Thema 21

Ethik und Informationskrieg

John Arquilla "ETHICS AND INFORMATION WARFARE"

Christoph Merkel 05.02.2008

Inhalt:

1. Begriffserklärungen

Ethik:
im Sinne von Konventionen und "gerechtem" Krieg

Informationskriegsführung (Inf.kriegsf.):

- Teil von "information operations"
- sehr weites Gebiet "a mosaic of forms"
  (Martin Libicki, 1996, p.6)
- es werden konventionelle Waffen zur Zerstörung von informationsreichen Zielen genutzt

1. Sabotage, Infiltration und Manipulation von Informationsanlagen resp. Kommunikationswegen/ -anlagen
2. Sabotage der gegnerischen Wirtschaft
3. Angriffe auf das öffentliche Leben
4. milit. Aufklärung

2. Grundsätze der klassischen Kriegsführung

Jus ad Bellum

- korrekter Kriegsgrund (Selbstverteidigung, Prävention)
- "duly constituted authority" (angemessene konstitutionelle Kontrolle)
- letzter Ausweg

Jus in Bello

- Immunität von Zivilisten (Ziele: Zerstörung des Transportwesens, Energie, Kommunikation und des Finanzwesens)
- Angemessenheit
- mehr Nutzen als Schaden

3. Gültigkeit der Grundsätze in der Informationskriegs-führung

- korrekter Kriegsgrund

  Selbstverteidigung entfällt, da Inf.kriegsf. ein Angriffspotential darstellt;
  Prävention entfällt, da der Aufbau dieses Angriffspotential nicht wahrnehmbar ist

- "duly constituted authority"

  der Staat verliert diese Kontrolle, da Gruppen oder Privatpersonen den Krieg führen werden;
  Verschleierung der Kriegsparteien u.U. des Krieges

- letzter Ausweg

  Autor vergleicht Inf.kriegsf. mit Wirtschafts-sanktionen

- Immunität von Zivilisten

  die Ziele (s.o.) haben gleichzeitig zivile Funktionen, d.h. es werden definitiv Zivilisten betroffen sein

- Angemessenheit

  lässt sich bei gleichartigen Angriffsmöglichkeiten gut, aber bei deutlichen Unterschieden nahezu gar nicht umsetzen (wenn ein Staat nicht elektronisch Zurückschlagen kann, muss er konventionelle Waffensysteme einsetzen), daher Gerfahr einer Eskalation insbesondere einer Nuklearen

- mehr Nutzen als Schaden

  umsetzbar aufgrund der geringeren Anzahl von Toten bei Angriffen in der Inf.kriegsf.

4. Richtlinien für die Informationskriegsführung

- aufgrund der leichten Umsetzbarkeit eine sehr große Gefahr, da es leicht zu einer Eskalation kommen kann
- in der Wirkung mit Massenvernichtungswaffen vergleichbar, auch wenn Inf.kriegsf. nur "Massenstörungswaffen" bereitstellt
- "Präventivmaßnahmen" sind u.U. mit Missbrauch gleichzusetzen

Regeln für Präventivmaßnahmen

1. Ziele sind ausschließlich milit. Natur
2. Ziele sollen zwar erreicht werden, aber schwerwiegende Schäden sollen verhindert werden
3. der Nutzen sollte deutlich überwiegen, es handelt sich schließlich um Interventionen

5. Zusammenfassung

- es gibt 2 Kategorien: tatsächliche Angriffe und Propaganda/Spionage
- kaum Unterscheidungsmöglichkeiten zwischen Zivilisten (Personen mit Internetzugang) und Kämpfenden (Personen die das Internet für Angriffe nutzen) resp. einfachen kriminellen Angriffen und Teilen einer Kriegskampagne (vor allem in der Wirtschaft)
- aufgrund der wachsenden Vernetzung wird die Inf.kriegsf. an Macht gewinnen
- heftige Angriffe können eine Nation ruinieren, daher ist sie für kleine Staaten und Gruppierungen eine ideale Alternative zu Massenvernichtungswaffen, es besteht allerdings die Gefahr einer Eskalation
- da die meisten Staaten sehr anfällig für Inf.kriegsf. sind, könnte sie als Abschreckung dienen
- für aggressive Staaten mit vielen Ressourcen (insbesondere die USA) sehr attraktiv, da sie andere Staaten "legal" wirtschaftlich ausschalten können

Es ist unmöglich zu entscheiden, ob wir uns aktuell in einem Informationskrieg befinden oder nicht, weil es keine Möglichkeit gibt die Informationen die wir bekommen zu verifizieren.

6. Leseempfehlung und Quellenangabe

Leseempfehlung:
Gerhard Wisnewski: Verschlußsache Terror, Knaur Verlag, München 2007

Text:
John Arquilla: Ethics and Information Warfare.
http://www.rand.org/publications/MR/MR1016/MR1016.chap13.pdf (1. 4. 2006)