Möglichkeiten und Grenzen zur Bestimmung von Cyberwaffen

Thomas Reinhold - reinhold@ifsh.de

Institut für Friedensforschung und Sicherheitspolitik
an der Universität Hamburg

Warum eine Definition für Cyberwaffen

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

- Stuxnet 2010 und das politische Nachspiel
  - Akteure mit "Cyber-Arsenalen"
  - Eigene Verwundbarkeit
  - Konsequenzen für die internationale Sicherheit
- UNIDIR Studie 2013*
  - 47 Staaten mit militärischen Cyberprogrammen,
    10 Staaten mit explizit offensiver Ausrichtung
- Neue Strategie des BMVg: Offensivbefugnisse und Kompetenzbündelung

* United Nations Institute for Disarmament Research
"The Cyber Index - International Security Trends and Realities", Genf, 2013

Warum eine Definition für Cyberwaffen II

- Fehlende internationale Vereinbarungen
- Übertragung existierender und Entwicklung neuer Regeln
  - Tallinn Manual*
  - Bilaterale Abkommen (China-Russland, China-USA)
- Perspektivisch:
  - Rüstungsbegrenzung und Abrüstung
  - Verifikation

- Notwendigkeit der Definition von "Cyberwaffen"
  - Grundlage für verbindliche Regeln
  - Einheitliches Verständnis der Dinge
  - Einzellfallprüfungen

* NATO CCDCOE - The Tallinn Manual on the International Law Applicable to Cyber Warfare, Tallinn, 2013

Übertragbarkeit bestehender Sicherheits-Konzepte

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

- Eigenschaften von Cyberwaffen als Problem für etablierte Konzepte
  - Immateriell
  - Virtuell
  - Duplizierbar
  - Keine spezifischen technischen Anlagen nötig
  - Doppel-Verwendbarkeit für zivile Zwecke (Dual-Use)
  - Attributionsproblem

Definitionsansätze I

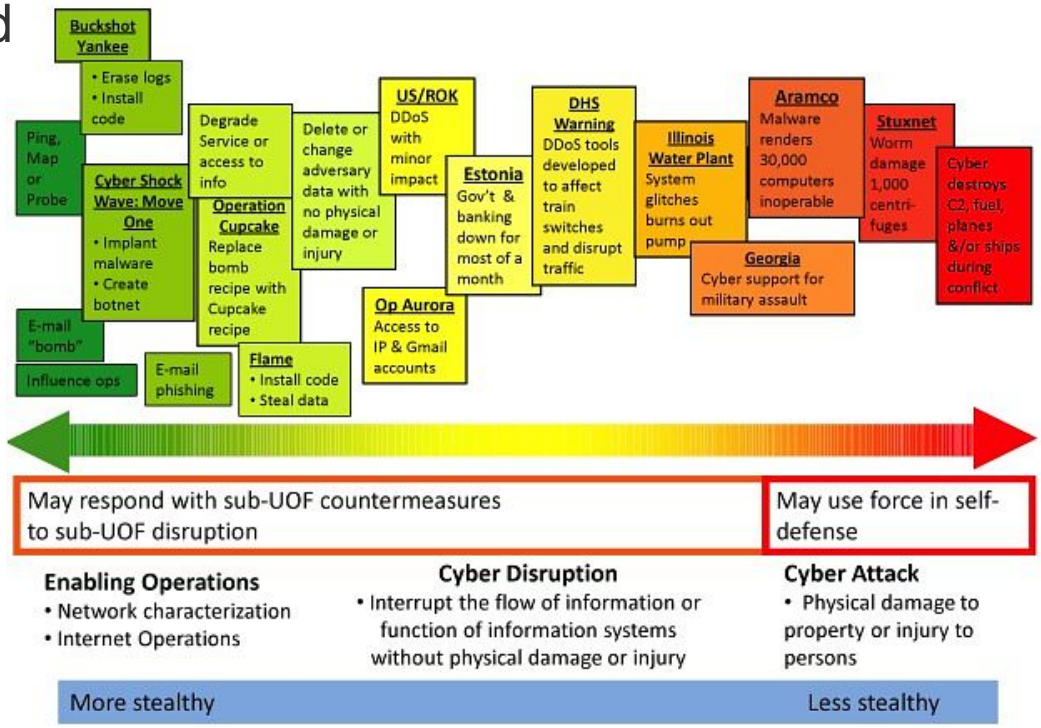
IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

- OECD-Studie “Reducing Systemic Cybersecurity Risk”, 2010*
  - Was sind übertragbare "technische" Eigenschaften klassischer Waffen?
  - *“A [cyber] weapon is “**directed force**” – its release **can be controlled**, there is a **reasonable forecast** of the [direct] effects it will have, and it will **not damage the user**, his friends or innocent third parties”*
  - Entdeckbarkeit der Cyberwaffe und Abwehrmöglichkeiten
- Aber
  - keine Unterscheidung zwischen Cybercrime und Cyberwar
  - keine Bewertung der Kriterien
- Kriterienkatalog in erster Linie Hilfsmittel und Ausschlußkriterium
  - *“On this basis it will be seen that the most common forms of virus (..) fail as credible cyberweapons, because they are relatively difficult to control. However a targeted DDoS is a likely cyberweapon.”*

Sommer, P. & Brown, I. - "Reducing Systemic Cybersecurity Risk" OECD/IFP Project on “Future Global Shocks”, 2010

Definitionsansätze II

- "On the Spectrum of Cyberspace Operations", 2012*
  - Was ist der tatsächlich bewirkte Schaden?
- Spektrum des beabsichtigten und unbeabsichtigten Schadens
  - enabling operations
  - cyber disruption
  - cyber attack
- "Cyber attacks" als Pendant zum "bewaffneten Angriff" im Sinne des Völkerrechts
- Ansatz für konkrete Bewertung und Reaktionsmöglichkeiten im Falle eines Angriffs



Brown, G. D. & Tullos, O. W.
"On the Spectrum of Cyberspace Operations", Small Wars Journal, 2012

Definitionsansätze III

- “Cyber-weapons: legal and strategic aspects”, 2013*
  - Was ist die Intention bei der Verwendung einer Schadsoftware?
- Technische Spezifika sind kein Kriterium für Bewertung
  - *“a weapon can be also an abstract concept thereby not necessarily a material one, as international and domestic legislation have considered it up to now”*
- Berücksichtigung juristischer und strategischer Dimensionen
  - Anwendungskontext und den Zweck eines Schadsoftware-Einsatzes
  - Beabsichtigter Schaden an einem explizit gewählten strategisch relevanten Ziel
- Betonung der Bewertung der Umstände gegenüber dem exakten Schaden entspricht der Herangehensweise staatlicher Institutionen

* Mele, S. "Cyber-weapons: legal and strategic aspects", 2013

Das Wassenaar-Abkommen als erster Schritt

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

- Wassenaar-Abkommen für ”Exportkontrollen von konventionellen Waffen und doppelverwendungsfähigen Gütern und Technologien”
  - Export/Import-Austausch zwischen Vertragspartnern (41 Staaten)
  - Seit Ende 2013 "Intrusion software" Bestandteil der regulierten Güter
    “Software” specially designed or modified to avoid detection by ‘monitoring tools’, or to defeat ‘protective countermeasures’, of a computer or network capable device, and performing any of the following:
    a.) The extraction of data or information, from a computer or network capable device, or the modification of system or user data; or
    *b.) The modification of the standard execution path of a program or process in order to allow the execution of externally provided instructions.**
  - Aber: Konkrete Auslegung der Regelung unterliegt staatlicher Souveränität

"The Wassenaar Arrangement - List of dual use goods and technologies" - WA-LIST (13) 1, 2013