

Inhaltsverzeichnis

Vorwort	7
Inhaltsverzeichnis	9
Abkürzungsverzeichnis	13
Einleitung: Problemaufriss und Gang der Arbeit	19
Kapitel 1 – Grundlagen	24
A. Cyberspace und Cyberkriegsführung	24
I. Informationstechnologien und Kriegsführung	24
II. Struktur und völkerrechtlicher Status des Cyberspace	26
II. Cyberkriegsführung und Computernetzwerkoperationen	29
IV. Verschiedene Formen von Computernetzwerkoperationen	30
V. Fälle in der Praxis	31
1. Estland 2007	31
2. Georgien 2008	33
3. Stuxnet und das iranische Atomprogramm 2010	33
4. Spionage: Das Bundestag-Intranet 2015	34
5. Ukraine 2014-2016	35
VI. Die Besonderheiten der Cyberkriegsführung	36
B. Das Kampfführungsrecht im Gesamtgefüge des Völkerrechts	39
I. Der Begriff und die Zielsetzung des Konfliktsvölkerrechts	39
II. Das Kampfführungsrecht und seine Grundprinzipien	42
1. Das Verbot überflüssiger Verletzungen und unnötiger Leiden	44
2. Der Grundsatz des gutgläubigen und ehrwürdigen Verhaltens	46
3. Das Gebot der diskriminierenden Kriegsführung	46
4. Der Verhältnismäßigkeitsgrundsatz	47
III. Rechtsquellen	47
1. Vertrags- und Gewohnheitsrecht im internationalen Konflikt	48
2. Voraussetzungen völkergewohnheitsrechtlicher Geltung	48
IV. Der Menschenrechtsschutz und das Konfliktsvölkerrecht	51

Kapitel 2 – Anwendbarkeit des Kampfführungsrechts im Cyberkrieg	60
A. Generelle Anwendbarkeit des Konfliktsvölkerrechts	60
B. Computernetzwerkoperationen als bewaffneter Konflikt	63
I. Der Anwendungsbereich des Kampfführungsrechts	63
II. Computernetzwerkoperation als internationaler bewaffneter Konflikt	66
1. Der Begriff der Gewaltanwendung	66
a) Der Gewaltbegriff im Friedenssicherungs- und Konfliktsvölkerrecht	67
b) Instrument-Based v. Consequence-Based Approach	70
c) Typische Auswirkungen einer Gewaltanwendung	73
d) Der Kausalitäts- und Zurechnungszusammenhang	76
aa) Direktheit des Schadens	78
bb) Unmittelbarkeit	79
cc) Vorhersehbarkeit (Foreseeability und Adäquanztheorie)	80
dd) Normative Bewertung des Einzelfalls	81
ee) Kriterien im Rahmen des Unmittelbarkeitsansatzes	82
e) Die Bedeutung der Intention des Angreifers	87
f) Intensitätsschwelle	90
g) Funktionalitätsverlust als physischer Schaden	93
aa) Daten als Objekte	94
bb) Target-Based Approach	99
i) Bank- und Finanzinfrastrukturen	102
ii) Militär/Staatsverwaltung	105
iii) Kommunikation	106
h) Zwischenergebnis	111
i) Das ex-post Dilemma des Consequence-Based Approach	113
2. Staaten als Konfliktparteien	116
a) Die Identifizierungsproblematik im Cyberspace	116
b) Die Zurechnung des Verhaltens privater Akteure	119
aa) Die Kriterien der Staatenverantwortlichkeit	119
bb) Das Kriterium der Konfliktklassifizierung	124
cc) Die Vorzugswürdigkeit eines einheitlichen Zurechnungsmaßstabs	126
dd) Overall Control über Hackergruppen?	128

ee) Beweisstandard und Beweislast	130
c) Zwischenergebnis	133
C. Computernetzwerkoperationen neben konventioneller Kriegsführung	134
Kapitel 3 – Schutz der Zivilbevölkerung und ziviler Objekte	138
A. Der Anwendungsbereich: Ein Angriff i.S.d. Art. 49 (1) ZPI	139
I. Der völkerrechtliche Gewaltbegriff und der konfliktsvölkerrechtliche Angriffsbegriff	139
II. Ein Angriff als Hürde zum Schutz?	142
III. Die Ausnahme: Das Verbot menschlicher Schutzschilder	148
IV. Die Angriffsdefinition	149
B. Das Gebot diskriminierender Angriffe	157
I. Militärische Objekte	159
II. Beschränkung des Angriffs auf die militärisch genutzte Komponente eines Objekts?	164
III. Objekte mit besonderem Schutzstatus	169
1. Medizinische Objekte	169
2. Lebensnotwendige Objekte für die Zivilbevölkerung	171
3. Anlagen und Einrichtungen, die gefährliche Kräfte enthalten	173
4. Besonderer Schutzstatus für ausgewählte Infrastrukturen?	175
C. Der Verhältnismäßigkeitsgrundsatz	176
D. Vorsichtsmaßnahmen	187
I. Die Schutzpflichten des Angreifers	188
1. Computernetzwerkoperationen als milderes Mittel	188
a) Exkurs: Militärische Notwendigkeit als ein allgemeiner Verhältnismäßigkeitsmaßstab?	190
b) Die Pflicht der Verwendung des mildesten Mittels zur Minimierung von Kollateralschäden	194
2. Die Pflicht zur Warnung	195
II. Die Schutzpflichten des Angegriffenen – Pflicht zur Trennung ziviler und militärischer Infrastrukturen	196
E. Psychologische Kriegsführung	199
I. Generelle Grenzen	200
II. Das Verbot der Schreckensverbreitung	201
1. Angriffe zum Zweck der Schreckensverbreitung	202
2. Gewaltandrohungen zum Zweck der Schreckensverbreitung	203
a) Psychische Leiden und der Angriffsbegriff	203

b) Androhungen eines Angriffs	206
F. Zwischenergebnis	208
Kapitel 4 – Perfidie und Missbrauch von Schutz-/Kennzeichen	211
A. Die Kennzeichnungspflicht im Allgemeinen	212
B. Die Identifizierungsfunktion von IP-/E-Mail-Adressen und <i>domains</i>	214
C. Der Missbrauch von Schutz- und Kennzeichen	216
I. Missbrauch von anerkannten Schutzzeichen	216
II. Verwendung des Emblems der VN und neutraler Kennzeichen	217
III. Verwendung gegnerischer Kennzeichen	219
D. Das Verbot der Perfidie	220
I. Eingriffe in die gegnerische Kommunikation	222
II. Vortäuschen einer zivilen Urheberschaft	223
Fazit	227
A. Ergebnisse der Arbeit	227
B. Gesamtbetrachtung	233
Literaturverzeichnis	237
Rechtsprechungsverzeichnis	254
Dokumentenverzeichnis	259