# Über die Militarisierung des Cyberspace

## Herausforderungen und Möglichkeiten einer friedlichen Entwicklung

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

- Vorstellung
- Ein Blick zurück
- Stand der Dinge
- Herausforderungen und Gefahren des Cyberspace
- Neue Probleme und alte Konzepte
- Politische und technische Lösungsansätze
- Diskussion

# Vorstellung

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

IFSH
Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg

ifsh.de

- Über mich
  - Dipl. Informatiker, Vertiefung Künstliche Intelligenz und Psychologie
  - Fellow am IFSH
  - Datenbank/Blog cyber-peace.org

# Ein Blick zurück

# Stuxnet

- 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“

# Was seit damals geschah

- UN-Bericht zur Militarisierung des Cyberspace 2013 (UNIDIR* / CSIS*) 40 Staaten mit offensiven militärischen Cyberprogrammen
- Tallinn Manual zur Anwendung des Völkerrechts und des humanitären Rechtes im Cyberspace
- Expertengruppen: UN GGE, OSCE ...

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

# Was seit damals geschah

- UN-Bericht zur Militarisierung des Cyberspace 2013 (UNIDIR* / CSIS*) 40 Staaten mit offensiven militärischen Cyberprogrammen
- Tallinn Manual zur Anwendung des Völkerrechts und des humanitären Rechtes im Cyberspace
- Expertengruppen: UN GGE, OSCE ...

- EternalBlue und seine Kinder
- Obamas Presidential Policy Directive PPD 20/2012
- Kommando CIR / Bundeswehr

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

## Erkenntnisse gewonnen aber auch neue Probleme aufgeworfen

?

- Offensive invasive Schadsoftware (“Cyberwaffen”)
- Cyberspace als zusätzliche militärische Domäne
- Eigene Verwundbarkeiten
- Konsequenzen für die internationale Sicherheit

## Erkenntnisse gewonnen aber auch neue Probleme aufgeworfen

?

- Offensive invasive Schadsoftware (“Cyberwaffen”)
- Cyberspace als zusätzliche militärische Domäne
- Eigene Verwundbarkeiten
- Konsequenzen für die internationale Sicherheit

# Stand der Dinge

# Stand der Dinge

- UN Institute for Disarmament Research „The Cyber Index - International Security Trends and Realities“, 2013
  - 47 Staaten mit militärischen Cyberdoktrinen,
    10 Staaten mit explizit offensiven Programmen
- Deutschland

  - Bundeswehr: "Kommando Cyber & Informationsraum" (CIR)
    (Aufbau bis 2021 abgeschlossen, bis zu 21.000 Dienstposten)
  - BMVg: Neue Abbteilung Cyber/ IT (CIT)
  - Bundeswehr Universität München: Neues Cyberforschungszentrum,
    neue Professurenund internationaler Master-Studiengang "Cybersicherheit"
  - BMI: ZITiS - Zentrale Stelle für Informationstechnik im Sicherheitsbereich mit u.a. Bundeswehr als Kunde, "Zwischenhändler" für Sicherheitslücken ?

# Stand der Dinge

- USA
  - US Cybercommand, demnächst auch als eigenständige Militäreinrichtung
- Russland
  - 2017 Einrichtung "Abteilung für Informationssicherheit und Cyberabwehr"
- China
  - APT1 / Militäreinheit 61398  in Beijing
  - Cyberfähigkeiten bislang eher bei Spionage / Datendiebstahl
- Nordkorea
  - UNIT 180, Mutmaßungen bzgl. WannaCry, Zentrabank-Hack von Bangladesh
- NATO
  - Cyberattacken seit 2016 Bestandteil von Artikel 5 und kollektiver Verteidigung

# Herausforderungen und Gefahren des Cyberspace

# Herausforderungen und Gefahren

- Anhaltender Trend der Digitalisierung
  - Gesellschaftliche, wirtschaftliche und politische Konsequenzen
  - Vernetzung von System schafft Abhängigkeiten
- Gefährung und Schutz kritischer Infrastrukturen
- Management staatlicher und gesellschaftlicher IT-Security
- Internet Governance – Wer bestimmt die Regeln im Cyberspace
- Freiheit vs. Kontrolle
- Neue Akteure durch “billige” Cyberwaffen ?

# Probleme staatlichen Agierens im Cyberspace

- Interesse von Nachrichtendienste vs. allgemeine IT-Sicherheit
  - Handel mit Sicherheitslücken
  - EternalBlue-Vorfall und das Sammeln von Sicherheitslücken
- Unterwanderung durch Dominanz einzelner Staaten und internationaler Unternehmen
- Abgrenzung von Defensive und Offensive
- Wieviel Wirken in fremde Netz ist zulässig
- Parlamentsvorbehalt im Cyberspace ?

# Neue Probleme - alte Konzepte

# Cybercrime vs. Cyberwar

- Cybercrime

  → Fragen nach Regelungen der internat. Strafverfolgung

- Cyberwar

  → Fragen nach den politischen Motivationen der Akteure
  → Fragen nach der Bewertung von Vorfällen

- Zentrales Problem:

  Welches Ausmaß einer nationalen Beeinträchtigung durch externe Cyberzugriffe entspricht einem kriegerischen Akt

# Völkerrecht & Cyberspace

- Was ist der „Cyberspace”
  - Informationssicherheit (Proposal Russland/China an die UN 2013)
  - Cybersicherheit (USA/Europa)
- Was sind „Cyberwaffen”
  - Vergleich zu analogen Waffen und situationsbezogene Vorfall-Bewertung

    *“A weapon is - directed force - its release can be controlled, there is a reasonable forecast of the [actual] effects it will have, and it will not damage the user, his friends or innocent third parties”*
  - Bewertung innerhalb eines Schadens-Spektrums, “kritische Schwelle” bei Schädigung von Objekten oder Personen
  - Bewertung anhand juristischer und strategischer Dimensionen:
    > Anwendungs-Kontext und Vermeintlicher Zweck
    > Beabsichtigter Schaden
    > Konkrete absichtsvolle Auswahl eines strategisch relevanten Ziels

# Völkerrecht & Cyberspace /2

- Anwendbarkeit etablierter Normen des Völkerrechts ?
- „Tallinn Manual“
  - NATO Exzellenz-Zentrum CCDCOE
    (NATO Cooperative Cyber Defence Centre of Excellence)
  - Analyse von Völkerrechtlern, Militärwissenschaftlern und militärischen Mitarbeiten
  - Analogien zu “kinetischen Wirkmitteln”
  - *Cyber activities that proximately result in death, injury, or significant destruction would likely be viewed as a use of force*
  - *Civilians are not prohibited from directly participating in cyber operations amounting to hostilities, but forfeit their protection from attacks for such time as they so participate.*

# Technische Schwierigkeiten

- Das “Payload”-Problem
  - Abgrenzung zwischen Kriminalität, 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
- Territoriale Souveränität und Grenzen im Cyberspace
- Duplizierbarkeit
- Weltweiter Markt von Sicherheitslücken („Waffenmaterial“)
- Abgrenzung von Offensive und Defensive

# Rüstungskontrolle und Non-Proliferation

- Ausbreitung militärischer Rüstungsgüter / kritischer Bestandteile
  - regulieren
  - kontrollieren
  - unterbinden
- Dual-Use-Problematik
- Virtualität & Immaterialität
- Problem der Quantifizierbarkeit oder “wie zählt man Malware”
- Verifikationsmöglichkeiten

# Politische und technische Lösungsansätze

# Vertrauensbildende Maßnahmen

- C(S)BM - Confidence (and security) building measures
  - Konzept in den 70'er Jahren im Rahmen der KSZE* entwickelt
  - Glaubhaft die Abwesenheit von Bedrohungen demonstrieren
  - Unsicherheiten über Absichten der gegnerischen Seite verringern
  - Eingrenzung der eigenen Möglichkeiten, in Krisensituationen Druck durch militärische Aktivitäten auszuüben
  - Kommunikation in Krisenzeiten verbessern
  - Transparenz über Aufgaben, Stärke und Doktrinen der Streitkräfte herstellen
- Maßnahmen
  - Seminare zu Sicherheit/Verteidigungs-Doktrinen
  - Defensive Orientierung von Streitkräften, Verzicht auf den „First use“
  - Demilitarisierte Zonen
  - Gemeinsame militärische Übungen
  - Bilaterale Vereinbarungen bis zu internationalen Abkommen

# Vertrauensbildende Maßnahmen /2

- Monitoring als wichtiger Bestandteil von CSBM
  - Signal der Verbindlichkeit
  - Verifikationsmöglichkeiten der Partner
- Etablierte Ansätze für bisherige waffenfähige Technologien
  - Genehmigungspflichten, Staatshoheit über Produktion, Import und Export gefährlicher Güter
  - Exporte/Importe an Partner oder öffentlich Datenbanken melden bspw. UN-COMTRADE*
  - Beschränkung auf maximale Mengen bestimmter Güter/Schlüsseltechnologien
  - Markierungen von Waffen für Rückverfolgbarkeit
  - Sensorik bspw. für geheime unterirdische Atomwaffentests
  - Möglichkeit der (unangekündigten) Inspektionen bspw. IAEA**

* COMTRADE - United Nations Commodity Trade Statistics Database - comtrade.un.org
** IAEA - International Atomic Energy Agency

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

!

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

# Ansätze für den Cyberspace – Politik

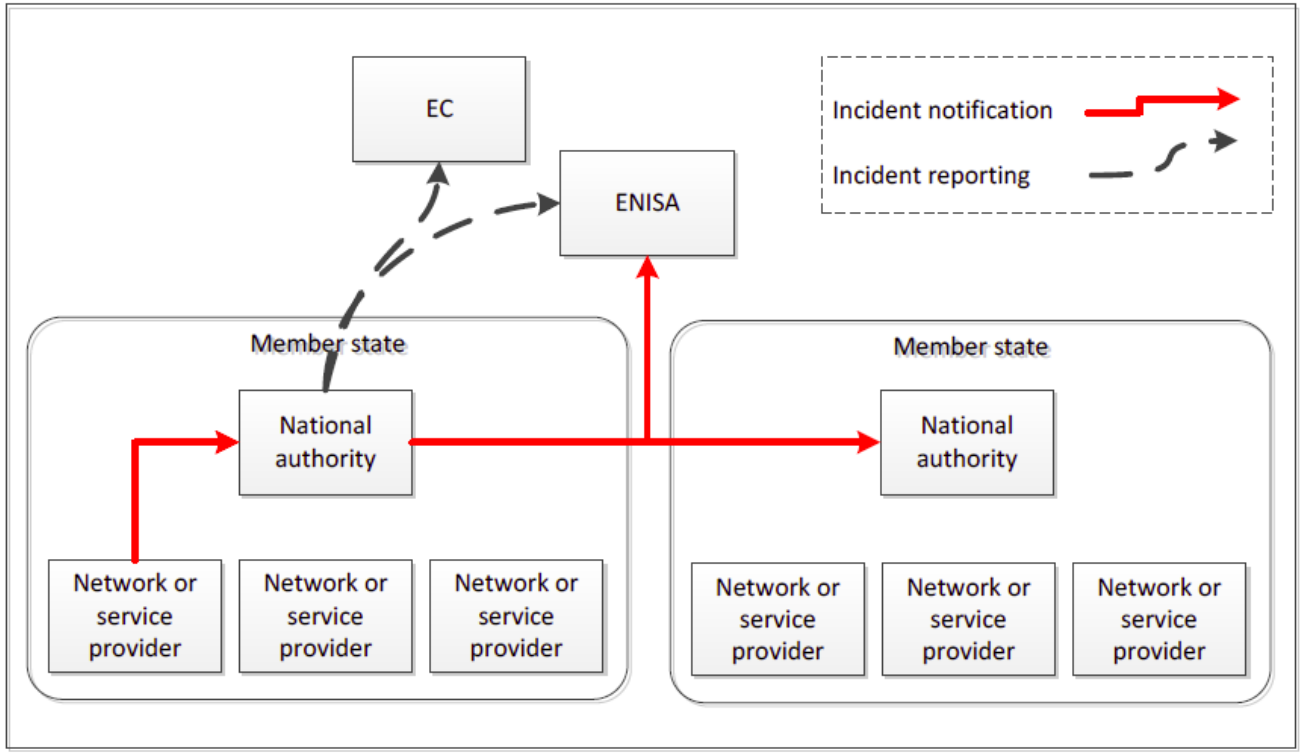
- Politische Ansätze
  - Verständigung auf gemeinsame Terminologie und Definitionen
  - Gemeinsame Arbeitsgruppen
  - Gemeinsame Krisenübungen
  - Meldepflichten für Unternehmen bei Cyberattacken
  - Regulierung des Handels sowie den Umgang mit Schadsoftware/Sicherheitlücken
  - Transparenz und Monitoring bei Cyberwaffen

# Ansätze für den Cyberspace – Praxis

- Praktische Ansätze
  - Ausbau von CERTs*

    > Nationale Melde- und Eskalationshierarchien

    > Internationale Schnittstellen für Austausch Sicherheitslücken und Vorfälle




* CERT - Computer Emergency Response Team

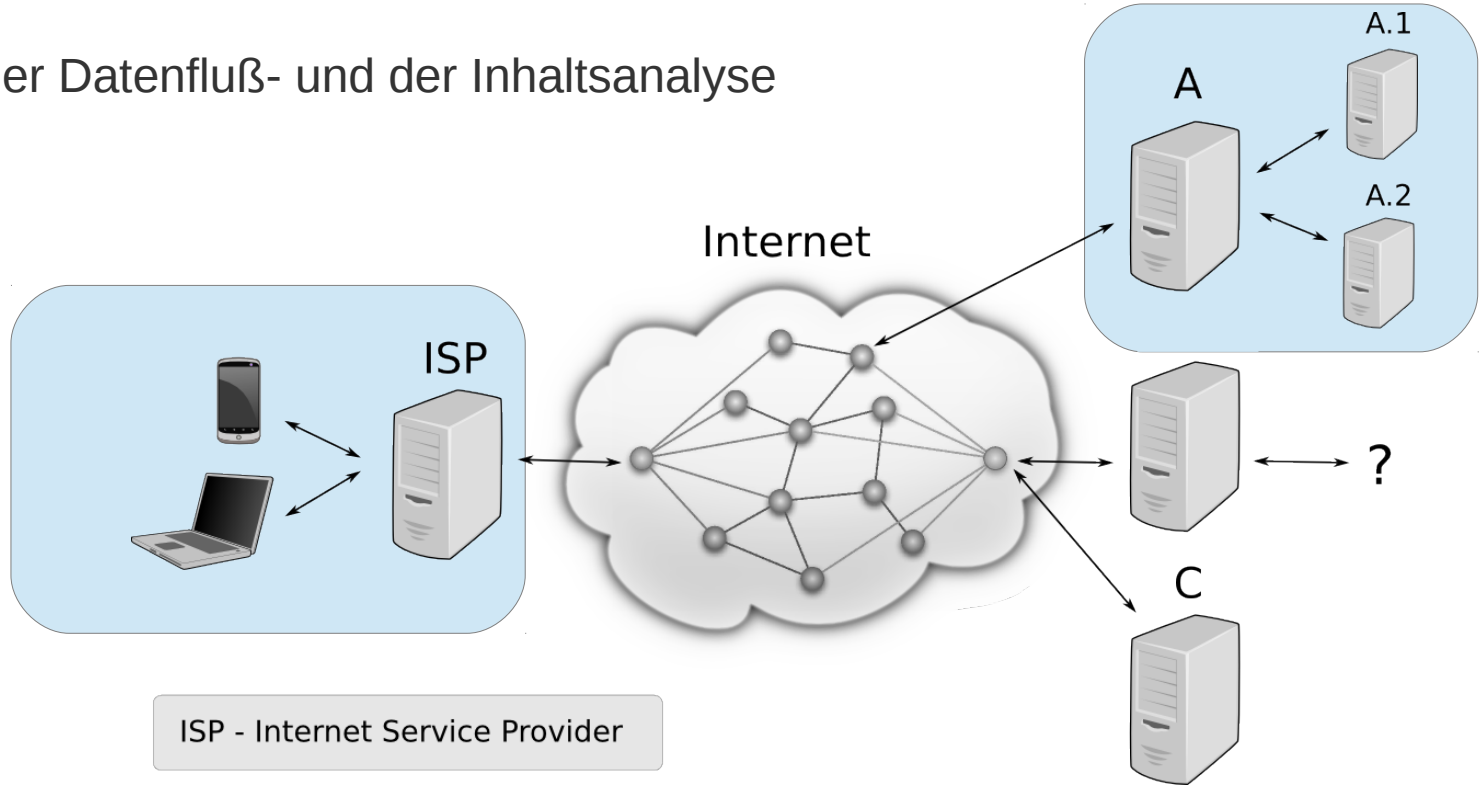
# Ansätze für den Cyberspace – Praxis /2

- Mögliche praktische Ansätze
  - Speicherung / Austausch / Sichtung von Verbindungsdaten

    > Unilaterale Selbstverpflichtung zur Transparenz

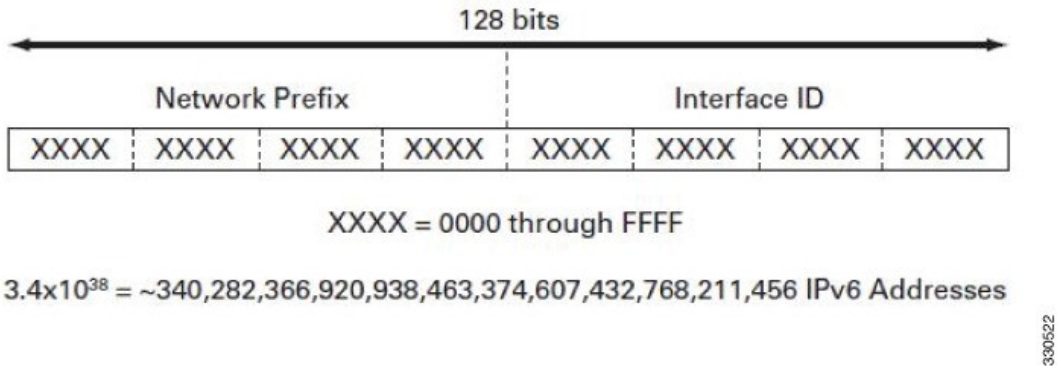
    > Überwachung der defensiven Orientierung von Cyberprogrammen

    > Rückverfolgung ungewöhnlicher Aktivitäten
  - Maßnahmen der Datenfluß- und der Inhaltsanalyse



# Ansätze für den Cyberspace – Fiktion

- Cyberspace als einzigartige “man made domain”
- Ideen für weitere technische Ansätze
  - Grenzen und Verantwortlichkeiten
    > Staatliche Souveränität
    > Verlässlichkeit für andere Staaten
  - Eindeutige Identifizierbarkeit sensibler Systeme
    > Markierung der Datenströme
    > Kennzeichen zur Reduktion irrtümlicher Annahmen

# The End

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