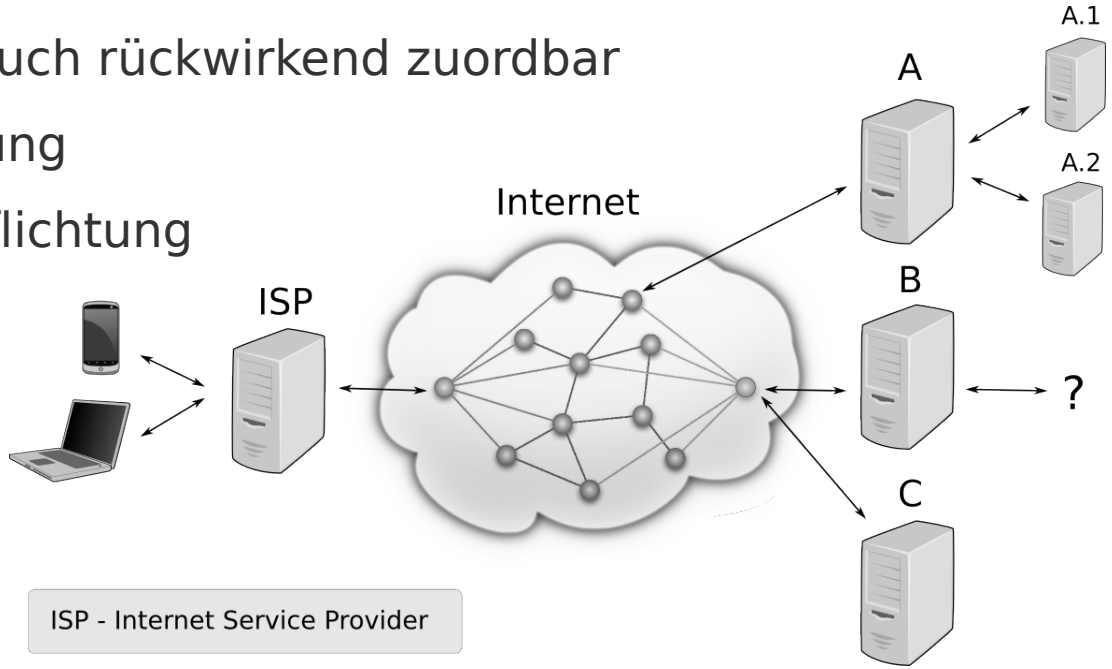
  - Unilateraler Ansatzpunkt
  - Internationale Harmonisierung möglich



Technische Ansätze - Verbindungsdaten

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

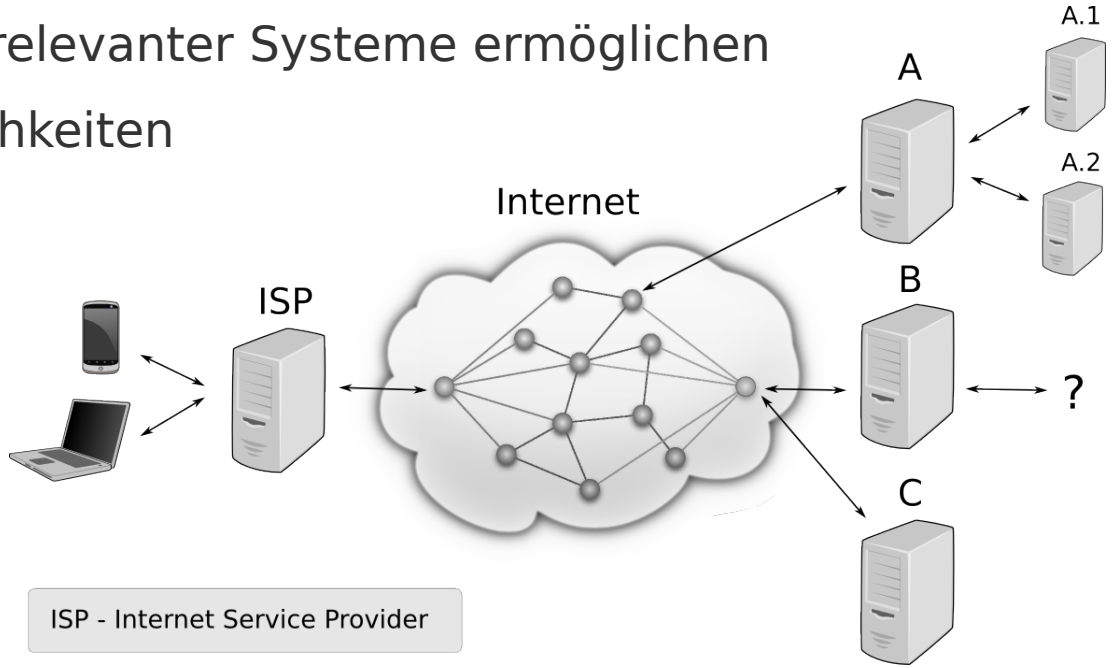
- Attribution von Angriffen
  - Recht auf Selbstverteidigung nach dem „ius ad bellum“
  - nachträgliche Rückverfolgung zur Herkunft eines Angriffs
- Speicherung von Daten über Netzwerkverbindungen
  - Verantwortlichkeiten auch rückwirkend zuordbar
  - Geographische Verortung
  - unilaterale Selbstverpflichtung zur Datenspeicherung
  - internat. Richtlinie



Technische Ansätze - Logdaten

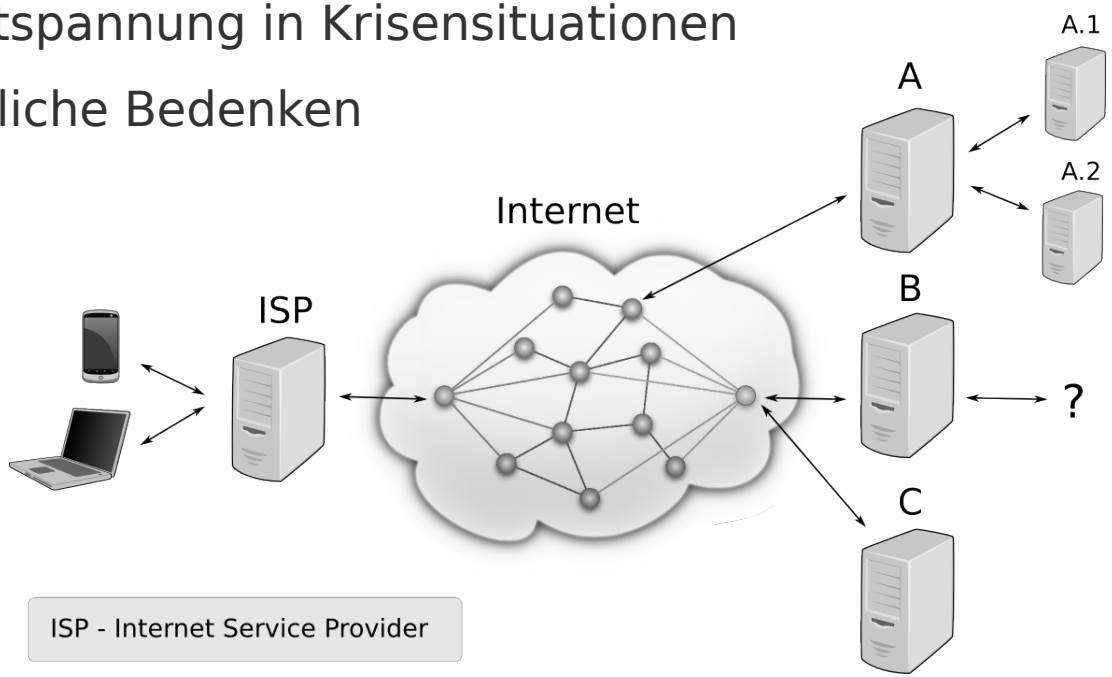
IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

- Log-Daten für detailierte Aktivitätsanalyse
  - Logdaten umfassen Zugriffe, Verbindungen, u.U. Datenzugriffe etc.
  - Detailiertes Abbild der Nutzerinterkationen mit einem System
  - Selbstverpflichtung zur Log-Daten-Speicherung
  - Zugriff auf Log-Daten relevanter Systeme ermöglichen
  - externe Kontrollmöglichkeiten
  - Unilaterale, Bilaterale & internat. Maßnahme



Technische Ansätze - DPI

- DPI – Deep Packet Inspection
  - Mittel zum „laufenden” Durchleuchten von aktuellen Netzwerk-Verbindungen und deren Inhalte (übertragende Daten)
  - Nur für relevante Netzwerke (Militär etc.) geeignet
  - Mittel für bilaterale Entspannung in Krisensituationen
  - Starke menschenrechtliche Bedenken



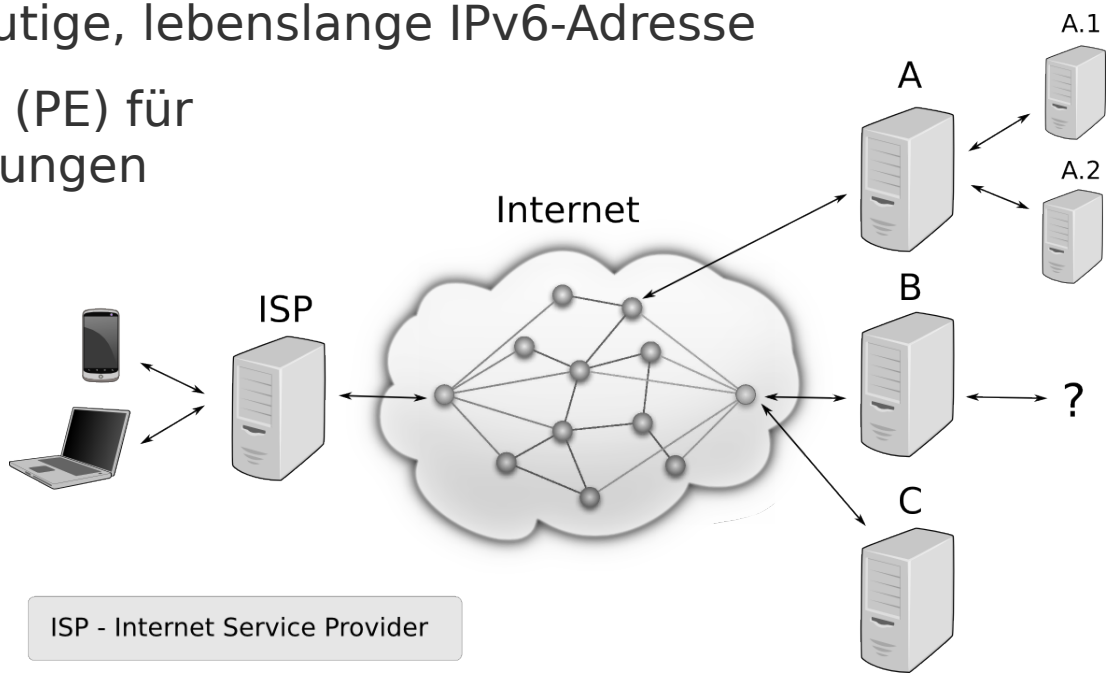
Technische Ansätze – Neutrale Zonen

- Genfer Konventionen 1949
  - Unterscheidung zwischen zivilen & militärischen Objekten/Personen
  - Einführung von Schutzzeichen für Personen und Gegenstände die neutral oder im Sinne der Genfer Konventionen im Einsatz sind
- Neutrale & zivile Computersystem identifizierbar machen
  - Nutzung der eindeutigen Adressen (Hardware-, IP-Adressen)
  - Abgleich gegen international gepflegte Liste
  - Schutz kritischer Infrastrukturen
  - Schutz vor „zufälliger“ Zerstörungen
- Internationale Maßnahme - Konvention nötig

Technische Ansätze – IPv6

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

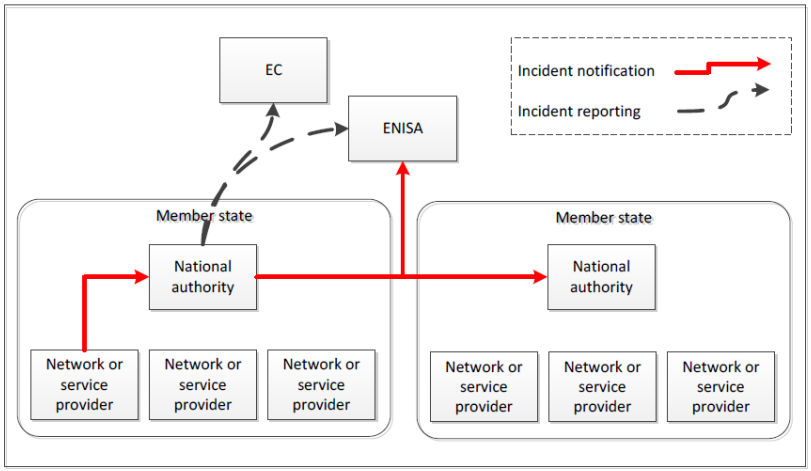
- Eindeutige weltweite Identifizierbarkeit von Computern
  - Nummernvergabe für Identifikation von Computern & Netzen
  - IPv4 → Adressen knapp → keine eindeutige Adresse je Gerät
  - IPv6 → $3{,}4*10^{38}$ Adressen verfügbar, theoretisch jedes Endgerät und jede Person eindeutige, lebenslange IPv6-Adresse
  - IPv6-Privacy Extension (PE) für anonymisierte Verbindungen
  - Unilaterale Selbst-verpflichtung IPv6 ohne PE einzusetzen



Weitere Ansätze – CERTs

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

- Austauschstrukturen zu Vorkomnissen und Problemen
  - CERT – Computer Emergency Response Team
  - Konzept für klare Etablierung, Hierarchisierung und Formalisierung
  - Austauschstrukturen auf internationaler Ebene ausbauen
  - bilaterale Maßnahme mit Erweiterungspotential auf Bündnisse



ENISA: Reporting-Schema nach Art. 13a

	1h<…<2h	2h<…<4h	4h<…<6h	6h<…<8h	>8h
1%<…< 2% of users					
2% < …< 5% of users					
5% <…< 10% of users					
10% <…<15% of users					
> 15% of users					

Table 1 Combination of thresholds

Weitere Ansätze – Non-Proliferation

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

- Markt für maßgeschneiderte Lösungen von Cyberwaffen
  - Vorfälle mit Spionage und Überwachungstools
  - Ausschreibung von General Dynamics, Ft. Meade, 2012 *„Exploit development of Microsoft Windows operating systems, Exploit development of Linux operating systems i. Exploit, development of personal computer device/mobile device operating systems“*
- Kontrolle durch Export-Vorbehalte
  - Benötigt klare nationale/internationale Normen zu Cyberwaffen
  - Klassifikation nach Schaden, Wirkungsdauer, Zielgerichtetheit etc.
  - Unilaterale Maßnahme, auch internationale Konvention möglich

Grenzen technischer Ansätze

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

- CBM basieren auf Verlässlichkeit der Partner
- Erfolg der Maßnahmen hängt oft an staatlicher Kooperationsbereitschaft
- Geheime Entwicklungen trotzdem nicht zu entdecken
- „Cloud“-Computing und die Frage, wo genau die Daten liegen
- Verschlüsselungs- und Anonymisierungsdienste
- Internationale Kooperationsbereitschaft bei allen technischen der Netzprotokolle und Netzstrukturen
- Datenschutz- / Menschenrechtliche Bedenken

Diskussion

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

*"to **reduce** and even **eliminate** the causes of **mistrust, fear, misunderstanding and miscalculations** with regard to relevant military activities and intentions of other States" (..) "to help to **prevent military confrontation** as well as covert preparations for the commencement of a war, to reduce the **risk of surprise attacks and of the outbreak of war by accident**."*

Wie können technische & technik-basierte Maßnahmen:

- Staatlich destabilisierende Aktivitäten eingrenzen ?
- Reichweite und das Zerstörungspotential von Aktivitäten klären ?
- Zwischenstaatliche Kontrolle ermöglichen ?

Welche Akteure und Verhandlungsebenen sind jeweils geeignet (unilateral, bilateral, Verteidigungs-Bündnisse, international)?