Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

Cyberspace and International Law

What are the challenges for international law, how does the Tallinn Manual deal with these challenges?

Stefan Oeter

Fakultät
für
Rechtswissenschaft

Structure

1. Cyberspace and International Law
2. Tallinn Manual – Background and Content
3. Adequate Response or Overreaction?
4. What does Cyberwar Mean for Current IL?
5. Challenges Ahead

1. Cyberspace and International Law

- Cyberspace is a largely unregulated realm
- Peculiar governance structure – dominance of private actors in internet governance
- States at unease – limited control (exit: clandestine surveillance)
- Perception of threat - ´hacking´ as common phenomenon
- Hackers are not always private raiders – some states very active with cyber operations

1. Cyberspace and International Law

- Major target of cyber operations typically are sensitive data – theft of confidential data

- Hostile cyber operations may threaten the integrity of information systems (denial attacks)

- Extreme case: Offensive operations intended to cause physical harm (exemplary case: Stuxnet)

- Discussion on cyberwar is a consequence of such threat perception – but largely academic until now

- What is ´cyberwar´?

2. Tallinn Manual – Background and Content

1. Tallinn Manual – Background

→ NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) founded 2007/08 in Tallinn.
→ In 2009 CCD COE invited an ´International Group pf Experts´ to produce a manual on the law governing cyber warfare.
→ Production of such manuals is not uncommon in LOAC
→ Based partly on national security strategies
→ Several rounds of deliberations from 2009-2012
→ Manual presented in 2012

2. Tallinn Manual – Background and Content

1. Tallinn Manual – Content

→ Two segments – Rules and Commentary

→ Rules part attempts to formulate a code reflecting the state of customary and treaty law – Commentary gives a reasoning for the rules and elaborates on the underlying rules of CIL and AP I.

→ Manual focuses on armed conflict – cyber operations passing the threshold of ´armed conflict´

→ Tallinn Manual accordingly has a very narrow focus – cyber operations in the scope of application of LOAC

→ Some general remarks on sovereignty, jurisdiction and state responsibility at the beginning

2. Tallinn Manual – Background and Content

1. Tallinn Manual – Content

→ Main sections focus exclusively on the meaning of ´ius ad bellum´ and ´ius in bello´ for cyber operations
→ ´Ius ad bellum´ - use of force and its restraints
→ ´Ius in bello´ - rules of LOAC disciplining states in the modalities of use of force
→ Tallinn Manual elaborates in detail what the rules of LOAC might mean for offensive cyber operations passing the threshold of ´armed conflict´
→ Exercise thus largely of an academic character
→ Reminder: Threshold of ´armed conflict´ - met only in extreme cases (but: tendencies to lower the threshold)

3. Adequate Response or Overreaction?

- Rules as such largely adequate – not that much criticism
- Major criticism goes against the focus on cyberwar
- Again: What is ´cyberwar´?
- Until now fortunately a largely academic issue
- Needs definitely conceptual clarification
- But should not be taken as reflection of IL on cyberspace
- Problems lie elsewhere
- Inherent tendency of ´militarization´ of IL rules on cyberspace

4. What does Cyberwar Mean for Current IL?

Has the discussion on cyberwar an importance for current IL?

Differentiated answer needed – demarcates the boundary line where offensive cyber operations enter the realm of armed conflict and where military countermeasures are justified

But at the same time discussion too much centered on phenomena of cyberwar – real problems lie in different parts of IL

Introductory part of Tallinn Manual of some help here – sovereignty, jurisdiction and state responsibility are relevant issues

4. What does Cyberwar Mean for Current IL?

Has the discussion on cyberwar an importance for current IL?

Basic principles of prohibition of intervention (linkage to jurisdiction) and human rights are at stake – much more relevant than LOAC for routine cases of cyber operations

Prohibition of intervention of particular relevance – to what degree must foreign states respect the legal order of the territorial state where operations are executed? – Proble,m of ´espionage´ and its grey zones

Protection of individual rights (privacy) by int´l. human rights

5. Challenges Ahead

1. Normative consensus on threshold of ´cyberwar´ needed: What are the constellations where military countermeasures might be justified?
2. Need of a clear code of conduct – and preventive agreements on banned types of operation
3. Search for more clarity on the routine cases of offensive cyber operations – Prohibition of intervention and human rights as yardsticks
4. Still too much disputed where the legal boundaries of offensive cyber operations might be set
5. Urgent need for clearer legal boundary lines

Thank you!