Menschenrechte im digitalen Zeitalter

Cyberkonflikte und Menschenrechte

Dr. iur. Nils Melzer
Universität Zürich, 2012

Überblick

I. **Das Phänomen:** Wettrüsten und Krieg im Cyberspace – Science Fiction oder Wirklichkeit? Was ist das reale Zerstörungspotenzial von Cyberkonflikten?

II. **Das Recht:** Begrenzende und regulierende Bedeutung von Menschenrechten und humanitärem Völkerrecht?

III. **Ein Ausblick:** Was kann die internationale Gemeinschaft tun, um der Gefahr von Cyber-Konflikten zu begegnen?

I. Das Phänomen

Fragestellung: Wettrüsten und Krieg im Cyberspace – Science Fiction oder Wirklichkeit? Was ist das reale Zerstörungspotenzial von Cyberkonflikten?

Erste Initiativen Ende 1990er; überschattet von 9/11 & Folgen.

- Weckruf: Estland (2007); Georgien (2008); Iran (Stuxnet, 2010)
- Bisher v.a. wirtschaftlicher Schaden / militärische Espionage; humanitäre Konsequenzen begrenzt.
- Zerstörungspotenzial jedoch enorm («critical infrastructure»)

Erkenntnis: Extreme Verletzlichkeit & fehlender Verhaltenskodex.

- Aufbau Cybercommands (z.B. USA, China, Indien, N&S Korea)
- Internationale & nationale Konferenzen, Initiativen, Policies, Analysen und Erklärungen

Unterschiedliche Interessen & Ängste der "Cyber-Mächte"

- Geheimhaltung & Wettrüsten vs. vertrauensbild. Massnahmen

II. Das Recht

Fragestellung: Welche Bedeutung haben Menschenrechte und humanitäres Völkerrecht in der Begrenzung und Regulierung von Cyber-Konflikten?

Menschenrechte: Verhältnis zwischen Staat und Individuum (Voraussetzung: «Hoheitsgewalt»)

- Territoriales / funktionales Verständnis von Hoheitsgewalt?
- Potenziell relevante Rechte: Leben (EMRK 2); Privat- und Familienleben (EMKR 8); Meinungsäusserung (EMRK 10); Versammlung und Vereinigung (EMRK 11).

Humanitäres Völkerrecht: Verhältnis zwischen Konfliktparteien und Zivilbevölkerung (Voraussetzung: «bewaffneter Konflikt»)

- Definition bewaffneter Konflikt / Gewalt / Feindseligkeiten etc?
- Potenziell relevante Grundsätze: Unterscheidung (Personen / Infrastruktur); Verhältnismässigkeit (Kollateralschaden); Vorsichtsmassnahmen (Zumutbarkeit); Perfidie-Verbot.

- Anwendbarkeit, aber Klärungs- und Interpretationsbedarf

III. Ein Ausblick

Fragestellung: Was kann die internationale Gemeinschaft tun, um der Gefahr von Cyber-Konflikten zu begegnen?

Internationale Gemeinschaft hat Dringlichkeit der Lage erkannt:

- Vertrauensbildende Massnahmen (Cyber-Konferenzen etc.)
- Klärung geltenden Rechts (Anwendbarkeit, Auslegung, Lücken)
- Jedoch noch keine klare multilaterale Handlungsrichtung
- Vorläufig keine Grundlage für multilaterales Abkommen

Mögliche weiterführende Schritte:

Unverbindlicher Verhaltenskodex (Vorbild: «Montreux Doc.»):

1. «Restatement» verbindlicher Prinzipien geltenden Rechts.
2. Unverbindliche weiterführende "Good Practices".

Ziel: Schutz der Grundlagen und Werte unserer internationalen Gemeinschaft auch im Cyber-Space («Rule of Law», Menschenwürde, Souveränität, Staatenverantwortlichkeit etc.).

Fragen?

Besten Dank für Ihre Aufmerksamkeit!

Kontakt: nils.melzer@uzh.ch