



universität
wien

DISSERTATION / DOCTORAL THESIS

Titel der Dissertation / Title of the Doctoral Thesis

„Der Krieg im Cyberspace und seine normativen
Grundlagen“

verfasst von / submitted by

Mag.(FH) Georg Kunovjanek, MSD

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Doctor of Philosophy (PhD)

Wien, 2020 / Vienna 2020

Studienkennzahl lt. Studienblatt /
degree programme code as it appears on the
student record sheet:

UA 794 242 101

Dissertationsgebiet lt. Studienblatt /
field of study as it appears on the student record
sheet:

Interdisciplinary Legal Studies

Betreut von / Supervisor:

ao. Univ.-Prof. MMag. DDr. Christian Stadler

Mag.(FH) Georg Kunovjanek, MSD

Der Krieg im Cyberspace und seine normativen Grundlagen

Eine kritische Analyse des Krieges der Zukunft

1 Ehrenwörtliche Erklärung

Ich, Mag.(FH) Georg Kunovjanek, MSD, erkläre hiermit ehrenwörtlich, dass ich die vorliegende Arbeit selbständig und ohne fremde Hilfe verfasst, andere als die angegebenen Quellen nicht benutzt und die den Quellen wörtlich oder inhaltlich entnommenen Stellen als solche kenntlich gemacht habe. Die Arbeit wurde bisher in gleicher oder ähnlicher Form keiner anderen inländischen oder ausländischen Prüfungsbehörde vorgelegt und auch noch nicht veröffentlicht. Die vorliegende Fassung entspricht der eingereichten elektronischen Version.

Außerdem habe ich die Reinschrift der Arbeit einer Korrektur unterzogen und ein Belegexemplar verwahrt. Ich erteile außerdem meine Zustimmung, die vorliegende Arbeit für wissenschaftliche Zwecke öffentlich zugänglich zu machen.

WIEN
2020

A handwritten signature in black ink, reading 'Georg Kunovjanek', written in a cursive style.

(Mag.(FH) Georg Kunovjanek, MSD)

2 Inhaltsverzeichnis

1	Ehrenwörtliche Erklärung	ii
2	Inhaltsverzeichnis	iii
3	Vorwort	1
4	Einleitung	3
5	Vom Begriff des Krieges	26
5.1	Zum Wesen des Krieges	27
5.1.1	Die Einordnung des Krieges als Moment des Konfliktes	27
5.1.2	Die Abgrenzung zwischen Krieg und Verbrechen	33
5.1.3	Das Verhältnis zwischen Krieg und Staat	38
5.1.4	Der Zusammenhang zwischen Krieg und Sicherheit	40
5.1.5	Das Verhältnis zwischen Krieg und Souveränität	42
5.1.6	Der Begriff vom Krieg	44
5.2	Zu den Akteuren im Krieg	45
5.2.1	Exkurs: Zur Definition der bewaffneten Akteure im Krieg	46
5.2.2	Die staatlichen Akteure	47
5.2.3	Die nichtstaatlichen Akteure	52
5.2.4	Die internationalen und transnationalen Akteure	58
5.3	Zu den Ursachen und dem Zweck von Kriegen	64
5.3.1	Asymmetrie und Symmetrie als Ursachen des Krieges	64
5.3.2	Exkurs: Macht als Parameter für die Ursache von bewaffneten Konflikten	69
5.3.3	Frieden als Zweck des Krieges	70
5.4	Zur Intensität von bewaffneten Konflikten	72
5.4.1	Der Große Krieg	73
5.4.2	Exkurs: Der Große Krieg am Beispiel des Fünf-Tage-Krieges in Georgien	75
5.4.3	Der Kleine Krieg	77
5.4.4	Exkurs: Der Kleine Krieg am Beispiel der Tschetschenien-Kriege	81
5.4.5	Der Zusammenhang zwischen den Formen des Krieges	84
5.4.6	Die Konfliktintensität und die Ebenen des Krieges	87
5.5	Zu den Methoden und Mitteln des Krieges	92
5.5.1	Folgerungen für die Kriegführung aus dem Dreißigjährigen Krieg	92
5.5.2	Die Kriegführung als angewandte Politik	94
5.5.3	Die Hochtechnologie und ihr Einfluss auf die Kriegführung	96
5.6	Zum Faktor Raum im Krieg	98
5.6.1	Land als erste Dimension des Krieges	98
5.6.2	See als zweite Dimension des Krieges	100
5.6.3	Luft als dritte Dimension des Krieges	101
5.6.4	Weltraum als vierte Dimension des Krieges	102
5.7	Zwischenergebnis zum Begriff des Krieges	103
6	Vom Begriff des Cyberspace	107
6.1	Zum Cyberspace als (technologischer) Raum	108
6.1.1	Die Momente des Cyberspace	108
6.1.2	Die Entgrenzung durch den Cyberspace	112
6.1.3	Die Rolle von Zeit und Raum im Cyberspace	115
6.2	Zum Cyberspace als menschlichen Handlungsraum	117
6.2.1	Die Information als zentrale Ressource	117

6.2.2 Die Interaktion im Netz	120
6.2.3 Attribution, Anonymität und Anarchie als zentrale Herausforderungen	122
6.3 Zum Cyberspace als militärischen Einsatzraum	126
6.3.1 Cyberraum als Dimension des Krieges	126
6.3.2 Eine Einsatzraumreflektion für den Cyberwar	128
6.4 Zwischenergebnis zum Begriff des Cyberspace	130
7 Vom Begriff des Cyberwar	133
7.1 Zur Intensität des Cyberwar	134
7.1.1 Der Cyber Angriff	135
7.1.2 Der Große Cyberwar	138
7.1.3 Exkurs: Der Große Cyberwar am Beispiel der Stuxnet-Attacke auf Natanz	140
7.1.4 Der Kleine Cyberwar	142
7.1.5 Exkurs: Der Kleine Cyberwar am Beispiel des Fünf-Tage-Krieges in Georgien	143
7.1.6 Der Zusammenhang zwischen den Formen des Cyberwar	144
7.1.7 Die Sicherheit im Cyberspace	149
7.2 Zu den Ursachen und dem Zweck des Cyberwar	154
7.2.1 Der Zusammenhang zwischen hohem und geringem Vernetzungsgrad	155
7.2.2 Verfügungsgewalt über Information als Ursache virtueller Konflikte	157
7.2.3 Der Kampf mit und um Informationen	159
7.2.4 Exkurs: Zum Zusammenhang zwischen Ziel und Zweck bezogen auf die Ebenen der Kriegführung	161
7.3 Zu den Akteuren im Cyberwar	162
7.3.1 Die staatlichen Akteure	163
7.3.2 Die nichtstaatlichen Akteure	166
7.3.3 Die internationalen und transnationalen Akteure	169
7.4 Zum Wesen des Cyberwar	172
7.4.1 Die Einordnung des Cyberwar als Moment des Krieges	172
7.4.2 Die Abgrenzung des Cyberwar zum konventionellen Großen Krieg	175
7.4.3 Die Abgrenzung des Cyberwar zu den anderen Konfliktformen im Netz	178
7.4.4 Das Verhältnis zwischen Souveränität und Cyberwar	180
7.4.5 Der Begriff vom Cyberwar	183
7.5 Zwischenergebnis zum Begriff des Cyberwar	185
8 Vom Recht des Cyberwar	188
8.1 Zum Cyberspace zwischen nationalem Recht und Völkerrecht	189
8.2 Zum Cyberwar im Völkerrecht	196
8.2.1 Das Völkerrecht und der bewaffnete Konflikt	197
8.2.2 Nationale Strategien zur Cyber Sicherheit	201
8.3 Zum Cyberwar im Europarecht	207
8.3.1 Die Gemeinsame Sicherheits- und Verteidigungspolitik und der Cyberwar	207
8.3.2 Die Cybersicherheitsstrategie der Europäischen Union und der Cyberwar	209
8.3.3 Die Cyber Verteidigung im Rahmen der Europäischen Union	211

8.4	Zum Cyberwar im Österreichischen Recht	212
8.4.1	Strafrecht im Cyberspace am Beispiel des österreichischen Strafgesetzbuches	213
8.4.2	Die rechtlichen Grundlagen für die Tätigkeit der Organe der bewaffneten Staatsgewalt am Beispiel Österreichs	215
8.4.3	Die Zuordnung der Führungsverantwortung zwischen Polizei und Militär am Beispiel der Raumschutzoperation	217
8.4.4	Zu den Aufgaben des Bundesheeres im Cyberspace	218
8.4.5	Einsatzfälle im Rahmen von Cyber Angriffen	221
8.4.5.1	<i>Einsatz zur Eigensicherung militärischer IKT-Infrastruktur</i>	221
8.4.5.2	<i>Einsatz im Rahmen der militärischen Landesverteidigung</i>	222
8.4.5.3	<i>Einsatz im Rahmen des sicherheitspolizeilichen Assistenzeinsatzes</i>	224
8.5	Zwischenergebnis zum Recht des Cyberwar	224
9	Synopse und Zusammenfassung	228
9.1	Zusammenfassung der Zwischenergebnisse	228
9.2	Möglichkeiten zur Festlegung der Führungsverantwortung bei Angriffen im und aus dem Cyberspace	231
9.2.1	Die Kategorisierung Kritischer Infrastruktur	232
9.2.1.1	<i>Einteilung Kritischer Infrastruktur nach deren Kritikalität</i>	232
9.2.1.2	<i>Einteilung Kritischer Infrastruktur nach deren Verwundbarkeit</i>	233
9.2.2	Das Drei-Faktoren-Beurteilungsverfahren der Führungsverantwortung	236
9.2.2.1	<i>Souveränitätsrelevanz als primärer Entscheidungsfaktor</i>	237
9.2.2.2	<i>Intensität als sekundärer Entscheidungsfaktor</i>	239
9.2.2.3	<i>Intention als tertiärer Entscheidungsfaktor</i>	240
9.2.3	Die Abgrenzung zwischen Verantwortung, Koordinierung und Führung	242
9.3	Ausblick	249
10	Abstract	251
10.1	Kurzbeschreibung	251
10.2	Abstract	251
11	Literaturverzeichnis	253
11.1	Primärliteratur	253
11.1.1	Gesetze, Vorschriften, Positionspapiere	253
11.1.2	Bücher (Monographien und Sammelbände)	258
11.2	Sekundärliteratur	259
11.3	Internetquellen	266
11.4	Zeitschriften, Fachjournale, Studien	266
12	Abkürzungsverzeichnis	269
13	Abbildungsverzeichnis	274
14	Lebenslauf	275

3 Vorwort

Das Interesse am Thema Cyberwar (CW) basiert zunächst auf einer persönlichen Betroffenheit als Nutzer der modernen Informationsinfrastruktur. Die Verwendung von Computern in allen Lebenslagen, sowohl privat als auch beruflich, bringt eine intensive Beschäftigung mit der Thematik der Sicherheit in Computernetzwerken mit sich.

Aus dem zunächst zutiefst persönlichen Interesse erwuchs, in Folge meiner beruflichen Tätigkeit, die Notwendigkeit, mich auch im Zusammenhang mit der militärischen Nutzung moderner Kommunikationssysteme und den Sicherheitsbelangen diesbezüglich zu beschäftigen.

Die Ereignisse um Edward Snowden, WikiLeaks, Anonymous, Stuxnet, web 2.0 und den arabischen Frühling, die sich in Bezug auf das Thema in der jüngeren Vergangenheit zugetragen haben, zeigen die Bedeutung des Gegenstandes für die Menschen, die Gesellschaft und letztlich auch für die Staaten. Die zunehmende Abhängigkeit von Computern in allen Lebenslagen hat unsere Informationsgesellschaft verwundbar gemacht.

Die Möglichkeit mit, in Relation zu konventionellen Waffen mit ähnlicher Reichweite, relativ günstigen Mitteln auf alle Bereiche des privaten und öffentlichen Lebens einwirken zu können, ergibt eine neue Art von Bedrohung, die nicht so einfach fassbar erscheint.

Die Menschen wiegen sich, ob der Unsichtbarkeit der Gefahr, allerdings in einer trügerischen Sicherheit. Gleiches gilt auch für vitale Bereiche der Gesellschaft, wie etwa die Energieversorgung. Einerseits führt der Einsatz von sauberen, nicht-letalen Waffen (Cyber Waffen) zu einem neuen, gehegten (begrenzten) Krieg, andererseits ist der hohe Vernetzungsgrad der Bevölkerung in den Industrienationen eher ein Indikator dafür, dass das Gegenteil der Fall sein könnte.

Eine Auseinandersetzung mit der Thematik ist für mich auch in Hinblick auf die Unterscheidung zwischen Krieg und Kriminalität in diesem neuen Konfliktfeld angezeigt. Nur wenn hier eine Verhaltenssicherheit in Bezug auf die Zuständigkeit von Militär und Polizei getroffen werden kann, sind die Gemeinwesen auch handlungsfähig. Es ist daher notwendig eine entsprechende Sensibilisierung für das Thema Cyber Sicherheit herbeizuführen.

Ich möchte mich bei meinem Betreuer Herrn Prof. MMag. DDr. Christian Stadler bedanken, der mir in vielen Gesprächen immer wieder neue Blickwinkel und Ideen zum Thema vermitteln konnte. Er ließ mir bei der inhaltlichen Ausgestaltung seine Unterstützung angedeihen und versorgte mich stets mit ergänzender Literatur.

Weiter möchte ich Herrn Dr. Karl Edlinger für seine Anregungen und Ratschläge zur Bearbeitung der völkerrechtlichen Grundlagen danken. Auch Herrn Mag.(FH) Markus Höfler möchte ich für die angeregten Diskussionen in Bezug auf diese Arbeit meinen Dank aussprechen.

Besondere Anerkennung gebührt vor allem meiner Lebensgefährtin Frau Mag. Kathrin Stissen, meinen beiden Töchtern Rubina und Soraya, sowie deren Mutter Henna Haq, die mich bei der Erstellung der Dissertation und der Absolvierung des Generalstabslehrganges stets aus vollen Kräften unterstützten. Besonders bedanken möchte ich mich bei meiner Schwester Frau RegR Dipl.-Päd. Johanna Kunovjanek für ihre Unterstützung in der formalen Ausgestaltung der Arbeit.

Diese Arbeit ist meinen Eltern Karoline und Gottfried Kunovjanek gewidmet.

Mag.(FH) Georg Kunovjanek, MSD
WIEN, 2020

4 Einleitung

„Bei der Cyber Thematik ist noch
nicht absehbar, was das in Zukunft für
die Streitkräfte bedeuten wird.“
Franzisci¹

Im Jahr 2007 wurde durch einen Angriff im Cyberspace² die syrische Luftabwehr ausgeschaltet und ermöglichte so die Zerstörung einer im Bau befindlichen Nuklearanlage der Syrer durch israelische Kampfflugzeuge. Auch im Rahmen des Georgien-Krieges 2008 oder der Annexion der Krim wurden begleitend Angriffe im Cyberspace durchgeführt. Neben diesen militärischen Handlungen erfolgt jedoch laufend eine Vielzahl von kriminellen Übergriffen im Cyberspace. Da alle diese Angriffe sich ähnlicher Instrumente bedienen und die Urheber oft im Dunkeln bleiben, ist eine klare Identifikation von Krieg in diesem neuen Handlungsraum nur schwer möglich.

Hier zeigt sich zum einen die Relevanz des Cyberspace als Handlungsraum auch für das Militär, aber genauso offenbart sich zum anderen die Frage nach dem Wesen des Krieges in diesem neuen Handlungsraum und daraus abgeleitet der Führungsverantwortung bzw. Durchführungsverantwortung im Fall von Angriffen im Cyberspace. Die aktuelle Österreichische Sicherheitsstrategie (ÖSS) beinhaltet einige Punkte zur Thematik der Cyber Sicherheit³. So findet sich darin zum Komplex der inneren Sicherheit folgende Aussage: „Cyberkriminalität⁴, Cyber-Angriffe⁵

¹ Vortrag von GenLt Franzisci zur Umfassenden Sicherheitsvorsorge (USV), Landesverteidigungsakademie, 05.12.2012.

² „Im allgemeinen Sprachgebrauch bezeichnet Cyber Space auch das weltweite Netzwerk von verschiedenen unabhängigen IK-Infrastrukturen, Telekommunikationsnetzen und Computersystemen. In der sozialen Sphäre kann bei Benutzung dieses globalen Netzwerkes zwischen Individuen interagiert werden, Ideen ausgetauscht, Informationen verteilt, soziale Unterstützung gewährt, Geschäfte getätigt, Aktionen gelenkt, künstlerische und mediale Werke geschaffen, Spiele gespielt, politisch diskutiert und vieles mehr getan werden.“ BKA, Österreichische Strategie für Cyber Sicherheit (ÖSCS), Wien, März 2013, S. 21.

³ „Cyber Sicherheit beschreibt den Schutz eines zentralen Rechtsgutes mit rechtsstaatlichen Mitteln vor aktorsbezogenen, technischen, organisations- und naturbedingten Gefahren, die die Sicherheit des Cyber Space (inklusive Infrastruktur- und Datensicherheit) und die Sicherheit der Nutzer im Cyber Space gefährden. Cyber Sicherheit trägt dazu bei, die Gefährdungen zu erkennen, zu bewerten und zu verfolgen sowie die Fähigkeit zu stärken, Störungen im und aus dem Cyberspace zu bewältigen, die damit verbundenen Folgen zu mindern sowie die Handlungs- und Funktionsfähigkeit der davon betroffenen Akteure, Infrastrukturen und Dienste wieder herzustellen.“ Ebd., S. 21.

⁴ „Cyberkriminalität umfasst rechtswidrige Angriffe aus dem Cyber Raum auf oder mittels IKT-Systemen, die strafrechtlich oder verwaltungsstrafrechtlich normiert sind und umfasst somit jede Form von Straftaten, die mit Hilfe von Informationstechnologien und Kommunikationsnetzen begangen werden. Auch die Internetkriminalität zählt dazu.“ Ebd., S. 20.

⁵ Ein Cyber Angriff ist ein Angriff mit Mitteln der IT im Cyber Raum, der sich gegen eines oder mehrere andere IT-Systeme richtet und zum Ziel hat, die Schutzziele der IKT Sicherheit als Teil oder Ganzes zu verletzen. Die Ziele der IT-Sicherheit (Vertraulichkeit, Integrität und Verfügbarkeit) können dabei als Teil oder Ganzes verletzt werden. Cyber Angriffe, die sich gegen die Vertraulichkeit eines IT-Systems richten, werden als Cyber Spionage bezeichnet und stellen somit Spionage auf digitalem Wege dar. Cyber Angriffe gegen die Integrität und Verfügbarkeit eines IT-Systems werden als Cyber Sabotage bezeichnet. Ebd., S. 20.

oder der Missbrauch des Internet für extremistische Zwecke oder Netzwerksicherheit stellen besondere neue Herausforderungen für alle betroffenen Akteure dar und erfordern ein breites Zusammenwirken im Rahmen eines Gesamtkonzepts.“⁶ Des Weiteren wird bei der Verteidigungspolitik die „[...] Bewältigung von subkonventionellen Bedrohungen oder von neuen Gefährdungen in Folge von Cyber-Angriffen [...]“⁷ als mögliches neues militärisches Aufgabenfeld genannt.

Die Aufgabenfelder werden hier angeführt, jedoch nicht der Übergangsbereich von einem zum anderen Aufgabenfeld. Die Definition und daraus abgeleitet die Identifikation von Krieg im Cyberspace wird umso wichtiger, da die zunehmende Vernetzung im zivilen – aber auch militärischen – Bereich, die Verwundbarkeit moderner Gesellschaften und Staaten steigert. Gekennzeichnet ist die daraus resultierende Bedrohung durch diese unklare Identifikation des kriegerischen Aktes im Cyberspace.

Zum neuen Handlungsraum für das Militär und den darin stattfindenden kriegerischen Handlungen tritt noch die rechtliche Dimension hinzu. Die Frage nach den rechtlichen Rahmenbedingungen für den Einsatz des Militärs als Instrument des Staates im Cyberspace ist in diesem Zusammenhang, sowohl international als auch national, noch zu klären. Gerade weil vielfach schon militärisches Handeln im Cyberspace stattfindet und die rechtlichen Grundlagen dafür nicht klar sind, ist eine Auseinandersetzung damit notwendig.

Zum Thema Cyberspace und Cyberwar gibt es reichhaltige Literatur, welche sich neben der Darstellung des virtuellen Raumes und des Krieges im Cyberspace auch mit den rechtlichen Belangen dazu beschäftigt. Sehr ausführlich setzen sich Martin Libicki⁸, Thomas Rid⁹, Peter Singer¹⁰, Richard Clarke¹¹, Mark Bowden¹², Sandro Gayken¹³, Yvonne Hofstetter¹⁴, Constanze Kurz und Frank Rieger¹⁵ mit der Cyberwar Thematik auseinander. Zur Thematik der Sicherheit im Cyberspace wird die einschlägige Literatur von Misha Glenny¹⁶, Julian Assange¹⁷, Parry Olson¹⁸ und dem Autorenteam Stefan Aust und Thomas Ammann¹⁹ herangezogen. Die im Literaturverzeichnis angegebene Literatur deckt ein breites Spektrum an

⁶ BKA, Österreichische Sicherheitsstrategie (ÖSS), 2013, S. 11.

⁷ Ebd., S. 11.

⁸ Libicki, Martin C.: What Is Information Warfare? National Defense University, August 1995.

⁹ Rid, Thomas: Cyberwar will not take place, Hurst & Company, London 2013.

¹⁰ Singer, Peter: Cybersecurity and Cyberwar. What everyone needs to know, New York 2014.

¹¹ Clarke, Richard: World Wide War. Angriff aus dem Internet, Hamburg 2011.

¹² Bowden, Mark: Worm. Der erste digitale Weltkrieg, Berlin 2012.

¹³ Gayken, Sandro: Cyberwar. Das Internet als Kriegsschauplatz, 1. Aufl., München 2011.

¹⁴ Hofstetter, Yvonne: Der unsichtbare Krieg. Wie die Digitalisierung Sicherheit und Stabilität in der Welt bedroht, Droemer Verlag, München 2019.

¹⁵ Kurz, Constanze; Rieger, Frank: Cyberwar. Die Gefahr aus dem Netz, Bertelsmann, München 2018.

¹⁶ Glenny, Misha: Cybercrime. Kriminalität und Krieg im digitalen Zeitalter, 1. Aufl., München 2012.

¹⁷ Assange, Julian u.a.: Cypherpunks. Unsere Freiheit und die Zukunft des Internets, 1. Aufl., s.l 2013.

¹⁸ Olson, Parry: Inside Anonymous. Aus dem Innenleben des globalen Cyber-Aufstands, München 2012.

¹⁹ Aust, Stefan; Ammann, Thomas: Digitale Diktatur, Econ Verlag, Berlin 2014.

Sichtweisen in Bezug auf den Krieg, den Cyberwar und andere Bedrohungen im Cyberspace, aber auch deren rechtlicher Aspekte ab.

In diesem Zusammenhang ist der Versuch einer Expertengruppe, unter Leitung des NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn, die bestehenden völkerrechtlichen Bestimmungen in einem Regelwerk, dem „Tallinn Manual 2.0 on the International Law applicable to Cyber Operations“²⁰, ausgerichtet auf die Herausforderungen der Cyber Thematik zusammenzufassen, anzuführen. Eine Auseinandersetzung mit dem „Tallinn Manual“ wird im Zusammenhang mit der rechtlichen Betrachtung des Cyberwar durchgeführt. Zum Gebrauch des Humanitären Völkerrechts im Cyberspace ist weiter eine Publikation von Katharina Ziolkowski²¹ zu nennen, welche sich mit der Anwendung der Genfer Zusatzprotokolle im Cyberwar beschäftigt. Weiter sind hier Michael N. Schmitt²² und Knut Dörrmann²³ anzuführen, welche sich ebenfalls mit der Anwendbarkeit des Humanitären Völkerrechts im Cyberspace auseinandersetzen.

National beschreibt die gesamtstaatlich aufgefasste Sicherheitsstrategie die Notwendigkeit der Umsetzung einer ebenso gesamtstaatlichen Strategie zur Cyber Sicherheit²⁴, welche im März 2013 verfügt wurde. In Österreich liegt – bezüglich der Entwicklung von Kapazitäten, um solchen Gefahren im und aus dem Cyberspace begegnen zu können – eine Kooperation zwischen Innen- und Verteidigungsministerium vor.

Österreichs Politik der inneren Sicherheit in diesem Bereich soll unter anderem nach folgendem Grundsatz gestaltet werden: „Erhöhung der Sicherheit von Computersystemen und des Internets durch Umsetzung der gesamtstaatlichen Strategie zur Cyber-Sicherheit, die Einrichtung eines Kompetenzzentrums zur Cyberkriminalität und die aktive Mitgestaltung der EU-Politik zum besseren Schutz der Bürger und Unternehmen im Cyberspace.“²⁵

Im Bereich der Verteidigungspolitik wird gefordert, dass der Schutz militärischer Einrichtungen vor Cyber Bedrohungen, auch in Zusammenarbeit mit geeigneten Partnern, zu verbessern ist und die hierzu entwickelten militärischen Fähigkeiten auch in das gesamtstaatliche Cyber Konzept einzubringen sind.²⁶ Im Rahmen der Assistenzleistung durch das

²⁰ Schmitt, Michael N. (Hrsg.): Tallinn Manual 2.0 on the International Law applicable to Cyber Operations, Cambridge University Press, New York 2017.

²¹ Ziolkowski, Katharina: Computernetzwerkoperationen und die Zusatzprotokolle zu den Genfer Abkommen. In: Humanitäres Völkerrecht Informationsschriften. Journal of International Law of Peace and Armed Conflict, Vol. 21, 2008, S. 202–213.

²² Schmitt, M.; Harrison Dinniss, H.; Wingfield, T.: Computers and War: The Legal Battlespace, Cambridge 2004.

<http://www.hpcrresearch.org/sites/default/files/publications/schmittetal.pdf>, [12.05.2020].

²³ Dörrmann, Knut: Applicability of the Additional Protocols to Computer Network Attacks, Genf 2004. <https://www.icrc.org/eng/resources/documents/misc/68lg92.htm>, [12.05.2020].

²⁴ Vgl. BKA, Österreichische Sicherheitsstrategie (ÖSS), 2013, S. 19.

²⁵ Ebd., S. 19.

²⁶ Vgl. ebd., S. 22.

Bundesheer sind zudem die Expertise- und Kapazitätenentwicklung²⁷ für Cyber Sicherheit²⁸ weiter auszubauen. Identifikationsmöglichkeiten für den Krieg im Netz und daraus abgeleitet eine genaue Zuordnung der Führungsverantwortung für den kriegesischen Akt im Cyberspace liefert der Empfehlungsteil nicht.

In der Strategie zur Cyber Sicherheit erfolgt lediglich eine Aufgabenzuweisung: „Aufgrund der über IKT [Informations- und Kommunikationstechnologie] hinausreichenden Betroffenheit und im Sinne der inneren Sicherheit übernimmt für übergreifende Bedrohungen der Cyber Sicherheit das BM.I die Federführung. Im Sinne der äußeren Sicherheit geht die Federführung für den Souveränitätsschutz im Rahmen der militärischen Landesverteidigung (Cyber Defence) auf das BMLVS über.“²⁹

Hier ist zwar eine Zuordnung von Aufgabenfeldern erfolgt, aber der Krieg im Cyberspace bleibt undefiniert. Diese Definition des Phänomens³⁰ und der Abgrenzung zu anderen Konfliktformen im Cyberspace ist noch zu leisten. Klar geht aus der Cyber Sicherheitsstrategie hervor, dass die Federführung im Cyber Defence Fall an das BMLVS übergeht. Undefiniert bleibt allerdings, wann dieser Cyber Defence Fall vorliegt. In der Österreichischen Strategie für Cyber Sicherheit werden die betroffenen Ressorts dazu angehalten „[...] Teilstrategien in ihren jeweiligen Verantwortungsbereichen [...]“³¹ zu erstellen. In der Teilstrategie Verteidigungspolitik ist die Beitragsleistung der Streitkräfte gegen Bedrohungen aus dem Cyberspace, vor allem im Zuge der militärischen Landesverteidigung und der Assistenzleistung für zivile Behörden, gefordert.³² Ungeklärt bleibt in diesem Strategiepapier auch wann genau das Phänomen Cyberwar vorliegt und daher die Führungsverantwortung beim Militär liegen sollte um der Bedrohung entsprechend begegnen zu können.

Eine klare Identifikation des Phänomens Cyberwar sowie eine Festlegung der daraus resultierenden Führungs- und Einsatzverantwortung erfolgt in der vorliegenden Literatur nur sehr oberflächlich. Zum Teil wird diese Festlegung in Konzepten und Strategiepapieren³³ getroffen, aber der Übergang zwischen den verschiedenen Konfliktformen im Cyberspace ist nicht oder nur unzureichend dargestellt. Wenn dies erfolgt, fehlt jedoch die Begründung für diese Grenze zwischen den Konfliktformen im Cyberspace.

²⁷ Anm. d. Verf.: Unter Kapazitätenentwicklung ist der Aufbau von Fähigkeiten zu verstehen, welche bei Bedarf durch das Innenministerium, analog der Assistenzleistungen im realen Raum, angefordert werden können. Dazu zählen Fähigkeiten in der Abwehr von Cyber Angriffen, der Wiederherstellung von angegriffenen Systemen und die Ausforschung von Urhebern solcher Angriffe.

²⁸ Vgl. BKA, Österreichische Sicherheitsstrategie (ÖSS), 2013, S. 22.

²⁹ BKA, Österreichische Strategie für Cyber Sicherheit (ÖSCS), Wien, März 2013, S. 11.

³⁰ Anm. d. Verf.: Hier geht es nicht um die Definition des Begriffes an und für sich, sondern um die Wesensmerkmale des Phänomens Cyberwar.

³¹ BKA, Österreichische Strategie für Cyber Sicherheit (ÖSCS), Wien, März 2013, S. 17.

³² Vgl. BMLVS, Teilstrategie Verteidigungspolitik 2014, Wien, Oktober 2014, S. 11f.

³³ Anm. d. Verf.: Dabei handelt es sich um die Cybersicherheitsstrategien folgender Staaten und Organisationen: Australien, Kanada, Deutschland, Frankreich, Großbritannien, Österreich, Vereinigte Staaten von Amerika, Europäische Union und NATO.

Im Zentrum der Betrachtung soll daher das Wesen des Krieges im Cyberspace in Abgrenzung zu anderen Konfliktformen in diesem Raum stehen. Es geht um den Cyberspace als neuen Handlungsraum von Krieg. Abgeleitet vom Begriff des Cyberspace und dem Kriegsbegriff wird der Bogen zum Cyberwar und der Rolle des Militärs in dieser „neuartigen“ Kriegsausprägung gespannt. Die Abgrenzung zu den verschiedenen Konfliktformen soll es ermöglichen, Krieg im Cyberspace als solchen zu erkennen, wenn dieses Phänomen tatsächlich in Erscheinung tritt.

Diese Abgrenzung kann an bestimmten Faktoren, der Intensität, der Intention und der Souveränitätsrelevanz, festgemacht werden. Wenn die Konfliktform der Intensität³⁴ nach sehr hoch, die ihr zu Grunde liegende Intention³⁵ keine individuelle, persönliche, der Bereicherung dienende ist und zudem noch eine Verletzung der Souveränität³⁶ darstellt, muss von einem Krieg im Cyberspace gesprochen werden.³⁷ Berücksichtigt werden muss, dass Handlungen anderer Konfliktformen (Kriegsverbrechen) auch in der Konfliktform des Krieges vorkommen, wie auch andere Konfliktformen (z.B. Kriminalität) die Form eines Krieges annehmen können.³⁸ Der Arbeit wird daher folgende forschungsleitende Frage zugrunde gelegt:

„Wann muss das Militär die Führungsverantwortung bei Angriffen im und aus dem Cyberspace übernehmen?“

Bei dieser Frage geht es um die generelle Abgrenzung des Krieges zu anderen Konfliktformen und daraus abgeleitet um die Verantwortung des Militärs im Cyberspace, als neuen Handlungsraum des Menschen, und damit auch der Verantwortung des Staates. Dabei stehen nicht nur die begriffliche Bestimmung des Phänomens Krieg im Cyberspace und dessen Identifikationsmöglichkeiten, sondern auch die rechtlichen Rahmenbedingungen für das Handeln des Militärs im Cyberspace, im Fokus der Betrachtungen. Wie das Phänomen Cyberwar identifiziert werden kann und welchen rechtlichen Rahmen das Militär als Handlungsgrundlage vorfindet, soll am Ende der Arbeit nachvollziehbar und abgeleitet dargestellt sein.

³⁴ Anm. d. Verf.: Die Intensität weist auf die Stärke des Konfliktes hin und ist zum Teil an den Auswirkungen ablesbar. Diese können unmittelbar oder mittelbar zu gravierenden Schäden an Personen und Material führen. Als Beispiel sind hier der Verlust von Menschenleben und/oder die Zerstörung von erheblichen Sachwerten zu nennen.

³⁵ Anm. d. Verf.: Die Intention liegt beim Krieg im politischen Zweck und nicht im Zweck sich persönlich zu bereichern. Diese persönliche Bereicherung kann dabei durchaus auch von Gruppen von Menschen verfolgt werden. Dies bedeutet, dass durchaus auch Staaten kriminelle Handlungen begehen können. Vereinfacht ist der Krieg auf das Allgemeinwohl und das Verbrechen auf das Wohl eines einzelnen als Zweck ausgerichtet.

³⁶ Anm. d. Verf.: Bei der Souveränität geht es um die generelle Handlungs- und Entscheidungsfähigkeit von Staaten. Ist diese angegriffen so kann der Konflikt in die Sphäre des Krieges verortet werden.

³⁷ Anm. d. Verf.: Die Deutungshoheit darüber, ob es sich um einen Cyberwar handelt, liegt dabei aber stets bei der politischen Führung. Nichtsdestotrotz braucht auch die politische Führung eine klar argumentierbare Entscheidungsgrundlage um einen Cyberwar auch als solchen identifizieren zu können.

³⁸ Anm. d. Verf.: Kriegsverbrechen auf der einen Seite und als Beispiel der Drogenkrieg in Mittel- und Südamerika auf der anderen Seite, zeigen, dass Krieg im Verbrechen und Verbrechen im Krieg verortet sein können.

Der Hauptteil der Arbeit ist in vier Abschnitte geteilt. Die Untersuchung des Cyberwar gliedert sich in die Herleitung des Kriegsbegriffes, die Auseinandersetzung mit dem Begriff des Cyberspace, die Definition und Erarbeitung des Begriffes vom Cyberwar und die rechtliche Untersuchung des Cyberspace.

Am Beginn der Arbeit werden ausgewählte geschichtliche Kriegsbegriffe einer *militärwissenschaftlichen* Untersuchung unterzogen. Ausgehend vom Kriegsbegriff bei Platon über den Begriff des Krieges bei Machiavelli und die kritisch-hermeneutische Diskussion des *naturrechtlichen* Kriegsbegriffs nach Grotius³⁹ wird zum *militärischen* Kriegsbegriff nach Clausewitz⁴⁰ übergeleitet. Hier soll die Basis für die Erarbeitung des Begriffes vom Cyberwar gelegt werden.

Den metatheoretischen Überbau der *militärwissenschaftlichen* Untersuchung liefert die philosophische Heuristik nach Leo Strauss. Strauss vertritt in seinem heuristischen Esoterizismus die These, dass Autoren, bezogen auf ihren Wirkungszeitraum und die gesellschaftlichen Umstände, ihre Ansichten in einer exoterischen Schreibweise verschleiert haben.⁴¹ Dies bedingt einen esoterischen Ansatz, um die wahren Standpunkte an das Licht zu bringen.⁴²

Wie Platon im sokratischen Dialog⁴³, geht es Strauss darum, aus bekannten Informationen auf unbekannte Inhalte zu schließen. Betrachtet man den Aufbau der Arbeit, so sieht man diesen dialektischen Theorieansatz darin, dass der Krieg nach Clausewitz der Ausgangspunkt der Dissertation ist und sich, unter Verwendung des metatheoretischen Ansatzes der Heuristik nach Leo Strauss, hin entwickelt zum Cyberwar, als eine Ausprägung des Kriegsbegriffes nach Clausewitz.

Im Rahmen dieses Ansatzes wird eine Kombination aus Hermeneutik, Quellenkritik, qualitativer Methode und realen Erfahrungen des Verfassers angewandt. Der gewählte heuristische Ansatz wird dabei von einer argumentativen Dialektik (These-Antithese-Synthese)⁴⁴ getragen und unterstützt. Die hermeneutische Methode, welche zur Anwendung gelangt, ist die kritische Hermeneutik nach Schleiermacher⁴⁵ in der Interpretation nach Clausewitz.

Schleiermacher unterscheidet zwischen zwei Methoden des Verstehens, wenn er davon spricht, dass „[...] alles Verstehen aus den zwei

³⁹ Kirchmann, J. H. (Hrsg.): Des Hugo Grotius drei Bücher über das Recht des Krieges und Friedens, Erster Band, Berlin 1869.

⁴⁰ Clausewitz, Carl von u.a.: Vom Kriege, Reinbek bei Hamburg 1963.

⁴¹ Vgl. Strauss, Leo; Kojève, Alexandre; Kittler, Friedrich: Kunst des Schreibens, Merve Verlag, Berlin 2009, S. 30f.

⁴² Vgl. ebd., S. 37ff.

⁴³ Vgl. Hartmann, Uwe: Carl von Clausewitz: Erkenntnis, Bildung, Generalstabsausbildung, Olzog Verlag, München 1998, S. 113.

⁴⁴ Anm. d. Verf.: Der dialektische Ansatz liegt darin begründet, dass Krieg und Kriminalität als These und Antithese einander gegenüberstehen und sich, unter Abgrenzung zu weiteren Konfliktformen im Cyberspace, zum Begriff des Krieges im Cyberspace synthetisieren.

⁴⁵ Vgl. Lücke, Friedrich (Hrsg.): Hermeneutik und Kritik mit besonderer Beziehung auf das Neue Testament von Dr. Friedrich Schleiermacher; Berlin 1838.

Momenten die Rede zu verstehen als herausgenommen aus der Sprache, und sie zu verstehen als Thatsache im Denkenden [...]“⁴⁶ besteht. Er beschreibt hier den Zusammenhang zwischen Sprache und dem, was mit dieser ausgedrückt werden soll.⁴⁷ Dort, wo beide Aspekte zusammentreffen, beginnt das Verstehen im hermeneutischen Sinn.⁴⁸

Clausewitz hat zusätzlich zu den Schleiermacherschen Kategorien des Verstehens – der grammatischen und der psychologischen Interpretation – das Verstehen von gesellschaftlichen Phänomenen in seine hermeneutische Methode integriert.⁴⁹ Dieser Ansatz ist im Zusammenhang mit der Analyse eines gesellschaftlichen Phänomens wie dem Krieg angezeigt und dadurch auch für die kritische Auseinandersetzung mit dem Cyberwar bestens geeignet. Jung führt in seiner Einführung zur Hermeneutik an, dass „[...] die Gegenstände des Verstehens Resultat einer sich ständig wandelnden kulturellen Sinnproduktion, die im engsten Zusammenhang mit technischen Entwicklungen steht [...]“⁵⁰ sind. Dies trifft in ganz besonderer Weise auf den Krieg und in weiterer Folge auch auf den Cyberwar zu. Als Form der sozialen Interaktion ist Krieg ganz besonders auf Verstehensleistungen angewiesen.⁵¹

Clausewitz beschreibt seine Methode einleitend in „Vom Kriege“ folgendermaßen: „Wir denken, die einzelnen Elemente unseres Gegenstandes, dann die einzelnen Teile oder Glieder desselben und zuletzt das Ganze in seinem inneren Zusammenhange zu betrachten, also vom Einfachen zum Zusammengesetzten fortschreiten. Aber es ist hier mehr als irgendwo nötig, mit einem Blick auf das Wesen des Ganzen anzufangen, weil hier mehr als irgendwo mit dem Teile auch zugleich immer das Ganze gedacht werden muß.“^{52 53}

Die Untersuchung des Kriegsbegriffes ist auf folgende Aspekte abgestützt durchzuführen:

- Welche Charakteristika kennzeichnen das Phänomen „Krieg“, sein Wesen und seine Natur?
- Welche Kategorien können den Krieg näher beschreiben?
- Worin unterscheidet sich der Krieg strukturell von anderen Konfliktformen?
- Welche Formen des Krieges sind beobachtbar?

⁴⁶ Lücke, 1838, S. 11f.

⁴⁷ Vgl. Jung, Matthias: Hermeneutik zur Einführung, Junius Verlag, Hamburg 2001, S. 65.

⁴⁸ Vgl. ebd., S. 66.

⁴⁹ Vgl. Hartmann, 1998, S. 103.

⁵⁰ Jung, 2001, S. 32.

⁵¹ Vgl. ebd., S. 17.

⁵² Clausewitz, Vom Kriege, S. 13.

⁵³ Anm. d. Verf.: Dies beschreibt den hermeneutischen Zirkel, welcher Clausewitz als Handlungsleitlinie zur Entwicklung einer Theorie des Krieges gedient hat und in der Abhandlung über den Cyberwar zur Anwendung gelangen soll. Auch Schleiermacher setzt den hermeneutischen Zirkel in das Zentrum des Verstehensprozesses. Er modifiziert ihn dahingehend, dass er kein geschlossener Zirkel, sondern vielmehr eine Spirale darstellt.

- Welche Rolle spielt der Kleine Krieg⁵⁴ im Verhältnis zum Großen Krieg⁵⁵?
- Welchen Stellenwert hat der Faktor Raum für den Krieg?

Im zweiten Abschnitt soll die begriffliche Basis der Thematik im Rahmen einer *verteidigungstechnologischen* Untersuchung aufbereitet werden. Hier wird der Cyberspace als technologischer Raum dargestellt und daraus abgeleitet seine Bedeutung als menschlicher Handlungsraum sowie als militärischer Einsatzraum untersucht.

Die Methode welche diesem Abschnitt zu Grunde gelegt ist, *ist die kybernetische Systemanalyse*. Dabei werden die wesentlichen Systemelemente, in Abgrenzung zur Systemumwelt des Cyberspace, dargestellt. Die Beziehung zwischen den Elementen sowie die Systemeigenschaften des Systems Cyberspace stehen dabei im Fokus. Hier wird der Begriff des Cyberspace nicht nur reduziert auf die technischen Komponenten und ihr Zusammenwirken verstanden, sondern darüber hinaus als System, in welchem letztlich auch der Mensch als Teil desselben zu verstehen ist.⁵⁶

Bei der Analyse des Cyberspace werden daher vor allem die Kybernetik nach Norbert Wiener⁵⁷ und die Informationstheorie nach Claude E. Shannon⁵⁸ zur Untersuchung des Gegenstandes herangezogen.

Folgende Fragestellungen werden dabei näher beleuchtet:

- Welche Momente umfasst der Cyberspace?
- Was charakterisiert den Cyberspace als Handlungsraum des Menschen?
- Wie begrenzt bzw. entgrenzt ist der Cyberspace?
- Welche Rolle spielen Zeit und Raum in der Cyber Thematik?
- Welchen Stellenwert hat der Cyberspace als Einsatzraum für das Militär?

Aufbauend auf die militärwissenschaftliche Begrifflichkeit vom „Krieg im Airspace“ nach Douhet⁵⁹ und die Ergebnisse der militärtheoretischen Untersuchung zum Kriegsbegriff sowie der verteidigungstechnologischen Analyse des Cyberspace, wird der Krieg im Cyberspace in Analogie zu Douhet erarbeitet. Hier wird die gleiche methodische Vorgehensweise wie beim Kriegsbegriff selbst angewandt. Dabei orientiert sich der Prozess des

⁵⁴ Anm. d. Verf.: Unter Kleinem Krieg werden traditionell militärische Verfahren verstanden, die zwar von Elementen konventioneller Streitkräfte ausgeführt werden, jedoch von subkonventionellem Charakter sind. Dazu zählen z.B. Kommandounternehmen, Hinterhalte und Überfälle.

⁵⁵ Anm. d. Verf.: Der Große Krieg ist die konventionelle Auseinandersetzung von Streitkräften im Kampf.

⁵⁶ Klauninger, Bert: Cyberspace als ein selbstorganisierendes System, o.J. http://archive.gpi-online.de/files/_klauninger_cyberspace.pdf, [12.05.2020].

⁵⁷ Wiener, Norbert: Kybernetik. Regelung und Nachrichtenübertragung im Lebewesen und in der Maschine, 1948.

⁵⁸ Shannon, Claude: A Mathematical Theory of Communication, 1948.

⁵⁹ Douhet, Giulio: Luftherrschaft, Berlin 1935.

Verstehens auch an der Ausrichtung auf entsprechende zukünftige Entwicklungen, im Speziellen in der Sphäre des Cyberwar.

Diese divinatorische Komponente findet sich sowohl bei Clausewitz als auch bei Schleiermacher.⁶⁰ Hartmann führt dazu Folgendes aus: „Wie bei Schleiermacher ist Verstehen bei Clausewitz ein methodisch geleitetes Vorgehen, das aus einem Ineinander von grammatischer und psychologischer Interpretation besteht und notwendig durch divinatorische Elemente ergänzt werden muss, um zukünftige Entwicklungen von Krieg und Kriegführung zu erfassen.“⁶¹ Verstehen ist dabei nicht nur als reproduktive Methode zu begreifen, sondern als kreativer Vorgang, der Neues hervorbringt.⁶²

Ausgehend von der Untersuchung des Kriegsbegriffes und der verteidigungstechnologischen Untersuchung, erschließen sich die wesentlichen Erkenntnisse für den Cyberwar über folgende Fragestellungen:

- Was ist jeweils unter Krieg und den weiteren Konfliktformen im Cyberspace zu verstehen?
- Welche Handlungsweisen und Interaktionsformen sind im Cyberspace zu beobachten?
- Welcher Typologie des Krieges ist der Cyberwar zuzuordnen?
- Kann es einen Krieg ohne Cyberwar geben?
- Ist Cyberwar mit anderen Modi der Kriegführung vergleichbar?
- Welche Rolle spielt der Cyberwar für das Militär bzw. welche Rolle sollte er spielen?

Diese *militärwissenschaftliche* und *verteidigungstechnologische* Untersuchung wird gefolgt von einer kritischen Darstellung der internationalen und nationalen *rechtlichen Rahmenbedingungen* für den „Krieg im Cyberspace“ in terminologischer und kompetenzrechtlicher Abgrenzung zu den anderen Konfliktformen im Cyberspace (etwa anhand der Definitionen der *Cybercrime Convention* des Europarates⁶³).

Die Untersuchung der Rechtslage basiert darauf, dass die rechtlichen Vorschriften zunächst dargestellt und hinsichtlich ihrer Anwendbarkeit im Cyberspace geprüft werden. Dies erfolgt in Form einer hermeneutisch-kritischen Analyse der Rechtsgrundlagen des militärischen Einsatzes im Cyberspace. Darauf aufbauend wird das Völkerrecht und in weiterer Folge das Europarecht (inklusive der relevanten EU-Strategiepapiere, wie z.B. Cybersicherheitsstrategie der EU, EU Cyber Defence Policy Framework) untersucht und hinsichtlich der Anwendbarkeit im Falle eines Cyberwar dargestellt. Abschließend folgt die Darstellung und Analyse der nationalen Rechtsgrundlagen (inklusive der Strategiepapiere, wie z.B. ÖSS, ÖCSC, Teilstrategie Verteidigungspolitik) zum Einsatz des Militärs im Cyberspace.

⁶⁰ Vgl. Hartmann, 1998, S. 111.

⁶¹ Ebd., S. 111.

⁶² Vgl. Jung, 2001, S. 21.

⁶³ <https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/090000168008157a>, [12.05.2020].

Die Untersuchung der Rechtslage geht folgenden Fragestellungen nach:

- Welche Rechtsnormen befassen sich mit dem Cyberspace?
- Wie ist die rechtliche Ordnung im Cyberspace gestaltet?
- Welche Rechtsnormen beschäftigen sich mit dem Einsatz des Militärs im Cyberspace?
- Welches Vorgehen des Militärs im Cyberspace ist rechtlich gedeckt?
- Ist der vorhandene Rechtsrahmen auf den Cyberwar, d.h. für den Einsatz des Militärs im Cyberspace, anwendbar?
- Welcher rechtliche Anpassungsbedarf lässt sich für den Einsatz des Militärs im Cyberspace ableiten?

In der Dissertation soll diskutiert werden, ob der existierende Rechtsrahmen in der Lage ist, die neue Form des Krieges fassen und dem Militär die entsprechende Handlungsgrundlage bereitstellen zu können.

Die Zielsetzungen der Arbeit sind:

- die hermeneutisch-philosophische Betrachtung des Krieges, die Ergründung des Wesens des Krieges, um daraus die Abgrenzung zu anderen Konfliktformen zu treffen und die Grundlage für die Ableitung des Wesens des Cyberwars zu schaffen;
- die Betrachtung des Cyberspace hinsichtlich dessen Rolle als neuem Konfliktraum sowie hinsichtlich der Besonderheiten in diesem, um die Notwendigkeit staatlichen Eingreifens darzustellen und damit auf die Relevanz für das Militär zu schließen;
- die Verortung des Cyberwar als Moment des Krieges und die Darstellung der Rolle von Streitkräften im Cyberspace;
- die Darstellung und Analyse der rechtlichen Rahmenbedingungen im Cyberspace als Handlungsgrundlage des Militärs im Cyberwar, um die Führungsverantwortung des Militärs, abgeleitet von den Akteuren denen sie gegenüberstehen und den von diesen ausgehenden Bedrohungen, darzustellen, mit dem Zweck, einen Beitrag im Rahmen der Militärwissenschaften zu erbringen, der eine Identifikation des Phänomens Krieg im Cyberspace ermöglicht und die Bereitstellung eines Argumentariums⁶⁴ für die Rolle der militärischen Streitkräfte im Cyberspace liefert.

In Anbetracht der jüngsten Ereignisse, rund um den islamistischen Terror in Frankreich, Belgien, Russland, der Türkei, im Maghreb und im Nahen Osten, der Vorgänge auf der Krim und im Donbass, aber auch bei den polizeilichen Übergriffen gegen afroamerikanische Jugendliche in den Vereinigten Staaten von Amerika, der Beeinflussung demokratischer Prozesse aus dem Cyberspace und der Diskussion um hybride

⁶⁴ Anm. d. Verf.: Hier geht es um eine Beurteilungsgrundlage für die politische Führung, um den Cyberwar zu identifizieren und damit die Aufgabe, in diesem zu handeln, dem Militär zuordnen zu können.

Konfliktaustragung⁶⁵, geht es in der öffentlichen Auseinandersetzung genau um die Identifikation von Krieg und kriegerischem Akt. Die Militarisierung der Polizei einerseits und die Verwendung des Militärs für polizeiliche Aufgaben – die Konstabilisierung – stellen die politischen Verantwortungsträger vor neue alte Herausforderungen. Dieser unklare Übergang zwischen Krieg und anderen Konfliktformen in der realen Welt manifestiert sich auch im neuen Handlungsraum der Menschen, dem Cyberspace.

Der Mehrwert der Dissertation liegt darin – bezogen auf ein gesamtstaatliches, Organisationen übergreifendes Handeln – eine begründete Entscheidungshilfe bereitzustellen, um die Identifikation des Cyberwar und die Festlegung der Führungsverantwortung in einem Einsatz zur Begegnung dieser Bedrohung aus dem Cyberspace, der Cyber Defence, zu ermöglichen.

Da Vorgaben für das militärische Vorgehen im Cyberspace nur sehr oberflächlich in der vorhandenen Literatur dargestellt werden, ist es das Bestreben der vorliegenden Arbeit diese Unschärfe genauer zu untersuchen und aufzulösen.

Die Dimension der konfliktiven Auseinandersetzung kann letztlich bis zum einzelnen Mobiltelefon-Nutzer getragen werden. Um entsprechend handeln zu können, ist das Phänomen Cyberwar herauszuarbeiten und darzustellen.

Zu Beginn der Dissertation werden die grundlegenden Begriffe der Arbeit dargestellt und definiert. Die Begriffsdefinitionen stützen sich in erster Linie auf einschlägige Literatur zum Themenkomplex des Krieges. Neben diesen Basisbegriffen werden die zentralen Begriffe, welche in der Arbeit verwendet werden, in den vier Hauptkapiteln des Argumentum erarbeitet.

Zunächst soll der Begriff des Gemeinwesens definiert werden, dann geht es um den Politikbegriff, der wesentlich für den Kriegsbegriff und seine Abgrenzung zur Kriminalität ist. Weiters wird der Begriff der Sicherheit und im Zusammenhang damit das Gewaltmonopol dargestellt. Für die Herausarbeitung der Schwelle für die Zuordnung der Führungsverantwortung zwischen Polizei und Militär ist besonders der Begriff der Souveränität von Bedeutung, dieser bildet den Abschluss des Definitionsteils.

Gemeinwesen sind der Zusammenschluss mehrerer Menschen, da ein Mensch den anderen braucht, um den verschiedenen Herausforderungen des Lebens entgegentreten zu können. Platon führt dazu aus:

⁶⁵ Anm. d. Verf.: Vorgänge im Cyberspace sind vielfach Teil hybrider Konfliktaustragung, die Arbeit behandelt allerdings nicht hybride Konflikte und die Kompetenzzuordnung darin, sondern widmet sich ausschließlich dem Phänomen Cyberwar.

„Es entsteht also, sprach ich, eine Stadt [Anm. d. Verf.: Stadt als Gemeinwesen.], wie ich glaube, weil jeder einzelne von uns sich selbst nicht genügt, sondern vieler bedarf.“⁶⁶

Gemeinwesen entstanden und entstehen aus Bedrohungen heraus. Da der einzelne nicht in der Lage ist sich auf Grund seiner beschränkten Macht im Dasein zu erhalten und sich gegen Gefahren durchhaltend zu wehren, schloss er sich mit anderen zusammen um aufgabenteilig diesen Gefahren zu widerstehen. Machiavelli verweist zur Entstehung von Gemeinwesen auf Folgendes:

„Um diesen Gefahren zu entgehen, ziehen sie sich aus eigenem Entschluß oder auf Veranlassung eines Mannes, der bei ihnen in besonderem Ansehen steht, an den Ort ihrer Wahl zurück, wo sie bequemer leben und sich leichter verteidigen können.“⁶⁷

Es handelt sich beim Gemeinwesen also um einen Zusammenschluss mehrerer Menschen zum Zweck des guten Lebens und der Verteidigung vor Gefahren.⁶⁸ Dieser Zusammenschluss führt auch zur Vermehrung der Macht. Spinoza sieht den Menschen nicht in der Lage sich im Zustand des Naturrechts vor allen Bedrohungen zu schützen.⁶⁹ Stadler führt dazu aus:

„Gesteigerte Sicherheit durch Machtvervielfachung ist der Kern von Staatlichkeit.“⁷⁰

Ein weiterer Aspekt für Spinoza ist die Tatsache, dass der Mensch ohne Austausch mit anderen sich geistig nicht entwickeln kann.⁷¹ Zum guten Leben und der Sicherheit kommt hier der Bildungsaspekt hinzu. Recht bedarf der Macht, denn

„Macht schafft Recht, nicht umgekehrt; denn ein Recht ohne Macht gilt nicht und Macht ohne Recht ist Unheil.“⁷²

Auch für Spinoza gehen Recht und Macht Hand in Hand und so fußt das Gemeinwesen für ihn auf der Grundlage gemeinsamer Rechtsgesetze, einer gemeinsamen Rechtsordnung, die den Rahmen für das Zusammenleben zur Verwirklichung von Sicherheit, Bildung und gutem Leben darstellt.⁷³ Der Mensch ist ein affektbehaftetes Wesen, menschliche Affekte sind kein Fehler sondern Eigenschaft des Menschen.⁷⁴ Der Mensch unterliegt Affekten und bedarf einer Ordnung um diese zu hegen. Da

⁶⁶ Platon: Sämtliche Werke. Lysis, Phaidon, Kleitophon, Politeia, Phaidros, 33. Aufl., Reinbek bei Hamburg 2011, S. 259.

⁶⁷ Machiavelli, Niccolò; Zorn, Rudolf: Der Fürst. Il principe, 6. Aufl., Stuttgart 1978, S. 7.

⁶⁸ Vgl. Kleemeier, Ulrike: Grundfragen einer philosophischen Theorie des Krieges. Akademie Verlag, Berlin 2002, S. 83.

⁶⁹ Vgl. Spinoza, Benedikt; Bartuschat, Wolfgang: Politischer Traktat. Lateinisch - deutsch = Tractatus politicus, 2. Aufl., Hamburg 2010, S. 17.

⁷⁰ Stadler, Christian: Krieg, 1. Aufl., Wien 2009, S. 59.

⁷¹ Vgl. Spinoza, Politischer Traktat, S. 17.

⁷² Freudenberg, Dirk: Theorie des Irregulären. Partisanen, Guerillas und Terroristen im modernen Kleinkrieg, 1. Aufl., Wiesbaden 2008, S. 61.

⁷³ Vgl. Spinoza, Politischer Traktat, S. 17.

⁷⁴ Vgl. ebd., S. 9.

Menschen immer danach streben an vorderster Stelle zu stehen, ergeben sich zwangsläufig Konflikte.⁷⁵ Um diese Konflikte und auch die Affekte einzuhegen bedarf es des Rechts.

Der Staat stellt nun eine besondere Form des Gemeinwesens dar. Ein Staat ist

„[...] als Gemeinschaft, im Rahmen einer politischen und auf bestimmten sittlich-rechtlichen Normen beruhenden Ordnung, die Merkmale des Staatsvolkes, des Staatsgebietes und der Staatsgewalt aufweist.“⁷⁶

zu verstehen. Diese Elemente finden sich auch in der Definition für das Gemeinwesen von Machiavelli; auch er spricht also schon von dieser speziellen Form des Gemeinwesens. Diese Definition des Staates ist auch völkerrechtlich verankert. Zentraler Bestandteil für den Staat ist eine rechtliche Ordnung auf Grund deren die Organe des Staates ihre Tätigkeit ausführen. Der Staat ist die verkörperte Gerechtigkeit, in der im platonischen Sinn jeder das Seine tut. Das Handeln zur Verwirklichung des guten Lebens, des Gemeinwohls, ist die Politik, welche als nächster Begriff zu definieren ist.

Im Zusammenhang mit dem Staat und dem Krieg stellt die Politik einen wesentlichen Faktor dar. Im ursprünglichen Sinn ist Politik die

„[...] Bezeichnung für das öffentliche Leben der stimmberechtigten Bürger eines Gemeinwesens [...]“. ⁷⁷

Politik vollzieht sich in verschiedenen Bereichen, dem nach innen gerichteten Politikbereich, der sich mit der Organisation und Lenkung des Staates beschäftigt und dem nach außen gerichteten Bereich, der sich mit den Beziehungen der Staaten zueinander auseinandersetzt. Ziel der Politik ist die Steuerung des Handelns innerhalb und zwischen den Gemeinwesen.

„Soziale Systeme bilden und stabilisieren sich über eine sinngeladete Differenzierung von Innen (zum System gehörig) und Außen (Umwelt).“⁷⁸

Dazu bedient die Politik sich dreier Elemente, den Politics, der Politie und der Policy. Politics behandelt den prozessualen Aspekt, Politie die Form der Politik und die Policy den inhaltlichen Aspekt.⁷⁹ Da die Politik bestimmend ist im Handeln nach innen wie nach außen, berührt sie sowohl den Krieg, als auch das Verbrechen, allerdings in unterschiedlicher Ausprägung. Der Staat handelt durch seine Institutionen zum Wohle des Gemeinwesens, wobei dieses Handeln als Politik zu bezeichnen ist.⁸⁰

⁷⁵ Vgl. ebd., S. 9.

⁷⁶ Stupka, Andreas: Militärwissenschaften. Ihre Grundlagen und ihr System, Wien 2011, S. 54.

⁷⁷ Schmidt, Manfred G.: Wörterbuch zur Politik, 2. Aufl., Stuttgart 2004, S. 538.

⁷⁸ Freudenberg, 2008, S. 40.

⁷⁹ Vgl. Schmidt, 2004, S. 538.

⁸⁰ Vgl. Stupka, 2011, S. 21.

Politik dient der Hegung von Konfliktualität nicht nur im Sinne eines Krieges, sondern auch im Sinne der Entwicklung und Verbesserung des Gemeinwesens, im Rahmen der Innenpolitik. Sie umfasst die Tätigkeit des Staates zur Erreichung von Zielen durch Einsatz von Ressourcen des Gemeinwesens, um Problemstellungen zu lösen. Diese betreffen in erster Linie das Gemeinwohl bzw. die Erreichung von Zielen, die für das Zusammenleben der Bürger des Staates von Bedeutung sind, wie die Sicherung des Friedens.⁸¹

Spinoza beschreibt explizit, dass den höchsten Gewalten im Staat das Recht zusteht, festzulegen

„[...] was jeder einzelne oder alle zusammen zu tun und zu lassen habe.“⁸²

Zu den weiteren Aufgaben der Staatsgewalt zählen das Recht Gesetze zu erlassen, deren Auslegung, also die Rechtsprechung, sowie das Recht Krieg zu erklären und Friedensverhandlungen zu führen.⁸³

„Da diese Aufgaben einschließlich der dafür einzusetzenden Mittel alles Geschäfte sind, die den ganzen Körper des Staates betreffen und darin das ausmachen, was man Staatsgeschäfte nennt, hängen sie auch einzig und allein von der Leistung desjenigen ab, der die Souveränität des Staates in Händen hat.“⁸⁴

Diese Staatsgeschäfte sind als Politik im vorhin beschriebenen Sinne zu verstehen.

„[...] und die öffentlichen Aufgaben, die der Leitung dessen unterliegen, der die Regierungsgewalt in Händen hält, heißen Staatsgeschäfte.“⁸⁵

Politik umfasst somit Aufgaben um den Staat zu erhalten und weiter zu entwickeln.

„Wer mehr auf den Lärm und das Geschrei solcher Parteikämpfe [Anm. d. Verf.: Gemeint sind innenpolitische Kämpfe.] sieht als auf deren gute Wirkungen, der bedenkt nicht, daß in jedem Gemeinwesen das Sinnen und Trachten des Volks und der Großen verschieden ist und daß alle zu Gunsten der Freiheit entstandenen Gesetze nur diesen Auseinandersetzungen zu danken sind.“⁸⁶

Gesetze sind ein Ausdruck, ein Ergebnis der Politik, welches sich im Konflikt zwischen den Parteien ergibt. Politik ist also im Fluss und ständige Reibung zwischen den politischen Einheiten.⁸⁷ Das aus dem Konflikt hervorgebrachte Recht dient in weiterer Folge wiederum der Einhegung des

⁸¹ Vgl. Schmidt, 2004, S. 539.

⁸² Spinoza, Politischer Traktat, S. 30.

⁸³ Vgl. ebd., S. 30f.

⁸⁴ Ebd., S. 31.

⁸⁵ Ebd., S. 21.

⁸⁶ Machiavelli, Der Fürst, S. 19.

⁸⁷ Vgl. Stadler, 2009, S. 18.

Konfliktes im Inneren.⁸⁸ Zur Politik im Inneren des Staates tritt die politische Auseinandersetzung zwischen den Staaten, in welcher die verschiedenen Interessen, teils ohne Gewaltanwendung, mittels Verhandlungen, und teils mit Gewaltanwendung, dem Krieg, behauptet werden.⁸⁹

Auch Clausewitz versteht Politik einerseits als soziopolitische Verhältnisse im Inneren und andererseits als internationale Beziehungen.⁹⁰ Der politische Zweck ist demnach auch in der Beeinflussung dieser beiden Bereiche zu finden.⁹¹ Die Verbindung zwischen Krieg und Politik ist hier bereits klar zu sehen. Ein großer Teilbereich der Politik, die Sicherheitspolitik, beschäftigt sich mit der Sicherheit des Staates, diese soll im Folgenden dargestellt werden.

Die Auseinandersetzung mit dem Sicherheitsbegriff und der Grenze zwischen innerer und äußerer Sicherheit ist für die Kompetenzzuordnung von Bedeutung. Gemäß der oben beschriebenen Aufteilung gibt es Aspekte beider Seiten der Sicherheit. Die Trennung in diese beiden Bereiche ist ein wichtiger Teil der Arbeit. Um diese Trennlinie, die Schwelle zwischen den Teilbereichen, erarbeiten zu können, ist die grundsätzliche Definition von Sicherheit voranzustellen.

Sicherheit kann generell als Abwesenheit von Unsicherheit gesehen werden. Dabei spielen Bedrohungen eine entscheidende Rolle.⁹² Sind diese nicht oder nur sehr schwach vorhanden, so herrscht ein Zustand der Sicherheit. Innere Bedrohungen gehen dabei vom Gemeinwesen selbst oder seinen Mitgliedern aus, während äußere Bedrohungen von anderen Gemeinwesen ausgehen. Für die Kompetenzzuordnung ist eine Unterscheidung in Innen und Außen wesentlich. So kann eine Zuordnung der Gefahren im Inneren an die Polizei und die Zuordnung der äußeren Gefahren an das Militär erfolgen.

Bedrohungen wirken auf die Institutionen und die Ordnung des Gemeinwesens. Hierbei kann zusätzlich zu Innen und Außen auch zwischen Störungen und existenzieller Bedrohung der staatlichen Ordnung unterschieden werden. Ordnet man die erste Gefahr der Polizei zu und die zweite dem Militär, erkennt man die Problematik, dass beide Ansätze nicht zur Deckung gebracht werden können, denn es können Störungen von außen nach innen getragen werden und existenzielle Bedrohungen auch im Inneren entstehen. Verschärft wird diese Divergenz durch den Umstand, dass innen und außen zusehends miteinander verschmelzen.⁹³

Aufgabe des Staates ist es das Gemeinwesen zu schützen. Die Aufgabe der Politik liegt im Abbau von Unsicherheiten, hier liegt die Verbindung zur Politik. Da es keine absolute Sicherheit gibt, ist das Gemeinwesen dazu bestimmt, ein Maß an Unsicherheit zu ertragen. Da die subjektive

⁸⁸ Vgl. ebd., S. 18.

⁸⁹ Vgl. Stupka, 2011, S. 128f.

⁹⁰ Vgl. Jäger, Thomas; Beckmann, Rasmus: Carl von Clausewitz' Theorie des Krieges. In: Jäger, Thomas; Beckmann, Rasmus: Handbuch Kriegstheorien, Wiesbaden 2011, S. 216.

⁹¹ Vgl. ebd., S. 219.

⁹² Schmidt, 2004, S. 638.

⁹³ Vgl. Freudenberg, 2008, S. 77f.

Wahrnehmung von Gefahr auch an die Sichtbarkeit dieser gebunden ist, werden Bedrohungen in der heutigen Zeit nicht mehr so einfach wahrgenommen.⁹⁴

Dies vermindert die Akzeptanz für die Notwendigkeit des Militärs. Viele Probleme und militärische Bedrohungen sind nicht mehr fassbar und damit aus unserer Wahrnehmung gerückt. Die Aufgabe des Staates ist es, diese Gefahren zu erkennen und die entsprechenden Maßnahmen zu veranlassen. Die Politik hat dem Bürger zu erklären, dass für die Gemeinschaft ein Schutz, auch gegen nicht vordergründig wahrnehmbare Gefahren, sicher zu stellen ist.⁹⁵

Es kann aber im Staat nicht nur zwischen innerer und äußerer Sicherheit unterschieden werden, sondern es tritt auch die individuelle Sicherheit zunehmend in den Fokus der Gesellschaft. Dieser Trend führt zu einem Abbau staatlicher Sicherheit. Zu Gunsten des Wohlstands des einzelnen Bürgers wird die individuelle Sicherheit, auf Kosten der Sicherheit aller, gesteigert. Diese Unsicherheit bringt den Staat in eine schwierige Lage. Da moderne Demokratien Konflikte kaum mehr militärisch austragen, ist die Notwendigkeit, Mittel zur Sicherstellung der äußeren Sicherheit bereitzustellen gegenüber den Bürgern kaum noch vertretbar. Dies wird durch die aktuellen Diskussionen über das Verteidigungsbudget in Österreich, aber auch im umliegenden europäischen Umfeld verdeutlicht.

Die Schaffung von Sicherheit durch den Staat, als Staatszweck und Grundlage der staatlichen Existenz, tritt zu Gunsten der oben erwähnten Unsicherheit in den Hintergrund. Sicherheit bestimmt aber auch im Umfeld demokratischer Staaten die Beziehung zwischen diesen. Auch wenn der bewaffnete Konflikt zwischen Staaten in den Hintergrund zu treten scheint, erscheinen neue Akteure auf dem Feld des Krieges. Durch die Fokussierung auf den individuellen Wohlstand, erfährt die Gesellschaft eine erhöhte Verwundbarkeit.⁹⁶ Unsicherheit als Abwesenheit von staatlicher Sicherheit führt zu einem Scheitern der Staatlichkeit. Beispiele hierzu finden sich in Afghanistan oder dem Irak.

Sicherheit und Staat bedingen einander. Es ist hier angezeigt klar zwischen individueller Sicherheit als menschlichem Grundbedürfnis und nationaler Sicherheit als Basis für die Existenz des Staates zu unterscheiden. Zwischen beidem gibt es eine Abhängigkeit, allerdings muss hier eine gewisse Ausgeglichenheit herrschen. Sicherheit als nationale Sicherheit kann als Dasein von Identität und Integrität des Staates verstanden werden. Der Staat hat somit, durch seine Bürger legitimiert, dafür Sorge zu tragen, dass ein die Sicherheit gewährleistender Ordnungsrahmen den Naturzustand der Menschen, im Konflikt zu leben, einhegt.⁹⁷

Hier liegt das Hauptproblem moderner demokratischer Staaten; sie haben im Wesentlichen ihre Bedrohungen, in Form eines Krieges, verloren.

⁹⁴ Vgl. ebd., S. 69ff.

⁹⁵ Vgl. ebd., S. 70f.

⁹⁶ Vgl. ebd., S. 77.

⁹⁷ Vgl. Kirchmann, 1869, S. 185.

Ohne diese Klammer zerfällt die nationale Sicherheit in lauter individuelle Sicherheitsbedürfnisse. Es kann daraus gefolgert werden, dass Bedrohungen für die Sicherheit und Existenz von Staaten notwendig sind.⁹⁸

Als Bedrohung kann dabei der Wille und das Vermögen verstanden werden, welches einen Akteur zu feindlich gesinnten Handlungen befähigen. Eine Bedrohung

„[...] liegt dann vor, wenn durch einen Akteur mit einem Potenzial (Kräfte, Mittel, Verfahren) und einer Intention (Absicht) eine Situation oder Entwicklung hergestellt werden kann, die sich negativ auf eine Person oder Sache auswirkt.“⁹⁹

Der Staat wird nur solange gebraucht als nur er in der Lage ist die Menschen vor Gefahren zu schützen. Dies ist die Grundlage für das staatliche Gewaltmonopol. Der Staat entledigt den Bürger von seiner Aufgabe sich selbst zu verteidigen unter Garantie seiner Sicherheit, um Kapazitäten für die Beitragsleistung zur Verwirklichung der Gerechtigkeit zu schaffen.¹⁰⁰

Der Staat schafft also einen inneren Ordnungsrahmen durch das Recht und schützt seine Bürger auch vor äußeren Gefahren. Bedrohung schafft ein Bedürfnis nach Sicherheit, welches im Staat verwirklicht werden kann. Der Staat schafft Sicherheit. Überall, wo es zu einer Entstaatlichung kommt steigt automatisch die Unsicherheit. Entstaatlichung ist somit gleichbedeutend mit Unsicherheit. Um ein Staatswesen zu erhalten muss der Staat die Sicherheit gewährleisten. Erst dann ist es möglich, dass sich alle anderen Aspekte eines gesellschaftlichen Lebens entwickeln können. Daraus folgt, dass Sicherheit die Kernaufgabe des Staates ist.¹⁰¹

Das Auftreten nichtstaatlicher Gewaltakteure (im Inneren die Kriminalität, im Äußeren der Terrorismus) setzt das Gewaltmonopol außer Kraft und führt daher auch zu einer Aushöhlung der Rechtsordnung, zum Recht des Stärkeren. Das Resultat daraus ist ein permanenter Zustand der Unsicherheit für die Bürger des Staates.¹⁰² Bezugnehmend auf die Evolution des Krieges ist festzustellen, dass zwischenstaatliche Konflikte zusehends in den Hintergrund treten. Die Bedrohungen für den Staat gehen zumeist nicht mehr von anderen Staaten aus, sie sind nicht mehr zwischenstaatlicher Natur.

Die zunehmende Globalisierung führt zu einem anderen Typus von Konflikt. Vielfach wirken Akteure (Kriminelle, Terroristen, Wirtschaftsunternehmen,...) global innerstaatlich, dies bedeutet, dass Akteure in der Lage sind, über Grenzen hinweg Unsicherheit von innen im Staat aufzubauen. Terrorismus verfügt über diese Möglichkeiten, ebenso wie die Kriminalität. Diese Bedrohungen werden auch über verschiedene Mittel

⁹⁸ Vgl. Spinoza, Politischer Traktat, S. 32.

⁹⁹ BMLVS, Erlass zur Neuregelung des Begleitschutzes, GZ S92000/199-GStbAbt/2010, Verfügung, Wien, Februar 2010, S. 1.

¹⁰⁰ Vgl. Kirchmann, 1869, S. 185.

¹⁰¹ Vgl. Spinoza, Politischer Traktat, S. 35.

¹⁰² Vgl. Kirchmann, 1869, S. 188.

wirksam, eines davon ist der Cyberspace, der zu einer Verstärkung der Entgrenzung von Konflikten beitragen wird.¹⁰³

Um den Bedrohungen begegnen und Sicherheit gewährleisten zu können, bedient sich der Staat des Gewaltmonopols.

In der Gemeinschaft übernimmt diese, die aus dem Naturrecht erwachsene Aufgabe, das Recht des Einzelnen, sich in seinem Dasein zu erhalten. Naturrechtlich steht jedem das Recht auf Erhalt im Dasein zu. Dieses Recht, auch Gewalt zur Abwehr von Gefahren für das Dasein anzuwenden, wird an den Staat abgetreten.¹⁰⁴ Dieses Abtreten der eigenständigen Verteidigung an das Gemeinwesen bedingt, dass dieses in der Lage ist seine Mitglieder zu schützen. Die deutsche Gerichtsbarkeit versteht unter Gewalt Folgendes:

„Der Begriff Gewalt bedeutet Etwas mit Zwang vor allem psychisch und physisch durchzusetzen. Dabei gibt es zwei Parteien. Zum einen den Täter, der die Gewalt ausübt und auf der anderen Seite das Opfer. In der Rechtsprechung wird Gewalt definiert als körperlich wirkender Zwang durch die Entfaltung von Kraft oder durch sonstige physische Einwirkung, die nach ihrer Intensität dazu geeignet ist, die freie Willensentschließung oder Willensbetätigung eines anderen zu beeinträchtigen.“¹⁰⁵

Es kann demzufolge zwischen körperlicher und psychischer Gewalt unterschieden werden. Gewalt wird oft synonym für die Anwendung körperlichen Zwanges verwendet, weil sie im Allgemeinen einfacher wahrnehmbar ist. Die Wahrnehmung spielt also für das Erkennen von Gewalt eine entscheidende Bedeutung. Eine besondere Art der Gewalt ist die Staatsgewalt, welche durch Ausübung beider Formen der Gewalt wirksam wird.

„Die Staatsgewalt ist die unmittelbare, oberste, umfassende und ausschließlich geordnete politische Herrschaftsgewalt in einem Staat.“¹⁰⁶

Es bedarf Institutionen, welche in der Lage sind Gewalt zum Schutz des Gemeinwesens und der einzelnen Mitglieder ausüben zu können. Diese Fähigkeit äußert sich im Gewaltmonopol des Staates, des Gemeinwesens. Staatsgewalt ist in ihrem Vollzug auf verschiedene Staatsorgane verteilt. Dabei übernimmt der Staat die Aufgabe den Einzelnen und damit die Gemeinschaft im Sein zu erhalten.

„Nach dem Naturrecht haben zwar Alle, wie erwähnt, das Recht, Schaden von sich abzuhalten. Aber wenn die bürgerliche Gesellschaft zum Schutze der öffentlichen Ruhe eingerichtet ist, so erwächst

¹⁰³ Vgl. Freudenberg, 2008, S. 38.

¹⁰⁴ Vgl. Konegen, Norbert: Zum Staatsverständnis von Hugo Grotius. in: IFS-Nachrichten, Vol. 1998, S. 21.

¹⁰⁵ Bundesgerichtshof, Neue Juristische Wochenschrift, 1995, S. 2643.

¹⁰⁶ <https://richtervereinigung.at/justiz/rechtssystem/staatsgewalten-und-gewaltentrennung>, [12.05.2020].

daraus für den Staat unmittelbar ein gewissermaassen höheres Recht gegen uns und das Unsrige, soweit er dessen zu jenem Zwecke bedarf. Der Staat kann deshalb dieses unbeschränkte Recht des Widerstandes um des Friedens und der öffentlichen Ordnung willen aufheben, und dass er dies gewollt hat, ist unzweifelhaft, da ohnedem er seinen Zweck nicht erreichen kann. Denn so lange jenes unbeschränkte Recht des Widerstandes besteht, ist noch kein Staat vorhanden, sondern eine Menge Einzelner, [...].“¹⁰⁷

Dadurch wird ein weiterer Effekt erzielt, dass nämlich für innere Ruhe und Ordnung gesorgt ist, da keiner in der Lage ist gewaltsam seine Rechte durchzusetzen. Er ist auf die staatlichen Institutionen angewiesen und dem bürgerlichen Recht unterworfen. Grotius führt dazu aus:

„Der Einzelne darf das nicht thun, was die Obrigkeit nach ihrem Amte vollziehen kann, weil dies sonst Anlass zu grossen Störungen giebt.“¹⁰⁸

und weiter:

„[...], denn wodurch unterschiede sich der Frieden von dem Kriege, wenn die Rechtsstreitigkeiten mit Gewalt erledigt werden könnten?“¹⁰⁹

Es besteht nicht nur die Gefahr, dass bei Auflösung des Gewaltmonopols innere Unruhe entsteht, es ist das Gemeinwesen, der Staat auch die einzige Einrichtung, welche mit diesem Monopol umzugehen weiß. Dazu bemerkt Eppler:

„Denn die einzige Institution, die verantwortungsvoll im Sinne des Gemeinwohls mit einem Gewaltmonopol umgehen kann, die dieses Monopol legitimiert und gleichzeitig begrenzt, ist der demokratische Rechtsstaat.“¹¹⁰

Diese Sicht verneint die Auslagerung von Aufgaben des Staates, das Gewaltmonopol betreffend. Eine Privatisierung von Aufgaben des Staates, vor allem das Gewaltmonopol betreffend, fördert nicht die Sicherheit, sondern hat vor allem finanzielle Aspekte, die dem Staat helfen seine Ausgaben auf Kosten der Sicherheit zu senken. Grotius beschäftigte sich auch damit, was denn eine Gewaltanwendung durch den einzelnen Bürger eines Gemeinwesens rechtfertigt und stellte als Bedingung das Fehlen der Gerichtsbarkeit fest. Dieses Fehlen konnte nun temporär oder dauerhaft sein.¹¹¹ Dies ist dann der Fall:

„Rechtlich, wenn sich Jemand an Orten aufhält, die zu keinem Staate gehören, wie auf dem Meere, in Einöden, auf wüsten Inseln; thatsächlich, wenn die Untergebenen dem Richter nicht gehorchen, oder wenn der Richter sein Amt verweigert.“¹¹²,

¹⁰⁷ Kirchmann, 1869, S. 185.

¹⁰⁸ Ebd., S. 133.

¹⁰⁹ Ebd., S. 133.

¹¹⁰ Eppler, Erhard: Auslaufmodell Staat?, 1. Aufl., Frankfurt am Main 2005, S. 124.

¹¹¹ Vgl. Kirchmann, 1869, S. 133.

¹¹² Ebd., S. 133.

also dort, wo einem die Gerichtsbarkeit nicht zur Hilfe kommen kann. Darauf basiert zum Beispiel auch die sehr weit gefasste Anwendung von Waffengewalt in den Vereinigten Staaten von Amerika. Hier war es auf Grund der räumlichen Weite und der Zersiedelung dem Staat nicht möglich, das Gewaltmonopol aufrechtzuerhalten und es wurde den Bürgern zugestanden ihren naturrechtlichen Verpflichtungen selbst nachzukommen. Der Staat hat notwendigerweise das Gewaltmonopol auszuüben, zur Abwehr der Gefahren von außen und zur Aufrechterhaltung der Sicherheit im Inneren. Diese Verpflichtung gegenüber seinen Bürgern hat aber auf dem Recht zu basieren um Willkür zu verhindern. Dieses,

„[...] das bürgerliche Recht [...] kann die natürliche Freiheit beschränken und das natürlich Erlaubte verbieten und selbst den natürlichen Erwerbsarten des Eigenthums durch seine Kraft entgentreten.“¹¹³,

ist somit Basis für das Gemeinwesen. Mit dem Gewaltmonopol und der Staatsgewalt, welche dieses ausübt, ist der Begriff der Souveränität eng verbunden.

Souveränität ist eine zentrale Eigenschaft von Staaten. Diese gründet sich auf der Macht unabhängig zu entscheiden und zu handeln. Dies bezieht auch die Fähigkeit mit ein, sich vor Unterdrückung und Beeinflussung durch andere zu schützen.¹¹⁴ Diese Souveränität ist daher nur im Gemeinwesen leistbar. Für Spinoza verfügt das Gemeinwesen über mehr Macht als der einzelne Mensch und steht daher unter eigenem Recht.

„Dieses Recht, das durch die Macht der Menge definiert wird, nennt man als Regierungsgewalt gewöhnlich die Souveränität des Staates.“¹¹⁵

Diese Souveränität erlaubt es als Gemeinwesen eine eigene Politik zu gestalten. Die Durchführung dieser basiert also auf der Souveränität des Gemeinwesens. Die Staatsgeschäfte, wie Spinoza die Politik bezeichnet, wirken nach innen und außen. Hier lässt sich bereits ein Territorialbezug ableiten.¹¹⁶ Es kann bereits eine Differenzierung in eine innere und äußere Souveränität erkannt werden. Spinoza sieht in diesem Zusammenhang auch die Verpflichtung des Staates die Souveränität aufrecht zu erhalten. Hinsichtlich der Souveränität im Inneren,

„[...] läßt sich in keiner Weise denken, daß das Prinzip des Gemeinwesens es einem jeden erlaubte, nach seiner eigenen Sinnesart zu leben; [...].“¹¹⁷

¹¹³ Ebd., S. 248f.

¹¹⁴ Vgl. Spinoza, Politischer Traktat, S. 17.

¹¹⁵ Ebd., S. 18.

¹¹⁶ Vgl. Benz, Arthur: Der moderne Staat. Grundlagen der politologischen Analyse, 2. Aufl., München 2008, S. 129.

¹¹⁷ Vgl. Spinoza, Politischer Traktat, S. 22.

Diese Forderung an den Staat zur Aufrechterhaltung der Souveränität im Inneren lässt sich auch auf die äußere Souveränität übertragen. Zur äußeren Souveränität führt Spinoza aus:

„Ein Gemeinwesen steht also so weit unter eigenem Recht, wie es für sich selbst sorgen und sich vor Unterdrückung durch ein anderes Gemeinwesen schützen kann; es ist so weit fremdem Recht unterworfen, wie es die Macht eines anderen Gemeinwesens fürchtet oder wie es von ihm an der Ausführung der eigenen Absichten gehindert wird oder schließlich wie es für die eigene Erhaltung oder auch das eigene Wachstum auf dessen Hilfe angewiesen ist.“¹¹⁸

Für die Souveränität nach innen sieht Spinoza die Möglichkeit, Gesetze zu erlassen als wesentlich und nach außen das Recht, Krieg zu erklären und Frieden anzubieten.¹¹⁹ Die Aufgabe der höchsten Staatsgewalt, des Souveräns, ist es, „[...] alles für Krieg und Frieden Erforderliche aufzubringen und einzusetzen [...]“¹²⁰, also die Mittel für die Aufrechterhaltung der Souveränität bereitzustellen. Die Instrumente dafür liegen in den Trägern der Staatsgewalt. Das Militär ist somit ein Instrument zu Erhaltung der Souveränität.

Die Souveränität, als Ausdruck der Staatsmacht, ist nicht absolut, sie unterliegt, sowohl nach innen wie nach außen, unterschiedlichen Wechselwirkungen. Grotius formuliert diese Wechselwirkung in Bezug auf die innere Souveränität wie folgt:

„In Wahrheit ist der Staat eine Verbindung zweier souveräner Autoritäten oder Mächte, des souveränen Königs und des souveränen Volkes; beide beschränken durch diese Verbindung einander; [...]“¹²¹

Diese Wechselwirkung ist in allen Staatsformen gegeben und daher auch dieser gegenseitigen Kontrolle und Beschränkung unterworfen.

„[...]“, dass es nie einen Staat gegeben hat, wo nicht die Macht des Herrschers durch die Macht des Volkes oder umgekehrt beschränkt gewesen ist. Dies folgt aus dem Begriff des Staats, welcher eben eine Verbindung dieser zwei souveränen Autoritäten oder Mächte darstellt. In allen Staatsformen ist deshalb die Staatsgewalt beschränkt, [...]“¹²²

Die oberste Staatsgewalt verkörpert so zwar die Souveränität, ist aber letztlich im Inneren durch die Legitimation des Volkes beschränkt. Nach außen gestaltet sich diese Wechselwirkung in den Beziehungen der Staaten zueinander. Diese beschränken sich gegenseitig in ihrer äußeren Souveränität. Zwar wird deren Souveränität als

¹¹⁸ Spinoza, Politischer Traktat, S. 27f.

¹¹⁹ Vgl. ebd., S. 30f.

¹²⁰ Ebd., S. 31.

¹²¹ Kirchmann, 1869, S. 159.

¹²² Ebd., S. 174.

„[...] die tatsächliche Macht der Autoritäten bezeichnet [...], welche wohl für die Untergebenen die Quelle des Rechts ist, aber selbst nicht von dem Rechte erfasst werden kann.“¹²³,

doch äußert sich die Begrenztheit der Souveränität nach außen durch die gegenseitige Abhängigkeit der Staaten in einer zunehmend globalisierten Welt.¹²⁴ Staaten unterliegen im Verhältnis zueinander der Gerechtigkeit. Es herrscht zwischen Staaten kein Verhältnis des Rechts, sondern Macht, diese ist der begrenzende Faktor.¹²⁵ Es gibt demzufolge auch kein übergeordnetes Recht und keine Rechtsprechung. Die Souveränität enthält somit zwei Momente, die sich in einer eigenen Rechtsordnung und in der selbstständigen Gestaltung und Ausübung der Staatsfunktionen widerspiegelt.¹²⁶ Es gibt also eine nach innen und eine nach außen gerichtete Souveränität.

Souveränität bedeutet in der Folge Selbstbestimmung in der konkreten Situation.¹²⁷ Die Souveränität nach außen ist geprägt von der gegenseitigen Anerkennung der Staaten. Nur unter dieser Voraussetzung ist es dem Gemeinwesen möglich, seine Souveränität, seine Selbstbestimmung, zu erhalten. Souveränität wird in der vorliegenden Abhandlung, als

„[...] Autonomie und höchste Befehlsgewalt im Inneren und nach außen als Unabhängigkeit und Gleichheit der Staaten untereinander [...]“¹²⁸,

gefasst. Carl Schmitt fasst die Souveränität als das Entscheidungsrecht über den Ausnahmezustand, es ist seiner Auffassung nach jene Kompetenz die grundsätzlich nicht normierbar ist.¹²⁹ In Zusammenschau mit vorher Gesagtem ist die Souveränität somit von staatlicher Dimension, unterliegen Staaten ja keinem gemeinsamen Recht. Für Schmitt ist eine der zentralen Fragen in Bezug auf die Souveränität deren Anwendung,

„[...] wer im Konfliktfall entscheidet, worin das öffentliche oder staatliche Interesse, die öffentliche Sicherheit und Ordnung, [...]“¹³⁰

besteht. Das bedeutet, dass es für einen Ausnahmezustand keine Aufzählung von Tatbeständen gibt und der Situation entsprechend von Fall zu Fall neu zu entscheiden ist.

¹²³ Ebd., S. 146.

¹²⁴ Vgl. Neuhold, Hanspeter u.a.: Österreichisches Handbuch des Völkerrechts, 2. Aufl., Wien 1991, S. 139.

¹²⁵ Vgl. Pesendorfer, Wolfgang: Staat und äussere Sicherheit. In: Neisser, Heinrich; Windhager, Fritz (Hrsg.), Wie sicher ist Österreich? Beiträge zu einer konzeptiven Sicherheitspolitik, Wien 1982, S. 97.

¹²⁶ Vgl. Neuhold/Hummer/Schreuer, 1991, S. 8.

¹²⁷ Vgl. Pesendorfer, 1982, S. 97. (in: Neisser, 1982)

¹²⁸ Neuhold/Hummer/Schreuer, 1991, S. 7.

¹²⁹ Vgl. Schmitt, Carl: Politische Theologie, Duncker u. Humblot, Berlin 1985, S. 11.

¹³⁰ Ebd., S. 12.

„Es kann weder mit subsumierbarer Klarheit angegeben werden, wann ein Notfall vorliegt, noch kann inhaltlich aufgezählt werden, was in einem solchen Fall geschehen darf, wenn es sich wirklich um den extremen Notfall und um seine Beseitigung handelt.“¹³¹

Da dieser Ausnahmezustand nicht einer Norm unterliegt, kann nach Schmitt nur in der Verfassung eines Gemeinwesens festgehalten werden, wer in einem solchen extremen Ausnahmefall handeln darf. Entscheidend ist in diesem Zusammenhang, dass Souveränität sich nach innen wie nach außen durch die Entscheidung über einen extremen Notfall zeigt. Sie kommt zum Tragen, wenn die staatliche Ordnung erhalten werden muss oder wiederhergestellt werden soll. „Es gibt keine Norm, die auf Chaos anwendbar wäre.“¹³² Wird nun die Souveränität eines Gemeinwesens angegriffen oder verletzt, so wird die selbstständige Entscheidungsfähigkeit des Souveräns zum Ziel. Es wird ihm quasi die Entscheidung aufgezwungen. Diese Verletzung der Souveränität ist somit eine Einschränkung der Entscheidungsfreiheit über einen extremen Notfall, welcher die staatliche Ordnung angreift oder auflöst. Vor allem völkerrechtlich bleibt zu überdenken, ob nicht auch nichtstaatliche Akteure in der Lage sind, gerade im neuen Handlungsraum, dem Cyberspace, souveränitätsgefährdende Handlungen setzen zu können.¹³³

Die staatliche Ordnung ist somit Voraussetzung und Zweck der Souveränität. Die Souveränität ist demnach also als Entscheidungs- und nicht als Herrschaftsgewalt zu fassen. Nach Schmitt ist die staatliche Souveränität nicht als „[...] Zwangs- oder Herrschaftsmonopol, sondern als Entscheidungsmonopol juristisch zu definieren [...]“¹³⁴. Souveränitätsrelevant sind somit all jene Handlungen im Inneren und von außen, die genau diese Entscheidungsfreiheit, dieses Entscheidungsmonopol angreifen. Diese Handlungen können unmittelbar oder mittelbar einen Einfluss auf die Souveränität eines Gemeinwesens haben.

Dieser Begriff der Souveränität hat in der vorliegenden Abhandlung im Falle eines Angriffes, vor allem im und aus dem Cyberspace, auch einen wesentlichen Einfluss auf die Kompetenzzuordnung an die Träger der Staatsgewalt. Diese Definition der wesentlichen Basisbegriffe beschließt die Einleitung und führt in den Argumentationsteil der Arbeit.

¹³¹ Ebd., S. 12.

¹³² Ebd., S. 20.

¹³³ Vgl. <https://www.faz.net/aktuell/politik/politische-buecher/terrorismus-und-souveraenitaet-auch-auf-fremdem-territorium-14117751.html> [12.05.2020]

¹³⁴ Schmitt, Politische Theologie, S. 20.

5 Vom Begriff des Krieges

„Krieg ist nach wie vor allgegenwärtig,
er ist ungebrochen der steinerne
Gast der internationalen Politik.“
Stadler¹³⁵

Für die Beantwortung der Forschungsfrage ist der Kriegsbegriff wesentlich. Es ist notwendig herauszuarbeiten, was der Krieg in der Gesamtheit ist, um den Cyberwar in diesen Kriegsbegriff einordnen zu können. Krieg als Kerntätigkeit von Streitkräften ist vorab zu definieren und darzustellen, um die Kompetenzgrenze zwischen Polizei und Militär herauszuarbeiten und in weiterer Folge auf den Cyberwar übertragen zu können. Krieg hat schon immer das menschliche Dasein auf Erden mitbestimmt. Die Ausprägungen des Krieges unterliegen einer Vielzahl an Einflussfaktoren, welche eine Typologisierung desselben erschweren. Im Zuge der Auseinandersetzung mit dem Kriegsbegriff, wird im Folgenden vor allem auf die Darstellung durch Carl von Clausewitz zurückgegriffen.

Verdichtet werden die Darstellungen des preußischen Militärtheoretikers und -praktikers durch die Perspektive anderer Philosophen und Denker auf den Krieg. Dabei wird in historisch chronologischer Folge von der Antike (Platon) über die Renaissance (Machiavelli), die frühe Neuzeit (Spinoza und Grotius) bis in die Neuzeit (Clausewitz) die Entwicklung des Kriegsbegriffes nachgezeichnet. Bevor der Krieg als Konfliktform näher bestimmt wird, soll eine generelle Einordnung und Abgrenzung, einerseits zu den anderen Konfliktformen und andererseits zum Verbrechen, erfolgen. Da in der Arbeit die Frage nach der Kompetenzzuordnung im Cyberspace gegenüber den Kräften zur Aufrechterhaltung der Inneren Sicherheit zur Beantwortung steht, ist eine Abgrenzung des Krieges zum Verbrechen, der Kriminalität notwendig.



Abbildung 1: Kategorisierung des Krieges¹³⁶

¹³⁵ Stadler, 2009, S. 7.

¹³⁶ Abbildung durch den Verfasser erstellt.

Danach folgt die Untersuchung des Kriegsbegriffes anhand einer Kategorisierung, welche es ermöglicht einen gewissen Abstraktionsgrad zu erhalten, um die Gültigkeit eines solchen Kriegsbegriffes auch im Informationszeitalter noch aufrechtzuerhalten.

5.1 Zum Wesen des Krieges

Die Typologie des Krieges lässt sich an vielen Faktoren oder Kategorien festmachen. Zuerst ist das Wesen des Krieges, was Krieg eigentlich ist, darzustellen. Um den Krieg weiter typologisieren zu können, ist eine Auseinandersetzung mit dieser Frage geboten. Da Menschen stets bemüht sind, sich in den Mittelpunkt zu stellen¹³⁷ und dabei ihren Willen durchzusetzen, kommt es zwangsläufig zum Konflikt.

Nicht jeder Konflikt ist dabei einem Krieg gleichzusetzen, obwohl jeder Krieg ein Konflikt ist. Daraus lässt sich ableiten, dass der Krieg Moment des Konfliktes sein muss. Die genauere Differenzierung der einzelnen Momente muss dann durch eine weitere Untersuchung erfolgen. Zunächst geht es im Folgenden um die Einordnung des Krieges als Moment des Konfliktes.

5.1.1 Die Einordnung des Krieges als Moment des Konfliktes

Der Krieg ist ein Moment des Konfliktes. Konflikt ist eine Auseinandersetzung oder anders formuliert ein Zwiespalt. Es treffen zwei Standpunkte, unterschiedliche Interessen oder Willen aufeinander. Es handelt sich um einen dialektischen Vorgang, der die Lösung eines Widerspruchs hervorbringt.

Ein Konflikt beruht auf entgegengesetzten Positionen und wird je nach Ausprägung in unterschiedlichen Momenten geführt. Es lassen sich hier verschiedene Ordnungsansätze formulieren, jedoch erscheint die Untergliederung und Kategorisierung nach der Ausdehnung des Konfliktes für diese Abhandlung als passend. Bei Platon finden wir in der Politeia die Unterscheidung in zwei Momente des Konfliktes.

„Mir scheinen nämlich, wie sie ja auch als zwei Wörter gesprochen werden, Krieg und Zwist, so auch zweierlei zu sein und sich auf zwei verschiedene Dinge zu beziehen; nämlich von diesen Zweien ist das eine Befreundetes und Verwandtes, das andere Fremdes und Ausländisches. Für Feindschaft nun mit dem Befreundeten brauchen wir das Wort Zwist, mit dem Fremden aber Krieg.“¹³⁸

Dabei ist beim Krieg vom interstaatlichen Konflikt auszugehen und beim Zwist vom interpersonellen Konflikt. Erst in der Nomoi spricht Platon

¹³⁷ Vgl. Spinoza, Politischer Traktat, S. 9.

¹³⁸ Platon, Politeia, S. 373f.

auch vom intrastaatlichen Krieg, dem Aufruhr, den er als Entzweiung bezeichnet.¹³⁹

„Wie aber der Ordner des Staates? Würde dieser der Bürger Lebensweise mehr mit Rücksicht auf den Krieg von außen regeln oder mit Rücksicht auf den in ihm selbst etwa sich erhebenden, den man Entzweiung nennt? Von welchem wohl jeder am meisten wünschen möchte, daß er in seinem Staate gar nicht sich erhebe, erhob er sich aber, auf das schleunigste beseitigt werde.“¹⁴⁰

Dies sind die drei Momente des Konfliktes, die sich aus dieser Einteilung ableiten lassen. Platon fasst somit schon in der Antike jene Typen von Konflikten zusammen, die sich in der weiteren Geschichte genauer ausdifferenzieren.

Machiavelli spricht neben dem Krieg, als Konflikt zwischen den Gemeinwesen, vom Aufstand und den allgemeinen Zwistigkeiten. Er sieht vor allem im politischen Konflikt niedriger Intensität, ohne physische Gewalt, innerhalb des Staates ein Entwicklungspotential für das Gemeinwesen. Er nennt diese Auseinandersetzungen zum Zweck der Weiterentwicklung des Staates Parteikämpfe.¹⁴¹ Man kann hier eine weitere Differenzierung des Konfliktes seiner Intensität nach erkennen.

Wie Machiavelli sieht auch Platon in der konfliktischen Auseinandersetzung, im Krieg und Aufruhr, ein gestaltendes Element. Obwohl bei Platon der Krieg vor allem der Existenzsicherung¹⁴² dient, steht er ihm und den innerhalb der Gemeinwesen liegenden Auseinandersetzungen ablehnend gegenüber¹⁴³. Dazu führt er in der Nomoi aus:

„Das Beste ist aber nicht Krieg und Entzweiung – es ist traurig, wenn es dieser bedarf -, sondern wechselseitiger Frieden und Wohlwollen; ja sogar, daß ein Staat über sich selbst den Sieg davontreibe, gehört nicht zu dem Besten, sondern zu dem Notgedrungenen.“¹⁴⁴

Die drei Momente des Konfliktes finden sich auch bei Grotius wieder. Er spricht von dreierlei Arten von Krieg.

„Die erste und wichtigste Eintheilung der Kriege ist die öffentliche, private und gemischte.“¹⁴⁵

¹³⁹ Anm. d. Verf.: Hinzu tritt noch der intrapersonelle Konflikt, welcher aber für die weitere Betrachtung keine Relevanz hat, da er im Clausewitzschen Sinn nicht als Konflikt mit politischem Zweck verstanden werden kann.

¹⁴⁰ Platon: Sämtliche Werke. Timaios, Kritias, Minos, Nomoi, 23. Aufl., Reinbek bei Hamburg 2009, S. 160.

¹⁴¹ Machiavelli, Niccolò: Discorsi. Gedanken über Politik und Staatsführung, 2. Aufl., Stuttgart 1977, S. 19.

¹⁴² Vgl. Platon, Politeia, S. 265.

¹⁴³ Vgl. ebd., S. 241.

¹⁴⁴ Platon, Nomoi, S. 160.

¹⁴⁵ Kirchmann, 1869, S. 138.

Wobei hier der Kriegsbegriff sehr weit gefasst wird. Er geht hier noch einen Schritt weiter als Platon, der davon spricht, dass es

„Allerdings zwei; die eine, die wir alle Entzweiung nennen, welche, wie wir eben behaupteten, der ärgste aller Kriege ist; als die zweite Gattung des Krieges aber werden wir alle denjenigen annehmen, den wir, als einen weit minder anstößigen, gegen Auswärtige und fremdem Stamm Entsprössene führen, mit denen wir in Streit gerieten.“¹⁴⁶

sind.

Erfolgt bei Machiavelli die Differenzierung zwischen Krieg, als Konfliktform zwischen den Gemeinwesen, und den internen Konflikten, welche nicht als Krieg bezeichnet werden, so fällt bei Grotius diese Unterscheidung. Er definiert die drei Momente dann näher und es lässt sich ableiten, dass der öffentliche Krieg mit dem Krieg im platonischen bzw. machiavellistischen Sinne gemeint ist.

Grotius widerspricht sich in Bezug auf seine einleitende Kriegsdefinition, die den Krieg als,

„Die Streitigkeiten zwischen Personen, welche durch kein gemeinsames bürgerliches Recht verbunden sind, beziehen sich entweder auf die Zeiten des Krieges oder des Friedens.“¹⁴⁷,

fasst. Er spricht hier den zwischenstaatlichen Konflikt, den zwischen unterschiedlichen Gemeinwesen, an. Diese haben jedes für sich eine eigene Rechtsordnung und unterliegen nicht einem gemeinsamen Recht. Für den innergemeinschaftlichen Konflikt trifft dies nicht zu. Er führt später zum Privatkrieg aus, dass es sich um

„[...] die Vertheidigung, welche der Einzelne zum Schutze seines Rechts gegen einen Angreifer unternimmt, oder die sogenannte Selbsthülfe im Privatleben, [...]“¹⁴⁸

handelt, was darauf schließen lässt, dass die Streitparteien sehr wohl unter einem gemeinsamen bürgerlichen Recht stehen können. Obwohl naturrechtlich erlaubt, ist der Privatkrieg Angelegenheit der Gerichte und damit eigentlich kein Krieg, sondern eine Konfliktform niedriger Intensität. Der gemischte Krieg ist jener, welchen die Untertanen gegen ihre Obrigkeit führt, der Bürgerkrieg. Den öffentlichen Krieg, der bestimmten Regeln unterliegt, welchen Grotius den feierlichen Krieg bezeichnet, sieht er als Rechtsetzungsmittel zwischen Gemeinwesen an.¹⁴⁹ Diese positive Haltung gegenüber dem Konflikt verliert er bei Betrachtung des Bürgerkrieges, in dem er Cicero zitiert.

¹⁴⁶ Platon, Nomoi, S. 161f.

¹⁴⁷ Kirchmann, 1869, S. 67.

¹⁴⁸ Ebd., S. 138.

¹⁴⁹ Vgl. ebd., S. 139.

„Mir scheint jeder Frieden unter den Bürgern nützlicher als der Bürgerkrieg.“¹⁵⁰

Damit sieht er den Erhalt der staatlichen Ordnung über das Wohl der Bevölkerung gestellt. Ähnlich sieht er den Verzicht auf das Naturrecht zur Selbstverteidigung zu Gunsten der Ruhe und Ordnung im Staat.¹⁵¹ Hierin begründet sich auch die Notwendigkeit, dass der Staat das Gewaltmonopol einrichtet. Solange jeder sein Recht auf Selbstverteidigung ausübt, kann er nicht dem Gemeinwohl dienen und es herrscht Willkür statt einer rechtlichen Ordnung. Dies führt zu Krieg jeder gegen jeden und letztlich zur Auflösung des Gemeinwesens. Auch bei Platon findet sich das Gewaltmonopol in dem er auf die Gerechtigkeit verweist und den drei Ständen ihre Aufgabe zuweist.¹⁵² Das Gewaltmonopol wird durch die Wächter wahrgenommen.

Spinoza fasst den Konflikt ebenfalls in drei Momente, es lässt sich bei ihm der Hinweis auf eine ähnliche Einteilung wie bei Grotius finden. Spinoza spricht bei der Auseinandersetzung zwischen einzelnen Menschen von den Feindseligkeiten.¹⁵³ Das Moment des innergemeinschaftlichen Konfliktes wird als Aufruhr¹⁵⁴ bezeichnet, während die zwischenstaatliche Auseinandersetzung der Krieg ist. Dazu unterteilt er im politischen Traktat,

„[...] Aufruhr, Kriege und Mißachtung oder Verletzungen von Gesetzen [...]“¹⁵⁵

Es kann hier festgehalten werden, dass es grundsätzlich vier Momente des Konfliktes gibt.¹⁵⁶ Es handelt sich dabei – gemessen an seiner Ausdehnung – um den intrapersonellen, den interpersonellen, den intragemeinschaftlichen und den intergemeinschaftlichen Konflikt. Um den Konflikt näher bestimmen zu können, ist es nicht ausreichend diesen in der bisher dargestellten Form zu bestimmen. Es muss vielmehr auch die Art und Weise wie der Konflikt geführt wird, seine Form, mit einbezogen werden. Bisher lässt sich nicht ergründen in welcher Form der Konflikt zu fassen ist, zu dem der Krieg als ultimatives Moment gehört.

Den Schlüssel zur Auflösung dieser Unschärfe liefert die Anwendung von Gewalt in seiner physischen Form. Unter physischer Gewalt ist nach Kleemeier zu verstehen,

„[...] daß [sic] einem Menschen von einem anderen mittels physischer Kraft ein fremder Wille aufgezwungen wird, der sich darüber hinaus auf Ziele richtet, die für jenen Menschen existenziell schädigend sind.“¹⁵⁷

¹⁵⁰ Ebd., S. 207.

¹⁵¹ Vgl. ebd., S. 185.

¹⁵² Vgl. Platon, Politeia, S. 333.

¹⁵³ Vgl. Spinoza, Politischer Traktat, S. 17.

¹⁵⁴ Vgl. ebd., S. 35.

¹⁵⁵ Ebd., S. 35.

¹⁵⁶ Vgl. Bonacker, Thorsten; Imbusch, Peter: Zentrale Begriffe der Friedens- und Konfliktforschung. In: Imbusch, Peter; Zoll, Ralf (Hrsg.): Friedens- und Konfliktforschung. Eine Einführung, Wiesbaden 2010, S. 69.

¹⁵⁷ Kleemeier, 2002, S. 18f.

Konflikte können ohne oder unter Anwendung von physischer Gewalt¹⁵⁸ geführt werden. Sie können als gewaltlose oder gewalttätige Auseinandersetzungen auftreten. Der Krieg ist der Form des gewalttätigen Konfliktes zuzurechnen.¹⁵⁹ Wird im politischen Konflikt niederer Intensität eher die psychische Gewalt¹⁶⁰ angewandt, so steht bei Krieg und Aufruhr die Anwendung von physischer Gewalt im Mittelpunkt des Aufeinandertreffens von zwei Willen.¹⁶¹ Hier setzt die Sichtweise von Clausewitz an. Er sieht den Krieg als Zweikampf, als

„[...] Akt der Gewalt, um den Gegner zur Erfüllung unseres Willens zu zwingen.“¹⁶²

Er bezieht dies allerdings nur auf den Krieg und den Aufruhr, der zunächst von ihm als Volkskrieg¹⁶³ bezeichnet wird. Dieser richtet sich gegen einen Besatzer und nicht gegen die eigene Staatsführung, ist also eine eingegrenzte Form des Aufruhrs. Gekennzeichnet wird dies auch dadurch, dass er den Einsatz des Volkskrieges als am effizientesten in Verbindung mit den regulären Streitkräften ansieht.¹⁶⁴ Diese beiden Formen des Krieges werden im späteren Verlauf als Großer und Kleiner Krieg bezeichnet und in weiterer Folge noch näher beleuchtet.

Physische Gewalt wird im einfachsten Sinn mit dem den Menschen angeborenen „Mitteln“ (Hervorhebung durch den Verfasser.) ausgeübt, in der Vergangenheit ist dies aber die Ausnahme. In der Regel bedient der Mensch sich eines Hilfsmittels zur Vergrößerung seiner Wirkung auf den Gegner, der Waffe.¹⁶⁵ Da Konflikte nun mit oder ohne Gewalt ausgetragen werden können, gibt es also eine Unterscheidung von bewaffneten und nicht-bewaffneten Konflikten.

Bei Clausewitz ist unter Gewalt physische Gewalt zu verstehen, sie stellt das Mittel zur Erreichung des Zweckes dar. Er definiert den Zweikampf nicht als ein Ringen um den Sieg, welches auch nur mit Worten ausfechtbar ist, sondern er fasst den Kampf enger, als Anwendung physischer Gewalt.¹⁶⁶ Der Kampf ist ein Aufeinanderwirken von zwei Kräften, der Kraft und der Gegenkraft.¹⁶⁷ Es braucht also im Kampf nach Clausewitz immer einen Angreifer und einen Verteidiger. Ohne Gegenpart gibt es keinen Kampf, dies ist für das Wesen des Kampfes die grundlegende Bedingung. Der Krieg bedient sich für Clausewitz aber nicht ausschließlich der physischen Komponente der Gewalt. Es geht für ihn auch um den Kampf zweier Willen,

¹⁵⁸ Anm. d. Verf.: Die physische Gewalt ist eine Form der Gewalt. Hierbei handelt es sich um Verletzungen und Beeinträchtigungen, die durch äußere Einwirkungen hervorgerufen werden.

¹⁵⁹ Vgl. Kleemeier, 2002, S. 17.

¹⁶⁰ Anm. d. Verf.: Psychische Gewalt als weitere Gewaltform erreicht verletzende und beeinträchtigende Wirkung nicht durch Anwendung physischer Mittel, sondern durch Maßnahmen auf vor allem emotionaler Ebene.

¹⁶¹ Vgl. Stupka, 2011, S. 123ff.

¹⁶² Clausewitz, Vom Kriege, S. 13.

¹⁶³ Vgl. ebd., S. 173.

¹⁶⁴ Vgl. ebd., S. 173f.

¹⁶⁵ Vgl. Stupka, 2011, S. 127.

¹⁶⁶ Vgl. ebd., S. 123.

¹⁶⁷ Vgl. ebd., S. 114ff.

hier tritt die psychische Komponente hervor. Die physische Gewalt zielt auf die Psyche des Gegners.

„Moralische Stärke und Willenskraft seien entscheidend für den Sieg.“¹⁶⁸

Dieser Zweikampf, den Clausewitz als Krieg fasst, ist einer, der von Gemeinwesen geführt wird. Dies geht auch aus der Einteilung der Momente des Konfliktes hervor. Der Krieg wird hier immer als ultimatives Moment gefasst, welches zwischen Gemeinwesen oder zwischen Gruppierungen innerhalb eines Gemeinwesens stattfindet. Hier lässt sich schon eine politische Dimension des Krieges erahnen. Ein bewaffneter Konflikt kann in allen vier Momenten des Konfliktes aufscheinen, wobei nur Krieg und Aufruhr als politische Ausprägungen zu fassen sind und daher als Krieg an und für sich gesehen werden können.

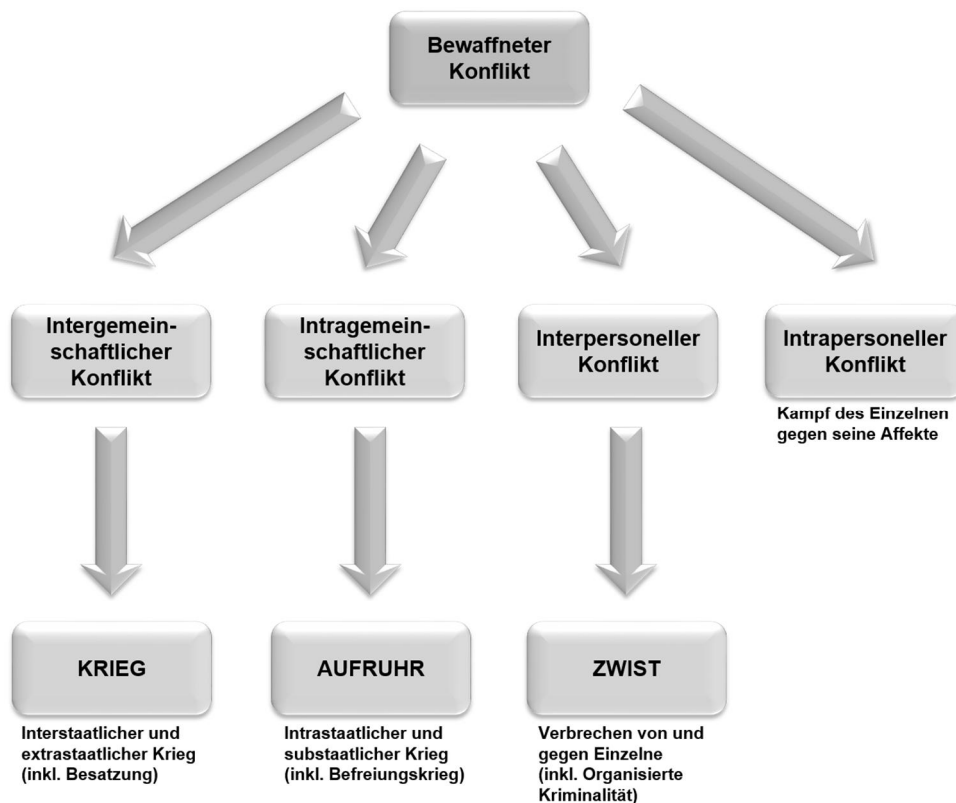


Abbildung 2: Momente des bewaffneten Konfliktes¹⁶⁹

Treten nun einzelne Personen in einem interpersonellen Konflikt einander mit physischer Gewalt gegenüber, so steht der politische Zweck vermutlich zu Gunsten des persönlichen Vorteils im Hintergrund, außer sie handeln im Namen ihrer Gemeinwesen und somit politisch.¹⁷⁰ Politisch kann der Einzelne nur in der Gemeinschaft handeln, weil nur da für ein

¹⁶⁸ Strachan, Hew: Hew Strachan über Carl von Clausewitz, Vom Kriege, Dt. Erstausg. Aufl., München 2008, S. 17.

¹⁶⁹ Abbildung durch den Verfasser erstellt.

¹⁷⁰ Vgl. Kleemeier, 2002, S. 44.

Gemeinwohl agiert werden kann. Einem Einzelnen alleine kann dies nur zu seinem eigenen Wohle gelingen.

Diese persönliche Bereicherung ist es, die diese Art des Konfliktes als Verbrechen definiert. Natürlich handeln Einzelpersonen gegeneinander durchaus auch politisch, aber nur in der Gemeinschaft¹⁷¹ und in der Regel in einer physisch gewaltlosen Form. Hier tritt nun der Zweck zu Ausdehnung und Form der Konfliktaustragung hinzu. Bei Konflikten mit physischer Gewalt lässt sich nun zum einen der politische Zweck dem der persönlichen Bereicherung gegenüberstellen. Es treten Krieg und Verbrechen einander gegenüber.

5.1.2 Die Abgrenzung zwischen Krieg und Verbrechen

Nach der Erfassung der ersten zwei Charakteristika des Krieges, der Ausdehnung in Bezug darauf, welche Teile eines Gemeinwesens in diesem Konflikt involviert sind und der Form des bewaffneten Konfliktes, als Anwendung physischer Gewalt, wird nun die Abgrenzung zum Verbrechen über die Intention, den Zweck des bewaffneten Konfliktes, hergestellt. Der bewaffnete Konflikt kann sowohl politischer Natur, als auch verbrecherischer Natur sein.¹⁷² Dabei ist zu beobachten, dass die Häufigkeit der beiden Phänomene indirekt proportional zu ihrer Ausdehnung ist. Gemeint ist hier, dass kriminelle Einzeltaten häufiger vorkommen, als etwa kriminelle Auseinandersetzungen zwischen Gemeinwesen und umgekehrt politische Konflikte nur zwischen und in Gemeinwesen (zwischen verschiedenen Gruppierungen) zum Tragen kommen. Clausewitz definiert den Krieg folgendermaßen:

„Der Krieg einer Gemeinheit – ganzer Völker – und namentlich gebildeter Völker, geht immer von einem politischen Zustande aus und wird nur durch ein politisches Motiv hervorgerufen. Er ist also ein politischer Akt [...].“¹⁷³

Da diese Anwendung der Gewalt durch ein Gemeinwesen oder durch Mitglieder des Gemeinwesens in dessen Namen erfolgt, kann hier von einem politischen Instrument gesprochen werden. Genau das meint Clausewitz, wenn er schreibt, dass

„[...] der Krieg nicht bloß ein politischer Akt, sondern ein wahres politisches Instrument ist, [...]“¹⁷⁴.

Der Zweck des politischen Zweikampfes ist es, dem Gegner den eigenen Willen mittels physischer Gewalt aufzuzwingen. Das Ziel des Krieges

¹⁷¹ Anm. d. Verf.: Zum Wohle des Gemeinwesens, also politisch, kann nur in der Gemeinschaft gehandelt werden. Der Einzelne handelt also nicht für sich, sondern das Gemeinwesen. Für den Einzelnen alleine, aber auch in der Gemeinschaft, ist Bereicherung möglich, jedoch benötigt der Verbrecher die Gemeinschaft, um sich einerseits gegenüber jemanden zu bereichern und andererseits um seinen Vorteil auskosten zu können.

¹⁷² Vgl. Kleemeier, 2002, S. 45.

¹⁷³ Clausewitz, Vom Kriege, S. 21.

¹⁷⁴ Ebd., S. 22.

liegt darin, den Gegner wehrlos zu machen. Der Wille äußert sich in den Handlungen des Staates, dieses Handeln ist die Tätigkeit der Politik, welche neben Zielen auch die Mittel bereitstellt. Der Wille hat eine somit politische Dimension, damit hat der Krieg einen politischen Zweck.¹⁷⁵

„So wird also der politische Zweck als das ursprüngliche Motiv des Krieges das Maß sein, sowohl für das Ziel, welches durch den kriegesischen Akt erreicht werden muß, als für die Anstrengungen, die erforderlich sind.“¹⁷⁶

Der Krieg ist also nicht nur Moment des Konfliktes, sondern er ist in der Art und Weise wie er hervortritt, ein mit Anwendung von Gewalt in physischer Ausprägung, geführter Konflikt. Da er durch Gemeinwesen zum Wohle derselben geführt wird, verfolgt er einen politischen Zweck und wird dadurch selbst zu einem politischen Instrument.

Der Ausgangspunkt liegt hier im politischen Feld. Krieg ist Mittel der Politik und nicht Mittel zur Bereicherung. Der politische Zweck definiert sich über den Erhalt des Gemeinwesens. Dieses ist gekennzeichnet durch eine bestimmte Ordnung, welche den Rahmen für das Gemeinwesen darstellt.¹⁷⁷ In diesem Rahmen vollzieht sich das Leben des Gemeinwesens. Um im Sinne von Clausewitz nun einem Gegner unseren Willen aufzuzwingen und ihn damit zu vernichten, ist es notwendig diesen Rahmen zu zerstören. Dann ist es dem Sieger möglich dem Gegner seine Ordnung aufzuerlegen.¹⁷⁸

Es geht darum, nicht den Gegner dem Erdboden gleich zu machen, ihn körperlich auszulöschen, sondern ihm die eigene Ordnung aufzuzwingen oder seine im eigenen Interesse soweit zu ändern, dass sie dieser entspricht. Das Wesen des Krieges – vom Zweck her betrachtet – ist am Obsiegen der eigenen Ordnung gegenüber der gegnerischen Ordnung festzumachen. Krieg als politischer, bewaffneter Konflikt zielt einerseits darauf ab eine gegnerische Ordnung zu beseitigen oder andererseits die eigene Ordnung vor der Beseitigung zu bewahren. Hier kann ein stark räumlich orientierter Zusammenhang ausgemacht werden, so ist immer die Ordnung am stärksten betroffen, in deren Territorium der Krieg stattfindet.

Krieg zerstört und schafft Ordnungen von Gemeinwesen. Diese Zerstörung ist umso umfassender, je existenzieller der Konflikt ist. Das Verbrechen ist um den Erhalt einer Ordnung bemüht, um seine Geschäfte unter dessen Schutzmantel auszuführen. Der Verbrecher verstößt gegen das Recht als zentrales Ordnungselement, aber er beseitigt es nicht, denn es ermöglicht ihm seine Gewinne auch auszukosten. Es „schützt“ (Hervorhebung durch den Verfasser.) die Ordnung den Verbrecher gleichermaßen wie sein Opfer. Dies gilt für Gemeinwesen in denen eine gewisse Ordnung existent ist.

¹⁷⁵ Vgl. ebd., S. 13ff.

¹⁷⁶ Ebd., S. 17.

¹⁷⁷ Vgl. Kleemeier, 2002, S. 17.

¹⁷⁸ Vgl. Stupka, 2011, S. 124f.

Es gibt aber auch Gemeinwesen, die über keine ausreichende staatliche Ordnung verfügen, hier hat derjenige, welcher

„[...] aus der Gewalt ein Geschäft macht, wer sich seinen Lebensunterhalt – und manches darüber hinaus – mit Gewalt verschafft, [...] kein Interesse am Frieden.“¹⁷⁹

Ist nur eine Kriegoordnung vorhanden und stellt diese die Basis für eine Kriegoökonomie dar, ist sie somit die Grundlage für die Bereicherung, so besteht kein Interesse seitens der Akteure diese Ordnung gegen eine umfassendere Rechtsordnung einzutauschen. Das Gewaltmonopol ist außer Kraft gesetzt und das Recht des Stärkeren gibt dem Kriegoökonom oder Warlord die Möglichkeit seinen erworbenen Gewinn auskosten zu können, solange er der Stärkere ist.

Verbrechen bleibt aber in diesem Fall noch immer kriminell, denn

„Es schweigen unter den Waffen die Gesetze; aber nur die des Verkehrs, der Gerichte und des Friedens, aber nicht jene ewigen und für alle Zeiten geltenden Gesetze.“¹⁸⁰

Wenn man Grotius weiter folgt, so ergibt sich, dass nur das jeweilige bürgerliche Recht, das Recht des Gemeinwesens, des Staates, nicht mehr zum Tragen kommt. Denn in einem fortwährenden Zustand des Krieges gibt es nach wie vor die anderen Elemente des Rechts, welches er in drei Elemente einteilt:

„1) Naturrecht, was sich aus der Natur der Sache ergibt; 2) Völkerrecht, was bei allen Völkern gilt, aber doch nicht aus der Natur der Sache sich ergibt, sondern nur auf dem freien Willen der Völker beruht; und 3) bürgerliches (positives) Recht des einzelnen Staates, was sich auf den besonderen Willen des Volkes stützt.“¹⁸¹

Nach Grotius sind dies das Naturrecht und vor allem das Völkerrecht, welche im Falle eines Krieges nach wie vor ihre Anwendung finden. Derjenige, welcher den Kriegszustand aufrechterhalten will, tut dies nicht um einen politischen Zweck zu verfolgen, sondern um sich zu bereichern. Es handelt sich in diesem Fall nicht um Krieg, sondern um Verbrechen. Die Aussage,

„Wer Geschäft und Gewalt verbunden hat, wer seinen Geschäften mit Gewalt nachhilft und mit solchen Geschäften neue Gewalt finanziert, will keinen Staat, kann ihn nicht wollen.“¹⁸²,

ist nur bedingt richtig. Der Verbrecher braucht die Staatlichkeit¹⁸³, um in den Genuss seiner Erträge zu kommen. Fehlt diese Staatlichkeit, so

¹⁷⁹ Eppler, 2005, S. 117.

¹⁸⁰ Kirchmann, 1869, S. 43.

¹⁸¹ Ebd., S. 56.

¹⁸² Eppler, 2005, S. 119.

¹⁸³ Anm. d. Verf.: Staatlichkeit im Sinne einer Ordnung für ein bestimmtes Gemeinwesen. Dies kann ein Ehrenkodex für kriminelle Vereinigungen sein, aber auch eine regionale

generiert er diese selbst. Warlords und ihre Gefolgsleute leben in Gemeinwesen zusammen, die ihren eigenen Gesetzen und ihrer eigenen Ordnung folgen. Der schwache Staat wird durch diese eigene Ordnung kompensiert.

Da diese auf den „Bedarfsträger“ (Hervorhebung durch den Verfasser.) optimiert ist, besteht von dessen Seite her auch kein Wunsch mehr nach einer „staatlichen Ordnung“ (Hervorhebung durch den Verfasser.) neben der eigenen. Andererseits herrscht in einem solchen Zustand keine Sicherheit, weil die Ursachen für einen Aufruhr durch keine, vom gesamten Gemeinwesen getragene, Rechtsordnung beseitigt werden. Auf Grund dessen, dass ständig Krieg zu befürchten ist und die Gesetze oft verletzt werden, herrscht der eigentliche Naturzustand.¹⁸⁴

Die rechtliche Ordnung und die Staatlichkeit sind für den Verbrecher eine Grundlage für seine Bereicherung. Denn wenn keine Staatlichkeit, kein positives Recht, existiert, dann herrscht ein Zustand des Naturrechts, von dem Spinoza ausführt:

„Nicht anders als Sünde und Gehorsam (strenggenommen) können deshalb auch Gerechtigkeit und Ungerechtigkeit nur innerhalb eines Staates verständlich gemacht werden. Denn in der Natur gibt es nichts, von dem sich zu Recht sagen ließe, es gehöre diesem und nicht einem anderen; vielmehr gehören alle Dinge allen, denen nämlich, die die Gewalt haben, sie sich anzueignen.“¹⁸⁵

Der Verbrecher benötigt Staatlichkeit, um einerseits jemanden seines Besitzes zu berauben, der ja nur im Staat möglich ist, und andererseits seinen Besitz durch den Staat gesichert zu sehen. Auch ist das Verbrechen als Unrecht, welches einem widerfahren kann, erst im Staat möglich, da erst Recht die Definition von Unrecht zulässt. Das Verbrechen definiert sich aus der Staatlichkeit heraus.

„[...] und ungerecht ist derjenige, der im Gegenteil danach strebt, zu dem Seinen zu machen, was einem anderen gehört.“¹⁸⁶

In Zusammenschau von Spinoza und Clausewitz lässt sich eine Abgrenzung zwischen Krieg und Verbrechen ziehen, welche sich an der Intention der beiden Phänomene orientiert. Für Spinoza ist Verbrechen Bereicherung zum persönlichen Vorteil, während der politische Zweck zum Nutzen des Gemeinwesens den Krieg bei Clausewitz beschreibt.

Obwohl beiden Phänomenen vieles gemeinsam ist – die Anwendung von Gewalt oder die widerstrebenden Interessen der Akteure – unterscheiden sie sich im Zweck, den sie verfolgen. Die Intention ist zum einen politischer Natur, im Falle des Krieges, zum anderen krimineller Natur, im Falle des

Ordnung von bestimmten Warlords, wie es sie zum Beispiel in Afghanistan oder vielen afrikanischen Ländern gibt.

¹⁸⁴ Vgl. Spinoza, Politischer Traktat, S. 35f.

¹⁸⁵ Ebd., S. 20f.

¹⁸⁶ Ebd., S. 21.

Verbrechens. Die Organisierte Kriminalität ist unpolitisch, gewinnorientiert und bemüht das bestehende System auszunutzen.¹⁸⁷ Obwohl sie sich hinsichtlich der Intention unterscheiden, sind politischer bewaffneter Konflikt und Gewaltkriminalität bestimmten Ausmaßes in der Erscheinung nicht mehr voneinander zu unterscheiden, die Grenze ist fließend.¹⁸⁸

Die Zerstörung einer existenten staatlichen Ordnung, im Falle des Krieges, und der Wunsch nach Aufrechterhaltung einer Ordnung, um diese im Falle des Verbrechens ausnützen zu können, stehen einander gegenüber. Krieg ist ein gestaltendes Element¹⁸⁹, im Positiven wie im Negativen, während Verbrechen keine Veränderung der Ordnung sucht. Die Organisierte Kriminalität ist daran interessiert Staatlichkeit schwach aber bestehen zu lassen, um das System auszunutzen.

In diesem Zusammenhang ist noch etwas bemerkenswert: Krieg ist nur dann gegeben, wenn es zwei widerstreitende Parteien gibt.¹⁹⁰ Ein Angriff ist nur dann ein kriegerischer Akt, wenn der Gegner sich verteidigt. Ist das nicht der Fall, so handelt es sich um einen Überfall und somit liegt ein verbrecherischer Akt vor. Dabei handelt es sich um ein bloßes Einwirken einer Kraft ohne Gegenkraft.¹⁹¹ Unter den hier dargelegten Überlegungen muss auch das Phänomen Terrorismus betrachtet werden. Ist Terrorismus Krieg oder Verbrechen?

Die Sichtweisen in der einschlägigen Literatur gehen von einem Extrem ins andere. Betrachtet man Terror unter den weiter oben diskutierten Gesichtspunkten, so kann auf Grund der Ausdehnung, der Form und der Intention, die der Terror verfolgt, eine klare Zuordnung getroffen werden. Terror ist keine Bereicherung, auch wenn kriminelle Taten zur Finanzierung des Terrors durchgeführt werden. Terror wird in der Regel von politisch oder religiös motivierten Gruppierungen unter Anwendung von bewaffneter Gewalt, die physisch, aber vor allem auch psychisch wirkt, ausgeübt. Wesentlich ist der Zweck, den der Terror verfolgt, welcher in der Zerstörung von politischen Ordnungen besteht und somit politischer Natur ist.¹⁹² Die Zuordnung der Verantwortung für die Bekämpfung des Terrors ist jedoch nicht einfach zu treffen.

Wenn die beiden Charakteristika, die Ausdehnung und die Form des Konfliktes, ergänzt werden um das dritte Element zur Feststellung des Wesens des Krieges, die Intention, so lässt sich folgendes Zwischenergebnis festhalten: Krieg erfolgt immer zwischen Gemeinwesen und unter Anwendung physischer Gewalt, in der Regel mit Waffen, und verfolgt einen politischen Zweck. Dieser Zweck orientiert sich immer an der Ordnung des Gegners, indem er sie auszulöschen versucht, um die eigene Ordnung einzusetzen. Diese Intention erlaubt auch eine Abgrenzung zum Verbrechen, welche einen wesentlichen Bestandteil zur Beantwortung der Forschungsfrage darstellt.

¹⁸⁷ Vgl. Freudenberg, 2008, S. 138.

¹⁸⁸ Vgl. Eppler, 2005, S. 119f.

¹⁸⁹ Vgl. Stupka, 2011, S.128.

¹⁹⁰ Vgl. Kleemeier, 2002, S. 20.

¹⁹¹ Vgl. Stupka, 2011, S. 115ff.

¹⁹² Vgl. Freudenberg, 2008, S. 122.

Da der Krieg zwischen und/oder innerhalb von Gemeinwesen stattfindet, gibt es eine besondere Beziehung zwischen Krieg und Staat, welche im Folgenden dargestellt wird.

5.1.3 Das Verhältnis zwischen Krieg und Staat

Es ist festzuhalten, dass Krieg auf Grund seines politischen Zwecks unmittelbar mit dem Staat, oder anderen Formen von Gemeinwesen, in Verbindung steht. Spinoza führt die Bildung von Gemeinwesen darauf zurück, dass der Einzelne nur begrenzte Macht und somit so viel Recht hat, wie seine Macht reicht. Um sich nun in seinem Sein zu erhalten, bedarf der Einzelne weiterer Menschen. Diese erweitern ihre Macht und weiten damit auch ihr Recht aus.

„Und je mehr Verbündete so ihre Kräfte zusammengeschlossen haben werden, um so mehr Recht werden sie alle zusammen haben.“¹⁹³

Der Mensch bedarf des Staates, um sich im Sein zu erhalten und auch um sich zu verwirklichen. Der Staat hilft durch seine Rechtsordnung dem Menschen der Vernunft zu folgen und seine Affekte zu bändigen. Machiavelli fasst die Rolle des Staates in ähnlicher Weise. Er sieht den Staat ebenfalls als Einrichtung, die es den Menschen ermöglicht, sich vernunftgemäß zu verhalten und ihre Affekte zu kultivieren.¹⁹⁴

Er definiert zwei Möglichkeiten eine Stadt zu gründen: Zum einen in einer kargen Gegend, in der die Menschen, um sich im Sein zu erhalten, gezwungen sind ihre Affekte zu kultivieren, sich einzusetzen, um die für das Überleben der Gemeinschaft notwendigen Güter zu erwirtschaften. Diese Stadt wäre aber immer an der Grenze zum Untergang, weil ihr die Rücklagen fehlen, um auch Angriffen zu widerstehen. Zum anderen erwähnt er die Möglichkeit eine Stadt in einer fruchtbaren Gegend zu errichten. Hier ist es aber notwendig, die Menschen durch eine staatliche Beschränkung an die Kultivierung ihrer Affekte zu erinnern. Dazu führt er in den Discorsi Folgendes aus:

„Wo aber die günstige Lage eines Landes Müßiggang zur Folge haben könnte, muß man dafür Sorge tragen, daß die Gesetze Pflichten auferlegen, zu denen die günstige Lage nicht zwingt.“¹⁹⁵

Diese Sicht der inneren Beschränkung des Volkes setzt sich fort in der Betrachtung der Gefahren, denen ein Herrscher und somit auch ein Staat ausgesetzt sind. Hier erfolgt eine Reflektion auf die Momente des Konfliktes. Er führt dazu im Fürst an:

¹⁹³ Spinoza, Politischer Traktat, S. 16.

¹⁹⁴ Vgl. Münkler, Herfried: Machiavelli. Die Begründung des politischen Denkens der Neuzeit aus der Krise der Republik Florenz, 10. Aufl., Frankfurt / Main, Fischer, 1984, S. 266.

¹⁹⁵ Machiavelli, Discorsi, S. 9.

„Ein Herrscher hat nämlich zweierlei zu fürchten: einmal die Gefahren im Inneren von seiten seiner Untertanen und ferner die äußeren Gefahren von seiten fremder Machthaber.“¹⁹⁶

Die Gesetze ermöglichen es dem Herrscher die Ordnung im Inneren aufrecht zu erhalten. Diese sollten der Vernunft entspringen und so die Bürger für den Herrscher gewinnen. Hier kommt ein interessanter Zusammenhang zwischen innerer und äußerer Sicherheit zum Tragen.

„Sobald der Friede nach außen eingetreten war, fing der Krieg im Inneren wieder an.“¹⁹⁷

Nicht nur, dass der Krieg zwischen und in den Gemeinwesen herrscht, wird hier auch der Zusammenhang zwischen Bedrohung und Sicherheit unterstrichen. Auch Hobbes sieht den Müßiggang als Bedrohung des Gemeinwesens, denn dann ist der Mensch seiner Ansicht nach am unleidlichsten.¹⁹⁸ Machiavelli überträgt dieses Prinzip auch auf die Soldaten selbst.

„Ist Zwietracht unter den Soldaten entstanden, so ist das beste Mittel, sie in Gefahr zu schicken, denn dadurch werden sie gewöhnlich wieder einig.“¹⁹⁹

Um ein Gemeinwesen am Leben zu erhalten ist absolute Sicherheit nicht angebracht, diese führt zur Auflösung des Gemeinwesens, da jeder nur noch zu seinem Vorteil handelt, da er ja keine Gefahr von außen zu fürchten braucht. Für Spinoza stellt sich dieser Zusammenhang ähnlich dar.

„Ein Gemeinwesen ist deshalb, um unter eigenem Recht zu stehen, gehalten, die Ursachen für Furcht und Achtung aufrechtzuerhalten, weil anders es aufhörte, ein Gemeinwesen zu sein.“²⁰⁰

Er bezieht diese Aussage zwar auf das Verhältnis des einzelnen gegenüber dem Gemeinwesen, doch ist sie auch auf das Verhältnis zwischen Gemeinwesen anwendbar. Diese Bedrohung ist aber stets vorhanden, weil die Gemeinwesen, anders als die Bürger eines Staates, nicht unter einem gemeinsamen Recht stehen,²⁰¹ sich also in einem Zustand des Naturrechts befinden, welches dazu führt, dass diese Gemeinwesen einander von Natur aus Feinde sind.²⁰² Hier wird der Zusammenhang zwischen Krieg und Staat besonders deutlich. Hobbes fasst die Bildung von Gemeinwesen nicht als von den Menschen aus freien Stücken, also freiwillig gewählt, auf. Er sieht den

¹⁹⁶ Machiavelli, Der Fürst, S. 75.

¹⁹⁷ Machiavelli, Niccolò: Geschichte von Florenz. In: Ulfig, Alexander (Hrsg.): Machiavelli, Niccolò. Gesammelte Werke, Frankfurt am Main, 2006, S. 521.

¹⁹⁸ Hobbes, Thomas: Leviathan, Suhrkamp, Berlin 1966, S. 133.

¹⁹⁹ Machiavelli, Niccolò: Die Kunst des Krieges. In: Ulfig, Alexander (Hrsg.): Machiavelli, Niccolò. Gesammelte Werke, Frankfurt am Main, 2006, S. 831.

²⁰⁰ Spinoza, Politischer Traktat, S. 32.

²⁰¹ Vgl. Kirchmann, 1869, S. 154.

²⁰² Vgl. Spinoza, Politischer Traktat, S.28.

Staat als das Bindemittel der Gesellschaft, welches durch die Macht alle einzuschüchtern erst in der Lage ist, einen Zusammenhalt zu generieren.²⁰³

Hobbes hat aber letztlich auch die Bedrohung, als den das Gemeinwesen stiftenden Faktor, im Auge, obwohl diese Bedrohung nicht unmittelbar, sondern im Wege der Staatsmacht die Menschen dazu bringt sich zusammenzuschließen. Es ist die Macht der Gesetze, die die Menschen vernünftig halten soll. Fehlt diese Macht, so lebt der Mensch in einem Kriegszustand, welcher sich nicht unbedingt in Kampfhandlungen äußern muss.²⁰⁴ Somit ist der Krieg für Hobbes die staatsstiftende Ursache und damit indirekt, im Wege der Staatsmacht, die Begründung von Staatlichkeit. Der latente Krieg ist also die Bedingung für die Staatlichkeit und andererseits ist der Staat die Bedingung für den Krieg.

Es kann hier auch ein Zusammenhang zwischen den Ebenen, den Momenten, des Konfliktes und der Unterscheidung zwischen innerer und äußerer Sicherheit hergestellt werden. Bedrohungen innerhalb des Gemeinwesens, wie Zwist oder Aufruhr, betreffen die Sphäre der inneren Sicherheit und Bedrohungen zwischen den Gemeinwesen, wie der Krieg, berühren die Sphäre der äußeren Sicherheit.

5.1.4 Der Zusammenhang zwischen Krieg und Sicherheit

Die Unterscheidung in diese beiden Bereiche der Sicherheit liefert einen Hinweis auf die Zuständigkeit der Träger der Staatsgewalt. Zunächst soll hier auf die Abhängigkeit zwischen Krieg und Sicherheit eingegangen werden. Die Staaten befinden sich in einem Zustand des Naturrechts, sie sind wie der Einzelne bemüht, sich im Dasein zu erhalten und können dies auch aus eigener Kraft erreichen.²⁰⁵ Und weil

„[...] Staaten im Gegensatz zueinander stehen und daher um ihre Sicherheit besorgt sein müssen.“²⁰⁶,

ist die Verbindung von Sicherheit mit dem Staat angezeigt. Diese Bedrohung ist permanent, denn es gibt kein allen Staaten gemeinsames Recht, dem diese unterliegen. Dieser latente Krieg kann manifest werden, wenn allein einer der Staaten den Willen dazu aufbringt.²⁰⁷ Zweck des Staates ist es, diese latente Bedrohung durch entsprechende innere Maßnahmen zu mindern, nicht zu beseitigen.

Es verhält sich wie mit den Affekten, welche zu kultivieren und nicht auszulöschen sind, da sie die Natur des Menschen ausmachen.²⁰⁸ Die Bedrohung ist zu kultivieren, einzuhegen, nicht zu beseitigen, da sie zur Existenz des Staates beiträgt. Es ergibt sich hier also die erste Verbindung zwischen Krieg und Sicherheit. Die äußere Sicherheit wird direkt durch

²⁰³ Vgl. Hobbes, Leviathan, S. 95.

²⁰⁴ Vgl. ebd., S. 96.

²⁰⁵ Vgl. Spinoza, Politischer Traktat, S. 27.

²⁰⁶ Pesendorfer, 1982, S. 92. (in: Neisser, 1982)

²⁰⁷ Vgl. Spinoza, Politischer Traktat, S. 28.

²⁰⁸ Vgl. ebd., S. 9.

Bedrohungen, wie dem latenten Krieg, beeinflusst. Um der äußeren Bedrohung entgegentreten zu können, braucht man Ruhe und Ordnung im Inneren, also Eintracht unter den Bürgern des Staates.

Spinoza sieht den Zweck des Staates darin Frieden und Sicherheit zu erhalten.²⁰⁹ Dies kann dann erreicht werden, wenn die Menschen in Eintracht zusammenleben und die Gesetze des Gemeinwesens eingehalten werden. Eine äußere Bedrohung ist somit Voraussetzung für innere Eintracht. Diese Eintracht kann durch dreierlei Faktoren gestört werden. Zum einen durch diejenigen, welche nichts fürchten und nur ihrem eigenen Recht unterliegen. Diese nennt Spinoza Feinde des Staates.²¹⁰ Zum anderen durch Wegfall der äußeren Bedrohung und schließlich dadurch, dass sich das Gemeinwesen vergeht.

„Ein Gemeinwesen vergeht sich also, wenn es solches ausführt oder geschehen läßt, was den eigenen Untergang verursachen kann.“²¹¹

Die Feinde des Staates können als Verbrecher verstanden werden, die sich einem Affekt des Hasses hingeben.²¹² Sie folgen dem Bereicherungsgedanken und müssen durch das Recht in Schranken gehalten werden. Ihre Taten fallen damit in die Zuständigkeit der Gerichte. Wie bereits ausgeführt, ist der Wegfall der äußeren Gefahr ein Faktor, der das Gemeinwesen seiner Auflösung zuführt.

Der Staat ist als höchste menschliche Macht nicht absolute Macht, sondern steht im Gegensatz zu anderen Staaten und deren Macht. Diese partikularen Mächte stehen im Widerspruch zueinander, man spricht von latentem Krieg.²¹³ Der Wegfall dieser Bedrohung würde dazu führen, dass die Macht des Staates keine andere Macht mehr hat, der sie gegenübersteht, der gegenüber sie sich behaupten muss. Dies führt dazu, dass die Menschen sich nicht mehr notwendigerweise zusammenschließen müssen, um ihre Macht zu vergrößern. Sie können sich ihren Partikularinteressen hingeben, was zweifellos zur Auflösung des Gemeinwesens führt. Machiavelli führt dazu Folgendes aus:

„Denn die Tapferkeit gebiert Ruhe, die Ruhe Müßiggang, der Müßiggang Unordnung, die Unordnung Verfall. Ebenso entsteht aus dem Verfall Ordnung, aus der Ordnung Tapferkeit, hieraus Ruhm und Glück.“²¹⁴

Nach Machiavelli bringen Friede und Stabilität Instabilität und Unfrieden hervor. Die Bedrohung der Sicherheit ermöglicht also erst Sicherheit. Sicherheit und Krieg, wenn auch nicht unbedingt der manifeste Krieg, stehen damit in einem direkten Verhältnis. Da aber die Staaten als Ausprägungen der Macht und des Rechts einander immer gegenüberstehen, besteht die Gefahr in der Wahrnehmung der Bedrohung. Wird diese

²⁰⁹ Vgl. ebd., S. 35.

²¹⁰ Vgl. ebd., S. 25.

²¹¹ Ebd., S. 32.

²¹² Vgl. ebd., S. 16.

²¹³ Vgl. Pesendorfer, 1982, S. 96. (in: Neisser, 1982)

²¹⁴ Machiavelli, Niccolò: Mensch und Staat, tredition Verlag, Hamburg 2012, S. 14.

Bedrohung nicht mehr wahrgenommen, führt dies zu dem oben beschriebenen Vorgang.

Hier kann der Staat sich sehr leicht vergehen, in dem er trotz Bedrohung, die jedoch nicht als solche wahrgenommen wird, sich nicht gegen diese rüstet. Seine Aufgabe besteht also darin Eintracht herzustellen. Diese soll, so Spinoza, nicht auf Furcht sondern auf Vernunft basieren.²¹⁵

„Friede ist nämlich nicht die Abwesenheit von Krieg, sondern eine Tugend, [...]“²¹⁶

Der Friede und damit die Sicherheit entspringen der Vernunft. Es ist vernünftig Frieden zu suchen.

„Hinzu kommt, daß die Vernunft durchaus lehrt, den Frieden zu suchen, der sich gewiß nur aufrecht erhalten läßt, wenn die gemeinsamen Rechtsgesetze des Gemeinwesens unangetastet bleiben.“²¹⁷

Sicherheit ist eine Wechselwirkung zwischen innerer Sicherheit, der Eintracht, und der äußeren Sicherheit, der Ausrichtung gegen die Bedrohung durch den latenten Krieg und steht in direktem Verhältnis zu diesen Bedrohungen. Sicherheit und Souveränität greifen ineinander, welches zur Betrachtung des Verhältnisses von Krieg und Souveränität führt.

5.1.5 Das Verhältnis zwischen Krieg und Souveränität

Der Krieg stellt eine Verletzung der Souveränität dar, er ist ein Eingriff in die Politik eines Gemeinwesens. Dabei spielt es keine Rolle, ob es sich dem Charakter nach um einen existenziellen oder einen instrumentellen Krieg handelt. Der Staat ist in seiner Machtausübung sowohl nach innen als auch nach außen eingeschränkt. Da ein Krieg entweder territorial oder aber institutionell wirkt, in dem er zum Ziel hat den Ordnungsrahmen eines der beiden Gegner zum Teil oder ganz zu verändern, greift er in die Souveränität der Gemeinwesen, die am Konflikt beteiligt sind, ein.

Der Staat muss in der Lage sein die Souveränität zu verteidigen oder wiederherzustellen. Der Inhaber der höchsten Staatsgewalt, der Souverän, hat damit die Wehrverantwortung.²¹⁸ Dies gründet darauf, dass ein Gemeinwesen nur dann das Gemeinwohl sicherstellen kann, wenn es seine Souveränität durchsetzen kann. Ein Angriff auf die Souveränität ist ein Angriff auf die Handlungsfähigkeit des Gemeinwesens und somit eine Beeinträchtigung der Erreichung des Gemeinwohls. Die Souveränität bedeutet die Möglichkeit der Umsetzung der Politik. Der Souverän ist letztlich der, der die Politik im Gemeinwesen gestaltet, somit ist der Schutz dieser

²¹⁵ Vgl. Spinoza, Politischer Traktat, S. 36.

²¹⁶ Ebd., S. 36.

²¹⁷ Ebd., S. 23.

²¹⁸ Vgl. Stupka, 2011, S. 237.

auch in seiner Verantwortung.²¹⁹ Dabei bedient er sich des Militärs als Institution zum Schutz und zur Wiederherstellung der Souveränität.

„Der Souverän, so sagten wir, ist wehrverantwortlich, denn seine Aufgabe als oberster Herrscher ist es die Existenz des Gemeinwesens und die Zufriedenheit seiner Bürger zu gewährleisten. Der Souverän gewährleistet dies durch die Aufbietung von Streitkräften, die er anwirbt und denen er selbst vorsteht.“²²⁰

Die Landesverteidigung bedeutet somit Souveränitätsschutz, im Sinne des Schutzes und der Wiederherstellung des Ordnungsrahmens, sowohl national als auch international.²²¹ Diese Aufgabe soll die Funktionalität der Institutionen des Gemeinwesens erhalten oder wiederherstellen, mit dem Zweck das Gemeinwohl zu ermöglichen. Krieg betrifft somit die Souveränität in zweierlei Hinsicht, zum einen greift er in das Machtgefüge zwischen den Staaten ein und zum zweiten wirkt er auf das Machtgefüge innerhalb der Kriegsparteien.

Der Krieg stellt also einen Angriff auf die oder eine Beeinflussung der Souveränität der Staaten dar. Die Handlungsfähigkeit der Gemeinwesen wird vermindert und damit der Zweck des Staates gefährdet. Dies geschieht sowohl im instrumentellen Krieg, hier beschränkt auf die Regierung und die staatlichen Institutionen, als auch im existenziellen Krieg, hier in totaler Weise auf das gesamte Gemeinwesen ausgedehnt. Krieg ist somit untrennbar mit dem Staat, der Sicherheit und der Souveränität verbunden.

Als Zwischenresümee wird festgehalten, dass der Krieg ein politisches Instrument ist, Politik ist wiederum – als Handeln für das Gemeinwohl – nur im Gemeinwesen möglich. Das Gemeinwesen benötigt, um unbeeinflusst diesen Staatszweck zu erreichen, die Souveränität, welche sich auf ein Mindestmaß an Sicherheit stützt.

„Die Souveränität des Staates wird mit seinen Funktionen des Schutzes und der Friedenssicherung nach innen wie nach außen begründet.“²²²

Die relative Sicherheit basiert auf Bedrohungen, die der Ausgangspunkt für die Notwendigkeit der Gefahrenabwehr sind. Diese Gefahrenabwehr obliegt den bewaffneten Trägern der Staatsgewalt. Manifestiert sich die Bedrohung und ist damit die Souveränität gefährdet, so ist es die Aufgabe des Gemeinwesens sich, auch mit Krieg, dagegen zur Wehr zu setzen, um die Handlungsfähigkeit aufrecht zu erhalten. Diese Handlungsfähigkeit dient dann wieder dem Gemeinwohl, also dem Letztzweck des Gemeinwesens.

Der Zusammenhang zwischen Krieg und den betrachteten Begriffen kommt in allen weiteren Momenten des Krieges zum Tragen. Es ist dabei

²¹⁹ Vgl. ebd., S. 237.

²²⁰ Ebd., S. 270.

²²¹ Vgl. Benz, 2008, S. 131.

²²² Ebd., S. 129.

notwendig das Wesen des jeweiligen Momentes zu fassen und mit den dargestellten Zusammenhängen in die richtige Relation zu setzen. Der Blick auf den Begriff vom Krieg beschließt dieses Kapitel.

5.1.6 Der Begriff vom Krieg

Der Krieg lässt sich somit als bewaffneter politischer Konflikt begrifflich wie folgt fassen:

„[...] a political conflict is a positional difference, regarding values relevant to a society (the conflict items), between at least two decisive and directly involved actors, which is being carried out using observable and interrelated conflict measures that lie outside established regulatory procedures and threaten core state functions, the international order or hold out the prospect to do so.“²²³

Dieser politische Konflikt muss allerdings in seinen conflict measures die Eskalationsstufe der bewaffneten Gewaltanwendung erreicht haben. Krieg findet zwischen zwei Kontrahenten statt, er ist ein Zweikampf. Als solcher ist der Krieg ein Moment des Konfliktes und da er mit Gewalt, im Sinne von Clausewitz mit physischer Gewalt, hervortritt, ist er eine Ausprägung des bewaffneten Konfliktes. Der Zweck des Zweikampfes ist es, dem Gegner den eigenen Willen aufzuzwingen, mittels physischer Gewalt.²²⁴ Das Ziel des Krieges liegt darin den Gegner wehrlos zu machen. Der Wille äußert sich in den Handlungen des Staates, dieses Handeln ist die Tätigkeit der Politik, welche neben Zielen auch die Mittel bereitstellt. Der Wille hat eine somit politische Dimension, damit hat der Krieg einen politischen Zweck.

Daraus folgt, dass der Krieg immer zwischen Gemeinwesen – oder Teilen davon – geführt wird. Denn nur in Gemeinwesen ist politisches Handeln möglich.²²⁵ Er grenzt sich durch seinen Zweck klar vom Verbrechen ab und zielt auf die Ordnung eines anderen Gemeinwesens, um diese durch die eigene Ordnung zu ersetzen. Er ist seinem Wesen nach auch begründend für die Existenz von Gemeinwesen. Einerseits bedarf es der Bedrohungen, wie dem Krieg, um ein Gemeinwesen zu bilden und andererseits braucht es das Gemeinwesen um ihn zu führen.²²⁶

Abgeleitet daraus lässt sich, aus der Unsicherheit hervorgerufen, durch die Bedrohung erst Sicherheit herstellen, in dem das Gemeinwesen sich derart gestaltet, dass es durch eine permanente Spannung von außen seine innere Sicherheit herstellt. Der Krieg ist seinem Wesen nach auch sicherheitsfördernd, oder anders gesagt, ein wesentliches gestaltendes Element des Gemeinwesens, des Staates.²²⁷

²²³ Bings, Felix u.a.: HIIK Conflict Barometer 2011. disputes, non-violent crises, violent crises, limited wars, wars, Campus Bergheim 2012, S. 108.

²²⁴ Vgl. Clausewitz, Vom Kriege, S. 13ff.

²²⁵ Vgl. Machiavelli, Die Kunst des Krieges, S. 720f. (in: Ulfing, 2006)

²²⁶ Vgl. Hobbes, Leviathan, S. 96.

²²⁷ Vgl. Douhet, 1935, S. 61.

Die Charakteristika, die in diesem Abschnitt dargestellt wurden, definieren das Wesen und die Natur des Krieges. Es sind dies die Ausdehnung, die Form, sowie die Intention des Konfliktes, welche ihn näher bestimmen und ihn vom Verbrechen abgrenzen. Alle diese Punkte finden sich in der Clausewitzschen Definition des Krieges wieder, wobei im weiteren Verlauf der Arbeit noch zu klären ist, inwieweit diese noch ihre Gültigkeit hat, besonders in Bezug auf den Cyberwar. Nachdem nun geklärt ist, was Krieg ist, werden die anderen für seine Typologisierung wichtigen Faktoren beleuchtet. Zunächst sollen die Akteure in diesem Konflikt untersucht werden.

5.2 Zu den Akteuren im Krieg

Wie schon festgestellt, ist ob seines Zweckes der Krieg Angelegenheit von Gemeinwesen. Es gibt viele Möglichkeiten die Akteure einzuteilen, hier wird eine Unterteilung in staatliche und nichtstaatliche Akteure im Krieg durchgeführt. Dabei meint staatlich, dass die Handlungen dieser Akteure auf der Basis des Rechts erfolgen, also rechtlich durch das Gemeinwesen legitimiert sind.

Wenn also die staatlichen Akteure rechtlich legitimiert sind, muss bei den nichtstaatlichen Akteuren davon ausgegangen werden, dass diese keine derartige Legitimation haben. Wie noch zu zeigen sein wird, kommt es dabei immer auf den Blickwinkel der Betrachtung an. Neben den staatlichen und nichtstaatlichen Akteuren sind noch internationale bzw. transnationale Akteure zu berücksichtigen.

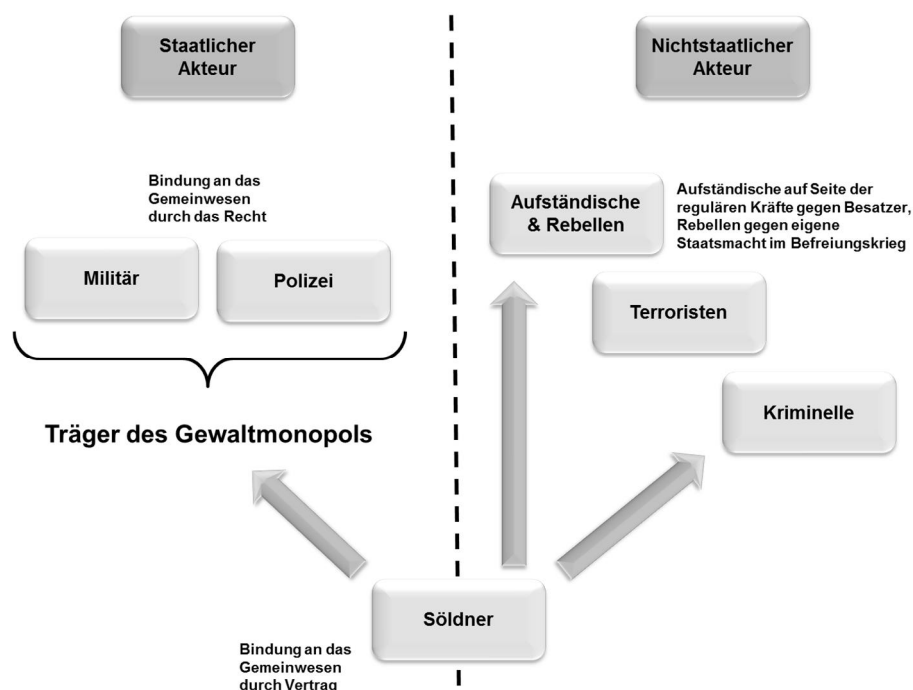


Abbildung 3: Akteure im Krieg²²⁸

²²⁸ Abbildung durch den Verfasser erstellt.

Da der Krieg die gewalttätige Austragung von Konflikten ist und diese mit Waffengewalt ausgefochten werden, sind im Fokus der Betrachtung die bewaffneten Akteure in solchen Konflikten zu sehen. Vor allem bei den nichtstaatlichen und den internationalen Akteuren werden auch solche angeführt, die nicht über diese Möglichkeit verfügen, ohne diese aber im Detail zu analysieren.

5.2.1 Exkurs: Zur Definition der bewaffneten Akteure im Krieg

In einem Krieg stehen einander verschiedene Streitkräfte gegenüber. Dabei wird als allgemeiner Begriff einer solchen Folgendes definiert:

„Streitkraft ist die Gesamtheit der organisierten bewaffneten Verbände, Einheiten und Gruppen, die militärische Handlungen ausführen kann und einer Führung untersteht, welche für das Verhalten ihrer Untergebenen verantwortlich ist. Dies gilt auch dann, wenn diese bewaffneten Kräfte durch eine Regierung oder ein Organ vertreten sind, welche von einem Gegner nicht anerkannt werden.“²²⁹

Grundsätzlich wird unter diesem Begriff die bewaffnete Macht eines souveränen Staates verstanden. Diese wendet die konventionellen Verfahren zur Führung des Gefechtes an. Zweck ist es, den Staat vor äußeren Gefahren zu schützen. In der Dienstvorschrift Truppenführung findet sich folgende Definition:

„Streitkräfte sind das Mittel des Staates zur Selbstbehauptung gegen Gewalt von außen. Daneben sind sie ein entscheidendes Mittel zur Wahrung seiner Interessen.“²³⁰

Dabei sind unter äußeren Gefahren auch jene zu verstehen, welche die Existenz des Staates sowie seiner Bevölkerung bedrohen. Im Rahmen der Beteiligung vieler Staaten an und in Bündnissen sind Aufgaben im Rahmen der Solidarität immer mehr in den Vordergrund tretend.²³¹ Das führt dazu, wie noch erläutert wird, dass sich verschieden Streitkräfte in Bündnissen zusammenschließen.

Eine besondere Form der bewaffneten Akteure sind die paramilitärischen Kräfte. Es handelt sich dabei um bewaffnete Kräfte, die nicht Teil der regulären Streitkräfte sind, diesen aber in Organisation, Ausbildung und Verfahren ähneln. Da die Aufgaben dieser Gruppierungen beinahe gleich denen regulärer Kräfte sind, ist eine Zusammenarbeit mit diesen durchaus möglich. Im Army Field Manual für Counter Insurgency Operations ist Folgendes zu finden:

²²⁹ BMLV, DVBH Führungsbegriffe, Wien, November 2005, S. 142.

²³⁰ BMLV, DVBH (zur Erprobung) Truppenführung, Wien, August 2004. S. 17.

²³¹ Vgl. ebd., S. 17.

„Forces or groups which are distinct from the regular armed forces of any country but resemble them in organisation and training and in the mission they undertake.“²³²

Diese Kräfte werden, wie auch die Polizeiverbände, oft als Milizen bezeichnet. Eine Gruppe der bewaffneten Akteure, denen die staatliche Legitimation fehlt, sind sogenannte Irreguläre Kräfte (IK).

Unter IK sind Guerillas, Partisanen, aber auch Terroristen, Aufständische sowie gewaltbereite Gruppen Organisierter Kriminalität oder bewaffnete Banden im Einsatzraum, in denen friedensunterstützende Operationen erfolgen, zu verstehen.²³³ Das Spektrum der möglichen Verfahren und Taktiken reicht bei IK von Terror, Sabotage, Guerilla-Kampf bis hin zum konventionellen Kampf (Anm. d. Verf.: Angriff, Verteidigung und Verzögerung.).²³⁴

„Terrorismus kann als Strategie substaatlicher Akteure verstanden werden und wird vor allem dort ausgelöst, wo es nationale, ethnische, soziale, wirtschaftliche oder religiöse Konflikte bzw. Defizite gibt und welche unter Androhung bzw. Einsatz von punktueller, unvorhergesehener und brutaler Gewalt das Erreichen eines politischen oder ideologischen Zieles verfolgen.“²³⁵

Beim Guerilla-Kampf handelt es sich um eine Form des bewaffneten Kampfes, welche vor allem von irregulären Kräften gegen eine Besatzungsmacht oder den eigenen Staat geführt wird. Ziel ist es dabei die vorherrschenden Machtverhältnisse zu ändern. Die taktischen Verfahren, welche zur Anwendung gelangen, sind der Überraschungsangriff (hit and run), der Hinterhalt und die Sabotage. Die britische Vorschrift, welche sich mit den Counter Insurgency Operations befasst, führt dazu Folgendes aus:

„Military and paramilitary operations conducted in enemy-held or hostile territory by irregular, predominantly indigenous forces.“²³⁶

Mit diesem Exkurs ist die begriffliche Basis für die folgenden Abschnitte gelegt.

5.2.2 Die staatlichen Akteure

Als staatliche Akteure im Krieg und als Träger des Gewaltmonopols des Staates lassen sich einerseits das Militär – als bewaffnete Macht des Staates²³⁷ – und die Polizei andererseits identifizieren. Die Trennung in zwei

²³² Royal Army, Army Field Manual, Volume 1, Combined Arms Operations, Part 10, Counter Insurgency Operations, (Strategic and Operational Guidelines) Revised and updated Version, 2007. S. xi.

²³³ Vgl. BMLVS, Militärstrategisches Konzept des Österreichischen Bundesheeres, Bundesheer 2010, (Beilage zu GZ. 92150/3-MilStrat/2006), Wien, Fassung 2006. S. 38f.

²³⁴ Vgl. Department of Defense, Directive Number 3000.07, 01. December 2008. S. 11f.

²³⁵ BMLVS, Terrorabwehr und Eventschutz, Operatives Fachkonzept, Wien, Juli 2009. S. 19.

²³⁶ Royal Army, Army Field Manual, Volume 1, Combined Arms Operations, 2007. S. xi.

²³⁷ Vgl. Stupka, 2011, S. 78f.

uniformierte Wachkörper war nicht von Anfang an gegeben. Bei Platon sind die beiden Aufgabenfelder schon klar herausgearbeitet, aber eine Aufteilung auf unterschiedliche Aufgabenträger erfolgt hier noch nicht.

„Wir aber wollen diese Erdensöhne ausrüsten und dann unter Anführung der Befehlshaber aufstellen. Sind sie nun zusammen: so sollen sie zusehen, wo es am vorteilhaftesten ist, in der Stadt das Lager aufzuschlagen, um von da aus sowohl die drinnen am besten im Zaum zu halten, wenn etwa einer den Gesetzen nicht gehorchen wollte, als auch die von außen abzuwehren, wenn etwa ein Feind wie ein Wolf die Herde anfallen wollte.“²³⁸

Platon sieht in der Politeia einen eigenen Stand für die Erledigung dieser Aufgaben vor. Dieser Wächterstand ist als der Träger des Gewaltmonopols vorgesehen und durch das Gemeinwesen legitimiert.²³⁹ Der Wächter als Krieger ist der staatliche Akteur schlechthin. Diese Zuweisung der Aufgabe an einen bestimmten Stand, wenn man so will an ein Berufsheer, sieht er im zweitbesten Staat, welchen er in der Nomoi beschreibt, nicht mehr gegeben.

Hier tritt zu Krieg und Zwist die Entzweiung, der Aufruhr hinzu, welcher ein innerer Krieg, ein Bürgerkrieg ist, der nur dann geführt werden kann, wenn die Bürger bewaffnet und in der Kriegführung geschult sind.²⁴⁰ Dies verweist auf die Heranbildung eines Bürgerheeres, welches die Aufgaben, die im besten Staat den Wächtern zukommen, erfüllen. Orientiert ist diese Einteilung an der Realität, welche Platon in der realen Polis vorfand.

Für Platon hat der Bürger als Krieger besondere Eigenschaften zu haben, um nicht im Aufruhr gegen die Obrigkeit zu kämpfen.

„Von diesem behaupten wir, daß er in einem verderblicheren Kriege sich um sehr vieles besser erwies als jener, um so viel fast, als Gerechtigkeit, Besonnenheit und Weisheit mit Tapferkeit vereint besser sind als eben die Tapferkeit allein. Denn treu und fest bei Entzweiungen dürfte er wohl niemals ohne die gesamte Tugend werden; in dem Kriege aber, von dem Tyrtaios spricht, wacker in die Schlachtreihen zu treten und kämpfend in den Tod zu gehen, dazu sind auch viele Söldner bereit, von denen die meisten, nur ganz wenige ausgenommen, sich als keck, ungerecht, übermütig und fast als die unverständigsten von allen zeigen.“²⁴¹

Der Bürgerkriegler hat also tugendhaft zu sein, anders als der Söldner, den Platon hier als wenig tugendhaft beschreibt. Der Bürger ist im Krieg durch das Gemeinwesen legitimiert und steht in einem besonderen Verhältnis zum Gemeinwesen, sein Handeln beruht auf Recht und Gerechtigkeit. Platon sieht den Grund für einen Bürgerkrieg hier in der Auflösung des Gewaltmonopols zum Zwecke der Kriegführung. Durch

²³⁸ Platon, Politeia, S. 314.

²³⁹ Vgl. ebd., S. 264ff.

²⁴⁰ Vgl. Platon, Nomoi, S. 162f.

²⁴¹ Ebd., S. 162f.

Bewaffnung der Bürger ist das Potential vorhanden, dass diese sich gegen die Obrigkeit erheben. Diese Aufständischen handeln hier aber nicht mehr auf der Grundlage der Gesetze der Polis. Dieser Akteur ist dann nicht mehr länger als staatlicher Akteur zu verstehen.

Söldner fanden im antiken Griechenland kaum ein Betätigungsfeld, jedoch wurden Griechen als Söldner vor allem von östlichen Herrschern angeworben, da die Griechen als fähige Soldaten galten.²⁴² Dabei spielten sie eine ähnliche Rolle wie Jahrhunderte später die Schweizer Landsknechte. Waren die Söldner in der griechischen Polis weniger von Bedeutung, so sind im Italien zur Zeit Machiavellis die Söldner die Hauptakteure im Krieg.

Obwohl sie auf Anordnung eines Gemeinwesens handeln, sind sie nicht in den Bereich der staatlichen Akteure einzureihen, denn ihr Verhältnis zum Staat ist nicht auf eine besondere rechtliche Basis gestellt, sondern auf reine Profitgier aufgebaut. Sie handelten auf vertraglicher Basis, der Condotta, und nicht auf Grundlage der Gesetze. Für den sogenannten Condottiere ging es um Gewinnmaximierung, entsprechend unzuverlässig waren diese Verbände. Sie boten sich dem Fürsten an, der mehr zahlte. Hier liegt eindeutig ein verbrecherischer Zweck dem Handeln des Akteurs zu Grunde. Dazu führt Machiavelli in den Discorsi aus:

„Diese Art von Soldaten raubt nach dem Siege sowohl den aus, für den sie gefochten, als auch den, gegen den sie gefochten haben; sie tun dies entweder aus Tücke des Machthabers, der sie ausgeschickt, oder aus persönlichem Ehrgeiz.“²⁴³

Mit Machthaber ist hier der Herrscher gemeint und der persönliche Ehrgeiz ist als persönliche Bereicherung zu verstehen. Machiavelli spricht sich daher für ein Bürgerheer aus, welches verlässlich für das Gemeinwesen auf Basis dessen Gesetze handelt.²⁴⁴ Für Platon – wie auch für Machiavelli – ist der Träger des Gewaltmonopols nach außen der Angehörige eines Bürgerheeres. Als staatlicher Akteur kann also der Soldat eines Gemeinwesens verstanden werden, dessen Wurzeln auch in diesem zu finden sind.

Grotius sieht vom Naturrecht aus betrachtet alle Bürger als wehrfähig an und formuliert,

„[...] dass von Natur alle Unterthanen zum Kriege verwendet werden dürfen; [...].“²⁴⁵

Staatsgewalt ist in ihrem Vollzug auf verschiedene Staatsorgane verteilt. Naturrechtlich steht jedem das Recht auf Erhalt im Dasein zu. Dieses Recht, auch Gewalt zur Abwehr von Gefahren für das Dasein anzuwenden,

²⁴² Vgl. Stoll, Oliver: Gemeinschaft in der Fremde. Xenophons "Anabasis" als Quelle zum Söldnertum im klassischen Griechenland? In: Göttinger Forum für Altertumswissenschaft (Hrsg.), Göttinger Forum für Altertumswissenschaft 5, Heidelberg 2002, S. 127f.

²⁴³ Machiavelli, Discorsi, S. 230.

²⁴⁴ Vgl. Machiavelli, Der Fürst, S. 49.

²⁴⁵ Kirchmann, 1869, S. 215.

wird an den Staat abgetreten.²⁴⁶ Auch Grotius sieht in der auf dem Recht basierenden Handlung der Träger der Staatsgewalt für das Gemeinwesen das wesentliche Charakteristikum des staatlichen Akteurs.

„[...] denn ein Soldat oder Beamter, der nicht für sich handelt, sondern für Andere, mit rechtmässig empfangener Gewalt.“²⁴⁷

Als staatliche Akteure fasst Spinoza explizit die von der höchsten Gewalt im Staate eingesetzten Organe zur Erfüllung der Staatsaufgaben und grenzt diese von nichtstaatlichen Akteuren ab:

„Weil also allein dem Souverän das Recht zusteht, die öffentlichen Geschäfte zu führen oder hierfür Verwalter zu benennen, ist es eine Anmaßung der Gewalt des Staates, wenn ein Untertan bloß nach eigenem Ermessen und ohne Wissen der dazu berufenen obersten Versammlung sich in irgendeiner öffentlichen Angelegenheit engagiert, selbst wenn er geglaubt hat, mit seiner Absicht das Beste im Interesse des Gemeinwesens zu tun.“²⁴⁸

Es obliegt also allein den staatlichen Organen im Auftrag des Gemeinwesens für das Gemeinwesen die Staatsgewalt auszuüben. Er verurteilt damit indirekt auch den Bürgerkrieg, als eine Einmischung nichtstaatlicher Akteure in die Geschäfte des Staates. Es sind die staatlichen Organe, die die Staatsgewalt ausüben und dies auf Basis der Gesetze tun; zudem stehen sie in einem besonderen Verhältnis zum Gemeinwesen.

Sie üben die Macht im Auftrag des Staates aus und sind diesem und seinen Bürgern dafür auch verantwortlich. Da Clausewitz vom Krieg als Gewaltakt zwischen Gemeinwesen ausgeht, sind für ihn die primären Akteure des bewaffneten politischen Konfliktes die legitimierten Streitkräfte der Gemeinwesen. Die Streitkräfte stehen hier synonym für die stehenden Heere der Zeit in der Clausewitz wirkte. Er grenzt diese von dem Volksheer ab, welches er als letztes Mittel im Kampf um die Existenz des Staates sieht.

„Zum Sterben ist es immer noch Zeit, und wie es ein Naturtrieb ist, daß der Untergehende nach dem Strohalm greift, so liegt es in der natürlichen Ordnung der moralischen Welt, daß ein Volk die letzten Mittel seiner Rettung versucht, wenn es sich an den Rand des Abgrundes geschleudert sieht.“²⁴⁹

Das Volksheer ist in diesem Sinn keine reguläre Streitkraft, sondern ein Notfallinstrument, welches rein defensiver Natur ist, da es nur im eigenen Land und im Zusammenwirken mit dem stehenden Heer zum Einsatz gelangt. Gemeinsam ist den hier aufgeführten Denkern, dass sie sich nur am Rande mit den Trägern der Staatsgewalt beschäftigen, die für die innere Sicherheit verantwortlich zeichnen, es erfolgt daher auch keine Abgrenzung zu diesen. Im weiteren Verlauf der Geschichte ergab sich, aus der sehr

²⁴⁶ Vgl. Konegen, 1998, S. 21.

²⁴⁷ Kirchmann, 1869, S. 135.

²⁴⁸ Spinoza, Politischer Traktat, S. 31.

²⁴⁹ Clausewitz, Vom Kriege, S. 174.

unterschiedlich werdenden Aufgabenstellung zwischen dem Innen und dem Außen, die Notwendigkeit für jede dieser Aufgaben eigene Elemente zu schaffen, die Polizei und das Militär.

Die Polizei hat vor allem im Frieden ihre Hauptaufgabe auszuführen, im Krieg wird die Ordnung angegriffen und dort, wo sie beseitigt wurde, ist nicht länger die Polizei, sondern das Militär dazu beauftragt einzuschreiten, um die Bedingungen für das Tätigwerden der Polizei wiederherzustellen. Diese klare Aufgabentrennung ist in der Realität allerdings nicht einfach zu erkennen. In zwischenstaatlichen Konflikten ist die Trennung klarer, bei Konflikten, deren Akteure nur teilweise staatlich sind, ist die Unterscheidung eher unklar. In diesen sogenannten neuen Konflikten kommt es zum Einsatz einer zentralistischen top-down Organisation in bottom-up Konflikten.²⁵⁰ Polizei und Militär stellen dabei zwei polare Typen von Organisationen des staatlichen Gewaltmonopols dar, im Sinne dessen, dass der eine Wachkörper innere Aufgaben und der andere Wachkörper äußere Aufgaben wahrzunehmen hat.

Gemeinsam sind ihnen die Bewaffnung und die Uniformierung. Organisatorisch sind sie jedoch gänzlich verschieden. Polizeikräfte dienen dem Erhalt eines staatlichen Ordnungsrahmens und verhelfen dem Recht zur Durchsetzung. Sie dienen der „[...] Bekämpfung der intrasozialen Mikroviolenz.“²⁵¹ Dabei bedienen sich Polizeikräfte der Mittel der soft power. Die Polizei ist ohne Feindbild (Unparteilichkeit ist elementare Voraussetzung), handelt reaktiv gegen Verletzungen der Gemeinschaftsordnung durch Mitglieder der Gemeinschaft und ist relativ umweltoffen.²⁵² Sie ist dezentral mit flacher Hierarchie organisiert. Es handelt sich um eine „[...] polyzentrische bottom-up Organisation.“²⁵³

Anders das Militär, welches „[...] auf die Androhung und Anwendung kollektiver Gewalt gegen fremde Streitkräfte bzw. eine fremde Sozialordnung [...]“²⁵⁴ ausgerichtet ist. Es dient der Bekämpfung der „[...] extrasozialen Makroviolenz [...]“²⁵⁵, es ist darauf ausgerichtet den staatlichen Ordnungsrahmen des Gegners zu zerstören und den eigenen wiederherzustellen. Dazu bedient es sich der hard power. Die Anwendung von Gewalt gegenüber Fremdgruppen basiert auf einem klaren Feindbild. Das Militär verfügt über eine zentralistische, stark hierarchische Organisationsform.²⁵⁶

Dazu leben Angehörige von Militärorganisationen zumeist abgeschieden von der zivilen Welt, es herrscht ein hoher Grad an Innenorientierung. Gewaltanwendung und Tötung eines Gegners sind legitimiert, wobei vom Soldaten gefordert wird zu Gunsten der Gemeinschaft

²⁵⁰ Vgl. Haltiner, Karl: Vom Landesverteidiger zum militärischen Ordnungshüter. In: Gareis, Sven; Klein, Paul (Hrsg.): Handbuch Militär und Sozialwissenschaft, 1. Aufl., Wiesbaden 2004, S. 480f.

²⁵¹ Ebd., S. 478.

²⁵² Vgl. ebd., S. 478.

²⁵³ Ebd., S. 479.

²⁵⁴ Ebd., S. 479.

²⁵⁵ Ebd., S. 479.

²⁵⁶ Vgl. ebd., S. 478.

auch von seinem Leben abzusehen.²⁵⁷ Ein weiterer Unterschied zur Polizei liegt in einer ausgeprägten Spezialisierung von Soldaten. Dies hat seine Ursache in der hohen Arbeitsteiligkeit der Streitkräfte. Es handelt sich um eine zentralistische top-down Organisation.²⁵⁸

Wesentlich ist für den staatlichen Akteur im Krieg seine Legitimation durch das Gemeinwesen, für welches er in den Kampf zieht. Hinzu kommt sein Zweck, die eigentliche Aufgabe des Staatsorgans. Die Funktion des Staates, für Frieden und Sicherheit nach innen und außen zu sorgen, wird durch diesen wahrgenommen.²⁵⁹ Es geht um die Ordnung, auf deren Recht die Legitimation der Akteure beruht.

Der Staat ist mit seinen Organen, welche die Staatsgewalt ausüben, die letzte Instanz, die in der Lage ist, Konflikte innerhalb der Gesellschaft, aber auch nach außen gegenüber anderen Gemeinwesen zu regeln.²⁶⁰ Er bedient sich der Androhung oder Anwendung von Zwangsmaßnahmen, welche aber alle durch das Recht begründet sind.²⁶¹ Für das Militär steht im Mittelpunkt, die Ordnung des Gemeinwesens zu verteidigen oder wieder herzustellen oder eine feindliche Ordnung zu zerstören. Für die Polizei steht die Einhaltung und Erhaltung der Ordnung im Fokus.

Die staatlichen Akteure handeln nicht nach eigenem Gutdünken, sondern im Auftrag des Gemeinwesens. Sie treffen keine selbstständige Entscheidung zum Handeln, wie es internationale oder etwa die nichtstaatlichen Akteure tun. Sie setzen die vom Gemeinwesen getroffenen Entscheidungen um. Diese Entscheidungsgebundenheit tritt zur Intention hinzu. Diese Intention kann bei nichtstaatlichen Akteuren ähnlich geartet sein, jedoch fehlt ihnen die rechtliche Basis im Gemeinwesen. Diese Akteure treffen die Entscheidungen, die zu ihrem Handeln führen, im Gegensatz zu den staatlichen Akteuren, selbst. Dies sind auch die wesentlichen Unterschiede zwischen den staatlichen und nichtstaatlichen Akteuren, die nun einer genaueren Betrachtung unterzogen werden.

5.2.3 Die nichtstaatlichen Akteure

Für Kriege braucht es keine Staaten mehr, es können zunehmend Akteure ausgemacht werden, welche keinen staatlichen Körper haben. Die Staaten stehen vor der Herausforderung, kein entsprechendes Gegenüber in einem Konflikt vor sich zu haben.²⁶² Für das Völkerrecht ist dies ein Problem, da die Charta der Vereinten Nationen von Nationalstaaten als Akteure in den internationalen Beziehungen ausgeht. Damit verbunden ist fraglich, ob die neuen Akteure die völkerrechtliche Ordnung akzeptieren.

Im Wesentlichen kann man drei Gruppen von nichtstaatlichen Akteuren ausmachen, welche sich an kriegerischen Auseinandersetzungen

²⁵⁷ Vgl. ebd., S. 480.

²⁵⁸ Vgl. ebd., S. 480.

²⁵⁹ Vgl. Benz, 2008, S. 129.

²⁶⁰ Vgl. ebd., S. 131.

²⁶¹ Vgl. ebd., S. 131.

²⁶² Vgl. Freudenberg, 2008, S. 38.

beteiligen können.²⁶³ Dies sind zum einen die Gruppe der Aufständischen und Rebellen²⁶⁴, die gegen einen staatlich legitimierten Gegner kämpfen, um das alte Ordnungssystem zu erhalten oder ein neues einzusetzen. Dann gibt es die Gruppe der Terroristen, welche durch asymmetrische Kampfführung die bestehende Ordnung, in ihrem Sinn, zu beseitigen trachten. Die letzte Gruppe stellen Kriminelle dar, die vor allem in Banden organisiert bestrebt sind, auch durch physischen Gewalteinsatz, eine bestehende, aber schwache Ordnung aufrecht zu erhalten²⁶⁵, um, einem Parasiten ähnlich, in dieser maximalen Gewinn durch unrechtmäßige Bereicherung zu erzielen.

Während man bei den beiden ersteren, den Insurgenten und den Terroristen, von Krieg sprechen kann, sofern die Intention als politische zu verstehen ist, handeln letztere rein kriminell im Rahmen des Verbrechens. Die Söldner bilden hier die Ausnahme, weil sie zum Zwecke der Bereicherung am Krieg teilnehmen. Sie sind also von der Intention her Verbrecher, unterstützen aber die Kriegsparteien in ihrem Kampf gegeneinander. Diese können sowohl reguläre als auch irreguläre Parteien sein.

Auf Grund dieser Charakteristik sind sie zwischen staatlichen und nichtstaatlichen Akteuren am Übergang zum Kriminellen einzuordnen. Sie sind Irreguläre mit verbrecherischem Zweck, die anders als der Kriminelle den Krieg als Lebensgrundlage brauchen. Dem Verbrecher ist eine staatliche Ordnung zur Gewährleistung seiner Sicherheit besonders wichtig, je besser es dem Wirt geht, umso besser geht es auch seinem Parasiten. Der Söldner ist nicht unbedingt daran interessiert eine Ordnung im Sinne einer Staatlichkeit zu erhalten, ihm genügen die Notordnungen des Krieges, um Profit zu machen, hier liegt die feine Unterscheidung zum Kriminellen an und für sich.

Der reine Verbrecher kann im Frieden genauso wirken wie in einem Krieg. Obwohl Verbrecherbanden keine Streitkraft im Zuge eines Krieges darstellen, können diese also auch in einem Krieg agieren. Dies macht es auch notwendig Polizeikräfte in einem Krieg, für ihre Aufgabe zur Aufrechterhaltung der Ruhe und Ordnung im Inneren, dort wo keine Kampfhandlungen stattfinden, vorzuhalten. Stark abhängig ist deren Einsatz allerdings von der Intensität des Konfliktes.

In Abgrenzung zu den legitimierten Streitkräften, den regulären Kräften, spricht man bei den Aufständischen, Rebellen und Terroristen, aber auch bei Kriminellen, die sich am Kampfgeschehen beteiligen, von Irregulären.

²⁶³ Vgl. Feichtinger, Walter: Differenzierung von Asymmetrie im Kontext bewaffneter Konflikte. In: Schröfl, Josef; Pankratz, Thomas (Hrsg.): Asymmetrische Kriegführung. Ein neues Phänomen der internationalen Politik?, 1. Aufl., Baden-Baden 2004, S. 117.

²⁶⁴ Anm. d. Verf.: Diese beiden Gruppen von nichtstaatlichen Akteuren werden in den Militärwissenschaften auch als Partisanen und Guerilla bezeichnet. Dabei richtet sich der Partisan gegen eine Besatzungsmacht, also fremde Streitkräfte auf eigenem Staatsgebiet, und der Guerilla richtet sein Handeln gegen die eigene Staatsmacht, wobei die Kampfweisen der beiden einander gleichen.

²⁶⁵ Anm. d. Verf.: Dies kann auch eine Kriegsordnung, also keine staatliche Ordnung im eigentlichen Sinn sein.

„Der Kampf von Irregulären gegen staatliche Akteure in Uniform ist so alt wie die Versuche, zentralistische Herrschaft zu errichten, und so alt wie die Geschichte selbst.“²⁶⁶

Bei Platon sind irreguläre Kräfte explizit nicht genannt. Außer dem Söldner, welcher von ihm nicht als irregulär gefasst wird, lassen sich nur Hinweise auf irreguläre Kräfte in Verbindung mit der Entzweiung finden.

„Von demjenigen Staate nämlich, in welchem die Besseren der Menge und den Schlechteren überlegen sind, kann man füglich sagen, daß er stärker ist als er selbst, und mit vollem Rechte verdient er, solches Sieges wegen gepriesen zu werden; im umgekehrten Falle aber umgekehrt.“²⁶⁷

Es handelt sich bei den Besseren und den Schlechteren um nichtstaatliche Akteure im Staat, von denen je nach Herrschaftsform, einer „legitimiert“ (Hervorhebung durch den Verfasser.), der andere nicht legitimiert ist. Und aus Ungerechtigkeit heraus geraten beide im Kampf aneinander. Bei Machiavelli ist die Verschwörung durch irreguläre Kräfte geführt. Diese Verschwörungen sind Maßnahmen gegen einen Herrscher, um ein politisches System auszutauschen. Dieses war in der Antike, aber auch in der Zeit Machiavellis, viel stärker an die Person des Herrschers gebunden als heute und so reichte es vielfach einfach den Herrscher zu beseitigen. Die Verschwörung ist also eine Form des Aufruhrs, eines Befreiungskrieges innerhalb eines Gemeinwesens. Im „Fürst“ schildert Machiavelli die Ursachen für die Verschwörung am Beispiel des Commodus:

„Doch kommen wir zu Commodus, für den es sehr leicht war, seine Herrschaft zu behaupten, da er sie rechtmäßig als Sohn des Marcus ererbt hatte. Er brauchte nur in die Fußstapfen seines Vaters zu treten, und Soldaten und Volk wären zufrieden gewesen. Aber da er grausam und unmenschlich war, ging er, um seine Raubgier am Volk auslassen zu können, dazu über, das Heer zu gewinnen und dessen Zügellosigkeit zu fördern. Da er andererseits seine Würde nicht wahrte und oft in die Arena hinabstieg, um mit den Gladiatoren zu kämpfen, und andere gemeine, der kaiserlichen Majestät wenig würdige Dinge tat, machte er sich in den Augen der Soldaten verächtlich. Von der einen Seite gehaßt, von der anderen verachtet, wurde er anläßlich einer Verschwörung ermordet.“²⁶⁸

Es geht hier allerdings nicht hervor, wer ihn nun getötet hat. Da er als Herrscher quasi den Staat repräsentierte, muss davon ausgegangen werden, dass es sich um irreguläre Kräfte handelte. Auslöser, für die Bildung irregulärer Bewegungen gegen die Staatsgewalt, stellen dabei ungerechte Zustände dar. Dazu führt Machiavelli Folgendes aus:

²⁶⁶ Freudenberg, 2008, S. 21.

²⁶⁷ Platon, Nomoi, S. 158.

²⁶⁸ Machiavelli, Der Fürst, S. 84.

„Verhaßt macht er sich vor allem, wenn er, wie ich schon sagte, raubgierig ist und sich am Vermögen und an den Frauen seiner Untertanen vergreift.“²⁶⁹

Demnach hat der Herrscher grundsätzlich zwei Bedrohungen zu fürchten, zum einen Gefahren von innen, durch die Bürger des Staates, dies vor allem, wenn er ein ungerechter Herrscher ist, zum anderen Bedrohungen von außen, von anderen Herrschern.²⁷⁰ Da es für nichtstaatliche Akteure nur schwer möglich ist, einen offenen Krieg mit der Staatsgewalt auszufechten, bleibt nur die Möglichkeit mit irregulären Methoden gegen die Obrigkeit vorzugehen.

„Nur wenige sind in der Lage, einen offenen Krieg mit einem Machthaber zu führen; sich gegen ihn verschwören aber kann jeder.“²⁷¹

Machiavelli sieht diese Art der Änderung des politischen Systems, der Ordnung, als letzten Ausweg in der Not, nicht als alltägliches Mittel, um Politik zu betreiben. Er warnt vor den Gefahren, die eine Verschwörung mit sich bringt und verweist darauf sich mit der gegebenen Ordnung abzufinden.²⁷² Wenn der Machthaber oder die Regierung aber gerecht handeln und Vernunft walten lassen, ist die Gefahr gering für eine Verschwörung. Die Not als Auslöser für den Aufstand jedoch bezeichnet er, Titus Livius zitierend, als die letzte und stärkste Waffe.²⁷³

Grotius geht davon aus, dass die Erhebung von irregulären Kräften gegen den Staat zu Lasten der inneren Sicherheit durchgeführt wird. Daher sieht er nur eine Rechtfertigung für Irreguläre sich gegen den Herrscher zu erheben, wenn dieser gegen die Gerechtigkeit verstößt und sich als Gesetzgeber in das Recht der anderen Elemente der Staatsgewalt, der Exekutive und der Rechtsprechung, einmischt.²⁷⁴ Unter Einmischung ist dabei die Beeinflussung zu Gunsten des Herrschers und nicht zu Gunsten des Gemeinwohles gemeint. Für Grotius ist das höchste Gut die innere Ruhe und Ordnung. Er führt aus, dass

„[...] wir in der Regel dieses Gut durch die Staatseinrichtungen erlangen; [...]“, denn „[...] das Glück der Herrscher besteht aber in dem Glücke ihrer Untergebenen.“²⁷⁵

Dabei können die Gesetze es nie allen recht machen, dennoch ist es besser einigen wenigen Unrecht zu tun als allen die Willkür einzuräumen.²⁷⁶ Sofern also grundsätzlich die Gesetze der Mehrheit und in der Hauptsache gerecht sind, ist ein Aufbegehren gegen die Staatsgewalt nach Grotius

²⁶⁹ Ebd., S. 75.

²⁷⁰ Vgl. ebd., S. 75.

²⁷¹ Machiavelli, Discorsi, S. 285.

²⁷² Vgl. ebd., S. 286.

²⁷³ Vgl. ebd., S. 326.

²⁷⁴ Vgl. Linares, Filadelfo: Einblicke in Hugo Grotius' Werk, Vom Recht des Krieges und des Friedens, Hildesheim, New York 1993, S. 73.

²⁷⁵ Kirchmann, 1869, S. 188.

²⁷⁶ Vgl. ebd., S. 189.

unzulässig und das Handeln von Irregulären verboten. Spinoza, als Zeitgenosse Grotius, sieht die Ursachen für die Entstehung irregulärer Kräfte in Dingen, welche der menschlichen Natur zuwiderlaufen und somit nicht Inhalt des Rechts des Gemeinwesens sein können. Es handelt sich um Vergehen seitens der Obrigkeit, welche einen staatlichen Zustand ausschließen und zu einem Zustand latenter Feindseligkeit werden.²⁷⁷ Die Regierungsführung ist somit verantwortlich für die Entstehung von irregulären Bewegungen.

„Denn sicherlich sind Aufruhr, Kriege und Mißachtung oder Verletzung von Gesetzen nicht so sehr der Bosheit der Untertanen wie der schlechten Regierungsform eines Staates anzulasten.“²⁷⁸

Die Ursache für die Bildung von irregulären Bewegungen liegt also in der Wahrnehmung der Menschen. Wenn ihnen Rechte auf Dauer genommen werden oder wenn sie unterdrückt werden, ihre Freiheit nicht mehr gegeben ist, kann eine solche Bewegung entstehen.²⁷⁹ Dabei handeln immer mehr nichtstaatliche Akteure mit militärischen Mitteln. Sie treten auch auf Seiten von regulären Streitkräften auf und können diese unterstützen. Dies ist zum Beispiel der Fall, wenn reguläre Verbände sich mit Aufständischen gegen einen feindlichen Besatzer zur Wehr setzen. Dies ist letztlich auch das, was Clausewitz unter der Volksbewaffnung versteht. Die Anwendung irregulärer Kampfweisen gegen einen Aggressor auf Seiten der eigenen regulären Streitkräfte.

„Die Anwendung des Landsturms und bewaffneter Volkshaufen kann und soll nicht gegen die feindliche Hauptmacht, auch nicht gegen beträchtliche Korps gerichtet sein; sie soll nicht den Kern zermalmen, sondern nur an der Oberfläche, an den Umgrenzungen nagen [...]“²⁸⁰

Der Kampf von Aufständischen, auf Seiten von regulären Verbänden gegen einen solchen Besatzer, gibt den Irregulären eine gewisse Legitimation. Anders verhält es sich bei Terroristen und Rebellen gegen die eigene Staatsgewalt. Im innerstaatlichen Konflikt kommen auf Seiten der Irregulären Kampfweisen zum Einsatz, mit denen die regulären Streitkräfte in der Regel nicht zurechtkommen. Dies macht diese Gruppierungen zu ernsthaften Gegnern des Staates. Dieser ist bemüht den Zustand des Ordnungssystems zu erhalten, während die Irregulären diesen zu ihren Gunsten verändern möchten.

Obwohl die regulären Streitkräfte in der Regel eine „[...] führungs- und kräftemäßige sowie waffentechnische Überlegenheit [...]“²⁸¹ haben, können die Irregulären durch Nichtbefolgung von Regeln und Verfahren diesen Vorteil der Staatsorgane abschwächen. Die Irregulären sind nicht an nationale und internationale Normen gebunden, sie können autonom entscheiden.²⁸² Letztlich sind sie aber bemüht ihre Irregularität gegen eine

²⁷⁷ Vgl. Spinoza, Politischer Traktat, S. 33.

²⁷⁸ Ebd., S. 35.

²⁷⁹ Vgl. Freudenberg, 2008, S. 23.

²⁸⁰ Clausewitz, Vom Kriege, S. 173.

²⁸¹ Feichtinger, 2004, S. 119. (in: Schröfl/Pankratz, 2004)

²⁸² Vgl. ebd., S. 120.

gewisse Staatlichkeit zu tauschen. Denn letztlich sind, außer den Kriminellen, alle irregulären Kräfte bemüht, ihre Ordnung, die sie einsetzen wollen, auch anerkannt zu bekommen, dies ist ihr Letztzweck.

Neben den Ursachen für die Entstehung von irregulären Gruppierungen in einem Gemeinwesen und deren Interaktionsmöglichkeiten mit den regulären Kräften im Gemeinwesen – sowohl mit als auch gegen sie – ist ein weiterer Faktor in diesem Zusammenhang von Bedeutung. Im Kampf gegen einen Besatzer ist der Gegner der Irregulären das feindliche Militär. Gegenüber Aufständischen, gegen die eigene Staatsgewalt, und Terroristen – wobei hier die Grenzen stark verschwimmen – ist die Polizei meist der Hauptakteur. Das polizeiliche Vorgehen gegen Rebellen oder Terroristen im nicht-internationalen bewaffneten Konflikt ist stark abhängig von der Intensität dieses Konfliktes. Vielfach agieren solche irregulären Gruppierungen auch über die Staatsgrenzen hinweg und nehmen dadurch den Charakter eines transnationalen Akteurs an.²⁸³

Die Intensität und ein unklares Bild über die Intention der Irregulären können auch bei der Ausübung der Staatsgewalt zu unklaren Kompetenzaufteilungen führen. Viele der Akteure sind daran interessiert aus einem Konflikt Geld zu erwirtschaften und halten diesen daher am Leben.²⁸⁴ Hier hilft neben der Identifikation der Intention von Irregulären, sei es mit politischem oder kriminellem Hintergrund, eben auch die Intensität des Kampfes, den sie führen. Als Beispiel sei hier der Drogenkrieg in Mexiko genannt, der auf Grund der Ausmaße und der Intensität, die er angenommen hat, durch die Polizei nicht mehr bewältigbar ist; hier ist trotz des kriminellen Zwecks, den die Akteure verfolgen, der Einsatz des Militärs angezeigt und notwendig geworden.

Generell ist die Trennung von Militäreinsatz und Kriminalitätsbekämpfung durch den Einsatz des Militärs im Inneren und von Polizeikräften im Auslandseinsatz längst aufgehoben. Vor allem sind terroristische Gruppierungen schwer als Kriminelle zu identifizieren, da sie sich in ihrem Erscheinungsbild vielfach an militärische Strukturen anlehnen.²⁸⁵ Zudem ist deren Zweck ein politischer und nicht der der Bereicherung. Oft benutzt ein Gemeinwesen die polizeilichen Kräfte gegen solche Irregulären, um ihnen nicht den Status eines Kriegsgegners zu gewähren und sie damit nicht quasi zu legitimieren.

Bei einem zwischenstaatlichen Konflikt, in dem sich die militärischen Streitkräfte beider Seiten im Kampf gegenüberstehen, ist das Militär aber auch nicht der einzige Akteur zur Verfolgung eines politischen Zweckes, vielmehr ist es nur eines von vielen Instrumenten der Politik. Vor allem die steigende Komplexität und Vernetzung aller Politikbereiche begründet ein umfassendes Vorgehen im Falle eines Konfliktes, sowohl bei zwischen- als auch innerstaatlichen Konflikten. Dies bedeutet, beim Kampf gegen Irreguläre ist das Militär umso mehr nur ein Teilaspekt eines umfassenden gesamtstaatlichen Ansatzes. Politisch wird der Erfolg nicht ausschließlich am

²⁸³ Vgl. Freudenberg, 2008, S. 81.

²⁸⁴ Vgl. ebd., S. 139.

²⁸⁵ Vgl. ebd., S.27f.

Gefechtsfeld errungen, das Militär stellt vielmehr die ultima ratio dar, um durch Ausübung unmittelbaren Zwanges zur Wiederherstellung einer grundlegenden rechtlichen Ordnung zu gelangen.²⁸⁶

Zu den nichtstaatlichen Akteuren sind die irregulären Gruppierungen, bedingt die Söldner und als Sonderform die privaten Militärdienstleister, die heute wieder vermehrt in Erscheinung treten, zu rechnen.²⁸⁷ Der Unterschied zu den staatlichen Akteuren liegt darin begründet, dass staatliche Akteure auf Grundlage der Gesetze des Gemeinwesens handeln. Diese Legitimation fehlt den nichtstaatlichen Akteuren grundsätzlich. Die meisten handeln auf Grundlage einer Ungerechtigkeit, einer Situation des verlorenen oder nicht zugestandenen Rechts, in Augen der jeweiligen Akteure. Neben der Intention dieser Akteure ist auch die Intensität mit der sie vorgehen ein Gradmesser dafür, in welchen Kompetenzbereich sie hineinwirken.

Ob das Militär oder die Polizei zum Hauptakteur gegen diese Gruppierungen wird, hängt aber auch von der jeweiligen politischen Intention des Gemeinwesens, des Staates, ab, dieses entscheidet auch darüber ob der Konflikt letztlich als Krieg aufgefasst wird. Hier spielt die Anerkennung von Aufständischen als Kriegspartei eine Rolle. Dies kann indirekt durch den Einsatz des Militärs erfolgen, welcher darauf schließen lässt, dass der irreguläre Gegner gewissermaßen anerkannt wird. Aber es können Aufständische auch durch eine formale Anerkennung zur Einhaltung völkerrechtlicher Normen angehalten werden.²⁸⁸ Dadurch wird der Aufstand oder Bürgerkrieg zu einem „[...] Krieg des Völkerrechts [...]“²⁸⁹ und hebt den Konflikt rechtlich auf eine internationale Ebene.

Ungeachtet dieser Anerkennung von Aufständischen und der damit verbundenen rechtlichen Implikationen, ist das gewaltvolle Vorgehen von nichtstaatlichen Akteuren, zur Verwirklichung eines politischen Zwecks, als Krieg zu betrachten. Neben staatlichen und nichtstaatlichen Akteuren gibt es noch internationale und auch transnationale Akteure. Diese sollen nun einer genaueren Betrachtung unterzogen werden.

5.2.4 Die internationalen und transnationalen Akteure

Neben den Staaten als eigentliche internationale Akteure und ihren bewaffneten Trägern der Staatsgewalt, den staatlichen Akteuren als deren Instrumente, zählen zu diesen vor allem Akteure, die Gemeinwesen übergreifend oder aber von Gemeinwesen unabhängig, agieren. Diesen Akteuren kommt, in der Zeit der Globalisierung und Entgrenzung im Zuge einer steigenden Vernetzung, immer größere Bedeutung zu.²⁹⁰ Zu den transnationalen Akteuren sind vor allem global agierende Unternehmen zu

²⁸⁶ Vgl. ebd., S. 45.

²⁸⁷ Vgl. ebd., S. 92f.

²⁸⁸ Vgl. Heydte, Friedrich August Freiherr von: Völkerrecht, Verlag für Politik und Wirtschaft, Köln, 1958, S. 195.

²⁸⁹ Ebd., S. 195.

²⁹⁰ Vgl. Freudenberg, 2008, S. 82.

zählen,²⁹¹ die vielfach einen bestimmenden Faktor in und um Konflikte darstellen.

Des Weiteren gehören zu den transnationalen Akteuren etwa Nicht-Regierungs-Organisationen (NGO) oder die Exekutiven von internationalen Organisationen (z.B.: das Generalsekretariat der Vereinten Nationen), die ihr Personal zwar aus den diversen Mitgliedsstaaten rekrutieren, die dann aber ihr Handeln von staatlichen Einflüssen abgekoppelt ausführen.²⁹² Sie haben in bewaffneten Konflikten, für die unmittelbaren Kriegshandlungen, keine direkte Relevanz und seien hier vollständigkeithalber erwähnt. Die internationalen Akteure, welche Gemeinwesen übergreifend agieren, sind weithin als Koalitionen, Allianzen oder aber als internationale Organisationen, welche unterschiedliche Beweggründe anführen können, aus denen sich ihre Mitglieder zusammenschließen, bekannt.

Beispielhaft werden hier die North Atlantic Treaty Organisation (NATO), die Europäische Union (EU) und die Vereinten Nationen (VN) hinsichtlich der Zielsetzungen kurz dargestellt. Es gibt neben diesen Organisationen, die im Wesentlichen den Aspekt des Friedens und der Sicherheit im Fokus haben, auch Gruppierungen oder Gebilde, welche eher wirtschaftliche Aspekte in ihren Mittelpunkt rücken. Dazu gehören auf jeden Fall transnational agierende Wirtschaftsunternehmen, deren Interessen an Gewinnmaximierung ausgerichtet sind und die einen wesentlichen Machtfaktor im globalen Gefüge darstellen. Diese Unternehmen sind jedoch nicht direkter Akteur in Kriegen, obwohl sie diese manchmal begünstigen oder durch indirekte Einwirkung hervorrufen. Deshalb wird hier nur auf die Akteure, die auch direkt Anteil an Kriegen haben, eingegangen.

Anders als ein Gemeinwesen ist das Bündnis zwischen Gemeinwesen fragiler. Vor allem erzwungene Bündnisse basieren auf Furcht und sind nicht von beiden Seiten aus freien Stücken gewählt worden.²⁹³ Aus demselben Grund wie Konflikte entstehen, entstehen auch Bündnisse. Es geht um Sicherheit, die mit mehr Macht durch Zusammenschluss mehrerer Gemeinwesen besser zu realisieren ist.

„Die Feindschaft kommt aus dem Widerstreit der Interessen, die Freundschaft aus ihrer Gemeinsamkeit.“²⁹⁴

Dabei zielt alles Handeln der Gemeinwesen auf deren Gemeinwohl ab. Das Besondere am Verhältnis zwischen Staaten ist, dass sie den Frieden aus eigenem Interesse suchen und nicht, weil sie unter einem gemeinsamen Recht stehen. Machiavelli beschreibt in den Discorsi einen Staatenbund, der auf gegenseitigem Nutzen aufgebaut ist und bei dem alle Partner gleiche Rechte und Pflichten haben und somit einer überstaatlichen Gerechtigkeit unterliegen. Diese Form eines Bündnisses entspricht dem, was heute in der EU verwirklicht wird. Daneben sieht er noch ein Hegemonialsystem und eine

²⁹¹ Vgl. ebd., S. 101.

²⁹² Vgl. Benz, 2008, S. 286.

²⁹³ Vgl. Machiavelli, Discorsi, S. 154.

²⁹⁴ Pesendorfer, 1982, S. 98. (in: Neisser, 1982)

Herrschaft über untergeordnete Staaten.²⁹⁵ Bündnisse mit anderen Gemeinwesen werden dann gebrochen, wenn es um existenzielle Fragen oder um Angelegenheiten der Nützlichkeit geht. Machiavelli beschreibt dies wie folgt:

„Wo ein Staat für seine Existenz fürchtet, wird man nie Treue finden.“²⁹⁶

und weiter:

„Bündnisse werden ferner aus Nützlichkeitsgründen gebrochen; [...]“²⁹⁷

Bündnisse sind daher keine an das Recht gebundenen Gebilde, sie orientieren sich am Willen der Bündnispartner. Der Vertrag zwischen ihnen ist lediglich der formale Rahmen, welcher, wenn es zu existenziellen Fragen kommt, auch wieder einseitig gelöst werden kann. Dazu führt Spinoza Folgendes aus:

„Folglich gehört das Recht, Krieg zu führen, zum Recht eines jeden isolierten Gemeinwesens, das Recht, Frieden zu beschließen, aber nicht zu dem von bloß einem, sondern von wenigstens zwei Gemeinwesen, die deshalb Alliierte heißen.“²⁹⁸

Und diese Allianz besteht nur solange ein Grund dafür vorhanden ist. Spinoza nennt hier die Furcht vor Schaden und die Hoffnung auf Profit.²⁹⁹ Profit zielt hier auf das Gemeinwohl des jeweiligen Gemeinwesens ab, nicht auf Gewinnmaximierung. Seiner Ansicht nach kann bei Wegfall eines dieser Gründe das Bündnis auch einseitig gelöst werden. Daraus lässt sich schließen, dass ein Gemeinwesen sich so zu gestalten hat, um auch ohne Bündnis seine Ordnung nach innen und außen aufrecht zu erhalten.

Entgegen dieser Folgerung kommt heute eine Strategie zur Anwendung, die Abhängigkeiten schafft, welche den Zwang zum Bündnis bewirken. Gerade beim Militär ist zum Beispiel im Rahmen der EU zu beobachten, dass die nationalen Streitkräfte immer kleiner werden, zum Teil Fähigkeiten abbauen, und somit ein alleiniger Einsatz einer nationalen Streitkraft bei robusten Krisen unmöglich scheint. Diese Abhängigkeiten gibt Bündnissen eine gewisse Haltbarkeit. Abgesehen von diesen Abhängigkeiten und den daraus resultierenden Bedrohungen, verfolgen alle Bündnisse eine ähnliche Zielsetzung. Im Gründungsvertrag der NATO findet sich einleitend der Zweck des Bündnisses:

„They are determined to safeguard the freedom, common heritage and civilisation of their peoples, founded on the principles of democracy,

²⁹⁵ Vgl. Machiavelli, Discorsi, S. 176ff.

²⁹⁶ Ebd., S. 154.

²⁹⁷ Ebd., S. 155.

²⁹⁸ Spinoza, Politischer Traktat, S. 28.

²⁹⁹ Vgl. ebd., S. 28.

individual liberty and the rule of law. They seek to promote stability and well-being in the North Atlantic area.“³⁰⁰

Sicherheit und Wohlstand sind die wesentlichen Grundlagen für dieses Bündnis, welches, als internationaler Akteur, wesentlich am Kampf gegen die Bedrohungen dieser Werte, zum Beispiel durch den internationalen Terrorismus, beteiligt ist. Zum anderen wird das Bündnis dazu genutzt, Stabilität in Randregionen des Bündnisgebietes zu bringen. Die NATO ist also ein wesentlicher Stabilisator des Bündnisraumes. Sie trifft politische Entscheidungen und hat durch ihre Bündnismitglieder auch das militärische Instrument zur Umsetzung von Entscheidungen verfügbar.

Grundsätzlich ist die NATO defensiv ausgerichtet und bietet ihren Mitgliedern die Möglichkeit zur gegenseitigen Unterstützung im Falle, dass sie angegriffen werden. Die NATO wurde als Verteidigungsbündnis gegen die Sowjetunion aufgestellt und hat sich nach deren Zerfall als einer der bedeutendsten internationalen Akteure positioniert. Die EU wurde als Wirtschaftsgemeinschaft gegründet und entwickelt sich zunehmend in die Richtung der NATO, nicht im militärischen, aber im politischen Sinn verstanden. Die Zielsetzungen der EU finden sich im Vertrag über die Europäische Union. Dazu findet sich in Artikel 3 Folgendes:

„(1) Ziel der Union ist es, den Frieden, ihre Werte und das Wohlergehen ihrer Völker zu fördern.“³⁰¹

Es lässt sich hier eine ähnliche Zielsetzung wie bei der NATO erkennen. Tatsächlich betreibt die EU eine ähnliche Strategie mit der Aufnahme von Staaten in die Union. Dies soll der Stabilisierung und dem Frieden in Europa dienen. Die EU geht sogar einen Schritt weiter als die NATO, indem sie nicht nur militärischen Beistand (die Mehrheit der EU-Staaten sind auch NATO-Mitglieder) bietet, sondern die Mitglieder auch in wirtschaftlichen Belangen unterstützt.

Es ist hier also eine doppelte Stabilisierungsfunktion gegeben. Wie bereits gezeigt, wird die Stabilität des Bündnisses dadurch erhöht, dass gegenseitige Abhängigkeiten geschaffen werden, die es einem einzelnen Mitglied nicht mehr ermöglichen Bedrohungen alleine zu bewältigen. Diese Vernetzung ist im Sinne von Spinoza also die Aufrechterhaltung von Furcht und Bedrohung, indem man durch die Abhängigkeiten diese erst entstehen lässt. Diese Abhängigkeiten sind allerdings noch keine Garantie dafür, dass diese Verträge auch eingehalten werden.

Bündnisse sind ein Mittel die eigene Macht zu vervielfältigen, Sicherheit zu gewährleisten und das Allgemeinwohl der Bündnispartner zu stärken. Sie basieren aber nicht auf einer Rechtsverbindlichkeit, sondern vielmehr auf gegenseitigem Vertrauen. Dass letztlich der Vertrag erfüllt wird,

³⁰⁰ The North Atlantic Treaty, 1949, S. 3. (in: NATO, Towards the new Strategic Concept, 2010)

³⁰¹ Schwartmann, Rolf: Der Vertrag von Lissabon. EU-Vertrag, Vertrag über die Arbeitsweise der EU - konsolidierte Fassungen, 3., überarb. und erw. Aufl., Stand: 1. Dezember 2009. Aufl., Heidelberg; München; Landsberg [u.a.] 2010, S. 4.

kann allerdings, vor allem bei existenziellen Situationen, für einzelne Mitglieder nicht garantiert werden.³⁰² Bündnisse haben als internationale Akteure nach außen das Ziel, die Stärke der einzelnen Mitglieder zu erhöhen und damit für Frieden und Stabilität zu sorgen. Es wird dadurch schon im Vorfeld eines möglichen Konfliktes durch die potentielle Macht des Bündnisses die Eskalation vermindert. Dieser Ansatz wird auch als System Integrativer Sicherheit bezeichnet.

„Ein System Integrativer Sicherheit zielt darauf ab, vermittels einer grundsätzlich vertraglichen Bindung von Staaten eine intensive Vernetzung aller Bereiche politischen Handelns zu erreichen mit dem Ziel, eine dauerhaft friedliche Ordnung innerhalb des Systems herzustellen und auf Grund dieser engen Bindung zueinander auch eine Stärkung insofern zu generieren, als durch das geschlossene gemeinsame Auftreten in seiner Außenwirkung die Bestandsgarantie im Sinne einer Existenzsicherung verstärkt wird.“³⁰³

Dabei darf ein Sicherheitssystem wie dieses nicht als Bündnis verstanden werden, sondern vielmehr als der einem Bündnis zugrundeliegende Ordnungsansatz.³⁰⁴ Bündnisse als internationale Akteure, denen ein solches Sicherheitssystem zu Grunde liegt, zielen darauf ab, Konflikte erst gar nicht entstehen bzw. wenn ein solcher Konflikt vorliegt, diesen nicht eskalieren zu lassen. Die Stärke oder Macht, die sich aus dem Zusammenschluss ergibt, soll Gegner abhalten mit militärischen Mitteln vorzugehen.

Zudem gibt es Bündnisformen, welche temporär für die Erreichung eines bestimmten Zweckes eingerichtet wurden und denen ein Sicherheitssystem als Basis fehlt.³⁰⁵ Diese sogenannten Koalitionen garantieren keine auf Integration oder sonstige Maßnahmen basierende Sicherheit zwischen den Partnern. Nach der Erreichung des festgelegten Zweckes ist eine Feindschaft, auf Grund unterschiedlicher Interessen, möglich. Eine Koalition ist also kein Instrument um den Frieden zu garantieren.

Einen Schritt weiter gehen Bündnisse, die in Form einer Wertegemeinschaft darum bemüht sind, den Frieden aufrecht zu erhalten. Diese Gemeinschaften werden als Allianzen³⁰⁶ bezeichnet und haben schon einen gewissen integrativen Charakter, welcher sich im Zusammenschluss von Gemeinwesen mit einer gemeinsamen Werterhaltung ausdrückt.³⁰⁷ Liegt einer solchen Allianz ein entsprechendes Sicherheitssystem zu Grunde, ist mit großer Wahrscheinlichkeit davon auszugehen, dass zwischen den Mitgliedern keine bewaffneten Konflikte ausbrechen.

Ungeachtet der Form des Bündnisses, sind diese Zusammenschlüsse Akteure in bewaffneten Konflikten internationalen Charakters. Ein

³⁰² Vgl. Stupka, 2011, S. 216ff.

³⁰³ Ebd., S. 123.

³⁰⁴ Vgl. ebd., S. 115.

³⁰⁵ Vgl. ebd., 109f.

³⁰⁶ Anm. d. Verf.: Darunter ist nicht die Allianz im Sinne Spinozas zu verstehen.

³⁰⁷ Vgl. Stupka, Andreas: Strategie denken, Wien 2008, S. 114.

besonderer internationaler Akteur sind die Vereinten Nationen, welche die globale Vermeidung von bewaffneten Konflikten und die Aufrechterhaltung des Friedens zur Zielsetzung haben. In den Satzungen der Vereinten Nationen findet sich folgende Zielsetzung:

„1. den Weltfrieden und die internationale Sicherheit zu wahren und zu diesem Zweck wirksame Kollektivmaßnahmen zu treffen, um Bedrohungen des Friedens zu verhüten und zu beseitigen, Angriffshandlungen und andere Friedensbrüche zu unterdrücken und internationale Streitigkeiten oder Situationen, die zu einem Friedensbruch führen könnten, durch friedliche Mittel nach den Grundsätzen der Gerechtigkeit und des Völkerrechts zu bereinigen oder beizulegen; [...]“³⁰⁸

Diesem Zusammenschluss der Mehrzahl der Staaten der Welt liegt ein System der Kollektiven Sicherheit zu Grunde. Auf Grund der Vielzahl an Gemeinwesen, die Mitglied der Vereinten Nationen sind, und der daraus resultierenden größeren Unsicherheit, dass sich alle an dieses Gewaltverbot halten, hat diese Organisation Kriege bislang nicht gänzlich verhindern können. Dennoch hat die VN mit ihren Organen, hier vor allem dem Sicherheitsrat, eine wesentliche Rolle bei der Durchführung von gewalttätigen Konflikten. Maßnahmen, die bei einem Bruch des Friedens von der Staatengemeinschaft zu ergreifen sind, werden durch den Sicherheitsrat legitimiert.³⁰⁹

Die hier exemplarisch angeführten internationalen Akteure verfolgen also die Aufrechterhaltung des Friedens und der Sicherheit, sei es in bestimmten Regionen oder auf der ganzen Welt. Da sich aber der Krieg nur in Abgrenzung vom Frieden denken lässt und Sicherheit dialektisch der Unsicherheit bedarf, ist die Zielerreichung niemals absolut, sondern immer nur unvollkommen. Auch vernachlässigt diese Forderung, nach einem weltweiten Gewaltverbot, das gestaltende Moment des Krieges.

„Aus der Gegnerschaft der Staaten folgt auch die Anstrengung, sich zu behaupten und weiterzuentwickeln, besser, mächtiger zu werden.“³¹⁰

Trotzdem oder gerade weil Konflikte so eine Wichtigkeit haben, spielen diese Akteure eine bedeutende Rolle bei gewaltvollen Konflikten. Nicht nur, dass Staaten keiner supranationalen Ordnung und keinem übergeordneten Recht unterliegen, so werden zunehmend nichtstaatliche Akteure zu den Trägern von bewaffneten Konflikten und Kriegen. Die hier dargestellten Akteurstypen sind in den meisten bewaffneten Konflikten, international wie auch nicht-international beteiligt. Die Frage, warum trotz vieler Bemühungen Kriege nach wie vor eine so bedeutende Rolle im Dasein der Menschen spielen, warum sie letztendlich entstehen und welche Zielsetzungen sie verfolgen, ist der Inhalt des folgenden Abschnittes.

³⁰⁸ United Nations Regional Information Centre for Western Europe (Hrsg.): Charta der Vereinten Nationen, 2009, Kapitel I, Artikel 1.

³⁰⁹ Vgl. ebd., Kapitel VII, Artikel 42.

³¹⁰ Pesendorfer, 1982, S. 98. (in: Neisser, 1982)

5.3 Zu den Ursachen und dem Zweck von Kriegen

Ursachen und Zweck von Konflikten sind von unterschiedlicher Natur. In der Darstellung dieser beiden Charakteristika des Krieges wird nach Universalien gesucht. Generell kann als Ursache für Konflikte eine Asymmetrie von Anspruch und Realität angenommen werden. Dieses Ungleichgewicht der Erwartung und dem, was wirklich verfügbar ist, gleichgültig worum es sich letztlich handelt, ist die Ursache von Konflikten. Ist dieser Unterschied durch nicht-gewalttätige Auseinandersetzungen nicht zu beseitigen, führt dies zur bewaffneten Austragung des Konfliktes.

Die Ursachen können dabei auf drei Ebenen zurückgeführt werden, die Mikro-, die Meso- und die Makroebene. Ähnlich den Ebenen des Konfliktes können die Ursachen hier auf der individuellen, der personellen Ebene liegen. Es kann sich um Ursachen, welche innergemeinschaftlich zum Tragen kommen, handeln oder der Auslöser ist auf Grund der Beziehungen der Staaten und Gemeinwesen untereinander zu finden. Es wird im Folgenden dargestellt, welche Ursachen auf den Ebenen zu finden sind und was letztlich Zweck eines Krieges ist.

5.3.1 Asymmetrie und Symmetrie als Ursachen des Krieges

Konflikte entstehen dann, wenn es zum Aufeinandertreffen unterschiedlicher Interessen kommt. Es kann in diesem Zusammenhang von einer Asymmetrie der Interessen gesprochen werden. Diese Asymmetrie findet sich auf verschiedenen Ebenen wieder. Es kann hier neben den verschiedenen Ebenen eine Aufteilung der Gründe, nach ihrem Zweck, erfolgen. So sieht Platon die Ursachen für Kriege in existenziellen Fragen. Weil die Gemeinwesen sich ausdehnen und immer mehr Menschen im Staat leben, führt dies zu Konflikten.

„Also werden wir von den Nachbarn Land abschneiden müssen, wenn wir genug haben wollen zur Viehweide und zum Ackerbau, und sie auch wieder von unserem, wenn sie sich auch gehenlassen und die Grenzen des Notwendigen überschreitend nach unangemessenen Besitz streben.“³¹¹

Hier geht es vor allem darum das Gemeinwesen ernähren zu können. Es ist von existenzieller Bedeutung, durch Krieg das eigene Gemeinwesen mit dem Notwendigen zum Überleben auszustatten, aber andererseits auch einen gewissen Wohlstand zu schaffen, um den inneren Frieden zu erhalten. Und da der Nachbar seine Lebensgrundlagen nicht unverteidigt aufgeben kann, kommt es zum Krieg. Geht dieses Bestreben über das bloße Sichern des Überlebens hinaus, tritt ein weiterer Zweck als Kriegsgrund hinzu. Das Erstreben von mehr Macht, um sich vor der Bedrohung durch andere Gemeinwesen zu schützen. Krieg entsteht, aus Machiavellis Sicht, immer aus einem Ungleichgewicht heraus,

³¹¹ Platon, Politeia, S. 265.

„[...] denn da der eine Teil der Menschen mehr haben möchte, und der andere das, was er hat, zu verlieren fürchtet, so kommt es zu Feindseligkeiten und Krieg, [...].“³¹²

Diese Aussage spiegelt die Gründe für Krieg wider, die schon Platon implizit genannt hat. Einerseits geht es um Herrschaft über andere und andererseits darum, dem anderen in diesem Bestreben zuvor zu kommen. Auch innerstaatlich, also in Gemeinwesen, lässt sich dies als Grund für Kriege ausmachen. Münkler etwa beschreibt:

„[...] das Nebeneinander von bitterem Elend und unermesslichem Reichtum ist ein aussagekräftiger Indikator für die Wahrscheinlichkeit, mit der innergesellschaftliche Auseinandersetzungen in offene Bürgerkriege umschlagen.“³¹³

Man führt nach Machiavelli aus folgenden Gründen Krieg,

„[...] erstens um ihn [Anm. d. Verf.: Den Staat.] zu beherrschen und zweitens aus Furcht, von ihm unterjocht zu werden.“³¹⁴,

Es lassen sich hier schon die Gründe ausmachen, die jedem Konflikt zu Grunde liegen, nämlich das Bedürfnis eine Asymmetrie der Macht auszugleichen. Symmetrie der Macht ist daher für Machiavelli die Lösung des Problems. Für ihn besteht die Kunst nun darin, das Staatswesen so stark auszubilden, dass es nicht leicht zu erobern ist, andererseits darf es nicht zu stark sein, um nicht eine Bedrohung darzustellen. Es geht darum diese Symmetrie der Macht, ein Gleichgewicht herzustellen.³¹⁵

„Ist ein Staatswesen schwer zu erobern, weil – [...] – gut für seine Verteidigung gesorgt ist, so wird es selten oder nie vorkommen, dass jemand die Absicht hat, es anzugreifen. Ebenso wenig wird ihm jemand aus Furcht den Krieg erklären, [...], dass es keine ehrgeizigen Absichten verfolgt [...]. Ich bin überzeugt, dass dies das wahre politische Leben und die wahre Ruhe für ein Gemeinwesen wäre, wenn man die Dinge auf diese Weise im Gleichgewicht halten könnte.“³¹⁶

Um Kriege zu verhindern, ist also ein Gleichgewicht, eine Symmetrie anzustreben, welche die Bedrohungen in eine Relation zu den Schutzmaßnahmen setzt. Eine über die Maßen gestützte Sicherheit kann zu einer Bedrohung für andere werden, die bemüht sind diese Asymmetrie durch Krieg auszugleichen. Diese Kriegsgründe sind der zwischenstaatlichen Ebene, der Makroebene zuzuordnen. Da die Staaten unter keinem gemeinsamen Recht stehen, herrscht ein Zustand der Anarchie, in dem Asymmetrien der Macht zu Konflikten führen können.

³¹² Machiavelli, Discorsi, S. 101.

³¹³ Münkler, Herfried: Die neuen Kriege, 4. Aufl., Reinbek bei Hamburg 2010, S. 17.

³¹⁴ Machiavelli, Discorsi, S. 27.

³¹⁵ Vgl. Machiavelli, Der Fürst, S. 49.

³¹⁶ Machiavelli, Discorsi, S. 28.

Auf der individuellen Ebene finden sich vor allem die Ursachen, die aus den Eigenschaften des Einzelnen hervorgehen. Machiavelli sieht eine der Ursachen für Krieg auf dieser Ebene darin, dass der Herrscher seinem Ehrgeiz folgt, um so seine Macht zu vergrößern. Er führt zu den zwei Arten von Kriegsursachen, wobei die eine von Machthabern ausgeht, Folgendes aus: Krieg wird von Machthabern,

„[...] die ihre Herrschaft auszudehnen suchen, aus Ehrgeiz geführt werden.“³¹⁷

Diese Kriegsursache ist in demokratischen Staaten auszuschließen, aber in anderen Staatsformen durchaus noch immer existent. Spinoza geht ebenfalls auf diese Konfliktursache ein, in dem er die Affekte des Menschen als den Grund für Auseinandersetzungen sieht. Der Mensch neigt eher zu den negativen Affekten und daher trachtet er danach andere zu schädigen. Weil die Menschen

„[...] danach streben, an vorderster Stelle zu stehen, die Menschen in Konflikt miteinander geraten [...]“. ³¹⁸

Wenn sich die Menschen also ihren Affekten hingeben, ihnen nachgeben, werden die Einzelinteressen in den Vordergrund gestellt. Bei Grotius findet sich eine ähnliche Sicht der Ursachen von Kriegen.

„Woher kommen die Kriege und Schlachten unter Euch? Kommen sie nicht aus Euren Begierden, die in Euren Gliedern die Gewalt haben? Ihr begehrt und werdet nicht erlangen; Ihr beneidet und erstrebt, und werdet nichts erreichen; Ihr kämpft und führt Krieg, und Ihr werdet nichts gewinnen, weil Ihr nicht gebeten habt. Ihr betet und empfanget nicht, weil Ihr schlecht gebeten habt, und in Euren Lüsten Euch verzehrt.“³¹⁹

Der Aspekt, der hier eine Rolle spielt, ist das Individualinteresse, welches, wenn es denn über das Allgemeinwohl gestellt wird, zur Ursache von Konflikten beiträgt. Dieser Aspekt kommt nicht unmittelbar zum Tragen. Dieser Effekt führt im Inneren zu einer Auflösung der Ordnung des Gemeinwesens. Dieser zielt also auf die innerstaatliche Ursache von Konflikten ab, welche der Mesoebene zu zuordnen ist. Diese Desintegration, das Aufgehen in den Partikularinteressen, führt in weiterer Folge auch auf zwischenstaatlicher Ebene, der Makroebene, zu einer Verschiebung der Macht. Es kommt zu einem Machtungleichgewicht, welches zu einer zwischenstaatlichen Asymmetrie führt.³²⁰

Man kann hier den Zusammenhang der verschiedenen Ebenen klar erkennen. Die Ursachen auf der Mikroebene führen über die Mesoebene zu den Ursachen auf der Makroebene. Partikularinteressen gehen, über die daraus folgende Desintegration, über in eine Machtasymmetrie, welche zum

³¹⁷ Ebd., S. 186f.

³¹⁸ Spinoza, Politischer Traktat, S. 9.

³¹⁹ Kirchmann, 1869, S. 117.

³²⁰ Vgl. Pesendorfer, 1982, S. 101. (in: Neisser, 1982)

Krieg führt. Die Basis für die Ursache von Konflikten liegt also in der Gesinnung des Einzelnen. Es finden sich auch bei Grotius die schlechten Eigenschaften des Menschen als Auslöser von Konflikten.

„Jeder Krieg zwischen den Menschen entspringt aus einer Schlechtigkeit. Bald aus Wollust, bald aus Habsucht, bald aus Ruhmsucht, bald aus Herrschsucht.“³²¹

Wenn aber die schlechten Eigenschaften zum Krieg führen, bleibt die Frage nach dem Politischen im Krieg. Des dem Allgemeinwohl Dienenden wird bei der Beschreibung der Ursachen keine Rechnung getragen.³²² Dieser Eindruck verstärkt sich durch einen weiteren Gedanken von Grotius:

„Jetzt ist Alles des Krieges voll; denn überall schweifen die Leidenschaften und erwecken in allen Ländern die Begierde nach fremdem Eigenthum.“³²³

Er löst diese Unklarheit damit auf, dass er vom rechtmäßigen Grund zum Krieg spricht.

„Wir kommen zu den Ursachen der Kriege, d.h. zu den rechtmässigen Ursachen derselben. Denn es giebt auch andere, welche von dem Nutzen hergenommen sind und mitunter von den aus dem Recht abgeleiteten Ursachen unterschieden werden.“³²⁴

Hier kann eine Unterscheidung in Krieg als politisches Instrument und in Krieg als Verbrechen gesehen werden. Wobei für Grotius die Bereicherung gegen das Naturrecht verstößt.

„Es sei gegen die Natur, dass man sich auf Unkosten eines Anderen bereichere; [...]“³²⁵

Seiner Auffassung nach gibt es drei Arten von Kriegen, welche einen rechtmäßigen Grund aufweisen:

„[...] die Vertheidigung, die Wiedererlangung des Genommenen und die Bestrafung.“³²⁶

Diese Gedanken finden sich auch in der Charta der Vereinten Nationen wieder. Grotius versteht den Krieg also auch als Rechtsmittel zwischen Gemeinwesen.

„[...]“; denn wo die Gerichte aufhören, da beginnt der Krieg.“³²⁷

³²¹ Kirchmann, 1869, S. 118.

³²² Anm. d. Verf.: Das politische Moment liegt vermutlich darin begründet, dass die Beseitigung einer Asymmetrie dem Gemeinwohl eines der Konfliktgegner dienlich ist.

³²³ Kirchmann, 1869, S. 118.

³²⁴ Ebd., S. 216.

³²⁵ Ebd., S. 381.

³²⁶ Ebd., S. 218.

³²⁷ Ebd., S. 218.

Krieg braucht also eine Ursache, einen Grund, denn grundlos geführt, ebenso wie aus unrechtmäßigen Gründen, ist der bewaffnete Konflikt ein Verbrechen. Die Ursachen liegen im Verhalten des Einzelnen, wobei hier eine verbrecherische Grundhaltung durchaus der Auslöser sein kann. Da aber Kriege nur in und zwischen Gemeinwesen stattfinden, ist die Grundhaltung Einzelner zwar von Bedeutung, doch braucht es die Gemeinschaft, um den Krieg manifest werden zu lassen.

Auch Symmetrie kann als Kriegsursache angesehen werden, nämlich dann, wenn Symmetrie in den Interessen mehrerer sich gegen ein Gemeinwesen richtet. Diese gleiche Interessenslage führt in weiterer Folge wiederum zu einer Asymmetrie, die sich als Konflikt manifestieren kann. Macht und Interessen sind im Zusammenhang mit den Kriegsgründen von entscheidender Bedeutung. Das Verhalten der Staaten zueinander orientiert sich an deren Interesse, deren *bonae commune*, dem Allgemeinwohl.

Dabei ist dieser Zweck der Orientierungspunkt für das Handeln der Gemeinwesen. Liegen die Interessen auseinander, so führt dies zur Gegnerschaft, in der sich der Staat zu behaupten versucht, um mächtiger zu werden. Daraus folgt, dass die Staaten Frieden halten, weil sie es aus eigenem Interesse wollen.³²⁸ Es gibt kein gemeinsames Recht, das sie zur Ordnung zwingt. In Form von Verträgen gehen Staaten Selbstverpflichtungen einander gegenüber ein. Diese haben nur solange Aussicht auf Bestand, als es sich nicht um existenzielle Fragen handelt. Weiter müssen diese Verträge das Machtverhältnis zwischen den Gemeinwesen widerspiegeln.³²⁹

Ziel der verschiedenen Verträge ist es, ein Gleichgewicht zwischen den Staaten herzustellen, denn Frieden gibt es nur im Zustand des Machtgleichgewichts.³³⁰ Dieses Gleichgewicht ist als ein dynamisches zu verstehen, da die Staaten im Inneren einer steten Weiterentwicklung und dadurch nach außen die Bedingungen zwischen den Staaten ebenso einem stetigen Wandel unterworfen sind. Da nun alle Gemeinwesen in dieser Dynamik existieren, sind die Ursachen für Konflikte nicht gänzlich zu beseitigen. Wie bereits mehrfach erwähnt, liegt im Krieg auch ein gestalterisches Element, das dazu führt Ungleichgewichte aufzuheben und zu beseitigen. Macht und Interesse sind der Ausgangspunkt für die Zusammenarbeit von Staaten³³¹, wie auch für deren Feindschaft.

Das Streben nach mehr Macht dient letztlich dem Wunsch nach Sicherheit und dem Bedürfnis, das Gemeinwesen in seiner Existenz zu erhalten.³³² Macht ermöglicht Bedrohungen abzuwehren oder zumindest einzudämmen. Machtgleichgewicht ist das Ziel der Interaktion von Gemeinwesen, denn nur dann haben sie einen Zustand einander gegenüber eingenommen, der Stabilität verspricht. In diesem Zustand ist die Aussicht darauf, dass Verträge eingehalten werden, am größten, da das System der

³²⁸ Vgl. Pesendorfer, 1982, S. 98f. (in: Neisser, 1982)

³²⁹ Vgl. ebd., S. 99.

³³⁰ Vgl. ebd., S. 99.

³³¹ Vgl. Freudenberg, 2008, S. 34.

³³² Vgl. Nye, Joseph S.: Macht im 21. Jahrhundert. Politische Strategien für ein neues Zeitalter, München 2011, S. 58.

Gemeinwesen untereinander ein anarchisches ist.³³³ Jeder Staat kann Verträge eingehen, ist aber letztlich selbst für sein Dasein verantwortlich.

Selbstentwaffnung im Zustand des Gleichgewichts zwischen den Staaten bedeutet, dass eine neue Asymmetrie geschaffen wird, die von anderen, zur Erlangung von mehr Macht, ausgenutzt werden kann.³³⁴ Die Ursache von Konflikten ist also in der Asymmetrie von Macht, und dem Bestreben diese auszugleichen, zu finden. Die Asymmetrie kann selbst herbeigeführt sein, durch den inneren Zerfall eines Gemeinwesens oder aber durch Zusammenschluss mehrerer Gemeinwesen, mit selben Interessen, von außen her entstehen. Ob sich diese Asymmetrie zu einem Krieg manifestiert, ist dann von den weiteren Faktoren, wie der Furcht vor dem Gegenüber und dem Wunsch nach mehr Macht dagegen, abhängig.

5.3.2 Exkurs: Macht als Parameter für die Ursache von bewaffneten Konflikten

Macht ist als Vermögen und Können, etwas mit Handlungen zu bewirken, zu verstehen.³³⁵ Anders als Gewalt entspringt sie der Allgemeinheit der Bürger und dient dem Allgemeinwohl des Gemeinwesens, der Erhaltung des Gemeinwesens im Dasein. Gewalt ist im Gegensatz dazu die Verwirklichung von willkürlichen Zielen. Macht ist die Möglichkeit den Willen auch gegen einen Widerstand durchzusetzen.³³⁶ Sie beruht also auf der Möglichkeit der Anwendung von Mitteln zu deren Durchsetzung. So kann Gewalt auch ein solches Mittel sein. Unter Macht versteht Spinoza zum Beispiel das Vermögen des Einzelnen sich im Dasein zu erhalten.³³⁷

Da der Einzelne nicht in der Lage ist sich allein im Dasein zu erhalten, schließt er sich mit anderen zusammen und vergrößert dadurch seine Macht. Diese wird dann an einen Einzelnen (den Herrscher) oder aber an ein Kollektiv (die Regierung) übertragen, um zur Anwendung gebracht zu werden. Da sie nicht aus einem selbst entspringt, sondern übertragen wird, muss sie auch verantwortet werden und zwar gegenüber jenem, von dem sie übertragen wurde bzw. dem gegenüber sie angewandt wird. Wenn der Staat auf die Ausübung seiner Macht verzichtet, kommt es zu einer Machtverschiebung nach unten und es herrscht das Recht des Stärkeren, die Willkür oder anders formuliert die Gewalt. Es kann in diesem Fall keinen Frieden geben.

Daraus lässt sich schließen, dass die staatliche Macht dem Allgemeinwohl dient, da sich sonst das Gemeinwesen auflöst. Andererseits besteht laut Spinoza auch die Gefahr, dass das Gemeinwesen, welches ohne Vernunft regiert wird, Furcht oder Ungerechtigkeit bei den Menschen

³³³ Vgl. Pesendorfer, 1982, S. 99. (in: Neisser, 1982)

³³⁴ Vgl. Nye, 2011, S. 58.

³³⁵ Vgl. Nohlen, Dieter; Schultze, Rainer-Olaf: Lexikon der Politik. in: Lexikon der Politik (op. 1995), S. 306.

³³⁶ Vgl. ebd., S. 306.

³³⁷ Vgl. Spinoza, Politischer Traktat, S. 11ff.

hervorrufen und dadurch diese Menschen gegen sich aufbringen, einen ähnlichen Effekt erzeugt.

„Und so hat sicherlich auch ein Gemeinwesen einiges zu befürchten; nicht anders als jeder Bürger oder jeder Mensch im Naturzustand steht auch ein Gemeinwesen umso weniger unter eigenem Recht, je mehr es Grund zur Furcht hat.“³³⁸

Als Teilmenge der Macht ist die Herrschaft anzusehen, die notwendig ist, um dem Gemeinwesen Zwecke und Ziele vorzugeben, die im Handeln verwirklicht werden sollen. Herrschaft ist staatliche Macht zur Durchsetzung von Gerechtigkeit und bedarf daher der Vernunft. Macht verhilft dem Recht zur Geltung, Herrschaft muss legitimiert sein, um sich entfalten zu können.³³⁹ Macht kann also als Triebfeder für oder gegen Konflikte gesehen werden. Das Gemeinwesen benötigt davon ein Mindestmaß, um sich gegen andere Gemeinwesen zu behaupten. Verliert es an Macht im Inneren, so führt dies zu einer Machtverschiebung im Äußeren. Diese Verschiebung kann letztlich im Krieg enden. Spinoza sieht die Macht eines Gemeinwesens in direktem Verhältnis zur Vernunft mit der es regiert wird. Er sagt, dass

„[...] dasjenige Gemeinwesen am mächtigsten ist und am meisten unter eigenem Recht steht, das auf der Vernunft sich gründet und dadurch sich regiert.“³⁴⁰

Gibt es keine Vernunft, verliert das Gemeinwesen an Macht und desintegriert sich. Desintegration führt zum Konflikt im Inneren und in weiterer Folge auch zum Konflikt mit anderen Gemeinwesen. Macht ist also ein bedeutender Faktor bei der Suche nach den Ursachen für den Krieg.

5.3.3 Frieden als Zweck des Krieges

Ziel des Krieges ist es ein Machtgleichgewicht zu erreichen, mit dem Zweck Frieden zu erlangen. Frieden ist also nur im Zustand des Machtgleichgewichtes von Dauer.³⁴¹ Asymmetrien, wie bereits erwähnt, bringen das Bestreben mit sich, diesen Potentialunterschied auszugleichen, welches im Konflikt endet. Ist ein Konflikt ausgebrochen, kann nur im Zuge eines konfliktischen Potentialausgleiches ein Zustand des Gleichgewichts eingenommen werden, welcher dann den Frieden manifestiert. Dies zeigt sich auch in der Theorie des demokratischen Friedens, welche eine Kriegführung zwischen demokratischen Staaten als unbedeutendes Mittel ansieht.³⁴²

Zwischen fortschrittlichen Demokratien herrscht eine Art Machtgleichgewicht. Dies äußert sich in internationalen Organisationen, genauso wie in regionalen Zusammenschlüssen solcher Staaten. Als Beispiel sei hier die EU genannt, die diese Tatsache als Friedens- und Stabilitätskonzept umsetzt. Es ist unwahrscheinlich, dass Mitgliedsstaaten

³³⁸ Ebd., S. 26.

³³⁹ Vgl. Freudenberg, 2008, S. 61.

³⁴⁰ Spinoza, Politischer Traktat, S. 24.

³⁴¹ Vgl. Pesendorfer, 1982, S.99. (in: Neisser, 1982)

³⁴² Vgl. Nye, 2011, S. 59.

einander in kriegerischer Auseinandersetzung gegenüberreten, da sie die Möglichkeit haben, ungeachtet ihrer Größe, gleich viel Macht untereinander, mit anderen Mitteln, auszuüben. Dies führt aber nicht dazu, dass alle Staaten friedvoll zueinander in Interaktion treten.

Platon sieht den Frieden nicht so sehr als den Zweck des Krieges, vielmehr ist für ihn der Friede die bessere Alternative zum Krieg. Er spielt hier auf ein Gleichgewicht als Grundlage an, welches er als Aufgabe des Gesetzgebers sieht. So ist für ihn kein guter Gesetzgeber der,

„[...] wer nicht lieber die kriegerischen Anordnungen des Friedens, als die friedlichen des Krieges wegen träge.“³⁴³

Diese Aussage zielt auf die Entstehung von Asymmetrien im Machtgleichgewicht durch innere Desintegration ab. Ist ein Krieg allerdings bereits ausgebrochen, so verweist er darauf diesen Zustand schleunigst zu beseitigen, also den Frieden zu suchen.³⁴⁴ Für Machiavelli ist der manifeste Frieden der latente Krieg.³⁴⁵ Da der Müßiggang aus der Abwesenheit von Bedrohungen und Gefahren – also im Frieden – am ehesten zum Vorschein tritt, ist die Gefahr einer Desintegration des Gemeinwesens groß und daraus gefolgt der nächste bewaffnete Konflikt absehbar. Wird aber ein Krieg geführt, so hat er kurz und schonungslos zu sein.³⁴⁶ Zweck des Krieges ist seiner Auffassung nach ein Friedensschluss.

„[...] eine Schlacht zu schlagen. Wurde sie gewonnen, so machten die Feinde Friedensvorschläge, um ihr Land vor der völligen Verwüstung zu bewahren; [...].“³⁴⁷

Der Friedensvorschlag geht hier vom Unterlegenen aus. Dies entspricht keinem aufgezwungenen Frieden, sondern der Unterlegene bietet Bedingungen an, die er vertreten kann. Es obliegt dem Sieger die Bedingungen so anzunehmen, dass der Friede dann Bestand hat, er also eine Symmetrie der jeweiligen Bedürfnisse bewirkt. Hier spielt die Vernunft des Siegers eine große Rolle. Ähnlich fasst Spinoza die Suche nach dem Frieden, in dem er feststellt,

„[...] daß die Vernunft durchaus lehrt, den Frieden zu suchen, [...].“³⁴⁸

Er bezieht diese Aussage auf den Zustand des Gemeinwesens im Inneren, damit fordert er, das Gemeinwesen vor Desintegration zu bewahren. Im Frieden zwischen Gemeinwesen gebietet die Vernunft, die sich ändernden Bedingungen für einen Friedensvertrag zu berücksichtigen und immer das Gemeinwohl im Blick zu halten, denn dies ist der Vernunft geschuldet.³⁴⁹ Für Spinoza ist ein Zustand ohne Krieg nicht unbedingt mit dem Frieden

³⁴³ Platon, *Nomoi*, S. 160.

³⁴⁴ Vgl. ebd., S. 160.

³⁴⁵ Vgl. Münkler, Herfried: *Über den Krieg. Stationen der Kriegsgeschichte im Spiegel ihrer theoretischen Reflexion*, 5. Aufl., Weilerswist 2008, S. 39.

³⁴⁶ Vgl. Machiavelli, *Discorsi*, S. 184.

³⁴⁷ Ebd., S. 184.

³⁴⁸ Spinoza, *Politischer Traktat*, S. 23.

³⁴⁹ Vgl. ebd., S. 28f.

gleichzusetzen, dann nämlich, wenn er erzwungen ist, also Furcht bei denen herrscht, welche daher nicht zu den Waffen greifen. Diesen Zustand nennt er einen ohne Krieg, um dann fortzusetzen:

„Frieden ist nämlich nicht die Abwesenheit von Krieg, sondern eine Tugend, die einer Stärke des Charakters entspringt; [...].“³⁵⁰

Frieden benötigt dazu, anders als der Krieg, den Willen mindestens zweier Akteure.³⁵¹ Er ist das Ergebnis und der Zweck des Krieges. Dieser kann nicht in ihm selbst begründet sein, denn der Krieg betrifft im Extremfall die Existenz der daran beteiligten Gemeinwesen.³⁵² Als Instrument der Politik dient er letztlich dem Frieden. Clausewitz sieht das Ziel des Krieges darin, dass ein politischer Zweck erreicht wird. Diesem politischen Zweck ist ein weiterer Zweck hinterlegt, die Herstellung des Friedens.³⁵³ Dabei muss, wie bereits erwähnt, festgehalten werden, dass die bloße Abwesenheit von Krieg nicht der Frieden im eigentlichen Sinn ist.

Damit der Staat also sein Interesse, das Allgemeinwohl, verwirklichen kann, bedarf es des Friedens, nicht eines fortdauernden Krieges. Aufgabe einer, der Vernunft nach handelnden, politischen Führung ist es, Frieden aufrecht zu erhalten oder Frieden zu schaffen.³⁵⁴ Krieg und Frieden stehen in einem komplexen, wechselseitigen Verhältnis zueinander. Einerseits bedarf es der Klammer einer potentiellen Gefahr, um eine Desintegration des Gemeinwesens zu verhindern, andererseits benötigt es Sicherheit, um den Staatszweck zu erreichen.

Da beide Zustände nicht absolut sind, kommt es immer wieder zu Krieg, dessen Letztzweck dann der Frieden ist.³⁵⁵ Ab wann kann nun von einem Krieg gesprochen werden? Um diese Frage in weiterer Folge zu beantworten, muss die Intensität von Konflikten näher untersucht werden. Es gibt durchaus Beispiele für Konflikte, die dem Wesen nach keine Kriege sind, aber ein Ausmaß annehmen, welches die staatliche Ordnung soweit ins Wanken bringt, dass sie in die Kompetenz des Militärs gehören.

5.4 Zur Intensität von bewaffneten Konflikten

Dieser Abschnitt widmet sich der Frage, ab welchem Intensitätsgrad in einem bewaffneten Konflikt die Verantwortung für die Reaktion darauf auf das Militär übergeht; es geht darum, ab wann von einem Krieg gesprochen werden kann. Krieg ist die Domäne des Militärs, das Verbrechen gehört in die Verantwortung der Polizei. Interessant erscheint im Hinblick auf Phänomene wie den Drogenkrieg in Mexiko oder den Kampf gegen die Mafia, wo die Schwelle für die Zuständigkeit zwischen den Trägern der bewaffneten Staatsgewalt liegt. Hier ist neben den Akteuren und dem Zweck, den diese verfolgen, die Intensität ein wesentlicher Parameter.

³⁵⁰ Ebd., S.36.

³⁵¹ Vgl. ebd., S. 28.

³⁵² Vgl. Pesendorfer, 1982, S. 102. (in: Neisser, 1982)

³⁵³ Vgl. Stupka, 2011, S. 145.

³⁵⁴ Vgl. Freudenberg, 2008, S.52.

³⁵⁵ Vgl. Stupka, 2011, S. 147.

In Bezug auf die Forschungsfrage ist dies ein zentraler Punkt, da sich die Akteure und/oder der Zweck oftmals nicht genau festlegen lassen. Im Zusammenhang damit geht es um die Formen des Krieges und die Ebenen, auf denen er letztlich ausgetragen wird. Diese sind der Ausdruck der Intensität des Konfliktes. Hier spielen Symmetrie und Asymmetrie eine große Rolle. Diese beiden Begriffe sind, anders als bei den Ursachen für Kriege, nicht im Sinne von Interessen oder Macht zu verstehen, sondern beziehen sich auf die Qualität der Akteure und deren Mittel und Kampfweisen. Diese spiegeln sich in den Formen des Krieges wider.

Die Intensität des Krieges wandelt sich entsprechend der daran teilnehmenden Akteure und der daraus resultierenden Form des Krieges. Clausewitz spricht in diesem Zusammenhang von der Trinität des Krieges, in der er sich, von seinem Charakter und seiner Natur her, wandeln kann. Der Krieg ist in diesem Sinne ein wahres Chamäleon.³⁵⁶ Es lässt sich aus der Dreifaltigkeit des Krieges die Einteilung in einen Großen und einen Kleinen Krieg ableiten.

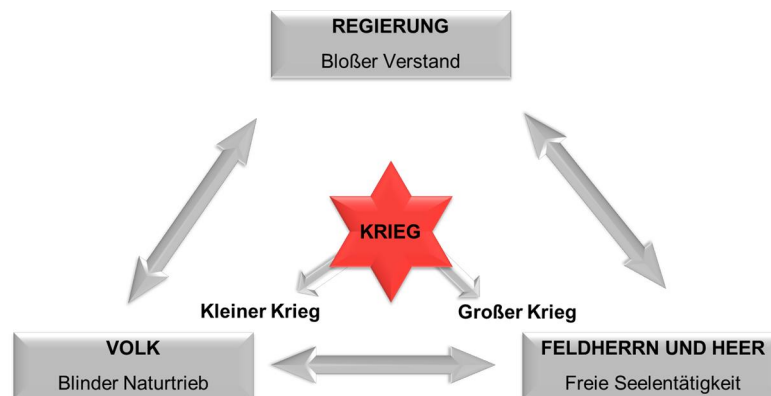


Abbildung 4: Die Trinität des Krieges³⁵⁷

Da Clausewitz die Einteilung des Krieges in diese zwei Formen getroffen hat, wird er auch bevorzugt für die Darstellung dieser Kriegsformen herangezogen. Die Wechselwirkung zwischen den drei Polen des Krieges ist derart, dass der Große Krieg dem Heer zuzuordnen ist, während der Kleine Krieg zwischen Volk und Heer liegen muss. Je näher er dem Naturtrieb kommt, umso existenzieller ist er. Die beiden Formen des Krieges werden nun näher dargestellt.

5.4.1 Der Große Krieg

Der Große Krieg ist von Symmetrien gekennzeichnet. Er ist als ein solcher zu fassen, der zwischen sich gegenseitig anerkennenden Akteuren stattfindet. Hier ist die erste Symmetrie des Großen Krieges zu erkennen. Er wird generell als der Krieg zwischen Staaten zur Anwendung gebracht. Die

³⁵⁶ Vgl. Clausewitz, Vom Kriege, S. 23.

³⁵⁷ Abbildung durch den Verfasser erstellt.

zweite Symmetrie besteht in der Qualität der Akteure. Diese sind nach ähnlichen Methoden ausgebildet, wenden dieselben Verfahren und Waffensysteme an.³⁵⁸ Krieg ist, wie schon festgestellt, eine Angelegenheit von Gemeinwesen. Diese Symmetrien werden von einer Asymmetrie hinsichtlich der Größe, der Kräfte und der Moral begleitet.³⁵⁹ Im Großen Krieg treffen die regulären Streitkräfte von Nationalstaaten aufeinander. Er ist auf eine symmetrische Kriegführung ausgerichtet. Er ist hinsichtlich der Faktoren Kraft, Raum und Zeit ein gehegter Krieg.³⁶⁰

Auch rechtlich ist der Große Krieg eingehengt, in dem er nach festen Regeln geführt wird.³⁶¹ Nach Münkler ergibt sich,

„[...] dass mit dem Staatenkrieg eine Form von Krieg und Kriegführung definiert wurde, die sich politisch und rechtlich regulieren ließ [...]“³⁶²

Diese rechtliche Hegung garantiert sozusagen ein Mindestmaß an Symmetrie. Es ist ein Anreizsystem, sich überstaatlich an rechtliche Regelungen zu halten, um nach einer Niederlage weiter bestehen zu können. Aber nicht nur für den Verlierer war dies ein Anreiz sich daran zu halten, auch der Sieger konnte der Wahrscheinlichkeit, einen dem Kriegsende folgenden Kampf gegen die Besatzung führen zu müssen, entgegenwirken, wenn er sich an den rechtlichen Rahmen hielt.³⁶³ Der Große Krieg kann, als institutionalisierte Konfliktaustragung zwischen gleichberechtigten Gemeinwesen verstanden werden und unterliegt auch einer politischen Kontrolle, indem er einem politischen Zweck dient.³⁶⁴

Stellvertretend für die Gemeinwesen kämpfen im Großen Krieg staatliche Akteure gegen staatliche Akteure.³⁶⁵ Dafür ist aber nicht nur die Hegung, im oben beschriebenen Sinn verantwortlich, sondern auch die technologische Entwicklung der Armeen. Mit dieser Entwicklung auf die später im Detail eingegangen wird, kam auch der wirtschaftliche Faktor ins Spiel. Vereinfacht gesagt können es sich nur Staaten leisten teures Kriegsgerät im Konflikt zum Einsatz zu bringen. Unter dem klassischen Großen Krieg ist also die symmetrische Form der zwischengemeinschaftlich ausgetragenen bewaffneten Konflikte zu verstehen.

Der Große Krieg ist durch seine Hegung auch sehr raumzentriert, es geht immer um die Beherrschung eines bestimmten physischen Raumes, in dem der Kampf durchgeführt wird. Ist die Kontrolle über den Raum hergestellt, so ist der Gegner in der Regel besiegt. Auf die Definition des Krieges bei Clausewitz reflektierend geht es um den Willen, der mittels

³⁵⁸ Vgl. Münkler, Herfried: Der Wandel des Krieges. Von der Symmetrie zur Asymmetrie, [Unveränd. Nachdr.] Aufl., Weilerswist 2010, S. 60f.

³⁵⁹ Vgl. Strachan, 2008, S.92.

³⁶⁰ Vgl. Münkler, 2010a, S. 24f.

³⁶¹ Vgl. ebd., S. 24f.

³⁶² Münkler, 2010b, S. 32.

³⁶³ Vgl. ebd., S. 63.

³⁶⁴ Vgl. Strachan, 2008, S. 24.

³⁶⁵ Vgl. Geis, Anna (Hrsg.): Den Krieg überdenken. Kriegsbegriffe und Kriegstheorien in der Kontroverse, Schriftenreihe der DVPW-Sektion Politische Theorien und Ideengeschichte, Baden-Baden 2006, S. 21.

physischer Gewalt durchgesetzt werden muss. Dies bedingt ein physisches Gegenübertreten der beiden Gegner, der Heereskörper, in einem bestimmten Raum. Die Wirkung auf die Psyche erfolgt über den Raum, über die Physis. Dies ist ein weiteres Kennzeichen des Großen Krieges.

Der Raum, um den gekämpft wird, ist durch den Angreifer gewählt und liegt im Territorium des Gegners. Dies hat auch den Schutz der eigenen Bevölkerung vor den Auswirkungen der Kampfhandlungen zum Grund. Daraus folgt, den Großen Krieg in der Dauer einzuhegen und eine rasche Entscheidung zu suchen.³⁶⁶

Vom Umfang – der Ausdehnung – her, ist der Große Krieg als begrenzt anzusehen, er bezieht sich nur auf das Militär der beiden Gemeinwesen. Hierbei ist noch keine Ableitung hinsichtlich der Intensität getroffen, welche je nach Sichtweise zu fassen ist. Für die Streitkräfte handelt es sich um eine Intensität, die als sehr hoch zu bewerten ist. In seiner reinen Form, als Kampf zwischen den legitimierten Trägern der Staatsgewalt, dem Militär, ist er von instrumentellem Charakter.

Im Zusammenhang mit dem Großen Krieg sind auch Verfahren der asymmetrischen Kriegführung, durch staatliche und nichtstaatliche Akteure, zu nennen. Diese kamen immer wieder gemeinsam zur Anwendung. Je mehr asymmetrische Elemente, zur Ergänzung des Großen Krieges, herangezogen wurden, je umfassender die Mitwirkung von nichtstaatlichen Akteuren ist, umso existenzieller ist der Charakter des Großen Krieges. Dies leitet, nach einem Exkurs zum Großen Krieg, über zum Kleinen Krieg, als zweite Form des Krieges bei Clausewitz.

5.4.2 Exkurs: Der Große Krieg am Beispiel des Fünf-Tage-Krieges in Georgien

Georgien war bemüht der NATO beizutreten. Diesen Beitritt zu verhindern und damit die NATO nicht direkt an der Südflanke der Russischen Föderation stehen zu haben, waren Kern der Auseinandersetzung der Russen mit Georgien. Die mögliche Erweiterung des Raketenabwehrschirmes³⁶⁷ der NATO in dieser Region ist dabei eine potentielle Gefahr, der die Russische Föderation entgegenwirken wollte. Die Kaukasus-Region spielt für Russland eine wesentliche Rolle, als Tor zum Mittleren Osten und als Transitraum für das Kaspische Erdöl.

Die Konfliktgeschichte in diesem Teil des Kaukasus' reicht bis in die Zarenzeit zurück. Durch die russische Verwaltungsgliederung wurden Nord- und Südossetien getrennt. Im Jahr 1989 wurde von den Südosseten die autonome Südossetische Sowjetrepublik gegründet. Die Anerkennung seitens Georgiens erfolgte nicht. 1990 erklärte sich Südossetien erneut für unabhängig. Beide Erklärungen zogen bewaffnete Auseinandersetzungen

³⁶⁶ Vgl. Haffner, Sebastian: Der neue Krieg. In: Tse-tung, Mao: Theorie des Guerillakrieges oder Strategie der Dritten Welt, Reinbek bei Hamburg 1966, S. 15f.

³⁶⁷ Vgl. Kuster, Matthias: Der Georgien-Krieg 2008 aus militärstrategischer Sicht. In: Military Power Revue der Schweizer Armee, Nr.1/2011, S. 57.

nach sich. 1992 wurde ein Waffenstillstand erreicht, welcher durch eine Friedenstruppe überwacht werden sollte. Im Juli desselben Jahres erklärte sich auch Abchasien für unabhängig. Ein georgischer Vorstoß konnte mit Unterstützung der Russischen Föderation (RF) bereinigt werden. Es wurde hier auch eine Friedenstruppe und eine UN Beobachter-Mission eingesetzt.³⁶⁸

Georgien wurde 1991 unabhängig. Anfangs noch Teil der Gemeinschaft unabhängiger Staaten (GUS), verfolgte Georgien unter Präsident Saakaschwili ab 2003 einen pro-westlichen Kurs. Der Beitritt zur NATO war dabei das erklärte Ziel Georgiens. Diese Bestrebungen und das, durch die beiden Tschetschenien-Kriege belastete Verhältnis zwischen Georgien und Russland, verschärften den Konflikt. Der georgische Präsident verfolgte neben der westlichen Orientierung auch die Wiederherstellung der territorialen Integrität Georgiens.³⁶⁹ Die vom Westen unterstützte Unabhängigkeitserklärung des Kosovo und die geplante Aufnahme der Ukraine und Georgiens in den Kreis der NATO-Beitrittskandidaten bildeten Anfang 2008 den Auslöser für den Fünf-Tage-Krieg. Zuvor hatte die Bush-Administration ein Ausbildungsprogramm für die georgischen Streitkräfte eingeleitet.

Die RF ging gegen Georgien in folgender Weise vor: Die Provokation Georgiens durch Angriffe südossetischer Separatisten sollte zu einem militärischen Eingreifen von Georgien führen. Dieses Eingreifen musste von der RF ebenfalls mit militärischen Mitteln beantwortet werden. Orientiert an der Terminologie des Vorgehens der NATO im Kosovo, wurde mit der Verhinderung eines behaupteten Völkermordes der südossetischen Bevölkerung durch Georgien und zum Schutze russischer Bürger und Friedenstruppen argumentiert.³⁷⁰ Die Lehren aus den beiden Tschetschenien-Kriegen wurden umgesetzt. Die Planung war lange vor dem militärischen Einsatz gegen Georgien begonnen worden. Die Verteilung russischer Pässe an die Bevölkerung von Abchasien und Südossetien ist hier ein Indiz dafür.

Die Verfügbarkeit eines stehenden operativen Kommandos in Form des Militärdistriktes Nordkaukasus, welches durch den zweiten Tschetschenienkrieg trainiert war, die Abhaltung der Übung „Kaukasus 2008“ und die Entsendung von russischen Ärzten und Journalisten in die südossetische Hauptstadt Zchinwali zeugten von den Vorbereitungen auf eine bevorstehende Invasion.³⁷¹ Der Georgien-Krieg stellte eine klassische Joint-Operation dar, an der alle Teilstreitkräfte (TSK) teilnahmen. Die operative Führung war vorbereitet und ausreichend trainiert. Eingeleitet wurde die Intervention seitens der RF durch Übergriffe der Separatisten auf georgische Friedenstruppen und Dörfer. Durch die Übung „Kaukasus 2008“ (Hervorhebung durch den Verfasser.) hatten die russischen Truppen einen hohen Bereitschaftsgrad. Die Bereitstellung wurde Anfang August in der

³⁶⁸ Vgl. ebd., S. 46ff.

³⁶⁹ Vgl. ebd., S. 48f.

³⁷⁰ Vgl. ebd., S. 49.

³⁷¹ Vgl. ebd., S. 49.

Nähe des Roki-Tunnels durchgeführt. Auf Seiten Georgiens erfolgte eine Verschiebung von Truppen Richtung Gori ab dem 6. August.³⁷²

Begleitet waren die Vorbereitungen durch massiven Einsatz von Artillerie. Auf Verhandlungsangebote und einen einseitigen Waffenstillstand seitens Georgiens erfolgte keine russische Reaktion. Am 7. August griff Georgien Südossetien an und traf auf einen vorbereiteten Gegner. Der Vorstoß der georgischen SK war der Auslöser für das Überschreiten der Grenze durch die Elemente der 58. Armee. Unter Einsatz der Luftwaffe, auch in das georgische Kernland, und Ansatz der Schwarzmeer-Flotte, zur Zerstörung der georgischen Seehäfen und Marine, sowie die Anlandung russischer Truppen in Abchasien, wurde eine zweite Front eröffnet.³⁷³ Der Kulminationspunkt aus Sicht der georgischen Streitkräfte (SK) war erreicht, als die russischen Truppen am 10. August auf Gori vorstießen und somit die georgischen SK zerschlagen waren.

Angesichts dieser Tatsache verkündete der georgische Präsident Saakaschwili einen einseitigen Waffenstillstand unter Rückzug der Truppen aus Südossetien. Die Russen stießen von Westen weiter Richtung Osten vor.³⁷⁴ Die Rückführung der ersten georgischen Brigade aus dem Irak erfolgte zu spät, der Krieg war schon zu Gunsten der Russen entschieden. Am 12. August 2008 war Georgien praktisch zweigeteilt und am Abend wurden die Kampfhandlungen eingestellt. Es folgte ein Waffenstillstandsabkommen, welches mit dem Abzug der russischen Truppen im Oktober seine Umsetzung fand. Eine Folge des Konfliktes war der Austritt Georgiens aus der GUS. Das strategische Ziel der RF, die Verhinderung eines NATO-Beitrittes, wurde durch den Krieg erreicht.³⁷⁵

Der Charakter eines Großen Krieges ist eindeutig ersichtlich, das Aufeinandertreffen von konventionellen Streitkräften zweier Gemeinwesen. Es zeigt sich aber auch die Einbettung des Militärs in politische und diplomatische Maßnahmen. Die Erreichung eines politischen Zwecks, nämlich des Nichtbeitritts Georgiens zur NATO, stand im Vordergrund.

5.4.3 Der Kleine Krieg

Im Gegensatz zum Großen Krieg ist der Kleine Krieg durch Asymmetrien geprägt. In ihm treten einander auf der einen Seite reguläre Kräfte, also staatliche Akteure, und auf der anderen Seite irreguläre Kräfte, also nichtstaatliche Akteure gegenüber. Im Gegensatz zum klassischen Krieg steht auch die unterschiedliche Qualität der Konfliktparteien. So ist der Irreguläre in der Regel technologisch unterlegen. Diese Unterlegenheit versucht er durch seine Kampfweise auszugleichen.

Anders als im klassischen Krieg, wird durch den Irregulären nicht die Konzentration der Kräfte, zum Zwecke einer Entscheidungsschlacht,

³⁷² Vgl. ebd., S. 50f.

³⁷³ Vgl. ebd., S. 50ff.

³⁷⁴ Vgl. ebd., S. 53.

³⁷⁵ Vgl. ebd., S. 53ff.

gesucht, sondern, durch Dezentralisierung seiner Kräfte, dem Gegner die Möglichkeit genommen wirksam gegen ihn vorzugehen; es gibt keine Front mehr und keine Unterscheidung von Kampfgebiet und Hinterland. Diese Zerstreuung bringt eine zeitliche Verschleppung des Konfliktes mit sich. Da der nichtstaatliche Akteur sich rechtlich keiner Hegung unterwirft, ist von einer gänzlichen Entgrenzung auszugehen. Die Wirkung auf den Raum erfolgt über die Psyche.

Clausewitz sieht das Volk als letzte Maßnahme zur Verteidigung des Staates gegen einen Angreifer, dann nämlich, wenn es sich an den Abgrund geschleudert sieht.³⁷⁶ Für Clausewitz stellt die Auflockerung und Vermeidung einer offenen Konfrontation mit dem Gegner eine logische Konsequenz für die schwächeren Streitkräfte dar.³⁷⁷ Der Übergang zu asymmetrischen Vorgehensweisen ist die einzige Möglichkeit die Niederlage zu verhindern.

Für die Gedanken von Clausewitz spielen vor allem die Beispiele des Volkskrieges seiner Zeit – in Spanien und Tirol – eine prägende Rolle. Der Kleine Krieg hat eine strategische Verteidigungsfunktion, er ist ein defensiver Krieg, der in der Regel im eigenen Land gegen einen Eindringling geführt wird. Damit gab Clausewitz dem Kleinen Krieg eine neue Bedeutung. Die Praxis der asymmetrischen Vorgehensweise findet heute in vielen Konflikten ihre Anwendung. So kann der Krieg in Tschetschenien als ein solches Beispiel genannt werden.

Der Kleine Krieg war, zu Zeiten von Clausewitz, der Einsatz von kleinen Einheiten der regulären Kräfte zur Sicherung und Aufklärung.³⁷⁸ Diese Verfahren wurden, auf Grund der geringen Stärke der eingesetzten Truppen, als Kleiner Krieg bezeichnet. Ein weiterer Zeitgenosse von Clausewitz, Decker, beschäftigte sich mit diesen Einsatzverfahren. Decker zitiert General Balentini mit seiner Definition des Kleinen Krieges:

„Unter kleinen Krieg verstehe ich alle diejenigen Verrichtungen im Kriege, welche die Operationen einer Armee oder eines Korps bloß begünstigen, ohne an und für sich eine unmittelbare Beziehung auf Eroberung oder Behauptung des Landes zu haben: [...]“³⁷⁹

Im Krieg der Parteigänger geht er auf die Verfahren und die Spezifika des Kleinen Krieges ein. Decker sieht den Parteigängerkrieg durchaus kritisch und rechnet ihn nicht zum Kleinen Krieg an und für sich. Er nennt ihn einen Krieg im Kleinen.³⁸⁰ Begründet ist dies in der Sichtweise der damaligen Zeit, in der der Kleine Krieg von regulären Truppen geführt wurde. Diese Sichtweise hat sich bis heute gewandelt, der Kleine Krieg wird heute vor allem von irregulären Kräften geführt. Parteigänger sind irreguläre Einheiten³⁸¹, die die Regulären bei ihrem Kampf unterstützen.

³⁷⁶ Vgl. Clausewitz, Vom Kriege, S. 174.

³⁷⁷ Vgl. Strachan, 2008, S. 109.

³⁷⁸ Vgl. ebd., S. 134.

³⁷⁹ Decker, Carl: Der Kleine Krieg im Geist der neueren Kriegführung. Abhandlung über die Verwendung und den Gebrauch aller drei Waffen im kleinen Kriege, Berlin, Poßen und Bromberg 1844, S. 1.

³⁸⁰ Vgl. ebd., S. 4f.

³⁸¹ Vgl. ebd., S. 312.

„Daher ist es erklärlich, warum in eigentlichen – nicht bloß sogenannten – Volkskriegen das ganze Land sich im Besitz des Feindes befinden kann, ohne erobert zu seyn; [...]“³⁸²

Der Parteigänger führt seinen Kleinen Krieg in Verbindung mit den Operationen der regulären Streitkräfte.³⁸³ Allerdings sind sie nur sehr lose an die regulären Truppen gebunden, um möglichst effizient zuschlagen zu können. Da der Parteigängerkrieg grundsätzlich im eigenen Land stattfindet, ist es wichtig die Bevölkerung zur Unterstützung auf seine Seite zu ziehen.³⁸⁴ Dies ist umso wichtiger, als oftmals hinter den Linien des Feindes und somit ohne Anbindung an die eigenen Streitkräfte agiert wird. Decker führt in diesem Zusammenhang Ziele für die Parteigänger an, welche für den Feind von Wert sind. Vor allem wichtige Infrastruktur ist dabei auszuschalten.³⁸⁵ Der Parteigänger ist auf Grund seiner Unterlegenheit dazu genötigt auf asymmetrische Methoden zurückzugreifen.

„Der Parteigänger ist fast immer der schwächere Theil, daher fällt auch die Methode weg [Anm. d. Verf.: Gemeint sind die Regeln des Großen Krieges.], denn alle Methode gründet sich auf eine gewisse Gleichheit der Kräfte.“³⁸⁶

Hier ist der Verweis auf Symmetrie und Asymmetrie im beschriebenen Sinne zu finden. Bemerkenswert ist der Hinweis darauf, dass ein Kleiner Krieg - anders als bei Clausewitz - auch außerhalb des eigenen Territoriums geführt werden kann.

„Es ist einleuchtend, daß ein solcher Auftrag sich im eigenen Lande unendlich leichter ausführen läßt, als im feindlichen, besonders, wenn die Einwohner nicht übel gewilligt sind, die Sache und den Krieg ihrer Armee durch thätige Mitwirkung zu unterstützen.“³⁸⁷

Die Formulierung legt zwar nahe den Einsatz der Parteigänger im eigenen Land durchzuführen, schließt den Einsatz, bei Gewinnung der Bevölkerung, aber außerhalb des eigenen Landes nicht aus. Auch Haffner schließt einen Kleinen Krieg außerhalb des eigenen Territoriums nicht aus, führt dazu aber Folgendes an:

„Die Totalguerilla ist nicht nur am stärksten im eigenen Land, sie ist wahrscheinlich nur im eigenen Land überhaupt möglich.“³⁸⁸

Bei Clausewitz und Decker ist der Kleine Krieg immer in Verbindung mit dem Großen Krieg zu denken. Beide sehen in ihm kein eigenständiges Element.³⁸⁹ Es braucht zum Sieg eine Legitimation, die nur der Träger der

³⁸² Ebd., S. 315.

³⁸³ Vgl. ebd., S. 315.

³⁸⁴ Vgl. ebd., S. 318.

³⁸⁵ Vgl. ebd., S. 322f.

³⁸⁶ Ebd., S. 325.

³⁸⁷ Ebd., S. 327.

³⁸⁸ Haffner, 1966, S. 19. (in: Tse-tung, 1966)

³⁸⁹ Vgl. Hahlweg, Werner: Lehrmeister des Kleinen Krieges. Von Clausewitz bis Mao Tse-Tung und (Che) Guevara, Darmstadt 1968, S. 50.

Staatsgewalt besitzen kann und die ein Irregulärer braucht, sofern er die Anerkennung der anderen Gemeinwesen für die Erreichung des Endzweckes des Krieges benötigt. Dies sieht auch Galula in seiner Analyse der Phasen eines Aufstandes:

„The aim of the insurgent is to change the occupied areas into guerrilla areas, guerrilla areas into guerrilla bases, and these into regular bases.“³⁹⁰

Ist dann eine Symmetrie hergestellt, ist es an den Aufständischen durch Verhandlungen und Friedensvorschläge die Situation auf eine rein politische Ebene zu heben.³⁹¹ Es kann aber auch der Kampf in einer anderen Qualität fortgeführt werden.

Da in einem solchen Kleinen Krieg, auf Seiten der Irregulären, nur begrenzte Mannstärken zum Einsatz kommen und sich die Ziele auf die zumeist zivile Infrastruktur konzentrieren, stellt sich die Frage, ob nicht die Polizei jene Kraft ist, die zur Aufrechterhaltung der Ordnung einzusetzen ist. Hahlweg sieht die Zuständigkeit bei der Polizei.³⁹² Dies trifft zu, wenn Ziele und Intensität der Angriffe als Beurteilungsgrundlage herangezogen werden. Wenn also Zweck und Akteur nicht eindeutig identifizierbar sind, so muss im Wege einer Kontextanalyse und unter Betrachtung der Intensität die Zuweisung der Kompetenz für diese Angriffe getroffen werden.

Liegt die Intensität in einem eng begrenzten Rahmen und führen die Aktionen im Kleinen Krieg nicht zu massiven Beeinträchtigungen der öffentlichen Ruhe und Ordnung, so ist der Einsatz von Polizeikräften durchaus angezeigt. Setzen jedoch die Kämpfe der Ruhe und Ordnung soweit zu, dass es der Polizei, auf Grund der Auswirkungen oder räumlichen Ausdehnung, nicht mehr möglich ist die Sicherheit zu gewährleisten, ist der Einsatz des Militärs notwendig, wobei die Frage der Führungsverantwortung noch nicht aufgelöst ist. Der Kleine Krieg zielt schließlich auf die Zerstörung des Ordnungsrahmens ab.³⁹³ Versuche die Intensitätsstufe dabei mathematisch exakt zu definieren sind schwierig. Die Polizei hat gegenüber dem Militär den Vorteil, dass sie ohne offenen Gegner in der Lage ist zu agieren, was besonders bei verdeckt kämpfenden Akteuren zutrifft. Das Militär hat hier seine große Schwäche, es bedarf eines erkennbaren Gegners, um effizient zum Einsatz gebracht zu werden. Der Polizei genügt ein Tatbestand, den es aufzuklären gilt.

Operativ betrachtet ist bei irregulärer Kampfweise die Polizei gegenüber dem Militär³⁹⁴ im Vorteil, dennoch fehlt es der Polizei an der Befähigung zum ultimativen Einsatz von Waffengewalt. Die Sicherheitsbehörden sind bemüht einen Rechtsbrecher seiner Strafe zuzuführen.³⁹⁵ Dies setzt eine Rechtsordnung und einen Rechtsbrecher voraus, der auf eine Bestrafung reflektiert. Doch wie steht es um Akteure, die

³⁹⁰ Galula, David: Counterinsurgency Warfare. Theory and Practice, 1964, S. 41.

³⁹¹ Vgl. ebd., S. 42.

³⁹² Vgl. Hahlweg, 1968, S. 13.

³⁹³ Vgl. ebd., S. 18.

³⁹⁴ Vgl. ebd., S. 32.

³⁹⁵ Vgl. Haltiner, 2004, S.478. (in: Gareis, 2004)

bereit sind zu sterben? Welche Strafe kann andere aus diesem Umfeld von einer Tat abhalten? In diesem Fall sind Polizeikräfte ein wenig geeignetes Mittel um die Sicherheit zu wahren.

Auf der anderen Seite sind die Verschmelzung der Irregulären mit der Bevölkerung und die nicht eindeutige Identifizierbarkeit der Kämpfer, vor allem in den ersten Phasen des Aufstandes, oder Kleinen Krieges, für eine Reaktion mit militärischen Kräften ungeeignet. Der Kleine Krieg ist, vor allem bei niedriger Intensität, in vielen Facetten von kriminellen Handlungen schwer zu unterscheiden. Die Möglichkeit für das Militär einzuschreiten richtet sich somit nach der Intensität und der Phase, in der sich der Kleine Krieg befindet. Um einen Sieg zu erreichen, ist es für den Kleinen Krieg notwendig sich zu wandeln.

„Eine Guerilla ohne geeignetes Ordnungs- und Staatsprinzip kann zwar, unter gewissen Vorbedingungen, lange in Gang gehalten werden, verkümmert aber leicht zu bloßem Bandenwesen, [...]“³⁹⁶

Grundsätzlich kann festgehalten werden, dass der Kleine Krieg eine Form des Krieges bleibt und somit Handlungsfeld des Militärs ist, die Frage bleibt nur, ab wann der Einsatz des Militärs Sinn macht. Weiter ist zu klären, ob eine auf Territorialität beruhende Unterscheidung von innen und außen noch zweckmäßig ist oder ein anderer Ansatz dieser Unterscheidung gefordert werden muss. Um die Basis für weiterführende Betrachtungen in dieser Hinsicht zu schaffen, wird nach dem Exkurs zum Kleinen Krieg das Verhältnis der Formen des Krieges zueinander tiefergehender untersucht.

5.4.4 Exkurs: Der Kleine Krieg am Beispiel der Tschetschenien-Kriege

Der Konflikt um Tschetschenien ist tief verwurzelt in der Geschichte Russlands. Seit der Kollaboration der Tschetschenen mit den Deutschen im Zweiten Weltkrieg und der darauf folgenden Deportation der gesamten Bevölkerung Tschetscheniens nach Zentralasien ist ein tiefer Bruch zwischen Tschetschenen und Russen vorhanden.³⁹⁷ Die Sippen konnten in weiterer Folge wieder zurückkehren, doch führte dies zu keinem Abbau des Misstrauens seitens der Russen und Tschetschenen. Eine gewisse Rolle dürfte auch eine potentielle Islamisierung des Kaukasus darstellen, ist doch der Anteil der Muslime in der Kaukasus-Region traditionell sehr hoch. Die föderale Integrität sowie der Erhalt des russischen „Kolonialreiches“ (Hervorhebung durch den Verfasser.) stehen im Vordergrund der Bestrebungen gegen den Zerfall der Kaukasus-Region in unabhängige Staatengebilde.³⁹⁸ Diese Einstellung der Russen führte zu den offenen Konflikten in der jüngeren Vergangenheit in und um diese Region.

Im Angesicht der umwälzenden Ereignisse, die mit dem Untergang der Sowjetunion einhergingen, versuchte Tschetschenien 1990/91, unter Führung des ehemaligen Generals Dschochar Dudajew, die Unabhängigkeit

³⁹⁶ Haffner, 1966, S. 23. (in: Tse-tung, 1966)

³⁹⁷ Vgl. Krech, Hans: Der russische Krieg in Tschetschenien (1994-1996), Ein Handbuch, 2. unveränderte Auflage, Verlag Dr. Köster, Berlin, 2000, S. 15f.

³⁹⁸ Vgl. Seiffert, Wolfgang: Wladimir W. Putin, Wiedergeburt einer Weltmacht?, Langen Müller, München 2000, S. 86.

zu erlangen. So unterzeichnete, auf dessen Druck, Tschetschenien am 31. März 1991 den neuen Föderationsvertrag nicht. Als gewählter Präsident erklärte Dudajew im November 1991 Tschetschenien für souverän und unabhängig. Unter Begleitung massiver Informationskampagnen gegen die Tschetschenen versuchte Russland eine Gegenregierung unter Führung von Ruslan Chasbulatow zu bilden.³⁹⁹

Ein Putschversuch misslang und der vorliegende Föderationsvertrag wurde erneut nicht von den Tschetschenen unterzeichnet. Daraufhin tolerierte Russland stillschweigend die einseitige Unabhängigkeitserklärung. Nach Verhängung einer massiven Wirtschaftsblockade, seitens Russlands, wurde Dudajew zunehmend kompromissbereiter und war zu einer Verhandlungslösung bereit. Russland versuchte trotzdem mit verschiedenen Methoden einen Sturz Dudajews zu erreichen. Dieser beherrschte zwar Grosny, jedoch nicht das Umland. Nach einem weiteren Putschversuch und einem missglückten Attentat auf Dudajew, drohte dieser Russland mit Krieg.⁴⁰⁰

Boris Jelzin war durch die Opposition innenpolitisch geschwächt. Er fand eine Ablenkung von seiner Schwäche in den Abspaltungstendenzen der Tschetschenen, welche er als Bedrohung für die Russische Föderation darstellte.⁴⁰¹ Russland versuchte die drohende Abspaltung der kleinen Kaukasusrepubliken und somit den Verlust des Kaukasus zu verhindern. Was auf politischer Ebene mit Verhandlungen und, von russischer Seite unterstützten, Aktionen der Opposition nicht gelang, lief zwangsläufig auf eine militärische Konfrontation hinaus.

Die Pattstellung zwischen der Opposition, welche den Großteil Tschetscheniens beherrschte, und der Nationalgarde Dudajews, welche Grosny fest in ihrer Hand hatte, drängte Russland dazu militärisch einzugreifen.⁴⁰² Dabei spielten auch wirtschaftliche Interessen eine große Rolle. So führt eine Erdöl-Pipeline von Baku durch Tschetschenien nach Noworossisk am Schwarzen Meer. Der Machtkampf um die Kontrolle der Exportwege für das Öl ist ein weiterer Mosaikstein, der zum militärischen Eingreifen Russlands in Tschetschenien geführt hat. Einen weiteren Faktor stellte der hohe Islamisierungsgrad der Kaukasus-Region dar. Dies führte zu zusätzlichen Spannungen.

Letztlich lief alles darauf hinaus Dudajew zu stürzen und ihn durch eine pro-russische Regierung zu ersetzen. Indiz dafür ist auch der Wechsel von der Lösung auf dem Verhandlungsweg, hin zu einer militärischen Lösung der Frage Dudajew. Die zunächst verdeckte Unterstützung der Opposition wandelte sich im Jahr 1994 zu einer Intervention und Übernahme der Kämpfe durch russische Streitkräfte. Es wurde ein breiter Ansatz mit Beteiligung von Verteidigungsministerium, Innenministerium und

³⁹⁹ Vgl. Krech, 2000, S. 18ff.

⁴⁰⁰ Vgl. ebd., S. 25.

⁴⁰¹ Vgl. ebd., S. 20.

⁴⁰² Vgl. ebd., S. 33ff.

Geheimdienst FSB gewählt.⁴⁰³ Oftmalige politische Richtungswechsel und eine mangelnde Informationspolitik erschwerten die Operation allerdings.

Im ersten Tschetschenien-Krieg waren die Streitkräfte nicht ausreichend auf die Operation gegen asymmetrisch agierende Kräfte vorbereitet. Trotz des Comprehensive Approach und der hohen Vernetzung waren die Joint-Fähigkeiten schwach ausgeprägt. Dies liegt vor allem darin begründet, dass die operative Führung nicht vorbereitet und eingespielt war.⁴⁰⁴ Die Planung erfolgte durch den Generalstab in Zusammenarbeit mit den anderen Ministerien.⁴⁰⁵ Das bedeutet, dass die militärstrategische Ebene für die Operationsplanung verantwortlich war. Teilweise griff der Verteidigungsminister Gratschow persönlich in Planungen ein. Die Aufstellung der operativen Führungsebene in Form der 58. Armee erfolgte erst gegen Ende des ersten Tschetschenien-Krieges.⁴⁰⁶ Die örtlich verfügbaren Kommanden des Militärdistrikts und der 58. Armee hatten nicht die Operationsverantwortung, sondern dienten dem Force Headquarter in Tschetschenien als Übermittlungsstelle. Dies führte zu einer unverhältnismäßig langen Befehlskette vom Generalstab zu den ausführenden Verbänden.⁴⁰⁷

Weiter war die Operationsplanung auf die Einnahme von Grosny ausgerichtet. Der weitere Operationsverlauf war nicht geplant worden. Eine Ausrichtung auf eine Aufstandsbekämpfung nach der Einnahme von Grosny wurde nicht vorgenommen.⁴⁰⁸ Als der Plan zur Einnahme von Grosny und zur Zerschlagung der Aufständischen nicht erfolgreich war, kippte die Operation zu Gunsten der Tschetschenen. Auch wechselte im Jahr 1995 die operative Führung von den Streitkräften zum Innenministerium.⁴⁰⁹ Die Stationierung von Truppen an der Grenze zu Tschetschenien und die Unterstützung der Opposition mit Luftmitteln der russischen Streitkräfte ist der Ausgangspunkt für das militärische Einschreiten Russlands. Die geringe Bereitschaft der einzusetzenden Truppen war ein limitierender Faktor. Es mussten aus allen Teilen der Föderation Verbände zusammengeführt werden, um die Kräfte für die Operation bereitstellen zu können.⁴¹⁰

Auf eine Einnahme der Hauptstadt waren die Landstreitkräfte nicht vorbereitet und somit konnte schon das wichtigste Operationsziel nicht erreicht werden. Erst im Februar 1995 konnte, nach verlustreichen Kämpfen, Grosny schließlich eingenommen werden. Die Phase Manöver ging in die Kulmination über, als die Rebellen Grosny aufgaben und ihre Guerilla-Kampfweise im Umland begannen. Ohne weitere Zufuhr von entsprechend ausgebildeten Truppen, war die Operation nicht mehr zu Gunsten der

⁴⁰³ Vgl. Kohlweg, Markus: Militärisches Denken in den Streitkräften der Russländischen Föderation-Ist Stand und Entwicklungstendenzen, Militärwissenschaftliche Arbeit, Universität Wien, April 2010, S. 133.

⁴⁰⁴ Vgl. ebd., S. 140.

⁴⁰⁵ Vgl. ebd., S. 129.

⁴⁰⁶ Vgl. Krech, 2000, S. 70.

⁴⁰⁷ Vgl. Boltentkov, Dimitry, Gayday, Aleksey, u.a.: Russia's New Army, Centre for Analysis of Strategies and Technologies, Moskau 2011, S. 13.

⁴⁰⁸ Vgl. Glenn, Russell W. (Hrsg.): Capital preservation. Preparing for Urban Operations in the Twenty-First Century, Santa Monica 2001, S. 22ff.

⁴⁰⁹ Vgl. Krech, 2000, S. 53.

⁴¹⁰ Vgl. ebd., S. 42f.

Russischen Föderation zu entscheiden. Dudajew vermochte sich in die Berge zurückzuziehen und nach seinem Tod⁴¹¹, im April 1996, wurde Grosny von den Tschetschenen zurückerobert.⁴¹² Der Verlust ihres Führers führte nicht zur Niederlage der Tschetschenen, da sie durch ihre Struktur der autarken Feldkommandanten in der Lage waren, weiter handlungsfähig zu bleiben.

Es kam zu Verhandlungen und einem Abkommen, welches den Krieg am 31. August 1996 für beendet erklärte. Dabei wurde eine Klärung des Status von Tschetschenien bis zum Ende des Jahres 2001 in Aussicht gestellt. Der Status Tschetscheniens blieb auch 2001 weiter ungeklärt und so setzte sich der Konflikt im zweiten Tschetschenien-Krieg fort, in dem die Russen die Lehren aus dem ersten Krieg teilweise umzusetzen wussten.⁴¹³ Die Probleme mit der asymmetrischen Kriegführung konnten jedoch nicht beseitigt werden. Auch der Wechsel der Führungsverantwortung vom Militär an den Geheimdienst konnte den Konflikt nicht entschärfen.⁴¹⁴ Die Russen setzten eine pro-russische Regierung ein, die letztlich die Tschetschenisierung des Konfliktes einleitete. Obwohl der Konflikt nicht in einem stabilen Frieden geendet hat, konnte die RF die Abspaltung Tschetscheniens verhindern.

5.4.5 Der Zusammenhang zwischen den Formen des Krieges

Die Intensität ist einer der Faktoren, die die Eskalationsstufe näher bestimmen. In den beschriebenen Konflikten liegt eine gewisse erhöhte Eskalationsstufe vor.⁴¹⁵ Der bewaffnete Konflikt hat, durch die Anwendung physischer Gewalt, bereits ein höheres Ausmaß, als Konflikte ohne Anwendung von physischer Gewalt. Nach Kahn bestimmen die Eskalationsstufe drei variable Faktoren: Die Intensität, die Ausdehnung hinsichtlich der Akteure und die räumliche Ausdehnung.⁴¹⁶ Die Intensität ist somit einer der bestimmenden Faktoren der Eskalation. Das Heidelberg Institute for International Conflict Research (HIK) definiert die Intensität eines politischen Konfliktes, zu dem auch der Krieg zählt, folgendermaßen:

„In addition to the three constituting elements – conflict actors, measures, and items – conflict intensity is an essential feature of political conflicts. A conflict intensity is an attribute of the sum of conflict measures⁴¹⁷ in a specific political conflict in a geographical area and a given space of time.“⁴¹⁸

⁴¹¹ Vgl. ebd., S. 113f.

⁴¹² Vgl. ebd., S. 122.

⁴¹³ Vgl. Krech, Hans: Der Zweite Tschetschenien-Krieg (1999-2002), Ein Handbuch, 1. Auflage, Verlag Dr. Köster, Berlin, 2002, S. 90f.

⁴¹⁴ Vgl. ebd., S. 155.

⁴¹⁵ Vgl. Kahn, Herman: On escalation. Metaphors and scenarios, New Brunswick, N. J. 2010, S. 39.

⁴¹⁶ Vgl. ebd., S. 5.

⁴¹⁷ Anm. d. Verf.: Unter conflict measures sind Handlungen und Äußerungen im Zusammenhang mit Konflikten zu verstehen, welche durch die Akteure unternommen werden.

⁴¹⁸ Bings, Felix u.a.: HIK Conflict Barometer 2011. disputes, non-violent crises, violent crises, limited wars, wars, Campus Bergheim 2012, S. 108.

Zusammen mit der räumlichen Ausdehnung und der Anzahl der Akteure spielt die Intensität eine wichtige Rolle. Je mehr Akteure und je tiefer im Gemeinwesen der Konflikt wirkt, desto intensiver ist die Auseinandersetzung und umso höher ist die Eskalationsstufe. Je breiter der bewaffnete Konflikt im Gemeinwesen wirkt, umso totaler ist der Krieg.⁴¹⁹

Der Dreh- und Angelpunkt ist der Krieg zwischen staatlichen Akteuren. Kommt zum zwischengemeinschaftlichen Krieg noch ein nichtstaatlicher Akteur hinzu, so ist eine hohe Intensität erreicht. Die Eskalationsstufe ist umso höher, je intensiver und/oder je breiter ein bewaffneter Konflikt wirkt.⁴²⁰ Dies ist der Fall, wenn sich zu einem staatlichen Akteur ein nichtstaatlicher Akteur hinzubegibt, der gemeinsam gegen einen Gegner vorgeht.

Ein Faktor, der hier mitberücksichtigt werden muss, ist die Souveränität. Souveränität ist für Staaten ein weiterer Gradmesser der Intensität von Konflikten. Ist die Souveränität eines Staates bedroht oder wird sie angegriffen, kann von einer hohen Konfliktintensität gesprochen werden. Die Souveränität kann als

„[...] Autonomie und höchste Befehlsgewalt im Inneren und nach außen als Unabhängigkeit und Gleichheit der Staaten untereinander [...]“⁴²¹

verstanden werden. Wird die Souveränität nach innen und/oder nach außen angegriffen, kann von einem für den Staat existenziellen Konflikt gesprochen werden und es ist damit die höchste Intensität angezeigt. Weiter zeigt die Definition, dass für andere Gruppierungen wohl eine Souveränität nach innen realisierbar ist, dass sie aber auf Grund fehlender Symmetrie, also Gleichheit untereinander, über keine Souveränität nach außen verfügen. Eine mögliche Souveränität nach außen ist abhängig von der Anerkennung der anderen Gruppen. Gruppen, die über keine Souveränität verfügen, können die eines Staates jedoch gefährden und angreifen.⁴²²

Unterhalb des zwischenstaatlichen Krieges liegt die Auseinandersetzung zwischen einem staatlichen und einem nichtstaatlichen Akteur, der sich von der herrschenden staatlichen Ordnung befreien möchte. Diese Stufe des Konfliktes ist ein klassischer Kleiner Krieg, der sich auf Grund der Wechselwirkung mit dem Großen Krieg und auf Grund der von Galula beschriebenen Legitimierung der nichtstaatlichen Kriegspartei hin zum zwischengemeinschaftlichen Konflikt bewegt, um dann zu einem Ergebnis zu kommen, welches im internationalen Umfeld von Bestand ist, zu einem international anerkannten Frieden.

⁴¹⁹ Vgl. Hahlweg, 1968, S. 7.

⁴²⁰ Vgl. Kahn, 2010, S. 4f.

⁴²¹ Neuhold/Hummer/Schreuer, 1991, S. 7.

⁴²² Vgl. <https://www.faz.net/aktuell/politik/politische-buecher/terrorismus-und-souveraenitaet-auch-auf-fremdem-territorium-14117751.html> [12.05.2020]

Auf der einen Seite unterstützt der Kleine Krieg den Großen Krieg⁴²³, z.B. im Falle eines Kampfes gegen einen Besatzer, und auf der anderen Seite bedarf der Kleine Krieg des Großen Krieges, z.B. im Falle des Befreiungskrieges, um zum Frieden zu gelangen.

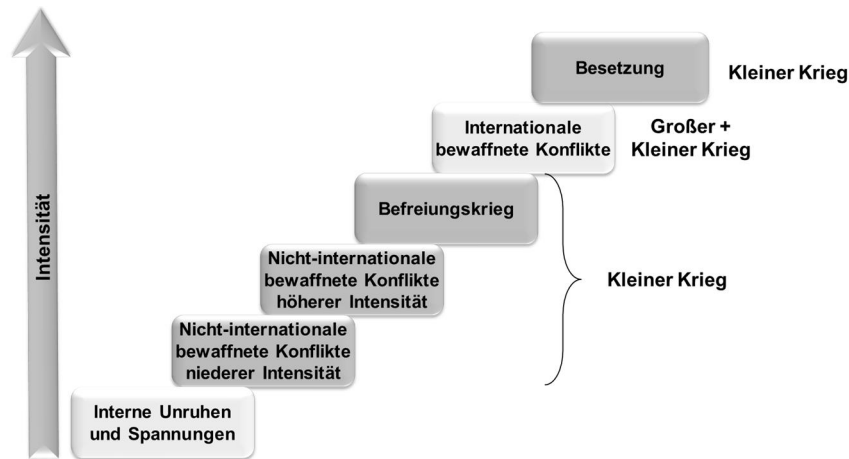


Abbildung 5: Intensität von Konflikten⁴²⁴

Die Eskalationsstufe lässt sich an der Menge der involvierten Akteure bemessen, muss aber auch die Auswirkungen mitberücksichtigen. Bezugnehmend auf die Beschaffenheit von militärischen Streitkräften erscheint die Verbindung von beiden Formen des Krieges logisch. Gerade die starre, zentralistische Ausrichtung des Militärs bietet viele Angriffspunkte für den Kleinen Krieg.⁴²⁵ Die verteilte Form des Kampfes im Kleinen Krieg zwingt den regulären Akteur sich selbst zu fragmentieren. Diese Tatsachen werden durch reguläre Streitkräfte in Form von Spezialkräften ausgenutzt.

Wird der Kleine Krieg auch oft eigenständig angewandt, so kann letztlich die Entscheidung nur über die Interaktion auf der gleichen Ebene herbeigeführt werden. Mao, der den Kleinen Krieg in der Form eines revolutionären Krieges geführt hat, strich dies besonders hervor.

„Ein revolutionärer Krieg bedeutet Geburt und Wachstum – Wachstum von einer kleinen Streitmacht zu einer großen Streitmacht, von Machtlosigkeit zur Machtergreifung, von Waffenlosigkeit zu Totalbewaffnung, von Landlosigkeit zum Besitz des ganzen Landes.“⁴²⁶

Hier zeigt sich der Zusammenhang zwischen Kleinem und Großem Krieg ganz deutlich, aber auch die Notwendigkeit, die Entscheidung im Großen Krieg zu suchen. Nur dann ist die Beendigung des Konfliktes möglich, nämlich zwischen Konfliktparteien, welche sich in einer Symmetrie befinden, die einander als Gegner anerkennen.

⁴²³ Vgl. Heuser, Beatrice: August Rühle von Lilienstern. In: Jäger, Thomas; Beckmann, Rasmus: Handbuch Kriegstheorien, Wiesbaden 2011, S. 211.

⁴²⁴ Abbildung durch den Verfasser erstellt.

⁴²⁵ Vgl. Hahlweg, 1968, S. 19.

⁴²⁶ Tse-tung, Mao: Theorie des Guerillakrieges oder Strategie der Dritten Welt, Reinbek bei Hamburg 1966, S. 20.

Um die Existenz zu sichern ist es für die Konfliktparteien notwendig aus der Asymmetrie herauszukommen und vom existenziellen in einen instrumentellen Bereich des Krieges zu wechseln.

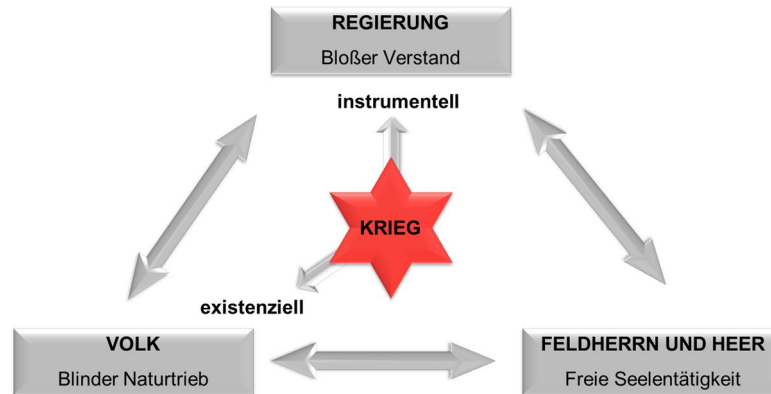


Abbildung 6: Intensität des Krieges⁴²⁷

Dies bedeutet eine Verschiebung der Intensität. Nach der Unterscheidung in völkerrechtlicher Hinsicht sind die Formen des Krieges, welche sich zwischen nichtstaatlichen Akteuren abspielen, jene niedriger Intensität und der zwischenstaatliche Konflikt jener der höchsten Intensität. In der Realität sind gerade jene Konflikte, die nicht in einem Waffengang zwischen dafür vorgesehenen Instrumenten, den regulären Streitkräften, ausgetragen werden, jene, welche für gravierendere Auswirkungen und eine höhere Intensität verantwortlich sind.

Betrachtet man die physikalische Definition der Intensität, welche besagt, dass die Intensität die aufgebrauchte Energie pro Zeit und Fläche (Anm. d. Verf.: Im Falle des Krieges ist dies gleichzusetzen mit dem Raum.) ist, muss ein Konflikt, der länger dauert und breiter wirkt, eine niedrigere Intensität aufweisen. So gesehen stimmt die Einteilung, jedoch ist ein breit angelegter Konflikt, der lange dauert, nicht mit dieser Formel von der Intensität her fassbar. Hier ist die Intensität mit der existenziellen Frage zu koppeln. Je totaler ein Konflikt ist und je länger er dauert, umso existenzieller und intensiver wird er für das Gemeinwesen. In diesem Zusammenhang tritt ein weiterer Faktor hinzu, die Komplexität. Diese steht in gegenseitiger Abhängigkeit zur Intensität von Konflikten. Dazu ist die Betrachtung der verschiedenen Ebenen des Krieges angezeigt.

5.4.6 Die Konflikintensität und die Ebenen des Krieges

Die Intensität lässt sich nicht nur an der Durchdringung des Gemeinwesens durch den Konflikt und der Form des Krieges bemessen, auch die Komplexität ist ein wesentlicher Faktor in der Betrachtung. Komplexität

⁴²⁷ Abbildung durch den Verfasser erstellt.

ist die Interdependenz der verschiedenen Bereiche eines Gemeinwesens.⁴²⁸ Diese Komplexität beeinflusst die Intensität eines Konfliktes wesentlich. Hohe Komplexität ist dabei ein Multiplikator der Intensität.

Hier ist der Blick auf die verschiedenen Ebenen der Konfliktaustragung im Rahmen eines Krieges zu richten. Diese umfassen die strategische, die operative, die taktische und die gefechtstechnische Ebene.⁴²⁹ Diesen Ebenen sind auch die entsprechenden Führungsebenen zugeordnet. Schon bei Machiavelli konnte eine Zuordnung der Ebenen, orientiert an den Römern, vorgenommen werden.

Die Personalunion von Herrscher und Feldherr vereinigte die strategische und die operative Ebene in sich. Auch wurden politische Entscheidungen direkt operativ wirksam. Machiavelli benannte diese Ebenen in seinen Werken noch nicht explizit nach heutigem Verständnis. Bei Clausewitz findet sich diese explizite Ebenenzuordnung, obwohl er diese nicht scharf voneinander trennt. Unter Strategie bei Clausewitz ist die Operation nach heutiger Sicht zu verstehen.

Die Ebenen waren in der vorindustriellen Zeit noch dichter beieinander. Ein bewaffneter Konflikt durchdrang diese Ebenen gleichermaßen und eine unterschiedliche Intensität war auf Grund der Ebenenzuordnung nicht erkennbar. Die Intensität in Verbindung mit der Komplexität drückt sich heute auf den verschiedenen Ebenen unterschiedlich aus. Auf der strategischen Ebene ist die Strategie der Ausgangspunkt der Betrachtung. Eine Strategie eines Gemeinwesens muss immer den Staatszweck im Fokus haben.⁴³⁰ Dieser liegt in der Erhaltung des Gemeinwesens und der Erreichung des Gemeinwohls. Montgomery definiert die Strategie als

„[...] die Koordinierung und Verwendung aller Hilfsquellen einer Nation oder einer Gruppe von Nationen zur Erreichung eines politischen Kriegsziels [Anm. d. Verf.: Eine Strategie verfolgt nicht nur die Erreichung eines Kriegszieles, sondern auch die Erreichung von Zielen ohne Krieg.] – das durch grundsätzliche politische Bestrebungen bestimmt wird. Das oberste Ziel der großen Strategie muß es sein, einen dauernden Frieden zu erreichen und zu sichern.“⁴³¹

Dazu sind Anstrengungen in vielen Bereichen des Gemeinwesens nötig. Die Strategie eines Staates gibt dazu den Rahmen, für alle vitalen Bereiche des Gemeinwesens, vor.⁴³² Die Komplexität steigt hier mit der Anzahl der zu berücksichtigenden Politikbereiche. Da sich diese Politikbereiche gegenseitig beeinflussen, kann die Komplexität in diesem Bereich zur Verstärkung oder zur Verhinderung von bewaffneten Konflikten führen. Eine Einwirkung auf einen bestimmten Politikbereich kann sich,

⁴²⁸ Vgl. Riemer, Andrea: Der Strategos 21. In Umbruchszeiten erfolgreich führen, Verlag Holzhausen, 2010, S.37.

⁴²⁹ Vgl. BMLVS, Dienstvorschrift für das Bundesheer, Operative Führung, 2009, S. 21.

⁴³⁰ Vgl. ebd., S. 22.

⁴³¹ Montgomery of Alamein, Bernard Law Montgomery: Kriegsgeschichte. Weltgeschichte der Schlachten und Kriegszüge, Sonderausg. Aufl., Frechen 1999, S. 14.

⁴³² Vgl. Riemer, 2010, S. 54f.

auch ohne physische Gewalt, auf mehrere oder alle anderen Politikbereiche, in einem Konflikt zwischen Gemeinwesen, auswirken.

Kriege treten im Zusammenhang mit Strategien in zweierlei Hinsicht auf: Zum einen als Weg in einer Strategie, zum anderen als Zustand einer gescheiterten Strategie. Im ersten Fall ist der Weg des Krieges, um eine strategische Zielsetzung zu erreichen, Bestandteil der Strategie, im zweiten Fall ist der Krieg Auslöser des Krisenmanagements oder der Weg innerhalb des Krisenmanagements, zur Beseitigung einer Abweichung, zu denen in einer Strategie festgelegten Zielen. Krieg ist somit einmal aktives und einmal reaktives Gestaltungsmerkmal in Bezug auf eine Strategie. Die von der hier gesprochen wird, ist die gesamtstaatliche Strategie oder die „Grand Strategy“⁴³³, wie sie im anglo-amerikanischen Raum bezeichnet wird. Die Militärstrategie ist dieser Gesamtstrategie untergeordnet.⁴³⁴

Im Agrarzeitalter waren territoriale Faktoren für den Staat von großer Bedeutung, da Land gleichbedeutend mit der Fähigkeit zum Überleben zu sehen war. Im Industriezeitalter kamen weitere Faktoren dazu, die vor allem den wirtschaftlichen und sozialen Bereich im Fokus hatten. Zur Strategieentwicklung im Informationszeitalter treten weitere Faktoren, wie z.B. die Informationssicherheit, für den Staat hinzu. Es treten verschiedene Politikbereiche in gegenseitige Abhängigkeit. Diese hohe wechselseitige Beeinflussung verschiedener Bereiche des Gemeinwesens zeigt, dass ein Konflikt auf der strategischen Ebene umfassende Auswirkungen in sich birgt. Die Intensität ist daher von anderer Qualität, wenn viele dieser verschiedenen Bereiche von einem bewaffneten Konflikt betroffen sind.

Ein strategischer, bewaffneter Konflikt ist auf der höchsten Eskalationsstufe anzusiedeln, da er einen existenziellen Charakter aufweist. Die österreichische Gesamtstrategie, in Form einer Umfassenden Sicherheitsvorsorge (USV), beinhaltet zehn Politikbereiche und ihre Teilstrategien.⁴³⁵ Daran lassen sich die verschiedenen Interdependenzen erkennen. Es geht hieraus auch klar hervor, dass das Militär nur ein Instrument von vielen für die Politik darstellt.⁴³⁶ Das lässt den Schluss zu, dass Kriege, auf der strategischen Ebene, den Charakter eines Comprehensive Approach aufweisen.

Ähnlich sind auch die Strategien anderer Staaten gestaltet.⁴³⁷ Da die Interdependenzen nicht nur innerhalb des Gemeinwesens gegeben sind, sondern die Strategien der Gemeinwesen auch zueinander in Abhängigkeit stehen, erhöht sich die Komplexität weiter. Diese gegenseitigen Abhängigkeiten können die Intensität bewaffneter Konflikte stark erhöhen. Ist also eine Abweichung zu den, in der Strategie vorgegebenen, Zielen gegeben, so entscheidet die politische Führung des Gemeinwesens, welche

⁴³³ Vgl. Vego, Milan: Operational Warfare, 2000, S. 412.

⁴³⁴ Vgl. Frank, Johann; Pucher, Johann: Österreichische Sicherheits- und Verteidigungspolitik unter geänderten Rahmenbedingungen – Chance zur Profilschärfung des Bundesheeres. In: Österreichische Militärische Zeitschrift, 5/2012, S. 554.

⁴³⁵ Vgl. BKA, Vortrag an den Ministerrat, BKA-406.200/0002-IV/6/2011, Österreichische Sicherheitsstrategie (ÖSS), Wien, März 2011, S. 1.

⁴³⁶ Vgl. Vego, 2000, S. 18.

⁴³⁷ Vgl. ebd., S. 412.

Instrumente zum Einsatz kommen, um im Rahmen des Krisenmanagements einen der Strategie entsprechenden Endzustand zu erreichen.

Die Strategie dient der Bereitstellung von Zielen, Wegen und Mitteln zur Erreichung des gewünschten Zustandes.⁴³⁸ Diese drei Begriffe stellen die strategischen Faktoren dar. Auf dieser Ebene kann das Gemeinwesen alle seine Instrumente zur Erreichung des Endzweckes einsetzen. Wie bereits festgestellt, kann der Krieg Bestandteil der Strategie eines Staates sein, er ist der Weg, der das Militär als Mittel einsetzt, um als Ziel den Frieden zu erlangen.

Obwohl die strategische Ebene die Rahmenbedingungen festlegt, gibt es auch Wirkmittel, die der strategischen Ebene in einem bewaffneten Konflikt vorbehalten sind. Der Einsatz von Nuklearwaffen stellt solch eine Möglichkeit dar. Die Auswirkungen des Einsatzes von Wirkmitteln ist aber nicht an die jeweilige Führungsebene, sondern an die Ebene des Krieges zuzuweisen, denn auf diesen Ebenen des Krieges werden die militärischen und nichtmilitärischen Mittel zur Anwendung gebracht.⁴³⁹ Dabei kann der Einsatz auf einer Ebene unmittelbare Auswirkung auf eine andere Ebene haben.

Der Einsatz von militärischen Wirkmitteln auf strategischer Ebene lässt also einen Rückschluss auf die Intensität eines Konfliktes zu. Diese Mittel sind in ihrer Wirkung besonders stark. Als Beispiel sei hier der Einsatz von Nuklearwaffen gegen Japan im Zweiten Weltkrieg genannt. Der strategische Krieg hat stets eine, das angegriffene Gemeinwesen in seiner Gesamtheit, bedrohende Wirkung. Die operative Führung setzt die Vorgaben der strategischen Führung in Anweisungen und Aufträge an die taktische Führung um. Sie erfüllt eine Scharnierfunktion zwischen Strategie und Taktik.⁴⁴⁰ Diese Ebene koordiniert zudem die verschiedenen Teilstreitkräfte.

Die eingesetzten Mittel auf dieser Ebene lassen ebenfalls einen Rückschluss auf die Intensität eines Konfliktes zu. Je breiter eine Operation angelegt ist, je mehr Elemente der unterschiedlichen Teilstreitkräfte zum Zusammenwirken gebracht werden, umso intensiver ist der Konflikt. Der bewaffnete Konflikt auf operativer Ebene ist jedoch von geringerer Intensität für das gesamte Gemeinwesen, als der auf der strategischen Ebene. Da Operationen im bewaffneten Konflikt vom Militär getragen werden, greift die Formel von der Intensität wieder. Diese ergibt sich aus der Menge an Kampfelementen (Kraft) die in einer bestimmten Zeit in einem begrenzten Operationsgebiet (Raum) zum Wirken gebracht werden.

Diese drei, die Intensität auf der operativen Ebene beschreibenden Größen, sind die operativen Faktoren, die die Basis für den Einsatz von militärischen Kräften auf der operativen und taktischen Ebene darstellen. Die Beurteilung für einen Einsatz des Militärs richtet sich an diesen Faktoren aus. Die Operation führt die Kräfte in Zeit und Raum zusammen.⁴⁴¹ Die

⁴³⁸ Vgl. Riemer, 2010, S. 54.

⁴³⁹ Vgl. Vego, 2000, S. 17.

⁴⁴⁰ Vgl. Freudenberg, 2008, S. 65.

⁴⁴¹ Vgl. ebd., S. 65f.

Taktik ist für die Operation das Mittel, dem Gegner den eigenen Willen aufzuzwingen. Die der Taktik untergeordnete gefechtstechnische Ebene ist jene, in der die Wirkung, an bestimmten Verfahren orientiert, ihr Ziel erreicht.

Diese Ebene des Krieges ist jene, in der die physische Gewalt unmittelbar zur Anwendung kommt. Diese unmittelbare Gewaltausübung stellt aus Sicht der militärischen Kräfte den höchsten Intensitätsgrad dar, obwohl der Raum noch begrenzter ist als auf den Ebenen darüber, ist die Intensität im Gesamtzusammenhang aber geringer. Wichtig ist es hier nochmals klar zu stellen, dass die Ebenen des Krieges nicht deckungsgleich mit den militärischen Führungsebenen sind.⁴⁴² Die Intensität ist immer in Zusammenhang mit den anderen bestimmenden Faktoren zu sehen. Dabei geht es darum, welche und wie viele Akteure in welchem Raum über welche Zeit zum Einsatz gebracht werden.⁴⁴³

Über diesen Zusammenhang ist die Intensität umso schwerer nur rein militärisch ableitbar, je höher die Ebene der Kriegführung ist. Hier fließen die Komplexität und die Eskalation mit ein. Je umfassender, also nicht nur auf einen begrenzten Raum gerichtet, ein Angriff erfolgt, je mehr andere Politikbereiche betroffen sind, umso mehr eskaliert der Konflikt und umso totaler wird der Krieg. Die Intensität für das gesamte Gemeinwesen steigt dadurch, da jeder in diesen Konflikt involviert werden kann. Werden also alle Instrumente der gegnerischen Politik zum Ziel der physischen Gewalt des Militärs, so wird der Krieg ein totaler sein. Ähnlich wie in den bewaffneten Konflikten, die zwischen nichtstaatlichen und staatlichen Akteuren stattfinden, kommt es zu einer Entgrenzung nach außen, bei der die Intensität für das Gemeinwesen steigt. Die Entgrenzung, die räumliche Ausdehnung, ist somit auch ein Faktor, der die Intensität eines bewaffneten Konfliktes beeinflusst.

Zusammengefasst ist festzuhalten, dass für die Bestimmung der Intensität des Krieges mehrere Faktoren ausschlaggebend sind. Es sind dies zum einen die Formen des Krieges, die von gehegtem zu entgrenztem Konflikt durch die Intensität beeinflusst werden. Die Breite, besser gesagt die Ausdehnung des Konfliktes, spielt hier die entscheidende Rolle. Weiter ist die Ebene, in der sich der Krieg darstellt, ein Gradmesser für die Intensität. Die Anwendung von militärischen Mitteln, auf der strategischen Ebene, hat eine wesentlich weitreichendere Wirkung und führt zu einer anderen Qualität der Intensität.⁴⁴⁴ Das Ziel ist vom Umfang her größer. Je größer das Ziel ist, umso höher ist die Ebene des Krieges.

Militärische und nichtmilitärische Mittel können auf der strategischen Ebene gegen mehrere Instrumente des gegnerischen Gemeinwesens gleichzeitig wirken. Dazu kommt der Faktor der Komplexität, der eine treibende Wirkung und somit Einfluss auf die Eskalation, als Folge einer Intensivierung des Konfliktes, haben kann. Komplexe Abhängigkeiten können einen Konflikt einerseits verhindern oder andererseits dahingehend

⁴⁴² Vgl. Vego, 2000, S. 17ff.

⁴⁴³ Vgl. BMLVS, Dienstvorschrift für das Bundesheer, Operative Führung, 2009, S. 59ff.

⁴⁴⁴ Vgl. Vego, 2000, S. 24.

verstärken, dass, auf Grund dieser Abhängigkeiten, eine Beeinflussung verschiedener Bereiche eines Gemeinwesens stattfinden kann. Ein Einwirken mit, aber auch ohne, militärische Mittel auf einen Politikbereich des Gegners, kann diesen, auf Grund der Komplexität, schon zur Aufgabe zwingen.

Für den Einsatz von militärischen Streitkräften ist der Intensitätsfaktor ein bestimmender. Je intensiver sich ein Konflikt gestaltet – das heißt je breiter die Wirkung bewaffneter Gewalt wirkt – und je höher die Eskalationsstufe ist, desto mehr ist der Einsatz des Militärs angezeigt. Hier geht es um die Verteidigung der Ordnung bzw. deren Wiederherstellung, beides Aufgaben, die die Polizei nicht erfüllen kann. Allerdings je höher die Ebene der Kriegführung, umso mehr Instrumente des Gemeinwesens treten hinzu. Im Zusammenhang mit der Intensität von Konflikten ist die Auseinandersetzung mit den Mitteln des Militärs notwendig. Im Lauf der Geschichte haben sich diese Mittel fortentwickelt und ebenso hat sich die Kriegführung dadurch gewandelt. Dies wird im Folgenden nun näher dargestellt.

5.5 Zu den Methoden und Mitteln des Krieges

Drei Bereiche im bewaffneten Konflikt haben sich im Laufe der Zeit gegenseitig beeinflusst und weiterentwickelt, die Technologie, die Verfahren und die Organisation von Streitkräften. Technologisch hat das Militär immer schon die Entwicklung vorangetrieben und damit auch wesentlich die zivile Welt beeinflusst. Selbst hat sich das Militär an den technologischen Fortschritt, durch Anpassung von Methoden der Kriegführung und Veränderung der Organisationsform, angepasst.

Im folgenden Abschnitt werden die wesentlichen Entwicklungsschritte und deren Auswirkung auf das Militär in Bezug auf den Krieg dargestellt. Die Betrachtungen auf den Wandel der Kriegführung beschränken sich mit Masse auf den Landkrieg, weil dieser letztlich die Entscheidung bringt. Es geht dabei nicht um eine lückenlose Darstellung aller Entwicklungsschritte, sondern um die Abbildung und Bewertung der Entwicklungstendenzen, es geht darum wie Krieg geführt wird.

5.5.1 Folgerungen für die Kriegführung aus dem Dreißigjährigen Krieg

Seit der Mensch Konflikte austrägt, nutzt er zur Ausübung der Gewalt in physischer Form Hilfsmittel. Diese Hilfsmittel vergrößern die Wirkmöglichkeiten des Menschen. Diese Hilfsmittel werden als Waffen bezeichnet. Die Urform einer Waffe ist der Mensch selbst. Rid führt dazu Folgendes aus:

„The body is also the first instrument of violence, the first weapon.“⁴⁴⁵

Dennoch wird der Mensch als solcher nicht als Waffe im eigentlichen Sinn verstanden, sondern Gegenstände die als Waffen Gebrauch finden. Eine

⁴⁴⁵ Rid, 2013, S. 18.

Waffe erlaubt es dem Individuum seine Kraft zu steigern und den Gegner zu behindern, zu verletzen oder zu töten. Im Waffengesetz ist die Waffe folgendermaßen definiert:

„Waffen sind Gegenstände, die ihrem Wesen nach dazu bestimmt sind, 1. die Angriffs- oder Abwehrfähigkeit von Menschen durch unmittelbare Einwirkung zu beseitigen oder herabzusetzen [...].“⁴⁴⁶

Im Laufe der Zeit haben sich die Waffen gewandelt. Technologisch bedeutend und bis in die heutige Zeit reichend, ist die Entwicklung des Schießpulvers.⁴⁴⁷ Nach Bogen und Armbrust ist es somit möglich geworden große Reichweite mit Durchschlagskraft zu verbinden. Als Wendepunkt in der Anwendung der darauf basierenden Waffen, der Kanone und dem Gewehr, kann das 17. Jahrhundert betrachtet werden.

Geprägt war diese Zeit vor allem durch die ausgedehnten Kriege zu Beginn des Jahrhunderts und die darauf aufbauende Staatenordnung, sowie die bis in die heutige Zeit reichenden Entwicklung von rechtlichen Normen zur Einhegung des Krieges. Der Beginn der modernen Taktik und die Verwendung von Feuerwaffen können als Paradigmenwechsel in der Kriegführung angesehen werden.⁴⁴⁸ In dieser Zeit war die Heeresorganisation auf Berufsheere, also Söldnerheere, ausgerichtet.

Im Dreißigjährigen Krieg wurde erstmals eine Art totaler Krieg geführt. Die Größe der Streitkräfte erforderte die Versorgung aus dem Land heraus und so wurde die Bevölkerung mit in die Kriegswirren gestürzt. Die Taktik, die in diesem Krieg angewandt wurde, war eine offensive. Es wurden der Feind und die Entscheidung gesucht. Krieg war ein Mittel zur Machtvergrößerung und so war der Dreißigjährige Krieg, zwar ausgelöst durch eine konfessionelle Streitigkeit, letztendlich ein Krieg um die Vorherrschaft in Europa.

Organisatorisch schafften die Schweden unter Gustav Adolf ein Volksheer,⁴⁴⁹ welches nicht nur von der Ausbildung her, sondern auch moralisch, den Söldnerheeren der Habsburger überlegen war.⁴⁵⁰ Bessere Ausbildung und Disziplin gipfelten in neuen Möglichkeiten bei den Verfahren, mit denen die Schweden in das Gefecht zogen. Sie kombinierten hohe Beweglichkeit mit der Feuerkraft ihrer Waffen. Die Hauptträger der schwedischen Taktik waren die Infanteristen.⁴⁵¹ Ergänzt und unterstützt wurden diese durch Artillerie und Kavallerie.⁴⁵² Es waren die Grundzüge der modernen Taktik bereits gegeben, die sich als Einsatz der verbundenen Waffen versteht.⁴⁵³

⁴⁴⁶ § 1, Bundesgesetz über die Waffenpolizei (Waffengesetz 1996 – WaffG) BGBl. I Nr.12/1997 idF BGBl. I Nr. 97/2018.

⁴⁴⁷ Vgl. Montgomery, 1968, S. 190.

⁴⁴⁸ Vgl. ebd., S. 263.

⁴⁴⁹ Vgl. Keegan, John: Die Kultur des Krieges, 2. Aufl., Reinbek bei Hamburg 2001, S. 486.

⁴⁵⁰ Vgl. Montgomery, 1968, S. 266.

⁴⁵¹ Vgl. ebd., S. 271.

⁴⁵² Vgl. Münkler, 2010b, S. 43.

⁴⁵³ Schadenböck, Dieter: Von der Taktik der Landstreitkräfte, Landesverteidigungsakademie, Wien 2013, S. 69.

Durch Gustav Adolf wurde eine lineare Aufstellung als Schutz vor der Artillerie eingeführt, welche sich, auch nach dem Dreißigjährigen Krieg, als Haupttaktik etablieren sollte. Bei der Schlacht von Breitenfeld kam es zum Aufeinandertreffen zweier grundlegend verschiedener Taktiken. Montgomery beschreibt dieses Aufeinandertreffen folgendermaßen:

„Das eine [taktische Konzept] gründete sich auf Stoßkraft des Massenangriffs, das andere auf die Beweglichkeit. Wieder einmal stand die Phalanx der Legion gegenüber.“⁴⁵⁴

Gustav Adolf darf als einer der großen Militärreformer begriffen werden, welche die Kriegführung maßgeblich beeinflusst haben. Er schaffte es, die wesentlichen Eigenschaften eines Heeres, Feuerkraft, Beweglichkeit und Stoßkraft, miteinander zu kombinieren. Das Ende des Dreißigjährigen Krieges leitete auch das Ende der großen Söldnerheere ein. Die neuen Taktiken erforderten disziplinierte und gut ausgerüstete Soldaten, es entstanden die stehenden Wehrpflichtigen-Heere.

Die Kavallerie bereitete den Einsatz der Infanterie vor und die Artillerie unterstützte diesen. Den entscheidenden Stoß führte wieder die berittene Truppe aus. Es war ein Zusammenwirken der Feuerkraft der Infanterie und der Stoßkraft der Kavallerie. Die Gevierthaufen der Landsknechte wurden durch eine aufgelockerte Aufstellung mit berittenen Reserven abgelöst. Wendigkeit wurde zu Gunsten der Kraft der Masse gewonnen. Die gemischte lineare Aufstellung vereinigte Feuerkraft, Beweglichkeit und Stoßkraft miteinander. Die Feuerkraft führte zur Herausbildung der Lineartaktik.

5.5.2 Die Kriegführung als angewandte Politik

Der Bedeutungswechsel zwischen der Kavallerie und den Fußtruppen kam mit der Einführung des Bajonetts. Die Pikeniere, die die Fußsoldaten beim Nachladen vor der Reiterei schützen mussten, wurden überflüssig. Hier zeigt sich wieder der Einfluss der Technologie auf die Organisation und die Verfahren des Militärs. Die gewonnene Beweglichkeit führte dazu, dem Gegner die Schlacht, zu einer günstigen Zeit, an einem günstigen Ort, aufzuzwingen. Neben der offensiven Einsatzführung entwickelten sich auch defensive Methoden weiter, wie der Festungsbau der Franzosen am Ende des 17. Jahrhunderts zeigt.⁴⁵⁵

Entscheidungen wurden in dieser Epoche immer mit, in Zeit und Raum konzentrierten, Kräften gesucht. Dies mag darin begründet sein, dass der vierte operative Faktor, die Information, durch eine langwierige Übermittlung, noch keine Rolle spielte. Es mussten die Truppen in einem Raum zum Zusammenwirken gebracht werden, weil es keine Möglichkeit gab, mit Informationsübertragungsmitteln eine räumlich getrennte Operationsdurchführung zu ermöglichen. Dies stellte auch besondere Herausforderungen an die Führung der Streitkräfte in einem Krieg.⁴⁵⁶ Die

⁴⁵⁴ Montgomery, 1968, S. 273.

⁴⁵⁵ Vgl. ebd., S. 295.

⁴⁵⁶ Vgl. Keegan, 2001, S. 487f.

Befehlshaber waren auf sich gestellt und hatten oft die Aufgabe als Diplomaten und Politiker zu agieren. Weiter wurden die Verfahren und Gefechtsabläufe komplexer, so dass die Offiziere besser ausgebildet sein mussten.

Im 18. Jahrhundert wandelte sich die Kriegführung zu einem politischen Instrument, wie es Clausewitz verstanden hat. Es wurde Krieg geführt, nicht um den Gegner zu vernichten, sondern um politische Entscheidungen, mit begrenzten Zielen, herbeizuführen. Es war die Zeit der Kabinetts-Kriege und der Manöverkriegführung.⁴⁵⁷ Dabei handelte es sich um symmetrische Kriege zwischen regulären Armeen. Waffentechnisch entwickelte sich die Artillerie weiter, die Kolonnentaktik löste am Ende dieses Jahrhunderts die Lineartaktik ab und damit verlor das Manöver seine Bedeutung zu Gunsten der Entscheidung in der Schlacht.⁴⁵⁸ Der Gegner sollte in der Schlacht vernichtet werden. Diese offensive Taktik wurde von Napoleon perfektioniert. Er verstand es, seine Truppen rasch und präzise zu bewegen und in einer gemischten Aufstellung, Line mit Kolonne, zu kombinieren.

Zunächst beschäftigte die Vorhut den Gegner, dann wurde durch die Linie der Einsatz der Kolonne vorbereitet, diese führte die Entscheidung. Es war die Verbindung von Feuerkraft und Stoßkraft.⁴⁵⁹ Der Träger des Kampfes war bei Napoleon die Infanterie, welche durch die Artillerie unterstützt wurde. Diese zog Napoleon zusammen und brachte deren Feuerkraft geschlossen zum Einsatz, um Lücken für den Durchbruch der Infanterie zu schaffen. Der Kavallerie gab er neue Aufgaben auf dem Gefechtsfeld, wie die Aufklärung oder Sicherung, welche bei Decker als Kleiner Krieg bekannt wurden.⁴⁶⁰ Napoleon war aber mit seiner Einbindung des Volkes in die Kriegführung indirekt der Wegbereiter des totalen Krieges und somit auch der asymmetrischen Kriegführung.

Die Wehrpflicht und die Industrialisierung im 19. Jahrhundert führten vom Krieg der Kabinette, über die Französische Revolution, hin zu den Kriegen der Nationen.⁴⁶¹ Die Bevölkerung wurde somit wieder zu einem wichtigen Bestandteil im Krieg. Die Fertigung von Waffen in großem Stil brachte eine Qualitätsverbesserung derselben mit sich. Tapferkeit und quantitative Überlegenheit hatten nun keine Chance mehr gegenüber der Disziplin und den modernen Waffen.⁴⁶² Da es im Zuge der Revolten im Jahre 1848 zu einer Reduktion der stehenden Heere, auf kleine Berufsarmeen, kam, spielten Technologieentwicklung, Mobilmachung und Transport eine immer größere Rolle. Damit ging auch die gesteigerte Bedeutung der Planung von Kriegen einher.

⁴⁵⁷ Vgl. Münkler, 2010b, S. 52.

⁴⁵⁸ Vgl. Montgomery, 1968, S. 330.

⁴⁵⁹ Vgl. ebd., S. 346.

⁴⁶⁰ Vgl. Decker, 1844, S. 122f.

⁴⁶¹ Vgl. Münkler, 2010b, S. 52.

⁴⁶² Vgl. Montgomery, 1968, S. 413.

5.5.3 Die Hochtechnologie und ihr Einfluss auf die Kriegführung

Im Krimkrieg wurde erstmals die Telegraphie in einem Krieg zur Informationsübertragung genutzt, damit hielt der operative Faktor Information Einzug in die Operationsführung.⁴⁶³ Die Kombination aus Verbindungsmittel und Feuerkraft führte zur Auflockerung im Operationsgebiet. Die Einführung von Granaten für die Artillerie und die Umrüstung der Marine auf Dampfschiffe sind weitere technologische Fortschritte in der Kriegführung dieser Zeit. Die Entwicklung der Unterseeboote und deren Einsatz im Amerikanischen Bürgerkrieg stellen marinetechnisch einen Meilenstein dar. Die Massenproduktion brachte die Waffentechnologie schneller in Umlauf und steigerte damit die Bedeutung der Logistik.

Im 20. Jahrhundert wurde die Kriegführung zunächst von der Erfindung des Maschinengewehrs und vom Stacheldraht beherrscht.⁴⁶⁴ Der Erste Weltkrieg wurde zu einem Stellungskrieg, in dem viele technologische Neuerungen hervorgebracht wurden. Hier sei als erstes die Luftwaffe genannt, welche zunächst noch als Aufklärungsmittel eingesetzt wurde. Der Einsatz von Gas, als Mittel im Grabenkrieg, zeigt die unterschiedslose Wirkung desselben und führte schließlich zu dessen Ächtung. Die Kavallerie ist, für die Herbeiführung der Entscheidung in einem Stellungskrieg mit massivem Artillerieeinsatz und der Verwendung von Maschinengewehren, völlig unbrauchbar.⁴⁶⁵ An ihre Stelle tritt die Panzerwaffe, die in diesem Krieg erste Erfolge verzeichnen kann.

Im Zweiten Weltkrieg findet eine neue Taktik ihre Anwendung, die des schnellen Bewegungskrieges, der Blitzkrieg.⁴⁶⁶ Getragen wird dieses Verfahren durch die Kombination von mechanisierten Kräften, mit entsprechenden Kommunikationsmitteln, und dem Einsatz von Luftmitteln. Die Luftwaffe führt zur Ausformung eines totalen Krieges. Einrichtungen, die hinter der Front liegen, wie die Produktionsstätten der Kriegführenden, werden nun zum Ziel.⁴⁶⁷ Die strategische Bombardierung ist ein Mittel des totalen Krieges geworden. Der Kampf um und mit Informationen wird immer wichtiger.⁴⁶⁸ Radar, Funkaufklärung und Kryptologie sind nur einige Schlagworte, die in diesem Krieg eine wichtige Rolle spielen.

Auf Grund der Erfolge in diesem Bereich gelingt es den Alliierten den U-Boot-Krieg im Atlantik zu beenden.⁴⁶⁹ Die Entwicklung eines Computers zur Dechiffrierung der deutschen Enigma ist der wesentliche Entwicklungsschritt in das Informationszeitalter. Durch die Entwicklung der Nuklearwaffen und deren Einsatz im Zweiten Weltkrieg wurde deren Vernichtungspotential offenbar. Dies führte zum Kalten Krieg, in dem, durch das potentielle Vernichtungsreservoir, eine neue Art des Krieges

⁴⁶³ Vgl. Beauchamp, K. G.: History of telegraphy, London 2001, S. 103ff.

⁴⁶⁴ Vgl. Keegan, 2001, S. 511.

⁴⁶⁵ Vgl. Eimannsberger, Ludwig: Der Kampfwagenkrieg, München 1934, S. 20.

⁴⁶⁶ Vgl. Keegan, 2001, S. 522.

⁴⁶⁷ Vgl. Douhet, 1935, S. 23.

⁴⁶⁸ Vgl. Keegan, 2001, S. 528.

⁴⁶⁹ Vgl. Johnson, Brian: Streng Geheim. Wissenschaft und Technik im 2. Weltkrieg, Stuttgart 1983, S. 210f.

hervortrat.⁴⁷⁰ Die Atommächte konnten nicht direkt in einem Krieg aufeinandertreffen, ohne die Gefahr der Vernichtung der Menschheit, so führten sie Stellvertreter-Kriege.⁴⁷¹ Diese Art des Krieges war vielfach von asymmetrischen Kampfweisen gekennzeichnet.

Technologie führte zu neuen Verfahren und diese brachten wiederum neue Technik zum Vorschein. Durch Kriege wurde eine Entwicklungsspirale in Gang gesetzt, die sich nach wie vor weiterdreht. Der Zusammenhang zwischen Krieg und technologischer Entwicklung ist klar erkennbar. Einerseits führt Krieg zu technologischem Fortschritt, andererseits führt Technologie zu neuen kriegerischen Auseinandersetzungen. Die Möglichkeiten ferngesteuerte Waffensysteme einzusetzen, ist der letzte große Entwicklungsschritt, der die Entgrenzung von bewaffneten Konflikten weiter vorantreibt.⁴⁷² Die vernetzte Operationsführung bringt Sensoren, Führungseinrichtungen und Wirkmittel in einen, nicht mehr von Entfernungen beeinflussten, Zusammenhang. Diese Systeme schaffen aber nicht nur neue Einsatzmöglichkeiten, der Drohnenkrieg in Afghanistan und Pakistan dient hier als Beispiel, sondern ermöglichen es nur noch Staaten diese komplexen Waffensysteme zu betreiben.

Mit der Verwendung von neuen Technologien stieg der Kostenfaktor an. Personal und Material kosteten erhebliche finanzielle Ressourcen.⁴⁷³ Dies ist ein Grund, warum zusehends die Kriegsführungsfähigkeit, vor allem mit hochkomplexen Waffensystemen, an den Staat überging, es kam vordergründig zu einer technologischen Entprivatisierung des Krieges und zu einer Förderung der Asymmetrie in kriegerischen Auseinandersetzungen. Gleichzeitig bringt die Technologisierung der Streitkräfte auch einen Effekt zu Tage, der es auch nichtstaatlichen Akteuren ermöglicht auf moderne Technik zurückzugreifen.

Die Staaten waren teilweise gezwungen, um die eigenen komplexen Systeme zu beschaffen, weniger komplexe Systeme an „potentielle Gegner der Zukunft“ (Hervorhebung durch den Verf.) zu verkaufen. Auch die Abfallprodukte der militärischen Entwicklung finden den Weg zum einfachen Bürger und bringen ihm nicht nur die Vorteile dieser Systeme, sondern steigern Abhängigkeiten und Verwundbarkeit der Menschen. Sie steigern aber auch die Möglichkeiten selbst an Konflikten mitwirken oder teilhaben zu können.⁴⁷⁴ Durch die Entwicklung neuer Technologien entstehen immer neue Interaktionsräume und somit auch Räume, in denen Konflikte zur Austragung gelangen. Diese technologische Entwicklung bringt somit auch neue Arten und Formen des Krieges zum Vorschein.

Abhängig war die Evolution des Krieges, seiner Mittel und Methoden deshalb stets von dem Umfeld in dem die kriegerischen Auseinandersetzungen stattfanden und weiterhin stattfinden. Der Computer ist hier die, unsere Welt am nachhaltigsten beeinflussende, Errungenschaft

⁴⁷⁰ Vgl. Keegan, 2001, S. 535.

⁴⁷¹ Vgl. Barnett, Thomas: The Pentagon's New Map, War and Peace in the Twenty-First Century, New York 2004, S. 80.

⁴⁷² Vgl. Byung-Chul Han: Clausewitz im Drohnenkrieg. In: Die Zeit vom 15.11.2012, S. 60.

⁴⁷³ Vgl. Keegan, 2001, S. 493.

⁴⁷⁴ Vgl. Barnett, 2004, S. 85.

des Militärs.⁴⁷⁵ Kommunikation wurde durch ihn für alle Menschen, unabhängig von Entfernungen, möglich. Es entstand ein Informationsraum und wie in allen Räumen, die sich der Mensch erschließt und in denen er in Interaktion zu anderen Menschen tritt, wird auch der Informationsraum zum Konfliktfeld.

Im Folgenden geht es darum, abseits des Cyberspace – dieser wird im nächsten Hauptkapitel genauer analysiert – der Rolle des Faktors Raum für den Krieg auf den Grund zu gehen. Die Beschreibung der verschiedenen Dimensionen des Krieges und deren Rolle im Gesamtsystem des bewaffneten Konfliktes beschließen die Auseinandersetzung mit dem Begriff des Krieges und schaffen so die Basis zur weiteren Erarbeitung des Begriffes vom Phänomen des Cyberwar.

5.6 Zum Faktor Raum im Krieg

Krieg wird in verschiedenen Räumen, den Dimensionen oder Domänen der Kriegführung, geführt. Diese Dimensionen haben unterschiedliche Bedeutung für den Krieg. Es gibt Bereiche, die für den Krieg entscheidend sind, andere haben nur eine Unterstützungsfunktion. Die Räume sind nicht voneinander zu trennen, sie wirken ineinander.⁴⁷⁶

Kriege werden vor allem an Land, auf See und in der Luft geführt. Auch der Weltraum wird militärisch genutzt, ohne dort aber unmittelbar kriegsgerichtete Handlungen zu setzen. Die verschiedenen Eigenschaften dieser Räume haben eine Auswirkung auf deren Bedeutung für den Menschen. Welche Bedeutung die klassischen Dimensionen für den Krieg haben, soll im Folgenden dargestellt werden, um den Cyberraum im Anschluss dazu richtig in Bezug setzen zu können.

5.6.1 Land als erste Dimension des Krieges

Menschen leben an Land und daher hat diese Dimension für den Krieg eine wesentliche Bedeutung. Kriege wurden zuerst an Land geführt. Land war als Ressource stets ein wichtiger Bestandteil unserer Erde. Es ernährt die Menschheit und liefert uns Rohstoffe, um unser Leben bestmöglich zu gestalten. Land gilt seit jeher als Sinnbild für Reichtum. Der Mensch benötigt einen Platz zum Leben und den liefert der Erdboden. Macht ist immer mit Ressourcen gekoppelt, Ressourcen, die aus dem Land gewonnen werden. Gemeinwesen sind abhängig von einem Territorium.

Heute werden Kriege nicht ausschließlich an Land geführt, die militärische Nutzung anderer Dimensionen ist hinzugekommen. Der Kampf auf See und in der Luft ist als Unterstützungsmaßnahme des Landkrieges hinzugekommen.

⁴⁷⁵ Vgl. Johnson, 1983, S. 363ff.

⁴⁷⁶ Vgl. USAF, Air Force Doctrine Document, Cyberspace Operations, 2010, S. 20.

„Die strategische Entscheidung, bei einem voll ausgekämpften Krieg oft auch das letzte Gefecht, wird immer um einen terrestrischen Raum ausgefochten und dies vor dem Hintergrund einer stetigen Urbanisierung und dem Erfordernis nach Schutz vor überlegenen westlichen Luftstreitkräften verstärkt in bebautem Gelände.“⁴⁷⁷

Der Kampf an Land ist geprägt durch das physische Umfeld, die unmittelbar auf Streitkräfte einwirkenden Gefahren und Bedrohungen, die Bevölkerung und schließlich durch die Einwirkung verschiedenster anderer Akteure. Diese Charakteristika sind dem Landkrieg eigen. Vor allem die Komplexität des Umfeldes erfordert eine Ausrichtung der Streitkräfte darauf. Schon Napoleon hat in seinem Russland-Feldzug die Weite des Landes und die klimatischen Bedingungen nicht richtig einzuschätzen gewusst. Dazu kamen Bedrohungen durch Nahrungsmittelknappheit und die Gefahr durch nachstoßende russische Truppen beim Rückzug.

Die Bevölkerung und deren rechtlicher Schutz im Krieg tragen zur Komplexität an Land bei, ebenso wie der mögliche Einsatz anderer Akteure, seien es Hilfsorganisationen oder aber andere bewaffnete Gruppierungen im Einsatzraum. Afghanistan ist hier ein aktuelles Beispiel, oft sind Akteure, welche gegen die Streitkräfte vorgehen, von der normalen Bevölkerung nicht zu unterscheiden. Dies erschwert die Bekämpfung solcher Akteure und zwingt das Militär nur zu reagieren.

Landstreitkräfte können nur durch andere Landstreitkräfte geschlagen werden. Land ist im Krieg die Ressource, um die es letztlich geht und nur Landstreitkräfte sind in der Lage Land zu erobern und auch gegen Angriffe zu halten. Auch massives Feuer, durch zum Beispiel Luftstreitkräfte, ist nicht in der Lage Land zu besetzen und zu halten.

„Remotely delivered firepower, even on a massive scale, has rarely proved capable of ejecting determined troops from terrain they occupy.“⁴⁷⁸

Weiter ermöglichen Landstreitkräfte den Einsatz anderer Akteure und stellen dadurch ein wesentliches politisches Signal dar. Durch den Krieg an Land wird ein komplexes und höchst dynamisches Umfeld generiert. In diesem ist es vielen, auch irregulären Akteuren, möglich in den Konflikt einzuwirken. Durch die Interaktion, welche unmittelbar erfolgt, mit der Bevölkerung und allen anderen Akteuren, ist der Landkrieg mit höchster Komplexität versehen. Das Land ist die Grundlage für die menschliche Existenz.

„Denn als Objekt wie als Voraussetzung politischen Handelns ist das Land unersetzlich, als Träger wichtiger Ressourcen, als Wirtschaftsraum und vor allem als Staatsgebiet, das heißt als

⁴⁷⁷ Mey, Holger: Zur Entwicklung der modernen Kriegführung. In: Reiter, Erich: Jahrbuch für internationale Sicherheitspolitik 2001, S. 19.

⁴⁷⁸ NATO, Allied Joint Doctrine for Land Operations, 2009, Chapter 1, S. 4.

physische Grundlage eines Staatswesens, seiner Eigenständigkeit und Handlungsfähigkeit.“⁴⁷⁹

Der Erfolg in einem Krieg kann nur an Land nachhaltig erzielt werden, die anderen Dimensionen der Kriegführung leisten dazu ihren Beitrag, im Grunde ist jede Kriegführung eine Landkriegführung.⁴⁸⁰ Neben dem Krieg an Land hat der Seekrieg die zweitlängste Tradition.

5.6.2 See als zweite Dimension des Krieges

Anders als der Landkrieg hat der Seekrieg vor allem eine ökonomische Dimension. Durch Krieg auf See kann eine indirekte Wirkung auf den Krieg als solches erzielt werden. Es geht um Kommunikationslinien, die für Nachschub genutzt werden. Die Invasion in der Normandie wäre ohne eine Versorgung und einen Aufmarsch über See nicht durchführbar gewesen.

Das Meer wird zwar vom Menschen nicht direkt bewohnt, ist aber ein geographisches Schlüsselement. Die Erde ist zu über 70 Prozent mit Wasser bedeckt.⁴⁸¹ Der Krieg auf dem Wasser hat also einen klar unterstützenden Charakter. Mit dem Einsatz von Seestreitkräften kann eine weltweite Machtprojektion und die Unterstreichung eines politischen Willens erzielt werden. Der Krieg auf See hat somit mitunter eine strategische Dimension. Auf Grund der freien Nutzung der hohen See ist es den Seestreitkräften möglich, die Operationsentfernungen zwischen Gemeinwesen zu verkürzen.

Die Vorkommen von Ressourcen im Meer haben die Bedeutung für die Gemeinwesen weiter erhöht, wobei sie nicht an die des Landes heranreichen. Durch die verschiedenen technologischen Entwicklungen wurde das Meer zu einem multidimensionalen Kampfgebiet. Seekrieg spielt sich über, auf und unter dem Wasser ab.⁴⁸² Die Rolle für die Unterstützung der Landkriegführung lässt sich aus der Tatsache ableiten, dass 90 Prozent der Menschen in Küstennähe leben und daher der Kampf an Land ebenfalls im Einflussbereich von Seestreitkräften liegen wird.⁴⁸³

Der wesentliche Unterschied zum Landkrieg liegt in der Komplexität, denn außer dem Wetter gibt es hier keine variierenden Faktoren, vor allem nicht in der Interaktion mit anderen Akteuren. Diese ist nicht so unmittelbar wie an Land. Auf Grund der physikalischen Eigenschaften des Meeres, aber vor allem, weil effektive Waffensysteme nur durch Staaten beschaffbar und auch einsetzbar sind, kommen andere als staatliche Akteure im Seekrieg kaum zum Tragen. Dies reduziert die Komplexität.

„However, skilfull seamanship and tactics can help to minimize these effects, and the inherent mobility of maritime forces may allow them to move to an area the conditions are more favourable.“⁴⁸⁴

⁴⁷⁹ Mey, 2001, S. 19. (in: Reiter, 2001)

⁴⁸⁰ Vgl. Freudenberg, 2008, S. 342.

⁴⁸¹ Vgl. NATO, Allied Joint Maritime Operations, 2004, Chapter 1, S. 1.

⁴⁸² Vgl. ebd., S. 2.

⁴⁸³ Vgl. ebd., S. 1.

⁴⁸⁴ Ebd., S. 1.

Die unterstützende Rolle wird zusätzlich durch die Möglichkeiten von Seestreitkräften in einem Konflikt unterstrichen. Die Aufgabe der Marine liegt entweder in der Erringung der Seeherrschaft, der Kontrolle über die See oder der Verhinderung der Nutzung des Meeres durch andere Seestreitkräfte. Neben der Machtprojektion sind dies die Effekte, welche Seestreitkräfte zu einem bewaffneten Konflikt beitragen können.

Der Zweck von maritimen Operationen liegt in der Ermöglichung von verschiedenen Unterstützungsleistungen.

„Maritime Operations can influence land and air operations by poisoning at sea and acting as a coercive force, reducing the need for host-nation support (HNS), manifesting deterrence, enabling access to the JOA [Joint Operations Area], providing battlespace dominance, projecting power ashore and providing sustainable logistics.“⁴⁸⁵

Nicht die Entscheidung, sondern die Unterstützung der Kräfte⁴⁸⁶, die die Entscheidung herbeiführen, ist die Aufgabe der Seestreitkräfte und des Krieges auf dem Meer. Wie in der multidimensionalen Seekriegführung angesprochen, ist die dritte Dimension, die Luft, für die Kriegführung von großer Bedeutung.

5.6.3 Luft als dritte Dimension des Krieges

Auf den Luftraum trifft Ähnliches zu wie auf die See. Wesentlich dabei ist, dass er beide anderen Dimensionen umschließt und somit die Luftkriegführung beider anderen Dimensionen nachhaltig unterstützen kann. Durch die Erschließung des Luftraums für die Nutzung durch den Menschen, wurde ein neuer Konfliktraum geschaffen.⁴⁸⁷ Im Luftraum finden sich jedoch keine vergleichbaren Ressourcen wie am Land und im Meer. Hier steht die unterstützende Rolle der Kriegführung im Vordergrund.

Der Vorteil des Krieges in der Luft ist die hohe Geschwindigkeit und die Feuerkraft, welche über große Distanzen in die Tiefe des gegnerischen Territoriums gebracht werden kann. Douhet sieht in der Luftwaffe die Möglichkeit, über Grenzen hinweg, Wirkmittel an den Gegner zu bringen.

„Sie [Anm. d. Verf.: Die Luftwaffe.] kann, einfach gesagt, außer Sprengstoffen auch chemisches und bakteriologisches Gift praktisch an jeden beliebigen Punkt des Feindesgebietes befördern, - bereits heute technisch gelöste Möglichkeiten, welche die Zukunft nur vervollkommen kann.“⁴⁸⁸

Der Abwurf der beiden Atombomben über Japan soll ihn einige Jahre später bestätigen. Die Luftwaffe führt zu einer Entgrenzung des Krieges bei

⁴⁸⁵ Ebd., S. 3.

⁴⁸⁶ Vgl. Mahan, Alfred Thayer: Der Einfluss der Seemacht auf die Geschichte, Überarbeitet und herausgegeben von Gustav-Adolf Wolter, Koehlers Verlagsgesellschaft mbH, Herford 1967, S. 49.

⁴⁸⁷ Vgl. Douhet, 1935, S. 13.

⁴⁸⁸ Ebd., S. 15.

Aufeinandertreffen von konventionellen Streitkräften. Dies trägt letztlich zu einer Totalisierung des Krieges, wie im Zweiten Weltkrieg zu sehen war, bei.

Dieser Raumkrieg ist charakteristisch für den Einsatz von Luftmitteln. Es gibt praktisch keinen Schutz gegen eine Luftwaffe, außer einer Luftwaffe.⁴⁸⁹ Diese können sich nur Staaten leisten und somit ist die Einwirkung von anderen Akteuren nur rudimentär möglich. Der russische Afghanistan Krieg hat gezeigt, dass moderne Luftabwehrwaffen eine Mitwirkung von anderen, irregulären Akteuren ermöglichen. Dennoch ist die Komplexität des Luftkrieges nicht mit dem des Landkrieges zu vergleichen.

Die Luftwaffe hat eine sehr starke Unterstützungsrolle, zielt sie im Krieg doch auf den Nerv des Gegners. Luftherrschaft ist somit eine Voraussetzung zu Erringung des Sieges im Krieg.⁴⁹⁰ Wie der Einsatz der NATO im Libyen Krieg gezeigt hat, ist der Einsatz einer Luftwaffe alleine nicht ausreichend, um einen Sieg im Krieg zu erringen. Ein Faktor der den Luftkrieg so wichtig für den Landkrieg macht ist, die rasche Verfügbarkeit von Unterstützungsleistungen.

„Air power has the unique ability to concentrate forces originating from diverse locations, perform a coordinated attack in time and space, then disperse quickly.“⁴⁹¹

Luftkrieg hat zwar direkten Einfluss auf die Kriegführung zu Wasser und an Land, kann aber nur unterstützend wirken, um eine Entscheidung im Krieg herbeizuführen. Im Gegensatz zur Seekriegführung ist der Einfluss allerdings ein unmittelbarer. Über dem Luftraum befindet sich das Weltall. Dieses umschließt alle anderen bisher genannten Dimensionen der Kriegführung.

5.6.4 Weltraum als vierte Dimension des Krieges

Diese vierte Dimension bringt wichtige Aspekte für die Kriegführung ins Spiel. Die Kriegführung selbst in dieser Dimension ist von großem Aufwand begleitet. Sowohl technologisch, wie auch finanziell ist es nur wenigen Akteuren möglich, am Krieg im Weltraum zu partizipieren. Trotzdem bietet die militärische Nutzung des Alls viele Vorteile.⁴⁹² Die Nützlichkeit liegt vor allem in unterstützenden Maßnahmen für die Kriegführung an Land, zur See und in der Luft.

Hierbei spielen Kommunikation, Aufklärung und Navigation eine starke Rolle. Durch die höchste Beobachtungsposition über einem Einsatzgebiet, der Bereitstellung von weltumspannenden Verbindungsrelationen und genauester Navigation durch Satelliten, wird das Militär bei seiner Einsatzführung unterstützt.

⁴⁸⁹ Vgl. ebd., S. 16.

⁴⁹⁰ Vgl. ebd., S. 16.

⁴⁹¹ NATO, Joint Air and Space Operations Doctrine, 2002, Chapter 2, S. 1.

⁴⁹² Vgl. ebd., Chapter 6, S. 1.

„As an integral element of military capabilities, space influences operations throughout the conflict, from peacetime engagement to general war.“⁴⁹³

Die Stationierung von Waffensystemen im Weltall ist schon angedacht worden, wurde aber bis jetzt nicht realisiert. Eine aktive militärische Konfrontation im All ist zwar denkbar, aber durch den Weltraumvertrag⁴⁹⁴ völkerrechtlich beschränkt. Die Vertragsparteien verpflichten sich darin zur friedlichen Nutzung des Weltraumes. Im Wesentlichen sind vier Punkte hervorzuheben:

„a. All nations have free access to space with liability for damage caused. b. Space will be used for peaceful purposes. c. No Weapons of Mass Destruction (WMD) will be placed in orbit around Earth or on the Moon. d. All space objects will be registered with the UN.“⁴⁹⁵

Operationen im All zielen vor allem auf die Produktion von Daten und Informationen sowie auf deren Übertragung ab. Die aktive Rolle in einem Krieg ist damit eine sehr beschränkte und bezieht keine Wirkmittel mit ein. Wie die hohe See und der Luftraum, sofern er nicht unter die Verantwortung eines Staates fällt, zählt der Weltraum zu den sogenannten Global Commons, die einer Nutzung durch alle Menschen offenstehen.

Damit ergibt sich ein weiterer Unterschied zur ersten Dimension. Land ist stets unter staatlicher Kontrolle, das Gemeinwesen legt fest, wer sich auf seinem Staatsgebiet aufhalten darf. Eine uneingeschränkte Nutzung des Landes ist daher nicht möglich. Durchdrungen werden diese Dimensionen der Kriegführung durch den Cyberraum, die fünfte Dimension der Kriegführung, der selbst schon eine wesentliche militärische Bedeutung hat. Nach dem Zwischenergebnis zum vorliegenden Kapitel wird die fünfte Dimension des Krieges näher untersucht.

5.7 Zwischenergebnis zum Begriff des Krieges

Der Konflikt umfasst vier Momente, von denen zwei den Krieg als solches betreffen. Es handelt sich um den Aufruhr und den Krieg selbst. Der erste ist als intragemeinschaftlicher Krieg zu fassen. Der zweite ist die intergemeinschaftliche Ausprägung des Krieges. Krieg ist das ultimative Moment des bewaffneten Konfliktes. Da das Militär im Falle eines solchen bewaffneten Konfliktes zuständig ist, egal ob er zwischen Gemeinwesen oder innerhalb eines Gemeinwesens stattfindet, sind es diese beiden Momente des Konfliktes, welche für das Militär relevant sind.

Die politische Dimension ist dafür der ausschlaggebende Grund. Es handelt sich beim Krieg um ein politisches Instrument, mit dem Zweck eine staatliche Ordnung zu beseitigen oder wiederherzustellen. Das Militär ist jenes Element der Staatsgewalt, welches in der Lage ist ohne staatlichen

⁴⁹³ Ebd., S. 2.

⁴⁹⁴ Vgl. Neuhold, Hanspeter u.a.: Österreichisches Handbuch des Völkerrechts, 2. Aufl., Band 2, Wien 1991, S. 383ff.

⁴⁹⁵ NATO, Joint Air and Space Operations Doctrine, 2002, Chapter 6, S. 3.

Ordnungsrahmen zu handeln. Die Polizei dient der Aufrechterhaltung, der Funktionsfähigkeit, der staatlichen Ordnung und benötigt diesen Ordnungsrahmen, um überhaupt handeln zu können. Dort wo er beseitigt ist, muss das Militär einschreiten, dies gilt auch innerhalb des Gemeinwesens.

Politik ist nur in Gemeinwesen möglich, egal wie diese beschaffen sind. Krieg als politisches Instrument kann daher nur in und zwischen solchen, einer Ordnung unterliegenden, Gemeinwesen stattfinden. Da Krieg als mit Waffengewalt ausgetragener Konflikt zu fassen ist, bedarf es bewaffneter Organe, wie dem Militär, welches als bewaffneter Träger der Staatsgewalt das Gemeinwesen verteidigt.

Wesentlich ist in diesem Zusammenhang das Verhältnis zwischen Bedrohung und Sicherheit. Der Staat ist das dialektische Verhältnis dieser beiden Faktoren. Anders ausgedrückt, wehrt das Militär die Bedrohungen von außen ab und die Polizei erhält die Sicherheit im Inneren. Dies sind die Voraussetzungen für die Politik, das Handeln zum Gemeinwohl. Daraus folgt die Notwendigkeit der Souveränität. Bedrohungen sind dann souveränitätsstiftend, wenn sie auch wahrnehmbar sind. Werden Bedrohungen nicht mehr wahrgenommen, so führt dies zur Desintegration des Gemeinwesens.

Eine permanente Spannung mit äußeren Bedrohungen führt zur Herstellung einer inneren Sicherheit, weil die Bedrohung gruppenbildend ist. Krieg, latent oder manifest, kann in diesem Kontext als gestaltendes Element gefasst werden. Für die Festlegung der Zuständigkeit gegenüber solchen Bedrohungen, zur Gefahrenabwehr, sind im Wesentlichen drei Faktoren ausschlaggebend: Die Ausdehnung, die Form und die Intention des Konfliktes. Diese Faktoren bestimmen das Moment des Konfliktes und somit auch die Zuständigkeit der Träger des Gewaltmonopols im Gemeinwesen.

Da zunehmend Konflikte geführt werden, in denen nichtstaatliche Akteure wirken, ist eine klare Aufgabenzuordnung von mehreren Faktoren abhängig. Hier spielen die oben beschriebenen Parameter, Ausdehnung (räumlich und kräftemäßig), Form und Intention die entscheidende Rolle, oder einfach ausgedrückt: Wer greift was/wen warum an? Anhand dieser Einflussgrößen ist eine Zuordnung der Führungsverantwortung zu leisten, aus der sich Aufgabenbereiche ableiten lassen. Der Einsatz des Militärs gegen die zunehmend nichtstaatlichen Akteure in bewaffneten Konflikten, stellt ein politisches Instrument, nämlich die Anerkennung als Gegner, dar.

Krieg hat eine Asymmetrie zwischen Anspruch und Wirklichkeit als Ursache, die im Zuge des bewaffneten Konfliktes beseitigt werden muss. Sicherheit ist ein die Symmetrie beeinflussender Faktor. Keine oder ein Zuviel an Sicherheit führt dazu, dass eine Asymmetrie im Machtgefüge erwächst, welche im Krieg beseitigt wird. Ein Ansatz, diese Asymmetrien zu minimieren, ist die Vernetzung der Gemeinwesen untereinander, um einerseits die Abhängigkeiten zu fördern und andererseits die Wahrscheinlichkeit von bewaffneten Konflikten zu senken.

Der Krieg umfasst zwei Momente oder Formen, es handelt sich dabei um den Großen und den Kleinen Krieg. Der Große Krieg ist jener zwischen regulären Streitkräften zweier Gemeinwesen. Er ist der symmetrische Typus des Krieges. Er ist ein gehegter Krieg in Hinblick auf die Faktoren Kraft, Raum und Zeit. Die Intensität ist, wenn nur das Militär eingesetzt wird, gesamtstaatlich geringer einzuschätzen als für das Militär selbst. In seiner ursprünglichen Form ist der Große Krieg von instrumentellem Charakter. Für den Staat ist die Intensität nicht maximal, außer er zeigt sich in seiner totalen Form. Denn er hat das Potential, auf Grund der Vernetzung des Militärs mit anderen Bereichen des Staates, eine totale Ausprägung zu erreichen.

Dies ist dann der Fall, wenn zum Großen Krieg das zweite Moment hinzutritt, der Kleine Krieg. Im Krieg kommen und kamen immer beide Formen zur Anwendung. Je mehr der Kleine Krieg, im Rahmen eines Krieges, in Erscheinung tritt, je mehr nichtstaatliche Akteure mitwirken, umso existenzieller wird sein Charakter. Die Folge ist ein totaler Krieg. Es geht hier klar hervor, dass der Krieg die Synthese aus Großem und Kleinem Krieg darstellt.

Der Kleine Krieg ist der asymmetrische Typus des Krieges. Um ihm begegnen zu können, ist eine Resymmetrierung zu betreiben, die es dem staatlichen Akteur erlaubt, gegen die asymmetrischen Wirkungsweisen vorzugehen. Dies bedeutet, im rechtlichen Rahmen, die Kampfweisen anzupassen oder die Transformation des rechtlichen Rahmens anzustreben. Hier ist der Einsatz von adäquaten Mitteln, zur Bekämpfung asymmetrisch kämpfender Akteure, angezeigt. Daraus folgt entweder die Polizei als Hauptakteur einzusetzen oder aber das Militär derart zu gestalten, dass es in der Lage ist, gegen diese Gruppierungen vorzugehen.

Die Verantwortung für das Handeln gegen diese Akteure kann von der Auswirkung der irregulären Aktionen und deren räumlicher Ausdehnung her bestimmt werden. Daher muss eine Schwelle festgelegt werden, ab wann, auch im Inneren, die Führungsverantwortung an das Militär übergeht. Dazu müssen Instrumente implementiert werden, welche die Intensität erkennbar machen. Hier geht es darum, die Bedrohung und die Auswirkungen aufzuklären und darzustellen. Dies kann durch Polizei, Militär und Nachrichtendienste geleistet werden.

Die technologische Entwicklung fördert die Entstehung neuer Konflikte, wobei vor allem territoriale Grenzen zunehmend in den Hintergrund gerückt werden. Globale Vernetzung und Steigerung der Komplexität sind hier als Schlagworte zu nennen. Es folgt daraus, dass zunehmend eine andere Betrachtungsweise von innen und außen, im Zusammenhang mit Gemeinwesen, herangezogen werden muss. Die Trennung kann nicht nur durch einen Territorialbezug geleistet werden, sondern bedarf einer systemischen Sichtweise. Daraus lassen sich dann auch Zuständigkeiten einfacher ableiten.

Krieg ist dialektisch in zwei Momente zu fassen, die entscheidende und die unterstützende Kriegführung. Diese Erkenntnis in Verbindung mit den

Formen des Krieges ergibt, dass der Kleine Krieg ein unterstützender ist, genauso wie alle Elemente des Großen Krieg, außer der Landkriegführung.

6 Vom Begriff des Cyberspace

„Die Beschaffenheit des Geländes
ist die Grundlage, um der Armee
zum Sieg zu verhelfen.“
Mei Yaochen⁴⁹⁶

Raum und Zeit sind die Kernfaktoren, die als Grundvoraussetzung für alles Seiende zu verstehen sind. Die Existenz von Gegenständen und Lebewesen ist durch Raum und Zeit bestimmt.⁴⁹⁷ Raum ist somit die Bedingung für den Ort und daraus abgeleitet, für dasjenige, welches im Raum verortet ist. In der realen Welt sind die Dimensionen Land, See, Luft und Weltraum die Kategorien in denen sich der Mensch zu verorten gelernt hat. Neu ist die virtuelle Dimension der sogenannte Cyberraum, welcher die anderen Dimensionen durchdringt. Dieser Raum kann aus unterschiedlichen Blickwinkeln betrachtet werden und je nach Betrachtungsweise unterschiedliche Bedeutung für den Menschen erlangen.

Zunächst ist der Cyberspace ein technologisches Konstrukt, bestehend aus technischen Komponenten, welche zusammen in einem Netzwerk ihre Wirkung entfalten. Er ist aber nicht nur das, sondern darüber hinaus viel mehr. Ein Raum ist stets etwas Eingegrenztes. Im Falle des Cyberspace offenbart sich jedoch eine Paradoxie, nämlich, dass dieser Raum quasi grenzenlos erscheint oder anders ausgedrückt Grenzen aufzulösen beginnt, die das menschliche Handeln bisher beschränkten.⁴⁹⁸ Zur Entgrenzung in räumlicher Hinsicht kommt die zeitliche Entgrenzung. Soziale Interaktionen werden so technologisch praktisch räumlich und zeitlich entgrenzt.

Spinnt man den Gedanken von Kant weiter, dass nämlich keine Anschauung ohne Begriff bzw. kein Begriff ohne Anschauung sein kann, so kann man ohne weiteres behaupten, dass es ohne Denken kein Sein und umgekehrt geben kann.⁴⁹⁹ Raum ist also für die Verortung des Seienden Grundvoraussetzung. Dieser Gedanke spiegelt sich auch bei Spinoza wider, in der Verbindung von Sein und Denken im Monismus.⁵⁰⁰

Information benötigt somit einen Informationsraum. Wenn der Cyberraum weit gefasst wird, so ist er durchaus als deckungsgleich mit diesem Informationsraum zu fassen. Der Cyberspace ist mehr als nur ein Netzwerk von Dingen.⁵⁰¹ Der Raum und die Informationen dienen dem

⁴⁹⁶ Griffith, B. Samuel: Sun Zi. Die Kunst des Krieges. Die neue illustrierte Ausgabe, Kerkdriel 2019, S. 197.

⁴⁹⁷ Vgl. Hähnel, Martin: ...um einer Vielheit statt. In: Schlitte, Annika; Hünefeldt, Thomas (Hrsg.): Ort und Verortung. Beiträge zu einem neuen Paradigma interdisziplinärer Forschung, Bielefeld 2017, S. 41f.

⁴⁹⁸ Vgl. Rasche, Michael: Der topographische Beginn der Philosophie: Anaximander. In: Schlitte, Annika; Hünefeldt, Thomas (Hrsg.): Ort und Verortung. Beiträge zu einem neuen Paradigma interdisziplinärer Forschung, Bielefeld 2017, S. 22f.

⁴⁹⁹ Vgl. Kant, Immanuel: Kritik der reinen Vernunft, Reclam, Stuttgart 1966, S. 119f.

⁵⁰⁰ Vgl. Spinoza: Ethik. In geometrischer Weise behandelt in fünf Teilen, Leipzig 1975, S. 83f.

⁵⁰¹ Vgl. Torkler, Rene: Einen Ort in der Welt haben. In: Schlitte, Annika; Hünefeldt, Thomas (Hrsg.): Ort und Verortung. Beiträge zu einem neuen Paradigma interdisziplinärer Forschung, Bielefeld 2017, S. 53.

Menschen dazu, Handlungen über diese beiden Parameter in der Realität zu verwirklichen. Dieser menschliche Handlungsraum kann nun auch dazu verwendet werden um Konflikte darin bzw. daraus auszutragen. Damit wird der Cyberspace unter Umständen zu einem militärischen Einsatzraum. Um zu verstehen wie sich Konflikte in dieser Umgebung äußern, ist es zunächst notwendig diesen Raum zu untersuchen und darzustellen.

6.1 Zum Cyberspace als (technologischer) Raum

Zunächst war es möglich einfache Signale zu nutzen, um Entfernungen in der Kommunikation zu überwinden. Dann gelang es schriftliche Informationen als Nachrichten zu „übertragen“ (Hervorhebung durch den Verfasser.), es folgten der Ton und schließlich das Übertragen von Bildern. Heute ist es den meisten Menschen möglich alle Formen von Informationen, unabhängig vom Ort an dem die Information bereitgehalten wird, überall zu nutzen. Der Informationsraum wuchs und verkürzte die Entfernungen zwischen den Nutzern desselben. Der Cyberspace ist dabei einem steten Wandel ausgesetzt:

„The geography of cyberspace changes without warning, and software updates and network reconfiguration create an environment where insurmountable obstacles and golden opportunities can appear and disappear as if by magic.“⁵⁰²

Der Cyberspace wurde zu einem, alle anderen Bereiche durchdringenden Raum, den es im Folgenden darzustellen gilt.

6.1.1 Die Momente des Cyberspace

Der Mensch ist laut Spinoza die Einheit von Geist und Materie. Beim Verhältnis von Realität zur Virtualität verhält es sich ähnlich wie beim Verhältnis vom Sein zum Denken.⁵⁰³ Für Spinoza ist beides eine Einheit, er beschreibt dies als Monismus, welcher Geist und Materie vereint.⁵⁰⁴ Der Geist braucht die Erregung des Körpers durch einen anderen Körper, um diesen wahrnehmen, ihn erfassen zu können. Der Geist kann nicht direkt durch den Geist zum Denken angeregt werden.⁵⁰⁵ Die Verbindung von Geist und Körper ist also notwendig.

„Das Objekt der Idee, die den menschlichen Geist ausmacht, ist der Körper oder eine gewisse Daseinsform der Ausdehnung, die in Wirklichkeit existiert, und nichts andres.“⁵⁰⁶

⁵⁰² Geers, Kenneth: Strategic Cyber Security: Evaluating Nation-State Cyber Attack Mitigation Strategies with DEMATEL, Tallinn University of Technology, Dissertation, 2011, S. 105.

⁵⁰³ Vgl. Vortrag von Prof. Dr. Ropolyi zur virtuellen Realität im Rahmen des Humanwissenschaftlichen Kolloquiums zum Thema Militär im Cyberspace, Landesverteidigungsakademie, 04.12.2012.

⁵⁰⁴ Vgl. Spinoza: Ethik, S. 83f.

⁵⁰⁵ Vgl. ebd., S. 159f.

⁵⁰⁶ Ebd., S. 97.

Für Spinoza ist nicht der Geist derjenige, der den Körper zur Bewegung anregt, sondern der Körper erfährt nur durch einen anderen Körper einen bestimmten Zustand. Dennoch sind beide eins, Geist und Körper. Und der Geist braucht einen Körper, um das Denken zu ermöglichen und im Umkehrschluss benötigt der Körper den Geist, um Handlungen zu ermöglichen. Ähnlich verhält es sich mit dem Cyberspace. Dieser besteht aus einer virtuellen Komponente, dem Geist in Spinozas Sinn und dem Körper, dem physikalischen Netz. Es stehen einander also reine Virtualität und reine Realität gegenüber. Der Cyberspace ist weder das eine noch das andere, er ist mehr.

Der Cyberspace wird im Allgemeinen als ein auf physikalische Komponenten beschränkter Raum gefasst. So definiert die Europäische Union ihn folgendermaßen:

„Cyberspace describes the man made, global commons domain within the information environment consisting of the interdependent networks of global, organisational and national information infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors.“⁵⁰⁷

Diese, nur auf die reine Realität abzielende, Definition ist unvollständig und fasst lediglich die physikalische Komponente. Die Attribute der Ausdehnung und des Denkens sind verschiedenen Ebenen zuordenbar. Die Ausdehnung entspricht dabei der reinen Realität, welche durch die Empirie fassbar und der physikalischen Ebene zuordenbar ist. Das Denken ist der reinen Virtualität zurechenbar und ist durch die Rationalität fassbar, welche der kognitiven Ebene entspricht. Beide Momente stellen im dialektischen Sinn somit These und Antithese dar, deren Synthese durch die virtuelle Realität geleistet wird.⁵⁰⁸

Der Cyberspace ist nicht nur reine Realität, sondern verbindet sich mit der reinen Virtualität zur Virtuellen Realität (VR).⁵⁰⁹ Der Cyberspace geht dabei weit über das Internet hinaus.

„Cyberspace is more than the internet, including not only hardware, software and information systems, but also people and social interaction within these networks.“⁵¹⁰

Er wird zu einer vom Menschen geschaffenen Realität, in der sich Denken in virtuellen Handlungen manifestiert. Diese Handlungen in einer virtuellen Realität können aber wieder in der Realität wirksam werden. Der große Nutzen dieser Erkenntnis liegt darin, dass der Handlungsraum durch diese Erfindung entgrenzt und extrem ausgeweitet wurde. Dabei bleibt er,

⁵⁰⁷ EUMS, EU Concept for Cyber Defence for EU-led Military Operations, 2012, S. 4.

⁵⁰⁸ Vgl. Schmidt, Eric; Cohen, Jared: Die Vernetzung der Welt. Ein Blick in unsere Zukunft, Rowohlt, Reinbek bei Hamburg, 2013, S. 19.

⁵⁰⁹ Vgl. Hülsmann, Thorsten: Geographie des Cyberspace. Wahrnehmungsgeographische Studien, Band 9, 2000, S. 47.

⁵¹⁰ Klimburg (Hrsg.), National Cyber Security Framework Manual, NATO CCD COE Publication, Tallinn 2012, S. 8.

anders als die anderen Dimensionen⁵¹¹, stets veränderbar.⁵¹² Shannon zeigt in seiner Kommunikationstheorie den Aufbau einer Interaktionsrelation im Cyberspace. Er spricht bei der Kommunikation von dem Informationsaustausch über fünf Elemente.⁵¹³

Eine Vernetzung vieler Sender und Empfänger, über ein Netzwerk von Kommunikationskanälen, führt zu einem physikalischen Kommunikationsnetzwerk. Wie aber Shannon schon richtig gefolgert hat, bedarf es auch noch der Elemente einer Informationsquelle und eines Abnehmers dieser Information, eines Zieles (Informationssenke). Somit kann auch der Informationsträger und der Informationsbedarfsträger als Teil der Kommunikationsrelation verstanden werden. Damit ist der Mensch, der an dieser Interaktion teilnimmt, ja sogar, wenn er nicht daran teilnimmt, Element des Cyberspace. Der Cyberspace als sozio-technisches System wird durch diese ganzheitliche Betrachtungsweise zu dem komplexen System, das wir in ihm sehen.⁵¹⁴ Ein wesentliches Element, welches den Cyberspace, nach heutigem Verständnis, erst zu dem werden lässt, was er ist, ist das Vorhandensein von Speicherkapazität im Netz.⁵¹⁵ Dieser Speicher ermöglicht es, Informationen im Netzwerk zu belassen, es somit selbst zum Informationsträger zu machen, und erst dann abzurufen, wenn diese wieder benötigt werden. Der Cyberspace kann somit als

„The environment formed by physical and non-physical components to store, modify, and exchange data using computer networks.“⁵¹⁶

verstanden werden, wobei der Mensch hier als wesentliches Element aus einer Verbindung von physischen und nicht-physischen Komponenten, wenn dies so mechanistisch fassbar ist, zu verstehen wäre. Hier äußert sich wieder die Dialektik des Cyberspace. In spinozistischer Art und Weise fasst diese Definition die Virtuelle Realität als Synthese von Realität und Virtualität, von Ausdehnung und Denken.

Der Cyberspace ist von Menschen geschaffen und bringt daher nur Dinge hervor, die vom Menschen herrühren. Der Mensch als Quelle einer Kommunikation führt den Denkprozess aus, dieser äußert sich dann in der Handlung, nämlich der Kommunikation und Interaktion über den Cyberspace. Die Kommunikationseinrichtung als Hilfsmittel erfasst die physikalischen Parameter, wie Sprache oder Schrift und verarbeitet sie nach bestimmten Regeln. Die Speicherung von Informationen innerhalb dieser Kommunikationsnetze schafft schließlich tatsächlich eine virtuelle Realität neben der reinen Realität.

⁵¹¹ Anm. d. Verf.: Darunter sind Land, See, Luft und Weltraum zu verstehen.

⁵¹² Vgl. Hansel, Mischa: Stuxnet und die Sabotage des iranischen Atomprogramms: Ein neuer Kriegsschauplatz im Cyberspace? In: Jäger, Thomas; Beckmann, Rasmus: Handbuch Kriegstheorien, Wiesbaden 2011, S. 568.

⁵¹³ Vgl. Shannon, 1948, S. 2.

⁵¹⁴ Vgl. Klauninger, Bert: Cyberspace als ein selbstorganisierendes System, o.J. http://archive.gpi-online.de/files/_klauninger_cyberspace.pdf, S. 1, [12.05.2020].

⁵¹⁵ Vgl. Holischka, Tobias: Zur Philosophie des virtuellen Ortes. In: Schlitte, Annika; Hünefeldt, Thomas (Hrsg.): Ort und Verortung. Beiträge zu einem neuen Paradigma interdisziplinärer Forschung, Bielefeld 2017, S. 203.

⁵¹⁶ Schmitt, 2017, S. 564.

Die Virtuelle Realität ist damit Information, die mittels eines Algorithmus verarbeitet und in einem physischen Netzwerk abgespeichert wird. Dieser Algorithmus, ist als syntaktisches Element, als Programmcode, Teil der Virtuellen Realität. Am Übergang von Virtueller Realität zur reinen Realität findet sich ein weiteres Element zur Spezifikation des Cyberspace, die semantische Ebene. Hier wird dem Informationsbedarfsträger die Information wieder zugänglich gemacht, das heißt sie wird lesbar und hinsichtlich ihrer Bedeutung bewertbar.⁵¹⁷ Am anderen Ende der Kommunikationskette kann die Information dem Bedarfsträger, unabhängig von Zeit und Raum, wieder zugänglich gemacht werden und er wird in die Lage versetzt, die Bedeutung der Information zu erfassen.

Die Gemeinwesen können als komplexe Systeme betrachtet werden, die auf verschiedenen Ebenen miteinander vernetzt sind. Diese Systeme können aufgeteilt werden in Subsysteme, welche diese verschiedenen Ebenen repräsentieren. Es kann hier ein politisches, ein soziales, ein militärisches, ein infrastrukturelles und ein informationelles Subsystem identifiziert werden. Diese Aufteilung wird auch PMESII (Political, Military, Economic, Social, Infrastructure, Information) genannt. Diese Subsysteme stehen in einer direkten Beziehung zueinander und sind so mehrfach vernetzt.⁵¹⁸ Jedes Gemeinwesen kann in dieser Form aufgeschlüsselt werden. Die Gemeinwesen untereinander sind ebenfalls vernetzt. Dies macht die ganze Welt zu einem, mehr oder weniger, stark vernetzten Gesamtsystem. Diesem Gesamtsystem überlagert ist der Cyberspace, der alle Bereiche durchdringt.⁵¹⁹ Hier ist eine gewisse Analogie zu den Dimensionen der Kriegführung zu erkennen, welche in der vorliegenden Abhandlung schon näher erläutert wurden.

Der neue Handlungsraum, die Virtuelle Realität des Cyberspace, ist nicht mehr ausschließlich territorial zu bestimmen, sondern systemisch.⁵²⁰ Das System eines Gemeinwesens ist nicht mehr nur an ein Staatsgebiet gebunden, sondern an die Vernetzungen, die dieses Gemeinwesen letztlich ausmachen. Dabei besteht das Netzwerk aus den oben beschriebenen Komponenten, einer über Kommunikationswege verbundenen Anzahl von Knoten.⁵²¹ Diese sind die Informationsträger (Speicher, Quellen und Ziele).⁵²² Diese Struktur und der hohe Vernetzungsgrad sind aus militärischer Sicht interessant, da ein Eingriff in ein Subsystem Auswirkungen auf andere Subsysteme haben kann.⁵²³ Angriffe erfordern daher nicht unmittelbar das Wirken von militärischen Streitkräften. Gleichzeitig ergibt sich eine Herausforderung beim Schutz, der Verteidigung dieser Subsysteme.

Die Vernetzung in diesen Systemen führt zur Vernetzung möglicher Ziele, was wiederum einer Vernetzung, der für den Schutz in Frage

⁵¹⁷ Vgl. Hansel, 2011, S. 568. (in: Jäger/Beckmann, 2011)

⁵¹⁸ Vgl. United States Joint Force Command, Doctrinal Implications of Operational Net Assessment, 2004, S. 11.

⁵¹⁹ Vgl. Hülsmann, 2000, S. 52ff.

⁵²⁰ Vgl. Klauninger, Bert: Cyberspace als ein selbstorganisierendes System, o.J. http://archive.gpi-online.de/files/_klauninger_cyberspace.pdf, S. 3, [12.05.2020].

⁵²¹ Vgl. Freudenberg, 2008, S. 41.

⁵²² Vgl. Holischka, 2017, S. 202. (in: Schlitte/Hünefeldt, 2017)

⁵²³ Vgl. Freudenberg, 2008, S. 44.

kommenden Akteure, bedarf. Bei der Vernetzung der Akteure tritt wieder die Frage, die der Arbeit zu Grunde liegt, in den Fokus. Wenn alle Akteure zusammenwirken müssen, muss die Frage nach der Führungsverantwortung gestellt werden. Diese Frage ist allerdings nicht nur an die räumliche Komponente gebunden, sondern bedarf einer ganzheitlichen Betrachtung von Konflikten im Netz. Der virtuelle Raum ist ein Interaktionsraum, in dem auch Konflikte ablaufen können.

„Zunächst ist das Internet nur ein hybrides Netzwerk aus Licht und Logik, das die imperative Welt der Bits und Bytes ins Sein wirft und weite Bereiche des Sozialen in maschinelle Rückkopplungsschleifen übersetzt.“⁵²⁴

Der Cyberspace ist ein Handlungshilfsmittel des Menschen, er leistet keine Denkarbeit. Er dient der Verarbeitung, Darstellung und Speicherung von Informationen. Die kognitive Leistung liegt beim Menschen. Da aber der Mensch Teil des Cyberspace ist, bezieht sich diese Feststellung, dass der Cyberspace ein Hilfsmittel ist, lediglich auf die physikalische Infrastruktur des Netzes. Obwohl Menschen über das Netz interagieren können, ist der Cyberspace ein von den anderen Dimensionen der Kriegführung zu unterscheidender Raum.

„Für Lebewesen in der uns vertrauten Gestalt ist der Cyber-Raum, der ein nicht-euklidischer ist, unzugänglich und unbewohnbar.“⁵²⁵

Trotzdem können sich Handlungen im Cyberspace in der Realität auswirken. Überall wo Menschen in Interaktion treten können, treffen im Clausewitzschen Sinn verschiedene Willen aufeinander. Das bedeutet, dort wo die Willen einander widerstreben, kommt es zum Konflikt. Damit unterscheidet sich der Cyberspace – hinsichtlich der Konfliktualität – keinesfalls zu den anderen Interaktionsräumen. Das Besondere ist die virtuelle Umgebung, deren zentraler Bestandteil Speichermöglichkeiten für Informationen sind, in der Handlungen ausgeführt werden können, ohne Rücksicht auf räumliche oder zeitliche Grenzen. Damit umfasst der Cyberspace nicht nur die technischen Einrichtungen, er bedarf auch der Information und des Menschen. Daraus lassen sich im weiteren Verlauf der Abhandlung die Angriffsvektoren im Cyberspace ableiten.⁵²⁶ Der Entgrenzung durch den Cyberspace wird im folgenden Kapitel nachgegangen.

6.1.2 Die Entgrenzung durch den Cyberspace

Obwohl auf einer physischen Plattform stehend, ist der Cyberspace ein Raum ohne territoriale Grenzen. Allgemein wird der Cyberspace auch als

⁵²⁴ Maresch, Rudolf; Rötzer, Florian: Cyberhypes. Möglichkeiten und Grenzen des Internet, 1. Aufl., Frankfurt 2001, S. 62.

⁵²⁵ Ebd., S. 62.

⁵²⁶ Vgl. Gayken, 2011, S. 99.

souveränitätsfreier Raum verstanden, wenngleich die ihm zu Grunde liegende Infrastruktur staatlicher Souveränität unterliegt.⁵²⁷ Netzwerke sind

„[...] gleichzeitig unberührbar, unsichtbar, einzigartig, überall und nirgends [...].“⁵²⁸

Die Grenzen lassen sich nur systemisch fassen. Teilnetze und einzelne Systeme im Netzwerk sind ansprechbar. Durch gewisse Zugangseinrichtungen kann eine systemische Trennung vom restlichen Netz erzielt werden. Auf Grund dieser Tatsache ist eine genaue territoriale Aufteilung in innen und außen nicht mehr möglich. Das Verständnis von innen und außen hat sich an anderen Parametern zu orientieren. Da das Internet nur einen Teil des Cyberspace darstellt und dessen Komponenten territorial über verschiedene Erdteile verstreut disloziert sind, ist eine Aufteilung in innen und außen nur über die Zuordnung von Nutzern an bestimmte Subnetze möglich.

Im Tallinn Manual findet sich ein Hinweis auf die Trennung von territorialer und systemischer Zugehörigkeit von Cyber Infrastruktur. Hier wird davon gesprochen, dass

„Any interference by a State with cyber infrastructure aboard a platform, wherever located, that enjoys sovereign immunity constitutes a violation of sovereignty.“⁵²⁹

Diese Souveränitätsverletzung geht also von staatlichen Trägersystemen aus, welche selbst den Souveränitätsschutz genießen.⁵³⁰ Dabei ist der Ort an dem sich diese Trägersysteme oder Plattformen befinden nach Ansicht der Expertengruppe irrelevant. Es ist ausschlaggebend, dass die darauf installierte Cyber Infrastruktur Teil des staatlichen Cyberspace ist.

Das bedeutet, dass Subsysteme des Cyberspace oder des Internets als solche erkannt und etwas einem Subsystem zugehörig, also innen, oder nicht zugehörig, also außerhalb des Systems, identifiziert werden kann. So besteht das Netzwerk des Österreichischen Bundesheeres aus verschiedenen Teilnetzen, welche unterschiedlichen Zwecken dienen und sich örtlich nicht unbedingt auf österreichischem Staatsgebiet befinden.⁵³¹

Diese Aufteilung in Subnetze ermöglicht eine gewisse Grenzziehung im systemischen Sinn. Es ermöglicht auch die Zuordnung einer bestimmten Verantwortung für diese Teilnetze. Ein Innen und ein Außen sind systemisch zuordenbar. Die Schere, zwischen territorialer Verantwortung des Staates

⁵²⁷ Vgl. Schaller, Christian: Internationale Sicherheit und Völkerrecht im Cyberspace. Für klarere Regeln und mehr Verantwortung, Stiftung Wissenschaft und Politik, Berlin 2014, S. 7.

⁵²⁸ Freudenberg, 2008, S. 42.

⁵²⁹ Schmitt, 2017, S. 27.

⁵³⁰ Anm. d. Verf.: Unter Plattform werden im Allgemeinen Trägersysteme wie Schiffe und Flugzeuge verstanden.

⁵³¹ Vgl. Vortrag von Ing. Mag. Kaponig im Rahmen des 19. Generalstabslehrganges zum Thema Führungsunterstützungszentrum, Landesverteidigungsakademie, 23.01.2013.

und systemischer Verantwortung, ist eine der großen Herausforderungen im Cyberspace.

Krieg in diesem Raum bedeutet, auf Grund der Vernetzung der Teilsysteme, dass eine räumlich begrenzte Einsatzführung schwer möglich ist. Durch die Interaktion zwischen den Systemen, kann ein Angriff große Auswirkungen mit sich bringen. Die sogenannte Migration von Schäden kann Bereiche, welche nicht Ziel sein sollen, aber auch den Angreifer selbst, treffen.⁵³² Dies macht den Cyberwar nicht zu einem Mittel der breiten Masse, sondern bedarf gewisser Kenntnisse, um solchen Gefahren zu begegnen. Die Entgrenzung birgt also nicht nur für die Verantwortung des Staates Probleme in sich, sondern hält auch für einen Angreifer Hürden bereit.⁵³³ Obwohl der Cyberraum grenzenlos scheint, ist er doch begrenzt. Seine Ausdehnung „[...] unterliegt also technischen Beschränkungen [...]“⁵³⁴, die sich im Wesentlichen an der vorhandenen Netz-Infrastruktur orientieren. Um ihn überhaupt als Raum fassen zu können, bedarf es als Voraussetzung der Grenze.⁵³⁵

Ein Aspekt, der hinsichtlich der Entgrenzung noch zu beachten ist, ist jener, dass die Netze, in welchen sich vitale Infrastrukturen des Gemeinwesens befinden, fast zur Gänze in privater Hand sind. Dies schränkt die Verantwortlichkeit der Staatsgewalt zu deren Schutz massiv ein. Hinsichtlich der Frage nach der staatlichen Verantwortung wird durch die Expertengruppe im Tallin Manual dahingehend argumentiert, dass der Staat die Kontrolle über den Zugriff auf sein Territorium ausüben muss. Auf den Cyberspace umgelegt bedeutet dies auch eine staatliche Verantwortung für die Cyber Infrastruktur, welche sich im Territorium des Staates befindet.

„A State enjoys sovereign authority with regard to the cyber infrastructure, persons, and cyber activities located within its territory, subject to its international legal obligations.“⁵³⁶

Dieses Recht umzusetzen beinhaltet bei den kritischen Infrastrukturen schon eine große Problematik, die im Cyberspace kaum auflösbar scheint. Diese weit gefasste Verantwortung würde dem Staat einerseits auch die heutzutage viel diskutierten Eingriffe (Datenspeicherung auf Vorrat) in den Cyberspace aufzwingen und andererseits die Beschaffenheit des Cyberspace gänzlich ignorieren. Es geht hier um funktionale und systemische Territorien nicht um physische Bereiche. Die Problematik lässt sich nur mit einer Änderung im Denkansatz bewältigen.⁵³⁷

Betrachtet man die Rolle des Staates beim Schutz der Cyber Infrastruktur und vergleicht man den Cyberspace mit dem offenen Meer, so kann man hier auf eine Aussage von Grotius verweisen, welcher über die Möglichkeiten der Staatsgewalt Folgendes sagte:

⁵³² Vgl. Gayken, 2011, S. 65f.

⁵³³ Vgl. Freudenberg, 2008, S. 44.

⁵³⁴ Holischka, 2017, S. 202. (in: Schlitte/Hünefeldt, 2017)

⁵³⁵ Vgl. Liessmann, Konrad Paul: Lob der Grenze. Kritik der politischen Urteilskraft, Wien 2012, S. 29.

⁵³⁶ Schmitt, 2017, S.13.

⁵³⁷ Vgl. ebd., S. 11ff.

„Die sogenannte Staatsgewalt über solche Meerestheile [Anm. d. Verf.: Diese sind in Analogie zum Cyberspace zu verstehen.] ist in jedem Falle viel beschränkter Natur als die Staatsgewalt über ein Landgebiet, [...]“⁵³⁸

Auch sind viele Unternehmen, die von staatlicher Bedeutung sind, nicht durch Militär oder Polizei vor Angriffen zu schützen, da sie sich durch den Standort ihrer physikalischen Netzkomponenten, der Zuständigkeit der territorial gebundenen Sicherheitskräfte entziehen. Dies ist ein weiterer Aspekt der Entgrenzung. Diese hohe Komplexität und die daraus resultierenden Abhängigkeiten legen den Schluss nahe, Krieg im Netz als – auf der strategischen Ebene der Kriegführung stattfindende – Auseinandersetzung zu begreifen. Nicht nur das Militär ist der Nutzer des Cyberspace, sondern auch eine Unzahl anderer Bedarfsträger, die aus den verschiedensten Bereichen wie Wirtschaft, Diplomatie oder Politik, kommen.

Kriege in diesem Raum haben immer auch Auswirkung auf die anderen Bereiche, es kann hier durchaus von einem totalen, virtuellen Krieg gesprochen werden. Die Frage – die es im Laufe der Abhandlung noch zu klären gilt – ist, wie Krieg in diesem Raum beschaffen und ob denn ein solcher im Cyberspace bis jetzt schon vorgekommen ist. Wenn man von Entgrenzung spricht, folgt unweigerlich die Frage nach der Bedeutung von Raum und Zeit in diesem Zusammenhang. Wie weit greift also die Entgrenzung und welche Implikationen hat dies für den Krieg im Netz.

6.1.3 Die Rolle von Zeit und Raum im Cyberspace

Da im Cyberspace Information offensichtlich von Bedeutung ist und dem Faktor der Kraft, also wer im Cyberspace agiert, später Rechnung getragen wird, wird im Folgenden der Bedeutung von Zeit und Raum im Netz die Aufmerksamkeit gewidmet. Der Cyberspace bietet uns eine alternative Raum-Zeit-Struktur.⁵³⁹ Da die Operation als Teil des Krieges ein koordiniertes Handeln nach Zeit und Raum bedeutet,⁵⁴⁰ ist es notwendig, sich damit in Bezug auf den Cyberwar auseinander zu setzen. Um diese Rolle zu analysieren sei darauf verwiesen, dass der Cyberwar durchaus in Analogie zum Luftkrieg steht. Daher wird zunächst die Bedeutung dieser beiden Faktoren an Hand einer Aussage von Douhet dargestellt.

„Gegen diese neue Waffe gibt es keinen Schutzpanzer. Sie vermag schnell und unvermutet schon mit dem ersten Schlag den Todesstoß bis ins Herz des Gegners zu führen.“⁵⁴¹

Dies trifft auch auf den Cyberwar zu, durch die Nutzung des physikalischen Netzes kann ein Effekt in Lichtgeschwindigkeit im Ziel zum Tragen kommen. Dieser Effekt kann durchaus verheerende Folgen mit sich bringen, denkt man hier an die Ausschaltung vitaler Infrastrukturen, wie

⁵³⁸ Kirchmann, 1869, S. 269.

⁵³⁹ Vgl. Klauninger, Bert: Cyberspace als ein selbstorganisierendes System, o.J.
http://archive.gpi-online.de/files/_klauninger_cyberspace.pdf, S. 2, [12.05.2020].

⁵⁴⁰ Vgl. Freudenberg, 2008, S. 58.

⁵⁴¹ Douhet, 1935, S. 17.

zum Beispiel der Elektrizitätsversorgung. Dieser Blackout ist in der Lage ein Gemeinwesen nachhaltig zu treffen. Die Geschwindigkeit ist aber relativ, vielfach sind Angriffe bereits in der physikalischen Ebene angelegt. Der Faktor Zeit wird insoweit unterlaufen, als dass ein System schon lange Zeit vor Angriffsbeginn korumpiert sein kann. Die Faktoren Raum und Zeit wurden zusehends irrelevanter für die Durchführung jeglicher Handlungen zwischen Menschen.⁵⁴²

Der Raum spielt für den, der einen Angriff im Netz durchführen will, nur eine untergeordnete Rolle, er kann sich von überall Zutritt verschaffen, allein in Bezug auf das Ziel hat der Raum hier eine Relevanz, das heißt wo es sich befindet. Ein Krieg ohne räumlichen Bezug ist deshalb nicht denkbar. Ein Kriegsgebiet kann sich soweit bestimmen, als die Waffenwirkung reicht. Im Cyberspace ist der gesamte Raum ein mögliches Kriegsgebiet, denn die Wirkung von Cyber Waffen ist total entgrenzt. Der Cyberspace hat auf bewaffnete Konflikte einen ähnlichen Einfluss wie das Vorgehen irregulärer Akteure. Durch das Netz und die irregulären Akteure hat das Gefechtsfeld der Zukunft eine gesteigerte Tiefendimensionierung erfahren.

Der Informationsraum erlaubt es Einzelpersonen oder kleinen Gruppen, praktisch über alle Grenzen hinweg, Macht auszuüben. Es können dies gezielte, politisch motivierte Angriffe, ohne Einbindung von Streitkräften, sein. Der Cyberwar wird dabei vor, während und nach klassischen Kampfhandlungen geführt. Der Krieg wird somit ortsungebunden, anonym und ohne Unterscheidung zwischen Militär und Zivil geführt. Information wird regelrecht zur Waffe. Es gibt hier aber auch die Möglichkeit zu beeinträchtigen – ohne zu zerstören. Der Einsatz kann überraschend und verdeckt erfolgen. Auch anderen Konfliktformen, wie dem Cyber Terror, werden neue Möglichkeiten eröffnet.

„Die Natur des Netzwerkes, der internationale Charakter, die chaotische Struktur, der einfache Zugang und seine Anonymität bieten eine ideale Arena für irreguläre Aktionen.“⁵⁴³

Dabei wird das Netz nicht nur zur Koordination genutzt, sondern auch um direkt auf Ziele zu wirken. Einerseits schrumpft der Raum auf Grund der Reichweite der Waffensysteme zusammen, andererseits wird er durch die Globalisierung weiter ausgedehnt. Diese neue Raumdimension führt zu einer weiteren Entgrenzung von Konflikten, an deren Spitze der Krieg steht. Das Denken von Entscheidungsträgern muss sich in gleichem Masse erweitern, da sich die Bedrohungen nicht mehr an unseren Grenzen manifestieren. Von Sicherheit muss man somit in Zukunft ein funktionales, systemisches und kein räumliches (innen und außen) Verständnis haben.

Der Konflikt im Cyberspace betrifft alle Bereiche eines Gemeinwesens und hat damit eine totale Dimension.⁵⁴⁴ Präziser ausgedrückt betrifft ein

⁵⁴² Vgl. Vortrag von Mag. Tatschl im Rahmen des 19. Generalstabslehrganges zum Thema Cyberspace, Landesverteidigungsakademie, 27.11.2012.

⁵⁴³ Freudenberg, 2008, S. 326.

⁵⁴⁴ Vgl. Klimburg, Alexander: Gesamtstaatliche Ansätze zur Cybersicherheit. Erfahrungen aus Österreich. In: Pucher, Johann; Frank, Johann (Hrsg.): Strategie und Sicherheit 2012.

Konflikt im Cyberspace alle Bereiche, aller miteinander durch diesen Raum verbundenen Gemeinwesen. Durch die totale Vernetzung zeigt sich die Entgrenzung deutlich. Diese Totalität hat massive Auswirkung auf die Art der Führung von bewaffneten Konflikten im Cyberspace.

Viele Bereiche eines Gemeinwesens sind zum Teil, wenn nicht gänzlich, auf den Cyberspace abgestützt.⁵⁴⁵ Die Raumkategorie ist somit eine wesentliche, um die Auswirkungen von bewaffneten Konflikten im Cyberspace zu verstehen. Konflikte sind eine Interaktionsform zwischen Menschen. Es geht im Folgenden darum darzustellen, was den Cyberspace als Handlungsraum des Menschen kennzeichnet und wie er diesen Raum, mit den damit zusammenhängenden Herausforderungen für sich nutzbar macht.

6.2 Zum Cyberspace als menschlichen Handlungsraum

Informationen und Daten sind die Kernressourcen im Cyberspace. Deren Übertragung, Verarbeitung und Speicherung im Netz schaffen einen virtuellen Raum, in dem ein Agieren und Interagieren von Menschen möglich wird. Dies gilt auch für den Konflikt als mögliche Interaktionsform in diesem virtuellen Raum. Dieser steht auch im Fokus der Betrachtung des Cyberspace als menschlicher Handlungsraum.

„Die bewaffneten Konflikte der modernen Welt zeichnen sich nicht nur durch neue Akteure – wie z.B. Terroristen oder private Sicherheitsfirmen –, sondern auch durch neue Waffen bzw. Methoden der Kriegsführung aus.“⁵⁴⁶

Die Waffen, welche in einem Konflikt in diesem Raum zur Anwendung gelangen, sind nicht nur virtueller Natur. Es handelt sich einerseits um Programme, also Algorithmen, welche die Informationen zerstören, stören oder verfälschen, also um direkte Wirkmittel bezogen auf den Cyberspace. Andererseits kann es sich um physische Gegenstände handeln, welche indirekt Einfluss auf die, die Information repräsentierenden, Zustände physikalischer Natur im Netz ausüben. Diese, seitens des Angreifers gewollte bzw. seitens des Angegriffenen ungewollte, Beeinflussung ist Ergebnis einer konfliktischen Interaktion im Cyberspace. Die Beschaffenheit von Informationen und die Bedeutung von Daten stehen am Anfang der folgenden Betrachtungen.

6.2.1 Die Information als zentrale Ressource

Daten und Informationen sind die zentralen Bausteine des virtuellen Raumes.⁵⁴⁷ Der Begriff der Information ist zwischen Empirie und Rationalität

Der Gestaltungsspielraum der österreichischen Sicherheitspolitik, 2012, S. 463ff. (in: Pucher/Frank, 2012)

⁵⁴⁵ Vgl. Gaycken, Sandro: Cyberwar. Das Wettrüsten hat längst begonnen; vom digitalen Angriff zum realen Ausnahmezustand, 1. Aufl., München 2012, S. 34.

⁵⁴⁶ Ziolkowski, 2008, S. 202. (in: Humanitäres Völkerrecht Informationsschriften, 2008)

⁵⁴⁷ Vgl. Hülsmann, 2000, S. 53f.

anzusiedeln. Er beinhaltet stets eine syntaktische und eine semantische Komponente. Die Informationsmenge gibt schließlich keinen Aufschluss darüber, welche Bedeutung die Information hat. Eine Information wird im Netz zur Interaktion benötigt. Informationen haben eine, die Realität beeinflussende, Bedeutung. Auf Grund von Informationen werden Handlungen ausgeführt oder unterlassen. Informationen geben Auskunft über Zustände in der virtuellen und realen Welt. Informationen werden im Netz codiert und als Daten übertragen und verarbeitet bzw. gespeichert. Information benötigt einen Träger, dies kann zum einen Energie, in Form elektrischer Signale, zum anderen Materie, wie etwa ein Buch sein. Information ist ohne Träger nicht existent. Im Sinne Spinozas ist Denken und Ausdehnung eine Einheit. Anders als deren Träger ist die Information in der Lage, erhalten zu bleiben bzw. vermehrt zu werden, wenn sie weitergegeben wird.

Gayken fasst die Information als Wissen und Meinen und sieht darin nicht nur die Schlüsselressource im Netz, sondern auch eines der potentiellen Angriffsziele.⁵⁴⁸ Wie bereits dargestellt, wirken Konflikte auf zwei Arten im Netz, zum einen auf die Informationen selbst, zum anderen durch die Informationen auf die reale Welt. Information als Ziel unterliegt der Manipulation, dem Diebstahl und der Zerstörung. Diese Wirkungen auf die Information stellen eine große Gefahr dar. Um sich davor zu schützen, wurden Daten im Netz immer zentral an besonders gut geschützten Orten verwahrt. Dabei spielte der Zugang zu diesem geschützten Bereich stets die entscheidende Rolle. Zugriffe auf solche besonders gut geschützten Systeme sind aber auf vielfältige Art und Weise möglich.

Ist der Angreifer erst im System, stehen ihm alle Daten auf einmal zur Verfügung. Eine Perplexität der Datenhaltung ist hier ein von Schönberger vertretener Ansatz.⁵⁴⁹ Viele Daten und deren dezentrale Datenhaltung sollen einen besseren Schutz gewährleisten. Daten werden aber deshalb zentral gehalten, um sie besser kontrollieren und überwachen zu können, wobei dies bereits einen Angriff für sich darstellt.⁵⁵⁰ Information ist nicht nur mögliches Ziel von Angriffen, sondern eben auch eine mögliche Waffe. Die Waffen, welche in diesem Raum zur Anwendung gelangen, können ebenfalls auf Daten und Informationen aufbauen. Saalbach definiert die Waffe im Cyberspace wie folgt:

„Cyberwaffen sind demnach Softwareprogramme, mit deren Hilfe man andere Computer angreifen, infiltrieren, ausspionieren und manipulieren kann und die ihre Ausbreitung selbsttätig steuern können.“⁵⁵¹

Diese Definition greift etwas zu kurz, denn sie bezieht sich nur auf die Waffen, die direkt im Netz zur Wirkung gelangen können, ohne jene Kategorie von Wirkmittel zu berücksichtigen, die indirekt auf Informationen wirken

⁵⁴⁸ Vgl. Gayken, 2011, S. 93ff.

⁵⁴⁹ Vgl. Vortrag von Dr. Schönberger im Rahmen der IKT-Sicherheitskonferenz zum Thema Cybersicherheit, Vila Vita, 12.11.2012.

⁵⁵⁰ Vgl. Assange/Apfelbaum/Müller-Maguhn, 2013, S. 86f.

⁵⁵¹ Saalbach, K.: Cyberwar. Grundlagen-Methoden-Beispiele Version 4.0, 2012, S. 15.

können. Um den Begriff der Waffe im Netz ganzheitlich zu fassen, ist eine Unterteilung der möglichen Waffen in drei Gruppen nötig.⁵⁵² Zum einen haben wir die Gruppe der logischen oder virtuellen Waffen, dazu zählen Schadprogramme, die auf die Informationen im Cyberspace wirken.⁵⁵³ Der zweiten Gruppe sind Waffen zuzurechnen, welche nicht auf die Informationen im Netz wirken, zumindest nicht direkt, sondern auf die physische Infrastruktur des Cyberspace wirken.⁵⁵⁴ Dazu zählen neben den konventionellen Mitteln spezielle Waffen, wie Nuklear-Elektromagnetische-Puls(NEMP)-Waffen.

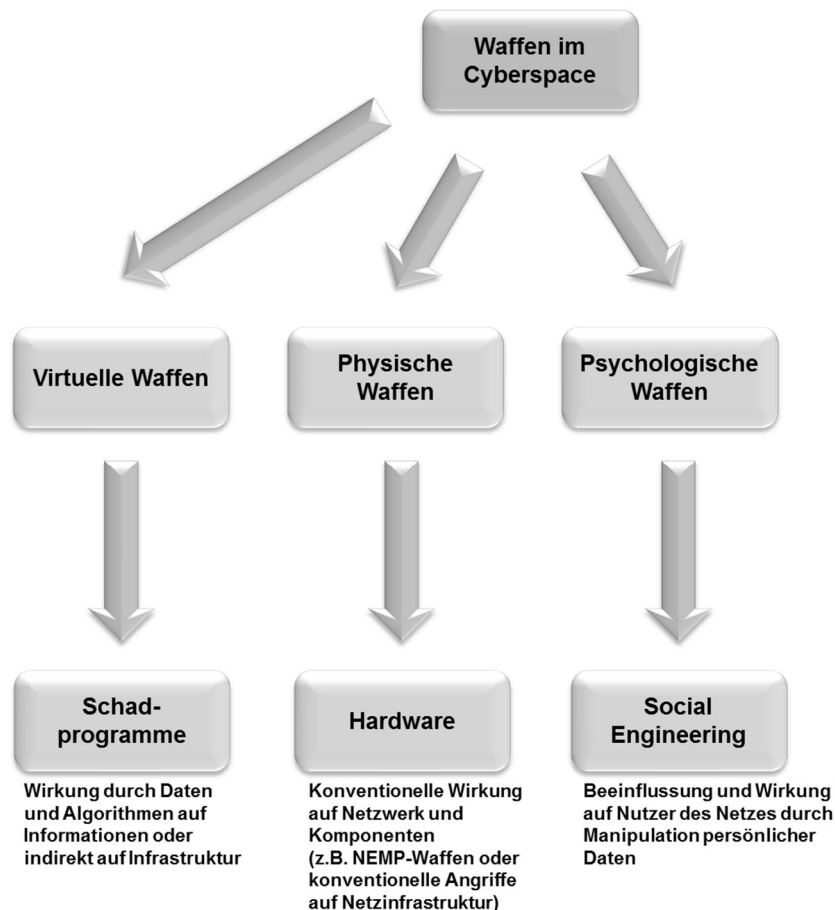


Abbildung 7: Einteilung der Waffen im Cyberspace⁵⁵⁵

In den Bereich der physischen Waffen sind auch die physikalischen Hintertüren in der Hardware der Netzwerke zu zählen.⁵⁵⁶ Der bewusste oder unbewusste Einbau von Schwachstellen in die Hardware ermöglicht deren Ausnutzung über spezielle Programme. Im Gegensatz zu den virtuellen und

⁵⁵² Vgl. Address, Jason; Winterfeld, Steve: Cyber Warfare, Techniques, Tactics and Tools for Security Practitioners, 1. Aufl., 2011, S. 119ff.

⁵⁵³ Vgl. Sommer, Peter; Brown, Ian: Reducing Systemic Cybersecurity Risk 2011, S. 25f. Anm. d. Verf.: Die Wirkung ist dabei nicht nur auf den Cyberspace beschränkt, sondern kann indirekt auf die davon abhängige Infrastruktur wirken.

⁵⁵⁴ Vgl. ebd., S. 27f.

⁵⁵⁵ Abbildung durch den Verfasser erstellt.

⁵⁵⁶ Vgl. Address/Winterfeld, 2011, S. 126f.

physischen Waffen haben die psychologischen Waffen, als dritte Gruppe, den Menschen, als Teil des Cyberspace, zum Ziel.

Dabei geht es um die Beeinflussung von Individuen, um deren Vertrauen zu gewinnen und durch deren Manipulation an Informationen zu gelangen.

„Social Engineering is the act of influencing someone`s behavior through manipulating their emotions, or gaining and betraying their trust to gain access to their system.“⁵⁵⁷

Durch die Schaffung einer Beziehung zur Zielperson und das Erlangen von Vertrauen, wird diese dazu gebracht Handlungen zu setzen oder Informationen preiszugeben, welche dann zu deren Nachteil genutzt werden können.⁵⁵⁸ Diese Ausnutzung zum Nachteil der Zielperson kann dann durch andere Waffen im Cyberspace realisiert werden. Die Wirkung durch die psychologische Waffe ist daher, anders als bei den anderen beiden Waffen, nicht unmittelbar gegeben.

Durch die enge Verschränkung – von physikalischer Infrastruktur und virtueller Netzwerkumgebung – ergibt sich einerseits die Infrastruktur als Ziel, aber andererseits auch als Waffe im Kampf im Cyberspace.⁵⁵⁹ Durch Ausnutzung von Einfallstoren ist die Wirkung auf Informationen im Netz möglich. Information ist sowohl Mittel als auch Ziel von Angriffen. Die virtuelle Welt ist abhängig von der realen Welt und umgekehrt. Eine wechselseitige Beeinflussung ist somit angezeigt. Um den Krieg im Netz zu fassen, ist eine Betrachtung beider Sphären, der Virtualität und der Realität, notwendig. Auf welche Art finden die Interaktionen im Netz statt, und wie äußert sich eine kriegerische Interaktion im Cyberspace?

6.2.2 Die Interaktion im Netz

Interaktionen im Netz reichen von der Kooperation bis hin zum Krieg. Das Besondere daran ist die Entgrenzung und die daraus resultierende Reichweite von Interaktionen. Viele davon finden nicht mehr an bestimmte Räume gebunden statt, sind also nicht mehr an territoriale Grenzen gebunden, es kann hier von einer Deterritorialisierung gesprochen werden.⁵⁶⁰ Akteure handeln in Netzwerken, welche nicht von territorialer Zugehörigkeit abhängen.

Es handelt sich um Funktionszusammenhänge und Interaktionen von, zu einem Netzwerk zusammengefügt, Knotenpunkten. Dies können einzelne Individuen, Organisationen oder auch Computer sein.⁵⁶¹ Diese Interaktionen basieren auf Informationen, die über das Netz ausgetauscht werden. Das Netz erweitert somit die menschliche Wahrnehmungs- und Handlungsmöglichkeiten. Dabei ist ein direktes Gegenübertreten zwischen

⁵⁵⁷ Andress/Winterfeld, 2011, S. 139.

⁵⁵⁸ Vgl. ebd., S. 140.

⁵⁵⁹ Vgl. Hofstetter, 2019, S. 78.

⁵⁶⁰ Vgl. Freudenberg, 2008, S. 37.

⁵⁶¹ Vgl. ebd., S. 41.

den Akteuren bzw. Beteiligten an der Interaktion nicht mehr zwingend notwendig.

In der kriegesischen Auseinandersetzung im Cyberspace kommen daher bestimmte Methoden zur Anwendung. Anders als im konventionellen bewaffneten Konflikt sind die meisten der virtuellen Methoden der offensichtlichen Wahrnehmung entzogen. Die Verfahren, die angewandt werden, orientieren sich an einem generellen Muster.

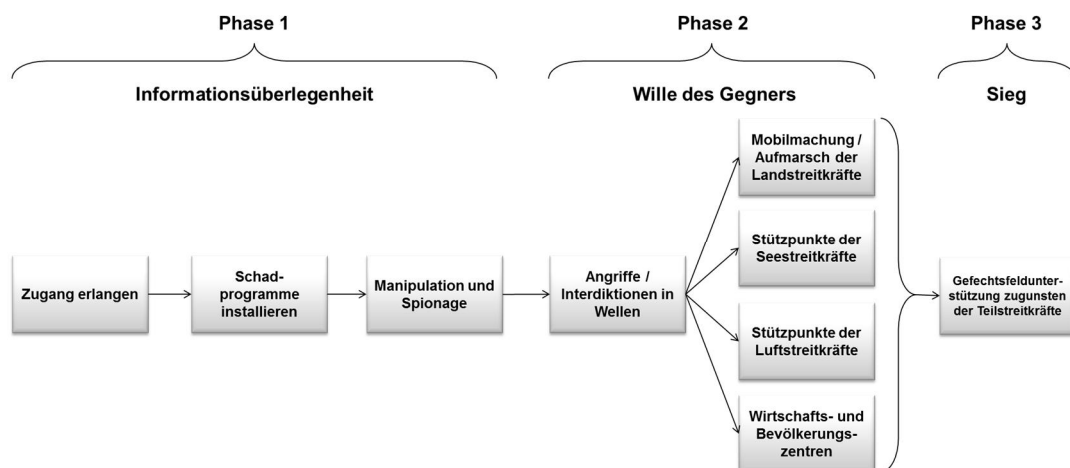


Abbildung 8: Das Konzept der virtuellen Kriegführung⁵⁶²

Hier kann eine Analogie in der Luftkriegführung gesehen werden. Nach Douhet erfolgt der Luftkrieg in drei Phasen.⁵⁶³ Die erste Phase dient der Erlangung der Luftherrschaft, indem die gegnerische Luftwaffe und die gegnerische Führung zerschlagen werden. Es folgt in Phase zwei die Brechung des Widerstandes und des Willens zur Verteidigung, um in Phase drei den Sieg zu erlangen.

Um nun die Informationsherrschaft (Anm. d. Verf.: Gemeint ist die Informationsüberlegenheit.) zu erzielen, ist in Phase eins des Cyberwar die Notwendigkeit gegeben, sich Zugang zum gegnerischen System zu verschaffen, um neben der Installation von entsprechenden Waffen auch Aufklärung und Informationsbeschaffung zu betreiben. Dazu gehört es, wichtige Informationen zu beeinflussen, um die Phase zwei einleiten zu können. Phase zwei zielt auf den Willen des Gegners, indem seine Streitkräfte und die Bevölkerung im Netz angegriffen werden. Die Angriffe auf vitale, kritische Infrastrukturen oder Waffensysteme sind hier zu nennen. In der letzten Phase werden, bei einem konventionellen Ansatz eigener Streitkräfte, diese mit Maßnahmen im Cyberspace unterstützt.

Vielfach ist die Phase eins jene, die im Frieden bereits erreicht ist. In Bezug auf eine Wettbewerbssituation zwischen Staaten ergibt sich die Nutzung von Wirkmitteln im Cyberspace, die es ermöglichen wichtige

⁵⁶² Abbildung durch den Verfasser erstellt. (nach einer Idee von Saalbach, 2012)

⁵⁶³ Vgl. Stahel, Albert A.: Klassiker der Strategie. Eine Bewertung, 4. Aufl., Zürich 2004, S. 212.

Informationen aus dem Netz zu generieren. Dabei handelt es sich meist um offene Informationen, welche für jedermann zugänglich sind. Diese dienen dann dazu eine Region, von Interesse für das Gemeinwesen, analysieren zu können. Diese Tätigkeiten, die der Generierung eines Lagebildes dienen, liegen unter der Wahrnehmungsschwelle.

Diese Mittel werden nicht nur von Staaten angewandt, sondern auch von anderen Akteuren, wie zum Beispiel von großen Wirtschaftsunternehmen. Diese stehen in einer permanenten Wettbewerbssituation und nutzen den Cyberspace, um sich hier Vorteile gegenüber den Mitbewerbern zu verschaffen. Dabei sind die Maßnahmen in Phase eins diejenigen, welche zur Anwendung gelangen. Interessant im Zusammenhang mit dem Krieg im Netz ist die Inversion zum konventionellen Krieg. Dabei werden Sichtbarkeit und Betroffenheit zu wichtigen Faktoren. Die Anwendung der Methoden in Phase eins eines Cyber Konfliktes wird nicht wahrgenommen, weil sie nicht sichtbar ist, sondern im Verborgenen stattfindet.

Die Inversion besteht nun darin, dass vor allem Gemeinwesen nicht daran interessiert sind, ihre Tätigkeiten offen durchzuführen, diese geschehen im Geheimen. Die Irregulären sind im Gegensatz dazu oft darauf bedacht, dass ihre Aktivitäten wahrgenommen werden. Gruppen wie Anonymous haben ihre Erfolge der Sichtbarkeit ihrer Aktionen zu verdanken. Im konventionellen Konflikt ist die Sichtbarkeit in der Wirkung gegeben, während im Cyberspace diese Sichtbarkeit bei regulären Streitkräften unerwünscht scheint. Als Begleitmaßnahme von konventionellen Konflikten, das bedeutet in Phase drei des Cyberwar Konzeptes, ist die Sichtbarkeit in der Wirkung wieder gegeben. Hier ist der Cyberwar eine klassische Unterstützungsmaßnahme der konventionellen Streitkräfte.

Es lassen sich von der Methodik her zwei Formen des bewaffneten Konfliktes im Cyberspace ableiten, der Krieg im Geheimen und die Unterstützung von konventionellen Kräften in einem konventionellen Konflikt. Man könnte diese beiden Formen des Cyberwar, in Analogie zum Krieg, auch als Großen und Kleinen Cyberwar bezeichnen. Bei der Kriegführung, aber auch bei anderen Formen der Interaktion im Netz, ergeben sich in diesem Zusammenhang einige besondere Herausforderungen. Diese werden im Folgenden erörtert.

6.2.3 Attribution, Anonymität und Anarchie als zentrale Herausforderungen

Attribution bedeutet die Zuordnung von Handlungen im Cyberspace, oder anders gesagt die Identifikation von handelnden Personen im Netz. Auf den Cyberwar ausgerichtet bedeutet dies, die Identifikation eines Angreifers und damit die Zuschreibung eines Angriffs.⁵⁶⁴ Will man einen Angriff verhindern, so besteht die Möglichkeit dies mit Mitteln der Abschreckung zu realisieren. Wenn aber die Identifikation nicht gegeben ist, bleibt Abschreckung wirkungslos. Auf Grund der fehlenden Attribution kann ein Angreifer davon ausgehen, nicht unmittelbar erkannt zu werden. Potentielle

⁵⁶⁴ Vgl. Gayken, 2011, S. 80.

Gegenmaßnahmen, also die Abschreckung, brauchen ein Ziel, ist dieses nicht identifizierbar, bleiben sie ohne Wirkung.

Je nach Motivlage und Zweck des Angreifers kann einem Angriff kriminalistisch oder militärisch begegnet werden. Ziolkowski sieht darin die Kernherausforderung für die Zuordnung der Führungsverantwortung:

„Dies dürfte die rechtliche Analyse eines *Cyber*-Angriffs sowie die Entscheidung über Handlungsalternativen des Angegriffenen erheblich erschweren. Bei Ungewissheit über das Vorliegen eines *Cyber*-Angriffs bzw. über die Identität des Angreifers und den Ursprungsort des Angriffs wird folgerichtig unklar bleiben, ob die Polizei bzw. die Staatsanwaltschaft des eigenen oder – im Rahmen der internationalen Rechtshilfe – eines anderen Staates, die Streitkräfte (falls der *Cyber*-Angriff in seiner Wirkung einem konventionellen Angriff fremder Streitkräfte gleicht) oder aber die Administratoren des eigenen Computernetzwerkes tätig werden müssen.“⁵⁶⁵

Dazu ist aber die Attribution eine Vorbedingung. Diese Identifikation ist auch für die Wahl der Gegenmaßnahmen wichtig. Diese können nur dann entsprechend ausfallen, wenn der Angreifer und seine Motivation klar identifiziert wurden. Eine ständige Beobachtung des Cyberspace und die Generierung eines entsprechenden Lagebildes sind für die Erkennung, woher ein Angriff kommt, essentiell. Dabei ist nicht nur die Motivation des Angreifers, sondern auch eine Anzahl weiterer Faktoren wichtig.

„To truly identify the enemy, we need to look at the targets, sources, attackers, and sponsors of the activity that we are monitoring.“⁵⁶⁶

Es können hier vier Arten der Attribution erkannt werden: Die territoriale Attribution, die personelle Attribution, die motivationale Attribution und die kontextuelle Attribution.⁵⁶⁷ Da Angriffe im Netz nicht nur direkt erfolgen, kann mit diesen Methoden eine genauere Analyse erfolgen. Dennoch lässt sich auch damit letztlich nicht eindeutig ermitteln, wer für einen Angriff verantwortlich zeichnet.⁵⁶⁸ Dies macht die Reaktion auf Angriffe im Netz so schwierig.

„Juristisch, politisch und strategisch ist Attribution also eine Kerngröße.“⁵⁶⁹

Die Non-Attribution im Cyberspace hat massive Auswirkungen auf die Reaktion bezüglich der Angriffe im Netz und somit auf die Konzeption von Kriegen.⁵⁷⁰ Der Krieg im Geheimen, der Große Cyberwar ist eine Form des Krieges, die für den Angreifer Vorteile hat. Dieser Krieg ist von asymmetrischer Natur, da der Angreifer einem Verteidiger meistens überlegen ist. Da er sich über eine große Bandbreite an Wirkungsbereichen

⁵⁶⁵ Ziolkowski, 2008, S. 205. (in: Humanitäres Völkerrecht Informationsschriften, 2008)

⁵⁶⁶ Andress/Winterfeld, 2011, S. 156.

⁵⁶⁷ Vgl. Gayken, 2011, S. 84ff.

⁵⁶⁸ Vgl. Hofstetter, 2019, S. 198.

⁵⁶⁹ Ebd., S. 81.

⁵⁷⁰ Vgl. ebd., S. 81.

(PMESII) erstreckt, hat er auch eine strategische Ausdehnung. Weniger problematisch erscheint die Non-Attribution im Rahmen eines konventionellen Konfliktes, in dem der Cyberwar als Unterstützungselement zum Tragen kommt.

Die Reaktion wird hier auf den Gegner gerichtet sein, welcher durch die konventionelle Kampfführung sichtbar ist. Dieser kleine Cyberwar wirkt vor allem auf der operativen und taktischen Ebene, da er hauptsächlich gegen militärische Systeme⁵⁷¹ gerichtet ist. Generell kann hier festgehalten werden, dass der Kampf gegen einen klar erkennbaren Gegner leichter fällt als gegen einen nicht erkennbaren Feind. Technisch verfügen die Datenpakete im Netz über Informationen, welche eine Attribution grundsätzlich ermöglichen könnten.

Der sogenannte Header beinhaltet Informationen über den Absender des jeweiligen Datenpaketes. Diese Information kann jedoch manipuliert und verändert werden. Somit ist eine Absenderadresse kein sicherer Indikator.⁵⁷² Eine direkte Rückverfolgung ist, auf Grund der dynamischen Zwischenspeicherung der Absenderdaten, nicht ohne weiteres möglich, eine Lösung stellt hier die umstrittene Vorratsdatenspeicherung⁵⁷³ durch die Provider dar. Diese würde eine Zuordnung eines Angriffes ermöglichen, ist jedoch rechtlich nicht unumstritten.

Die Non-Attribution schafft eine Anonymität im Cyberspace, die einen Angreifer schützt. Anonymität fördert aber auch zunehmend rechtswidriges Verhalten im Netz und ist somit nicht nur ein Problem bei der Identifizierung eines Angreifers. In der Geschichte vom Ring des Gyges zeigt Platon, dass Anonymität oder besser der Glaube daran, nicht erwischt zu werden, dazu führt, dass selbst Gerechte einen Hang zur Ungerechtigkeit zeigen.⁵⁷⁴ Die Gesetze greifen dann, wenn die Vernunft gebietet, sich an die Regeln zu halten, weil man sich für sein Handeln verantworten muss. Der Vernünftige ist dazu geneigt gerecht zu sein. Platon zeigt hier, dass sich der Mensch, wenn er sich nicht zu verantworten hätte, nicht regelkonform verhalten würde.

Diese Anonymität, die durch die Non-Attribution entsteht, ist der Faktor, der den Angreifer gegenüber dem Verteidiger bevorteilt.

„The low cost and largely anonymous nature of cyber space makes it an attractive domain for use by those who seek to use cyber space for malicious purposes. These include criminals, terrorists, and states, whether for reasons of espionage, influence or even warfare.“⁵⁷⁵

⁵⁷¹ Anm. d. Verf.: Dazu zählen auch Subsysteme der politischen Entscheidungsebene.

⁵⁷² Vgl. Gayken, 2011, S. 82.

⁵⁷³ Anm. d. Verf.: Bei der Vorratsdatenspeicherung würde eine ständige Überwachung des Datenverkehrs stattfinden ohne konkreten Verdacht. Hier käme es zu einer Verletzung des Datenschutzes und der informationellen Selbstbestimmung. Ein hochbegabter Angreifer wird trotzdem in der Lage sein seine Identität zu verschleiern, weil zum Beispiel nicht alle Staaten die Möglichkeit der Vorratsdatenspeicherung einführen werden. Wenn also nicht alle Staaten kooperieren, bleiben Hintertüren für Angreifer offen.

⁵⁷⁴ Vgl. Platon, Politeia, S. 248f.

⁵⁷⁵ United Kingdom Cabinet Office, Cyber Security Strategy, 2009, S. 12.

Es kommt zu einer Asymmetrie, zwischen leicht durchführbarem Angriff und extrem schwieriger Verteidigung. Diese Asymmetrie macht den Großen Cyberwar zu einer Konfliktform, in der höchstens die Auswirkungen offensichtlich und erkennbar sind. Akteure und Motivation bleiben im Verborgenen. Personell ist eine Zuordnung zwischen Kombattanten und Nicht-Kombattanten für den Einsatz des Militärs entscheidend. Auch die Frage nach der Absicht eines Angriffs liefert Rückschlüsse, mit welchen Mitteln man auf ihn reagieren darf. Handelt es sich um einen kriminellen oder einen politischen Hintergrund? Allein diese Absichten sind aus einem Angriff, einer Handlung im Netz nur schwer ablesbar.

Motivationen haben einen hohen Unsicherheitsfaktor und sind ein Kernproblem von Kriegen. Zu der Non-Attribution und der daraus resultierenden Anonymität, kommt ein weiterer Faktor, die Anarchie des Cyberspace hinzu. Diese äußert sich darin, dass selbst Individuen in der Lage sind, in gleicher Art und Weise im Netz zu handeln wie Gruppen von Menschen oder Gemeinwesen. Hinter einem Cyber Angriff können verschiedene Akteure stecken, denn auch nichtstaatliche Akteure können einen Cyber Konflikt beginnen. Alle Akteure sind gleich in ihrer Anonymität und es fehlt an einem übergeordneten Ordnungsprinzip im Cyberspace.

Die drei Parameter, die als die Herausforderungen im Netz gefasst werden können, stehen in gegenseitiger Abhängigkeit. Die Unregulierbarkeit, die Anarchie des Cyberspace, fußt vor allem auf der Non-Attribution und der daraus resultierenden Anonymität. Angriffe sind nicht als zivile oder militärische erkennbar und müssen daher erst geklärt werden.⁵⁷⁶ Dieses Clearing kann entweder vom Militär oder der Polizei wahrgenommen werden.

„Die hohe Zahl kriminell motivierter Angriffe spricht für ein Clearing durch Kriminalisten, während die wesentlich höheren Risiken durch militärische Angriffe für ein Clearing durch Militärs sprechen.“⁵⁷⁷

Diese Feststellung lässt die Frage nach der Unterscheidung zwischen den Zuständigkeiten aufkommen. Welche Intensität entspricht einem hohen Risiko? Dieser Frage wurde beim Kriegsbegriff bereits nachgegangen. Eines lässt sich hier festhalten: der Große Cyberwar ist von seinem Wesen her als Krieg im Verborgenen, als sogenannter Kleiner Krieg, zu fassen. Er kann von jedermann geführt werden und bedient sich asymmetrischer Mittel und Methoden. Wird er von Staaten geführt, kann auf Grund der Anonymität keine Zuordnung an das Gemeinwesen als Akteur getroffen werden.

Der Kleine Cyberwar ist hingegen eine Unterstützungsmaßnahme des konventionellen bewaffneten Konfliktes zwischen Gemeinwesen und, auf Grund dieser Interaktion, zumindest grob den Akteuren an diesem Konflikt zuordenbar (Anm. d. Verf.: Auch hier sind Täuschung und Einmischung dritter Akteure möglich.). Im Zusammenhang mit der Attributionsproblematik ergeben sich auch Friktionen in der Anwendung des Völkerrechts und des Rechts auf Selbstverteidigung nach der Satzung der Vereinten Nationen. Den Möglichkeiten der rechtlichen Ordnung im

⁵⁷⁶ Vgl. Gayken, 2011, S. 196.

⁵⁷⁷ Ebd., S. 196.

Cyberspace wird in der rechtswissenschaftlichen Untersuchung des Cyberwar nachgegangen.

Zunächst soll nun aber die Rolle des Cyberspace als Domäne des Krieges dargestellt werden, um diesen Raum als möglichen Handlungsraum für das Militär – als militärischen Einsatzraum – zu beschreiben.

6.3 Zum Cyberspace als militärischen Einsatzraum

Da der Cyberspace, wie bereits festgestellt wurde, der Interaktion von Menschen dient und überall wo Menschen in Interaktion treten auch Konflikte entstehen, kommt dem Cyberspace als Ganzem eine große Bedeutung hinsichtlich der Kriegführung zu. Im folgenden Abschnitt wird der Cyberspace einer genauen militärischen Betrachtung unterzogen, um seine Möglichkeiten, aber auch seine Gefahren- und Bedrohungspotentiale, darzustellen.

6.3.1 Cyberraum als Dimension des Krieges

Auf Grund der technologischen Entwicklung des Militärs hat der Cyberraum eine entscheidende Bedeutung bei der Steigerung der Effizienz von Streitkräften. Das Verfahren, welches dabei zur Anwendung gelangt, ist die sogenannte Netzwerkorientierte Operationsführung, die ein Zusammenwirken von Aufklärung, Führung und Wirkung anstrebt. Dabei werden Informationen und Daten auf drei miteinander verbundenen Netzwerkebenen ausgetauscht.

Der militärische Teil des Cyberraums ermöglicht also die Unterstützung der Streitkräfte, unabhängig von der Dimension in welcher sie agieren, in dem er den Austausch von Daten zwischen den einzelnen Teilstreitkräften und den drei Netzwerkebenen ermöglicht. Das Einwirken auf die Netzwerkebenen des Gegners stellt somit eine logische Maßnahme dar, um dessen Effizienz beim Einsatz seiner Mittel zu minimieren.

Der Kampf um und mit Informationen durchwirkt damit alle Teile des Militärs und ermöglicht so erst neue Konzepte der Kriegführung, wie die sogenannten Multidomain Operations.⁵⁷⁸ Der Begriff des Cyberspace ist dabei nicht zu eng zu fassen. Die Möglichkeiten zur indirekten Wirkung auf den Staat und seine Streitkräfte ist auf allen Ebenen dieses Raumes, mit unterschiedlicher Qualität, möglich.

„Netzwerkorientierte Verfahren verwenden in der idealtypischen Form die Entwicklungen der Informationstechnologie um eine höhere Geschwindigkeit im Führungsprozess sowie eine bessere Synchronisierung aller militärischen Kräfte (teilstreitkraftübergreifend) zu erreichen. Dies wird erreicht, indem

⁵⁷⁸ Vgl. Reilly, Jeffrey M.: Multidomain Operations, A Subtle but Significant Transition in Military Thought. In: Air & Space Power Journal (ASPJ), Volume 30, Issue 1, Spring 2016, S. 61-73. https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-30_Issue-1/V-Reilly.pdf, [12.05.2020].

Computernetzwerke mit Sensoren, Führungseinrichtungen und Waffensystemen verbunden werden und ein gemeinsames Lagebild in nahezu Echtzeit an alle räumlich aufgeteilten Kräfte, Systeme und Kommandanten verteilt wird, und zwar in dem Ausmaß, wie sie es benötigen. Das Netzwerk wird von Komponenten mit sehr genau definierten Schnittstellen gebildet. Dieserart wird die Grundlage für Interoperabilität und eine kontinuierliche Entwicklung erreicht, wobei unter Interoperabilität die Kooperation von Systemen zur Erfüllung von Aufträgen verstanden wird. Das Netzwerk ermöglicht es, wertvolle Systemeigenschaften (z.B. Lagedarstellungen, Reichweiten von Waffensystemen usw.) zusammenzuführen, was insgesamt zu einer höheren Effizienz führt.“⁵⁷⁹

Bei diesem Verfahren werden alle Plattformen und Führungsebenen miteinander vernetzt, sodass alle gleichzeitig über ein aktuelles Lagebild verfügen. Dieses ermöglicht zu einem bestimmten Zeitpunkt das jeweilig bestmögliche Mittel zum Einsatz zu bringen und mit konzentrierten Effekten, ohne Massierung von Truppen, zu wirken.⁵⁸⁰ Diese Informationsübertragung und -verarbeitung findet in einem vom Militär genutzten Teil des Cyberraumes statt. Die Schnittstellen in diesen Raum hinein sind in den meisten Fällen nicht technischer, sondern humaner Natur. Dies birgt einen gewissen Schutz, aber auch Gefahren in sich, wenn es um die Einwirkung von außen geht.

Rein militärisch betrachtet ist der Krieg im Cyberraum der Kampf in den beschriebenen Netzwerkebenen des militärischen Teils dieser Dimension.⁵⁸¹ Viele militärische Netze haben aber Übergänge in den Rest des Cyberspace (zum Beispiel in das Internet), was zu einer möglichen Einwirkung von nicht-militärischen Akteuren in die militärischen Netze führt.

Die Tatsache, dass unser Leben von Computern durchdrungen ist und praktisch fast jeder Mensch auf der Erde Zugang zu solchen Systemen und damit zum Cyberspace hat, macht den Kampf in Computernetzen nicht zu einer alleinigen Angelegenheit der Militärs. Als möglicher Konfliktraum wird der Cyberspace, als potentieller Einsatzraum des Militärs, einer Analyse unterzogen. Es gilt nun zu untersuchen, durch welche Bereiche dieser Raum in welcher Art und Weise beeinflusst wird. Mit Hilfe einer Methode der operativen Planung, der Comprehensive Preparation of the Operational Environment (CPOE)⁵⁸², werden nun Schlüsselabhängigkeiten kurz dargestellt, um ein Gefühl für die Besonderheiten des Cyberspace zu bekommen.

⁵⁷⁹ BMLV, Netzwerkorientierte Verfahren Austria, 2006, S. 11.

⁵⁸⁰ Ebd., S. 13.

⁵⁸¹ Ebd., S. 8.

⁵⁸² Vgl. NATO, Comprehensive Operations Planning Directive, 2010, Chapter 4, S. 36.

6.3.2 Eine Einsatzraumreflektion für den Cyberwar

Diese Analyse des Einsatzraumes, für die Durchführung von militärischen Operationen, schafft ein Verständnis für die spezifischen Raumfaktoren des Cyberspace. Dieser ermöglicht den Zugang von jedem beliebigen Ort. Dabei kann die Anwendung verschiedener Schnittstellen, humaner oder technischer Natur, genutzt werden. Eine Abstützung auf Räume, die zur Bereitstellung von militärischen Kräften dienen, ist auf Grund der Unmittelbarkeit der aus den Aktionen resultierenden Effekten, nicht erforderlich. Operationen können sich auf die vorhandenen Kommunikationsrelationen abstützen. Entfernungen spielen in diesem Zusammenhang keine Rolle.

Durch die Unmittelbarkeit und Anonymität sind Aufklärung und Infiltration von Systemen begünstigt. Hindernisse stellen vor allem Zugangseinrichtungen dar, welche Subsysteme vom Netz trennen. Diese können auch als Schlüsselräume angesprochen werden. Aber auch die dahinterliegenden kritischen Infrastrukturen⁵⁸³ können als solche definiert werden. Dazu zählen alle jene Einrichtungen, die von vitalem Interesse für das Gemeinwesen sind. Der Cyberspace erlaubt die Operationsführung ohne Rücksicht auf klimatische oder meteorologische Parameter.

Ein Großteil der Bevölkerung in den hochintegrierten Regionen der Welt ist auf das Netz als Kommunikations- und Arbeitsmittel angewiesen. Diese Abhängigkeit fördert die Verwundbarkeit der Gemeinwesen. Andererseits fördert die Vernetzung die Interaktion zwischen räumlich getrennten Individuen und Gruppen von Individuen. Dieser Austausch über Grenzen hinweg fördert auch die Entwicklung. Die Beeinflussung der politischen Situation in den Gemeinwesen ist durch die Vernetzung und den Austausch von Informationen erleichtert. Regierungen werden dadurch leichter beeinflussbar. Diese haben jedoch die Möglichkeit im Umkehrschluss die Bevölkerung leichter mit Botschaften zu erreichen. Auf Ebene der Verwaltung werden Abläufe vereinfacht und für die Menschen leichter zugänglich gemacht.

Durch die hohe Vernetzung hat sich, aus militärischer Sicht, die Sicherheitslage massiv verändert.⁵⁸⁴ Ein Einwirken auf vitale Bereiche des Staates durch Aggressoren wird erleichtert. Diese Bereiche können aber nicht umfassend geschützt werden, da sie vielfach in privater Hand und die dazugehörige Informations- und Kommunikationstechnologie nicht auf dem Staatsgebiet des davon abhängigen Staates sind. Auch ist die Durchsetzung von Zwangsmaßnahmen, auf Grund der unzureichenden rechtlichen Rahmenbedingungen, erschwert. Die bei Angriffen im Netz verwendeten Waffen können in den seltensten Fällen als solche identifiziert werden.

Auch die Wirtschaft ist in vielerlei Hinsicht vom globalen Informationsnetz abhängig. Produktionsanlagen, der Handel und die Nutzung von Gütern sind direkt mit dem Cyberspace verwoben. Vor allem in

⁵⁸³ Vgl. BKA, Österreichische Strategie für Cyber Sicherheit (ÖSCS), 2013, S. 23.

⁵⁸⁴ Vgl. Glenny, 2012, S. 222.

der Finanzwirtschaft ist eine massive Abstützung auf den Cyberspace gegeben. Transaktionen und Wertpapierhandel werden über die Grenzen hinweg unter Nutzung des Cyberspace durchgeführt. Die Verwundbarkeit auf Grund der Vernetzung ist als sehr hoch zu beurteilen.

Gesellschaftlich ermöglichte das Internet einen tiefgreifenden Wandel. Es bilden sich Parallelgesellschaften im virtuellen Raum.⁵⁸⁵ Die Bildung von virtuellen Gruppen, die auf politische Weise im Netz tätig werden, ist eine Erscheinung, die immer stärker in den Vordergrund tritt. Die Anonymität begünstigt dabei die Partizipation an solchen Fraktionen. Hinzu kommt die schwere Rückverfolgbarkeit von Aktionen im Cyberspace. Der Zeitfaktor spielt hier eine große Rolle. Durch die weltweite Ausdehnung ergibt sich auch rechtlich ein Problem. Da der Cyberspace ein Interaktionsraum zwischen Menschen ist, bedarf er auch rechtlicher Regelung. Die Umsetzung dieser Folgerung ist jedoch durch unterschiedliche Rechtsauffassungen behindert.

Hinsichtlich der Verfügbarkeit entsprechender Infrastruktur kann festgehalten werden, dass viele Menschen über die notwendigen technischen Hilfsmittel verfügen, die den Zugang zum Cyberspace ermöglichen. Geräte, wie Smart-Phones oder Personal-Computer, stehen bereits in großer Anzahl zur Verfügung. Die Industrie versorgt die Gesellschaft ständig mit neuer Technik. Der Zugang über die Luftschnittstelle in den Cyberspace ist schon State of the Art. Der Cyberspace erneuert sich ständig und verändert dabei auch seine Ausdehnung.

Im Bereich der Informationsverbreitung und –gewinnung stehen Möglichkeiten zur Verfügung, die es erlauben unbemerkt Information zu requirieren, sie zu verbreiten oder zu manipulieren. Meinungsbildung wird vielfach durch die neuen Medien angefacht. Ereignisse werden durch das Netz verbreitet, durch die Empfänger interpretiert und führen dann zu Reaktionen, die oft mit den realen Gegebenheiten nichts mehr zu tun haben. Diese sogenannte Thought Bomb⁵⁸⁶ ist ein Phänomen, welches durch das Netz seine Verbreitung erhalten hat. Der Kampf mit Informationen fußt auf diesem Prinzip.

Neben der Macht der neuen Medien gilt der Blick auch der restlichen Kommunikationsinfrastruktur. Die Hauptbestandteile des Cyberspace liegen, wie die kritischen Infrastrukturen, in privater Hand, somit ist eine staatliche Einflussnahme stark begrenzt. Die Behördenanteile am Cyberspace sind als Subsysteme durch die entsprechenden Organisationen – wie Militär und Polizei – überwachbar und geschützt. So kann die Sicht von Grotius bezüglich des freien Zugangs zum Meer als Analogie zum Cyberspace verstanden werden. Zum natürlichen Recht zählen unter anderem das Recht auf nationale Selbstbehauptung, wie auch der ungehinderte Zugang zum Cyberspace (Anm. d. Verf.: Im Original wird von den Weltmeeren gesprochen.).⁵⁸⁷ Auf Grund der Freiheit des Internet sind alle anderen Subsysteme an den Willen der Betreiber, zum Schutz derselben, gebunden.

⁵⁸⁵ Vgl. Olson, 2012, S. 36.

⁵⁸⁶ Vgl. Vortrag von Dr. Sandawi im Rahmen des 19. Generalstabslehrganges zum Thema Sicherheitspolitische Vorausschau 2025, Landesverteidigungsakademie, 25.10.2011.

⁵⁸⁷ Vgl. Konegen, 1998, S. 9f.

Der Cyberspace umfasst einen breiten Bereich an Parametern und Abhängigkeiten. Er ist ein virtueller Raum, der eingebettet ist in die reale Welt. Diese Einbettung bringt es mit sich, dass Aktionen im Cyberspace stets auch Auswirkungen in der realen Welt zur Folge haben können. Im einfachsten Fall handelt es sich um die Beeinflussung von Meinungen, denen dann Handlungen in der Realität folgen. Andererseits können Handlungen im Cyberspace direkt Umsetzung in der Realität zeitigen, dann nämlich, wenn mit IKT gesteuerte Infrastruktur beeinflusst wird. Weitergedacht kann sich Krieg im Netz auf zweierlei Art manifestieren: Zum einen als Wirkung auf die virtuelle Ebene, die Meinungen oder anders ausgedrückt auf die Information. Zum anderen kann er auf die reale Ebene wirken, die Infrastruktur. Es ist also in einem virtuellen Raum ein Kampf um und mit Information möglich.

Zum Abschluss der Untersuchung des Cyberspace werden die wesentlichen Aussagen in einem Zwischenergebnis zusammengefasst.

6.4 Zwischenergebnis zum Begriff des Cyberspace

Der virtuelle Raum ist eingebettet in die reale Welt und Handlungen im Cyberspace haben auch Effekte in der Realität. Die Wirkung, die daraus abgeleitet wird, ist die Synthese aus virtueller und realer Handlung. Der Cyberspace besteht nicht nur aus den technischen Komponenten, sondern der Mensch ist selbst Teil dieses Raumes. Damit bildet der Cyberspace ein sozio-technisches System ab, in welchem die Information als zentrale Ressource zu betrachten ist. Fasst man den Menschen als Teil des Cyberspace, so ist dies auch auf Gruppen von Menschen und schließlich auf Gemeinwesen anwendbar.

Der so gefasste Begriff vom Cyberspace bildet einen neuen Handlungsraum des Menschen, der nicht mehr ausschließlich territorial zu verstehen ist. Es bedarf hier neuer Zugänge zur Definition von territorialer Souveränität. Dieser Raum ist nicht mehr ausschließlich an das Staatsgebiet gebunden, obgleich die physischen Komponenten weiterhin einen Territorialbezug haben. Die Systeme von hochintegrierten Gemeinwesen sind an deren Vernetzung gebunden, nicht nur an den physischen Raum. Es hat daher eine andere Definition von innen und außen, bezogen auf das Gemeinwesen, zu erfolgen und damit auch eine andere Definition der Souveränität.

Die Faktoren Raum und Zeit sind im Cyberspace von schwindender Bedeutung. Obwohl eine Abhängigkeit von physischen Komponenten vorliegend ist, scheint es keine räumlichen und zeitlichen Grenzen zu geben, Informationen werden mit Lichtgeschwindigkeit übertragen und können überall dort verarbeitet werden, wo sich dieser Raum ausgebreitet hat. Zum Faktor Kraft ist anzumerken, dass alle Akteure denselben Raum nutzen und rein theoretisch über dieselben Mittel verfügen. Der Raum ist allerdings, wie bereits gezeigt, anarchisch organisiert. Mit der Fähigkeit, die Mittel auch für Schädigungshandlungen einzusetzen, ergibt sich im Cyberspace eine Asymmetrie. Diese erwächst aus dem Vermögen zu schaden.

Die IKT-Infrastruktur ist hier nicht die Waffe⁵⁸⁸, sondern die Waffen sind fast ausschließlich virtueller Natur.⁵⁸⁹ Schadprogramme, sogenannte Malware, sind das Mittel im Netz, um kriegerisch wirken zu können. Information wird im erweiterten Sinn zur Waffe, sie ist ein Multirole-Mittel. Daneben gibt es noch Waffen, die physisch auf das Netz wirken können. Den Methoden und Mitteln, die im Cyberwar zur Anwendung gelangen, wird in einem späteren Abschnitt noch Rechnung getragen.

Durch die Abhängigkeiten der Staaten vom Cyberspace und der darauf basierenden gegenseitigen Vernetzung, ist der Cyberspace ein neuer möglicher Konfliktraum. Das bedeutet, für einen Angriff auf ein Gemeinwesen ist nicht mehr unbedingt der Einsatz konventioneller Streitkräfte notwendig. Mit gezielten Aktionen im Cyberspace kann durch unterschiedliche Akteure (auch nichtstaatliche Akteure) auf Staaten eingewirkt werden. Diese hohe Abhängigkeit vom Cyberspace und die Komplexität des Netzes an und für sich, lassen den Schluss zu, dass Krieg im Cyberspace der strategischen Ebene der Kriegführung zurechenbar ist. Daraus abgeleitet, kann das Militär nur noch ein Akteur von vielen sein. Betrachtet man den Krieg im Netz genauer, so lassen sich zwei Formen des bewaffneten Konfliktes im Cyberspace erkennen.

Zum einen der strategische Große Cyberwar, der im Geheimen stattfindet und zum anderen der taktische bzw. operative Kleine Cyberwar, der im Rahmen konventioneller Kriege zwischen Streitkräften seine Anwendung findet. Diese Tatsache hat Einfluss auf die Art und Weise, wie bewaffnete Konflikte, speziell im Cyberspace, in Zukunft geführt werden. Dies erfordert eine Erweiterung des Kriegsbegriffes und eine neue Definition des bewaffneten Konfliktes. Da der Krieg im Netz ein internationales Problem darstellt, ist die Findung eines gemeinsamen rechtlichen Zuganges eine notwendige Basisarbeit, die zu leisten sein wird.

Hier zeigen sich neben der Entgrenzung vor allem die Non-Attribution, die Anonymität und die anarchische Ordnung im Netz als große Herausforderungen für die Cyber Sicherheit. Da nicht eindeutig feststellbar ist, ob ein Akteur staatlich legitimiert ist oder nicht, müssen Instrumente geschaffen werden, die im Bedarfsfall eine Attribution ermöglichen; dabei ist die Kombination verschiedener Attributionsmethoden auch unter Einsatz des Militärs zu erwägen. Abgeleitet davon muss sich das Militär neue Zugänge, organisatorisch, methodisch und auch von der Art der Mittel her betrachtet, erschließen. Diese Folgerung bezieht sich sowohl auf den Angriff als auch auf die Verteidigung. Aus Sicht des Militärs erscheint es notwendig, sich im Denken an diese Art des bewaffneten Konfliktes anzunähern, um letztlich in dem Bereich Fähigkeiten aufzubauen und im Cyberspace agieren zu können.

Durch den globalen Zusammenschluss aller Nutzer des Cyberspace treten die operativen Faktoren – Kraft, Zeit und Raum – immer mehr in den

⁵⁸⁸ Vgl. § 17 Ziff. 3, Bundesgesetz über Aufgaben und Befugnisse im Rahmen der militärischen Landesverteidigung (Militärbefugnisgesetz – MBG) BGBl. I Nr. 86/2000 idF BGBl. I Nr. 102/2019.

⁵⁸⁹ Anm. d. Verf.: Diese Feststellung ist in Analogie zum Krieg an Land zu sehen. Das Land ist nicht die Waffe, sondern der Raum in dem der Kampf stattfindet.

Hintergrund. Nur hinsichtlich der Ziellage ist der Raum noch von Belang. Die Information bekommt durch diese neue Art der Interaktion eine gesteigerte Bedeutung. Die Tatsache, dass alle Bereiche des Gemeinwesens miteinander verbunden sind und des Weiteren auch, dass diese vernetzten Bereiche der Gemeinwesen wiederum miteinander ein Netzwerk bilden, steigert nicht nur die Möglichkeit zur Interaktion, sondern auch die Verwundbarkeit. Um nun Bedrohungen, die daraus resultieren, zu erfassen, bedarf es geeigneter Instrumente, die sowohl in der Realität als auch in der Virtuellen Realität, zur Schaffung eines Lagebildes geeignet sind. Es müssen beide Sphären berücksichtigt werden, da eine gegenseitige Beeinflussung gegeben ist.

Auf der Beschaffenheit des Cyberspace basierend, kann eine Zuteilung der Verantwortung nicht auf die territoriale Unterscheidung von innen und außen zurückgeführt werden. Der Ansatz muss systemisch und funktional erfolgen. Dabei ist der Cyberspace nicht analog einem realen Raum zu fassen. Seine Spezifika sind gänzlich anders geartet. Allen Akteuren im Netz ist dieser eine Raum gemeinsam. Innen und außen kann sich nur an den, einem Akteur zugehörigen, Systemen orientieren, ungeachtet dessen, wo sich die Teile des Systems territorial befinden.

Um Verantwortlichkeiten für das Militär definieren und den rechtlichen Rahmen für das Handeln des Militärs im Cyberraum abstecken zu können, ist neben einer eindeutigen Aufgabenzuordnung, auch die Definition der Kernaufgabe des Militärs im Cyberraum zu treffen. Ein klares Bild vom bewaffneten Konflikt im Cyberspace, dem Cyberwar, und dessen rechtliche Einbettung sind die Bedingung dafür.⁵⁹⁰

⁵⁹⁰ Vgl. Hofstetter, 2019, S. 181.

7 Vom Begriff des Cyberwar

„Man verfügte plötzlich über eine Kampfwanne,
deren Charakter unklar, deren wehrtechnische und
sonstigen Eigenschaften noch völlig unergründet waren.
Das führte zu Unsicherheit in der Verwendung,
bedingte eine Entwicklungslinie, die an sich schon
die Quelle für Fehler und Fehlgriffe darstellte.“
Giulio Douhet⁵⁹¹

Information ist ein mächtiger Parameter, die gesamte menschliche Interaktion, sowohl zwischen Menschen, aber auch mit der Umwelt, baut auf Informationen auf. Einen Großteil seiner Existenz hat der Mensch, um Information nutzen zu können, direkt in Kontakt mit dem Träger dieser Informationen treten müssen. Der Informationsraum beschränkte sich also auf das unmittelbare Umfeld dessen, der die Information benötigte. Mit der technologischen Entwicklung wandelten sich die Informationsträger und mit ihnen die Informationsübertragung. Der Informationsraum weitete sich zusehends aus.⁵⁹²

Deutlich wird die Bedeutung von Information in der Entwicklung hinsichtlich der militärischen Fähigkeiten in diesem Bereich. So ist Information neben Kraft, Raum und Zeit der vierte operative Faktor für die Planung und Durchführung von militärischen Einsätzen. Der Cyberspace ist die fünfte Domäne der Kriegführung und auch auf strategischer Ebene hat die Information eine wesentliche Bedeutung, ist sie doch neben dem Militär, der Wirtschaft und der Diplomatie das vierte Machtinstrument der Staaten.⁵⁹³

Dass Kriege von Informationen abhängig sind, liegt auf der Hand, aber die Kriegführung ausschließlich mittels Informationen, in einem eigenen Raum, stellt eine neue Herausforderung an die militärischen Kräfte aller Staaten.⁵⁹⁴ Die Möglichkeit aus der virtuellen Welt heraus, in der Realität Effekte zu erzielen, ist dabei eine neuartige Möglichkeit militärisch wirksam zu werden. Für die Beantwortung der Forschungsfrage ist hier von Bedeutung diesen virtuellen Raum näher zu untersuchen, um die Basis für den Unterschied zwischen Krieg und Verbrechen im Cyberspace zu schaffen und die Zuständigkeiten für Militär und Polizei daraus abzuleiten. Aufbauend auf die Raum-Untersuchung hat die Analyse von Angriffen im Cyberspace nach den Kriterien zu erfolgen, welche den Krieg näher bestimmen.⁵⁹⁵ Erst dann ist eine Zuordnung zu den Trägern des Gewaltmonopols möglich. Wesentlich sind hier Akteur, Zweck und Intensität des Angriffs.

⁵⁹¹ Douhet, 1935, S. 13.

⁵⁹² Vgl. Klauninger, Bert: Cyberspace als ein selbstorganisierendes System, o.J.
http://archive.gpi-online.de/files/_klauninger_cyberspace.pdf, S. 8, [12.05.2020].

⁵⁹³ Vgl. Andress/Winterfeld, 2011, S. 7.

⁵⁹⁴ Vgl. Bendrath, Ralf: Militärpolitik, Informationstechnologie und die Virtualisierung des Krieges. In: Forschungsgruppe Informationsgesellschaft und Sicherheitspolitik FoG:IS, Texte zur Sicherheitspolitik in der Informationsgesellschaft, 1997-99, FoG:IS Arbeitspapier Nr. 1, November 1999, S. 33.

⁵⁹⁵ Vgl. Hofstetter, 2019, S. 181.

Wann es sich um einen Krieg handelt, wie der Krieg im Informationsraum zu fassen ist und wie er in den klassischen Kriegsbegriff einzureihen ist, wird im Folgenden erarbeitet.

7.1 Zur Intensität des Cyberwar

In diesem Abschnitt geht es um die Verortung des Cyberwar und ab wann von einem Krieg im Netz gesprochen werden kann. Die Intensität ist dabei ein wichtiger Parameter. Die Ausdehnung eines Konfliktes im Cyberspace muss dabei unter einem neuen Gesichtspunkt gefasst werden. Es geht im Cyberspace um die Anzahl angegriffener Systeme und darum, welche Systeme angegriffen wurden. Intensität ist also quantitativ fassbar. Um zu erkennen, dass es sich um einen Krieg im Netz handelt, ist auch die Unterscheidung zwischen innen und außen von Bedeutung. Wie bereits festgestellt, ist diese Unterscheidung systemischer Natur. Es geht um spezifische Systeme, die funktional eine Einheit bilden. Intensität ist somit auch abhängig von der Anzahl, der angegriffenen funktional zusammengehörigen Systeme.

Um die Intensität des Cyberwar fassen zu können, muss die Einordnung des Cyberwar in die Kriegführung als solches vorgenommen werden. Libicki verortet den Cyberwar als eine von sieben Unterkategorien des Informationwar.⁵⁹⁶

Diese Einteilung orientiert sich nicht an dem Raum, der Dimension der Kriegführung, in der um und mit Informationen gekämpft wird. Aus Sicht des Verfassers ist eine Einteilung, die nicht alle Kategorien wie Mittel, Ziele, Akteure und Räume miteinander vermengt, zielführend. Der Cyberraum – oder auch Informationsraum – ist die Domäne, in der alle diese Handlungen ablaufen. Alle hier angeführten Arten der Kriegführung nutzen den Cyberspace oder Komponenten daraus, um zu wirken. Die Benennung der übergeordneten Kategorie sollte demnach als Informationsraum-Kriegführung oder eben als Cyberwar tituliert werden. Bedacht werden muss, dass Libicki den Begriff des Cyberwar nicht nach heutigem Verständnis fasst. Die heutige Auslegung des Cyberwar trifft eher jene Definition des Informationwar (IW) nach Shackelford:

„IW itself in general refers to a hostile attack by one hostile nation against the important IT systems and networks of another (as compared to a criminal or terrorist attack involving private parties). Second, IW refers to actions taken to defend IT systems and networks. IW waged by terrorists, or a hostile state, against any modern society replete with IT, such as the United States, is a matter of national concern.“⁵⁹⁷

Ergänzt werden müsste diese Definition noch um, wie bereits festgestellt, nichtstaatliche Akteure, die ebenso in einem Cyberwar auftreten

⁵⁹⁶ Vgl. Libicki, 1995, S. 7.

⁵⁹⁷ Shackelford, Scott J.: From Nuclear War to Net War: Analogizing Cyber Attacks in International Law. In: Berkeley Journal of International Law, 2009, S. 198f.

können. Neben der Urheberschaft und der Intention einer Attacke im Netz ist die Intensität wichtig für die Zuordnung von Verantwortlichkeiten. Globalisierung – und die daraus resultierende Vernetzung – sind verantwortlich für eine Verschränkung verschiedener Bereiche innerhalb und zwischen den Gemeinwesen. Hinsichtlich der Wirkung und des Ausmaßes von Angriffen im Netz muss zunächst „a hostile attack“ (Hervorhebung durch den Verfasser.), der Cyber Angriff als solches, gefasst werden, um dann, an Hand seiner Intensität, eine erste Zuordnung zu den Formen des bewaffneten Konfliktes im Netz zu treffen.

7.1.1 Der Cyber Angriff

Der Cyber Angriff ist jene Aktion im Netz, die einem bewaffneten Konflikt in diesem Raum zu Grunde liegt. Ein Cyber Angriff kann dabei in allen Konfliktformen zum Tragen kommen. Die österreichische Definition eines Cyber Angriffes entstammt dem Cyber Security Glossar zur ÖSCS:

„Ein Cyber Angriff ist ein Angriff mit Mitteln der IT im Cyber Raum, der sich gegen einen oder mehrere andere IT-Systeme richtet und zum Ziel hat, die Schutzziele der IKT Sicherheit als Teil oder Ganzes zu verletzen. Die Ziele der IT-Sicherheit, Vertraulichkeit, Integrität und Verfügbarkeit können dabei als Teil oder Ganzes verletzt werden. Cyber Angriffe, die sich gegen die Vertraulichkeit eines IT-Systems richten, werden als Cyber Spionage bezeichnet und stellen somit Spionage auf digitalem Wege dar. Cyber Angriffe gegen die Integrität und Verfügbarkeit eines IT-Systems werden als Cyber Sabotage bezeichnet.“⁵⁹⁸

Diese Definition beinhaltet jeglichen Eingriff⁵⁹⁹ in ein IT-System. Es werden sowohl Spionage als auch Sabotage miteingeschlossen. In welchem Konfliktmoment auch immer dieser Angriff ausgeführt wird, bleibt hier nicht näher bestimmt. Diese Form eines Cyber Angriffs kann, sowohl im Zuge eines Verbrechens als auch im Krieg, zum Einsatz gelangen. Im Zuge der Abhandlung geht es allerdings um eine spezifische Form des Cyber Angriffes, den im Rahmen von bewaffneten Konflikten, also Kriegen.⁶⁰⁰ Um die Cyber Attacke diesbezüglich näher zu bestimmen, muss der Zweck, die Intention, mitberücksichtigt werden.

„A cyber-attack consists of any action taken to undermine the functions of a computer network for a political or national security purpose.“⁶⁰¹

⁵⁹⁸ BKA, Österreichische Strategie für Cyber Sicherheit (ÖSCS), 2013, S. 20.

⁵⁹⁹ Anm. d. Verf.: Die Literatur unterscheidet drei Formen von Cyber Angriffen. Es handelt sich um nicht autorisierte Akquisition, die Sabotage und die Verhinderung der autorisierten Nutzung von Informationen. Diese drei Formen werden auch als Angriff auf Vertraulichkeit, Integrität und Verfügbarkeit bezeichnet.

⁶⁰⁰ Anm. d. Verf.: Es handelt sich also um bewaffnete Gewalt nach Art. 2 Ziff. 4 der VN-Charta, die demzufolge von Gemeinwesen mit politischem Motiv in einem bewaffneten Konflikt oder als bewaffneter Konflikt zur Anwendung kommt.

⁶⁰¹ Hathaway, Oona u.a.: The Law of Cyber-Attack, 2011, S. 10.

Diese Definition inkludiert nicht nur Cyber Waffen als Mittel, um die Aktionen auszuführen, sondern fasst auch physische und psychologische Waffen als Wirkmittel. Dieser ganzheitliche Ansatz lässt Akteur und Intensität nicht unberücksichtigt. Da politischer Zweck und nationale Sicherheit nur durch Gemeinwesen verwirklicht werden können, und diese sich dazu der Staatsgewalt bedienen, ist in einem Satz eine umfassende Definition der Cyber Attacke im Rahmen des Krieges geleistet.

Cyber Angriffe, Cyber Kriegführung und Cyber Kriminalität stehen in engem Zusammenhang. Cyber Angriffe sind nicht gleichbedeutend mit Krieg im Netz. Es können auch andere Maßnahmen, mit politischer Intention, als Cyber Angriff gefasst werden. Dies können direkte politische oder auch diplomatische Aktionen sein. Zum Beispiel könnten durch staatliche Akteure Maßnahmen getroffen werden, die einem Cyber Embargo gleichen. Diese Aktion stellt einen Eingriff in den Cyberspace dar, der nicht krimineller, aber auch nicht kriegserischer Natur, also unterhalb der Kriegsschwelle, aber politischer Art ist. Daraus folgt, nicht jede Cyber Attacke ist ein Cyberwar, obwohl jede Cyber Kriegführung eines Cyber Angriffes bedarf.

Die Intensität eines Cyber Angriffes richtet sich einerseits nach dessen Auswirkungen und andererseits nach der Anzahl der durch diesen Angriff betroffenen Systeme. Durch diese Intensität lassen sich Zuständigkeiten für die jeweiligen Angriffe ableiten. Grundsätzlich kann bei der Intention der Angriffe zwischen Ausnutzung und Schwächung unterschieden werden.

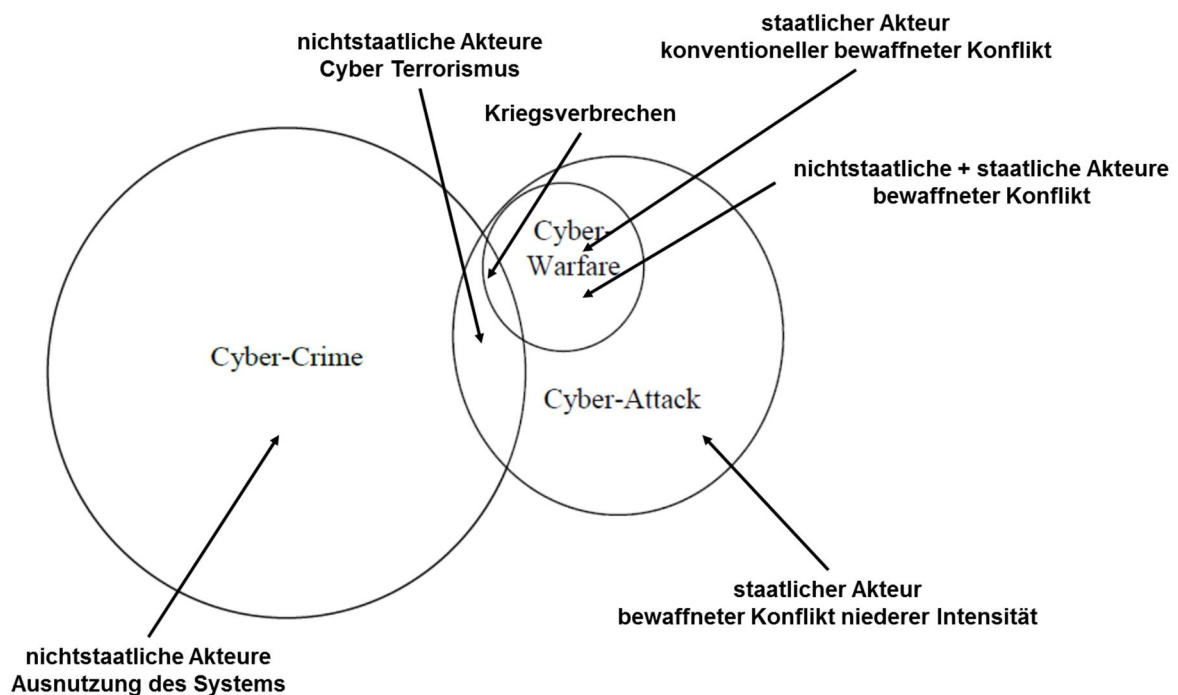


Abbildung 9: Beziehung zwischen den Aktionen im Cyberspace⁶⁰²

⁶⁰² Ebd., S. 18. (Ergänzungen durch den Verfasser.)

Es können zwei große Bereiche angesprochen werden.⁶⁰³ Zum einen Cyber Kriminalität und zum anderen die Cyber Angriffe. Im Bereich der Kriminalität steht die Ausnutzung des Netzes im Vordergrund. Bei den Cyber Attacken steht die Schwächung des Netzes im Fokus. Im Cyber Crime kommen nichtstaatliche Akteure zur Wirkung, während im Bereich der Cyber Attacke staatliche Akteure tätig sind.⁶⁰⁴ Cyberwar ist dann vorliegend, wenn Akteure (staatlich oder nichtstaatlich) Aktionen im Netz, im Zusammenhang mit einem bewaffneten Konflikt, oder staatliche Akteure Cyber Angriffe ausführen, die einem konventionellen bewaffneten Angriff entsprechen.

Der Überschneidungsbereich der beiden Kreise zeigt die Aktionen von nichtstaatlichen Akteuren mit politischem Hintergrund an. Diese können bis zum Ausmaß eines Cyberwar führen. Die Verortung des Cyber Terrorismus ist hier zu sehen. Wird ein Cyber Angriff als Handlung in einem bewaffneten Konflikt durchgeführt, so können staatliche und nichtstaatliche Akteure tätig werden. Auf Grund der Anonymität und der Anarchie im Netz, sind im Cyberwar alle möglichen Akteure vorzufinden. Für die Zuordnung von Verantwortlichkeiten ist eine Kategorisierung der Konfliktformen im Cyberspace sehr wichtig.

„Stattdessen ist eine konzeptionelle Kategorisierung verschiedener Konfliktformen im Cyberspace nötig. Erst auf dieser Basis lassen sich die konkrete Gefahr und deren Tragweite einschätzen, Verantwortlichkeiten zuweisen, präventive und reaktive Gegenmaßnahmen implementieren und allfällige strafrechtliche Untersuchungen einleiten.“⁶⁰⁵

Es spielen dabei Ausdehnung, Form und Intensität eine ähnliche Rolle wie beim Kriegsbegriff an und für sich. Auf Grund dieser drei Faktoren wird im Folgenden eine Einteilung des Virtuellen Krieges vorgenommen. Der Cyberwar, der Virtuelle Krieg selbst, kann in zwei Formen auftreten, dem Großen (strategischen) und dem Kleinen (operativen/taktischen) Cyberwar.

Die Ausdehnung ist, im Fall eines strategischen Cyberwar, als hoch einzustufen und in der rein militärischen Anwendung, also wenn Militär auf gegnerische militärische Systeme, mittels Cyber Kriegführung, einwirkt, als niedrig zu beurteilen. Die Intensität ist dabei an der Ausdehnung orientiert, je höher die Ausdehnung, desto höher die Intensität. Ein Punkt, der zu den drei genannten Faktoren tritt, ist die Wahrnehmbarkeit.

Da Angriffe, die nicht wahrgenommen werden, lange Zeit im System wirksam bleiben, geht von diesen eine größere Gefahr aus und damit auch eine höhere Intensität. Daher kann der Cyber Terrorismus, der um hohe Wahrnehmbarkeit bemüht ist – nur so kann er seine Wirkung entfalten – als von der Intensität her geringer eingestuft werden. Es lassen sich, neben den bereits genannten Aktionsformen, noch weitere Formen der

⁶⁰³ Vgl. ebd., S. 18.

⁶⁰⁴ Anm. d. Verf.: Rein hypothetisch können auch im Bereich der Cyber Attacke nichtstaatliche Akteure tätig werden, aber die Verletzung des Rechts ist dabei höchst wahrscheinlich.

⁶⁰⁵ Center for Security Studies, CSS Analysen zur Sicherheitspolitik: Cyberwar: Konzept, Stand und Grenzen, 2010, S. 1.

Auseinandersetzung im Cyberspace feststellen, wie Vandalismus, Haktivismus, Spionage und Sabotage.

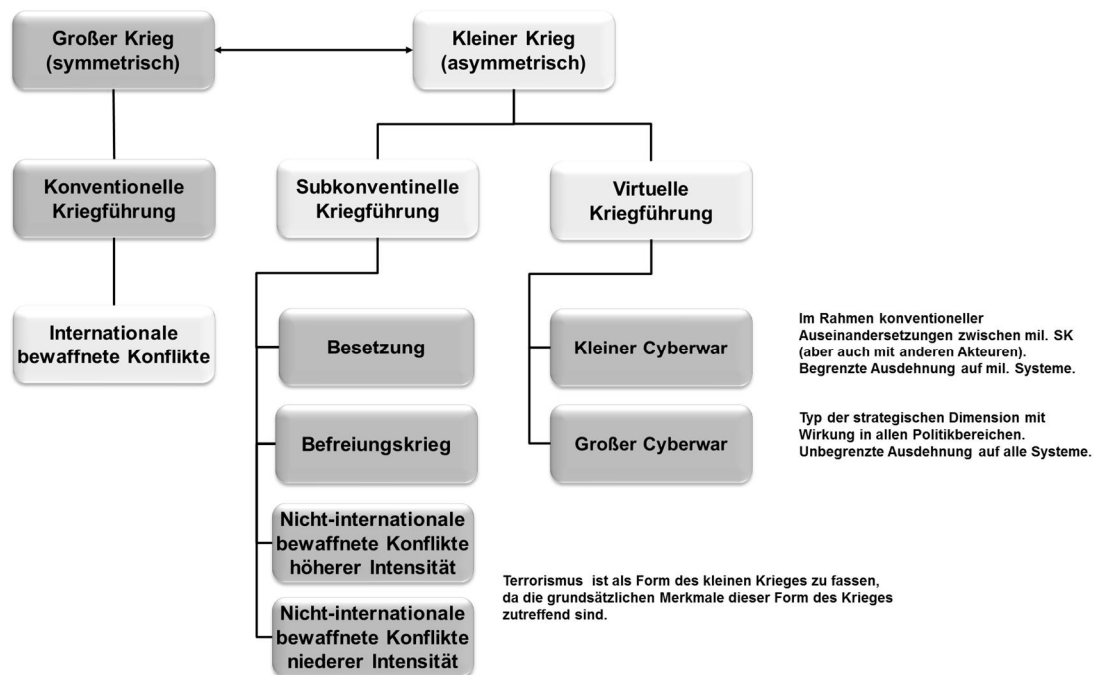


Abbildung 10: Einordnung des Cyberwar⁶⁰⁶

In der weiteren Bearbeitung wird vor allem dem Großen und dem Kleinen Cyberwar das Hauptaugenmerk zuteil. Die Inversion, zu den Begriffen „Groß“ und „Klein“ in Bezug auf den konventionellen Krieg, wird hier dargestellt. Die Ausdehnung und die Intensität, der beiden Formen des Krieges im Cyberspace, stehen dabei im Mittelpunkt.

7.1.2 Der Große Cyberwar

Diese Form des Cyberwar ist nicht von Symmetrie geprägt, wie der Große Krieg, bezogen auf die konventionelle Kriegführung. Der Ausprägung nach gehört diese Form der Kriegführung vom Wesen her zum Kleinen Krieg, ist also von Asymmetrie getragen. Der Große Cyberwar wird über die Ausdehnung gefasst. Diese Ausprägung des Virtuellen Krieges umfasst alle Bereiche eines Gemeinwesens. Bezugnehmend auf das Gesamtsystem (PEMSII), werden durch den Großen Cyberwar alle Bereiche bewirkt. In ihm können alle Akteure des Cyberspace wirksam werden. Diese Konfliktform ist als großer Typus zu fassen, da eben alle Bereiche und Akteure wirken und bewirkt werden können. Der Intensität nach handelt es sich um die intensive Art der Kriegführung im Cyberspace.

Obwohl alle Bereiche bewirkt werden können, muss ein Großer Cyberwar nicht unbedingt immer in allen Bereichen eines angegriffenen Gemeinwesens wirken. Der Große Cyberwar geschieht im Geheimen, er nutzt

⁶⁰⁶ Abbildung durch den Verfasser erstellt.

die Beschaffenheit des Cyberspace und erzeugt eine Asymmetrie, die im Extremfall nicht erkannt werden kann. Im Cyberwar herrscht generell ein starkes Missverhältnis zwischen Abwehr und Angriff. Der Angreifer ist dem Verteidiger gegenüber stets im Vorteil. Wenn wir die Phasen des Cyberwar Konzeptes heranziehen, sind im Großen Cyberwar die Wirkmaßnahmen solcher Art, dass sie nicht oder nur schwer erkannt werden können. Manipulation und Beeinflussung, durch gezielte Angriffe zur Schwächung des Gesamtsystems, sind hier im Vordergrund zu sehen.

Der Große Cyberwar ist mit dem Netwar, den Arquilla und Ronfeldt definiert haben, zu vergleichen. Diese beiden Autoren fassen den Netwar als:

„[...] an emerging mode of conflict (and crime) at societal levels, involving measures short of war, in which the protagonists use - indeed, depend on using - network forms of organization, doctrine, strategy, and communication. These protagonists generally consist of dispersed, often small groups who agree to communicate, coordinate, and act in an internetted manner, often without a precise central leadership or headquarters. Decisionmaking may be deliberately decentralized and dispersed.“⁶⁰⁷

Hinsichtlich der Mittel unterhalb der Kriegsschwelle ist anzumerken, dass diese Formulierung auf die Wahrnehmbarkeit und die Zuordenbarkeit zurückzuführen ist. Aktionen, welche sich im Geheimen zutragen, können auch nicht als kriegerische Handlungen wahrgenommen werden. Diese Tatsache schmälert allerdings nicht die hohe Eskalationsstufe, die dem Großen Cyberwar zu Grunde liegt.⁶⁰⁸ Die räumliche Ausdehnung ist total entgrenzt, der gesamte Cyberspace kann zum Konfliktraum werden. Die Anzahl der Akteure ist entgrenzt, alle Nutzer des Cyberspace können an einem Konflikt teilnehmen. Schließlich ist auch die Intensität als potentiell hoch zu bewerten, da alle Mittel, die im Informationsraum zur Verfügung stehen, zur Anwendung gelangen können.

Der Große Cyberwar kann in der Eskalation nochmals erhöht werden, indem er wahrnehmbar wird. Die Wirkung auf alle Bereiche des öffentlichen Lebens kann dabei erheblichen Schaden anrichten.⁶⁰⁹ Diese Art des Großen Cyberwar tritt dann im Ergebnis zu Tage, nicht in der Kampfführung selbst. Die Manipulation bzw. Beeinflussung, die der Wirkung vorausgeht, ist nicht wahrnehmbar, das Ergebnis schon.

Ein Großer Cyberwar wirkt in ganzer Breite und damit nur indirekt auf und gegen das Militär. Die Möglichkeit einer solchen Kriegführung bedarf allerdings eines gewissen Vernetzungsgrades.⁶¹⁰ Nur integrierte Gemeinwesen können mit solchen Mitteln auch auf strategischer Ebene bekämpft werden. Da der Große Cyberwar die vitalen Bereiche einer

⁶⁰⁷ Arquilla, John; Ronfeldt, David: The Advent of Netwar, Santa Monica 1996, S. 5.

⁶⁰⁸ Vgl. Bilban, Christoph; Grininger, Hanna (Hrsg.): Mythos „Gerasimov-Doktrin“, Ansichten des russischen Militärs oder Grundlage hybrider Kriegsführung?, Schriftenreihe der Landesverteidigungsakademie, Wien 2019, S. 40f.

⁶⁰⁹ Anm. d. Verf.: Für den Einsatz des Militärs ist die Zielart von Bedeutung, insbesondere ob es sich um souveränitätsrelevante Systeme handelt.

⁶¹⁰ Vgl. Barnett, 2004, S. 50.

Gesellschaft treffen kann, ist seine politische Dimension immanent. Potentiell hat diese Form des Cyberwar auch die Möglichkeit politische Zwecke, ohne Einsatz konventioneller Streitkräfte, zu erreichen. Trotzdem bedarf es einer physischen Komponente, die letztlich die Macht durchzusetzen vermag.⁶¹¹ Daher ist der Große Cyberwar letztlich kein entscheidender Krieg, sondern ein unterstützender, ermöglichender Faktor.⁶¹²

Da der Große Cyberwar seinem Wesen nach entgrenzt ist und er weitgehend unbemerkt passiert, ist nur reaktiv gegen ihn vorzugehen. Diese Reaktion ist auf Grund der unklaren Urhebererschaft und der damit einhergehenden Ermittlungsarbeit eher im Bereich der Polizei zu verorten. Dennoch geht es um die Beeinflussung eines Gesamtsystems zum Zwecke einer politischen Zielsetzung, es geht um die Änderung des Systems. Damit wären die Kriterien für einen Krieg gegeben und somit die Verantwortung beim Militär. Systemisch handelt es sich schließlich immer um einen Angriff von außen und damit kann die Polizei nur noch bedingt verantwortlich sein. Anders, wenn es sich nicht um die Veränderung, sondern die Ausnutzung eines Systems handelt.

Diese Form des virtuellen Krieges verwischt die Grenze zwischen Krieg und Frieden, die Aktionen des Großen Cyberwar,

„[...] unterhalb der Schwelle offener und organisierter Gewaltaustragung liegen in der Grauzone zwischen direkter militärischer Aktion und indirekter geheimdienstlicher Unterstützung.“⁶¹³

Da aber der strategische Cyberwar⁶¹⁴ ein alle Bereiche durchdringender Krieg ist, können nicht nur Polizei und Militär der Bedrohung entgegentreten. Vielmehr ist ein gesamtheitlicher Ansatz, aller möglichen Betroffenen, gegen diese Gefahr angezeigt. Einfacher erscheint die Zuständigkeit im Kleinen Cyberwar zu finden zu sein. In diesem findet der gezielte Einsatz des Cyberwar gegen militärische Ziele seinen Niederschlag. Ein Beispiel für den Großen Cyberwar stellt der Angriff auf das iranische Atomprogramm dar.

7.1.3 Exkurs: Der Große Cyberwar am Beispiel der Stuxnet-Attacke auf Natanz

Dieser Angriff stellt ein gutes Beispiel für die Bedrohungen dar, welche im Krieg im Geheimen auf unsere vitale Infrastruktur einwirken können. Das Ziel des Angriffes lag in der Manipulation einer herkömmlichen speicherprogrammierbaren Steuerung (SPS), wie sie in vielen Industrie- aber

⁶¹¹ Vgl. Bilban/Grininger, 2019, S. 42.

⁶¹² Vgl. Nye, 2011, S. 205.

⁶¹³ Minkwitz, Olivier: Ohne Hemmungen in den Krieg? Cyberwar und die Folgen, Frankfurt 2003, S. 18.

⁶¹⁴ Anm. d. Verf.: Diese strategische Form des Krieges im Netz wird im Rahmen der hybriden Kriegführung zur Anwendung gebracht. Der Hybride Krieg ist dabei als Einsatz aller Instrumente des Staates unterhalb der Kriegsschwelle zur Erreichung politischer Zielsetzungen zu verstehen.

auch anderen Produktionsanlagen zur Anwendung kommt. Überall, wo automatisierte Prozesse ablaufen, werden solche Steuerungen verwendet. So wurden in der iranischen Atomanlage Zentrifugen zur Anreicherung von Uran mittels einer solchen Anlage gesteuert.⁶¹⁵ Die Steuerung ist wie ein Computer aufgebaut und ermöglicht es, Daten über Sensoren aufzunehmen und entsprechende Steuerbefehle an Aktoren auszugeben.

Stuxnet wurde, da die iranische Anlage keine physikalische Verbindung zum Internet hatte, über eine Human-Schnittstelle eingebracht.⁶¹⁶ Dies zeigt, dass eine Entnetzung als Sicherheitsstrategie unwirksam ist. Der Mensch stellt, als Teil des Cyberspace, nach wie vor den größten Unsicherheitsfaktor dar. Das Programm selbst setzt sich aus mehreren Teilen zusammen. Dabei sind diesen Programmteilen verschiedene Aufgaben zugeordnet. Eines dieser sogenannten Exploits verschafft sich Zugang zum zu infizierenden System, ein weiteres Exploit ist für die Verbreitung zuständig.⁶¹⁷

Man kann sich diese Attacke wie eine militärische Operation vorstellen. Es wurde Aufklärung betrieben und Informationen über das Zielsystem gesammelt. Auf Grund der Komplexität und Zielgenauigkeit von Stuxnet, kann davon ausgegangen werden, dass eine Testumgebung realisiert wurde, um die Wirkung zu überprüfen.⁶¹⁸ Eintrittspunkte wurden ermittelt, die Zugriffsrechte durch Exploits erlangt und schließlich die Schadsoftware, mittels Malware-Dropper, angelandet. Die Steuerungen der Zentrifugen wurden nicht einfach zerstört, sondern durch Funktionen des Schadprogramms in ihrer Drehzahl variiert.⁶¹⁹ Dies konnte durch falsche Anzeigen der Kontrollinstrumente verschleiert werden und führte dazu, dass die Zentrifugen über das normale Maß hinaus belastet wurden.⁶²⁰

Das Besondere an Stuxnet ist seine Fähigkeit, sich nur auf den Systemen zu installieren, welche letztlich auch bewirkt werden sollen. Dazu verwendet er eine Prüfroutine, die es dem Schadprogramm ermöglicht, an Hand der verschiedensten Parameter, zu bestimmen, ob dieses Ziel zu bewirken ist oder nicht.⁶²¹ Die Kenntnisse über die Anlage von Natanz, der Aufbau und die Wirkungsweise von Stuxnet legen den Schluss nahe, dass diese Schadsoftware von sehr gut ausgebildeten Programmierern entwickelt wurde.⁶²² Der Angriff diente dem Zweck, das iranische Atomprogramm, welches im Verdacht steht für militärische Zwecke genutzt zu werden, nachhaltig zu schädigen.

Dass Stuxnet letztlich an die Öffentlichkeit kam, kann als eine Maßnahme der Abschreckung gesehen werden. Auch wenn der Urheber letztlich nicht eindeutig geklärt wurde, die Vereinigten Staaten von Amerika

⁶¹⁵ Vgl. Falliere, Nicolas u.a.: W32.Stuxnet Dossier 2011, S. 2.

⁶¹⁶ Vgl. Hansel, 2011, S. 569. (in: Jäger/Beckmann, 2011)

⁶¹⁷ Vgl. Gayken, 2011, S. 176.

⁶¹⁸ Vgl. Falliere/O'Murchu/Chien, 2011, S. 3.

⁶¹⁹ Vgl. ebd., S. 41.

⁶²⁰ Vgl. Albright, David u.a.: Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? In: Institute for Science and International Security Report, 2010, S. 4.

⁶²¹ Vgl. Falliere/O'Murchu/Chien, 2011, S. 38ff.

⁶²² Vgl. Assange/Apfelbaum/Müller-Maguhn, 2013, S. 178.

und Israel stehen im Verdacht, zeigt sich hier gegenüber dem Iran eine abschreckende Wirkung. Zudem kann eine solche Demonstration auch finanzielle Zuwendungen, für den weiteren Ausbau der Kapazitäten der jeweiligen Entwickler, bewirken.⁶²³ Stuxnet hat klar eine strategische Zielsetzung verfolgt, indem er auf verschiedene Bereiche der iranischen Politik einwirkte. Das Schadprogramm hatte auch den Effekt zu zeigen, welche Möglichkeiten bestehen, eine Cyber Waffe zum Einsatz zu bringen, ohne jedoch den Urheber preiszugeben. Die psychologische Wirkung ist dabei enorm.

Der Angriff wirkte nicht direkt auf das Militär, jedoch behinderte er die Entwicklung möglicher militärischer Nuklearfähigkeiten des Iran. Es ist dies also ein anschauliches Beispiel für eine strategische Informationskriegführung⁶²⁴ bzw. einen Großen Cyberwar.

7.1.4 Der Kleine Cyberwar

Der Kleine Cyberwar ist jene direkte Unterstützungsmaßnahme, die Streitkräfte einsetzen, um ihre Ziele in einer Operation zu erreichen. Hansel bezeichnet diese Form des Cyberwar auch als taktischen Informationskrieg. Er dient der „[...] Minderung der militärischen Schlagkraft des Gegners [...]“⁶²⁵ und wirkt daher in erster Linie auf militärische Systeme.⁶²⁶ Die Abgrenzung zum Großen Cyberwar ist darin begründet, dass die Ausdehnung begrenzt ist. Obwohl er auch dem Kleinen Krieg konventioneller Ausprägung zuzuordnen ist, liegt sein Wirken ausschließlich im militärischen Bereich.

„Cyberwar refers to conducting, and preparing to conduct, military operations according to information-related principles.“⁶²⁷

Besonderes Merkmal des Kleinen Cyberwar ist also seine Einbettung in eine militärische Operation. Er wirkt auf operativer und taktischer Ebene der Kriegführung.

„Computernetzwerke bilden das infrastrukturelle Rückgrat moderner Streitkräfte. Sie sind essentiell für das Führen von Militäroperationen geworden. Dies macht sie zu hochwertigen Zielen in einer militärischen Auseinandersetzung.“⁶²⁸

Der Kleine Cyberwar kann in vier Bereichen zum Einsatz kommen. Auf Grund des hohen Vernetzungsgrades von modernen Streitkräften und dem Konzept der vernetzten Operationsführung, kann der Cyberwar auf der Ebene der Übermittlung, der Entscheidung, der Wahrnehmung und/oder

⁶²³ Vgl. Gayken, 2011, S. 179.

⁶²⁴ Vgl. Hansel, 2011, S. 568f. (in: Jäger/Beckmann, 2011)

⁶²⁵ Ebd., S. 570.

⁶²⁶ Vgl. Forgò, Nikolaus; Helfrich, Marcus; Schneider, Jochen: Betrieblicher Datenschutz. Rechtshandbuch, 3. Auflage, München 2019, S. 821.

⁶²⁷ Arquilla, John; Ronfeldt, David: Cyberwar is coming! In: Comparative Strategy, Vol. 12, 1993, S. 146.

⁶²⁸ Minkwitz, 2003, S. 20.

Wirkung angewandt werden.⁶²⁹ Die Übermittlungs-, die Wahrnehmungs- und die Wirkungsebene sind dabei als ausschließlich militärische Bereiche zu fassen, während die Entscheidungsebene durchaus auch zivile Entscheidungsträger der politischen Führung beinhalten kann.

Auch bei weniger hoch technisierten Streitkräften kann der Kleine Cyberwar zur Anwendung gebracht werden, er wirkt dann nur begrenzt auf wenige Systeme des Militärs. Die Intensität dieser Form des Virtuellen Krieges ist, auf Grund der Begrenztheit, niedriger als beim Großen Cyberwar anzusehen. Für die militärischen Streitkräfte selbst ist die Intensität als hoch einzustufen, jedoch gesamtstaatlich handelt es sich um eine geringere Intensität als beim Großen Cyberwar. Die Urheberschaft ist auch hier nicht eindeutig feststellbar, aber hinsichtlich der Wahrnehmbarkeit der Wirkung ist der Kleine Cyberwar nicht im Verborgenen liegend.

Auch wenn die Aktionen im Verborgenen vorbereitet werden, zeitigen sie einen Effekt, der auch als solcher erkannt werden kann. Der Kleine Cyberwar ist Teil einer militärischen Gesamtoperation und unterstützt in diesem Rahmen die Zielerreichung. Es besteht damit eine Analogie zum klassischen Kleinen Krieg zur Unterstützung eines konventionellen Krieges.

In Georgien zum Beispiel, wurden nicht direkt militärische Systeme bewirkt, jedoch mittelbar, durch den Angriff auf für die Informationskriegführung wichtige Ressourcen, die Einwirkung auf den Willen des Gegners und die Entscheidungsabläufe realisiert. Der Kleine Cyberwar wirkt also mittelbar oder unmittelbar gegen militärische Komponenten des Cyberspace und ist damit klar in der Verantwortung des Militärs. Diese Form des Virtuellen Krieges bedarf der Einbettung in eine militärische Gesamtoperation.⁶³⁰ Eine selbstständige Durchführung eines Kleinen Cyberwar ist rein hypothetisch – militärische Cyber Kapazitäten gegen militärische Cyber Kapazitäten – möglich, doch bedarf es zur Herbeiführung einer Entscheidung des Einsatzes der konventionellen Streitkräfte. Eine Verbindung mit dem konventionellen Krieg ist damit angezeigt.

7.1.5 Exkurs: Der Kleine Cyberwar am Beispiel des Fünf-Tage-Krieges in Georgien

In der vorliegenden Literatur sind die Kriegsziele eindeutig definiert.⁶³¹ Die strategischen Zielsetzungen sind hier die Verhinderung eines NATO-Beitritts Georgiens und die Herbeiführung des Rücktritts von Saakaschwili. Der NATO-Beitritt hätte, neben einer regionalen Einflussnahme der Vereinigten Staaten von Amerika, auch die potentielle Gefahr der Stationierung des Raketenabwehrschildes an der Südflanke der Russischen Föderation nach sich gezogen.

⁶²⁹ Vgl. Netzwerkorientierte Verfahren Austria, 2006, S. 18.

⁶³⁰ Vgl. Bilban/Grininger, 2019, S. 43.

⁶³¹ Vgl. Kuster, 2011, S. 50.

Die Machtprojektionsfähigkeit im Schwarzen Meer, die Erhaltung der militärischen Kapazitäten in der Transkaukasus-Region und die Herbeiführung der Handlungsunfähigkeit der staatlichen Einrichtungen und Medien Georgiens stellen die militärstrategischen Zielsetzungen dar.

Die Operationslinien sind im Wesentlichen an der räumlichen Aufteilung der Operation orientiert. Neu ist dabei die Dimension einer Computer Network Operation als Teil der militärischen Gesamtoperation. Obwohl nicht offiziell bestätigt, ist der Angriff im Cyberspace Georgiens wahrscheinlich durch militärische Stellen koordiniert und auch teilweise durchgeführt worden. Die Fähigkeiten hinsichtlich solcher Vorgehensweisen sind einerseits beim FSB und andererseits bei den Weltraumtruppen angesiedelt.⁶³²

Auch die Ziele in dieser Operation sind in der Literatur ausführlich beschrieben. Die Erhaltung und Wiederherstellung der Integrität der beiden autonomen Republiken steht dabei im Vordergrund. Allein die operativen Ziele, in der Operationslinie Computer Network Operation, sind durch die Beurteilung und Analyse der Ereignisse abgeleitet worden.⁶³³ Die Beschränkung der Nutzung der staatlichen Internetseiten, sowie die Unterbindung einer medialen Berichterstattung über das Netz, sind hier hervorzuheben.

Die Centers of Gravity sind auf Seiten der Russischen Föderation die Streitkräfte und deren Joint-Fähigkeiten und seitens der Georgier das Zusammenwirken der Streitkräfte, sowie die Fähigkeit zur Nutzung der modernen Kommunikationseinrichtungen.⁶³⁴ Die Vorbereitung auf den Kleinen Cyberwar erfolgte Großteils unerkannt bereits vor Operationsbeginn.

Die Auswirkungen wurden erst am Beginn der Kampfhandlungen manifest und damit auch wahrnehmbar. Hier greift der Kleine Cyberwar die Entscheidungsebene an, indem er die Kommunikationsinfrastruktur auf politischer Ebene bewirkte. Durch die eingeschränkte Kommunikation, über das Internet und die dadurch auch eingeschränkte Medienarbeit, ist die Handlungsfähigkeit der Politik stark behindert worden.

7.1.6 Der Zusammenhang zwischen den Formen des Cyberwar

Der Cyberwar findet viele Analogien in der Luftkriegführung. Das Verhältnis zwischen Großem und Kleinem Cyberwar ist ähnlich dem Verhältnis von Bomber zu Jagdflieger. Der Bomber wirkt gegen die Tiefe des Gegners und auf sein gesamtes System, die Wirtschaft, die Verkehrsinfrastruktur, die Bevölkerung. Der Jagdflieger kämpft gegen andere militärische Luftfahrzeuge im Rahmen einer Gesamtoperation. Der Zusammenhang der Formen des Cyberwar soll daher im Folgenden, an Hand der Überlegungen von Douhet, näher erläutert werden.

⁶³² Anm. d. Verf.: Diese Kompetenzen sind zurzeit nicht belegbar, aber durchaus logisch ableitbar.

⁶³³ Vgl. Council of the European Union (Hrsg.), Independent International Fact-Finding Mission on the Conflict in Georgia (IIFFMCG), Volume II, 2009, S. 217ff.

⁶³⁴ Vgl. Kuster, 2011, S. 55.

Das Verhältnis des Cyberwar zu den anderen Kriegsformen lässt sich folgendermaßen ableiten:

„Man hat erkannt, daß die Luftmacht logischerweise zu Armee und Marine in dasselbe Verhältnis gebracht werden muß, indem diese beiden zueinander stehen.“⁶³⁵

Daraus folgert, dass die Cyber Kriegführung in einem ähnlichen Verhältnis zu den anderen Arten der Kriegführung steht. Der unterstützende Charakter für den Landkrieg ist dabei schon impliziert.

„A pure Cyberwar, (wherein only cyberweaponry is deployed) is unlikely. Future wars and the skirmishes that precede them will involve a mixture of conventional or kinetic weapons with cyberweaponry acting as a disrupter or force multiplier.“⁶³⁶

Ähnlich wie beim klassischen bewaffneten Konflikt ist eine Verbindung zwischen Großem und Kleinem Cyberwar gegeben. Der Große Cyberwar hat, in seiner strategischen Wirkung, Ähnlichkeit mit den Bombereinheiten Douhets. Dieser sieht diese Einheiten als die Schlüsselmittel im Kampf gegen die gegnerischen Ziele in der Tiefe. Zur Absicherung dieses Vorgehens kann der Kleine Cyberwar gegen militärische Kräfte im Netz, die als Gegenmaßnahmen gegen den Großen Cyberwar eingesetzt werden, zur Anwendung kommen.⁶³⁷

Für den Kleinen Cyberwar ergeben sich somit zwei mögliche Einsatzspektren, zur Unterstützung im Rahmen konventioneller bewaffneter Konflikte, tritt die Unterstützung des Großen Cyberwar hinzu. Douhet führt dazu Folgendes aus:

„Der Gegner muß in seinen Stützpunkten, seiner Etappe, seinen Produktionsgebieten, d.h. also in seiner strategischen, taktischen und wirtschaftlichen Etappe vernichtet werden.“⁶³⁸

Dies entspricht der Anforderung an den Großen Cyberwar und dazu benötigt man Unterstützung durch den Kleinen Cyberwar, da:

„[...] die Bombereinheiten jedoch bei der Durchführung ihrer Aufgaben während des Anflugs auf fremde Luftstreitkräfte stoßen werden, selbst jedoch ihrem Wesen nach nicht besonders zum Kampf in der Luft geeignet sind, müssen Luftstreitkräfte besonderen Charakters die Aufgabe übernehmen, den Bombereinheiten den Weg nach ihren Kampfzielen zu bahnen und Abwehrmaßnahmen der gegnerischen Luftstreitkräfte durch Luftkampf zu vereiteln.“⁶³⁹

⁶³⁵ Douhet, 1935, S. 14.

⁶³⁶ Sommer/Brown, 2011, S. 14.

⁶³⁷ Vgl. Kurz/Rieger, 2018, S. 189.

⁶³⁸ Douhet, 1935, S. 29.

⁶³⁹ Ebd., S. 29.

Mit dem Zusammenhang zwischen Kleinem und Großem Cyberwar verhält es sich ähnlich. Da der operative Kleine Cyberwar zusätzlich zum Großen Cyberwar zur Anwendung gelangen kann, ergibt sich auch daraus die höhere Intensität des Virtuellen Krieges insgesamt. Neben der Ausdehnung und der Wirkung, auf alle Bereiche eines Gemeinwesens, ist dies ein weiterer Hinweis auf die hohe Intensität des Virtuellen Krieges, des Cyberwar. Die Aktionen im Cyberspace können in einer, auf der steigenden Intensität basierenden, Abfolge verstanden werden.

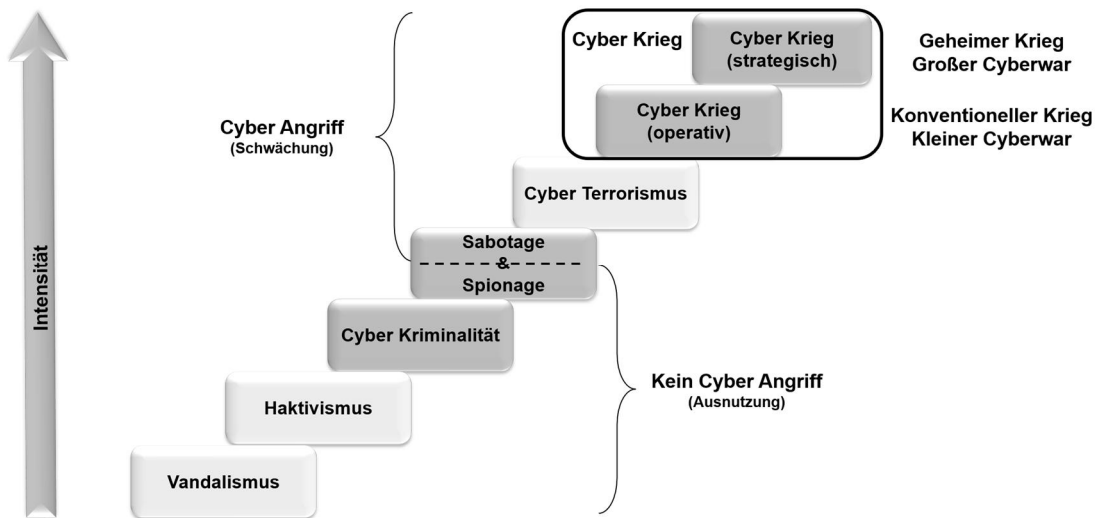


Abbildung 11: Intensität der Aktionen im Cyberspace⁶⁴⁰

Dabei ist klar zu erkennen, dass Aktionen, die der Ausnutzung des Cyberspace dienen, eine niedrigere Intensität aufweisen, als solche, die zur Schwächung von spezifischen Bereichen desselben angewandt werden. Hervorstreichen ist, dass die niedrigeren Intensitätsstufen in den Stufen höherer Intensität enthalten sein oder zusätzlich dazu auftreten können, welches die Intensität nochmals erhöht.

Der Cyberwar und seine beiden Formen, seine Momente, sind als Unterstützungsmaßnahmen für konventionelle bewaffnete Konflikte zu fassen. Geers führt dazu Folgendes aus:

„[...] every political and military conflict, will also take place in cyberspace.“⁶⁴¹

Der Kleine Cyberwar wirkt dabei unmittelbarer, vor allem in zeitlicher Hinsicht, bedarf aber entweder eines konventionellen Krieges oder eines Großen Cyberwar, die er unterstützt. Der Große Cyberwar kann selbstständig geführt werden und zeitlich mittelbar zum Einsatz kommen.

⁶⁴⁰ Abbildung durch den Verfasser erstellt.

⁶⁴¹ Geers, Kenneth: Demystifying Cyber Warfare. In: Schröfl, Josef; Muhr, Dieter; Rajaei, Bahram M. (Hrsg.): Hybrid and cyber war as consequences of the asymmetry. A comprehensive approach answering hybrid actors and activities in cyberspace: political social and military responses, Frankfurt am Main, New York 2011, S. 119.

Letztlich braucht es zur Entscheidung den Einsatz konventioneller Kräfte.⁶⁴² Dabei spielt der Vernetzungsgrad eines Gemeinwesens eine wesentliche Rolle. Die Streitkräfte, welche im Zusammenhang mit dem Großen Cyberwar zum Einsatz gelangen, sind nicht von der Natur, wie die klassischen konventionellen Streitkräfte. Barnett bezeichnet diese Kräfte als „System Administrator Force“ (Hervorhebung durch den Verfasser.).⁶⁴³ Diese Art von Streitkräften ist auf hohe Vernetzung ausgerichtet und nutzt diese zur Herbeiführung von Sicherheit.

„[...] the Sys Admin will seek preventive cures that emphasize making networks more robust and crisis situations more transparent.“⁶⁴⁴

Diese Kräfte sind das Resultat einer neuen Art der Kriegführung. Sie dienen nicht nur der Stärkung der eigenen Netzwerke, sondern auch der Schwächung von gegnerischen Netzwerken. Diese Doppelrolle ist in der obigen Aussage impliziert. Der Kleine Cyberwar ist, wie gefolgert, einerseits Unterstützungsmaßnahme für den Großen Cyberwar, aber andererseits auch Unterstützungsmaßnahme im konventionellen bewaffneten Konflikt. Barnett sieht hier den Einsatz klassischer Streitkräfte angezeigt, welche er als „Leviathan Forces“ (Hervorhebung durch den Verfasser.) bezeichnet.⁶⁴⁵

„The Leviathan will be punitive, bringing down enemy networks and blindsiding foes, [...]“⁶⁴⁶

Aus dieser Einteilung moderner Streitkräfte in zwei Gruppen ist erkennbar, dass die Eigenschaften der eingesetzten Streitkraft vom Vernetzungsgrad des Gemeinwesens abhängen. Klassisch konventionell geführte Konflikte sind dort angezeigt, wo der Vernetzungsgrad ein geringer ist. In hoch vernetzten Gesellschaften wirken Streitkräfte anders. Der Große Cyberwar bedarf also besonderer Streitkräfte konventionellen Typs, da die Wirkungsbreite durch den Cyberwar eine sehr hohe ist. Der Kleine Cyberwar ist auf militärische Systeme anzuwenden, welche auch in weniger vernetzten Gemeinwesen einen gewissen Vernetzungsgrad aufweisen. Dies erfolgt zur Unterstützung klassischer konventioneller Streitkräfte.

Der Vernetzungsgrad ist somit ein Hinweis darauf, welche Form des Cyberwar, in Verbindung mit welcher Art von Streitkräften, zur Anwendung gelangt. Die Intensität des Cyberwar ist dabei direkt proportional zum Vernetzungsgrad. Je höher dieser ist, desto intensiver werden die Konflikte im Cyberspace. Ist nur das Militär hoch vernetzt, so ist der Intensitätsgrad ein geringerer. Angriffe können nur auf die militärischen Systeme wirken. Diese Folgerung bestätigt die Einteilung des Krieges im Netz in einen Großen und Kleinen Cyberwar.

Der Zusammenhang zwischen den beiden Formen des Cyberwar ist durch den Umstand begründet, dass der Kleine und Große Cyberwar

⁶⁴² Anm. d. Verf.: Dieser Einsatz muss sich nicht manifestieren, aber latent möglich sein.

⁶⁴³ Vgl. Barnett, 2004, S. 315ff.

⁶⁴⁴ Ebd., S. 320.

⁶⁴⁵ Vgl. ebd., S. 315ff.

⁶⁴⁶ Ebd., S. 320.

Momente des Virtuellen Krieges sind. Der Kleine kann ohne Großen Cyberwar, im Rahmen konventioneller Militäroperationen, zur Anwendung gelangen. Werden beide Formen des Cyberwar zur Anwendung gebracht, so hat der Virtuelle Krieg seine totale Ausprägung und somit die höchste Intensität erreicht. Zum Zusammenhang von Großem und Kleinem Krieg führt Lilienstern Folgendes aus:

„[...] daß der Krieg [Anm. d. Verf.: Auch der Cyberwar als Element des Krieges an und für sich.] überhaupt aus beiden Kriegsarten zusammengenommen, oder gemeinschaftlich gebildet wird, und die im Laufe der Feldzüge vorkommenden Ereignisse und Unternehmungen daher theils in das Gebiet des kleinen, theils in das Gebiet des großen Krieges gehören müssen [...]“⁶⁴⁷

Diese Aussage ist auch auf den Cyberwar anzuwenden. Die beiden Formen des Krieges im Cyberspace zählen zum Kleinen Krieg und sind daher als Unterstützungsmaßnahmen zu fassen, ob sie dennoch einen existenziellen Charakter aufweisen können, wird im Weiteren noch zu klären sein. Bei einer Einordnung – der beiden Formen des Cyberwar – in die Clausewitzsche Trinität des Krieges, zeigt sich die Inversion der Formen des Cyberwar gegenüber den Formen des klassischen konventionellen Krieges.

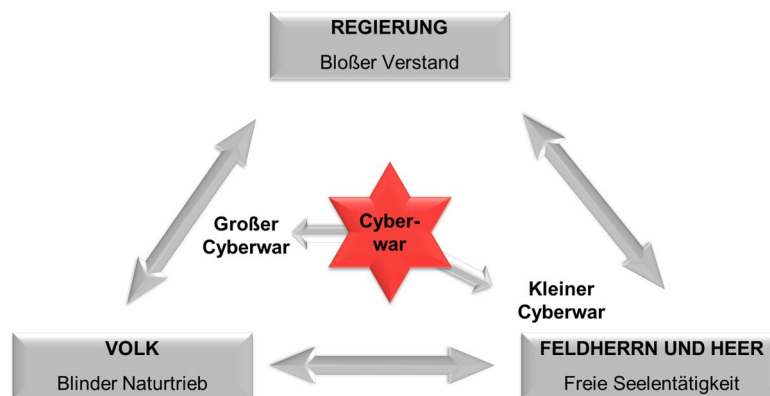


Abbildung 12: Die Trinität des Cyberwar⁶⁴⁸

Während der Große Krieg die begrenzte Form darstellt, ist der Kleine Krieg die entgrenzte Form des bewaffneten Konfliktes. Beim Cyberwar ist die begrenzte Form der Kleine Cyberwar, der eingebettet in eine militärische Gesamtoperation stattfindet. Die totale Form des Krieges im Netz ist der, vor allem auf strategischer Ebene stattfindende, Große Cyberwar. Der Schutz gegenüber diesen Formen des Krieges im Netz steht im Mittelpunkt der folgenden Betrachtungen.

⁶⁴⁷ Lilienstern, August Rühle von: Handbuch für den Offizier zur Belehrung im Frieden und zum Gebrauch im Felde, Berlin 1818, S. 1.

⁶⁴⁸ Abbildung durch den Verfasser erstellt.

7.1.7 Die Sicherheit im Cyberspace

Cyber Sicherheit ist nur eine Form der Sicherheit, in Verbindung mit der Thematik Cyberspace. Es können verschiedene Domänen der Sicherheit identifiziert werden. Als zentraler Sicherheitsbereich berührt Cyber Sicherheit alle anderen Sicherheitsdomänen im Cyberspace und stellt somit den Oberbegriff für Sicherheit im Netz dar.⁶⁴⁹ Der Schutz gegen Kriminalität und Vorkommnisse, die nicht aus dem Netz heraus, sondern von außen schädigend einwirken, bilden den äußeren Sicherheitsbereich. Der innere Bereich teilt sich in die Informationssicherheit und den Schutz der kritischen Informationsinfrastruktur. Netzwerksicherheit meint den Schutz in sich geschlossener Netzteile, welche auch miteinander verbunden sein können. Internetsicherheit umfasst den Schutz des Internet, als Erweiterung von Heim- und Arbeitsumgebung im Cyberspace.⁶⁵⁰ Der Bereich, der hier nicht explizit aufscheint, ist die Cyber Defence, als Teil der Cyber Sicherheit.

Im weiteren Verlauf werden die anderen Domänen der Sicherheit im Cyberspace unter dem Begriff Cyber Security subsumiert. Aus dem bisher Dargestellten lassen sich, in Bezug auf die Sicherheit im Netz, zwei große Bereiche herausarbeiten. Die Cyber Sicherheit kann in eine militärische und eine zivile Komponente gegliedert werden. Da die Kräfte, welche in den beiden Formen des Cyberwar zum Einsatz kommen unterschiedlich sind, liegt es nahe, dass auch die Maßnahmen zum Schutz vor den beiden Formen des Cyberwar, von unterschiedlicher Art sind. Hier kann zwischen Cyber Defence und Computer Network Operations unterschieden werden. Als Überbegriff umfasst die Cyber Security alle Maßnahmen zum Schutz, der im Cyberspace befindlichen Systeme, vor Angriffen. So definiert das Department of Homeland Security (DHS) Cyber Security wie folgt:

„The prevention of damage to, unauthorized use of, or exploitation of, and, if needed, the restoration of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability. Includes protection and restoration, when needed, of information networks and wireline, wireless, satellite, public safety answering points, and 911 communications systems and control systems.“⁶⁵¹

Es geht hier noch keine Trennung – in militärische und nicht-militärische Aktionen im Cyberspace – hervor, wobei nicht die gänzliche Vermeidung von Gefahren gefordert ist, sondern die Beseitigung von Unsicherheiten im Cyberspace. Die Möglichkeit, Angriffe oder Aktionen gegen eigene IKT-Systeme zu erkennen, bietet hier schon die geforderte Reduzierung von Unsicherheit. Die Prävention jeglicher Bedrohung im und durch den Cyberspace ist im Fokus dieser Maßnahmen zu sehen. Darauf aufbauend soll eine gewisse Handlungsfähigkeit der wesentlichen Einrichtungen erhalten werden.

⁶⁴⁹ Vgl. Klimburg, 2012, S. 10.

⁶⁵⁰ Vgl. ebd., S. 10.

⁶⁵¹ DHS, The Cybersecurity Strategy for the Homeland Security Enterprise, 2012, S. D-2.

Auch die österreichische Definition der Cyber Sicherheit schließt alle Bedrohungen mit ein. Es gibt auch hier keine explizite Unterscheidung zwischen militärischen und nicht-militärischen Gefahren.

„Cyber Sicherheit beschreibt den Schutz eines zentralen Rechtsgutes mit rechtsstaatlichen Mitteln vor akteursbezogenen, technischen, organisations- und naturbedingten Gefahren, die die Sicherheit des Cyber Space (inklusive Infrastruktur- und Datensicherheit) und die Sicherheit der Nutzer im Cyber Space gefährden. Cyber Sicherheit trägt dazu bei, die Gefährdungen zu erkennen, zu bewerten und zu verfolgen sowie die Fähigkeit zu stärken, Störungen im und aus dem Cyberspace zu bewältigen, die damit verbundenen Folgen zu mindern sowie die Handlungs- und Funktionsfähigkeit der davon betroffenen Akteure, Infrastrukturen und Dienste wieder herzustellen.“⁶⁵²

Da sich die Definition sowohl mit präventiven als auch reaktiven Maßnahmen beschäftigt, ist ableitbar, dass es sich nicht um absolute Sicherheit, sondern um einen Zustand handelt, der durch die Aufrechterhaltung der Funktionsfähigkeit gewährleistet werden soll. Dass es bei der Cyber Sicherheit nicht um absolute Sicherheit im Cyberspace geht, zeigt auch die Definition in der Cyber Sicherheitsstrategie für Deutschland aus dem Jahr 2011, die Cyber Security fasst, als

„[...] der anzustrebende Zustand der IT-Sicherheitslage, in welchem die Risiken des globalen Cyber-Raums auf ein tragbares Maß reduziert sind.“⁶⁵³

Auch unterscheidet die deutschen Strategie zwischen ziviler und militärischer Cyber Sicherheit.⁶⁵⁴ Bei der Cyber Security steht die Wahrnehmung von Bedrohungen im Vordergrund. Aus militärischer Sicht ist dies vor allem für den Krieg im Geheimen, den Großen Cyberwar, von Bedeutung. Die Erkennung der Gefahren, welche für die eigenen Systeme im Netz bestehen, ist von großer Wichtigkeit. Wenn man die Gefahren erkennen kann, ist der Große Cyberwar nicht mehr ein Krieg im Geheimen und man kann Gegenmaßnahmen treffen. Diese können dann aktiver oder reaktiver Natur sein. Als Unterkategorie der Cyber Sicherheit – und zwar der militärischen Cyber Security – ist die Cyber Defence zu verstehen. Diese ist eine

“Policy / Activity to prevent, react to and recover from a Cyber Attack on our information and data. Cyber Defence is a subset of Cyber Security.”⁶⁵⁵

Dabei unterscheidet diese Definition nicht zwischen militärischer und ziviler Cyber Sicherheit. Betrachtet man die Definition in der Österreichischen Strategie für Cyber Sicherheit ist Cyber Defence eindeutig dem Militär zuzurechnen. Cyber Defence ist

⁶⁵² BKA, Österreichische Strategie für Cyber Sicherheit (ÖSCS), 2013, S. 21.

⁶⁵³ BMI, Cyber-Sicherheitsstrategie für Deutschland, 2011, S. 15.

⁶⁵⁴ Vgl. ebd., S. 15.

⁶⁵⁵ EUMS, EU Concept for Cyber Defence for EU-led Military Operations, 2012, S. 4.

„[...] die Summe aller Maßnahmen zur Verteidigung des Cyber-Raumes mit militärischen und speziell dafür geeigneten Mitteln zur Erreichung militärstrategischer Ziele. Cyber Defence ist ein integriertes System und besteht in seiner Gesamtheit aus der Umsetzung der Maßnahmen zur IKT-Sicherheit und der Informationssicherheit, aus den Fähigkeiten des milCERTs, der CNO (Computer Network Operations) und der Unterstützung durch die physischen Fähigkeiten der Streitkräfte.“⁶⁵⁶

Etwas ungenau erscheint, bei dieser Auslegung der Cyber Verteidigung, die Formulierung der Unterstützung von Cyber Kräften durch die physischen Fähigkeiten der Streitkräfte. Gemeint sein kann hier vor allem der Fähigkeitsbereich des Militärs, der es ermöglicht physisch auf den Cyberspace zu wirken. Der Cyberwar ist ja als Unterstützung der konventionellen Streitkräfte zu fassen, nicht umgekehrt. Wird unter Cyber Defence die militärische Landesverteidigung im Cyberspace analog zur Landesverteidigung im herkömmlichen Sinn verstanden, so ist eine Fokussierung auf rein militärische Aspekte zu eng gefasst.⁶⁵⁷ Landesverteidigung ist Souveränitätsschutz und greift damit massiv in den zivilen Bereich ein, es muss daher ein Zusammenspiel zwischen militärischer und ziviler Cyber Sicherheit geben, dies umso mehr als die Masse der souveränitätsrelevanten Kritischen (Cyber) Infrastruktur von zivilen Betreibern betrieben wird.

Ist der Staat durch den Großen Cyberwar bedroht, erfolgt der Einsatz des Militärs, im Rahmen der Cyber Defence, im Zusammenwirken mit unterstützenden Maßnahmen der zivilen Cyber Security.

Darüber hinaus kann das Militär auch einen Beitrag zur Unterstützung der zivilen Cyber Sicherheit leisten. Die militärische Cyber Sicherheit ist Aufgabe der Streitkräfte, diese haben in erster Linie für ihren Eigenschutz zu sorgen, im Rahmen militärischer Operationen erfolgt dies durch Anwendung von Computer Network Operations. Diese beinhalten Verteidigung, Angriff und Aufklärung. Die militärische Cyber Security umfasst also, im Rahmen des Kleinen Cyberwar, drei Teilbereiche: Die Computer Network Exploitation (CNE), die Computer Network Attack (CNA) und die Computer Network Defence (CND). Unter CNO sind folgende Fähigkeiten zu verstehen:

„Capability and action taken to protect, control and optimise computer networks, associated hardware and software and to contribute towards information superiority and thereby deny an adversary this capability.“⁶⁵⁸

Die Formulierung „Gegner“ impliziert die Anwendung der CNO im militärischen Kontext. Die Teilbereiche der CNE und CND werden durch das

⁶⁵⁶ BKA, Österreichische Strategie für Cyber Sicherheit (ÖSCS), 2013, S. 21.

⁶⁵⁷ Vgl. BMLVS, Militärische Cyber Handlungen und Verfahren (Cyber Operations), Anlage zum Militärstrategischen Konzept, Entwurf, 2013, S. 7ff.

⁶⁵⁸ EUMS, EU Concept for Cyber Defence for EU-led Military Operations, 2012, S. 4.

Militär schon in Friedenszeiten praktiziert und konzentrieren sich nicht ausschließlich auf die Anwendung im Cyberwar. Im Zusammenhang mit der getroffenen Einteilung des Cyberwar, in einen Großen und einen Kleinen Cyberwar, ergibt sich eine Zuweisung der Begriffe bezüglich der Sicherheit im Netz. Der Große Cyberwar betrifft sowohl die Cyber Defence, im Rahmen der militärischen Cyber Sicherheit, als auch die zivile Cyber Sicherheit, da er auf politisch-strategischer Ebene wirkt. Der Kleine Cyberwar berührt die militärische Cyber Sicherheit – und die daraus erwachsende Fähigkeit zu Computer Network Operations – auf Grund seiner Beschränkung auf militärische Systeme.

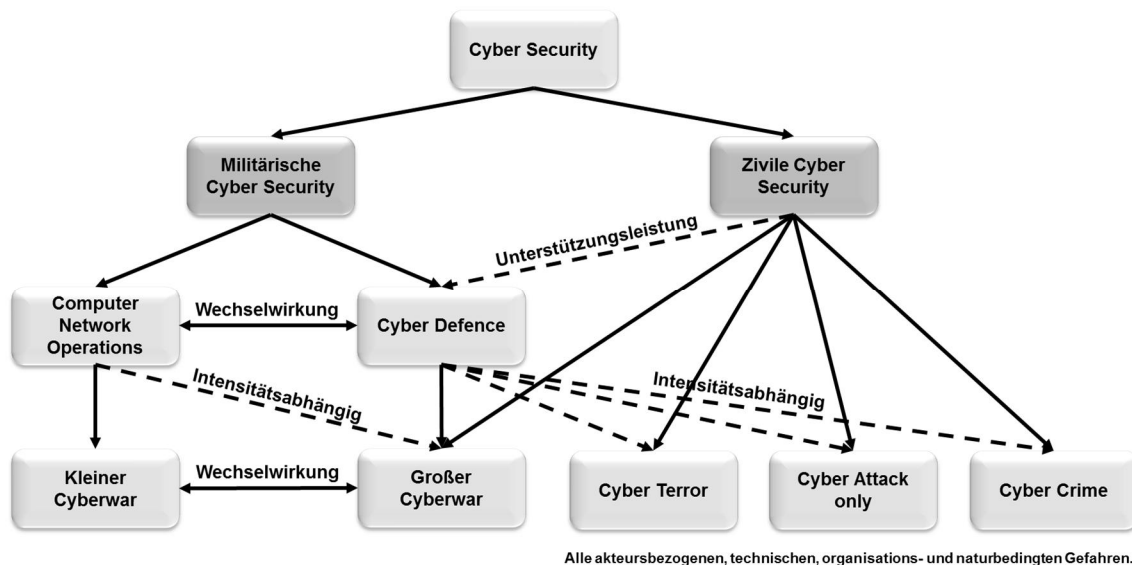


Abbildung 13: Die Teilbereiche der Cyber Security⁶⁵⁹

In der Praxis ist eine scharfe Trennung nicht durchführbar, denn der Große Cyberwar kann durch Elemente des Kleinen Cyberwar unterstützt werden. Auch können für das Gemeinwesen vitale Bereiche, die grundsätzlich in die Zuständigkeit der zivilen Cyber Security fallen, soweit betroffen sein, dass eine militärische Unterstützung angezeigt ist. Hier lässt sich eine Analogie zum Raumschutz – welcher im Kapitel vom Recht im Cyberwar dargestellt wird – herstellen. Es kann eine erste Rollenverteilung abgeleitet werden. Im Großen Cyberwar kommt dem Militär in einer ganzheitlichen Lösung nur eine Teilverantwortung zu, die, je nach Intensität, veränderbar sein muss. Im Kleinen Cyberwar ist die Verantwortung klar beim Militär zu finden, da vorrangig militärische Systeme Ziele von Angriffen sind.

„Dem Militär die Führungsrolle beim Schutz ziviler Netzwerke zu überlassen ist höchst unklug. Aber angesichts der Tatsache, dass Cyberwaffen das Potenzial haben, die lebenswichtige nationale Infrastruktur eines Landes (und damit auch das Leben der Menschen) zugrunde zu richten, müssen Vorkehrungen getroffen werden, damit

⁶⁵⁹ Abbildung durch den Verfasser erstellt. Vgl. BMLVS, Militärische Cyber Handlungen und Verfahren (Cyber Operations), 2013, S. 22ff.

das Militär in Extremsituationen eingreifen kann. Dies sollte sich aber auf außergewöhnliche, überprüfbare Situationen beschränken.“⁶⁶⁰

Es ist sehr schwer im ersten Ansatz zu erkennen, welches Potential ein Cyber Angriff zum Zeitpunkt seiner Wahrnehmung schon erreicht hat. Daher ist ein Übergeben von operativer Verantwortung während eines Angriffes sehr problematisch, vor allem wenn eine ansteigende Intensität feststellbar wird. Dennoch lassen sich aus der Form des Cyberwar die Formen der Sicherheit und daraus eine erste Zuordnung der Verantwortung dafür ableiten. Da Cyber Sicherheit nur ein Aspekt von Sicherheit ist, muss in diesem Zusammenhang die Verbindung, von Cyber Sicherheit mit der Sicherheit an und für sich, angesprochen werden.

„America can only increase its security when it extends connectivity or expands globalization’s reach, and by doing so, progressively reduces those trouble spots or off-grid locations where security problems and instability tend to concentrate.“⁶⁶¹

Diese Aussage gilt global und nicht nur für Amerika allein. Vernetzung schafft Abhängigkeiten, welche es den Akteuren in einem solchen System zunehmend schwerer macht, gegen das Netz zu agieren.

„Ein Eingriff, der einen Teil des Systems betrifft oder betreffen soll, wirkt auch auf viele andere Teile des Systems.“⁶⁶²

Die Sicherheit wird vordergründig erhöht, bei gleichzeitiger Steigerung der Verwundbarkeit. Damit einher geht ein Wandel in der Austragung von Konflikten in hoch vernetzten Gemeinwesen. Während in wenig vernetzten Regionen der Einsatz der konventionellen Streitkräfte indiziert ist, muss in hochintegrierten Gebieten ein Militär mit spezifischen Fähigkeiten zum Einsatz kommen. Barnett spricht in diesem Zusammenhang von der Teilung der Welt, in einen hochintegrierten Kern, dem Core, und einen nichtintegrierten Teil, das Gap.⁶⁶³ Für Barnett ist der Weg, zu einem Mehr an Sicherheit, allein durch Vernetzung⁶⁶⁴ vorgezeichnet.

Gayken sieht den Schlüssel zu mehr Sicherheit in einer Entnetzung vor allem in technischer Hinsicht.⁶⁶⁵ Zweck ist es dabei, die Systeme nicht angreifbar zu machen und die Verwundbarkeit zu minimieren. Nüchtern betrachtet scheint dies jedoch bereits der Niederlage in einem Cyberwar zu entsprechen, ohne sich der Auseinandersetzung gestellt zu haben. Diese Ambivalenz spiegelt sich in den sogenannten fünf Dilemmata der Cyber

⁶⁶⁰ Glenny, 2012, S. 222.

⁶⁶¹ Barnett, 2004, S. 56.

⁶⁶² Freudenberg, 2008, S. 44.

⁶⁶³ Vgl. Barnett, 2004, S. 8.

⁶⁶⁴ Anm. d. Verf.: Diese Vernetzung bezieht sich nicht nur auf den Cyberspace, sondern auf alle relevanten Bereiche der Gemeinwesen. Durch sie kommt wirtschaftliche Entwicklung und Wohlstand zu den Menschen und das Bedürfnis Krieg zu führen tritt in den Hintergrund.

⁶⁶⁵ Vgl. Gayken, 2011, S. 206.

Sicherheit wieder.⁶⁶⁶ Sicherheit ist aus Sicht des Verfassers durch Integration zu erreichen, da diese die Menschen zum Teil eines Ganzen macht und ein Angriff immer auch den Angreifer mitbeeinträchtigen würde.

Weiter fördert Vernetzung die Entwicklung des Gesamtsystems und damit das Gemeinwohl. Andererseits muss im Auge behalten werden, dass Vernetzung die Verwundbarkeit erhöht und es Akteure gibt, denen eine Selbstbeeinflussung bei einem Angriff nicht abschreckend genug erscheint. Dies sind meist jene, die nicht an einer Integration ins Gesamtsystem interessiert und daher von einer Selbstbeeinflussung nicht so stark abhängig sind. Sicherheit und Verteidigung haben sich den neuen Herausforderungen anzupassen. Die Herausforderung, vor allem im Bereich der zivilen Cyber Sicherheit, ist die fehlende Wahrnehmung. Eine Bedrohung der Sicherheit ist schließlich nur dann ein Sicherheitsproblem, wenn es als solches wahrnehmbar ist. Dies ist vor allem beim Großen Cyberwar kaum der Fall.

Krieg im Netz hat verschiedene Ursachen und Ziele, je nachdem welche Akteure ihn führen. Ohne auf die Akteure im Detail eingehen zu wollen, wird im Folgenden analysiert, welche Ursachen, Ziele und welcher Zweck dem Cyberwar zu Grunde liegen.

7.2 Zu den Ursachen und dem Zweck des Cyberwar

Für den Krieg konnte als Ursache eine Asymmetrie der Interessen festgestellt werden. Es geht dabei um einen Potentialunterschied, welcher durch den bewaffneten Konflikt ausgeglichen werden soll. Ursache für den Ausbruch des Krieges kann dabei sowohl ein Zuviel, als auch ein Zuwenig an Macht sein. Entscheidend ist die Asymmetrie. Der Cyberwar ist ein Element des Krieges an und für sich und daher an der Ursache desselben orientiert. Macht spielt daher auch hier eine entscheidende Rolle und zwar in Form der Information.⁶⁶⁷ Es ist

„[...] die Kontrolle der Informationstechnologie (Anm. d. Verf.: Und damit die Kontrolle der Informationen.) der Schlüssel zur Macht im 21. Jahrhundert.“⁶⁶⁸

Es gibt unterschiedliche Akteure im Cyberwar, wobei grundsätzlich zwischen zwei großen Gruppierungen unterschieden werden kann: Die hoch integrierten und vernetzten und die nichtintegrierten, gering vernetzten Akteure. Beide Gruppen können sich den Cyberwar zu Nutze machen. Die Zielsetzungen, die dabei verfolgt werden, sind grundsätzlich unterschiedlicher Natur. Es folgt eine Darstellung der Ursachen für den

⁶⁶⁶ Anm. d. Verf.: Im National Cyber Security Framework Manual des CCD COE der NATO finden sich fünf Gegensätze, welche mit der Ent- versus Vernetzungsstrategie einhergehen: Dies sind wirtschaftliche Entwicklung und Verbesserung der Sicherheit; Infrastrukturmodernisierung und Schutz der Infrastruktur; privater und öffentlicher Bereich; Datenschutz und Information Sharing; sowie Gestaltungsfreiheit und politische Stabilität.

⁶⁶⁷ Vgl. Forgò/Helfrich/Schneider, 2019, S. 820.

⁶⁶⁸ Rosenbach, Marcel; Stark, Holger: Der NSA Komplex. Edward Snowden und der Weg in die totale Überwachung, München 2014, S. 119.

Cyberwar, um dann die Ziele zu analysieren und die grundsätzliche Ausrichtung des Cyberwar, einerseits als Kampf um Informationen und andererseits als Kampf mit Informationen, einer Betrachtung zuzuführen. Die Antwort auf die Frage, worin letztlich der Zweck des Cyberwar liegt, beschließt den Abschnitt.

7.2.1 Der Zusammenhang zwischen hohem und geringem Vernetzungsgrad

Ein geringer Vernetzungsgrad führt zwangsläufig zu einer anderen Art der Kriegführung in Bezug auf den Cyberwar. Da die geringe Integration in den Cyberspace, in diesem Fall, nicht alle Bereiche eines Gemeinwesens so stark miteinander verknüpft, hat Krieg im Geheimen, der Große Cyberwar, nicht die Reichweite, die er in einer hochintegrierten Gesellschaft hat. Vielfach sind kritische Infrastrukturen nicht in das Netz eingebunden und so für einen Angriff aus dem Netz nicht erreichbar. In diesen Fällen kommen, im Falle eines bewaffneten Konfliktes, konventionelle Streitkräfte zum Einsatz. Da Streitkräfte über ein Mindestmaß an Vernetzung verfügen, greifen hier die Methoden des Kleinen Cyberwar.

Vernetzte militärische Systeme werden zum Ziel dieses Kleinen Krieges im Netz, als Unterstützungsmaßnahme konventioneller Streitkräfte. Die Möglichkeit zur Anwendung des Cyberwar ist direkt abhängig vom Vernetzungsgrad. Dieser ist also ein Parameter der Kriegführungsfähigkeit im Netz, aber auch ein Indikator für die Form des Cyberwar. In einer hochintegrierten Gesellschaft besteht die Möglichkeit den Großen Cyberwar zu führen.

Dieser Krieg im Geheimen bedarf einer ganz anderen Streitkraft. Es wird mit den Methoden des Großen Cyberwar letztlich nicht eine militärische Entscheidung gesucht, sondern vielmehr eine Beeinflussung verschiedener Politikbereiche bezweckt, wenn möglich unbemerkt.⁶⁶⁹ Nicht die Schwächung durch Zerstörung steht im Vordergrund, sondern die Schwächung durch Kontrolle und Beeinflussung. Dies macht den Großen Cyberwar so gefährlich, nämlich die Aktionen, welche der Wahrnehmung fast gänzlich entzogen sind.

Der Vernetzungsgrad beeinflusst nicht nur die Anwendung der Formen des Cyberwar, sondern hat generell einen Einfluss auf die Art der Kriegführung. Dort, wo die Beeinflussung von Politikbereichen und die Erreichung politischer Zielsetzungen ohne Einsatz von konventionellen Streitkräften erzielt werden kann, ist der konventionelle bewaffnete Konflikt, der klassische Krieg, obsolet geworden. Krieg zwischen Staaten oder innerhalb von Staaten, innerhalb des „Functioning Core“ (Hervorhebung durch den Verfasser.), ist defacto nicht mehr existent.⁶⁷⁰ Die Einflussnahme erfolgt anderwärtig, im Geheimen.

⁶⁶⁹ Anm. d. Verf.: Wie es auch im amerikanischen Präsidentschaftswahl im Jahr 2016 der Fall war. Vgl. Kurz/Rieger, 2018, S. 203ff.

⁶⁷⁰ Vgl. Barnett, 2004, S. 8.

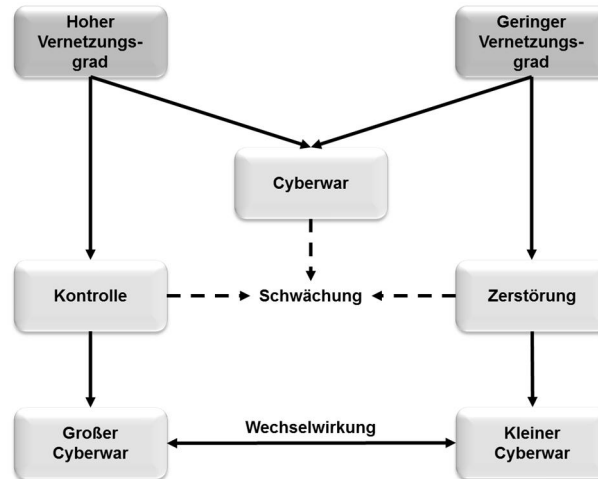


Abbildung 14: Einfluss des Vernetzungsgrades⁶⁷¹

In modernen Konflikten wird der Gegner als komplexes System verstanden. Um eine Wirkung bei ihm zu erzielen, ist eine direkte militärische Konfrontation oft nicht mehr nötig.⁶⁷² Wenn seine Beziehungen, Abhängigkeiten und Verwundbarkeiten identifiziert sind, kann auf ein direktes militärisches Kräfteressen verzichtet werden. Information wird damit zu einem Schlüsselfaktor. Voraussetzung für die Handlungsüberlegenheit ist Informationsüberlegenheit.⁶⁷³

Ein hoher Vernetzungsgrad führt zu einer Transformation von Konflikten und speziell von bewaffneten Konflikten. Die Vernetzung steigert die Sicherheit, in Bezug auf den klassischen Krieg, führt aber zu einer Erhöhung der Unsicherheit, in Bezug auf den Cyberwar. Der Wandel der Kriegführung vollzog sich dahingehend, dass früher der Gegner und dessen Strukturen klar erkennbar waren. Mit der Entwicklung weitreichender Waffen, und dazu zählen die Cyber Waffen zweifellos, sank der Grad der Erkennbarkeit.⁶⁷⁴ Mit der Vernetzung kommt noch eine weitere Herausforderung hinzu, die der Erhöhung der potentiellen Akteure in einem Konflikt.

Ein hoher Vernetzungsgrad senkt die Gefahr eines konventionellen bewaffneten Konflikts, bei gleichzeitiger Steigerung anderer Bedrohungen. Dazu zählen die eingeschränkte Wahrnehmbarkeit, die Entgrenzung und die Erhöhung der möglichen Akteure. Die Bedrohungen werden dann schlagend, wenn es, wie beim klassischen Krieg, zu einer Asymmetrie zwischen Anspruch und Wirklichkeit kommt. Diese bezieht sich vor allem auf die Kernressource des Cyberspace, die Information.

⁶⁷¹ Abbildung durch den Verfasser erstellt.

⁶⁷² Vgl. Bilban/Grininger, 2019, S. 43.

⁶⁷³ Vgl. Freudenberg, 2008, S. 49f.

⁶⁷⁴ Vgl. ebd., S. 23.

7.2.2 Verfügungsgewalt über Information als Ursache virtueller Konflikte

Die Informationsasymmetrie, als Ungleichgewicht in der Verfügungsgewalt über Information, ist der Haupttreiber für Konflikte im Cyberspace. Information ist ein wichtiger Machtfaktor und da im Informationszeitalter immer mehr Menschen Zugang zu dieser Ressource haben, wird Macht breiter gestreut.⁶⁷⁵ Diese Verbreitung bewirkt eine breitere Streuung des Konfliktpotentials. Durch diese neue Verteilung von Macht wird die Macht des Staates ausgehöhlt und sein Bedürfnis nach Information erhöht. Diese Machtasymmetrie, bezogen auf die Informationen, ist ein wesentlicher Grund für Konflikte im Cyberspace.

„Weiß man - idealerweise - über seinen Gegner alles, der Gegner über einen selbst aber nur exakt das, was man ihm glauben lassen möchte, hat man eine maximale Informationsasymmetrie geschaffen, die einen folgenden militärischen Sieg selbst bei physisch geringeren Möglichkeiten wahrscheinlich macht.“⁶⁷⁶

Da aber diese Informationsüberlegenheit den Einsatz konventioneller Streitkräfte ganz ausschließen kann, ist sie von umso größerer Bedeutung.⁶⁷⁷ Die Informationsasymmetrie kann auf drei Ebenen zum Tragen kommen: Der interpersonellen, der intragemeinschaftlichen und der intergemeinschaftlichen Ebene. Wie beim Krieg ist auf der Mikroebene eher der kriminelle Hintergrund zu sehen, obwohl es dem Einzelnen durch die Vernetzung nun möglich ist, quasi politisch zu wirken. Da aber politisches Handeln eine Gemeinschaft voraussetzt, ist diese Möglichkeit rein hypothetisch. Ein Einzelner kann für sich allein nur zu seinem eigenen Wohle, nicht zum Allgemeinwohl, also politisch handeln.

Durch ein Einwirken auf Informationen wird ein Mehr an Macht generiert. Diese Beeinflussung zielt auf Verfügbarkeit, Integrität und Vertraulichkeit der Informationen. Um sich gegen Gefahren behaupten zu können, ist ein Machtzuwachs auch im Cyberspace auf der Meso- und der Makroebene notwendig. Hier ist die Ursache für Konflikte im Cyberraum zu finden. Einerseits herrscht eine Informationsasymmetrie, die Spannungen erzeugt, und andererseits ist das Bedürfnis da, diese Asymmetrie auszugleichen. Die Ursache von Konflikten ist in der Verteilung von Information zu sehen und dem Bestreben möglichst mehr Information zu beeinflussen als der Gegner.

Bei dieser Informationsasymmetrie geht es also nicht nur darum, Informationen zu gewinnen, sondern auch darum, diese zu beeinflussen. Informationsüberlegenheit führt zur Macht im Cyberspace, zur Cybermacht.⁶⁷⁸ Diese Macht ist ein wesentlicher Faktor für die Ursache von Konflikten im Cyberspace. Dabei geht es darum, nicht nur im Cyberspace Macht auszuüben. Da dieser auch Auswirkungen auf die Realität ermöglicht,

⁶⁷⁵ Vgl. Nye, 2011, S. 179.

⁶⁷⁶ Gayken, 2011, S. 97.

⁶⁷⁷ Anm. d. Verf.: Um einen Erfolg im Cyberspace ausnutzen zu können, bedarf es trotzdem der Verfügbarkeit von konventionellen Streitkräften. Diese wirken letztlich dadurch entscheidend, auch ohne eingesetzt zu werden, sozusagen als potentielle Kraft.

⁶⁷⁸ Rosenbach/Stark, 2014, S. 15.

ist Cybermacht nicht nur auf die Virtualität beschränkt.⁶⁷⁹ Mit Informationen ist ein Einwirken auf strategisch-politischer Ebene, physisch und virtuell, möglich.⁶⁸⁰

Informationsasymmetrie ist also eine einseitige Informationsüberlegenheit. Diese auszugleichen und/oder umzukehren, ist die Ursache für Konflikte im Cyberspace. Informationsüberlegenheit ist dabei höchst komplex, da sie nicht nur im Wissen über den Gegner begründet ist, sondern auch die aktive Einwirkung auf Informationen meint. Ähnlich der Luftüberlegenheit bzw. Luftherrschaft ist das Bedürfnis nach Informationsüberlegenheit zu fassen:

„Die Luftherrschaft erobern bedeutet: sich in die Lage zu versetzen, Angriffe von einer Größenordnung zu entfalten, die alles Bisherige in den Schatten stellen; bedeutet, die Armee und Flotte des Gegners von ihren Stützpunkten abzuschneiden und sie nicht nur am Kampf, sondern auch am Durchhalten zu verhindern; bedeutet daher, das eigene Land vor derartigen Angriffen zu bewahren und den Gegner in unverhältnismäßig kurzer Zeit ohne die langwierigen zermürbenden Verluste des bisher bekannten Stellungskrieges zur Annahme eines bedingungslosen Frieden zu zwingen.“⁶⁸¹

Der Bezug zu den Streitkräften ist noch zu erweitern, da der Cyberwar darüber hinaus auf andere Bereiche des Gemeinwesens wirken kann. Die physische Wirkung ist, um die Wirkung auf die Informationen selbst, zu ergänzen. Da der Cyberwar eine rein unterstützende Funktion einnimmt, ist das Ziel desselben nicht unmittelbar der Frieden, sondern zunächst die Erringung der Informationsüberlegenheit zum Zweck des Sieges und in weiterer Folge zum übergeordneten Zweck eines Friedens.⁶⁸² Informationsüberlegenheit ist dabei wie folgt zu verstehen:

„The ability to collect, process and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.“⁶⁸³

Die Beeinflussung der Informationen des Gegners ist hier explizit ableitbar. Der Beitrag zur Herstellung des Friedens liegt hier nicht in der Schaffung einer Symmetrie im Cyberspace, also nicht in der Herstellung eines Informationsgleichgewichts. Dieses ist schwer messbar, da Information zwar quantitativ eindeutig fassbar, aber qualitativ nicht eindeutig festzulegen ist.

Information hat eine für die Akteure durchaus unterschiedliche Bedeutung. Die Eindeutigkeit eines Informationsgleichgewichts ist daher enden wollend. Die Konfliktualität ist somit im Cyberspace immanent vorhanden. Anders ausgedrückt ist Frieden in diesem Raum nicht als

⁶⁷⁹ Vgl. Nye, 2011, S. 189.

⁶⁸⁰ Vgl. Bilban/Grininger, 2019, S. 44.

⁶⁸¹ Douhet, 1935, S. 24.

⁶⁸² Vgl. Rosenbach/Stark, 2014, S. 15.

⁶⁸³ EUMS, EU Concept for Computer Network Operations in EU-led Military Operations, 2009, S. 8.

Zustand zu fassen, sondern vielmehr als ein unterstützender Prozess, welcher die Bedingungen für einen Frieden, durch Zugriff auf Informationen, ermöglicht. Dies ist ein weiterer Hinweis darauf, dass eine Integration in den Cyberspace, als Beseitigung von Informationsasymmetrie zu fassen ist.

Einerseits schafft ein hoher Vernetzungsgrad einen Zugang zu Informationen, andererseits führt er zu dem Bedürfnis und der Möglichkeit eine Informationsasymmetrie zu erzeugen. Der Vernetzungsgrad hat also eine duale Funktion hinsichtlich der Konfliktualität des Cyberspace. Der Cyberwar hat, abhängig von der Form, in der er angewandt wird, zwei große Zielsetzungen: Im Großen Cyberwar die unerkannte Kontrolle von Informationen und im Kleinen Cyberwar die Beeinflussung von Informationen militärischer Systeme. Dabei wirkt der Cyberwar sowohl physisch, als auch virtuell. Es geht also um den Kampf mit und um Informationen.

7.2.3 Der Kampf mit und um Informationen

Die virtuelle oder besser gesagt die informationelle Dimension von Cybermacht kann sowohl im als auch außerhalb des Cyberspace zur Anwendung gelangen.⁶⁸⁴ Ziele beim Kampf mit Informationen sind daher in zwei Gruppen einteilbar: In Ziele im und in Ziele außerhalb des Cyberspace. Die Ziele in diesem Raum sind einerseits die Informationen selbst und andererseits, im Zusammenhang damit, Identitäten. Gayken sieht Identitäten im Cyberspace als Schlüssel zur Beeinflussung von Informationen.

„Bestimmte Identitäten identifizieren und vortäuschen zu können, ist eine wichtige Eigenschaft, wenn Wissen und Meinen [Anm. d. Verf.: Damit sind Informationen gemeint.] beeinflusst werden sollen und auch, wenn der Zugang zu Systemen erlangt werden soll.“⁶⁸⁵

Damit sind die beiden wesentlichen virtuellen Angriffsvektoren im Cyberspace abgedeckt. Es handelt sich um einen Kampf mit Informationen.⁶⁸⁶ Das Wissen und Meinen repräsentiert die Information selbst und die Identitäten im Netz basieren auf Informationen. Der Cyberspace dient schließlich der Interaktion von Individuen, welche über den Austausch von Informationen erfolgt.

Die Einwirkung mittels Informationen erschließt einen weiteren physischen Angriffsvektor, die mittels Informationstechnologie betriebene Infrastruktur, deren Steuerung mittels Informationen über den Cyberspace erfolgt. Gayken teilt diese Infrastruktur in drei Gruppen ein: In lokale, nationale und globale Infrastrukturen.⁶⁸⁷ Beim Kampf mit Information sind die Angriffsvektoren nicht im Träger der Information zu sehen, sondern in der Information selbst bzw. mittelbar in der davon abhängigen Infrastruktur.

⁶⁸⁴ Vgl. Nye, 2011, S. 194.

⁶⁸⁵ Gayken, 2011, S. 96.

⁶⁸⁶ Vgl. Kurz/Rieger, 2018, S. 202.

⁶⁸⁷ Vgl. Gayken, 2011, S. 108ff.

Der Kampf um Informationen bietet die Möglichkeit innerhalb bzw. außerhalb des Cyberspace wirksam zu werden. Dies geschieht vorwiegend mit physischen Mitteln, die von juristischer Zwangsgewalt bis hin zur physischen Zerstörung von Teilen des Netzes gehen können.⁶⁸⁸ Es ist beim Kampf um Informationen ein direktes Einwirken auf den Träger der Information gemeint. Dabei gibt es die Möglichkeit beide Kampfformen zu kombinieren, um zum Beispiel, durch den Einsatz von Informationen, einen Informationsträger und dessen Information zu verändern. Das Überschreiben von gespeicherten Daten sei hier beispielhaft genannt.

Ziel dieser Kampfformen ist es, in einem Konflikt die Informationsüberlegenheit, zum Zwecke des Sieges, zu erlangen. Dieser Zweck ist nicht der des Krieges an und für sich, sondern ein ihm untergeordneter Zweck. Um dies darzustellen, sei auf Lilienstern verwiesen, der dazu ausführte:

„Jedem Krieg und jeder Operation liegt ein Wozu und ein Warum, ein Zweck und eine Ursach zum Grunde, denen gemäß der darin ausgeübten Thätigkeit ein gewissen Charakter und eine bestimmte Richtung gegeben wird.“⁶⁸⁹

Der Zweck des Cyberwar kann dem Zweck des Krieges nur von untergeordneter Natur sein. Dies wird damit begründet, dass der Cyberwar, egal welcher Form, eine unterstützende, ermöglichende Funktion für den Krieg selbst darstellt.

„Die einzelnen Operationen haben militärische Zwecke, der Krieg im Ganzen aber hat stets einen politischen Endzweck, [...]. Die Operationen aber dienen bloß dazu, diesen Endzweck des Krieges möglich zu machen. Das was durch die einzelnen Operationen gewonnen wird, ist nicht letzter Zweck an sich, sondern nur Mittel oder Annäherung des Endzweckes.“⁶⁹⁰

Krieg wird, wie dargestellt, dort entscheidend sein, wo der Mensch lebt. Dies ist nicht das Meer, die Luft, der Weltraum oder der Cyberspace, sondern das Land. Daher haben kriegsartige Auseinandersetzungen in den anderen Domänen lediglich unterstützende Wirkung. So formuliert Schmidt Folgendes:

„Egal wie fortschrittlich die Technologie auch sein wird, die Konflikte und Kriege werden immer in der physischen Welt verankert bleiben, in der Menschen über den Einsatz von Maschinen und Cyberstrategien entscheiden.“⁶⁹¹

Daraus folgt, dass auch der Zweck des Cyberwar eine unterstützende Funktion für den Zweck des Krieges darstellt. Betrachtet man die Phasen des Cyberwar, so ergeben sich drei mögliche Ziele beim Krieg im Cyberspace: In

⁶⁸⁸ Vgl. Nye, 2011, S. 195.

⁶⁸⁹ Lilienstern, 1818, S. 8.

⁶⁹⁰ Ebd., S. 8.

⁶⁹¹ Schmidt/Cohen, 2013, S. 312.

Phase eins die Informationsüberlegenheit, in Phase zwei der Wille des Gegners und in Phase drei der Sieg im Kampf im und um das Netz. Betrachtet man diese drei Zielsetzungen, so sind der Wille und der Sieg jene Ziele, die in Verbindung mit den konventionellen Streitkräften erreicht werden. Diese sind also gemeinsam zu erreichen. Im Führungsunterstützungskonzept des ÖBH findet sich folgende Zielsetzung des Cyberwar:

„Ziel des Kampfes in Computernetzwerken ist die Erlangung der Führungsüberlegenheit im Informationsraum.“⁶⁹²

Diese Führungsüberlegenheit, die auf der Informationsüberlegenheit im Informationsraum basiert, kann ausschließlich in diesem erzielt werden und die konventionellen Streitkräfte können hier nur unterstützen. Der Zweck, dem dieses Ziel dient, ist in diesem Konzept,

„[...] das anlassbezogene Setzen von Maßnahmen unter Nutzung von Computern und Computernetzwerken zur Ausnutzung von gegnerischen und fremden Computern, Computernetzwerken und den darauf gespeicherten Informationen sowie zur Einwirkung auf gegnerische Computer, Computernetzwerke und die darauf gespeicherten Informationen.“⁶⁹³

Die Ursache von virtuellen Konflikten und der eigentliche Zweck des Cyberwar sind somit der jederzeitige Zugriff auf Informationen⁶⁹⁴, das jederzeitige Einwirken auf die Systeme des Gegners, als Ergebnis der Erlangung der Informationsüberlegenheit. Es ist dies die Summe von Maßnahmen, die

„[...] auf der Ebene von Information und Informationssystemen darauf abzielt, den Willen und die Entscheidungsfähigkeit der politischen Führung und der Streitkräfte eines Gegners und/oder die Einstellung der Zivilbevölkerung in Einsatzgebieten zu beeinflussen [...]“⁶⁹⁵,

um politische Ziele zu verwirklichen. Der nächste Schritt ist nun, nach einem Exkurs zum Ziel-Zweck-Zusammenhang, darzustellen, welche Akteure im Cyberwar anzutreffen sind und welche Rolle sie dabei einnehmen.

7.2.4 Exkurs: Zum Zusammenhang zwischen Ziel und Zweck bezogen auf die Ebenen der Kriegführung

Das Ziel dient dem Zweck, d.h. der Sieg im Krieg dient dem politischen Zweck, der das Ziel der Politik darstellt und dem übergeordneten Zweck, dem Frieden dient. Dieser ist letztlich der Endzweck eines jeden Konfliktes.

⁶⁹² BMLVS, Operatives Fachkonzept Führungsunterstützung im ÖBH, 2012, S. 41.

⁶⁹³ Ebd., S. 41.

⁶⁹⁴ Anm. d. Verf.: Dabei handelt es sich um eine ständige Zugriffsmöglichkeit, die Verfügungsgewalt, auf die Systeme des Gegners und der darauf enthaltenen Informationen, um diese zu beeinflussen. Dazu zählen die Ausnutzung aber auch die Zerstörung von diesen beiden Ressourcen.

⁶⁹⁵ Center for Security Studies, CSS Analysen zur Sicherheitspolitik: Cyberwar: Konzept, Stand und Grenzen, 2010, S. 2.

Betrachten wir die Aussage Liliensterns, der davon spricht, dass jeder Krieg und jede Operation (Anm. d. Verf.: Damit ist nicht die Operation nach heutigem Verständnis gemeint, sondern vielmehr jede Handlung in einem Krieg.) einen Zweck erfüllen, so lässt sich ableiten, dass dies auch für alle Ebenen der Kriegführung gültig sein muss.

Damit dient also das Ziel – als erstes Ziel auf der untersten, der gefechtstechnischen Ebene – einem Zweck, welcher zugleich das Ziel auf taktischer Ebene darstellt. Es ergibt sich hier ein Zweck-Ziel-Zusammenhang, welcher bis zum Endzweck, der Erreichung eines stabilen Friedens, zu einer stetigen Annäherung, die eine Vervollkommenung bewirkt, führt. Dabei kann unter dem politischen Zweck des Krieges die Erhaltung der Souveränität des Staates verstanden werden.⁶⁹⁶ Auf den Cyberwar übertragen, heißt dies, dass der Zweck desselben zusammenhängt mit dem Ziel des Krieges, dem Sieg über den Gegner.

Im Informationsraum ist der potentielle, ständige Zugriff auf alle relevanten Informationen der Zweck, welcher mittels der Erreichung der Informationsüberlegenheit erzielt wird. Das Besondere am Cyberwar ist, dass er, trotz der Zugehörigkeit zum Kleinen Krieg, das Potential hat, auf politischer Ebene Ziele zu erreichen, indem er auf strategischer Ebene einen Zweck verwirklichen kann. Er tritt damit vor die, einen Krieg entscheidenden, Streitkräfte, ohne aber auf sie verzichten zu können. Wie schon beschrieben braucht es diese, um den Erfolg im Cyberwar glaubhaft zu untermauern.

Letztlich ist der strategische Cyberwar also wieder nur eine Unterstützungsmaßnahme der konventionellen Streitkräfte, nämlich insofern als, dass diese nicht zum Einsatz kommen müssen. Clausewitz hat diesen Zweck-Ziel-Zusammenhang nicht in der Tiefe erkannt, wie sein Zeitgenosse Lilienstern, dennoch ist das Prinzip bei ihm zu finden.

7.3 Zu den Akteuren im Cyberwar

Das Besondere an den Akteuren im Cyberspace stellt die Tatsache dar, dass jeder Nutzer des Cyberspace ein potentieller Akteur im Cyberwar sein kann. Die Akteure repräsentieren die unterschiedlichen Bedrohungsformen, die vom Cyberspace ausgehen. Die Entgrenzung des Cyberspace führt dazu, dass alle, vom privaten Einzelakteur bis hin zu ganzen Staaten, an einem Konflikt im Cyberspace teilnehmen können.⁶⁹⁷ Die Motivationen, die hinter den Handlungen stehen, sind für die Definition der Akteure mitverantwortlich.

Es wird wieder zwischen staatlichen, nichtstaatlichen und internationalen Akteuren unterschieden. Betrachtet man zusätzlich die Bedrohungen, die vom Cyberspace ausgehen, ergibt sich, vor allem bei den nichtstaatlichen Akteuren, eine weitere Unterteilungsmöglichkeit. Die Strategien für die Sicherheit im Netz stellen eine Richtschnur für die staatlichen und internationalen Akteure und deren Agieren im Cyberspace

⁶⁹⁶ Vgl. Strachan, 2008, S. 40.

⁶⁹⁷ Vgl. MOD, Joint Doctrine Publication 01, 2008, Chapter 1, S. 7.

dar, um den Bedrohungen begegnen zu können. Diese Strategien werden in der rechtswissenschaftlichen Untersuchung noch näher beleuchtet. Hier zeigt sich die Herangehensweise der Staaten an die Herausforderung Cyber Sicherheit und den Cyberwar.

Neben den Motiven der Akteure zeigt sich, welche Aufgaben wem zugeordnet sind. Trotz dieser grundlegenden Darstellung der Absichten der Nationalstaaten ist, auf Grund der Entgrenzung, der Sichtbarkeit und der Anonymität, eine klare Identifikation eines Krieges im Netz schwer bis gar nicht möglich. Am ehesten ist der Kleine Cyberwar, als direkter Begleiter klassischer Militäreinsätze, identifizierbar. Doch auch hier ergeben sich bei der Zuweisung – an die Verursacher solcher Kampfhandlungen im Kleinen Cyberwar – Probleme.

Neben dem Staat als Hauptakteur auf der internationalen Bühne, werden immer mehr nichtstaatliche Akteure tätig. Durch die neuen Technologien haben die Bürger Zugriff auf die Macht.⁶⁹⁸ Die Informationsrevolution führt zu einer Perplexität im Hinblick auf die Akteure. Dieser Anstieg an Akteuren führt zu einer steigenden Unsicherheit im Cyberspace und in der realen Welt. Es herrscht eine andauernde Informationsexplosion, in der die Datenbestände im Cyberspace stetig anwachsen. Die zunehmende Vernetzung und die kaum bewältigbare Informationsflut schaffen neue Verwundbarkeiten. Durch diesen Umstand verändert sich das Wesen des Regierens und es kommt zu einer Machtdiffusion.⁶⁹⁹

Informationen sind weit gestreut und können, durch eine Vielzahl an Akteuren, genutzt werden. Zudem begünstigt der Cyberspace eine grenzenlose und globale Kommunikation. Information ist somit ein wesentlicher Machtfaktor. Die Informationsexplosion führt zu einer immer breiter werdenden Machtverteilung. Dies ermöglicht kleinen Staaten an Macht zu gewinnen, während große Staaten dadurch Macht verlieren können. Es ergibt sich eine informatorische Asymmetrie. Moderne Informationstechnologie birgt für kleine Staaten einen Vorteil in sich, während sie für große Staaten die Verwundbarkeit erhöht.⁷⁰⁰ Die Fähigkeit zur Vernetzung führt zur Macht, dabei kommt es nicht auf die modernsten Komponenten an, sondern auf die Fähigkeit, diese zu einem Netzwerk zu verbinden.⁷⁰¹ Dies hat direkten Einfluss auf die Akteure in einem Cyberwar.

7.3.1 Die staatlichen Akteure

Auf Grund der zunehmenden Vernetzung im Governance-Bereich steigt die Anzahl der staatlichen Akteure im Cyberspace. In hochintegrierten Staaten wird die Verwaltung fast ausschließlich über das Netz und die IKT-Infrastruktur abgewickelt. Dies macht einen Großteil der Staatsdiener zu Akteuren im Cyberspace. Diese können nun zu Zielen von Angriffen im Netz,

⁶⁹⁸ Vgl. Nye, 2010, S. 176.

⁶⁹⁹ Vgl. ebd., S. 182.

⁷⁰⁰ Vgl. ebd., S. 181.

⁷⁰¹ Vgl. ebd., S. 182.

bis hin zu Zielen im Cyberwar werden. Da bereits festgestellt wurde, dass der Kleine Cyberwar sich nur gegen militärische Systeme oder Systeme, die direkten Einfluss auf das Militär haben, richtet, sind diese Staatsdiener, die nicht dem Militär angehören, Ziele in einem Großen Cyberwar.

Wer ist nun von staatlicher Seite her der Hauptakteur in einem Großen Cyberwar? Hier kommen nicht, wie beim konventionellen bewaffneten Konflikt, nur zwei Akteure in die engere Wahl. Zum Militär und zur Polizei treten nun vor allem Nachrichten- und Geheimdienste hinzu.⁷⁰² Die Handlungen von Militär und Polizei sind im konventionellen, in der Realität stattfindenden Konflikt einfach zuordenbar. Im einen Fall geht es um Gefahrenabwehr von außen und im anderen Fall um Gefahrenabwehr im Inneren. Weiter präzisiert, einmal um die Wiederherstellung des Ordnungsrahmens und das andere Mal um die Aufrechterhaltung bzw. Bewahrung desselben.

Für die Dienste (Anm. d. Verf.: Synonym verwendet für Nachrichten- wie auch Geheimdienste.) ist der Krieg im Geheimen das Betätigungsfeld schlechthin.⁷⁰³ Es geht vor allem um Überwachung und daraus resultierend um Kontrolle des Cyberspace.⁷⁰⁴ Wie andere staatliche Akteure handeln die Dienste auf der Grundlage von Gesetzen oder sind anders staatlich legitimiert.⁷⁰⁵

„Jeder geheime Nachrichtendienst hat den Auftrag – [...] –, die Staatsführung mit all den geheimen Informationen in ausgewerteter Form zu versorgen, die für die Führung der eigenen Politik von Nutzen und deren Kenntnis für die äußere Sicherheit des eigenen Staates von Bedeutung sind.“⁷⁰⁶

Durch die Natur und das Wesen eines im Verborgenen agierenden Instruments des Staates⁷⁰⁷ und durch die Beschaffenheit des Cyberspace, ist eine umfassende Kontrolle der Handlungen von Diensten nicht gegeben. Der Krieg im Geheimen ist also wie geschaffen für Nachrichtendienste ihre Handlungen auszuführen. Da die meisten solcher Dienste ein Naheverhältnis zum Militär aufweisen, ist einer der Hauptakteure im Großen Cyberwar das Militär.⁷⁰⁸ Da aber viele Handlungen im Großen Cyberwar nicht offensichtlich militärischen Ursprungs sind und vor allem der politische Zweck dabei ebenfalls nicht vordergründig hervortritt, ist auch die Polizei einer der Akteure in dieser Form des Cyberwar.

Die Zuordnung der Führungsverantwortung im Cyberspace ist dabei nicht so einfach zu treffen. Innen und außen sind rein systemisch zu fassen, dass bedeutet ein Angriff auf staatliche IKT-Systeme wäre als ein solcher Angriff von außen zu werten. Hier ist ein möglicher Ansatzpunkt für eine Aufgabenzuordnung, der sich am Ziel orientiert. Doch allein das Ziel kann

⁷⁰² Vgl. Kurz/Rieger, 2018, S. 188.

⁷⁰³ Vgl. Assange/Apfelbaum/Müller-Maguhn, 2013, S. 180ff.

⁷⁰⁴ Vgl. ebd., S. 27ff.

⁷⁰⁵ Vgl. Rosenbach/Stark, 2014, S. 111f.

⁷⁰⁶ Gehlen, Reinhard: Der Dienst, München 1973, S. 185.

⁷⁰⁷ Vgl. ebd., S. 188.

⁷⁰⁸ Vgl. Rosenbach/Stark, 2014, S. 93.

hier nicht entscheidend sein. Die Intention, die hinter einem Angriff steht, muss auch ihre Berücksichtigung finden. Es muss für eine Zuordnung der Kompetenz festgestellt werden, ob es sich um kriminelle oder politische Zwecke handelt, die dem Angriff zu Grunde liegen.

Die Intensität ist ein weiterer Baustein, der die Entscheidung unterstützt, die Einsatzverantwortung festzulegen. Je breiter der Angriff wirkt, je mehr er die eigene Handlungsfähigkeit im Cyberspace einschränkt, umso eher ist er in die Zuständigkeit des Militärs gehörend. Im Falle der CNO ist die Verantwortung eindeutig beim Militär, bei der Cyber Defence im Großen Cyberwar liegt die Zuweisung nicht so klar auf der Hand.

Es sind nicht nur das Ziel, sondern auch der Akteur und seine Intention von Bedeutung. Es muss feststellbar sein, von wo der Angriff kommt, um eine Führungsverantwortung zuweisen zu können. Ähnlich wie bei der Unterscheidung von innen und außen, muss ein systemischer Ansatz miteinbezogen werden. Es ist also etwas dem System zugehörig, also innen oder eben nicht, also außen. So können, wie bereits beschrieben, Gefahren im territorialen Innen eine systemische Bedrohung von außen darstellen. Umgekehrt kann eine Bedrohung territorial außen liegen, aber systemisch innen wirken. Gerade diese Unterscheidung macht das Handeln der staatlichen Akteure kompliziert.

Gesetzliche Regelungen eines Staates haben keinen Anspruch auf Durchsetzung in einem anderen Staat. Ist der Angreifer zwar im System, der Teil des Systems aber nicht auf dem Territorium des angegriffenen Staates, dann können die Träger des Gewaltmonopols nicht tätig werden. Das heißt, abgesehen von der Zuständigkeit, ergibt sich ein weiteres Problem, das der Territorialität. Da die Organe der Staatsgewalt auf Grundlage der Gesetze tätig werden, können sie dies nur dort tun, wo diese Gesetze wirken. Dieser Raum ist das eigene Staatsgebiet.

Für die staatlichen Akteure im Cyberwar ist also entscheidend, was angegriffen wird, welche Intensität der Angriff aufweist und wer ihn mit welchem Zweck ausführt. Im Kleinen Cyberwar ist die Verantwortung und somit der Hauptakteur im Militär zu finden. Hier handelt es sich um direkte Angriffe auf militärische Systeme. Beim Großen Cyberwar sind die staatlichen Akteure weit gestreut. Neben dem Militär und der Polizei treten vor allem die Dienste in Aktion. Sie nutzen das Netz, um durch Überwachung Kontrolle zu ermöglichen.

Ein hoher Vernetzungsgrad ist für diese staatlichen Akteure von großer Bedeutung, um diese Kontrolle zu erlangen. Kontrolle führt damit zu einem, aus ihrer Sicht, höheren Maß an Sicherheit⁷⁰⁹, indem man Dinge von Wichtigkeit, über potentielle oder wahrhaftige Gegner, in Erfahrung bringt.

„Der Erste Weltkrieg hatte gezeigt, daß der geheimen Nachrichtengewinnung im Zeitalter der alle Bereiche des gesellschaftlichen Lebens umfassenden Kriegführung, [...], eine im

⁷⁰⁹ Anm. d. Verf.: Hier ist eine Analogie zur Medizin zu sehen. Um sich zu immunisieren, verabreicht man sich den Erreger selbst.

Vergleich zu früher noch erhöhte Bedeutung zukam. Es genügte jedenfalls nicht mehr, vornehmlich militärische Geheimnisse auszuspähen. Die Beschaffung rechtzeitiger Erkenntnisse über die Außenpolitik des Gegners, das Wirtschaftspotential, sowie auch über die psychopolitische Lage, d.h. also über den Durchhaltewillen, sowie über andere politische Vorkommnisse wurden im Vergleich zu früheren Zeiten immer interessanter.“⁷¹⁰

Dafür eröffnet der Cyberspace den Diensten von heute ungeahnte Möglichkeiten. Dabei geht es vordergründig um die Früherkennung von möglichen neuen Konflikten. Neben der Aufbereitung von Daten für die Staatsführung,⁷¹¹ können Angriffe, auf potentielle Zielsysteme, bereits in der Beobachtungsphase angelegt werden. Diese sind dann bei Ausbruch eines Konfliktes einfach abzurufen.

Betrachtet man das Konzept des Cyberwar, so ist das Schwergewicht, der Methoden des Großen Cyberwar und somit der Einsatz von Diensten, vor allem in Phase eins zu finden. Wendet man den Blick auf die Intensitätsstufen, so muss man berücksichtigen, dass die vorhergehenden Stufen in der nächst höheren immer enthalten sein können. Gemeinsam ist allen staatlichen Akteuren in einem Cyberwar, dass sie nicht oder nur schwer, auf Grund ihrer Tätigkeit, voneinander zu unterscheiden sind. Ob eine Aktion durch die Polizei, das Militär oder einen Nachrichtendienst durchgeführt wurde, ist für Außenstehende nicht offensichtlich. Die Grenzen zwischen deren Einsatz und Handeln sind fließend. Dies zeigt sich besonders eindeutig bei der National Security Agency und dem Cybercommand der Armee der Vereinigten Staaten von Amerika:

„Diese Militäreinheit ist für die Kriegführung im Internet zuständig, und seit ein paar Jahren ist der NSA-Direktor auch Chef des Cybercommands – ein Schritt, der die Grenzen zwischen Geheimdienst und Armee im Netz faktisch aufgehoben hat.“⁷¹²

Weitere Gemeinsamkeiten der staatlichen Akteure sind ihre Legitimierung durch den Staat und dass sie vom Gemeinwesen getroffene Entscheidungen umsetzen. Diese Merkmale treffen auf die staatlichen Akteure im konventionellen Krieg auch zu. Allein die nicht offensichtliche Unterscheidbarkeit, welche dem Cyberspace immanent ist, kommt im konventionellen Krieg so nicht zum Tragen. In dieser Eigenschaft decken sich staatliche mit den nichtstaatlichen Akteuren im Cyberspace.

7.3.2 Die nichtstaatlichen Akteure

Noch mehr als in den realen bewaffneten Konflikten, kommt den nichtstaatlichen Akteuren im Cyberwar eine bedeutende Rolle zu. Es ist von vornherein nicht eindeutig feststellbar, ob ein Akteur nun staatlich legitimiert

⁷¹⁰ Gehlen, 1973, S.184.

⁷¹¹ Vgl. ebd., S. 185f.

⁷¹² Rosenbach/Stark, 2014, S. 93.

ist oder nicht.⁷¹³ Informationen tragen keine Uniform und sind auch sonst nur schwer zuordenbar. Bei den nichtstaatlichen Akteuren, im Cyberspace und im Speziellen im Cyberwar, sind verschiedene Kategorien zu unterscheiden. Je nach Art des Konfliktes und der Ziele, die damit verfolgt werden, kann eine grobe Einteilung in vier Gruppen erfolgen.

Die erste Gruppe sind individuelle Akteure, die unterschiedliche Zielsetzungen verfolgen können. Dazu zählen in erster Linie kriminelle Motive. Bei dieser Gruppe von Tätern steht vor allem die persönliche Bereicherung im Fokus. Dabei spielt oft die Erlangung von Einfluss oder Anerkennung, noch vor dem materiellen Gewinn, die wesentliche Rolle.⁷¹⁴ Dazu zählen neben Akteuren, die aus reiner Lust und Laune heraus Schäden im Netz verursachen, auch Personen, die Schadsoftware herstellen und anbieten. Ebenfalls gehören Netzaktivisten oder Hacktivist*innen zu dieser Gruppe von nichtstaatlichen Akteuren. Diese Gruppe der individuellen Akteure ist in allen Formen des Cyberwar einsetzbar.

Als Beispiel sind die beiden Vorfälle in Estland und Georgien zu nennen, bei denen man patriotische Hacker offiziell als Urheber der Cyber Angriffe bezeichnet. Vor allem in Georgien hat das Zusammenwirken, von angeheuerten oder zur Mitwirkung animierten Akteuren, mit dem Einsatz konventioneller Streitkräfte, eine neue Qualität des bewaffneten Konfliktes eingeläutet. Da diese Personen aber nur über begrenzte Ressourcen verfügen, ist die Wahrscheinlichkeit, dass deren Attacken erkannt werden, als sehr hoch einzustufen. Eine Mitwirkung dieser Gruppierungen an einem Großen Cyberwar ist zwar möglich, aber eher unwahrscheinlich. Gerade Hacktivist*innen suchen die Öffentlichkeit, um ihre Ziele zu erreichen.⁷¹⁵ Diese Aktionen sind daher auf der Eskalationsleiter bzw. der Intensitätsskala weit unten angesiedelt.

Die zweite Gruppe von nichtstaatlichen Akteuren sind Wirtschaftsunternehmen. Diese spielen im Cyberspace eine gewichtige Rolle. Wirtschaft und Macht sind eng miteinander verwoben und der ständige Wettbewerb zwischen den Unternehmen bringt es mit sich, Wettbewerbsvorteile zu generieren.⁷¹⁶ Aber auch als potentielle Angriffsziele in einem Großen Cyberwar, sind die Unternehmen von Bedeutung. Das heißt vielfach, dass die Spionage die Hauptangriffsform von Akteuren, die im wirtschaftlichen Bereich des Cyberwar tätig sind, ist. Die Palette reicht von einfachen Kriminellen bis hin zu Staaten, die Wirtschaftsunternehmen ausspionieren. Diese Art von Cyberwar, von Staaten durchgeführt, bezeichnet Gayken als Economic Operations.⁷¹⁷

Wirtschaftsunternehmen bieten ihre Dienstleistungen auch im Bereich der Cyber Kapazitäten an, in dem sie ihre Expertise für Kunden, vorzugsweise Staaten, offerieren und diesen ermöglichen, verstärkte Kontrolle im Netz auszuüben. Dies ist die legale Form der Teilnahme von

⁷¹³ Vgl. Hofstetter, 2019, S. 184.

⁷¹⁴ Vgl. Olson, 2012, S. 36.

⁷¹⁵ Vgl. Assange/Apfelbaum/Müller-Maguhn, 2013, S. 19.

⁷¹⁶ Vgl. ebd., S. 57.

⁷¹⁷ Vgl. Gayken, 2012, S. 103ff.

Unternehmen an Aktivitäten im Cyberwar. Als Beispiel seien hier Google oder Facebook genannt, die es den Behörden der Vereinigten Staaten ermöglichen, auf deren Datenbestände zuzugreifen.⁷¹⁸ Dabei nehmen diese Unternehmen in einem Cyberwar eine ähnliche Rolle ein, wie private Militärunternehmen, Private Military Companies (PMC).

Ein weiterer Aspekt ist, dass große Konzerne ihre Kapazitäten im Cyberspace dazu verwenden, um andere Firmen in einen Wettbewerbsnachteil zu versetzen. Diese Fähigkeiten können allerdings nur großen Konzernen zugetraut werden.⁷¹⁹ Diese Angriffe zielen auf den Bereich der Wirtschaftspolitik eines Gemeinwesens ab. Die Konzerne sind aber nicht nur nichtstaatliche Akteure, sondern oft auch transnationale Akteure in einem Cyberwar. Dies trifft speziell auch auf die dritte Gruppe von nichtstaatlichen Akteuren zu, die Cyber Terroristen.

Der Terrorismus im Netz betrifft vor allem die unentdeckte Koordinierung, Rekrutierung und Ausbildung.⁷²⁰ Aktionen aus dem Cyberspace, die einem terroristischen Anschlag gleichkommen, sind potentiell möglich. Viele kritische Infrastrukturen sind über das Netz zugänglich und können, ähnlich wie bei Stuxnet, auch von Terroristen bewirkt werden. Dass solch ein Angriff noch nicht stattgefunden hat, reduziert keinesfalls das hohe Risiko, das von einer solchen Attacke ausgeht. Dabei sind die Terroristen wohl, in der Vorbereitung auf solche Angriffe, bemüht unentdeckt zu bleiben, ihre Aktionen selbst brauchen hingegen eine breite öffentliche Wirksamkeit.⁷²¹ Anders als beim Krieg im Geheimen ist, aus Sicht der Terroristen, die Wahrnehmbarkeit Kriterium für den Erfolg.

Die vierte Gruppe an nichtstaatlichen Akteuren ist ebenfalls oft über die Grenzen von Staaten hinaus agierend. Es handelt sich um die Organisierte Kriminalität (OK), welche sich auch im Cyberspace manifestiert.⁷²² Bekannt geworden sind in diesem Zusammenhang vor allem Delikte, die sich mit Kreditkartenbetrug beschäftigen. Diese Angriffe können im Zuge eines Cyberwar natürlich zum Tragen kommen, sind dort aber eher Begleiterscheinung denn eigentliche Ursache oder Ziel vom Krieg im Netz. Die Motivation, die hinter diesen Angriffen steht, ist eine typisch ausnutzende und den Cyberspace nicht schwächende Angriffsform. Es gibt auch Gruppierungen der OK, wie zum Beispiel das Russian Business Network (RBN), welches im Verdacht steht an den Cyber Angriffen in Estland und Georgien maßgeblich beteiligt gewesen zu sein.

Neben diesen vier nichtstaatlichen Akteuren, die, zum Teil auf Grund der Beschaffenheit des Cyberspace, auch über territoriale Grenzen hinweg agieren können, gibt es noch die internationalen Akteure im Cyberwar.

⁷¹⁸ Vgl. Assange / Apfelbaum / Müller-Maguhn, 2013, S. 61.

⁷¹⁹ Vgl. Andress / Winterfeld, 2011, S. 198.

⁷²⁰ Vgl. Nye, 2011, S. 186.

⁷²¹ Vgl. Freudenberg, 2008, S. 81.

⁷²² Vgl. Glenny, 2012, S. 57ff.

7.3.3 Die internationalen und transnationalen Akteure

Da grundsätzlich alle Akteure auch international bzw. transnational agieren können, behandelt dieser Abschnitt vor allem internationale Organisationen, Bündnisse und Staatengemeinschaften. Diese werden vor allem hinsichtlich der Maßnahmen, welche sie im Zuge der Erhöhung der Sicherheit des Cyberspace wahrnehmen, analysiert. Die übrigen internationalen und transnationalen Akteure werden, da sie zum Teil auch bei den Akteuren im (konventionellen) Krieg behandelt wurden, nicht mehr näher untersucht. Die Analyse wird exemplarisch anhand der NATO der EU und den VN durchgeführt.

Die Rolle, die internationale Akteure im Rahmen eines Krieges im Netz spielen, ist etwas anders gelagert als beim konventionellen internationalen bewaffneten Konflikt. Durch die Beschaffenheit des Cyberspace und die Bedrohungen, die daraus erwachsen, ist eine Kooperation bei der Bewältigung von kriegerischen Auseinandersetzungen, nicht nur national, sondern auch international angezeigt. Durch den Faktor der Entgrenzung und der systemischen Teilung von Sicherheit, in innen und außen, wird die Bewältigung von Gefahren aus dem Netz auf eine internationale Ebene gehoben.

Neben der nationalen Cyber Sicherheit ist vor allem die globale Cyber Sicherheit im Fokus der internationalen Organisationen. Dabei wird diese Sicherheit durch gemeinsame Maßnahmen, das heißt mittels Steigerung der Macht durch Zusammenschluss, zu erreichen versucht. Es können hier im Wesentlichen folgende Bedrohungen identifiziert werden, an welchen sich die Konzepte der internationalen Organisationen ausrichten: Die Cyber Kriminalität, der Cyber Terrorismus und der Cyberwar, aus welchen sich die Dimensionen der Sicherheit im Cyberspace ableiten lassen. Die Regelungen und Maßnahmen der Organisationen beziehen sich in erster Linie auf die vordergründig häufigsten Bedrohungen im Netz.

Interessant erscheint, dass der jeweilige Fokus dabei nicht auf dieselben Bedrohungen gerichtet ist. Die NATO erfasst in ihrem strategischen Konzept verschiedene Akteure als potentielle Gefahr im Cyberspace und sieht im Falle einer Cyber Attacke auch die Auslösung des Bündnisfalles nach Artikel 5 angezeigt.⁷²³

„NATO members will always assist each other against attack, in accordance with Article 5 of the Washington Treaty. That commitment remains firm and binding. NATO will deter and defend against any threat of aggression, and against emerging security challenges where they threaten the fundamental security of individual Allies or the Alliance as a whole.“⁷²⁴

Dazu wird im strategischen Konzept von 2010 weiter ausgeführt, dass die NATO:

⁷²³ Vgl. Klimburg, 2012, S. 181ff.

⁷²⁴ NATO, Strategic Concept, 2010, S. 7.

„[...] develop further our ability to prevent, detect, defend against and recover from cyberattacks, including by using the NATO planning process to enhance and coordinate national cyber-defence capabilities, bringing all NATO bodies under centralized cyber protection, and better integrating NATO cyber awareness, warning and response with member nations; [...]”⁷²⁵

Die Koordinierung der nationalen Cyber Defence Kapazitäten und der Eigenschutz der NATO-Einrichtungen sind hier explizit Ziel der Anstrengungen der NATO im Cyberspace. Die NATO priorisiert diese Maßnahmen nach folgenden Bedrohungen:

„Foreign militaries and intelligence services, organised criminals, terrorist and/or extremist groups can each be the source of such attacks.“⁷²⁶

Trotz der Erwähnung der Organisierten Kriminalität, ist die Ausrichtung an kriegesischen Bedrohungen zu erkennen. In der NATO Cyber Defence Policy ist das Ziel, in allen Missionen der NATO, Cyber Defence zu integrieren.⁷²⁷ Hier ist die ursprüngliche Orientierung der NATO, als Verteidigungsbündnis, klar erkennbar.

Die EU führt in ihrer Cyber Security Strategie fünf Wege an, um die Sicherheit im Cyberspace zu erzielen.⁷²⁸ Darunter fällt die Entwicklung einer Cyber Defence Policy und der entsprechenden Fähigkeiten, um diese umzusetzen. Der Ansatz, der dabei gewählt wird, liegt, auf Grund der vielfältigen Bedrohungen und Akteure, in einem zivil-militärischen Zugang.⁷²⁹ Die europäische Cyber Sicherheitsstrategie orientiert sich an folgenden Maßnahmen:

„Bei den Cybersicherheitsmaßnahmen in der EU wird auch der Aspekt der Cyberverteidigung berücksichtigt. Um die Robustheit der Kommunikations- und Informationssysteme zu erhöhen, die dem Schutz der Verteidigungs- und Sicherheitsinteressen der Mitgliedstaaten dienen, sollte der Schwerpunkt bei der Entwicklung der Cyberverteidigungskapazitäten auf der Erkennung komplexer Cyberbedrohungen, der Reaktion darauf und der Wiederherstellung danach liegen.“⁷³⁰

Damit hat die, bisher sehr auf Cyber Kriminalität ausgerichtete, Herangehensweise der EU (Anm. d. Verf.: Hier ist vor allem die Cyber Crime Convention⁷³¹ des Europarates hervorzuheben.) den Cyberwar als Handlungsfeld zur Erhaltung der Cyber Sicherheit erkannt. Ausdruck findet

⁷²⁵ Ebd., S. 16f.

⁷²⁶ Ebd., S. 11.

⁷²⁷ Vgl. NATO, Defending the networks, The NATO Policy on Cyber Defence, 2011, S. 1.

⁷²⁸ Vgl. Europäische Kommission, Cybersicherheitsstrategie der Europäischen Union, 2013, S. 5ff.

⁷²⁹ Vgl. ebd., S. 13.

⁷³⁰ Ebd., S. 13.

⁷³¹ Vgl. <https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/090000168008157a>, [12.05.2020].

diese Neuausrichtung in den militärischen Konzepten der EU. Im Bereich der Cyber Defence⁷³² und der CNO⁷³³ liegen zwei Konzepte für die Durchführung von EU geführten Militärmissionen vor. Hier spiegelt sich in den Konzepten allerdings nur das Vorgehen im Rahmen des Kleinen Cyberwar wider, während die Formulierung im obigen Zitat auch auf den Großen Cyberwar angewandt werden kann.

Sowohl die NATO als auch die EU sehen, auf Grund der vielen möglichen Angriffsvektoren, die Aufgabe einer Cyber Defence in einem gemeinsamen Vorgehen aller Mitgliedsstaaten. Eine zivil-militärische Zusammenarbeit ist die logische Konsequenz daraus. Denn in einem Cyberwar ist nicht das Militär der ausschließliche Akteur. Wie bereits im vorigen Abschnitt gezeigt, gibt es eine Vielzahl an potentiellen Mitwirkenden in einem Cyberwar. Dem tragen die strategischen Ausrichtungen der NATO und der EU Rechnung.

Die Vereinten Nationen sind der dritte internationale Akteur, der hier zu untersuchen ist. Die VN haben die Verbindung zwischen internationaler Sicherheit und der Entwicklung auf dem technischen Sektor erkannt und in einer Resolution dieser Verbindung Rechnung getragen. Darin wird festgehalten, dass

„[...] the dissemination and use of information technologies and means affect the interests of the entire international community and that optimum effectiveness is enhanced by broad international cooperation, [...].“⁷³⁴

Dabei ist es das Ziel der VN den Gefahren, die sich aus der Nutzung der Informationstechnologie ergeben, mittels eines multilateralen Ansatzes zu begegnen. Es geht in dieser Resolution nicht nur um Cyber Crime und Terrorismus im Cyberspace, sondern auch um den Krieg im Netz. Dies zeigt sich an der Aussage, dass

„[...] these technologies and means can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the security of States, [...].“⁷³⁵

Auch bezogen auf die Nutzung des Cyberspace ist es das Ziel der VN, den Weltfrieden und die internationale Sicherheit zu wahren. Da die Entgrenzung des Cyberspace eine Entgrenzung des Cyberwar mit sich bringt, spielen internationale Akteure in diesem Feld der Kriegführung eine bedeutende Rolle. Die NATO und die EU suchen einen gemeinschaftlichen Lösungsansatz, mit ihren Mitgliedsstaaten, um, ähnlich der Lösungsansätze auf nationalstaatlicher Ebene, in einem Comprehensive Approach den Gefahren aus dem Netz entgegentreten. Es spielt gerade die unklare

⁷³² Vgl. EUMS, EU Concept for Cyber Defence for EU-led Military Operations, 2012.

⁷³³ Vgl. EUMS, EU Concept for Computer Network Operations in EU-led Military Operations, 2009.

⁷³⁴ United Nations, General Assembly, Resolution 53/70, 1999, S. 2.

⁷³⁵ Ebd., S. 2.

Akteurslage eine wesentliche Rolle, um militärische und zivile Kapazitäten gemeinsam einzusetzen.

Die VN sieht vor allem in der Schaffung eines rechtlichen Rahmens ihren Beitrag zur internationalen Sicherheit im Cyberspace. Dies äußert sich bereits in der General Assembly Resolution 53/70, wenn hier von

„[...] developing international principles that would enhance the security of global information and telecommunications systems and help to combat information terrorism and criminality;“⁷³⁶

gesprochen wird. Die drei exemplarisch angeführten internationalen Akteure sind sich ihrer Rolle im Cyberwar bewusst und haben dies auch in diversen Dokumenten festgeschrieben. Die internationale Sicherheit im Cyberspace ist abhängig von diesen Akteuren, die wiederum auf der Wahrnehmung der Cyber Sicherheit ihrer Mitgliedsstaaten beruht. Die Rolle der Staaten im Cyberwar, als Träger der internationalen Akteure, spiegelt sich in nationalen Cyber Sicherheitsstrategien, welche in der rechtswissenschaftlichen Untersuchung zum Teil vorgestellt werden, wider.

7.4 Zum Wesen des Cyberwar

Grundsätzlich treten im Cyberwar einander Gemeinwesen oder Teile davon in einem virtuellen bewaffneten Konflikt gegenüber, dennoch ist, wie gezeigt wurde, die Teilnahme vieler verschiedener Akteure an einem solchen Krieg möglich.

„Im Cyberspace tobt ein körperloser Kampf zwischen den bösen und den guten Jungs, bei dem die eine Seite raubend und plündernd durch das Internet zieht, während die andere versucht, sie daran zu hindern.“⁷³⁷

Da er seinem Wesen nach dem Kleinen Krieg zuzuordnen ist, bleibt er einerseits eine Unterstützungsmaßnahme, für einen konventionellen bewaffneten Konflikt, und andererseits eine asymmetrische Kriegsform. Die Besonderheit im Falle eines Krieges im Netz ist, dass so viele verschiedene Akteure daran partizipieren können. Dabei sind Intention und Intensität – neben den Akteuren – die Beurteilungskriterien, ob es sich letztlich um einen Krieg im Netz handelt.

7.4.1 Die Einordnung des Cyberwar als Moment des Krieges

Der Große Krieg ist ein bewaffneter Konflikt zwischen Staaten, der durch deren militärische Streitkräfte ausgetragen wird. Der Kleine Krieg hingegen involviert auch nichtstaatliche Akteure. Der Große Krieg beruht auf Symmetrie zwischen den Akteuren, d.h. auf gegenseitiger Anerkennung als Gegner im Konflikt. Auch zählen Ausbildung, Bewaffnung und Methoden der

⁷³⁶ Ebd., S. 2.

⁷³⁷ Bowden, 2012, S. 20.

Kriegführung zu dieser Symmetrie. Der Kleine Krieg ist von asymmetrischer Natur und zumindest eine der Konfliktparteien nutzt Verfahren, die den Gegner in eine nachteilige Position bringen. Es handelt sich um keinen offenen Kampf, sondern um einen verdeckt geführten Krieg eines, an physischer Stärke unterlegenen, Akteurs gegen einen überlegenen Feind.

Dieser Krieg kann als Begleiter eines Großen Krieges auftreten, dann hat diese Form des Krieges einen unterstützenden Charakter, ähnlich wie der Einsatz der Luft- und Seestreitkräfte.⁷³⁸ Der Unterschied ist nur der, dass diese, auf Grund der Waffensysteme, deren Komplexität und Kosten, nur von militärischen Streitkräften der Gemeinwesen betrieben werden können. Der Kleine Krieg wird jedoch mit Waffen ausgetragen, welche von einfacher und günstiger Art sind. Somit ist in diesem Krieg der Akteursbegriff weiter zu fassen. Der Angreifer ist dem Verteidiger in der Wahl des Angriffszieles überlegen, er bestimmt Ort und Zeit des Angriffs.

Im Cyberwar haben wir genau dieselben bestimmenden Parameter. Er geschieht im Verborgenen, er ist in der Regel ein Krieg im Geheimen. In ihm kommen eine Vielzahl von Akteuren zum Tragen, er bevorteilt den Angreifer gegenüber dem Verteidiger und hat für den konventionellen Krieg einen unterstützenden Charakter. Zum Einsatz der Kleinkriegskräfte führt Clausewitz aus: „Ihre Gefechte sind fast alle auf Unterstützung berechnet.“⁷³⁹ Der Kleine Krieg wie auch der Cyberwar können selbstständig geführt werden, benötigen aber für eine Entscheidung konventionelle Streitkräfte. Das Ziel des verdeckten Krieges ist,

„[...] in unserem Hinterland Unordnung und Verwirrung zu stiften, und das sowohl als selbstständige Aggressionshandlung als auch zur Vorbereitung und als Nebenhandlung in anderen Arten des Krieges.“⁷⁴⁰

Politische Zielsetzungen sind zwar durch diese Form des Krieges erreichbar, aber nur durch den Einsatz oder die Verfügbarkeit von militärischen Streitkräften auch durchsetzbar. Bei Galula ist die Transformation einer Kleinkriegsarmee in eine reguläre Streitkraft, im Rahmen eines Aufstandes, Bedingung zum dauernden Erfolg. Während der Große Krieg einen Zweikampf zwischen Staaten, geführt durch deren Streitkräfte, darstellt, hat der Kleine Krieg und somit auch der Cyberwar, einen totaleren Charakter.

Diese Form des Krieges betrifft nicht nur das Militär⁷⁴¹ und damit nur diesen einen Politikbereich eines Gemeinwesens, sondern kann alle Bereiche

⁷³⁸ Vgl. Hahlweg, 1968, S. 15.

⁷³⁹ Clausewitz, Carl von: Meine Vorlesungen über den kleinen Krieg. In: Hahlweg, Werner: Lehrmeister des Kleinen Krieges. von Clausewitz bis Mao Tse-Tung und (Che) Guevara, Darmstadt 1968, S. 49.

⁷⁴⁰ Riedel, Siegfried: Vorwort zur deutschen Übersetzung der Militärstrategie von Sokolowski. In: Hahlweg, Werner: Lehrmeister des Kleinen Krieges. Von Clausewitz bis Mao Tse-Tung und (Che) Guevara, Darmstadt 1968, S. 15.

⁷⁴¹ Anm. d. Verf.: Die Luftwaffe hat zum Beispiel die Möglichkeit strategisch zu wirken und kann dadurch andere Bereiche des Gemeinwesens, nicht nur das Militär, beeinflussen.

eines Gemeinwesens betreffen. Durch Hahlweg wird diese Eigenschaft als Form

„[...] des totalen Kampfes aus dem zivilen, politisch-sozialen Raum für den zivilen, politisch-sozialen Raum, [...]“⁷⁴²

gefasst.

Da sich der Cyberwar der Wahrnehmung weitgehend entzieht, kann er als ein verdeckter Kampf, im Sinne des Kleinen Krieges, erkannt werden. Damit ist er eine Form eines, schon immer und über alle Zeiten aufgetretenen, Krieges,⁷⁴³ der durch die Französische Revolution nochmals totalisiert wurde. Das gesamte Gemeinwesen wurde zum Zwecke des Krieges mobilisiert. Die Intensität war dementsprechend hoch und damit wurde das Volk, neben dem Militär, zum Hauptakteur.

Ist die Intensität auf einem niedrigen Niveau, so ist, auf Grund der zivilen Akteure, die Zuständigkeit zur Aufrechterhaltung der Sicherheit und Ordnung im öffentlichen Leben eine polizeiliche Aufgabe. Ist die Intensität jedoch so hoch, dass nicht nur die Anzahl der Akteure entsprechend vielfältig ist, sondern ist die Sicherheit und Ordnung beseitigt, dann fehlt der Ordnungsrahmen, welchen die Polizei benötigt, um handeln zu können. Dann geht es um die Souveränität des Gemeinwesens und es muss das Instrument des Staates zum Einsatz kommen, welches zum Schutz derselben vorgesehen ist, das Militär.

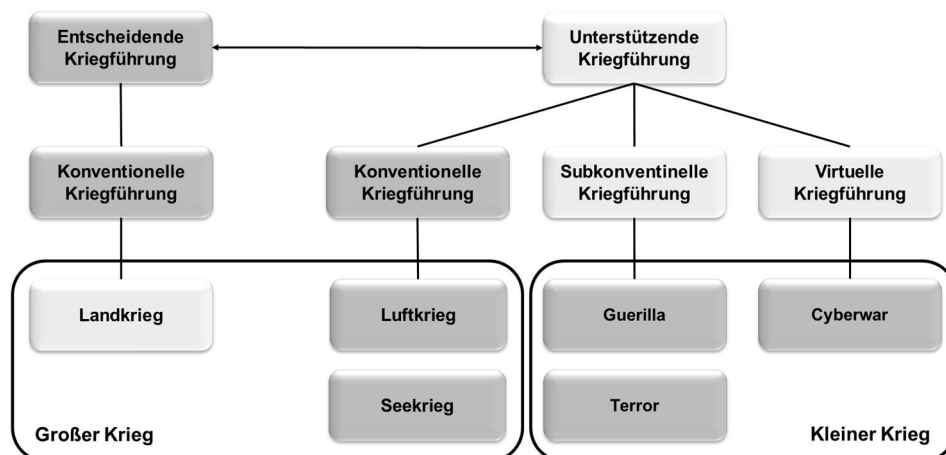


Abbildung 15: Einordnung des Cyberwar in den Kriegsbegriff⁷⁴⁴

In diesem Zusammenhang ist die Unterscheidung von innen und außen nochmals anzusprechen. Da der Kleine Krieg in der Regel im Inneren eines Gemeinwesens geführt wird, ist die Zuteilung der Verantwortung nicht auf diese Unterscheidung zurückführbar. Ähnlich verhält es sich mit dem Cyberwar, der total entterritorialisiert ist. Hier kann die Verantwortung nur

⁷⁴² Hahlweg, 1968, S. 7.

⁷⁴³ Vgl. ebd., S. 10.

⁷⁴⁴ Abbildung durch den Verfasser erstellt. Anm. d. Verf.: Da im Weltraum eine Kriegführung noch nicht wahrscheinlich ist, wird diese Domäne nicht angeführt.

systemisch festgelegt werden. Eine Loslösung vom Territorialdenken ist im Cyberspace ein möglicher Zugang, um Zuständigkeiten festzulegen. Systeme sind funktional zu erfassen und bestimmten Akteuren zuordenbar.

Als Moment des Krieges ist der Cyberwar als Kleiner Krieg des virtuellen Typus zu charakterisieren. Er steht damit neben den anderen Formen des Kleinen Krieges, die sich der subkonventionellen Kriegführung bedienen. Diese Formen des Krieges sind Unterkategorien der unterstützenden Kriegführung, zu der auch der See- und der Luftkrieg als Formen der konventionellen Kriegführung zählen.

Zum Vorteil des Angreifers gegenüber dem Verteidiger ist eine Analogie zur Luftwaffe angebracht. Douhet fasst den Vorteil des Angriffs folgendermaßen:

„Dank seiner Unabhängigkeit von der Erdoberfläche und seiner überlegenen Geschwindigkeit ist das Flugzeug die ideale Angriffswaffe. Der größte Vorteil der Angriffstaktik ist die Initiative in der Einleitung der Operationen, welche durch freie Wahl des Angriffspunktes die Möglichkeit frei gibt, die Masse der eigenen Streitkräfte zweckmässig zusammenzuziehen und einheitlich anzusetzen, während der in die Defensive gedrängte Gegner, im unklaren über Angriffspunkt und Stoßrichtung, gezwungen ist, seine Streitkräfte auf alle angreifbaren Punkte zu verteilen, um sie später in die sich klärende Stoßrichtung des Gegners zu werfen, falls es ihm gelingt, die Absichten des Angreifers rechtzeitig zu erkennen.“⁷⁴⁵

In dieser Aussage finden sich die wesentlichen Eigenschaften des Cyberwar wieder. Die Losgelöstheit von der Erdoberfläche, im Sinne der Losgelöstheit vom euklidischen Raum, die freie Wahl des Angriffspunktes, die Schwierigkeit der Defensive und die eingeschränkte Wahrnehmbarkeit eines Cyber Angriffes werden hier genannt. Im Gegensatz zur Luftwaffe stehen die Möglichkeiten der virtuellen Kriegführung nicht nur Staaten zur Verfügung. Seinem Wesen nach ist der Cyberwar ein Kleiner Krieg. Cyberwar ist Teil des Krieges, jedoch ist er nicht der Krieg an und für sich. Damit ist die Zuständigkeit und Führungsverantwortung abhängig von verschiedenen Parametern, darunter vor allem vom Grad der Intensität. Um das Wesen und die Natur des Cyberwar nun weiter zu analysieren, ist die Abgrenzung zum Großen Krieg angezeigt.

7.4.2 Die Abgrenzung des Cyberwar zum konventionellen Großen Krieg

Der symmetrische Große Krieg, welcher auch als gehegter Krieg bezeichnet wird, da er sich auf die militärischen Streitkräfte von Gemeinwesen bezieht und dadurch auch den internationalen rechtlichen Normen unterliegt, ist durch fünf Grundsätze kategorisiert, die Haffner in einem Essay zusammenfasst.⁷⁴⁶ Die Abgrenzung des Cyberwar zum Großen Krieg wird über diese Grundsätze geführt.

⁷⁴⁵ Douhet, 1935, S. 19.

⁷⁴⁶ Vgl. Haffner, 1966, S. 15f. (in: Tse-tung, 1966)

Disziplin der Streitkräfte ist der erste Grundsatz, welcher bezüglich des Cyberwar zu untersuchen ist. Komplexität der Waffensysteme und das Zusammenwirken dieser am Gefechtsfeld erfordert eine auf Befehl und Gehorsam abgestützte Armee.⁷⁴⁷ Um die Effizienz aufrecht zu erhalten und die Wirkung auf den Gegner zu erzielen, ist ein koordiniertes und aufeinander abgestimmtes Agieren von großer Bedeutung. Eine gewisse Disziplin ist zwar im Cyberwar notwendig, um Attacken genau dort zu platzieren, wo deren Wirkung auch erwünscht ist, oder um das Agieren im Geheimen nicht öffentlich zu machen, jedoch ist Kreativität und Experimentierfreude von noch größerer Bedeutung. Schwachstellen zu finden, sie auszunutzen und Waffen zu fertigen, die eine gezielte Wirkung ermöglichen, stehen im Vordergrund. Vielfach ist derjenige, welcher die Waffe herstellt, auch derjenige, der sie zum Einsatz bringt. Die spezifische Charakteristik von Schwachstellen, die für Angriffe genutzt werden können, erfordert eine andere Art von Disziplin.

Der zweite Grundsatz betrifft die Einteilung der Akteure im Krieg. Stehen sich im Großen Krieg Kombattanten als Kämpfer gegenüber,⁷⁴⁸ ist die Unterscheidung zwischen Kombattant und Nicht-Kombattant im Cyberspace nicht möglich. Eine Begrenzung der Kampfhandlungen auf die kämpfende Truppe ist daher im Cyberwar nicht gegeben. Hier offenbart sich die totale Eigenart des Cyberwar. Er ist hinsichtlich der Akteure entgrenzt. Dies bedeutet die Auflösung zwischen kriegführenden Streitkräften und der nicht am Kampf beteiligten Zivilbevölkerung. Damit wird gegen die völkerrechtlichen Bestimmungen gehandelt, da die Kampfhandlungen von und gegen Zivilisten geführt werden.⁷⁴⁹ Der Cyberwar ist, wie der Kleine Krieg, hinsichtlich der rechtlichen Regelung desselben entgrenzt. Bei aller Entgrenzung wird der Cyberwar, als Moment des Krieges von Gemeinwesen oder Teilen davon, geführt. Politische Ziele bleiben nur in der Gemeinschaft verwirklichtbar. Einzeltäter streben im Cyberspace nach persönlicher Bereicherung. Diese Form der virtuellen Gewalt ist dem Verbrechen zuzuordnen.

Der dritte Grundsatz des gehegten Krieges bezieht sich auf den Ort der Kriegführung. Im Großen Krieg trachten die Konfliktparteien danach den Krieg in das Feindesland zu tragen.⁷⁵⁰ Dies ist beim Kleinen Krieg nicht der Fall, dort ist derjenige der Stärkere, welcher sich auf seinem Territorium bewegt, oder wie es Mao formuliert „wie der Fisch im Wasser schwimmt“ (Hervorhebung durch den Verfasser.). Dies ist in Analogie auf den Cyberwar anzuwenden. Sowohl Angreifer wie auch der Verteidiger sind im selben Raum unterwegs. Der Cyberspace kennt keine Grenzen, daher ist ein dort ausgetragener Konflikt immer einer, der durch den Angreifer im eigenen Territorium ausgeführt wird.⁷⁵¹ Dies zeigt sich in der Gefahr der potentiellen Eigenbeeinflussung durch einen Angriff, auf Grund der hohen Vernetzung in diesem Aktionsraum.

⁷⁴⁷ Vgl. ebd., S. 16.

⁷⁴⁸ Vgl. ebd., S. 16.

⁷⁴⁹ Vgl. Freudenberg, 2008, S. 119.

⁷⁵⁰ Vgl. Haffner, 1966, S. 16. (in: Tse-tung, 1966)

⁷⁵¹ Vgl. ebd., S. 29.

Die zeitliche Hegung des Konfliktes ist Thema des vierten Grundsatzes. Der Große Krieg sucht die Entscheidung so rasch als möglich.⁷⁵² Dies liegt zum einen in der räumlichen Begrenztheit und zum anderen in der Komplexität der Waffensysteme. Zweiteres hat Einfluss auf die Kosten eines Krieges, die bei einer langen Dauer das Gemeinwesen wirtschaftlich ruinieren können. Um die Entwicklung des Gemeinwesens nicht zu behindern und es in seiner Existenz nicht zu bedrohen, muss der Krieg die Ausnahme und nicht die Regel sein. Der Kleine Krieg zielt auf eine lange Dauer ab, um genau diesen Effekt herbeizuführen und die Staatsmacht zu stürzen. Da der Cyberwar ein ständig durchgeführter Krieg im Geheimen ist, der sich in der Intensität, um die Schwelle des bewaffneten Konfliktes herum, ausprägt, ist er nicht dem Großen Krieg zuzuschreiben. Er bereitet einen potentiellen Großen Krieg vor oder unterstützt diesen.

Der fünfte Grundsatz beschäftigt sich mit der Eskalation des Krieges. Der Große Krieg sucht die rasche Entscheidung und verhindert dadurch, dass er zum Äußersten kommt. Nicht die totale Vernichtung des Gegners spielt hier die entscheidende Rolle, sondern die Durchsetzung des eigenen Willens. Dies kann auch ohne Erreichung der höchsten Eskalationsstufe geleistet werden. Abschreckung ist ein Konzept, das hier zum Tragen kommt. Dies funktioniert allerdings nur dann, wenn die Aktionen im Krieg einer Konfliktpartei zuordenbar sind. Diese Wahrnehmbarkeit fehlt im Cyberwar. Er wirkt im Geheimen, also anonym. Anonym ist Abschreckung nicht zu gewährleisten.

Der Cyberwar ist als Moment des Krieges vom Großen Krieg, dem traditionellen, konventionellen zwischenstaatlichen Krieg, abzugrenzen. Der Cyberwar ist grundsätzlich dem Kleinen Krieg zuzuordnen, er ist damit eine asymmetrische Konfliktform. Wie auch beim Großen Krieg handelt es sich beim Cyberwar um einen Kampf zweier Willen, einen Zweikampf im Sinne von Clausewitz. Von der Einsatzdurchführung her betrachtet, ist der Einsatz des Militärs, der Streitkräfte, in Luft, See, Weltraum und Cyberspace unterstützend.

Der Kleine Krieg steht nicht neben dem Großen Krieg, sondern ist eine Unterstützungsmaßnahme dessen, der Cyberwar ist damit ständiger Begleiter des Großen Krieges. Dies ist vor allem darauf zurückzuführen, dass Staaten über hochtechnisierte und vernetzte Waffensysteme verfügen, die damit zumindest Ziel für den Kleinen Cyberwar werden. Da das Militär als Akteur keine Kennzeichnung im Cyberspace trägt, ist eine Unterscheidung von Akteuren recht schwierig. Ein privater Akteur, ein Bürger, ist damit in der Lage in einem solchen Konflikt wirksam zu werden. Er agiert also im Sinne des Kleinen Krieges als Unterstützer regulärer Streitkräfte.

Der Große Krieg beginnt auf dem Höhepunkt der Kraftentfaltung eines Gemeinwesens, ist also eine Strategie des Stärkeren. Der Kleine Krieg und somit auch der Cyberwar wird aus der Schwäche heraus begonnen, er ist eine Strategie der Schwachen. Nichtsdestotrotz wenden auch starke Gemeinwesen den Cyberwar an, um Kontrolle und Macht auszuüben. Dies dient zum Wohl des eigenen Gemeinwesens. Die Motivation des Akteurs ist,

⁷⁵² Vgl. ebd., S. 16.

bei der Differenzierung zwischen Krieg und Verbrechen im Netz, von Bedeutung. Nach der Einordnung in den Begriff vom Krieg, wird diese Differenzierung näher analysiert.

7.4.3 Die Abgrenzung des Cyberwar zu den anderen Konfliktformen im Netz

Die Unterscheidung des Krieges und somit auch des Cyberwar zur Kriminalität liegt in der Motivation, die diesen Formen des Konfliktes zu Grunde liegt. Krieg verfolgt immer eine politische Zielsetzung, sein Zweck liegt im Politischen. Die Kriminalität hat ihren Zweck in der persönlichen Bereicherung der Akteure. Im Krieg verfolgen die Akteure die Auflösung des gegnerischen Ordnungssystems, um ihr eigenes installieren zu können. Den Willen des Gegners zu brechen ist dazu die Vorbedingung. Bei konkurrierenden Staaten ist die Implementierung des eigenen Systems beim Gegner das Ziel.

Ebenso sind Bürger-, Guerillakriege und der Terrorismus unter diesem Blickwinkel zu betrachten. Hier geht es um die Auflösung des Ordnungsrahmens, um einen eigenen, nach Niederringung des Gegners, zu schaffen bzw. ihn im eigenen Sinn zu ändern. Im Rahmen der Organisierten Kriminalität wird auch oftmals von Krieg gesprochen (Drogen-, Mafiakrieg). Zwischen den verschiedenen Banden und Kartellen herrscht tatsächlich ein Kriegszustand im oben beschriebenen Sinn. Dennoch steht die Bereicherung im Fokus dieser Tätigkeiten und es handelt sich somit um kriminelle Handlungen.⁷⁵³ Kriminelle nutzen den bestehenden Ordnungsrahmen zu ihrem Vorteil. Es ist nicht das Ziel eine eigene Ordnung zu installieren. Eine gewisse, schwache rechtliche Ordnung ist notwendig, um die Gewinne aus der Bereicherung ausnutzen zu können. Neben dem Zweck ist dies der wesentliche Unterschied zwischen Krieg und Kriminalität.

Dieser Unterschied lässt sich auf den Cyberwar und die Kriminalität im Netz übertragen. Die Kriminalität im Cyberspace hat als Hauptintention die Ausnutzung von Informationen. Es geht darum Daten zu gewinnen, welche sich in der Realisierung persönlicher Ziele umsetzen lassen. Gemeint sind persönliche Gewinne, die sich einerseits monetär, aber andererseits auch in einer Steigerung, des persönlichen Machtgefühls, äußern können.⁷⁵⁴ Diese persönliche Bereicherung wird wahrnehmbar, wenn sich der Schaden beim Opfer manifestiert.⁷⁵⁵ Dies ist vom Täter gewünscht, denn nur wenn der Geschädigte den Schaden merkt, hat der Kriminelle seine Genugtuung erreicht. Cyber Kriminalität hat eine höhere Wahrnehmbarkeit.

Betrachtet man den Terrorismus, so liegt diesem ein politischer Zweck zu Grunde, auch dem Terrorismus im Netz, und somit ist er der Domäne des Krieges zuzuordnen. Die Methoden, die zur Anwendung kommen, verletzen vielfach strafrechtliche Bestimmungen und man ist daher versucht diese Konfliktform mit der Kriminalität gleichzusetzen. Hier kommt wieder die Intensität zum Tragen, ist diese gering und damit einem Verbrechen

⁷⁵³ Vgl. Freudenberg, 2008, S. 138.

⁷⁵⁴ Vgl. Olson, 2012, S. 36.

⁷⁵⁵ Vgl. Bowden, 2012, S. 17.

gleichzusetzen, dann ist die Verantwortung bei der Polizei zu suchen. Herrscht jedoch eine hohe Intensität, in den Angriffen von Cyber Terroristen, ist der Einsatz des Militärs angezeigt. Die Intensität spielt eine umso größere Rolle, als dass die Trennung zwischen inneren und äußeren Angriffen nicht mehr eindeutig zu treffen ist.

Die verschiedenen Arten des Konfliktes lassen sich, hinsichtlich ihrer grundsätzlichen Ausrichtung, in symmetrische und asymmetrische Konfliktformen einordnen. Die Unterscheidung der verschiedenen Konflikte ist in Summe wie folgt vorzunehmen: Nach Intention, Akteur, Mittel, Ort/System, Ausmaß/Intensität und Ziel. Aus diesen Faktoren ist die jeweilige Verantwortung für den Konflikt, die Konfliktform, abzuleiten.

Dem Militär obliegt der Schutz des Systems des Staates vor seiner Auslöschung, die Aufrechterhaltung der Souveränität, oder aber die Aufgabe, die Errichtung einer neuen Ordnung zu ermöglichen. Die innere Sicherheit soll die Funktion des Systems gewährleisten, während äußere Sicherheit sich mit dem Erhalt, der Herstellung oder der Auslöschung des Systems beschäftigt. Es ist eine ständige Abhängigkeit zwischen den Sicherheitsbereichen gegeben. So können Konflikte, welche das System gefährden, im Inneren entstehen und zur Aufgabe des Militärs werden. Grundsätzlich kann von einer Kompetenzzuordnung ausgegangen werden, welche zum einen zweckorientiert ist und zum anderen systemisch, funktional verstanden wird.

Der Akteur, mit politischem Zweck als Grundlage für seine Handlungen, bedarf des Eingreifens des Militärs. Der Akteur, der sich nur bereichern will, ist der Zuständigkeit der Polizei unterworfen. Neben dem Zweck ist der Akteur von Bedeutung, allerdings eine „[...] Kategorisierung von Cyber-Attacken primär nach Urhebern ist in der Praxis zunehmend schwierig.“⁷⁵⁶ Mit zu berücksichtigen ist stets die Intensität des Konfliktes, da Kriminalität besonders hoher Intensität das Eingreifen des Militärs erfordern kann, wobei die Führungsverantwortung hier trotzdem bei der Polizei verbleibt.

Erfolgt der Angriff systemisch von außen, ist das Militär in der Verantwortung. Es kann daraus gefolgert werden, dass die Schwelle, für die Entscheidung der Führungsverantwortung, zwischen den verschiedenen bewaffneten Trägern der Staatsgewalt, im Übergangsbereich von der Spionage über die Manipulation hin zum Terrorismus liegt. Im Cyberwar sind einige, der oben genannten sechs Parameter, nicht eindeutig zuordenbar. Vor allem im Großen Cyberwar liegen diese Faktoren oft im Dunkeln. Im Kleinen Cyberwar treten die Faktoren klarer in die Wahrnehmung ein.

Eine Zuordnung der Zuständigkeit ist vor allem bei den Konfliktformen schwierig, bei denen die Wahrnehmbarkeit eingeschränkt ist. Bei den hoch wahrnehmbaren Konfliktformen kann, zwischen den ausnützenden und den schwächenden, eine klare Zuordnung getroffen werden. Diese beruht auf der

⁷⁵⁶ Center for Security Studies, CSS Analysen zur Sicherheitspolitik: Cyberwar: Konzept, Stand und Grenzen, 2010, S. 1.

Abgrenzung zwischen politisch motivierten und an der Bereicherung orientierten Formen des Konfliktes im Netz.

Zu der Begriffsinversion von Kleinem und Großem Cyberwar tritt eine weitere Inversion hinzu. Kriminalität im Netz wird öffentlich, d.h. sichtbarer als der Krieg im Cyberspace. Die Wahrnehmbarkeit ist somit ein wesentlicher Faktor zur Abgrenzung des Cyberwar zu den anderen Konfliktformen im Netz. Da die subjektive Wahrnehmung von Gefahr an die Sichtbarkeit dieser gebunden ist, werden Gefahren in der heutigen Zeit nicht mehr so einfach wahrgenommen. Dies vermindert die Akzeptanz für die Notwendigkeit des Militärs. Viele Probleme und militärische Bedrohungen sind nicht fassbar und damit aus unserer Wahrnehmung gerückt. Die Aufgabe des Staates ist es, diese Gefahren zu erkennen und die entsprechenden Maßnahmen zu veranlassen.

Die Politik hat dem Bürger zu erklären, dass für die Gemeinschaft ein Schutz, gegen nicht vordergründig wahrnehmbare Gefahren, sicherzustellen ist.⁷⁵⁷ Da ein Krieg, so auch der Cyberwar, zum Ziel hat den Gegner zu besiegen, d.h. ihn handlungsunfähig zu machen, ist eine Verbindung des Cyberwar mit der Souveränität angezeigt.

7.4.4 Das Verhältnis zwischen Souveränität und Cyberwar

Für die Führungsverantwortung des Militärs im Cyberspace ist der Souveränitätsbegriff von großer Bedeutung. In einer Bewertung der ÖSCS durch das BMLVS wird nochmals auf die Aussage in der Cyber Strategie reflektiert, die dem BMLVS die Führungsverantwortung für die militärische Landesverteidigung zum Souveränitätsschutz, im Sinne der äußeren Sicherheit, überträgt.⁷⁵⁸ Der mit der äußeren Sicherheit einhergehende Begriff der äußeren Souveränität wird hier in einem territorialen Bezug gesehen. Dieser Territorialbezug ist im Cyberspace nicht einfach herstellbar. Der Cyberspace ist ein entgrenzter Raum, ein systemisches Verständnis von Souveränität ist hier notwendig. Wenn man den Souveränitätsbegriff hier rein territorial fasst, muss der Cyberspace als souveränitätsfreier Raum gesehen werden.⁷⁵⁹

Da ein systemisch, funktionaler Ansatz bei der Unterscheidung von innen und außen erfolgen muss, ist es eine Vorbedingung festzustellen, welche Systeme von Relevanz für die Souveränität sind. Diese Souveränitätsrelevanz hängt direkt mit der Cyber Defence, im Rahmen der militärischen Landesverteidigung, zusammen. Dort, wo die Souveränität angegriffen wird, ist der Einsatz des Militärs angezeigt. Das Militär ist jenes staatliche Instrument, welches der Aufrechterhaltung und Wiederherstellung der Souveränität dient. Um innere Souveränität zu erlangen, braucht es die Unabhängigkeit nach außen.

⁷⁵⁷ Vgl. Freudenberg, 2008, S. 69ff.

⁷⁵⁸ Vgl. BMLVS, Begleitschreiben zum Ministerratsbeschluss 180/8, GZ S92100/6-MilStrat/2013, Wien 2013, S. 2f.

⁷⁵⁹ Vgl. Schaller, 2014, S. 7.

Dabei entsteht eine Wechselwirkung zwischen Intensität eines Konfliktes und der Souveränität. Je mehr vitale Bereiche eines Gemeinwesens angegriffen werden, umso breiter also ein Konflikt wirkt, desto eher ist der Staat in seinem Handlungsspielraum, in seiner Entscheidungsfreiheit eingeschränkt, er verliert seine Souveränität teilweise oder ganz. Es kann eine direkte und eine indirekte Souveränitätsrelevanz festgestellt werden. Direkt souveränitätsrelevant sind staatliche IKT-Systeme, indirekt souveränitätsrelevant sind Systeme, welche für das Gemeinwesen und die Handlungsfähigkeit des Gemeinwesens als Ganzes notwendig sind.

D.h. je breiter ein Cyber Angriff wirkt, je höher die Intensität ist, desto relevanter wird dies für die Souveränität. Dabei können bewusst Kaskadeneffekte herbeigeführt werden, um einen Angriff möglichst breit wirken zu lassen. Neben der Intensität lässt sich die Relevanz für die Souveränität an den Formen des Cyberwar festmachen. Der Angriff auf militärische Systeme oder Systeme von denen die militärischen Systeme direkt abhängen, also im Kleinen Cyberwar, hat eine direkte Souveränitätsrelevanz. Ebenso der Angriff auf Regierungssysteme, die für die Handlungsfähigkeit des Staates notwendig sind.

Im Großen Cyberwar ist die angesprochene Relevanz dann gegeben, wenn die Intensität hoch ist, d.h. der Angriff sehr breit wirkt. Dann kann von einer indirekten Relevanz für die Souveränität gesprochen werden. Angriffe im Großen Cyberwar können direkt und/oder indirekt wirken, wobei die indirekte Wirkung die vorherrschende sein wird. Angriffe können nach ihrem Ziel eine unterschiedliche Relevanz für die Souveränität haben. Hierbei ist die Frage, ob es um Infrastruktur geht, also den Kampf im Netz mit Zielen außerhalb des Cyberspace, oder ob es sich um Informationen handelt, also Ziele innerhalb dieses Raumes.

Im letzten Fall ist die Information die angegriffene „Infrastruktur“ (Hervorhebung durch den Verfasser.). Um eine Infrastruktur, hinsichtlich ihrer Bedeutung für die Souveränität, zu bewerten, benötigt man Kriterien. Diese orientieren sich an der Ausdehnung (Betroffene, Raum), der Auswirkung (wirtschaftlich, psychologisch, politisch und ökologisch), der Dauer, der Möglichkeit die Infrastruktur zu ersetzen und der Wechselwirkung mit anderen Bereichen.⁷⁶⁰ Viele dieser Kriterien geben einen Hinweis auf die Relevanz für die Souveränität.

Die Angriffe, die hier von Bedeutung sind, richten sich gegen Infrastrukturen, die in dem Zusammenhang als Kritische Infrastrukturen bezeichnet werden. Darunter können

„[...] jene Infrastrukturen oder Teile davon, die eine wesentliche Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen haben und deren Störung oder Zerstörung schwerwiegende Auswirkungen auf die Gesundheit, Sicherheit oder

⁷⁶⁰ Vgl. BKA, Vortrag an den Ministerrat, BKA-406.300/0001-IV/6/2008, Das österreichische Programm zum Schutz kritischer Infrastrukturen, Masterplan APCIP, Wien, März 2008, S. 6.

das wirtschaftliche und soziale Wohl der Bevölkerung oder die effektive Funktionsweise von Regierungen haben [...]“⁷⁶¹,

verstanden werden. Diese Infrastruktur wird vielfach als strategische Infrastruktur bezeichnet, weil Angriffe auf diese eine breite Wirkung in der Öffentlichkeit nach sich ziehen. In der EU werden elf verschiedene Sektoren definiert.⁷⁶² Die darin angeführten Infrastrukturen haben eine wesentliche Bedeutung für das Gemeinwesen.

Zum Beispiel hat die Stromversorgung eine indirekte Souveränitätsrelevanz, die als sehr hoch zu beurteilen ist. Ohne Stromversorgung sind wesentliche Bereiche eines Gemeinwesens nicht mehr aufrecht zu erhalten.⁷⁶³ Durch den Ausfall von Systemen, die von der Stromversorgung abhängig sind, ist eine zunehmende Handlungsunfähigkeit des Staates zu erwarten. Diese richtet sich zunächst nach innen und in weiterer Folge auch nach außen.

Ein Angriff aus dem Cyberspace auf die Stromversorgung ist eine durchaus machbare Beeinflussung der Handlungsfähigkeit und damit der Souveränität, sowohl der inneren als auch der äußeren, eines Gemeinwesens. Diese Tatsache wirft einige Fragen auf. Grundsätzlich ist für die Durchsetzung der Souveränität nach innen die Polizei, als Sicherheitsbehörde, zuständig, doch muss für die Zuordnung der Führungsverantwortung zusätzlich eine Trennung in territoriale und systemische Verantwortung getroffen werden.

Durch einen Cyber Angriff auf die Stromversorgung wird zunächst die innere Souveränität berührt, es geht um die Aufrechterhaltung der Ruhe und Ordnung im Inneren. Auf Grund der Eigenschaften des Cyberspace handelt es sich jedoch in jedem Fall um einen Angriff von außen. Territorial ist die Führungsverantwortung, im Beispiel der Stromversorgung, klar bei den Sicherheitsbehörden, systemisch allerdings ist das Militär zur Abwehr der Gefahr von außen (systemisch verstanden) verantwortlich. Es treten noch weitere verantwortliche Akteure hinzu, nämlich die Betreiber der Kritischen Infrastrukturen, deren Aufgabe ein grundlegender Schutz derselben ist. Eine Frage die es hier auch zu klären gilt ist, von wem der Angriff auf die souveränitätsrelevanten Systeme ausgeht. Die gängige Lehrmeinung sieht eine Gefährdung der Souveränität nur dann gegeben, wenn der Verursacher ein staatsnaher oder staatlicher Akteur ist.⁷⁶⁴ Hier ist im Falle eines Cyber Angriffes eine differenziertere Betrachtung notwendig.

Die Souveränitätsrelevanz ist ein wichtiges Kriterium für die Zuordnung der Führungsverantwortung. Sie umfasst eine innere und eine äußere Komponente, die nicht nur territorial fassbar sind. Neben diesen beiden Faktoren ist die Unmittelbarkeit ein wichtiger Parameter, d.h. es ist zu klären ob es sich dabei um eine direkte oder indirekte Einwirkung auf die

⁷⁶¹ Ebd., S. 5.

⁷⁶² Vgl. ebd., S. 5.

⁷⁶³ Vgl. Ladinig, Udo; Saurugg, Herbert: Black Out. Nichts geht mehr. In: Truppendienst, Nr. 326, 2/2012, S. 130.

⁷⁶⁴ Vgl. <https://www.faz.net/aktuell/politik/politische-buecher/terrorismus-und-souveraenitaet-auch-auf-fremdem-territorium-14117751.html>, [12.05.2020].

Souveränität handelt. Zusammengefasst kann festgehalten werden, dass bei Angriffen auf souveränitätsrelevante Systeme oder Infrastrukturen (wie z.B. die Stromversorgung) aus dem Netz, die Führungsverantwortung zur Abwehr von Gefahren von außen (systemisch) dem Militär obliegt.

Da aber eine hohe Interdependenz zwischen diesen Systemen herrscht und die Betreiber mehrheitlich aus dem zivilen Umfeld kommen, ist ein gesamtstaatlicher Ansatz zur Bewältigung von Angriffen aus dem Cyberspace notwendig.⁷⁶⁵ Nach der Einordnung des Cyberwar in den Kriegsbegriff und der Abgrenzung zum konventionellen Krieg und den anderen Konfliktformen im Cyberspace, wird der Cyberwar einem Definitionsversuch unterzogen, der die erarbeiteten Erkenntnisse miteinbeziehen soll.

7.4.5 Der Begriff vom Cyberwar

Der Cyberwar ist der Krieg im Cyberspace. Orientiert man sich an der Definition des Krieges nach Clausewitz, so handelt es sich um einen Zweikampf, der, mittels Anwendung von Gewalt, den Gegner zur Erfüllung des eigenen Willens bringt, um einen politischen Zweck zu verwirklichen.⁷⁶⁶ Da der Cyberwar, als virtuelle Form des Kleinen Krieges, ein Moment des Krieges ist, richtet sich dieser am Kriegsbegriff aus. Mit Cyberwar ist

„[...] die kriegserische Auseinandersetzung im virtuellen Raum vorwiegend mit Mitteln aus dem Bereich der Informationstechnik gemeint.“⁷⁶⁷

Zusätzlich dazu werden auch Maßnahmen, die den Streitkräften aus dem Cyberspace heraus zur Unterstützung dienen, unter dem Cyberwar Begriff subsumiert. Dazu zählen vor allem Leistungen von automatisierten bzw. aus dem Cyberspace gesteuerten Waffensystemen. Der Einsatz von Drohnen kann ohne Informationstechnik nicht durchgeführt werden und stellt in diesem Fall eine Ausformung des Cyberwar dar. Die Definition schließt somit als kriegserische Auseinandersetzung die Kernpunkte der Definition nach Clausewitz mit ein.

Damit fällt auch das Argument, welches Rid ins Feld führt, dass Krieg gewaltvoll und somit immer tödlich oder zumindest potentiell tödlich sein muss, dies aber auf den Cyberwar nicht oder nur eingeschränkt zutrifft.⁷⁶⁸ Gewalt ist für Rid einer von drei Faktoren, die einen kriegserischen Akt kennzeichnen.⁷⁶⁹ An Clausewitz orientiert formuliert er den instrumentellen Charakter und den politischen Zweck als die beiden anderen Faktoren des Kriegsbegriffs, die alle drei immer gemeinsam erfüllt sein müssen, um von einem Krieg zu sprechen. Nicht nur der Einsatz von Drohnen im Krieg erfüllt diese Kriterien, auch der Stuxnet Angriff beinhaltet alle drei Faktoren.

⁷⁶⁵ Vgl. Hofstetter, 2019, S. 181.

⁷⁶⁶ Vgl. Clausewitz, Vom Kriege, S. 13 und S. 21.

⁷⁶⁷ Center for Security Studies, CSS Analysen zur Sicherheitspolitik: Cyberwar: Konzept, Stand und Grenzen, 2010, S. 2.

⁷⁶⁸ Vgl. Rid, 2013, S. 1f.

⁷⁶⁹ Vgl. ebd., S. 4.

Allerdings ist der Cyberwar nicht der Ersatz für den Krieg, er tritt nicht an dessen Stelle, sondern er ist nur ein Teil davon. Physische Gewalt spielt im Cyberwar eine wesentliche Rolle und manifestiert sich nicht unbedingt in gleicher Weise wie im konventionellen Krieg.⁷⁷⁰ Von der Kontrolle bis zur Zerstörung der Infrastruktur, von der mittelbaren bis zur unmittelbaren Gewaltausübung gegenüber Menschen, reicht hier das Spektrum im Cyberwar. Wirkt die physische Gewalt im Netz auf der Mikroebene, so kann sie außerhalb des Netzes auch auf der Makroebene wirksam werden. Bei der klassischen physischen Gewaltanwendung bedarf der Wille zur Gewalt eines Körpers, der diese latente Gewalt in eine manifeste umwandelt. Für die Gewaltanwendung aus dem Cyberspace heraus, also auf der Makroebene, bedarf es eines Körpers, meist in Form des angegriffenen Zielsystems, um die Gewalt physisch zu manifestieren.

Clausewitz spricht in seiner Kriegsdefinition auch vom Gegensatzpaar des Angreifers und des Verteidigers. Kampf kann es nur dort geben, wo diese einander gegenüberstehen. Dies trifft nach Ansicht des Verfassers nur auf den Großen Krieg zu. Der Kleine Krieg sucht genau die Stelle, an der sich der Gegner nicht verteidigt, um ihn zu treffen und zu schwächen.

Setzen wir die Begriffsinversion voraus, so haben wir einen Großen Cyberwar, der für den Angegriffenen oft nicht wahrnehmbar ist, da er im Geheimen von staten geht. Es darf nicht vergessen werden, dass sowohl der Kleine Cyberwar als auch der Große Cyberwar, beide Momente des Virtuellen Krieges und damit auch des Kleinen Krieges sind. Da sich der Cyberwar zusehends zu einer eigenen Kategorie von Krieg entwickelt hat, der in einer eigenen Domäne wirkt, ist die Unterordnung des Krieges mit und um Informationen unter den Begriff des Information War nicht mehr zeitgemäß.

Eine Definition, die somit in abgewandelter Form⁷⁷¹ für den Cyberwar zutrifft, bezeichnet den Cyberwar als

„[...] an expansive category of military activities. It includes physical attacks on information systems by traditional military means, psychological operations, military deception, and electronic warfare operations such as jamming.“⁷⁷²

In dieser Definition finden sich die Arten der Waffen im Cyberwar wieder. Sie lässt offen, ob die Akteure, welche diese militärischen Aktivitäten ausführen, auch Angehörige von regulären Streitkräften sind, legt dabei aber fest, dass es sich um ein politisches Mittel handelt. Dies begründet sich darin, dass militärische Aktivitäten, auch wenn sie nicht durch reguläre Streitkräfte ausgeführt werden, von Gruppierungen, zur Erreichung eines politischen Zweckes, angewandt werden.

Unter dem Begriff der Informationssysteme können die Informationen selbst subsumiert werden. Es liegt also eine sehr umfassende Definition vor,

⁷⁷⁰ Vgl. Bowden, 2012, S. 76f.

⁷⁷¹ Anm. d. Verf.: Shackelford definiert hier den Information War, wobei durch den Verfasser der Information War durch den Cyberwar ersetzt wird.

⁷⁷² Shackelford, 2009, S. 230. (in: Berkeley Journal of International Law, 2009)

die, in ihrer freien Interpretierbarkeit, sehr weit gefasst ist. Sie beinhaltet, bis auf die Intensität und die Ursachen/Ziele, alle Kategorien des Cyberwar. Um die Definition zu vervollständigen, sind zusätzlich unter Cyberwar

„[...] alle Aktionen zu subsumieren, die unternommen werden, Informationsüberlegenheit zu erzielen, indem die Informationen des Feindes beeinflusst werden, oder dazu beigetragen wird, eigene Ziele zu erreichen. Mit inbegriffen sind gezielte, politisch motivierte Angriffe mit Hilfe der IT, die Auswirkungen auf die politische Handlungsfähigkeit von Staaten haben, bis hin zur Einbeziehung von Streitkräften.“⁷⁷³

Der Cyberwar ist ein politischer Konflikt, der mit realen und/oder virtuellen Waffen geführt wird. Ziel ist es, über den jederzeitigen Zugriff und somit die jederzeitige Einwirkung auf die Informationssysteme des Gegners zu verfügen, um die politische Handlungsfähigkeit des gegnerischen Gemeinwesens beeinflussen zu können.

Damit trifft diese Definition die Kerninhalte des Kriegsbegriffes nach Clausewitz, wenn dieser damit auch vorrangig den Großen Krieg definiert hat. Der Cyberwar erfüllt ebenso die drei Kriterien nach Rid, denn er ist gewaltvoll, instrumentell und auch politisch motiviert. Da aber der Krieg und somit auch der Cyberwar wie ein Chamäleon sind, welches seine Erscheinungsform verändert und dadurch ein sich ständig wandelndes Wesen darstellt, werden im virtuellen Kleinen Krieg diese Kriterien entsprechend unterschiedlich ausgeprägt zum Vorschein kommen.⁷⁷⁴ Der Cyberwar hat in seinen Ausprägungen eine militärische und eine gesamtstaatliche Form, die einer unterschiedlichen Wahrnehmung unterliegen. Der Kleine Cyberwar ist eine rein militärische Aufgabenstellung, während der Große Cyberwar nicht nur alle Bereiche eines Gemeinwesens treffen kann, sondern auch eine gesamtstaatliche Anstrengung zur Abwehr erfordert.

7.5 Zwischenergebnis zum Begriff des Cyberwar

Die Wirkung im Cyberwar kann auf Informationen oder durch Informationen erfolgen. Information ist sowohl Ziel als auch Waffe. Die virtuelle Waffe bedarf einer Definition, welche allgemein anerkannt ist. Darauf aufbauend können dann rechtliche Normen formuliert werden, welche auch international kompatibel werden. Ein generelles Verbot von Cyber Waffen erscheint aus Sicht des Verfassers problematisch, da Informationen, wie oben gezeigt, ein Multirole-Mittel sind und daher unterschiedlichen Zwecken zugeführt werden können. Der Schädigungseffekt ist hier nicht im Vordergrund stehend.

Die Tätigkeiten von Staaten erfolgen vielfach unter dem Deckmantel der Anonymität, während irreguläre Akteure um Sichtbarkeit ihrer Aktionen

⁷⁷³ Lau, Torsten: Cyber-Crime und Cyber-Crime-Kontrolle. Zum möglichst rationalen Umgang mit weltweiten Bedrohungsszenarien: Cyber-Kriege und Cyber-Terror, Bonn 2003, S. 2f.

⁷⁷⁴ Vgl. Stadler, Christian: Clausewitz zwischen Morsetelegraph und IFMIN. In: FMTSforum, 5. Jahrgang, 1/1995, S. 19.

bemüht sind. Dies hat eine Inversion des Kriegsbegriffs zur Folge. Im Cyberwar ist die Sichtbarkeit der Aktionen von Streitkräften unerwünscht.

Der Krieg im Netz umfasst also zwei Momente oder Formen des Cyberwar. Zum einen eben den Krieg im Geheimen und zum anderen die Unterstützung von konventionellen Kräften in einem bewaffneten Konflikt. Die entscheidenden Herausforderungen im Cyberwar, egal welcher Form, sind dem 3A-Ansatz zuzurechnen. Dieser Ansatz umfasst die Kernprobleme bei Konflikten im Netz. Es handelt sich dabei um die Attribution, die Anonymität und die Anarchie im Cyberspace. Die Herausforderung besteht darin, dass praktisch jeder Nutzer des Cyberspace, zu einem Akteur im Cyberwar werden kann.⁷⁷⁵

Diese Tatsache erschwert die Zuweisung von Verantwortungen im Netz. Da Jedermann theoretisch in der Lage ist, diesen Krieg im Netz zu führen, ist er vom Wesen her als Kleiner Krieg zu fassen. Da das Moment des Cyberwar, welches im Geheimen durchgeführt wird, ein umfassenderes ist, kann diese Form als Großer Cyberwar bezeichnet werden. Die Unterstützung von konventionellen Streitkräften bezieht sich nur auf einen begrenzten Bereich des Gemeinwesens und ist damit als Kleiner Cyberwar zu bezeichnen. Beide Formen sind Momente des Kleinen Krieges. Eine mögliche Zuweisung von Verantwortungen kann sich an der Form des Cyberwar orientieren.

Die Intensität richtet sich nach den Auswirkungen, die mit einem Angriff erzielt werden. Im Netz kann die Intensität eines Angriffs an der Anzahl der betroffenen Systeme bemessen werden. Die Intention orientiert sich daran, ob das System, welches angegriffen wurde, ausgenutzt oder geschwächt wird. Die Ausnutzung lässt auf einen kriminellen Hintergrund schließen. Die Schwächung weist auf einen kriegesischen Hintergrund hin. Im ersten Fall obliegt die Führungsverantwortung der Polizei, im zweiten Fall dem Militär.

Von der Intensität her betrachtet, ist der Große Cyberwar höher einzustufen, als der Kleine Cyberwar. Auch wirkt der Cyberwar des großen Typus nur mittelbar auf das Militär. Der Kleine Cyberwar wirkt direkt gegen militärische Systeme und damit ist die Zuständigkeit für diese Form des Virtuellen Krieges auch beim Militär angesiedelt. Da diese Form des Virtuellen Krieges sich nicht der Wahrnehmbarkeit entzieht, ihre Wirkung ist im Zuge eines konventionellen Konfliktes offensichtlich, bedarf es auch unterschiedlicher Instrumente in den beiden Formen des Cyberwar.

Da der Kleine gemeinsam mit dem Großen Cyberwar auftreten kann und diese beiden sich zum Cyberwar an und für sich synthetisieren, ist die Intensität des Virtuellen Krieges als am höchsten einzustufen. Hier kann festgehalten werden, dass sich die Intensität ähnlich wie beim konventionellen Krieg gestaltet. Es folgert aus der Beschaffenheit des Cyberwar, dass hier das Militär nur ein Mittel von vielen darstellt. Es muss hier gesamtstaatlich vorgegangen werden. Hochvernetzte Gemeinwesen haben mit dem Cyberwar die Möglichkeit, bewaffnete Konflikte auf eine neue

⁷⁷⁵ Vgl. Hofstetter, 2019, S. 198.

Art und Weise auszutragen. Es benötigt die konventionellen Streitkräfte zwar, um den Sieg zu untermauern, ein Einsatz derselben ist nur als potentielle, als latente, Größe notwendig.

Der Zweck des Cyberwar richtet sich an den Formen desselben aus. Der Krieg im Geheimen verfolgt die Einwirkung auf möglichst viele Politikbereiche eines Gemeinwesens, er wirkt strategisch. Dabei zielt er nicht auf die Zerstörung, sondern die Kontrolle und Beeinflussung der Informationen ab. Vernetzung reduziert dadurch die Anzahl an konventionellen bewaffneten Konflikten, fördert aber andererseits die Konflikte im Cyberspace. Im Großen Cyberwar werden vor allem Mittel und Methoden einer, mehr oder weniger, offensiven Aufklärung angewandt.

Im Kleinen Cyberwar ist die Beeinträchtigung der gegnerischen Netze Zweck des Handelns. Dabei ist Schwächung durch Zerstörung ein durchaus gebräuchliches Mittel. Da die Form des Virtuellen Krieges vom Vernetzungsgrad mitbestimmt wird, orientieren sich die Mittel und Methoden ebenfalls daran.

Der Cyberwar ist, als unterstützendes Element des bewaffneten Konfliktes, eine Form des Kleinen Krieges. Der Cyberwar weist viele Eigenschaften auf, die auch den Kleinen Krieg kennzeichnen. Dazu zählen die territoriale Losgelöstheit, die freie Wahl des Angriffspunktes, die Schwierigkeit der Defensive und die eingeschränkte Wahrnehmbarkeit eines Cyber Angriffes. Als Kleiner Krieg ist der Cyberwar aber Teil des Krieges.

Da der Krieg im Netz eine asymmetrische Form des Krieges darstellt, ist ein Einsatz asymmetrischer Mittel und Methoden durch das Militär angezeigt. Der Cyberwar ist der ständige Begleiter des Krieges, egal in welcher Form, ob als Großer Cyberwar, zwischen hochgradig vernetzten Akteuren, oder aber als Kleiner Cyberwar, zwischen gering vernetzten Akteuren. Alle Gemeinwesen verfügen über ein Mindestmaß an Vernetzung. Daher hat sich jedes Gemeinwesen mit dem Krieg im Netz auseinander zu setzen.

Dies umso mehr, als die Wahrscheinlichkeit eines Cyberwar indirekt proportional zu einem konventionellen bewaffneten Krieg zu sehen ist. In Bezug auf die Kriminalität im Netz ist festzuhalten, dass die Intention nicht in der Zerstörung und Schwächung, sondern in der Ausnutzung begründet liegt. Dadurch entsteht eine Begriffsinversion zum Krieg, der im Verborgenen geführt werden möchte, während die Kriminalität einer hohen Wahrnehmbarkeit unterliegt. Dies mag auch der Grund dafür sein, dass die nationalen Strategien sich – wie im Folgenden dargestellt wird – an dieser Form des Konfliktes im Netz ausrichten. Es ist die Aufgabe der Gemeinwesen den Krieg im Netz sichtbar zu machen, um durch die Wahrnehmung der Bedrohung, in diesem Bereich, Sicherheit generieren zu können.

8 Vom Recht des Cyberwar

„Das Internet hat das Gefüge der Demokratie
schon grundlegend verändert.
[...] Gerade in diesen aufgeregten Zeiten
müssen wir also das Recht
gegen die Macht stellen.“
Ferdinand von Schirach⁷⁷⁶

Im Cyberspace wirken unterschiedliche Normen, die dessen Nutzung regulieren.

„Just as in real space, behavior in cyberspace is regulated by four sorts of constraints. Law is just one of those.“⁷⁷⁷

Neben dem Recht beschränkt vor allem die Natur – die Architektur des Raumes – die Handlungen des Menschen im Cyberspace. Die technischen Rahmenbedingungen – die zur Verfügung stehende Technologie – bestimmen maßgeblich die Handlungsmöglichkeiten. Ausgehend davon sind diese Möglichkeiten die Basis für eine rechtliche Regelung. Die Architektur des Cyberspace ist seine Verfassung, aus der heraus sich die rechtlichen Regelungen ableiten lassen.⁷⁷⁸

Der Cyberspace basiert allerdings nicht nur auf einer Architektur, sondern verschiedene Teile dieses Raumes sind verschieden verfasst.⁷⁷⁹ Diese unterschiedlichen Teile beruhen auf differenzierten technischen Rahmenbedingungen. Es gibt Netze, welche besonderer Zugangsvoraussetzungen bedürfen, andere Netze sind wiederum frei zugänglich. Zusätzlich unterliegt der Cyberspace einem ständigen Wandel. Auf Grund dieser Tatsachen wird eine rechtliche Regelung des Cyberraumes noch erschwert.

Konflikte ergeben sich hier nicht nur aus den verschiedenen technischen Rahmenbedingungen, sondern auch aus dem unterschiedlichen Nutzungsverhalten der in diesem Raum handelnden Menschen und Gemeinwesen. Dieses reicht vom kriminellen Akt bis hin zum Krieg, auch in diesem Handlungsraum.

Krieg findet zwischen Gemeinwesen statt. Die rechtlichen Regelungen müssen demnach Gemeinwesen übergreifend getroffen werden. Findet ein Krieg innerhalb eines Gemeinwesens statt, so gelten fast ausschließlich die Regeln desselben, also das nationale Recht. Völkerrechtlich ist der Akteur der Staat, das Primärsubjekt im Völkerrecht. Dieser ist gekennzeichnet durch die drei Faktoren Staatsvolk, Staatsgebiet und Staatsgewalt. Krieg bezieht sich stets auf diese drei Faktoren. Was den Krieg charakterisiert, hat direkt Einfluss auf die rechtliche Normierung desselben.

⁷⁷⁶ Festansprache zur Eröffnung der Salzburger Festspiele 2017.

⁷⁷⁷ Lessig, Lawrence: The Laws of Cyberspace. Essay presented at the Taiwan Net 98 conference, Taipei 1998, S. 4. Anm. d. Verf.: Lessig spricht hier vom Recht, sozialen Normen, dem Markt und von der Architektur (der Natur) des Raumes.

⁷⁷⁸ Vgl. ebd., S. 9.

⁷⁷⁹ Vgl. ebd., S. 8f.

Die folgende Betrachtung zielt auf die zweite Art des Rechts nach Grotius ab, das Völkerrecht.⁷⁸⁰ Dieses regelt das Verhalten der Völkerrechtssubjekte zueinander. Normen, die das Verhalten innerhalb der Staaten betrafen, wurden davon nicht berührt. Zweck ist die Vermeidung von Konflikten und wenn ein Konflikt ausgebrochen ist, diesen nach bestimmten Regeln ablaufen zu lassen. Ersteres wird durch das klassische Völkerrecht, Zweiteres durch das Humanitäre Völkerrecht geregelt.

Direkt beeinflusst wurde die Schaffung eines Kriegs- und Humanitätsrechts von der Entwicklung moderner Waffen und den daraus resultierenden Methoden der Kriegführung.⁷⁸¹ Hier zeigt sich der Zusammenhang zwischen Mittel, Methoden und Recht. In den nationalen Cyber Strategien zeigen die Völkerrechtssubjekte ihr Verständnis vom Umgang mit dem Cyberwar. An die Betrachtung des Völkerrechts und ausgewählter nationaler Strategien zur Cyber Sicherheit schließt die Untersuchung des europäischen Rechtsrahmens hinsichtlich des Umganges der EU mit der Thematik des Cyberwar an. Wie der Cyberwar vom EU-Recht erfasst wird, leitet dann zur Analyse des österreichischen Rechts, in Bezug auf das Phänomen Cyberwar, über.

Ausgehend vom Völkerrecht wird im Folgenden der Bogen über das Europarecht zum nationalen Rechtsrahmen gespannt und darin beleuchtet, wie der jeweilige Normenkomplex mit der Kriegsthematik bzw. daraus abgeleitet mit dem Cyberwar umzugehen pflegt.

8.1 Zum Cyberspace zwischen nationalem Recht und Völkerrecht

Grotius sieht das Recht nicht als reinen Willkürakt, sondern es orientiert sich an der Gerechtigkeit als Verhalten von Menschen gegenüber anderen Menschen. Er folgert daraus, dass es in einer Gemeinschaft keine rechtsfreien Räume geben kann.⁷⁸² Somit ist der Cyberspace, als (virtueller) Raum, in dem Menschen in einem sozialen Beziehungsgeflecht eingebunden sind, ein Raum, in dem Rechtsbeziehungen entstehen.⁷⁸³ Um den drei großen Gefahren im Cyberspace, der Cyber Kriminalität, der Industriespionage und der Cyber Kriegführung, begegnen zu können, sind rechtliche Rahmenbedingungen notwendig.⁷⁸⁴

Anarchie, Anonymität und die fehlende örtliche Zuordnung, innerhalb des Cyberspace, behindern die Wirksamkeit einer rechtlichen Ordnung im Netzwerk. Rechtlich befinden wir uns im Cyberspace in einer sehr frühzeitlichen Phase.

„Die naturrechtliche Verfasstheit des Internets – also der Umstand, dass der Stärkste am meisten Präsenz zeigen kann – gemeinsam mit der hohen Intransparenz über die Wahrheit hinter digitalen Personen

⁷⁸⁰ Vgl. Kirchmann, 1869, S. 56.

⁷⁸¹ Vgl. Neuhold/Hummer/Schreuer, 1991, S. 293.

⁷⁸² Vgl. Konegen, 1998, S. 16.

⁷⁸³ Vgl. Lessig, 1998, S. 4.

⁷⁸⁴ Vgl. Glenny, 2012, S. 214f.

oder Institutionen wird in Zukunft immer mehr Manipulatoren anziehen.“⁷⁸⁵

Dies bedeutet, dass im Cyberspace das Recht des Stärkeren in weiten Bereichen zur Anwendung gelangt. Die Lösung dieser Problematik ergibt sich in der Installierung einer Institution, die in der Lage ist, übergeordnet Zwang auszuüben.⁷⁸⁶ Dies bedingt aber eine Auflösung der Anarchie des Cyberspace, zu Gunsten einer stärkeren Kontrolle. Hier würde am eigentlichen Zweck des Netzes, dem freien Zugang und der freien Nutzung, gerüttelt.⁷⁸⁷ Kontrollmechanismen, wie die Vorratsdatenspeicherung, sind, wie bereits erwähnt, nicht unumstritten.⁷⁸⁸

Diese Freiheit, die viele Nutzer vom Netz als Medium erwarten und einfordern, ist aber nicht gleichzusetzen mit der Möglichkeit, der Freiheit, das zu tun, was man will. Hier werden Versuche ein Recht zu implementieren grundsätzlich missverstanden. Dies soll nicht der Einschränkung der Freiheit dienen, sondern vielmehr ihr erst zu ihrem Recht verhelfen. Soweit die idealistische Sicht.

Man muss hier allerdings auch die Intentionen derer verstehen, die solche Gesetze für das Netz erlassen wollen, und diese sind nicht immer der Freiheitsverwirklichung der Gemeinschaft untergeordnet.⁷⁸⁹ Hier präsentiert sich das Dilemma, in welchem sich die moderne Informationsgesellschaft momentan befindet.

„Die Freiheit des Internets muss immer von den Herrschenden akzeptiert werden. Sie ist ihnen nicht übergeordnet.“⁷⁹⁰

Den Cyberspace betrifft nicht nur eine Rechtsmaterie, sondern es werden durch das Handeln – in diesem Informationsraum – viele verschiedene Rechtsgebiete berührt. Die Komplexität an verschiedenen Rechtsgebieten, die ineinandergreifen, ist weder national noch international leicht aufzulösen.

Hat ein Staat sich zu einer Gesetzgebung, zur Etablierung eines rechtlichen Rahmens für das Netz, entschlossen, so sind damit die Herausforderungen nicht beseitigt. Die Architektur des Cyberspace besteht aus vielen miteinander vernetzten Komponenten, welche sich auf verschiedene Territorien verteilen können. Dies hat vor allem die Ursache darin, dass große Teile der Netzinfrastruktur entstaatlicht sind.

Große Wirtschaftsunternehmen z.B. agieren transnational und haben ihre Ressourcen im Cyberspace über viele Staaten verteilt. So können, gegen den Missbrauch in einem Land, Gesetze erlassen worden sein, aber gerade der den Missbrauch Verursachende ist physisch in einem anderen Land, in

⁷⁸⁵ Gaycken, 2012, S. 162f.

⁷⁸⁶ Vgl. Forgò/Helfrich/Schneider, 2019, S. 48.

⁷⁸⁷ Vgl. Gaycken, 2012, S. 163.

⁷⁸⁸ Vgl. Forgò/Helfrich/Schneider, 2019, S. 823f.

⁷⁸⁹ Vgl. Lessig, 1998, S.3.

⁷⁹⁰ Gaycken, 2012, S. 31.

dem keine entsprechenden rechtlichen Rahmenbedingungen vorhanden sind.

Nach Auffassung der Expertengruppe im Tallinn Manual hat die Verfügungsgewalt über die territorial zuordenbare Cyber Infrastruktur zur Folge, dass diese den Gesetzen des jeweiligen Staates unterliegt und sie auch durch diesen geschützt wird.⁷⁹¹ Dass die territorial zuordenbare Cyber Infrastruktur in der Regel global vernetzt ist und somit Teil von auf verschiedenen Territorien befindlichen Netzen ist, stellt keine Einschränkung der staatlichen Zuständigkeit für diese Netzteile dar.⁷⁹² Hier ist durchaus eine Loslösung vom Territorialgedanken zu sehen, weil im Umkehrschluss auch Netzteile, welche funktional einem Staat zuordenbar sind, unabhängig von ihrem Standort, der Kontrolle dieses Staates unterliegen.

Es eröffnet sich dadurch eine Kluft zwischen territorial orientierter Strafverfolgung und entterritorialisierter Souveränitätsverantwortung.⁷⁹³ Die Verfolgung von Straftaten gestaltet sich hier sehr schwierig. Bevor man aber von einer solchen sprechen kann, muss zuerst der Rechtsverletzer lokalisiert werden. Das nationale Recht hat in vielen Fällen eine internationale Dimension.⁷⁹⁴ Im Falle von kriminellen Handlungen im Netz kommt in Österreich das Cyber Strafrecht zum Einsatz. Um den Täter oder Akteur einer Strafverfolgung zuzuführen, ist oftmals eine grenzüberschreitende Maßnahme zu setzen.

Für eine Zuordnung zum jeweiligen Rechtsrahmen ist die Grenze zwischen Kriminalität und Krieg wichtig. Beim Krieg greift grundsätzlich das Humanitäre Völkerrecht. Im Bereich der Kriminalität ist das nationale Strafrecht der Ordnungsrahmen. Hier kommt der Faktor der Anonymität zum Tragen. Wenn es nicht möglich ist, ein Vergehen zuzuordnen, dann ist die Strafverfolgung unmöglich. Im Falle eines Krieges ist die Zuordnung eines feindseligen Aktes ebenso unmöglich, und eine Reaktion darauf ist nicht durchführbar, denn wenn ein Angriff im Cyberspace keinem Staat zuordenbar ist, so liegt rein rechtlich kein Krieg zwischen Staaten vor, auch wenn es sich dem Wesen nach um einen solchen handelt.⁷⁹⁵ Es ist also auf den ersten Blick, auf Grund der Anonymität, keine klare Abgrenzung zu treffen.

Ohne genaue Attribution ist eine Zuführung des Rechtsbrechers an eine zuständige Gerichtsbarkeit undenkbar. Wenn eine Zuordnung erfolgen kann, liegt der Angreifer meist nicht im Zuständigkeitsbereich des betroffenen Staates. Eine Trennung in äußere und innere Bedrohung wird hier, im rechtlichen Sinne, unscharf.

Im Cyberspace wird eine Vielzahl von Rechtsgebieten berührt. Dadurch, dass der Cyberspace ein integraler Bestandteil unseres alltäglichen Lebens geworden ist, ist er auch Teil des Rechtsalltages.⁷⁹⁶ Der Cyberspace

⁷⁹¹ Vgl. Schmitt, 2017, S. 13.

⁷⁹² Vgl. ebd., S. 14.

⁷⁹³ Vgl. ebd., S. 55ff.

⁷⁹⁴ Vgl. Gayken, 2012, S. 112.

⁷⁹⁵ Vgl. Schmitt, 2017, S. 379ff.

⁷⁹⁶ Vgl. Glenny, 2012, S. 210.

ist, auf Grund der Auswirkungen von Handlungen im Netz auf die reale Umwelt, kein rechtsfreier Raum. Bei der Frage nach dem nationalen Recht im Netz kommt man, in erster Linie mit Vergehen im Zusammenhang mit Kinderpornographie und Wiederbetätigung, im Sinne des Nationalsozialismus (NS)-Verbotsgesetzes, in Kontakt. Dies sind vor allem die in den Medien stets präsenten Themen. Daneben gibt es vor allem Betrugsdelikte, welche immer mehr begangen werden. Weiters sind Datenschutz und Persönlichkeitsrecht, das Recht im Zusammenhang mit der Identitätsproblematik oder die Meinungsfreiheit im Cyberspace relevante Rechtsbereiche im Netz.

Neben diesen nationalen „Cyber Rechtsnormen“ (Hervorhebung durch den Verfasser.) gibt es im nationalen Recht noch weitere Bestimmungen, welche sich mit verbotenen Inhalten, Missbräuchen im Zahlungsverkehr, aber auch mit gewöhnlichen Delikten beschäftigen, welche über den Cyberspace begangen werden können. Erkennbar ist, dass bei unklarer Attribution selbst Streitkräfte anderer Staaten, bei Zugriff oder Angriff auf Computersysteme in Österreich, stets im Bereich des Strafrechts agieren, sofern kein internationaler bewaffneter Konflikt vorliegt. Erst wenn eine eindeutige Zuordnung des Angriffs an eine Nation möglich ist, so begibt man sich in den Bereich des Völkerrechts. Diese Tatsache legt den Schluss nahe, dass auch in diesen, strafrechtlich relevanten Fällen, die Sicherheitsexekutive für die Strafverfolgung verantwortlich sein sollte.

Zum nationalen Recht, hier vor allem dem Strafrecht, kommt eine Vielzahl von internationalen Verträgen und Regelungen, welche einer Beachtung im Cyberspace bedürfen. Es gibt neben dem Gewaltverbot noch weitere völkerrechtliche Bestimmungen, die auf den Cyberwar angewendet werden können. Dies liegt vor allem an der Entgrenzung im Cyberspace, da viele der Interaktionen im Netz über verschiedene Staaten hinweg durchgeführt werden, wobei territoriale Souveränität und Neutralitätsrecht betroffen sind. Eine Einflussnahme auf fremde Computersysteme stellt möglicherweise eine völkerrechtlich verbotene Einmischung dar.⁷⁹⁷

Auch die unterschiedlichen Übertragungswege haben einen Einfluss auf das Völkerrecht, so etwa, wenn Satelliten für die Datenübertragung genutzt werden. Dabei werden Weltraum- und Satellitenvertragsrecht berührt. Weiters haben internationales Telekommunikationsrecht und Urheberrecht beachtet zu werden. Hinzu kommen Regelungen des Humanitären Völkerrechts (HVR), der Menschenrechtsabkommen, das Fernmeldegeheimnis, der Datenschutz, das Recht auf Informationsempfang, -beschaffung und -weitergabe, das Diplomaten- und Konsularrecht, die einen Einfluss auf die rechtliche Betrachtung des Cyberspace haben.⁷⁹⁸

In einem bewaffneten Konflikt, einem Krieg also, findet das HVR seine Anwendung. Dieser liegt dann vor, wenn ein Völkerrechtssubjekt, ein Staat, Waffengewalt, gegen den völkerrechtlich geschützten Bereich eines anderen Völkerrechtssubjekts, einsetzt, um einen politischen Zweck zu verwirklichen.

⁷⁹⁷ Vgl. Ziolkowski, 2008, S. 205. (in: Humanitäres Völkerrecht Informationsschriften, 2008)

⁷⁹⁸ Vgl. ebd., S. 206.

Wichtig dabei ist, dass diese Waffengewalt dem einen Staat auch zurechenbar ist.

Es gibt nun verschiedene Möglichkeiten einen Cyber Angriff völkerrechtlich zu kategorisieren. Zunächst ist ein Cyber Angriff dann als bewaffnete Gewalt zu werten, wenn er staatlichen Ursprungs ist und einer Gewaltanwendung nach Art. 2 Ziff. 4 der VN-Charta entspricht.⁷⁹⁹

„A cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force.“⁸⁰⁰

Da das Verfahren, welches Streitkräfte in einem Krieg im Netz zur Anwendung bringen, die sogenannten Computer Network Operations (CNO) sind, beschränkt sich die Darstellung der rechtlichen Rahmenbedingungen auf diese Form des Einsatzes militärischer Kräfte im Cyberspace.⁸⁰¹ Werden nun Cyber Operationen in einem internationalen bewaffneten Konflikt durchgeführt, unterliegen sie dem Law of Armed Conflict (LOAC). Dieser bewaffnete Konflikt liegt auch dann vor, wenn nur Cyber Operationen zwischen Staaten zur Anwendung kommen.⁸⁰²

Dabei wird davon ausgegangen, dass es sich hier um bewaffnete Gewalt im obigen Sinn handelt, der der Angegriffene wiederum nur mit Waffengewalt begegnen kann. Diese Einschätzung bedarf der Verwendung einer Waffe, wobei hier klassischerweise ein Hilfsmittel oder Werkzeug verstanden wird, welches physisch, das heißt kinetisch, auf den Menschen oder ein Objekt einwirken kann. Dies liegt bei der Verwendung von Cyber Waffen in einer CNO so nicht vor.

Bezieht man die Definition einer Waffe allerdings auf deren Wirkung, so ist mit den Verfahren der CNO (Angriff, Verteidigung und Ausnutzung) ein gleichwertiger Effekt erzielbar.⁸⁰³ Hier findet das ergebnisethische Prinzip seine Anwendung. Dies ist allerdings nicht ausreichend, um den Angriff als Verbrechen oder Krieg einordnen zu können. Eine kriminelle Handlung im Netz kann dasselbe Ergebnis zeitigen wie ein militärischer Angriff mit politischem Motiv. Es kann also nur bei einer politisch motivierten Auseinandersetzung von einem Krieg gesprochen werden. Es ist auch der Motivation Rechnung zu tragen, also ein motivationsethischer Ansatz zu wählen.

Neben der Wirkung, um festzustellen ob es sich um einen bewaffneten Angriff handelt, ist die Motivation, das Warum, von entscheidender Bedeutung, um einen Angriff im Cyberspace auch als Krieg zu klassifizieren.

⁷⁹⁹ Vgl. ebd., S. 206.

⁸⁰⁰ Schmitt, 2017, S. 330.

⁸⁰¹ Anm. d. Verf.: Die Applikation des HVR auf den Großen Cyberwar stellt eine besondere Herausforderung dar, da militärische Handlungen, auf Grund des bisher Dargestellten, in dieser Form des Virtuellen Krieges, nur schwer feststellbar sind.

⁸⁰² Vgl. Schmitt, 2017, S. 379ff.

⁸⁰³ Vgl. Ziolkowski, 2008, S. 206. (in: Humanitäres Völkerrecht Informationsschriften, 2008)

Da sich die Charta der Vereinten Nationen⁸⁰⁴ auf Nationalstaaten als Akteure bezieht und deren Handeln einen politischen Zweck verfolgt, kann davon ausgegangen werden, dass die Motivation einer Gewaltanwendung nach Art. 2 Ziff. 4 der VN-Charta im Cyberspace eine politische ist.

Um einen Cyber Angriff als bewaffnete Gewalt zu identifizieren, sind, als weitere Kategorisierungsmöglichkeit, der Vergleich und die Analogie zu biologischen und chemischen Waffen heranziehbar, deren Einwirkung ebenfalls nicht kinetischer Natur ist. Ein Cyber Angriff kann als bewaffnete Gewalt gesehen werden, wenn durch ihn bezweckt wird Menschen zu töten, zu verwunden oder aber wenn Sachwerte physisch zerstört werden sollen.⁸⁰⁵ Beides trifft zu, wenn z.B. ein Flugsteuerungssystem so manipuliert wird, dass ein Passagierflugzeug abstürzt. Diese Folgen werden, im Falle eines Angriffes im Rahmen einer CNO, mittelbar herbeigeführt.

Eine weitere Möglichkeit fasst die Verfahren einer CNO nur dann als bewaffnete Gewalt, wenn sie als sogenannte strukturelle Gewalt zur Anwendung kommt. Darunter sind physische Einwirkungen auf ein Völkerrechtssubjekt zu verstehen, welche ohne Einsatz konventioneller Waffen durchgeführt werden und der Angegriffene nur mit Waffengewalt reagieren kann.⁸⁰⁶ Diese strukturelle Gewalt ist nur dann als Gewaltanwendung im Sinne des Art. 2 Ziff. 4 der VN-Charta zu sehen, wenn sie wie ein bewaffneter Angriff wirkt, der das Selbstverteidigungsrecht nach Art. 51 der VN-Charta auslöst.⁸⁰⁷

Dies ist laut der Expertengruppe, welche das Tallinn Manual erarbeitet hat, dann der Fall, wenn der Staat durch den Angriff auf die Cyber Infrastruktur in seiner Handlungsfähigkeit eingeschränkt wird und es sich dabei um vitale Systeme (Kritische Infrastrukturen) handelt.⁸⁰⁸ Allerdings ist dies nur dann der Fall, wenn die Akteure staatlicher Natur sind. Nach Ansicht der Experten gefährden Angriffe durch nichtstaatliche Akteure die staatliche Souveränität nicht. Anders sieht dies Katja Weigelt, welche davon ausgeht, dass nichtstaatliche Akteure durchaus in der Lage sind, souveränitätsgefährdend gegen Staaten zu agieren.⁸⁰⁹ Gerade die Möglichkeiten, die der Cyberspace solchen Gruppen bietet, lässt diese Ansicht als zweckmäßig erscheinen.

Zwischen bewaffneter Gewalt und bewaffnetem Angriff besteht ein qualitativer Unterschied. Ein bewaffneter Angriff liegt dann vor, wenn die bewaffnete Gewalt eine erhebliche Intensität erreicht hat.⁸¹⁰ Da der Cyberwar im Informationsraum geführt wird, kann ein Angriff auf Daten durchaus als

⁸⁰⁴ Anm. d. Verf.: Die Charta regelt das Recht zum Krieg. Eine Klärung der Motivation ist hier ebenfalls angezeigt. Da die Charta aber als Völkerrechtssubjekte neben einigen Ausnahmen ausschließlich Nationalstaaten fasst, ist bei der darin verwendeten Begrifflichkeit des Angriffs ein politisch motivierter zu fassen.

⁸⁰⁵ Vgl. Ziolkowski, 2008, S. 206. (in: Humanitäres Völkerrecht Informationsschriften, 2008)

⁸⁰⁶ Vgl. ebd., S. 207.

⁸⁰⁷ Vgl. ebd., S. 207.

⁸⁰⁸ Vgl. Schmitt, 2017, S. 18.

⁸⁰⁹ Vgl. <https://www.faz.net/aktuell/politik/politische-buecher/terrorismus-und-souveraenitaet-auch-auf-fremdem-territorium-14117751.html>, [12.05.2020].

⁸¹⁰ Vgl. Ziolkowski, 2008, S. 207. (in: Humanitäres Völkerrecht Informationsschriften, 2008)

Anwendung bewaffneter Gewalt gewertet werden, es geht hier um die Zerstörung von Sachwerten im erweiterten Sinn, vor allem dann, wenn diese Daten unmittelbar mit der Funktion von Kritischen Infrastrukturen zusammenhängen und die Auswirkungen analog einem kinetischen Angriff sind.⁸¹¹

Die Expertendefinition aus dem Tallin Manual setzt einen Cyber Angriff einem konventionellen Angriff gleich:

„A cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects.“⁸¹²

Hier geht klar hervor, dass sich ein Cyber Angriff immer in der Realität manifestiert, entweder mittel- oder unmittelbar. Der Begriff von der Cyber Attacke ist somit weiter zu fassen, da die beschriebenen Effekte auch mittelbar eintreten können.

Ziolkowski geht allerdings davon aus, dass die Einwirkung auf Daten nicht mit der Wirkung von konventionellen Waffen vergleichbar ist. Dies stellt einen Widerspruch dar, da offensive Verfahren einer CNO nicht mittelbar, sondern unmittelbar auf Informationen wirken, also analog konventioneller Waffen in der realen Welt. Ein Angriff auf Daten der Kritische Infrastrukturen des Staates, im Rahmen einer CNO, ist daher durchaus als bewaffneter Angriff zu werten. Um diese Angriffe wiederum als Teil eines Krieges fassen zu können, ist die Motivlage mit zu berücksichtigen.

Neben der Motivlage gibt aber auch die Intensität einen Hinweis darauf, ob es sich um Krieg oder Verbrechen handelt (Anm. d. Verf.: Wenn ein einzelnes Konto angegriffen wird, bedeutet dies meist einen kriminellen Hintergrund und das Strafrecht kommt zur Anwendung; wird die komplette Finanzwirtschaft angegriffen, so kann dies als Krieg gefasst werden und das Völkerrecht ist anzuwenden.).

Der Diebstahl⁸¹³ von vitalen Daten des Staates gilt nicht als bewaffnete Gewalt, da die Spionage als solche völkerrechtlich grundsätzlich erlaubt ist.⁸¹⁴ Die Zerstörung oder langfristige Störung von Führungseinrichtungen und Kommunikationsmitteln ist als bewaffnete Gewalt in einem bewaffneten Konflikt zu benennen. Dabei ist der Einsatz von Verfahren der CNO mit der Wirkung konventioneller Waffen vergleichbar und dient einem militärischen Ziel. Obwohl das Militär auch zivile Kommunikationssysteme nutzt, ist ein Angriff auf diese dem auf militärische Einrichtungen nicht gleichzusetzen, da zivile Einrichtungen nicht generell mit militärischen gleichzusetzen sind.⁸¹⁵

Die massive Störung von kritischen Infrastrukturen (z.B. Energieversorgung, Post, Eisenbahn, Luftverkehr) kommt in der Wirkung

⁸¹¹ Vgl. Schmitt, 2017, S. 340ff.

⁸¹² Ebd., S. 415.

⁸¹³ Anm. d. Verf.: Der Diebstahl ist als Kopierung von Daten zu verstehen.

⁸¹⁴ Vgl. Ziolkowski, 2008, S. 208. (in: Humanitäres Völkerrecht Informationsschriften, 2008)

⁸¹⁵ Vgl. ebd., S. 208.

einer massiven Friedensstörung gleich, vergleichbar mit einem Einsatz von Luftmitteln zur Bombardierung. Die Wirkung würde der des Einsatzes konventioneller Waffen entsprechen und damit als Anwendung bewaffneter Gewalt gewertet, wobei zur Klassifizierung des Angriffs, als Teil eines bewaffneten Konfliktes, die Motivation, die Intention betrachtet werden muss.⁸¹⁶ Hinsichtlich des Genfer Rechts sieht Ziolkowski die Anwendung auf den Konflikt im Cyberspace ebenfalls gegeben. Sie sieht in der Auslegung des HVR den Schlüssel zur Anwendung auf den Cyberwar.

„Die Konfliktparteien, die in der Zukunft einen *cyberwar* im „virtuellen“ – und aufgrund der möglichen physischen Auswirkungen auch im materiellen – Raum führen sollten, dürfen die Zusatzprotokolle zu den Genfer Abkommen nicht als ein Überbleibsel aus einer vergangenen Zeit ansehen.“⁸¹⁷

Die Herausforderung besteht, bei der Applikation der verschiedenen Rechtsnormen auf Angriffe im Cyberspace, darin, zu erkennen wer und aus welchem Grund dieser einen Angriff durchführt. Die Frage nach dem Akteur und seiner Motivation, aber auch nach der Intensität eines Angriffes, ist hier von entscheidender Bedeutung, um Cyber Attacken rechtlich zuordnen zu können. Entsprechend dieser Zuordnung ist dann die Verantwortung zuzuweisen.

8.2 Zum Cyberwar im Völkerrecht

War der Krieg früher ein Rechtsetzungsmittel zwischen den Gemeinwesen⁸¹⁸, kamen in jüngster Vergangenheit die Ächtung des Krieges und die völkerrechtliche Verankerung eines Kriegs- und Gewaltverbotes zum Tragen.⁸¹⁹ Das Gewaltverbot ist in den Satzungen der Vereinten Nationen festgeschrieben:

„Alle Mitglieder unterlassen in ihren internationalen Beziehungen jede gegen die territoriale Unversehrtheit oder die politische Unabhängigkeit eines Staates gerichtete oder sonst mit den Zielen der Vereinten Nationen unvereinbare Androhung oder Anwendung von Gewalt.“⁸²⁰

Dieses Gewaltverbot hebt das Souveränitätsrecht zur freien Entscheidung des Staates zum Krieg auf.⁸²¹ Damit wird der rechtliche Zustand des Krieges nicht mehr als Rechtsdurchsetzungsmaßnahme gesehen, sondern geht im System Kollektiver Sicherheit auf. Zudem wird versucht Konflikte unterhalb der Kriegsschwelle auszutragen.⁸²² Diese Form der Auseinandersetzung wird auch als hybrider Konflikt bezeichnet. Eine in diesem Zusammenhang oft genutzte Form der Konfliktaustragung findet im

⁸¹⁶ Vgl. ebd., S. 209.

⁸¹⁷ Vgl. ebd., S. 213.

⁸¹⁸ Vgl. Pesendorfer, 1982, S. 101. (in: Neisser, 1982)

⁸¹⁹ Vgl. Neuhold/Hummer/Schreuer, 1991, S. 4.

⁸²⁰ Charta der Vereinten Nationen, Kapitel I, Artikel 2, Absatz 4.

⁸²¹ Vgl. Spinoza, Politischer Traktat, S.28.

⁸²² Vgl. Bilban/Grininger, 2019, S. 42.

Cyberspace statt. Hier liegt die Notwendigkeit den Cyberspace auch aus völkerrechtlicher Sicht zu betrachten.

Die Entstehung des Völkerrechts beruht auf der Interaktion der Gemeinwesen, es fußt auf der konkreten Auseinandersetzung zwischen verschiedenen Willen. Dabei werden Räume der Interaktion, im zwischenstaatlichen Bereich, zu Rechtsräumen im völkerrechtlichen Sinn.⁸²³ Dort wo Menschen im Rahmen der Gemeinwesen wirksam werden, wie zum Beispiel im Weltraum, werden Regelungen zur Eindämmung möglicher Rivalitäten getroffen.

Ziel des Völkerrechts ist die Schaffung eines Gleichgewichts, wie es schon Machiavelli als notwendig erkannt hatte. Ohne eine rechtliche Normierung dieses Zustandes, wird es weiterhin Kriege geben, so seine Schlussfolgerung.⁸²⁴ Konnten Staaten früher Probleme für sich lösen, so ist auf Grund der steigenden internationalen Komplexität, eine Problemlösung nur noch unter Einbindung aller Akteure möglich. Die Schaffung eines von allen Völkerrechtssubjekten anerkannten Rechts, zur Regelung der Beziehungen untereinander, ist hier der Lösungsansatz.

Wichtig hierfür ist die Herausbildung von Grenzen, die den gemeinschaftlichen Teil vom individuellen Teil trennen. Diese Trennung ist das Hauptmerkmal der staatlichen Souveränität und Ausdruck der Befehlsgewalt nach innen und der Unabhängigkeit nach außen.⁸²⁵ Durch immer neue Technologien und eine zunehmende globale Vernetzung, einer Steigerung der Komplexität, wird diese Grenzziehung immer problematischer. Staaten haben es immer schwerer die Sicherheit nach innen und außen aufrecht zu erhalten. Um Bedrohungen, die auf Grund der Komplexität alle treffen können, zu minimieren, bieten die Vereinten Nationen ein System der Kollektiven Sicherheit.

8.2.1 Das Völkerrecht und der bewaffnete Konflikt

Zunächst geht es darum herauszufinden, welche Aspekte des Völkerrechts für den Krieg im Allgemeinen und für den Cyberwar im Speziellen von Relevanz sind. Hier ist die Unterscheidung in das Recht zum Krieg (*ius ad bellum*) und das Recht im Krieg (*ius in bello*) zu berücksichtigen. Ersteres wird grundsätzlich durch die Satzung der VN geregelt. Hier finden sich keine spezifischen Inhalte zum Cyberwar. Es ist daher davon auszugehen, dass die Charta der VN beim Krieg im Cyberspace in Analogie zur Anwendung gelangen muss. Besonders interessant ist die Frage, wann und ob eine Cyber Attacke einen bewaffneten Angriff darstellt oder eben nicht.⁸²⁶ Basierend darauf greifen dann die Bestimmungen der Satzungen der VN. Vor allem geht es um das Selbstverteidigungsrecht nach Artikel 51 der Charta und damit verbunden auch um die Maßnahmen, die durch einen

⁸²³ Vgl. Neuhold/Hummer/Schreuer, 1991, S. 5.

⁸²⁴ Vgl. Machiavelli, Discorsi, S. 28.

⁸²⁵ Vgl. Neuhold/Hummer/Schreuer, 1991, S. 7.

⁸²⁶ Anm. d. Verf.: Hier gibt es unterschiedliche Auslegungen des Begriffes vom bewaffnete Angriff im Cyberspace. (Vgl. Kapitel 7.1.1) Passend und durchaus in Analogie zur Charta der VN erscheint die Definition im Tallin Manual. (Vgl. Kapitel 8.1)

Attackierten ergriffen werden dürfen. Die Kernfrage ist also, ob ein bewaffneter Angriff vorliegt. Ein solcher ist jedoch nicht gleichbedeutend mit einem bewaffneten Konflikt.⁸²⁷ Dieser ist jedoch Vorbedingung für die Anwendung des *ius in bello*.

Ein bewaffneter Angriff ist also nicht zwingend Auslöser eines bewaffneten Konfliktes.⁸²⁸ Hier sind vor allem der Organisationsgrad der bewaffneten Gruppierung und die Intensität der Auseinandersetzung zu beurteilen.⁸²⁹ Handelt es sich schließlich um einen bewaffneten Konflikt, kommen die Haager Landkriegsordnung, die Genfer Abkommen, sowie die Zusatzprotokolle zu diesen Abkommen zum Tragen. Diese Regelungen werden im Allgemeinen als Humanitäres Völkerrecht (*ius in bello*) bezeichnet. Da dieses Regelwerk sich nicht explizit mit dem Cyberwar beschäftigt, findet es in der Cyberdomäne, wie bereits festgestellt, nur in Analogie seine Anwendung. Die Prinzipien des HVR sind also im Cyberspace ebenso zu berücksichtigen.⁸³⁰

Problembereiche für die Umsetzung des HVR im Cyberwar sind die Spezifika des Cyberraumes. Zusätzlich zur Herausforderung der Erkennung eines bewaffneten Angriffs in dieser Domäne, kommen die Schwierigkeit der Identifikation der Akteure und damit deren Kennzeichnung zur Unterscheidung zum Tragen.⁸³¹ Auch die Prinzipien der Begrenzung und Verhältnismäßigkeit stellen das Militär als Hauptakteur im Krieg, auch in einem Cyberwar, vor große Probleme.⁸³² Die Frage, ob nichtstaatliche Akteure souveränitätsgefährdend wirken können, steht technisch, aber nicht rechtlich, außer Frage. Hier besteht Regelungsbedarf, um dem Militär und damit den Staaten, welche es einsetzen, Handlungssicherheit zu geben.⁸³³

Bei inneren Unruhen und Spannungen tritt der jeweilige nationale Rechtsrahmen in den Vordergrund. Hier gibt es, wie im weiteren Verlauf am Beispiel Österreichs noch gezeigt wird, eine Fülle von Normen, die sich mit dem Cyberspace beschäftigen.⁸³⁴ Nun wird im Folgenden den allgemeinen Herausforderungen des Völkerrechts, in Bezug auf den Krieg und damit auch auf den Cyberwar, nachgegangen.

Vergleichbar mit dem Staat, der durch das Gewaltmonopol den einzelnen Bürger von seiner Verpflichtung zur Erhaltung im Dasein befreit, soll das Völkerrecht durch Regelungen, gegen Friedensbrecher und andere

⁸²⁷ Vgl. Edlinger, Karl: Die völkerrechtliche Klassifizierung bewaffneter Konflikte. Konflikttypen, Abgrenzungen sowie Rechtsfolgen und deren Auswirkungen auf die Planung und Durchführung militärischer Operationen, Frankfurt am Main 2016, S. 46f.

⁸²⁸ Vgl. ebd., S. 47.

⁸²⁹ Vgl. ebd., S. 47.

⁸³⁰ Vgl. Fazal, Tanisha M.: [Kein] Recht im Krieg? Nicht intendierte Folgen der völkerrechtlichen Regelung bewaffneter Konflikte, Hamburg 2019, S. 370.

⁸³¹ Vgl. International Committee of the Red Cross (Hrsg.): Handbook on international Rules governing military Operations, Genf 2013, S. 54.

⁸³² Vgl. ebd., S. 54f.

⁸³³ Vgl. Fazal, S. 371.

⁸³⁴ Anm. d. Verf.: Die militärische Landesverteidigung in Österreich tritt aber nicht nur im Falle eines Krieges, sondern auch bei Vorgängen im Inneren – analog zu internen Unruhen und Spannungen – in Kraft. Hier wirkt zunächst vorrangig nationales Recht. (Vgl. Kapitel 8.4.5)

Bedrohungen, die einzelnen Staaten von der gewaltsamen Selbsthilfe befreien. Das Problem ist, dass auf völkerrechtlicher Ebene ein Rechtsdurchsetzungsorgan fehlt. Daher sind diese Regelungen von der Mitwirkung der Staaten abhängig. Nach Phasen der Einhegung des bewaffneten Konfliktes, zum Beispiel als rein politisches Instrument zur Zeit der Kabinettskriege, welche durch die Französische Revolution beendet wurden, folgten zusehends Phasen der Entgrenzung von Konflikten. Der Zweite Weltkrieg stellte den letzten negativen Höhepunkt, hinsichtlich der Entgrenzung, in Europa dar.

Vor allem auf substaatlichem Niveau kommt es vermehrt zu bewaffneten Konflikten, die sich einer Regelung durch das Völkerrecht weitgehend entziehen. Die Bildung von Kriegsökonomien involviert einen Großteil der Menschen in den betreffenden Regionen in diese Konflikte. Ein weiterer Faktor stellt die Begrenzung des Gewaltverbotes auf die Anwendung von Waffengewalt dar, weil dadurch andere Machtmittel weiterhin einsetzbar bleiben.⁸³⁵ Die Verflechtung auf globaler Ebene schafft die Möglichkeit mit wirtschaftlichen und anderen Mitteln Druck auszuüben.

Die Möglichkeit auf andere Weise Druck auszuüben, hat den bewaffneten Konflikt in den internationalen Beziehungen nicht gänzlich beseitigt. Selbst Waffen mit ungeheurer Zerstörungskraft haben die internationale Zusammenarbeit nicht so weit vorangetrieben, dass Konflikte nicht mehr vorkommen. Gewaltanwendung auf internationaler Basis ist drei möglichen Kategorien unterzuordnen: Entweder ist die Gewaltanwendung rechtswidrig, erlaubt im Sinne der Selbstverteidigung oder aber eine zulässige Sanktion, welche durch den Sicherheitsrat der VN festgelegt wurde.

Die Selbstverteidigung ist in den Satzungen der VN folgendermaßen definiert:

„Diese Charta beeinträchtigt im Falle eines bewaffneten Angriffs gegen ein Mitglied der Vereinten Nationen keineswegs das naturgegebene Recht zur individuellen oder kollektiven Selbstverteidigung, bis der Sicherheitsrat die zur Wahrung des Weltfriedens und der internationalen Sicherheit erforderlichen Maßnahmen getroffen hat.“⁸³⁶

Dieses Recht besteht also solange, bis der Sicherheitsrat Maßnahmen trifft, um diese Situation zu bereinigen. Eine präventive Selbstverteidigung in Erwartung eines Angriffes ist nicht zulässig, der Artikel 51 darf also nur reaktiv zur Anwendung gebracht werden. Diese Maßnahmen können die Anwendung von Gewalt in unterschiedlicher Form beinhalten und sind wie folgt definiert:

„Der Sicherheitsrat kann beschließen, welche Maßnahmen - unter Ausschluß von Waffengewalt - zu ergreifen sind, um seinen Beschlüssen Wirksamkeit zu verleihen; er kann die Mitglieder der Vereinten Nationen auffordern, diese Maßnahmen durchzuführen. Sie

⁸³⁵ Vgl. Neuhold/Hummer/Schreuer, 1991, S. 18.

⁸³⁶ Charta der Vereinten Nationen, Kapitel VII, Artikel 51.

können die vollständige oder teilweise Unterbrechung der Wirtschaftsbeziehungen, des Eisenbahn-, See- und Luftverkehrs, der Post-, Telegraphen- und Funkverbindungen sowie sonstiger Verkehrsmöglichkeiten und den Abbruch der diplomatischen Beziehungen einschließen.“⁸³⁷

Weiter kann der Einsatz militärischer Kräfte zur Beseitigung des Zustandes herangezogen werden:

„Ist der Sicherheitsrat der Auffassung, daß die in Artikel 41 vorgesehenen Maßnahmen unzulänglich sein würden oder sich als unzulänglich erwiesen haben, so kann er mit Luft-, See- oder Landstreitkräften die zur Wahrung oder Wiederherstellung des Weltfriedens und der internationalen Sicherheit erforderlichen Maßnahmen durchführen. Sie können Demonstrationen, Blockaden und sonstige Einsätze der Luft-, See oder Landstreitkräfte von Mitgliedern der Vereinten Nationen einschließen.“⁸³⁸

Der Artikel VII der Satzungen der VN stellt somit das System Kollektiver Sicherheit dar. Diese Regelungen in den Satzungen der VN sind jene rechtlichen Grundlagen, die einen Einsatz von Gewalt regeln. Sie greifen allerdings nur in den internationalen Beziehungen und nicht im Falle eines innerstaatlichen bewaffneten Konfliktes, eines Bürgerkrieges.⁸³⁹ Ist ein bewaffneter Konflikt ausgebrochen, so treten weitere völkerrechtliche Regelungen in Kraft, welche im Humanitären Völkerrecht zusammengefasst sind.

Zweck des HVR ist es, Kriege methodisch und technologisch zu begrenzen. Die Idee hinter dem HVR ist es, Regeln für den Schutz von Personen und Regeln für Beschränkung von Mitteln und Methoden bereitzustellen, um unnötige Leiden zu verhindern. Das Recht der bewaffneten Konflikte wird durch zwei große Rechtsmaterien gebildet, das Genfer und das Haager Abkommen. Das erste dient dem Schutz der Opfer des Krieges, das zweite behandelt Methoden und Mittel des Krieges.⁸⁴⁰ Ergänzt wurden diese beiden Rechtsbestände durch verschiedene Konventionen, die auf die Entwicklung von Waffen und Methoden im Laufe der Zeit eingehen.

⁸³⁷ Ebd., Kapitel VII, Artikel 41.

⁸³⁸ Ebd., Kapitel VII, Artikel 42.

⁸³⁹ Vgl. Neuhold/Hummer/Schreuer, 1991, S. 302.

⁸⁴⁰ Vgl. ebd., S. 434ff.

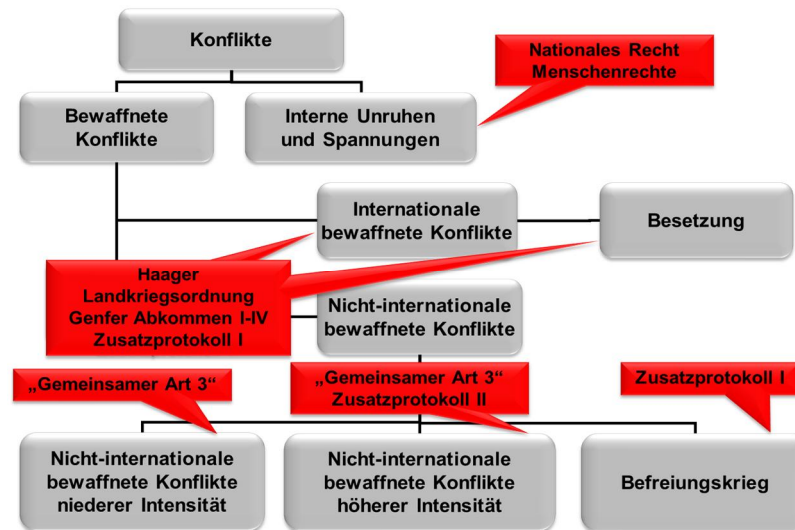


Abbildung 16: Anwendungsbereich des HVR⁸⁴¹

Das HVR orientiert sich an einigen grundlegenden Prinzipien, wie der Begrenzung, der Unterscheidung, der Verhältnismäßigkeit, der militärischen Notwendigkeit, dem Vertrauen und der menschlichen Behandlung und dem Diskriminierungsverbot.⁸⁴² Während die Satzungen der Vereinten Nationen das Recht zum Krieg regeln, regelt das HVR das Recht im Krieg. Wann welches Recht zum Tragen kommt, hängt von der Art des bewaffneten Konfliktes ab und ist auch am Innen und Außen von Staaten orientiert. Die Raumdimension ist also ein wesentlicher Faktor dafür, wann welches Recht zur Anwendung kommt.

Um mit dem Cyberwar im Rahmen des Völkerrechts adäquat umzugehen, muss die Sicht der einzelnen Staaten auf diese Thematik miteinbezogen werden. Im Folgenden ist es daher notwendig die einzelnen Sichtweisen, hinsichtlich der Sicherheit im Cyberspace, darzustellen, um sowohl Trennendes wie auch Einendes zwischen den Staaten besser einordnen zu können. Die nationalen Strategien zur Cyber Sicherheit geben Aufschluss darüber, wie die Staaten mit Gefahren aus dem Netz umzugehen gedenken, und ob es hier Gemeinsamkeiten über die Grenzen hinweg gibt.

8.2.2 Nationale Strategien zur Cyber Sicherheit

Strategien sind Absichtserklärungen und Zielvereinbarungen der Staaten, zur Stärkung von verschiedenen Politikbereichen. Sie sind oftmals Ausgangspunkt von Rechtsetzungsverfahren zur Erfassung und Abdeckung von Bereichen, die einer entsprechenden Gesetzgebung bedürfen. In diesem Zusammenhang ist die Betrachtung dieser nationalen Strategien zur Cyber Sicherheit für die Bildung von nationalrechtlichen und völkerrechtlichen Normen von Bedeutung. Im Falle der Nationalen Cyber Strategien ist festzuhalten, dass

⁸⁴¹ Abbildung durch Dr. Karl Edlinger erstellt.

⁸⁴² Anm. d. Verf.: Diese Prinzipien finden sich über das gesamte HVR verteilt.

„National cyber security strategies (NCSS) are used to provide guidance to policy-makers and other stakeholders regarding cyber security policy priorities and potential resource allocations. They can also form an important part of a nation's declaratory policy.“⁸⁴³

Die International Telecommunication Union (ITU) hat, als Hilfestellung zur Erstellung einer nationalen Cyber Sicherheitsstrategie, einen Wegweiser herausgebracht. Dabei appelliert die ITU an die Staaten, die diesen Wegweiser verwenden wollen, ihre nationalen Werte als Basis für die Erstellung einer Strategie zu verwenden. Dies soll aus folgenden Gründen so durchgeführt werden:

„Firstly, culture and national interests influence the perception of risk and the relative success of defences against cyber threats. Secondly, a strategy rooted in national values is likely to gain support of stakeholders such as the judiciary and private sector.“⁸⁴⁴

Die Wahrnehmung von Gefahren ist kulturabhängig und die Bedarfsträger sind an die nationalen Werte gebunden. Dennoch gibt die ITU eine grobe Gliederung vor. Dabei lassen sich die drei Kernelemente einer Strategie wiederfinden. Es handelt sich um den Zusammenhang zwischen Ziel, Weg und Mittel. Betrachtet man die verschiedenen nationalen Strategien, die in dieser Arbeit miteinander verglichen werden, so sind diese drei Parameter jene, die eine Vergleichbarkeit erst ermöglichen. Dabei liegt der Fokus des Vergleiches auf dem Bereich Cyber Defence bzw. der militärischen Cyber Security.

Zum Vergleich wurden die Cyber Sicherheitsstrategien folgender Staaten herangezogen: Australien, Kanada, Deutschland, Frankreich, Großbritannien, Österreich und die Vereinigte Staaten von Amerika. Der Vergleich wird an den oben genannten Faktoren ausgerichtet. Die unterschiedlichen quantitativen Ansätze bei den verschiedenen Strategien haben den Blick vor allem auf die Prioritäten und Aktionen der einzelnen Staaten gelenkt. Mit Prioritäten meint die ITU die Wege der Nationen, ihre strategischen Ziele zu erreichen und mit Aktionen, die dafür einzusetzenden Mittel. Der Vergleich der Strategien zielt vor allem auf die Rolle des Militärs in den jeweiligen Strategien ab. Dabei werden die Strategien auch hinsichtlich ihrer Weiterentwicklung betrachtet. Der Vergleich zwischen früheren und aktuellen Strategien gibt Aufschluss darüber, wie die einzelnen Staaten die Kompetenzverteilung hinsichtlich der Bedrohungen aus dem Cyberspace auffassen.

Grundsätzlich lassen sich bei den Prioritäten fünf große Bereiche festlegen: Legistische, technische bzw. prozessuale, strukturelle Maßnahmen, sowie Fähigkeitenaufbau und internationale Kooperation. Zu diesen Wegen gibt es – in der Umsetzung – die Zuweisung der entsprechenden Mittel. Dieser Aufbau, orientiert an den Vorgaben der ITU, schafft die Möglichkeit einen Vergleich anzustellen. Augenscheinlich ist, dass die Strategien vor allem den Bereich der Kriminalität im Netz abdecken. Den

⁸⁴³ Klimburg, 2012, S. 44.

⁸⁴⁴ ITU, National Cybersecurity Guide, 2011, S. 5.

Krieg im Netz behandeln die Strategien nur im entferntesten Sinne. So finden wir in der Österreichischen Strategie für Cyber Sicherheit (ÖSCS) den Hinweis, dass sich das Militär um den Eigenschutz der eigenen Netze kümmert und, im Falle der militärischen Landesverteidigung, zum Schutz der Souveränität Österreichs die Federführung übernimmt.⁸⁴⁵

Die Cyber Security Strategy Australiens sieht den Einsatz der militärischen Kräfte im Cyberspace, des Australian Signals Directorate (ASD), vor allem im Schutz der sensiblen Regierungsnetze und zur Assistenzleistung vor, verfolgt also einen ähnlichen Ansatz wie die ÖSCS.⁸⁴⁶ Die grundsätzliche Ausrichtung der australischen Strategie hat sich dabei im Bezug auf die Rolle des Militärs nicht wesentlich verändert.⁸⁴⁷ Kanada weist dem Departement of National Defence ebenfalls den Eigenschutz und die Assistenzleistung für andere Regierungsstellen zu.⁸⁴⁸ In der aktuellen nationalen kanadischen Cyber Strategie findet sich keine Information zur Rolle des Militärs, der Fokus liegt hier in der verstärkten Einbindung der Betreiber Kritischer Infrastrukturen, des privaten Sektors, sowie lokaler und regionaler Regierungseinrichtungen.⁸⁴⁹

Die deutsche Strategie von 2011 unterscheidet klar zwischen militärischer und ziviler Cyber Sicherheit und weist dem militärischen Bereich den Eigenschutz zu.⁸⁵⁰ Die Rolle des Militärs wird im Strategiepapier von 2016 noch mehr detailliert:

„Cyber-Verteidigung umfasst die in der Bundeswehr im Rahmen ihres verfassungsmäßigen Auftrages und dem völkerrechtlichen Rahmen vorhandenen defensiven und offensiven Fähigkeiten zum Wirken im Cyber-Raum, die zur Einsatz- und Operationsführung geeignet und erforderlich sind oder zur Abwehr von (militärischen) Cyber-Angriffen und damit dem Schutz eigener Informationen, IT, sowie Waffen- und Wirksysteme dienen.“⁸⁵¹

Die französische Cyber Strategie aus dem Jahr 2011 sticht hier etwas heraus. Zum einen stellt sie die Cyber Defence in den Mittelpunkt, in dem sie das erste von vier strategischen Zielen wie folgt definiert:

„While maintaining its strategic independence, France must work to ensure that it belongs to the inner circle of leading nations in the area of cyberdefence.“⁸⁵²

Zum anderen definiert sie den Begriff Cyber Defence, anders als die anderen Nationen, sehr weit gefasst:

⁸⁴⁵ Vgl. BKA, Österreichische Strategie für Cyber Sicherheit (ÖSCS), 2013, S. 11.

⁸⁴⁶ Vgl. Australian Government, Cyber Security Strategy, 2009, S. 29.

⁸⁴⁷ Vgl. Australian Government, Cyber Security Strategy, 2016, S. 30ff.

⁸⁴⁸ Vgl. Government of Canada, Canada's Cybersecurity Strategy, 2010, S. 10.

⁸⁴⁹ Vgl. Public Safety of Canada, National Cyber Security Strategy, 2018, S. 6.

⁸⁵⁰ Vgl. BMI, Cyber-Sicherheitsstrategie für Deutschland, 2011, S. 15.

⁸⁵¹ BMI, Cyber-Sicherheitsstrategie für Deutschland, 2016, S. 46.

⁸⁵² French Network and Information Security Agency (ANSSI), Information systems defence and security, France's strategy, 2011, S. 7.

„The set of all technical and non-technical measures allowing a State to defend in cyberspace information systems that it considers to be critical.“⁸⁵³

In der Weiterentwicklung der Strategie aus dem Jahr 2015 findet sich die Cyber Defence noch immer an oberster Stelle von nunmehr fünf strategischen Zielsetzungen. Zu beobachten ist allerdings, dass der Schutz Kritischer Infrastrukturen und der Wirtschaft in den Fokus gerückt sind.⁸⁵⁴ Auch lässt Frankreich in beiden Strategien eine genaue Zuordnung von Zuständigkeiten weg, in dem immer vom Staat als Ganzem gesprochen wird. Für die Belange der Cyber Defence wurde die Nationale Agentur für Sicherheit der Informationssysteme (ANSSI), ein staatliches Instrument, geschaffen.

Die britische Strategie von 2011 sieht das Verteidigungsressort federführend in der Fähigkeit, die britischen Interessen im Cyberspace zu schützen. Darin sind folgende Aufgaben enthalten: Zum einen die Erkennung von Gefahren im Netz und zum anderen die Fähigkeit der Abschreckung und Abwehr von Angriffen.⁸⁵⁵ Großbritannien verfügt ähnlich wie Frankreich über eine eigene Behörde, die für die Belange der Cyber Defence zuständig ist, das Government Communications Headquarters (GCHQ), einen militärischen Nachrichtendienst, der in Bezug auf die Cyber Security dem Außenminister untersteht.⁸⁵⁶ Die National Cyber Security Strategy aus dem Jahr 2016 spricht von einer Active Cyber Defence (ACD), welche sowohl Cybercrime als auch Angriffe und Bedrohungen im Cyberspace durch andere Staaten zerschlagen soll.⁸⁵⁷ Diese ACD wird durch das National Cyber Security Centre durchgeführt und koordiniert und liegt in der gesetzlichen Verantwortung des Außenministeriums.⁸⁵⁸ Dem Militär fällt in Großbritannien die Rolle der Entwicklung offensiver Fähigkeiten im Cyberspace zu, um gemeinsam mit dem GCHQ diese Fähigkeiten weiter auszubauen.⁸⁵⁹

Die Vereinigten Staaten von Amerika verfügen über eine Fülle von staatlichen Einrichtungen und Organisationen, welche jede für sich über eine eigene Cyber Sicherheitsstrategie verfügen. Betrachtet werden im Folgenden die Strategien des Weißen Hauses, des Department of Homeland Security und des Department of Defense. Die Strategie des Weißen Hauses von 2003 ist das älteste Dokument im Vergleich, geht aber als einziges konkret auf den Cyberwar ein. Es deckt sogar beide Formen des Cyberwar, auf die in der militärwissenschaftlichen Untersuchung dieses Phänomens näher eingegangen wurde, ab. In der Schilderung möglicher Bedrohungen wird auf den Cyberwar im Großen, der auch schon im Frieden beginnt, und den Angriff auf militärische Systeme, den Kleinen Cyberwar, eingegangen.

⁸⁵³ Ebd., S. 21.

⁸⁵⁴ Vgl. Secrétariat général de la Défense et de la Sécurité nationale (SGDSN), French National Digital Security Strategy, 2015, S. 14.

⁸⁵⁵ Vgl. Cabinet Office, The UK Cyber Security Strategy, 2011, S. 39.

⁸⁵⁶ Vgl. Cabinet Office, National Cyber Security Strategy 2016-2021, Progress Report, 2019, S. 23.

⁸⁵⁷ Vgl. HM Government, National Cyber Security Strategy 2016-2021, 2016, S. 33.

⁸⁵⁸ Vgl. Cabinet Office, National Cyber Security Strategy 2016-2021, Progress Report, 2019, S. 23.

⁸⁵⁹ Vgl. ebd., S. 9.

„We face adversaries, including nation states and terrorists, who could launch cyber attacks or seek to exploit our systems. In peacetime America's enemies will conduct espionage against our government, university research centers, and private companies. Activities would likely include mapping U.S. information systems, identifying key targets, lacing our infrastructure with “back doors” and other means of access. In wartime or crisis, adversaries may seek to intimidate by attacking critical infrastructures and key economic functions or eroding public confidence in information systems. They may also attempt to slow the U.S. military response by disrupting systems of the Department of Defense (DoD), the Intelligence Community, and other government organizations as well as critical infrastructures.“⁸⁶⁰

Die Hauptträger des Krieges im Netz sind, mit dem Verteidigungsministerium und den Nachrichtendiensten, eindeutig benannt. Als Maßnahmen definiert die Strategie folgende Aktionen:

„The intelligence community, DoD, and the law enforcement agencies must improve the Nation's ability to quickly attribute the source of threatening attacks or actions to enable timely and effective response. Consistent with the National Security Strategy, these efforts will also seek to develop capabilities to prevent attacks from reaching critical systems and infrastructures.“⁸⁶¹

Es muss hier nochmals hervorgestrichen werden, dass die Vereinigten Staaten von Amerika über eine große Anzahl an strategischen Dokumenten für die Bewältigung von Cyber Bedrohungen verfügen.⁸⁶² Dies zeigt die Bedeutung, die das Thema Cyber Security für die USA einnimmt. Im National Cyber Incident Response Plan (NCIRP) 2010 wird die Verantwortung des Militärs wie folgt festgelegt:

„Among other missions, DoD establishes and maintains shared situational awareness and directs the operation and defense of the .mil network.“⁸⁶³

Wieder steht der Eigenschutz der militärischen Systeme im Vordergrund, wobei zu den Zuständigkeiten der Streitkräfte noch zählt, dass die Elemente, die verantwortlich sind

„[...] for computer security and computer network defense of DoD systems may exercise those duties in support of the national response effort in four primary roles: (1) Defense Support of Civil Authorities; (2) intelligence and information sharing, (3) law enforcement investigations, and (4) military operations to defend the homeland.“⁸⁶⁴

⁸⁶⁰ The White House, The National Strategy to Secure Cyberspace, 2003, S. 49f.

⁸⁶¹ Ebd., S. 50.

⁸⁶² Anm. d. Verf.: Hier wären die International Strategy for Cyberspace des Weißen Hauses, die Strategien des DHS und der National Cyber Incident Response Plan (NCIRP), sowie die Department of Defense Strategy for Operating in Cyberspace zu nennen.

⁸⁶³ DHS, National Cyber Incident Response Plan (NCIRP), 2010, S. 6.

⁸⁶⁴ Ebd., S. 6.

Der Eigenschutz der militärischen Netze zur Aufrechterhaltung der Einsatzfähigkeit der amerikanischen Streitkräfte ist auch für das Weiße Haus 2011 außer Frage gestellt.⁸⁶⁵ Die Rolle des Militärs ist seitens des Departments of Homeland Security vor allem darin zu sehen, als Partner gemeinsam den Bedrohungen aus dem Netz entgegenzutreten.⁸⁶⁶ Die Cyber Strategy des Department of Defense greift diese Aufgaben für das Militär auf und sieht mit Priorität den Eigenschutz an erster Stelle. Eine hohe Bedeutung kommt in diesem Dokument auch der Unterstützung anderer staatlicher Akteure im Kampf gegen Bedrohungen im Cyberspace zu.⁸⁶⁷ Im NCIRP 2016 finden sich die Aufgaben für das Militär in unveränderter Form.

„DoD is responsible for threat response to cyber incidents affecting DoD assets and the DoD Information Network (DoDIN). DoD can also support civil authorities for cyber incidents outside the DoDIN when requested by the lead federal agency, and approved by the appropriate DoD official, or directed by the President. Such support would be provided based upon the needs of the incident, the capabilities required, and the readiness of available forces.“⁸⁶⁸

Die Strategie des Department of Homeland Security sieht in der Fassung von 2018 den Schutz der souveränitätsrelevanten Systeme in der eigenen Verantwortung.⁸⁶⁹ Diese Sichtweise muss aber im Zusammenhang mit den Aufgabenzuordnungen im NCIRP gesehen werden. Es lässt sich hier klar ableiten, dass die Verantwortung für die strategische Ausprägung des Cyberwar, aber natürlich auch für die Cybercrime, in den USA nicht beim Militär, sondern bei anderen Einrichtungen des Staates liegen. Dies wird in der National Cyber Strategy des Weißen Hauses von 2018 nochmals untermauert.⁸⁷⁰ Die Zuständigkeiten sind ähnlich denen, die in der ÖSCS für das BMLVS festgelegt wurden. In fast allen Strategien, die hier miteinander verglichen wurden, steht für das Militär der Eigenschutz an erster Stelle, die Assistenzleistung, für andere Behörden oder Bedarfsträger, ist die Zusatzleistung militärischer Cyber Kräfte.

Nur die amerikanische Cyber Strategie behandelt den Cyberwar in seinen beiden Ausprägungen und definiert Maßnahmen dafür. Die strategischen Ziele sind durchwegs unterschiedlich, jedoch wurde durch die Beziehung auf die ITU Richtlinie zur Erstellung einer nationalen Cyber Strategie, im Bereich der Wege und Mittel, eine weitgehende Übereinstimmung der verschiedenen Strategien erzielt.

Die Ausrichtung der Cyber Strategien erfolgt vor allem an der Bedrohung durch Cyber Kriminalität und Cyber Terrorismus. Das dem Militär nur wenig Raum in den vorliegenden Strategien gegeben wird, liegt vor allem an einem Whole of Nation Approach (WoNA), der der Bewältigung

⁸⁶⁵ Vgl. The White House, International Strategy for Cyberspace, 2011, S. 20.

⁸⁶⁶ Vgl. DHS, The Cybersecurity Strategy for the Homeland Security Enterprise, 2012, S. 7.

⁸⁶⁷ Vgl. Department of Defense, Cyber Strategy, 2015, S. 3.

⁸⁶⁸ DHS, National Cyber Incident Response Plan (NCIRP), 2016, S. 14.

⁸⁶⁹ Vgl. DHS, Cybersecurity Strategy, 2018, S. 8f.

⁸⁷⁰ Vgl. The White House, National Cyber Strategy of the United States of America, 2018, S. 6.

von Bedrohungen aus dem Netz zu Grunde liegt. Dies spiegelt die strategische Bedeutung der Thematik wider. Die Bedeutung ist auch an der weltweit großen Zahl bereits verfügbarer Strategien zur Thematik zu erkennen. Nach der Auseinandersetzung mit den Cyber Sicherheitsstrategien wird klar, dass vor allem die Bedrohung durch Kriminalität und Terrorismus im Fokus steht, also Bedrohungen, die kaum Wert auf Anonymität legen.

8.3 Zum Cyberwar im Europarecht

Die Europäische Union als Gemeinschaft von hochentwickelten Industrienationen sieht sich angesichts der steigenden Bedrohung durch und aus dem Cyberspace besonderen Herausforderungen gegenüber. Die Mitgliedsstaaten haben die Verpflichtung europäische Entschlüsse in ihr nationales Recht zu übertragen, doch steht die Union allgemein vor der Aufgabe diese Normen im Konsens zu definieren.

Welche über das Völkerrecht hinausgehenden Rechtsinhalte sind hier formuliert und letztlich schon implementiert? Dies sind die zentralen Fragestellungen, wenn man sich dieser Thematik annehmen möchte. Kern der Diskussion bleibt dabei die Abgrenzung zwischen Kriminalität und Krieg auf der einen Seite und andererseits die Frage nach der Kompetenzverteilung innerhalb der Union.

Die Gemeinsame Sicherheits- und Verteidigungspolitik ist die Basis für diese Überlegungen. Sie definiert zum einen, was Teil dieses Politikfeldes der Union ist, und andererseits liefert sie die Grundlage für die Ausrichtung der nationalen Streitkräfte der Mitgliedsstaaten. Dabei geht es um die grundsätzlichen Einsatzszenarien ohne diese genauer zu spezifizieren.

8.3.1 Die Gemeinsame Sicherheits- und Verteidigungspolitik und der Cyberwar

Die Basis für die europarechtliche Untersuchung des Cyberwar liefern die Vertragswerke der Europäischen Union (EU), allen voran der Vertrag von Lissabon. Da es sich beim Cyberwar um den Einsatz des Militärs im Cyberspace handelt und dieses im Rahmen der Gemeinsamen Sicherheits- und Verteidigungspolitik (GSVP) zur Anwendung kommen sollte, ist die Grundlage dafür in den Artikeln 42, 43 und 44 des Vertrages über die Europäische Union (EUV) zu finden.⁸⁷¹ Diese Ausführungen werden in der Entschlüsselung des Europäischen Parlamentes zur Umsetzung der GSVP näher erläutert.

Das Europäische Parlament

⁸⁷¹ Vgl. Schwartzmann, 2010, S. 27ff.

„[...] verweist auf die unmittelbare Bedrohung im Cyber-Bereich und hält es für dringend geboten [...] auf Cyberkrisen – auch im Kontext der GSVP – zu reagieren; [...]“.⁸⁷²

Es wird von den Mitgliedsstaaten gefordert ihre Cyber Abwehrkapazitäten zu erhöhen. Interessant ist auch die Hervorhebung von Synergieeffekten zwischen ziviler Cyber Sicherheit und militärischer Cyber Abwehr und dass sich diese zu ergänzen haben.⁸⁷³ Die Aufgaben werden hier zwar explizit genannt und auch die Notwendigkeit der gegenseitigen Unterstützung, doch fehlt eine klare Zuordnung der operativen Verantwortung. Die Reaktion auf Cyberkrisen im Kontext der GSVP meint hier offensichtlich die mit militärischen Mitteln.

Der Vertrag über die Arbeitsweise der EU (AEUV) regelt vor allem die Zusammenarbeit der Justiz und der Polizei der Mitgliedsstaaten.⁸⁷⁴ Diese Regelungen beschäftigen sich auch mit der Cyber Kriminalität. Konkretisiert wird die GSVP in Bezug auf den Cyberspace im EU Cyber Defence Policy Framework. Die Nationen der EU werden hier dazu angehalten, eine Entwicklung von

„[...] cyber defence capabilities [...] including doctrine, leadership, organisation, personnel, training, technology, infrastructure, logistics and interoperability.“⁸⁷⁵

vorzunehmen. In der Aktualisierung des EU-Politikrahmens von 2018 wird dieses Ansinnen noch verstärkt dargestellt. Explizit wird der Schutz der IKT-Infrastruktur, der im Rahmen der GSVP genutzt wird, angesprochen.

„Hauptschwerpunkt dieses Politikrahmens ist die Entwicklung von Cyberabwehrfähigkeiten sowie der Schutz der für die GSVP der EU genutzten Kommunikations- und Informationsnetze.“⁸⁷⁶

Sind im Cyber Defence Policy Framework 2014 die zivilen Netze des European External Affairs Services (EEAS) dem Managing Directorate for Resources (MDR) zugeordnet, so wird in der Aktualisierung des Politikrahmens der Schutz der GSVP-relevanten Netze dem EEAS überantwortet. Zudem werden European Union Military Staff (EUMS), das Crisis Management and Planning Directorate (CMPD) und die Civilian Planning and Conduct Capability (CPCC) zur Unterstützung genannt.^{877 878}

⁸⁷² Entschließung des Europäischen Parlaments vom 21. Mai 2015 zur Umsetzung der Gemeinsamen Sicherheits- und Verteidigungspolitik (nach dem Jahresbericht des Rates an das Europäische Parlament zur Gemeinsamen Außen- und Sicherheitspolitik) 2014/2220(INI) ABl. C 353/12, S. 6.

⁸⁷³ Vgl. Entschließung 2014/2220(INI)/EU ABl. C 353/12, S.6.

⁸⁷⁴ Vgl. Schwartmann, 2010, S. 41ff.

⁸⁷⁵ European Union, Political and Security Committee, EU Cyber Defence Policy Framework, 2014, S. 4.

⁸⁷⁶ Rat der Europäischen Union, EU-Politikrahmen für die Cyberabwehr (Aktualisierung 2018), 2018, S. 8.

⁸⁷⁷ Vgl. European Union, Political and Security Committee, EU Cyber Defence Policy Framework, 2014, S. 6.

⁸⁷⁸ Rat der Europäischen Union, EU-Politikrahmen für die Cyberabwehr (Aktualisierung 2018), 2018, S. 12.

Im Framework 2014 erfolgt keine klare Zuweisung der Verantwortung. Nur die Informationssysteme, welche in GSVP Operationen eingesetzt werden, sind einer „[...] unified chain of command [...]“⁸⁷⁹ zuzuordnen.

Hier sind der Eigenschutz des Militärs und der in gemeinsamen Operationen mitwirkenden zivilen Organisationselemente der EU im Fokus. Im EU Concept for Cyber Defence for EU-led Military Operations sind die Zuständigkeiten und Kompetenzen geregelt. So sind generell die Framework- und Truppensteller-Nationen für die Cyber Abwehr in ihren Netzen verantwortlich.⁸⁸⁰ Der IT-Abteilung des EEAS obliegt hier in erster Linie die Richtliniensetzungs-Kompetenz.

Nicht geregelt ist in vorliegenden Dokumenten die Zuständigkeit bei Cyber Angriffen auf Mitgliedsstaaten und/oder auf die Europäische Union selbst. Kann davon ausgegangen werden, dass die Mitgliedsstaaten für ihre nationalen Netze selbst verantwortlich sind, so ist nicht klar, wer letztlich die Netzwerke der Europäischen Union und ihrer Institutionen verteidigt. Klar scheint in den oben genannten EU Konzepten die Verantwortung für die Reaktion auf den Kleinen Cyberwar geregelt zu sein. Hingegen fehlen rechtliche – aber auch politisch/strategische – Handlungsleitlinien für die Zuweisung der Aufgaben in einem Großen Cyberwar.

8.3.2 Die Cybersicherheitsstrategie der Europäischen Union und der Cyberwar

In der Cybersicherheitsstrategie definiert die EU den Cyberspace als Raum, in dem „[...] dieselben Gesetze und Normen wie in anderen Lebensbereichen.“⁸⁸¹ gelten. Im Fokus steht der Kapazitätsaufbau zur Begegnung von Cyber Angriffen. Dabei wird eine enge Zusammenarbeit des privaten mit dem öffentlichen Sektor eingefordert. Die Stärkung der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) stellt dabei eine wichtige Maßnahme dar. Ebenso werden Programme definiert, die eine Sensibilisierung für die Gefahren im und aus dem Cyberspace gewährleisten sollen.

In Zusammenhang mit der GSVP beinhaltet die europäische Cybersicherheitsstrategie einige Punkte die Cyber Verteidigung betreffend. Die Überprüfung der operativen Anforderungen an die Cyber Verteidigung der EU wird dabei genauso thematisiert wie der Aufbau von Kapazitäten und Technologien zur Cyber Abwehr auf EU-Ebene.⁸⁸² Der schon zitierte EU-Rahmen für die Cyber Verteidigungspolitik basiert ebenfalls auf der Cybersicherheitsstrategie der EU.

Cyber Verteidigung wird in dem Strategiepapier aber nicht als alleinige Aufgabe des Militärs betrachtet, sondern ist auf Grund der Komplexität der

⁸⁷⁹ European Union, Political and Security Committee, EU Cyber Defence Policy Framework, 2014, S. 6.

⁸⁸⁰ Vgl. EUMS, EU Concept for Cyber Defence for EU-led Military Operations, 2012, S. 10.

⁸⁸¹ Europäische Kommission, Cybersicherheitsstrategie der Europäischen Union, 2013, S. 4.

⁸⁸² Vgl. ebd., S. 13f.

Bedrohung eine Angelegenheit die „[...] Synergien zwischen dem Vorgehen auf ziviler und auf militärischer Ebene beim Schutz kritischer Cyberanlagen und –daten [...]“⁸⁸³ zu nutzen hat. Diese Formulierung mag auf politischer und strategischer Ebene durchaus genügen, doch schärft sie die Aufgaben der Träger der Staatsgewalt nicht unbedingt. Aus Sicht der EU und fehlender stehender EU Streitkräfte lässt sich diese Aufgabenzuordnung auf EU-Ebene auch gar nicht treffen.

Basierend auf der Cybersicherheitsstrategie wurde eine Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union durch das Europäische Parlament und den Rat erlassen.⁸⁸⁴ Diese sogenannte Netz- und Informationssysteme-sicherheit (NIS)-Richtlinie konkretisiert teilweise die in der Cybersicherheitsstrategie formulierten Forderungen. Hinsichtlich der Kompetenzzuordnung zwischen Polizei und Militär führt die NIS-Richtlinie aus, dass „[...] die Mitgliedsstaaten befugt sein [sollten], mehr als eine nationale Behörde zu benennen, die für die Erfüllung der Aufgaben im Zusammenhang mit der Sicherheit von Netz- und Informationssystemen [...]“⁸⁸⁵ verantwortlich zeichnen.

Auch wenn hier nicht explizit ausgeführt, lässt sich daraus ableiten, dass auch in diesem Dokument zwischen kriminellen und kriegesischen Akten im Cyberspace unterschieden wird. Zusätzlich zu den Behörden wird den Betreibern der IKT-Infrastruktur eine erhebliche Mitverantwortung für die Sicherheit der Systeme zugesprochen.⁸⁸⁶ Zur Unterstützung der Mitgliedsstaaten wird der ENISA eine wesentliche Rolle zugeordnet, diese besondere Rolle der ENISA zeigt sich im Mandat dadurch, dass die Agentur

„[...] aufgrund ihrer Unabhängigkeit, der wissenschaftlichen und technischen Qualität der von ihr geleisteten Beratung und Unterstützung, der von ihr bereitgestellten Informationen, ihrer operativen Verfahren, ihrer Arbeitsmethoden sowie der Sorgfalt bei der Wahrnehmung ihrer Aufgaben als Kompetenzzentrum [...]“⁸⁸⁷

dient. Zudem werden Staaten der EU dazu angehalten, im Bereich der Netzsicherheit gewisse Minimalfähigkeiten und Strategien zu entwickeln.⁸⁸⁸ Dies hat auch auf Österreich als Mitglied der EU einen wesentlichen Einfluss auf die Gestaltung eines entsprechenden Rechtsrahmens.

⁸⁸³ Ebd., S. 13.

⁸⁸⁴ Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union ABl. L 194.

⁸⁸⁵ RL 2016/1148/EU, ABl. L 194, S. 5.

⁸⁸⁶ Vgl. RL 2016/1148/EU, ABl. L 194, S. 7.

⁸⁸⁷ Verordnung (EU) 2019/881 des europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit) ABl. L 151/15, S. 20.

⁸⁸⁸ Vgl. RL 2016/1148/EU, ABl. L 194, S. 2ff.

8.3.3 Die Cyber Verteidigung im Rahmen der Europäischen Union

Die EU verfügt mit dem Cyber Defence Policy Framework über ein Dokument, welches vor allem die Kommunikationseinrichtungen und Netzwerkkomponenten, welche im Rahmen der GSVP von den Mitgliedsstaaten genutzt werden, in den Mittelpunkt der Cyber Defence stellt.⁸⁸⁹ Es geht hier allerdings weniger um eine Zuordnung von Verantwortlichkeiten, sondern um die Entwicklung gemeinsamer Kapazitäten, um die Netze mit Bezug zur GSVP sicherer zu machen. Dabei ist die zivil-militärische Zusammenarbeit genauso essentiell wie die Zusammenarbeit mit internationalen Partnern.⁸⁹⁰ Aus militärischer Sicht ist vor allem die explizite Nennung der NATO als Partner hervorzuheben.

In der Cybersicherheitsstrategie der EU von 2013 ist aus Sicht der Cyber Defence vor allem der Aufbau und die Entwicklung entsprechender Fähigkeiten in diesem Bereich angeregt.⁸⁹¹ Im Upgrade dieser Strategie von 2017 werden aus militärischer Sicht vor allem die EU-geführten Operationen und Missionen als jene Bereiche genannt, die durch die dabei eingesetzten militärischen Kräfte zu verteidigen sind.⁸⁹² Gegenüber vielen nationalen Strategien zur Cyber Sicherheit, zeigen die Dokumente der EU eine ausgewogenere Beschäftigung mit den unterschiedlichen Kompetenzbereichen von Militär und Polizei, ohne aber dabei genauer auf Details der Abgrenzung einzugehen.

Die genannten Operationen und Missionen im Rahmen der GSVP beruhen vor allem darauf, dass die EU das Militär auch als politisches Instrument zum Einsatz bringt und diese militärischen Kräfte auf eine sichere Nutzung des Cyberspace angewiesen sind.⁸⁹³ Im Konzept der EU zur Cyber Verteidigung von EU-geführten Militär-Operationen werden alle Aspekte der Computer Network Operationen behandelt und deren Anwendung ein grundsätzlicher Rahmen abgesteckt.⁸⁹⁴ Der Fokus des Schutzes der militärischen Netze in Einsätzen liegt hier vor allem auf den Führungseinrichtungen.⁸⁹⁵

Für diese Führungseinrichtungen wurde ein Maßnahmenpaket entwickelt, welches auf Erfahrungen bisheriger Einsätze und anderer Organisationen aufbaut.⁸⁹⁶ Interessant ist, dass sehr wohl auf die Verteidigung des Cyberspace in militärischen Einsätzen eingegangen wird,

⁸⁸⁹ Vgl. European Union, Political and Security Committee, EU Cyber Defence Policy Framework, 2014, S. 6.

⁸⁹⁰ Vgl. Federal Ministry of Defence of the Republic of Austria: Handbook on Cybersecurity, The Common Security and Defence Policy of the European Union, 2019, S. 21.

⁸⁹¹ Vgl. Europäische Kommission, Cybersicherheitsstrategie der Europäischen Union, 2013, S. 13.

⁸⁹² Vgl. Europäische Kommission, Gemeinsame Mitteilung an das europäische Parlament und den Rat, Abwehrfähigkeit, Abschreckung und Abwehr: die Cybersicherheit in der EU wirksam erhöhen, 2017, S. 35.

⁸⁹³ Vgl. Federal Ministry of Defence of the Republic of Austria: Handbook on Cybersecurity, 2019, S. 21.

⁸⁹⁴ Vgl. EUMS, EU Concept for Cyber Defence for EU-led Military Operations, 2012, S. 17.

⁸⁹⁵ Vgl. Federal Ministry of Defence of the Republic of Austria: Handbook on Cybersecurity, 2019, S. 39.

⁸⁹⁶ Vgl. ebd., S. 40.

dass das Militär aber bei der Verteidigung der EU als Ganzes eher unbeachtet bleibt. Das liegt, wie bereits angedeutet, möglicherweise darin begründet, dass die Verantwortung der nationalen Streitkräfte für die einzelnen Mitgliedsstaaten gegeben ist und eine gemeinsame europäische Armee nicht realisiert ist. Das bedeutet aber auch, dass es keine militärische Zuständigkeit für Einrichtungen der EU gibt, um deren IKT-Infrastruktur zu schützen.

Cyber Verteidigung ist zudem ein Begriff, der in der EU keiner gemeinsamen Sichtweise unterliegt. So wird im Konzept zur Verteidigung des Cyberspace in Militäroperationen der EU darauf hingewiesen, dass die dort getroffene Definition keine EU-weite Auslegung darstellt.⁸⁹⁷ Cyber Defence ist darin zudem sehr offen definiert ohne wirklich ins Detail zu gehen. Diese ungenaue begriffliche Darstellung führt dazu, dass die Mitgliedsstaaten in dieser Hinsicht gefordert sind, die begriffliche Klarheit herzustellen. Auch Österreich hat hier eine wesentliche Aufgabe, national wie auch im Rahmen der EU, um in Hinblick auf den Umgang mit dem Cyberwar Handlungssicherheit herzustellen.

8.4 Zum Cyberwar im Österreichischen Recht

Ausgangspunkt für die Erstellung eines Rechtsrahmens ist die Entwicklung einer gemeinsamen Sichtweise auf das Bedrohungsspektrum im neuen Handlungsraum Cyberspace. Die ÖSS ist dieser Ausgangspunkt, aus welchem heraus die ÖSCS erwachsen ist. Diese beiden strategischen Dokumente haben im Wesentlichen die Entwicklung rechtlicher Normen in Bezug auf den Cyberspace ausgelöst. Hier finden sich vor allem wesentliche Anregungen, um die Rolle des Militärs in Abgrenzung zur Polizei zu entwickeln. Im Bereich der Kriminalität im Netz ist die Entwicklung des Rechtsrahmens auf die Cybercrime Convention des Europarates zurückzuführen.

Mit zehnjähriger Verspätung und nach mehreren, international Aufsehen erregenden, Vorfällen wurde eine Auseinandersetzung mit den kriegesischen Konfrontationen im Netz eingeleitet. Nicht nur die Strafverfolgung wurde nun betrachtet, sondern auch die rechtliche Würdigung von staatlich organisiertem Vorgehen im Netz gegen andere Staaten. Der Begriff vom Cyberwar wurde einer differenzierten Betrachtung unterzogen.

Um auf die Kompetenzverteilung bei Vorfällen im Cyberspace schließen zu können, ist eine Auseinandersetzung mit den rechtlichen Grundlagen für das Tätigwerden der Organe der bewaffneten Staatsgewalt im Netz notwendig. Weiters wird von den Aufgaben des Bundesheeres in der realen Welt in Analogie abgeleitet, welche Aufgaben sich für das österreichische Militär im Cyberraum ergeben. In Österreich ist zunächst das Strafrecht zu nennen, welches sich mit Angriffen krimineller Natur im Netz auseinandersetzt.

⁸⁹⁷ Vgl. EUMS, EU Concept for Cyber Defence for EU-led Military Operations, 2012, S. 17.

8.4.1 Strafrecht im Cyberspace am Beispiel des österreichischen Stragesetzbuches

Es gibt in Zusammenhang mit dem Cyberspace viele spezifische Delikte, die einer Regelung im Strafrecht bedürfen. Diese wurden vor allem in zwei Strafrechtsänderungen (2002 und 2004) erfasst.⁸⁹⁸ Im Jahr 2002 wurde im Wesentlichen die Cyber Crime Konvention des Europarates⁸⁹⁹ auf nationaler Ebene umgesetzt. Dabei stand die Erfassung neuer Delikte und die Anpassung der bereits bestehenden Bestimmungen, gegen den Computermisbrauch, im Stragesetzbuch im Vordergrund. Es geht um Computerdelikte im engeren Sinn. Im Fokus stehen unerlaubte Angriffe auf und die Nutzung von Computersystemen für die Begehung von Straftaten.

Die wesentlichen Bestimmungen sind: Widerrechtlicher Zugriff auf ein Computersystem (§118a StGB), Verletzung des Telekommunikationsgeheimnisses (§119), Missbräuchliches Abfangen von Daten (§119a), Datenbeschädigung (§126a), Störung der Funktionsfähigkeit eines Computersystems (§126b), Missbrauch von Computerprogrammen oder Zugangsdaten (§126c), Betrug (§§146 ff), Betrügerischer Datenverarbeitungsmissbrauch (§148a) und Datenfälschung (§225a). Im Jahr 2004 erfolgte die Modernisierung einiger Delikte des Sexualstrafrechts, mit Bezug auf den Cyberspace.⁹⁰⁰ Auch kamen, im Rahmen dieser Änderung des Strafrechts, Änderungen hinsichtlich von Delikten bezüglich unbarer Zahlungsmittel (§§241a ff) hinzu.⁹⁰¹ In der Änderung des Stragesetzbuches zur Verhinderung von Terrorismus im Jahr 2011 wurde das Internet zur Verbreitung von Informationen, welche zu terroristischen Akten anleiten, erfasst.⁹⁰²

Der Angriff auf Netzwerke rückt, bei der genaueren Untersuchung der strafrechtlichen Regelungen, in Bezug auf das Thema der Arbeit, in den Fokus. Bei näherer Betrachtung der Regelungen hinsichtlich der Delikte, welche einen Angriff auf Daten und Systeme darstellen, sind einige Strafrechtsbestimmungen hervorzuheben. Besonders der Umstand, dass Hacking nur dann strafbar ist, wenn ein entsprechender Schutzmechanismus (Firewall, Passwort, etc.) überwunden werden musste, in Zusammenhang mit der Absicht Daten zugänglich zu machen (vgl. Anonymous) oder aber sich zu bereichern.⁹⁰³ Der Tatbestand des widerrechtlichen Eindringens in ein Computersystem, ist erst dann zur Gänze erfüllt, wenn der Täter tatsächlich im System tätig werden könnte, er sich also im System befindet.⁹⁰⁴

⁸⁹⁸ Vgl. http://www.internet4jurists.at/strafrecht/recht_oe1a.htm, [12.05.2020].

⁸⁹⁹ Vgl. <https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/090000168008157a>, [12.05.2020].

⁹⁰⁰ Vgl. http://www.internet4jurists.at/strafrecht/recht_oe1a.htm, [12.05.2020].

⁹⁰¹ Vgl. ebd.

⁹⁰² Vgl. § 278f, Bundesgesetz vom 23. Jänner 1974 über die mit gerichtlicher Strafe bedrohten Handlungen (Stragesetzbuch – StGB) BGBl. Nr. 60/1974 idF BGBl. I Nr. 70/2018.

⁹⁰³ Vgl. § 118a StGB.

⁹⁰⁴ Vgl. http://www.internet4jurists.at/strafrecht/recht_oe1a.htm, [12.05.2020].

Die Strafverfolgungsbehörden werden nur dann tätig, wenn sie vom Geschädigten ermächtigt werden.⁹⁰⁵ Zur Umsetzung dieser Regelung bedarf es also einer entsprechenden Cyber Sicherheit und der Bereitschaft, das Delikt auch zur Anzeige zu bringen. Hier bestehen in der Realität vielfach wesentliche Hürden. Mangelhaftes Sicherheitsbewusstsein und die fehlende Bereitschaft, vor allem von geschädigten Unternehmen, Sicherheitseinbrüche in die Öffentlichkeit zu tragen, sind nicht einfach aufzulösen. Oft sind sich die Geschädigten gar nicht im Klaren darüber, dass sie Opfer einer Cyber Attacke wurden.

In Bezug auf das Agieren von Streitkräften hat diese Bestimmung, im Falle der Informationsbeschaffung in Friedenszeiten, einen wesentlichen Einfluss. In diesem Zusammenhang ist auch das missbräuchliche Abfangen von Daten zu sehen. Nicht nur das Abfangen von Nachrichten am Übertragungsweg ist strafbar, sondern auch das Ausspionieren über eine Abstrahlung am System selbst, wenn eine Bereicherungs- oder Schädigungsabsicht vorliegt.⁹⁰⁶

Wenn Daten einer Beschädigung zugeführt werden, so handelt es sich um eine Sachbeschädigung, falls die Daten einen gewissen Vermögenswert aufweisen.⁹⁰⁷ Vielfach ist der Wert aber nicht eindeutig bezifferbar. Nüchtern betrachtet bestehen Datensätze auf der physikalischen Ebene aus digitalen Zuständen, die für sich betrachtet keinen Wert darstellen. Wenn der bestimmungsgemäße Gebrauch nicht verhindert oder beeinträchtigt wird, so ist selbst eine Veränderung der Daten nicht strafbar. Eine Implementierung von Programmteilen, die die eigentliche Funktion nicht beeinträchtigen, ist daher in diesem Sinn nicht strafrechtlich zu verfolgen.

Oft ist die Kombination von verschiedenen rechtlichen Bestimmungen angezeigt (z.B.: §118a mit §126a). Ist das Ziel des Angriffs die Störung des Systems selbst, muss eine schwere Störung vorliegen, damit ein Tatbestand erfüllt ist; allerdings gibt es im Gesetz keine Definition hinsichtlich der Schwere der Störung.⁹⁰⁸ Ist ein vorbereitender Denial of Service Angriff, für den Einsatz von Streitkräften in einem Konflikt, nicht als ein bewaffneter Angriff, gemäß den völkerrechtlichen Bestimmungen, klassifiziert, so handelt es sich um eine Verletzung des Strafrechts.

Im Fall von Angriffen auf Betreiber wesentlicher Dienste⁹⁰⁹ greift das Netz- und Informationssystemsicherheitsgesetz (NISG), welches die NIS-Richtlinie der EU für Österreich konkretisiert. Hier liegt die Zuständigkeit für solche Übergriffe im Netz beim Innenministerium. Zudem obliegt dem

⁹⁰⁵ Vgl. § 118a StGB.

⁹⁰⁶ Vgl. § 119a StGB.

⁹⁰⁷ Vgl. § 126a StGB.

⁹⁰⁸ Vgl. § 126b StGB.

⁹⁰⁹ Anm. d. Verf.: Gemäß Netz- und Informationssicherheitsgesetz (NISG) werden Betreiber wesentlicher Dienste danach beurteilt, wie hoch die Zahl der Nutzer, die Abhängigkeit anderer wesentlicher Sektoren (Energie, Verkehr, etc.), der Marktanteil, die geographische Ausbreitung, das Ausmaß und die Dauer der Auswirkungen und die Bedeutung der Aufrechterhaltung des Dienstes in ausreichendem Umfang ist. Vgl. § 16 Abs. 2 Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG) BGBl. I Nr. 111/2018.

Innenminister die Deutungshoheit hinsichtlich einer Cyberkrise.⁹¹⁰ Eine Cyberkrise sind

„[...] ein oder mehrere Sicherheitsvorfälle, die eine gegenwärtige und unmittelbare Gefahr für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen darstellen und schwerwiegende Auswirkungen auf die Gesundheit, die Sicherheit oder das wirtschaftliche und soziale Wohl großer Teile der Bevölkerung oder das effektive Funktionieren von staatlichen Einrichtungen nach sich ziehen können;“⁹¹¹

Dies ist im Hinblick auf die Aufgaben des Militärs mit Bezug auf den Schutz souveränitätsrelevanter Einrichtungen im Rahmen der militärischen Landesverteidigung problematisch, da gerade das effektive Funktionieren von staatlichen Einrichtungen hier miteinzubeziehen ist. Zwar ist im Fall einer Cyberkrise das Militär in der Funktion des Chefs des Generalstabes im Koordinationsausschuss miteingebunden, doch bleibt die Verantwortung in einer solch kritischen Situation allein beim Innenressort.⁹¹² Dies führt zur Auseinandersetzung mit den rechtlichen Grundlagen der Kompetenzzuordnung an Militär und Polizei.

8.4.2 Die rechtlichen Grundlagen für die Tätigkeit der Organe der bewaffneten Staatsgewalt am Beispiel Österreichs

Die Kompetenzen scheinen klar geregelt und finden ihren Niederschlag in den rechtlichen Rahmenbedingungen. So sind in Österreich das Bundes-Verfassungsgesetz (B-VG) und das Bundesministeriengesetz (BMG) die Rechtsquellen, welche die Aufteilung der Kompetenzen zwischen Polizei und Militär, dem Bundesheer (ÖBH), regeln.

Das Handeln der bewaffneten Exekutivkörper ist als Verwaltungshandeln definiert, als Vollziehung der Verwaltung. Dazu wird im B-VG ausgeführt:

„Die gesamte staatliche Verwaltung darf nur auf Grund der Gesetze ausgeübt werden.“⁹¹³

Das bedeutet, dass das Handeln von Polizei und Militär sich am Gesetz orientiert. Im B-VG ist zu den Aufgaben von Polizei und Militär festgehalten:

„(1) Bundessache ist die Gesetzgebung und die Vollziehung in folgenden Angelegenheiten: [...] 7. Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit einschließlich der ersten allgemeinen Hilfeleistung; [...] 14. Organisation und Führung der Bundespolizei; Regelung der Errichtung und der Organisierung sonstiger Wachkörper

⁹¹⁰ Vgl. § 24 NISG.

⁹¹¹ § 3, Abs. 22 NISG.

⁹¹² Vgl. § 25, Abs. 2 NISG.

⁹¹³ Artikel 18 Bundes-Verfassungsgesetz (B-VG) BGBl. Nr. 1/1930 idF BGBl. I Nr. 22/2018.

mit Ausnahme der Gemeindewachkörper; Regelung der Bewaffnung der Wachkörper und des Rechtes zum Waffengebrauch; [...]“⁹¹⁴

Hier ist für die Polizei festgehalten, dass ein solcher Wachkörper eingerichtet und dieser Teil der Bundesverwaltung ist. Die Aufgaben sind hier zwar determiniert, aber der Polizei nicht dezidiert zugeordnet. Es lassen sich nur aus dem Artikel 78 B-VG Aufgaben ableiten, da die Polizei das Vollzugsorgan der Sicherheitsbehörden darstellt. Für das Militär lässt sich im B-VG schon konkreter ableiten, was es zu leisten hat.

„(1) Österreich bekennt sich zur umfassenden Landesverteidigung. Ihre Aufgabe ist es, die Unabhängigkeit nach außen sowie die Unverletzlichkeit und Einheit des Bundesgebietes zu bewahren, insbesondere zur Aufrechterhaltung und Verteidigung der immerwährenden Neutralität. Hierbei sind auch die verfassungsmäßigen Einrichtungen und ihre Handlungsfähigkeit sowie die demokratischen Freiheiten der Einwohner vor gewaltsamen Angriffen von außen zu schützen und zu verteidigen.“⁹¹⁵

Diese Aufgaben werden im Artikel 79 B-VG konkret dem Bundesheer zugewiesen. Im Rahmen der Zugehörigkeit zur Europäischen Union (EU) erwachsen noch weitere Aufgaben, welche im Artikel 23j B-VG festgeschrieben sind. Die Mitwirkung an der gemeinsamen Außen- und Sicherheitspolitik der EU beinhaltet auch die Mitwirkung an EU-Operationen mit zivilen und militärischen Mitteln. Die Aufgaben beziehen sich dabei auf den Artikel 43 des Vertrages über die EU (EUV)⁹¹⁶ und umfassen Maßnahmen

„[...] der militärischen Beratung und Unterstützung, Aufgaben der Konfliktverhütung und der Erhaltung des Friedens oder Kampfeinsätze im Rahmen der Krisenbewältigung einschließlich Frieden schaffender Maßnahmen und Operationen zur Stabilisierung der Lage nach Konflikten [...]“⁹¹⁷

Sowohl Polizei als auch Militär können in solchen Missionen zum Einsatz gebracht werden. Diese Aspekte werden im Verlauf der Abhandlung zum Teil noch beleuchtet. Die Aufteilung der Zuständigkeiten, die Kompetenzabgrenzung zwischen den Ministerien, als Teil der Verwaltung, wird im BMG geregelt. In den Zuständigkeitsbereich des Innenministeriums fallen demzufolge alle

„Angelegenheiten des Sicherheitswesens, soweit sie nicht in den Wirkungsbereich eines anderen Bundesministeriums fallen.“⁹¹⁸

⁹¹⁴ Artikel 10 B-VG.

⁹¹⁵ Artikel 9a B-VG.

⁹¹⁶ Vgl. Schwartmann, 2010, S. 29.

⁹¹⁷ Artikel 23j B-VG.

⁹¹⁸ Anlage Teil 2 H zu § 2 Bundesgesetz über die Zahl, den Wirkungsbereich und die Einrichtung der Bundesministerien (Bundesministeriengesetz 1986 – BMG) BGBl. Nr. 76/1986 idF BGBl. I Nr. 61/2018.

Dabei steht die „[...] Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit; Maßnahmen der Wiederherstellung der subjektiven und objektiven Sicherheit von Verbrechenopfern. [...]“⁹¹⁹ im Vordergrund.

Für das Militär findet sich lediglich ein Verweis auf die im B-VG bereits formulierten Aufgaben. Dem Bundesministerium für Landesverteidigung (BMLV) obliegen demnach

„[...] Militärische Angelegenheiten. Dazu gehören insbesondere auch: Angelegenheiten der Besorgung der verfassungsgesetzlich festgelegten Aufgaben des Bundesheeres. Angelegenheiten der operativen und taktischen Führung des Bundesheeres. [...]“⁹²⁰

Diese Bestimmungen beschäftigen sich mit den Aufgaben von Polizei und Militär, sagen aber noch nichts darüber aus, welche Maßnahmen zur Erfüllung dieser Aufgaben gestattet sind. Diese Regelungen finden sich in weiteren Gesetzen. Das für das polizeiliche Handeln relevante Gesetz ist das Sicherheitspolizeigesetz (SPG), die Befugnisse des Militärs sind im Wehrgesetz (WG) und im Militärbefugnisgesetz (MBG) geregelt.

In der Sicherheitsdoktrin des Innenressorts findet sich die Forderung nach der Schaffung eines Bundesgesetzes für Cyber Sicherheit. Damit sollen neben „[...] zusätzlichen Befugnissen für die [operative] nationale zuständige Behörde [...]“⁹²¹ auch „[...] Strukturen, Aufgaben und Befugnisse für das Cyber-Krisenmanagement [...]“⁹²² festgelegt werden. Durch dieses Gesetz sollen Verfahren und Vorgehensweisen ermöglicht werden, die durchaus im militärischen Aufgabenspektrum anzusiedeln sind.⁹²³

8.4.3 Die Zuordnung der Führungsverantwortung zwischen Polizei und Militär am Beispiel der Raumschutzoperation

In Bezug auf die Assistenzleistung des Bundesheeres für die Sicherheitsexekutive ist das Merkblatt Raumschutz klar formuliert. Hier wird zwischen vier Stufen der Eskalation unterschieden.⁹²⁴ In der ersten Stufe sind vor allem Handlungen definiert, die vorwiegend einen kriminellen Hintergrund haben oder als Einzeltaten mit terroristischer Absicht zu fassen sind. Dabei liegt die Verantwortung bei der Sicherheitsexekutive, die ihrer Aufgabe, der Bekämpfung der Mikroviolenz, nachgehen muss. In der zweiten Stufe nehmen diese Aktionen an Umfang zu, wobei der Mitteleinsatz sich erhöht und die Sicherheitsexekutive Assistenz durch das Bundesheer erhält.

Bei einer weiteren Eskalation und weiterem Kräftebedarf kommt eine dritte Stufe zum Tragen, wobei zum Schutz von Objekten nun auch Verfahren

⁹¹⁹ Anlage Teil 2 H zu § 2 BMG.

⁹²⁰ Anlage Teil 2 I zu § 2 BMG.

⁹²¹ Bundesministerium für Inneres (Hrsg.): Mehr Freiheit. Mehr Sicherheit. Die Sicherheitsdoktrin des BMI für Österreich 2017 - 2020, Wien 2017, S. 22.

⁹²² Ebd., S. 22.

⁹²³ Vgl. ebd., S. 22.

⁹²⁴ Vgl. BMLV, Merkblatt für das Bundesheer, Raumschutz, 2000, S. 12f.

des Raumschutzes, also nicht nur polizeiliche, sondern militärische Verfahren, zur Anwendung gelangen. Der Übergang zur vierten Stufe in der das Bundesheer die Führungsverantwortung übernimmt, um auf Grund der Makroviolenz tätig zu werden, bedingt eine Identifikation wer diese Angriffe und Aktionen durchführt. Es sind also neben der Ausdehnung in räumlicher Hinsicht und in Hinblick auf die Akteure, die Intensität der Aktionen, sowie der Zweck von Bedeutung, um die Führungsverantwortung festzulegen.

Die Vorschrift spricht von Kriterien eines militärischen Angriffes von außen. Im Rahmen der militärischen Landesverteidigung kommt der Raumschutz dann zur Anwendung,

„[...] wenn diese Angriffe insgesamt als militärische vom Ausland gesteuerte und genährte Operation zu qualifizieren sind.“⁹²⁵

Diese Qualifizierung richtet sich nach den bekannten Kriterien: Der Ausdehnung, der Intensität und dem Zweck. Der Raumschutz stellt dabei jenes operative Verfahren dar, das es dem Bundesheer ermöglicht, gegen Kräfte im Kleinen Krieg vorzugehen. Kommen diese Kräfte vorgestaffelt oder begleitend zu einem konventionellen Angriff, einem Großen Krieg, zum Tragen, so wird keine Raumschutzoperation durchgeführt, sondern im Rahmen der konventionellen Einsatzarten des Bundesheeres der Schutz durchgeführt.⁹²⁶ Handelt es sich also bei der Bedrohung um eine von außen eingebrachte, aber im Inneren wirksam werdende Bedrohung, so ist das Militär, wenn die politische Führung sich dazu entschließt, ab einem gewissen Eskalationsniveau (ab der vierten Stufe) führungsverantwortlich. Diese Regelung beschränkt den Einsatz des Bundesheeres im Inneren gegen Gefahren von außen.

8.4.4 Zu den Aufgaben des Bundesheeres im Cyberspace

In der rechtlichen Stellungnahme des BMLVS bezüglich der ÖSCS werden die Aufgaben, die das Bundesheer im Cyberspace zu erfüllen hat, rechtlich genauer dargestellt.⁹²⁷ Grundlage für das Tätigwerden des Bundesheeres sind die in der Bundesverfassung definierten Aufgaben. Die Kernaufgabe ist die militärische Landesverteidigung, sowie zusätzlich die Durchführung von Assistenz- und Auslandseinsätzen.⁹²⁸

Militärische Landesverteidigung meint grundsätzlich die Abwehr von Gefahren von außen, aber auch von Vorgängen im Staatsinneren, die im Zusammenhang mit äußeren Gefahren stehen.⁹²⁹ Dies trifft dann zu, wenn die wirksame Abwehr nur mit militärischen Mitteln geleistet werden kann. Diesem Umstand wird zum Beispiel im Raumschutzmerkblatt des ÖBH

⁹²⁵ Ebd., S. 9.

⁹²⁶ Vgl. ebd., S. 15f.

⁹²⁷ Vgl. BMLVS, ÖSCS, GZ S91018/14-GrpRechtLeg/2012, Ersuchen um rechtliche Würdigung, Stellungnahme, 2012. S. 1ff.

⁹²⁸ Vgl. Artikel 79 B-VG.

⁹²⁹ Vgl. Republik Österreich, Beilagen zu den stenographischen Protokollen des Nationalrates, 15. Band, Wien, 1974, Beilage 1461, S. 5.

Rechnung getragen. Der Übergang von der Assistenzleistung zur militärischen Landesverteidigung erfolgt dann,

„[...] wenn die im eigenen Staatsgebiet wirksam werdenden subversiven Kräfte eindeutig als Angehörige einer fremden Streitmacht, unabhängig, ob offen oder verdeckt vorgehend, identifiziert worden sind.“⁹³⁰

Hieraus ist ersichtlich, dass die Bedrohung, gegen die das Bundesheer aktiv werden kann, nicht zwingend von außen kommen muss, sondern eine innenwirksame Bedrohung mit Außenbezug sein kann.⁹³¹ Wird also die Souveränität Österreichs teilweise oder zur Gänze angegriffen, so hat das Bundesheer im Rahmen der militärischen Landesverteidigung einzuschreiten.⁹³²

Im Rahmen der Aufrechterhaltung der Ordnung und Sicherheit im Inneren überhaupt, kann das Bundesheer zur Assistenzleistung herangezogen werden.⁹³³ Darunter würden die Unterstützungsleistungen im Rahmen der Cyber Kriminalität, des Cyber Terrorismus und der Cyber Angriffe, die nicht dem Cyberwar zurechenbar sind, fallen. Da diese Aufgaben Angelegenheiten der Sicherheitspolizei sind,⁹³⁴ kommt das Bundesheer für den gesamten Aufgabenbereich als Assistenzleister in Frage. Im Bereich der Amtshilfe ist ein Konnex zu den eigenen Aufgaben notwendig, das heißt eine erbetene Amtshilfe, im Zuge der Amtshilfe, hat zugleich eine Aufgabe der militärischen Landesverteidigung zu sein.⁹³⁵

Im Zuge der Cyber Defence ist die Abwehr von Cyber Angriffen, im Rahmen der Aufgaben der militärischen Landesverteidigung, durchzuführen. Dabei ist folgender Beurteilungsdreiklang anzuwenden: Wer, hat was/wen, mit welcher Intention angegriffen?⁹³⁶ Hier muss zuerst das Ziel betrachtet werden, welches für den Einsatz des Militärs von zweierlei Gestalt sein kann: Einerseits Einrichtungen des Militärs selbst oder andererseits Einrichtungen von Relevanz für die Souveränität Österreichs. Sind die Ziele relativ einfach zu fassen, hat man bei Intention und Akteur, auf Grund der Beschaffenheit des Cyberspace, schon einige Schwierigkeiten, diese genau herauszufinden.

Unabhängig von diesen beiden Faktoren fällt ein Angriff, der nicht gegen die Souveränität des Staates gerichtet ist, unter eine allgemeine Gefahr für Leben, Gesundheit, Sicherheit, öffentliche Ruhe und Ordnung im Inneren.⁹³⁷ Hier ist die Führungsverantwortung rechtlich eindeutig bei der Sicherheitspolizei.⁹³⁸ Bei der hohen Vernetzung, der verschiedenen

⁹³⁰ BMLV, Merkblatt für das Bundesheer, Raumschutz, 2000, S. 14.

⁹³¹ Vgl. Republik Österreich, Beilagen zu den stenographischen Protokollen des Nationalrates, 15. Band, Wien, 1974, Beilage 1461, S. 6.

⁹³² Vgl. BMLVS, ÖSCS, Ersuchen um rechtliche Würdigung, Stellungnahme, 2012, S. 3.

⁹³³ Vgl. Artikel 79 B-VG.

⁹³⁴ Vgl. § 3 Bundesgesetz über die Organisation der Sicherheitsverwaltung und die Ausübung der Sicherheitspolizei (Sicherheitspolizeigesetz – SPG) BGBl. Nr. 566/1991 idF BGBl. I Nr. 56/2018.

⁹³⁵ Vgl. BMLVS, ÖSCS, Ersuchen um rechtliche Würdigung, Stellungnahme, 2012, S. 3.

⁹³⁶ Vgl. ebd., S. 4.

⁹³⁷ Vgl. ebd., S. 4.

⁹³⁸ Vgl. § 3 SPG.

staatlichen und nichtstaatlichen Systeme, ist die Identifikation, welche Systeme Relevanz für die Souveränität besitzen, nicht einfach zu beantworten. Souveränität kann im Cyberspace nicht rein territorial gefasst werden. Diesem Problembereich wurde in der Arbeit an anderer Stelle bereits nachgegangen.

Auf Ebene des Verfassungsrechts ist der Zweck des ÖBH normiert. Dieser ist explizit im Bundes-Verfassungsgesetz angeführt und für das ÖBH als einzigem Verwaltungsorgan auf dieser Ebene zugeordnet.⁹³⁹ Der primäre Zweck des ÖBH ist demnach die militärische Landesverteidigung, hinzukommen noch Assistenzen, die das ÖBH auf Anforderung durch zivile Behörden zu leisten hat. Alle weiteren Aufgaben des ÖBH sind ebenfalls verfassungsgesetzlich zu regeln.⁹⁴⁰

Dies trifft so auch auf die Mitwirkung im internationalen Krisenmanagement und die Solidarbeitragsleistung im Rahmen der Europäischen Union (EU) zu. Diese Auslandseinsätze sind zum einen im Bundesverfassungsgesetz über Kooperation und Solidarität bei der Entsendung von Einheiten und Einzelpersonen in das Ausland (KSE-BVG)⁹⁴¹ und zum anderen in der Bundesverfassung⁹⁴² geregelt. Die Aufgaben, welche sich aus dem Zweck des ÖBH im B-VG ergeben, werden im Wehrgesetz näher definiert.⁹⁴³

Es sind hier vier originäre Kernaufgaben formuliert, die in der Österreichischen Sicherheitsstrategie bzw. in der Teilstrategie Verteidigungspolitik auch als verteidigungspolitische Aufgaben des ÖBH bezeichnet werden. Auch hier steht der militärische Beitrag zur Landesverteidigung an erster Stelle, gefolgt von der sicherheitspolizeilichen Assistenz, der Assistenz zur Katastrophenhilfe und den Auslandseinsätzen in der oben beschriebenen Form.⁹⁴⁴

Alle Aktivitäten des ÖBH und dienstlichen Aktivitäten seiner Angehörigen haben sich im verfassungsrechtlichen Rahmen zu bewegen. Sind diese Tätigkeiten nicht unter die genannten Aufgaben subsumierbar, haben sie zu unterbleiben. Dies gilt auch für den Einsatz des Bundesheeres im Cyberraum. Abgeleitet vom Zweck, den Aufgaben und den Befugnissen des ÖBH, also den rechtlichen Rahmenbedingungen, lassen sich im Wesentlichen drei Einsatzfälle konstruieren.

⁹³⁹ Vgl. Artikel 79 B-VG.

⁹⁴⁰ Vgl. Artikel 79 Abs. 3 B-VG.

⁹⁴¹ Vgl. Bundesverfassungsgesetz über Kooperation und Solidarität bei der Entsendung von Einheiten und Einzelpersonen in das Ausland (KSE-BVG) BGBl. I Nr. 38/1997 idF BGBl. I Nr. 35/1998.

⁹⁴² Vgl. Artikel 23j Abs. 3 B-VG.

⁹⁴³ Vgl. § 2 Abs. 1 Wehrgesetz 2001 – WG 2001 BGBl. I Nr. 146/2001.

⁹⁴⁴ Vgl. § 2 Abs. 1 lit. a-d WG 2001.

8.4.5 Einsatzfälle im Rahmen von Cyber Angriffen

8.4.5.1 Einsatz zur Eigensicherung militärischer IKT-Infrastruktur

Sofern die militärische IKT-Infrastruktur als militärisches Rechtsgut⁹⁴⁵ verstanden werden kann, ist ein Angriff auf dieses⁹⁴⁶, im Zuge eines Cyber Angriffs, im Rahmen des Wachdienstes zum Eigenschutz zu beenden.⁹⁴⁷ Dies gilt dann, wenn der Angriff eine strafrechtlich relevante Handlung darstellt und somit etwa mit dem Ziel erfolgt, in ein militärisches Netz einzudringen, militärische Computersysteme zu stören, zu beschädigen oder zu zerstören.

Der Wachdienst muss dabei dem militärischen Organ gemäß Militärbefugnisgesetz durch besonderen Auftrag, dem Wachauftrag gem. der Allgemeinen Dienstvorschrift für das Bundesheer (ADV), angeordnet worden sein.⁹⁴⁸ Eine Ausnahme stellt hier das subsidiäre Einschreiten anderer militärischer Organe ohne besonderen Auftrag bei Gefahr in Verzug dar. Das heißt, der Cyber Angriff steht unmittelbar bevor oder findet schon statt und geeignete Organe sind zu dessen Abwehr nicht verfügbar.

Die Befugnis zur Beendigung von Angriffen gegen militärische Rechtsgüter betrifft nur aktuelle, also laufende oder unmittelbar bevorstehende Angriffe. Präventive Maßnahmen sind hier nicht berücksichtigt, können aber im Rahmen der Befugnisse der nachrichtlichen Abwehr angewandt werden.⁹⁴⁹ Unter dem Grundsatz der Verhältnismäßigkeit sind Zwangsmaßnahmen, etwa das Eindringen in fremde Netze oder das Stören, Beschädigen oder Zerstören fremder Computersysteme, zur Beendigung eines Angriffes erlaubt.⁹⁵⁰

Da österreichische Organe Hoheitsgewalt nur auf österreichischem Staatsgebiet ausüben dürfen, richten sich die Gegenmaßnahmen nur auf fremde IKT-Infrastruktur auf österreichischem Staatsgebiet. Bei der Befugnisausübung im Ausland sind entsprechende völkerrechtliche Grundlagen zu beachten.

Erfolgt ein Angriff im Cyberraum aus dem Ausland gegen das Bundesheer, so sind zunächst die völkerrechtlichen Grundlagen zu berücksichtigen. Hier fehlt im Völkerrecht eine ausdrückliche Grundlage, die ein Tätigwerden im Ausland, zum Zwecke des Eingriffs in eine fremde staatliche Souveränität, rechtfertigen könnte.⁹⁵¹ Es gibt hier im Bereich der Völkerrechtslehre einige Konzepte und Überlegungen, die vor allem die

⁹⁴⁵ Vgl. § 1 Abs. 7 Bundesgesetz über Aufgaben und Befugnisse im Rahmen der militärischen Landesverteidigung (Militärbefugnisgesetz – MBG) BGBl. I Nr. 86/2000 idF BGBl. I Nr. 32/2018.

⁹⁴⁶ Vgl. § 1 Abs. 8 MBG.

⁹⁴⁷ Vgl. § 6a MBG.

⁹⁴⁸ Vgl. § 22 Abs. 2 Verordnung der Bundesregierung vom 9. Jänner 1979 über die Allgemeinen Dienstvorschriften für das Bundesheer (ADV) BGBl. Nr. 43/1979 idF BGBl. II Nr. 362/2014.

⁹⁴⁹ Vgl. §§ 21 ff MBG.

⁹⁵⁰ Vgl. §§ 16 ff MBG.

⁹⁵¹ Vgl. BMLVS, Rechtliche Rahmenbedingungen der Abwehr von Cyber-Angriffen durch das Bundesheer, GZ S91018/17-GrpPräsRechtLeg/2017, Rechtsgutachten, 2017, S. 3f.

Verantwortung von Staaten für Handlungen auf und aus ihrem Staatsgebiet heraus behandeln.

Zum einen sind Staaten für die Handlungen ihrer Organe verantwortlich, zum anderen tragen sie die völkerrechtliche Verantwortung dafür, dass innerhalb ihres Hoheitsbereichs keine Handlungen geschehen, die andere Staaten in ihren Rechten verletzen. In Bezug auf den Cyberraum bedeutet das, dass die Nutzung von Cyber Einrichtungen, auf dem Hoheitsgebiet dieses Staates, nicht für Angriffe gegen andere Staaten missbraucht werden dürfen.⁹⁵²

Sind Erkenntnisse vorhanden, die nahelegen, dass Einrichtungen, wie Server oder Netze, zu Cyber Attacken gegen andere Staaten genutzt werden, so hat der betreffende Staat einzuschreiten.⁹⁵³ Dies hat allerdings nach seinen technologischen Möglichkeiten zu erfolgen. In jedem Fall ist der betreffende Staat dazu verpflichtet Schutzlücken zu schließen, an der Aufklärung des Vorfalls mitzuwirken und eine Wiedergutmachung zu leisten. In diesem Zusammenhang sind Staaten auch für Handlungen nichtstaatlicher Akteure auf ihrem Territorium in einem gewissen Ausmaß verantwortlich.⁹⁵⁴

Ein Staat, der durch völkerrechtswidriges Verhalten verletzt wurde, ist berechtigt, Gegenmaßnahmen in einem verhältnismäßigen Umfang zu ergreifen. Diese Maßnahmen dürfen allerdings nicht die Schwelle eines bewaffneten Konfliktes überschreiten. Diese Maßnahmen richten sich gegen den Staat, der seiner Verpflichtung zur Verhinderung einer Cyber Attacke nicht nachgekommen ist.⁹⁵⁵ Die Verhältnismäßigkeit bezieht sich daher nicht auf den Angriff selbst, sondern auf die Verletzung durch den zur Verhinderung verpflichteten Staat.

Hier ergibt sich die Schwierigkeit, die Folgen von Gegenmaßnahmen im Cyberraum abschätzen zu können. Daher gibt es zurzeit auch keine Darstellung zulässiger Cyber Gegenmaßnahmen. Abgeleitet daraus bedeutet dies für das ÖBH, dass offensive militärische Gegenmaßnahmen, gegen Einrichtungen im Ausland, aus völkerrechtlicher Sicht zu unterbleiben haben. Zulässig ist vielmehr den Staat, von dessen Hoheitsbereich der Angriff ausgeht, darüber zu informieren und ihn um Mithilfe bei der Verhinderung und Aufklärung zu ersuchen, dies kann bis zu einem Amtshilfeersuchen zur Mithilfe bei der Strafrechtspflege führen.⁹⁵⁶

8.4.5.2 Einsatz im Rahmen der militärischen Landesverteidigung

Im Rahmen der militärischen Landesverteidigung kann es auch zu Handlungen im Cyberraum kommen. Dabei können, auch im Cyberraum, nicht nur Angriffe von außen relevant sein, sondern, wie bereits beschrieben, auch Vorgänge im Inneren, wenn sie denn im Zusammenhang mit drohenden

⁹⁵² Vgl. Schmitt, 2017, Rule 6, S. 30ff.

⁹⁵³ Vgl. ebd., Rule 7, S. 43ff.

⁹⁵⁴ Vgl. Schaller, 2014, S. 9.

⁹⁵⁵ Vgl. Schmitt, 2017, Rule 7 (28), S. 50.

⁹⁵⁶ Vgl. BMLVS, Rechtliche Rahmenbedingungen der Abwehr von Cyber-Angriffen durch das Bundesheer, Rechtsgutachten, 2017, S. 5.

Gefahren von außen stehen und zudem eine wirksame Abwehr nur mit militärischen Mitteln erfolgen kann.⁹⁵⁷

Zielen Cyber Angriffe auf die Souveränität Österreichs ab, mit dem Zweck diese gänzlich oder teilweise auszuschalten, ist der Einsatz des Bundesheeres zur Abwehr angezeigt.⁹⁵⁸ Sofern dies überhaupt erkennbar ist, richten sich die Maßnahmen gegen staatliche oder staatsnahe Akteure, die direkt die Souveränität angreifen oder gegen staatlich gelenkte Organisationen, welche indirekt auf diese wirken.⁹⁵⁹ Einem solchen Einsatz ist eine Einsatzverfügung, durch den für die militärischen Angelegenheiten zuständigen Minister, voranzustellen.

Ist eine Aggression gegen österreichisches Staatsgebiet völkerrechtlich als Krieg zu klassifizieren, so entfällt eine vorangestellte Einsatzverfügung und die militärische Landesverteidigung fängt unmittelbar mit dem Beginn der Feindseligkeiten an.⁹⁶⁰ Dies trifft auch sinngemäß auf eine entsprechende Cyber Attacke zu. Das bedeutet ein Cyber Angriff, mit dem Ziel der gänzlichen oder teilweisen Ausschaltung der österreichischen Souveränität, löst den Verteidigungsfall aus.

In einem solchen Verteidigungsfall kommen die Bestimmungen des Humanitären Völkerrechts zur Anwendung. Gemäß der Satzung der Vereinten Nationen ist die Drohung mit oder die Anwendung von Gewalt gegen das Hoheitsgebiet oder die Streitkräfte eines anderen Staates untersagt.⁹⁶¹ Ausgenommen von diesem generellen Gewaltverbot ist die staatliche Selbstverteidigung oder eine zulässige Sanktion eines zentralen Organs, wie dem Sicherheitsrat der VN.^{962 963}

Die staatliche Selbstverteidigung greift allerdings nur im Zusammenhang mit einem bewaffneten Angriff und bei eindeutiger Zuordenbarkeit (direkt oder indirekt, s.o.) an einen anderen Staat. Die Frage, ob ein Cyber Angriff die Kriterien eines bewaffneten Angriffs erfüllt, unterliegt in der gängigen Lehrmeinung dem sogenannten effektbasierten Zugang, wonach die Auswirkung bzw. Wirkung einer Cyber Attacke jener eines kinetischen Angriffs gleich sein muss, um als bewaffneter Angriff aufgefasst zu werden.

Wenn ein Cyber Angriff zwar schwerwiegende Folgen für einen Staat hat, aber die Wirkung nicht der eines bewaffneten Angriffs gleichzusetzen ist, herrscht derzeit keine Klarheit darüber, ob solche Attacken als bewaffnete Angriffe zu werten sind. Auf Grund der Zweifel in diesem Fall ist eine Anwendung des HVR nicht angezeigt. Erfolgt nun ein bewaffneter Angriff auf Österreich, so ist die für die militärische Reaktion maßgebliche

⁹⁵⁷ Vgl. Republik Österreich, Beilagen zu den stenographischen Protokollen des Nationalrates, 15. Band, Wien, 1974, Beilage 1461, S. 5.

⁹⁵⁸ Vgl. BMLVS, ÖSCS, Ersuchen um rechtliche Würdigung, Stellungnahme, 2012, S. 2f.

⁹⁵⁹ Vgl. Republik Österreich, Beilagen zu den stenographischen Protokollen des Nationalrates, 15. Band, Wien, 1974, Beilage 1461, S. 5.

⁹⁶⁰ Vgl. ebd., S. 6.

⁹⁶¹ Vgl. Charta der Vereinten Nationen, Kapitel I, Artikel 2, Abs. 4.

⁹⁶² Vgl. ebd., Kapitel VII, Artikel 51.

⁹⁶³ Vgl. Schmitt, 2017, Rule 71, S. 339ff.

Rechtsgrundlage das HVR; dies ist auch im Rahmen eines Cyber Angriffs, unter oben genannten Gesichtspunkten, heranzuziehen.

8.4.5.3 Einsatz im Rahmen des sicherheitspolizeilichen Assistenzeinsatzes

Ist weder das Bundesheer selbst noch die Souveränität Österreichs das Ziel einer Cyber Attacke, sondern sind die verfassungsmäßigen Einrichtungen, die demokratischen Freiheiten der Einwohner oder die innere Ordnung und Sicherheit Österreichs gefährdet, so fällt diese Aufgabe an die Sicherheitsbehörden.⁹⁶⁴ Im Rahmen der sicherheitspolizeilichen Assistenz besteht die Möglichkeit das Bundesheer für eine Unterstützungsleistung anzufordern.⁹⁶⁵

Diese Hilfe ist nur dann zulässig, wenn die Sicherheitsbehörden die Situation nicht mit eigenen Ressourcen bewältigen können. Für die Organe des Bundesheeres kommen jene Befugnisse zu Anwendung, über die die anfordernde Sicherheitsbehörde verfügt.⁹⁶⁶ Diese Befugnisse sind vor allem in den für die primär zuständige Sicherheitsbehörde relevanten Bundesgesetzen geregelt. Beispielhaft sind hier das Sicherheitspolizeigesetz und das Waffengebrauchsgesetz genannt.

Die zuständige Sicherheitsbehörde kann die Befugnisse für das Bundesheer allenfalls auch einschränken. Die zur Anwendung gebrachten militärischen Mittel leiten sich aus der Primäraufgabe der militärischen Landesverteidigung ab. Es können keine Strukturen oder Ressourcen durch die Leistung möglicher Assistenzen begründet werden.⁹⁶⁷

8.5 Zwischenergebnis zum Recht des Cyberwar

Durch den Cyberspace werden viele verschiedene Rechtsgebiete berührt. Dieser Raum ist somit kein rechtsfreier Raum. Auf Grund seiner Beschaffenheit ist die Anwendbarkeit des nationalen Rechtsrahmens an internationale Kooperationen gebunden. Die Anwendbarkeit des HVR, im Rahmen eines Konfliktes im Cyberspace, scheint hier, hinsichtlich des internationalen Charakters des Cyberspace, einfacher. Jedoch bedarf es einer vergemeinschaftlichten Sichtweise. Gemeinsame Definitionen und Interpretationen, sowie daraus abgeleitet eine gemeinsame Sprache, sind als Bedingung, für die Anwendung des Völkerrechts im Netz, zu sehen.

Die internationalen Akteure haben für den militärischen Einsatz entsprechende Fähigkeiten definiert. Im Rahmen der Cyber Defence ist ein gesamtheitlicher Ansatz zu erkennen. In den verschiedenen nationalen Cyber Strategien sind vor allem Maßnahmen gegen Cyber Kriminalität und Cyber Terrorismus festgeschrieben. Eine Ausrichtung an einem möglichen Cyberwar wird nur von wenigen Nationen explizit erfasst. Dieser blinde Fleck in den nationalen Strategien muss zumindest auf konzeptiver Ebene erfasst

⁹⁶⁴ Vgl. Anlage Teil 2 H zu § 2 BMG.

⁹⁶⁵ Artikel 79 Abs. 2 Z. 1 B-VG.

⁹⁶⁶ Vgl. BMI, Richtlinie über die Zusammenarbeit zwischen Sicherheitsexekutive und Bundesheer im Assistenzeinsatz (RLAsE), ZI. BMI-EE2510/0004-II/2/b/2017, S. 16.

⁹⁶⁷ Vgl. ebd., S. 9.

und beseitigt werden. Es bedarf, auf Grund des internationalen Charakters des Cyberspace, einer gemeinsamen Begriffsbasis in den Strategien, um auf internationaler Ebene Schnittstellen zu schaffen.

Die Abgrenzung zwischen Krieg und Verbrechen im Netz stellt die Voraussetzung dar, um Verantwortungen an die Organe des Staates zu übertragen. Dabei spielen Intention und Intensität eine entscheidende Rolle. Instrumente, die es ermöglichen beides festzustellen, müssen zum Einsatz gebracht werden. Dies führt nicht nur zur Zuweisung, wer für die Schadhandlungen im Netz zuständig ist, sondern legt auch die Basis dafür, welches Recht zur Anwendung gelangt.

Wenn man sich der Frage nach den gesetzlichen Grundlagen für das Handeln des Militärs, im Speziellen des Österreichischen Bundesheeres, im Cyberraum stellt, berührt man im Wesentlichen drei große Rechtsbereiche. Dies sind die nationalen Rechtsnormen, das Europarecht und die völkerrechtlichen Normen. Das Österreichische Bundesheer unterliegt, je nach Einsatz, einem oder mehreren dieser Normenkomplexe.

Das Militär ist grundsätzlich für den Einsatz im Krieg vorgesehen, als „ultima ratio“ eines Gemeinwesens bzw. Staates. Wann ein solcher Krieg im Cyberraum vorliegt, ist nicht klar zu definieren. Hier behindern viele Einflussfaktoren eine eindeutige Definition des Kriegszustandes in diesem neuen Handlungsraum des Menschen. Dennoch gibt es, abseits der Deutungshoheit der Politik⁹⁶⁸ in Bezug auf den Kriegszustand im Netz, rechtliche Normen, die ein Einschreiten des Militärs im Cyberraum regeln.

Hier steht vor allem die Frage nach den rechtlichen Möglichkeiten, Cyber Angriffe wirksam abwehren zu können, im Fokus der Betrachtung. Es werden teils Forderungen nach eigenen Rechtsgrundlagen zu dieser Thematik artikuliert und dieser Forderung in den verschiedenen Normenkomplexen auch teilweise entsprochen. Neben Absichtserklärungen, vor allem in Form verschiedener Strategiedokumente, sind sowohl auf völker-, europa- und nationalrechtlicher Ebene verschiedene Normen hinsichtlich der Cyber Thematik vorhanden bzw. geschaffen worden.

Das Österreichische Bundesheer ist dem Zweck nach in der Bundesverfassung niedergeschrieben. Dieser Zweck ergibt die vom Bundesheer zu erfüllenden Aufgaben. Die Aufgaben und daraus abgeleitet die Befugnisse des ÖBH und seiner Angehörigen, in Ausübung ihres Dienstes, sind somit verfassungsrechtlich verankert.

Für den Einsatz des ÖBH im Cyberraum ergeben sich verschiedene Szenarien, welche mit unterschiedlichen rechtlichen Grundlagen abzudecken sind. Während der Eigenschutz, hauptsächlich durch das Militärbefugnisgesetz, in Zusammenhang mit dem Strafgesetz, als Grundlage für ein Einschreiten des Bundesheeres im Inland, abgedeckt ist, stellt sich die Lage bei Cyber Angriffen aus dem Ausland (außerhalb eines bewaffneten Konflikts) sehr eingeschränkt dar.

⁹⁶⁸ Vgl. Hofstetter, 2019, S. 181.

Hier kommt vor allem die Verantwortlichkeit jenes Staates zum Tragen, von dem aus der Angriff erfolgt. Ein Eingreifen in die Souveränität eines fremden Staates entbehrt einer ausdrücklichen rechtlichen Grundlage. Der Eigenschutz militärischer IKT-Infrastruktur, im Rahmen eines Auslandseinsatzes, wäre noch gesondert zu untersuchen. Auf jeden Fall bleibt die Möglichkeit, den Staat, von dem aus der Angriff erfolgte, um Mithilfe bei der Verhinderung und Aufklärung zu ersuchen.

Im Rahmen der militärischen Landesverteidigung ist das ÖBH ermächtigt, Angriffe aus dem Cyberraum abzuwehren, die auf die Ausschaltung der Souveränität (gänzlich oder teilweise) abzielen. Gerichtet sind diese Abwehrmaßnahmen gegen Akteure, die direkt, als staatliche bzw. staatsnahe Handelnde, oder indirekt, als staatlich gelenkte Organisation, gegen die Souveränität Österreichs vorgehen.⁹⁶⁹ Ein solcher Cyber Angriff, der Österreichs Souveränität zum Ziel hat, löst unmittelbar den Verteidigungsfall aus. In diesem Fall greifen die Bestimmungen des HVR.

In Bezug auf die Anwendung militärischer Gewalt, ist im Zusammenhang mit der Satzung der VN zu berücksichtigen, dass nach geltender Lehrmeinung erst dann ein bewaffneter Angriff vorliegt, wenn die Auswirkungen der Cyber Attacke gleich denen eines kinetischen Angriffs sind. Ist das nicht der Fall, so sind die Maßnahmen, die zu setzen sind, nicht militärischer Natur und die Bestimmungen des HVR kommen nicht zur Anwendung. Es müssen für das militärische Einschreiten also zumindest eine von zwei Bedingungen erfüllt werden.

Zielt der Cyber Angriff eines staatlichen oder staatsnahen Akteurs direkt auf die Souveränität Österreichs ab, so tritt der Verteidigungsfall ein. Nimmt die Cyber Attacke die Ausmaße eines kinetischen Angriffs an und liegt somit ein bewaffneter Angriff auf Österreich vor, so tritt der Selbstverteidigungsfall nach der Satzung der VN ein. In beiden Fällen ist das ÖBH der Hauptträger der Abwehrmaßnahmen.

Auf Ersuchen der Sicherheitsbehörden ist das ÖBH ebenfalls, im Rahmen einer sicherheitspolizeilichen Assistenz, befugt Cyber Angriffe abzuwehren, die nicht auf das Bundesheer selbst oder die Souveränität Österreichs abzielen. Hier ist die Aufrechterhaltung der inneren Ordnung und Sicherheit im Fokus des Einschreitens der Sicherheitsbehörden und damit auch des ÖBH. Neben dem Eigenschutz und der Unterstützung der Sicherheitsbehörden liegt das Schwergewicht der Handlungen des ÖBH vor allem in der militärischen Landesverteidigung im Cyberraum.

Im Folgenden werden die Erkenntnisse aus den Zwischenergebnissen zusammengefasst dargestellt und darauf aufbauend wird die operative Führungsverantwortung für Cyber Attacken, an Hand der Kategorisierung von Kritischen Infrastrukturen, der Klassifizierung von Cyber Angriffen und

⁹⁶⁹ Anm. d. Verf.: Ist der Angreifer nicht staatlicher oder staatsnaher Natur, so ist eine klare Zuordnung eines souveränitätsrelevanten Angriffes an das Militär, nach vorherrschender Lehrmeinung, völkerrechtlich nicht möglich. Das Völkerrecht bezieht sich in erster Linie auf völkerrechtssubjekte als mögliche Gefährder der Souveränität von Gemeinwesen. Angesichts der Möglichkeiten einzelner Akteure im Cyberraum ist diese Sichtweise durchaus diskussionswürdig.

der Deeskalation von Führung, abgeleitet und Methoden dargestellt welche diese Zuordnung unterstützen.

9 Synopse und Zusammenfassung

„[...] wird die virtuelle Welt
die bestehende Weltordnung weder
überholen noch erneuern.
Stattdessen wird sie fast
alles komplizierter machen.“
Eric Schmidt⁹⁷⁰

In der Synopse werden die Erkenntnisse und Ableitungen aus dem Argumentum dargestellt. Es werden die wesentlichen Aussagen aus Sicht des Verfassers angeführt und daraus die Ableitungen getroffen, um so die Forschungsfrage beantworten zu können. Die Zusammenfassung der Erkenntnisse bildet dabei den Ausgangspunkt für die Argumentation einer möglichen Aufgaben- bzw. Kompetenzzuordnung bei Angriffen im und aus dem Cyberraum.

Es werden Möglichkeiten dargestellt, wie in einem solchen Fall die Führungsverantwortung zugeteilt werden sollte. Basierend auf der Darstellung wesentlicher Bereiche der Kritischen Infrastruktur und deren Kategorisierung wird ein Verfahren zur Beurteilung der Zuständigkeit der Organe der bewaffneten Staatsgewalt vorgestellt. Dieses richtet sich an den wesentlichen Beurteilungskriterien – der Souveränitätsrelevanz, der Intensität eines Angriffs und dessen Intention – für die Identifizierung eines Cyberwar aus.

Nach der Erläuterung dieses Verfahrens wird, in Bezug auf die Beantwortung der Forschungsfrage, auf den Begriff der Führung eingegangen und welche Bedeutung die unterschiedlichen Ausprägungen von Führung auf den verschiedenen Führungsebenen, für den Cyberwar und die Behandlung desselben durch das Militär, aufweisen. Abschließend wird ein Ausblick auf künftige Entwicklungen gegeben, um hier eine gewisse Sensibilisierung vor allem in den Entscheidungsgremien der beiden hauptverantwortlichen Ministerien und anderer politischer Institutionen zu erreichen.

9.1 Zusammenfassung der Zwischenergebnisse

Um den Cyberspace als Konfliktraum fassen zu können, bedarf es einer klaren begrifflichen Aufarbeitung. Hierzu muss eine genaue Betrachtung des Wesens der verschiedenen Konfliktformen durchgeführt werden. Dabei wird vom Allgemeinen auf das Spezielle geschlossen. Der Krieg als politisches Instrument ist dabei die Domäne des Militärs. Das deshalb, weil bei Auflösung eines Rechtsrahmens die Handlungsfähigkeit der anderen Träger der bewaffneten Staatsgewalt limitiert ist. Hier hilft auch das politische Moment des Krieges, da Politik grundsätzlich einer Gemeinschaft bedarf.

Der Krieg wirkt zwischen und innerhalb von Gemeinwesen, daher muss sich die Identifikation eines Konfliktes an diesen orientieren.

⁹⁷⁰ Schmidt/Cohen, 2013, S. 365f.

Bedrohungen sind gemeinschaftsstiftend und erhöhen die Sicherheit des Einzelnen. Diese Sicherheit ermöglicht das unbeeinflusste Handeln des Gemeinwesens, seine Souveränität. Ziel eines kriegerischen Aktes ist stets diese Handlungsfähigkeit oder aber die Beeinflussung eines Gegners bestimmte Handlungen zu setzen oder zu unterlassen. Im Sinne von Clausewitz geht es um den Willen des Gegners.

Je nach Art der Akteure kann zwischen Großem und Kleinem Krieg unterschieden werden. Dabei ist der Große Krieg die gehegtere Form und je mehr Akteure zu den regulären Streitkräften hinzutreten, also der Kleine Krieg hinzukommt, desto umfassender, totaler wird der Krieg. Aus den unterschiedlichen Akteuren lassen sich auch unterschiedliche Zuständigkeiten ableiten. Da der Krieg sich in unterschiedlichen Ausprägungen präsentiert und dies durch technologische Entwicklungen unterstützt wird, kommen neue Konfliktformen zum Vorschein.

Der Cyberraum als neuer Handlungsraum des Menschen besteht aus verschiedenen aufeinander abgestützten Komponenten, neben den physischen Bestandteilen sind dies vor allem die Informationen bzw. Daten im Netz und schließlich der Mensch als Nutzer selbst. Der Mensch ist in der Lage, Handlungen im und aus diesem Raum heraus zu setzen. Damit bleiben diese Interaktionen nicht allein in einer virtuellen Realität verortet, sondern zeitigen auch Effekte in der Realität. Von einer rein territorialen Betrachtung ist allerdings abzusehen und vielmehr ein systemischer Ansatz zu verfolgen. Der Cyberspace ist aber nicht nur Handlungs- sondern auch Konfliktraum auf unterschiedlichen Ebenen. Daraus ergibt sich auch eine Relevanz für die rechtliche Eingrenzung dieser Handlungen im Cyberspace.

Obwohl territorial schwer fassbar, ergeben sich verschiedene Rechtsgebiete, der Cyberspace ist damit kein rechtsfreier Raum. Besitz und Eigentum sind zum Beispiel durch Daten ebenso repräsentiert wie durch Gegenstände in der realen Welt. Somit sind auch Verletzungen dieser Bereiche im Netz möglich. Dies gilt aber nicht nur für das Handeln einzelner Personen, sondern auch für das Agieren von Gruppen von Menschen bis hin zu Staaten oder anderen Formen von Gemeinwesen. Die Schwierigkeit, die sich dabei in der Zuweisung der Verantwortung und damit auch in der rechtlichen Verortung ergibt, liegt in der Auflösung zwischen Innen und Außen bezogen auf die territoriale Entgrenzung des Cyberspace.

Die physischen Komponenten sind territorial zuordenbar, aber die systemische Zugehörigkeit kann sich durchaus verteilt über ein Territorium hinaus darstellen. Vor allem das Völkerrecht ist auch im Cyberraum noch sehr territorial ausgerichtet. Hier ist eine gemeinsame Sicht auf die rechtliche Behandlung des Raumes notwendig um die Verantwortung bei Konflikten im Netz eindeutiger zuweisen zu können. Es ist jedoch nicht nur von Bedeutung, wo sich Handlungen ereignen, sondern auch welcher Art diese Handlungen sind. Die Rechtsnormen welche von Relevanz sind, sind von Ort und Art der Interaktionen abhängig. Erst daraus kann dann geschlossen werden, wer für die Behandlung der jeweiligen Konfliktart zuständig ist.

Um diese Herausforderung aufzulösen, muss das Phänomen, dieser neuen Kriegsausprägung im Cyberspace, sichtbar gemacht werden. Diese

Form des Krieges zu identifizieren ist allerdings eine große Aufgabe. Hier kann unter dem Deckmantel der Anonymität von verschiedenen Akteuren gewirkt werden. Zu beobachten ist allerdings, dass es hier in der Wahrnehmbarkeit einen Zusammenhang zwischen Sichtbarkeit und Akteur gibt. Staaten agieren dabei eher verdeckt und Akteure mit krimineller Intention sind eher sichtbar. Man kann beim Einsatz staatlicher Cyberkräfte zwei Ausprägungen beobachten. Zum einen den Krieg im Geheimen und zum anderen den Einsatz von Cyberkräften zur Unterstützung konventioneller Streitkräfte.

Der umfassende Große Cyberwar als Krieg im Geheimen steht hier neben dem Kleinen Cyberwar als Mittel von Streitkräften in einem konventionellen Konflikt. Beide Formen des Cyberwar sind als Teil des Kleinen Krieges zu fassen. Die Zuordnung von Verantwortlichkeiten kann sich somit auch an der Form des Cyberwar orientieren. Ausnutzung und Schwächung als Intention sind, neben der Form des Konflikts im Netz und der Ausdehnung desselben, ein weiterer Beurteilungsfaktor. Kleiner und Großer Cyberwar sind Momente des Virtuellen Krieges. Da der Kleine Cyberwar unmittelbar auf militärische Systeme wirkt, ist hier eindeutig die militärische Verantwortung für diese Form des Cyberwar angezeigt.

Treten beide Momente gemeinsam zu Tage, so ist der Virtuelle Krieg in seiner höchsten Intensität angelangt. Hier wirkt der Cyberwar umfassend auf Gemeinwesen ein, es werden durch die Kombination des Kleinen mit dem Großen Cyberwar verschiedene Politikbereiche bewirkt. Vor allem durch den Krieg im Geheimen ist hier eine strategische Wirkung ableitbar. Hier stellt das Militär nur eines von verschiedenen Instrumenten dar. Das hat operative Auswirkungen auf eine Kompetenzzuordnung für die Begegnung dieser Form des Cyberwar.

Die Abgrenzung zwischen den Konfliktformen im Cyberraum, vor allem von Kriminalität zum einen und Krieg zum anderen, sind hier als Voraussetzung zu begreifen, um den Organen der Staatsgewalt die richtigen Aufgaben in diesem neuen Handlungsraum zuzuordnen. Um den Aufgabenbereich des österreichischen Militärs zu fassen, sind drei Rechtsbereiche zu berücksichtigen, das Völkerrecht, das Europarecht und das nationale Recht. Hier ist der Deckungsbereich der drei Normenkomplexe zu finden, um die Aufgaben des Militärs mit diesen in Einklang zu bringen. Kern dieses Deckungs- bzw. Überschneidungsbereiches ist der Souveränitätsbegriff. Die Verletzung der Souveränität ist sowohl in den drei Normenbereichen, wie auch in den diversen Strategien zur Cyber Sicherheit als die Herausforderung für das Militär definiert.

Die verschiedenen nationalen Strategien zur Cyber Sicherheit behandeln die kriminelle und terroristische Bedrohung sehr eingehend, die Rolle des Militärs scheint zwar auf, dies aber nur sehr oberflächlich. Im Wesentlichen sieht man einen gesamtheitlichen Ansatz, der verfolgt wird um das jeweilige Gemeinwesen vor Angriffen im Cyberwar zu schützen. Das zeigt sich besonders stark bei der NIS-Richtlinie der EU, hier werden selbst die Unternehmen, welche sich des Cyberspace bedienen, in die Pflicht genommen einen Beitrag zur gesamtstaatlichen Cyber Sicherheit

beizutragen. Diese Verteilung der Zuständigkeit setzt sich in einer ungeklärten Kompetenzzuordnung fort.

Neben der Souveränität sind auch die Ausdehnung des Angriffs sowie die Absicht, die hinter dem Angriff steht, von Bedeutung bei der Zuordnung zum richtigen Normenkomplex. Für das Militär, im Speziellen für das Bundesheer, kommen in unterschiedlichen Einsatzszenarien verschiedene Rechtsgebiete zur Anwendung. Welcher Normenkomplex wirksam ist und welche Rolle das Militär spielt, ist dabei vom konkreten Einsatzfall abhängig. Wie allerdings dieser Einsatzfall im Cyberraum einzuordnen ist, bleibt eine gewisse Herausforderung.

Festzustellen ist auch, dass der Grad der Vernetzung von Gemeinwesen die Anzahl von Konflikten konventioneller Ausprägung reduzieren kann, aber die Zahl von Konflikten im Netz erhöht. Konflikte unterhalb der Schwelle zum bewaffneten Konflikt sind die Folge, die aber letztlich die konventionellen Streitkräfte benötigen, um den Konflikt zu entscheiden. Der Cyberwar ist somit ein unterstützendes Element des Krieges. Da alle Gemeinwesen über ein Mindestmaß an Vernetzung verfügen und die Wahrscheinlichkeit der Konfliktaustragung im Cyberspace als sehr hoch einzustufen ist, werden im nächsten Abschnitt die Möglichkeiten zur Festlegung der operativen Führungsverantwortung im Falle eines Cyberangriffes dargestellt.

9.2 Möglichkeiten zur Festlegung der Führungsverantwortung bei Angriffen im und aus dem Cyberspace

Um die Schwelle der Zuständigkeit auf Basis der Inhalte der Abhandlung festzulegen, ergeben sich verschiedene Möglichkeiten. Ausgehend von den möglichen Zielen, der Kritischen Infrastruktur eines Gemeinwesens, ist die Ausrichtung an einer Kategorisierung dieser Infrastrukturen eine erste Variante der Festlegung der Führungsverantwortung. Eine weitere Art und Weise diese Verantwortung zuzuordnen liegt in der Klassifizierung eines Cyber Angriffs. Dabei geht es darum, ob dieser die Kriterien eines kriegerischen Aktes im Cyberspace erfüllt oder nicht. Es geht also darum, ob es sich um einen Cyberwar (Großer oder Kleiner Cyberwar) handelt.

Die dritte Variante die Führungsverantwortung festzulegen liegt darin, eine These hinsichtlich der Eskalation bzw. Deeskalation von Führungsverantwortung näher zu beleuchten. Hier spielt die Ebene in der die Führung angesiedelt wird die entscheidende Rolle. Es kann davon ausgegangen werden, dass eine Anhebung (Eskalation) der Führungsverantwortung wesentlich aufwendiger ist als die Führungsverantwortung zu deeskalieren. Gerade bei Vorgängen wie einer Attacke im Cyberspace, die von vorne herein unübersichtlich ist, darf hier kein Nachteil für die dagegen antretenden Kräfte entstehen. Die Betrachtung dieser drei Möglichkeiten stellt wesentliche Antworten für die Zuordnung der Führungsverantwortung bereit.

9.2.1 Die Kategorisierung Kritischer Infrastruktur

Wie in der Abhandlung dargestellt, geht es beim Kampf mit und um Informationen nicht ausschließlich um Ziele in der virtuellen Realität des Cyberspace. Vielmehr liegen diese Ziele in der realen Welt und können, neben der Information, als Kritische Infrastruktur angesprochen werden.⁹⁷¹ Diese Kritische Infrastruktur ist von Natur aus schon mit einer gewissen Relevanz für das Gemeinwesen behaftet. Die Auswirkungen eines Angriffes können die Handlungsfähigkeit beeinträchtigen oder vollends ausschalten. Damit wäre die Relevanz für die Souveränität, also die Handlungsfähigkeit und Unabhängigkeit eines Gemeinwesens in seinen Handlungen, betroffen.

Es muss in diesem Zusammenhang der Begriff der Kritikalität betrachtet werden, also wie äußert sich das Kritische an einer Infrastruktur und wie kann man es kategorisieren. Kritikalität bezieht sich auf die Auswirkungen, welche der Ausfall oder die Beeinträchtigung einer bestimmten Infrastruktur auf das Gemeinwesen hat. Je umfassender diese sind, umso höher ist die Kritikalität. Kritikalität ist also ein Maß dafür, wie stark ein Gemeinwesen durch einen Angriff auf wichtige Einrichtungen betroffen ist. Dieses Ausmaß oder die Kritikalität ist über den Eskalationsbegriff eng mit dem Begriff der Intensität eines Angriffs verbunden.

9.2.1.1 Einteilung Kritischer Infrastruktur nach deren Kritikalität

Kritische Infrastrukturen werden im Allgemeinen nach Sektoren eingeteilt. Diese Sektoren können weiter in Teilsektoren oder sogenannte Branchen unterteilt werden.⁹⁷² Die Einstufung dieser Infrastrukturen und ihrer Teilsektoren ist eine Möglichkeit Führungsverantwortung zuzuweisen, da das Ausmaß eines Angriffes für diese Zuordnung von Bedeutung ist. Die Einteilung erfolgt hierbei nach dem Gesichtspunkt welche Infrastruktur für das Gemeinwesen wie kritisch ist, wie sehr sich also deren Ausfall oder Beeinträchtigung auf andere Bereiche auswirkt. Diesen Faktor bezeichnet man auch als Kritikalität.

„Die Kritikalität bezieht sich dabei auf die Auswirkungen, die bei einem Ausfall, einer Störung oder einer Zerstörung eines Infrastruktur-Objekts entstehen könnten.“⁹⁷³

Dieser Parameter steht somit in direktem Verhältnis zur Intensität, wie sie in der Abhandlung gefasst wird. Für die Intensität eines Konfliktes reicht es nicht aus diese als hoch zu bezeichnen, wenn

„[...] in einem kurzen Zeitraum durch unmittelbare Einwirkung eine hohe Anzahl von Ausfällen erwartbar ist.“⁹⁷⁴

⁹⁷¹ Vgl. Schmidt/Cohen, 2013, S. 120.

⁹⁷² Vgl. Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS, Methode zur Erstellung des SKI-Inventars, 2010, S. 4f.

⁹⁷³ Vgl. ebd., S. 4f.

⁹⁷⁴ BMLVS, Intensität von Auslandseinsätzen, GZ S92107/10-MilStrat/2013, Festlegung der Begriffe, Wien 2013, S. 2.

Bei dem in der vorliegenden Arbeit verwendeten Intensitätsbegriff spielt auch das Ausmaß eines Konfliktes eine Rolle. Damit kommt der Kritikalität eine wichtige Beurteilungsfunktion für Konflikte zu. Kritikalität ist einer der drei Faktoren für die Bestimmung des Eskalationsniveaus, neben der Intensität und der räumlichen Ausdehnung. Kritikalität kann als Ausdehnung hinsichtlich der Akteure verstanden werden. Sie führt die Anzahl der Akteure und die Auswirkungen eines Konfliktes auf diese zusammen. Eine Einbeziehung der Kritikalität in die Beurteilung der Schwelle für die Zuordnung der Führungsverantwortung scheint hier zunächst durchaus angezeigt.

Die Kritikalität ermittelt sich über drei Faktoren: Das Gefahrenpotential, welches von einem Objekt ausgeht, die quantitative und die qualitative Leistung der betreffenden Infrastruktur.⁹⁷⁵ Am Beispiel der Bewertung der Teilsektoren der Kritischen Infrastrukturen der Schweiz kann eine Einstufung dieser in Bezug auf die Kritikalität erfolgen.⁹⁷⁶

Diese Reihung bzw. Einstufung stellt die Bedeutung von Kritischer Infrastruktur für das Gemeinwesen dar. Dabei spielen die gegenseitige Beeinflussung der Sektoren bzw. Teilsektoren – welche Auswirkungen sich auf diese ergeben – und die Beeinflussung von Bevölkerung und Wirtschaft die wesentliche Rolle. Die eigentliche Souveränitätsrelevanz ist hier explizit nicht erfasst. Dennoch können die Systeme erkannt werden, welche für das Gemeinwesen, nicht für dessen Souveränität, relevant sind.

Da Kritische Infrastrukturen von Haus aus als kritisch betrachtet werden müssen, sind hier drei Stufen der Kritikalität (sehr groß, groß und regulär) zu unterscheiden.⁹⁷⁷ Eine Zuordnung der Führungsverantwortung ausschließlich auf Grund dieser Einteilung ist allerdings bei genauerer Betrachtung nicht zweckmäßig. Ein Angriff auf einen Teilsektor großer Kritikalität hat zwar eine weitreichende Wirkung auf das Gemeinwesen, ein Einsatz des Militärs wäre daher angezeigt, doch ist bei der Einteilung der Kritischen Infrastruktur im Zusammenhang mit der Kritikalität auch deren Verwundbarkeit zu betrachten.

9.2.1.2 Einteilung Kritischer Infrastruktur nach deren Verwundbarkeit

Verwundbarkeit ist ein gefahrenspezifischer Faktor, der im Weiteren auch von Raum und Zeit abhängig ist.⁹⁷⁸ Die Verwundbarkeit der Kritischen Infrastrukturen orientiert sich, im Konnex mit dem Cyberspace, an der Gefahr eines Cyber Angriffs. Unter Verwundbarkeit bzw. Vulnerabilität ist

„[...] die gefahrenspezifische Anfälligkeit einer Kritischen Infrastruktur für Beeinträchtigung oder Ausfall ihrer Funktionsfähigkeit, welche zur Unterbrechung der Versorgung der Bevölkerung mit wichtigen Gütern und Diensten führen können.“⁹⁷⁹

⁹⁷⁵ Vgl. Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS, Methode zur Erstellung des SKI-Inventars, 2010, S. 7ff.

⁹⁷⁶ Vgl. ebd., S. 6.

⁹⁷⁷ Vgl. ebd., S. 6.

⁹⁷⁸ Vgl. Lenz, Susanne: Vulnerabilität Kritischer Infrastrukturen, Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), Band 4, 2009, S. 31ff.

⁹⁷⁹ Ebd., S. 30.

zu verstehen.

Um die Verwundbarkeit bezüglich einer Cyber Attacke zu bestimmen, müssen verschiedene Parameter analysiert werden. Der Grad der Verwundbarkeit für Cyber Angriffe wird an Hand des Assessment-Verfahrens nach Krings ermittelt.⁹⁸⁰ Zunächst geht es dabei um die Exponiertheit der betreffenden Systeme bzw. von Teilen dieser Systeme. Dabei ist deren Lage und Erreichbarkeit zu beurteilen.⁹⁸¹ Handelt es sich zum Beispiel um besonders gut gesicherte Systeme im Cyberspace oder sind diese direkt mit dem Internet verbunden und daher relativ leicht erreichbar? Auf Grund des Grades der Exponiertheit kann festgestellt werden, ob es Systemkomponenten oder ganze Systeme gibt, die von einem Angriff bzw. Angreifer leicht erreicht werden können.

Es gilt nun weiter zu prüfen, wie funktionsanfällig oder anders ausgedrückt, wie funktionsfähig diese Systeme im Falle eines Cyberangriffes bleiben.⁹⁸² Ist die Funktionsfähigkeit nicht mehr gegeben, stellt sich die Frage, ob die angegriffenen Systeme technisch ersetzbar sind oder deren Funktion von anderen Systemen übernommen werden kann.⁹⁸³ In einem weiteren Analyseschritt sind neben den technischen Voraussetzungen auch personell-organisatorische Faktoren zu prüfen.

Dabei geht es um die Verfügbarkeit von qualifiziertem Personal, welches in der Lage ist, die gegebene technische Substitution umsetzen zu können.⁹⁸⁴ Aus diesem Analyseverfahren resultiert nun die Zuordnung zu verschiedenen Verwundbarkeitsklassen⁹⁸⁵, die in Verbindung mit dem Grad der Kritikalität eine sehr gute Einteilung der Kritischen Infrastrukturen und damit auch der im Cyberspace befindlichen kritischen Systeme ermöglicht. Diese Assessment-Methode dient der Bestimmung des Grades der Verwundbarkeit von Infrastrukturen.

Da die Kritikalität sich ausschließlich mit den Auswirkungen eines Angriffes und der Bedeutung für das Gemeinwesen beschäftigt, sollte auch die Gefährdung hinsichtlich der Angreifbarkeit der Kritischen Infrastruktur untersucht werden. Die Verwundbarkeit gibt nun Auskunft darüber wie leicht ein bestimmtes System angegriffen und damit gestört oder gar zerstört werden kann. Fasst man diese beiden Faktoren nun zusammen, so lässt sich eine plausible Einteilung Kritischer Infrastrukturen bzw. Systeme vornehmen.

⁹⁸⁰ Vgl. Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), Abschätzung der Verwundbarkeit gegenüber Hochwasserereignissen auf kommunaler Ebene, Band 4, 2010, S. 25.

⁹⁸¹ Vgl. ebd., S. 31f.

⁹⁸² Vgl. ebd., S. 33.

⁹⁸³ Vgl. ebd., S. 35.

⁹⁸⁴ Vgl. ebd., S. 36.

⁹⁸⁵ Vgl. ebd., S. 26f.

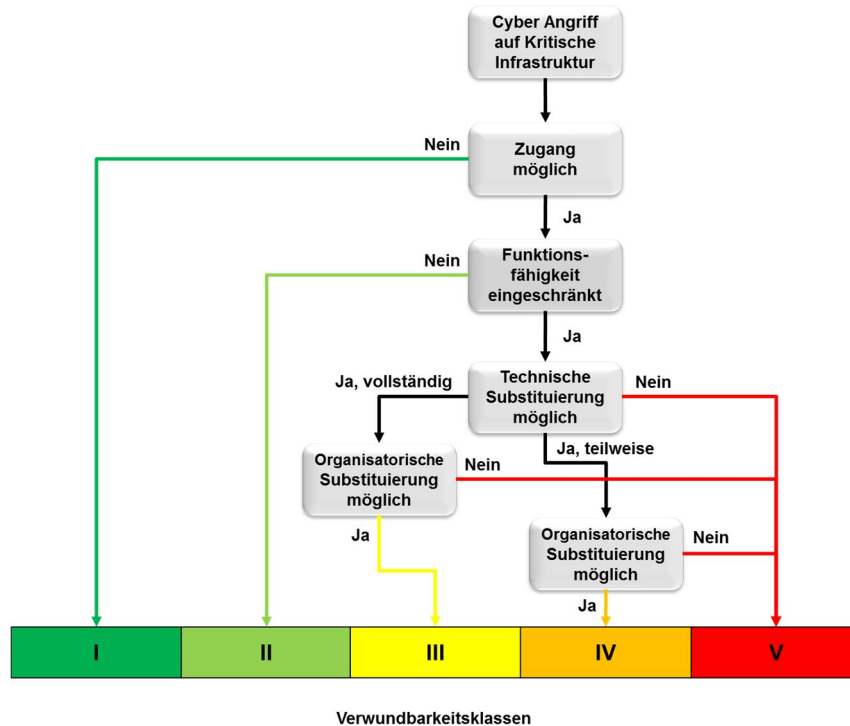


Abbildung 17: Verfahren zur Abschätzung der Verwundbarkeit⁹⁸⁶

Dies ist umso mehr angezeigt, da sich die immanente Verwundbarkeit Kritischer Infrastrukturen in deren Kritikalität – in deren Auswirkung auf das Gesamtsystem – erst dann manifestiert, wenn eine Gefährdung diese Vulnerabilität ausnutzt und konkret wird.⁹⁸⁷ Es herrscht also ein direkter Zusammenhang zwischen Gefahr – einem potentiellen Cyber Angriff –, Verwundbarkeit und Kritikalität, den es bei der Kategorisierung von Kritischer Infrastruktur und Systemen zu berücksichtigen gilt.

Weiter lässt sich in dieser Kategorisierung ein Hinweis auf den Verantwortungsbereich des Militärs finden. Das bedeutet, dass bei Angriffen aus dem Netz auf Systeme, die sowohl eine hohe Verwundbarkeit aufweisen, als auch eine entsprechende Kritikalität besitzen, tendenziell eher das Militär die Führungsverantwortung tragen sollte. Dabei finden wir aber weiterhin wichtige Faktoren unberücksichtigt.

Zum einen die Relevanz für die Souveränität⁹⁸⁸ eines Staates, hier sei nur der oben angeführte Schienenverkehr (sehr große Kritikalität und Verwundbarkeit) erwähnt, der aber für die Handlungsfähigkeit der Regierung eines Gemeinwesens nicht eine entscheidende Rolle spielt. Die Regierung und Verwaltung weist jedoch nur eine große (mittlere) und das Militär eine reguläre (niedrige) Kritikalität auf. Zum zweiten fehlt die Berücksichtigung der Intention eines Angriffes. So sind die meisten Attacken aus dem

⁹⁸⁶ Vgl. ebd., S. 25.

⁹⁸⁷ Vgl. Lenz, 2009, S. 32.

⁹⁸⁸ Anm. d. Verf.: Darunter ist nicht die Kritikalität, im Sinne der Bedeutsamkeit der Kritischen Infrastruktur für das Gemeinwesen, sondern die Bedeutung für dessen Handlungsfähigkeit, zu verstehen.

Cyberspace auf Banken (große Kritikalität und Verwundbarkeit) nicht politischer, sondern krimineller Natur. Bei Cyber Angriffen auf das Militär hingegen ist in der Regel von politisch motivierten Handlungen auszugehen.

Die Zuweisung der Verantwortung an das Militär, bei Angriffen auf Einrichtungen mit sehr großer Kritikalität (und Verwundbarkeit), und die Zuordnung der Führungsverantwortung an die Polizei, bei Angriffen auf Infrastrukturen großer und regulärer Kritikalität (und geringerer Verwundbarkeit), ist in diesem Zusammenhang nicht schlüssig möglich. Die Zuweisung der Führungsverantwortung ausgerichtet an der Kritikalität und Verwundbarkeit scheint daher nur bedingt durchführbar und zweckmäßig, wenngleich die beiden Faktoren in eine Gesamtbeurteilung einfließen müssen. Man kann also allein von der Einteilung der Kritischen Infrastruktur nicht auf eine Führungsverantwortung schließen.

Der zweite Ansatz der Festlegung zur Lösung der Frage, wer nun für Cyber Angriffe ab wann zuständig sein soll, versucht nun die anderen Parameter mit einzuschließen. Hier sollen nun die drei wesentlichen Faktoren in Beziehung zueinander gesetzt werden.

9.2.2 Das Drei-Faktoren-Beurteilungsverfahren der Führungsverantwortung

Die Faktoren, die es hier zu betrachten gilt, sind die Souveränitätsrelevanz, die Intensität und die Intention. Diese Faktoren erlauben es einen Angriff aus dem bzw. im Cyberspace zu kategorisieren. Wenn einer dieser drei Faktoren, hinsichtlich seiner Ausprägung in einem Cyberwar, vorzufinden ist, ist eine klare Zuordnung an das Militär, bezogen auf die Verantwortung für die Begegnung dieser Attacke, gegeben. Ist das Ziel des Angriffes ein souveränitätsrelevantes System, so ist grundsätzlich von einer hohen Intensität auszugehen.

Ein Angriff auf ein solches System hat die Handlungsunfähigkeit des Gemeinwesens, im Speziellen seiner Entscheidungsträger, zur Folge. Um die Souveränitätsrelevanz in eine Einteilung von Kritischer Infrastruktur einfließen zu lassen, müsste die Kritikalität und Verwundbarkeit, hinsichtlich der Entscheidungs- und Handlungsfähigkeit des Staates mitberücksichtigt werden. In der oben angeführten Einteilung ist dies noch entsprechend miteinzubeziehen.

Weiters muss eine Attacke, wenn sie nicht souveränitätsrelevant ist, hinsichtlich Intensität und Intention untersucht und analysiert werden. Ist sie, auf Grund dieser Analyse, dem Cyberwar zurechenbar oder diesem sehr nahe, so fällt die Zuständigkeit in die Verantwortung des Militärs. Wie die Intensität zu fassen ist, muss anlassbezogen bestimmt werden. Der Schwellenwert kann sich dabei auf die Anzahl der betroffenen Systeme oder auf die Höhe des verursachten Schadens beziehen. Es gelten damit, wie bei der Kritikalität schon angeführt, das Gefahrenpotential, quantitative und qualitative Kriterien als wesentliche Parameter.

Wird ein souveränitätsrelevantes System angegriffen, hat das Militär, ungeachtet der Intensität und der Intention, die Führungsverantwortung zu übernehmen. Liegt keine Souveränitätsgefährdung vor, so entscheidet die Intensität über das weitere Vorgehen. Ist die Intensität als niedrig zu beurteilen, so muss letztlich die Intention genauer betrachtet werden. Erst wenn alle drei Parameter als nicht ausschlaggebend beurteilt sind, kann die operative Führungsverantwortung an die Polizei zugeordnet werden. Die Schlüsselgrößen sind somit die Souveränitätsrelevanz, die Intensität und die Intention. Daraus ergibt sich ein möglicher Beurteilungskreislauf für die Zuordnung der Verantwortlichkeit.

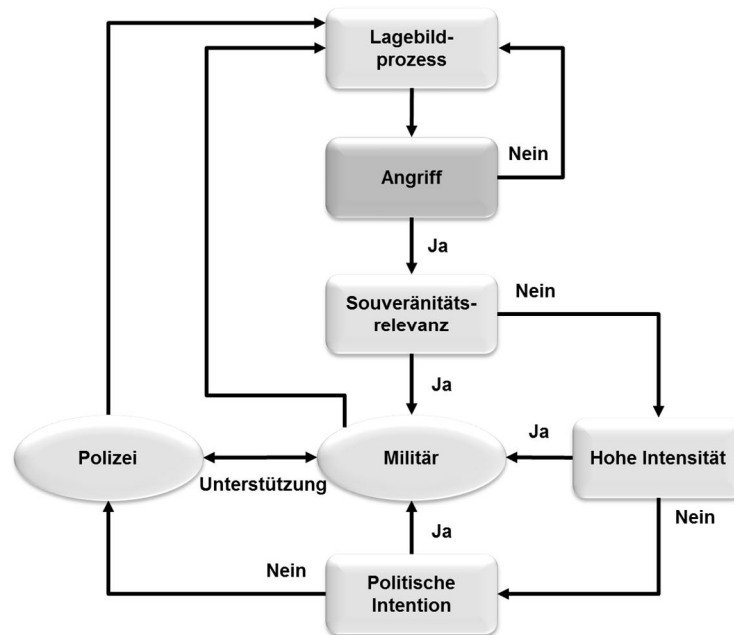


Abbildung 18: Beurteilungskreislauf zur Zuordnung der Führungsverantwortung ⁹⁸⁹

Die ständig durchzuführende Lagefeststellung ist wesentlicher Bestandteil des Beurteilungsprozesses, um festzustellen wem die Führungsverantwortung zugeordnet werden muss. Liegt nun ein Angriff vor, so müssen die oben beschriebenen Faktoren geprüft werden, wobei die folgende Reihung dieser Faktoren die Wichtigkeit aus Sicht des Verfassers darstellt. Um nun die erarbeiteten theoretischen Grundlagen zu operationalisieren, wird jeder Faktor anhand von Beispielen dargestellt. Dabei wird auch auf den Zusammenhang von der Dauer eines Angriffes mit der Relevanz für die Souveränität des Staates näher eingegangen.

9.2.2.1 Souveränitätsrelevanz als primärer Entscheidungsfaktor

Die Souveränitätsrelevanz tritt zwischen zwei Ausprägungen zum Vorschein, der direkten und der indirekten Relevanz. Direkt relevant sind jene Systeme, die für den Staat von entscheidender oder sogar existenzieller Bedeutung sind. Dazu zählen vor allem Einrichtungen des Militärs und der Regierung eines Staates. Diese Einrichtungen können bei Ausfall den Staat

⁹⁸⁹ Abbildung durch den Verfasser erstellt.

handlungsunfähig machen. Indirekt relevante Systeme sind überwiegend Kritische Infrastrukturen, deren Ausfall nicht im ersten Moment zu einer Handlungsunfähigkeit des Gesamtstaates führen, sondern vielmehr mit Andauern der Attacke Probleme für die Sicherheit und Funktionsfähigkeit des Gemeinwesens bedeuten.

Als Beispiel für die indirekte Ausprägung können hier die Stromversorgung und das Finanzwesen eines Landes gesehen werden. Ist der Angriff auf eine Bank für die Kunden dieser meist ein unangenehmer Einschnitt in deren Alltag, welcher meist krimineller Natur ist, so kann hier keine Souveränitätsrelevanz abgeleitet werden. Indirekt relevant für die Handlungsfähigkeit des Gemeinwesens ist der Angriff auf das gesamte Finanzwesen, welcher Börse, Banken und andere Finanzdienstleister trifft.

Ist die Dauer dieses Angriffes entsprechend lang und sind die Menschen nicht in der Lage ihre Zahlungen zu leisten, weil Geldautomaten, elektronische Überweisungs- und Zahlungsmöglichkeiten nicht mehr funktionieren, wird die Relevanz immer direkter. Dies führt zu einem Niedergang der Sicherheitslage und schließlich zur Handlungsunfähigkeit des Staates. Hier erkennt man den Zusammenhang zwischen Souveränitätsrelevanz und Dauer einer Cyber Attacke.

Als Beispiel für eine solche souveränitätsrelevante Attacke im Cyberspace kann der Georgien-Krieg herangezogen werden. Hier wurden Regierungsseiten angegriffen und die Arbeit der Medien im Netz derart behindert, dass zum einen keine unterstützende Kommunikation seitens der Regierung und zum anderen keine Medienarbeit zur Beeinflussung der pro-georgischen Position im Ausland möglich waren.

Im Zusammenhang mit dem konventionellen Angriff Russlands ergab diese Cyber Attacke einen massiven Eingriff in die georgische Souveränität im Netz. Inwieweit auch die Kommunikation der Staatsführung zu den Streitkräften beeinflusst war, bleibt hier unbeantwortet. Egal wie hier auf solch einen Angriff aus rechtlicher Sicht zu antworten ist, liegt in diesem Fall die Führungsverantwortung eindeutig beim Militär.

Für die Zuordnung der Führungsverantwortung ist also der Grad der direkten Souveränitätsrelevanz ausschlaggebend. Dieser Grad ist durch die Beurteilung der Wichtigkeit der Systeme, welche angegriffen werden, zu ermitteln. Dabei ist zu berücksichtigen, dass bei Ausfall von direkt relevanten Systemen die Entscheidung für eine Zuordnung der Führungsverantwortung wahrscheinlich nicht mehr eingeholt werden kann, schließlich handelt es sich hier in der Regel um die Systeme, die es dem Staat ermöglichen seine Geschäfte zu erledigen (Verwaltung, Führung, Entscheidung). Denkt man dabei an den Angriff auf die Entscheidungsebene eines Staates, also die Regierung, wie es in Georgien der Fall war, ist dies mehr als einleuchtend.

Der Cyberspace ist ein anarchisches System ohne Territorialbezug, ein Angriff auf nationale oder besser gesagt unter nationaler Verantwortung stehender Systeme ist stets ein Angriff von außen. In diesem Fall muss vom worst-case ausgegangen und der Angriff als einer auf die Souveränität des

Staates verstanden werden. Dieser Fakt weist darauf hin, dass die Erstverantwortung bei der militärischen Führung liegen sollte.

Kann keine Relevanz für die Souveränität abgeleitet werden – oder ist die Souveränitätsrelevanz nur indirekt gegeben – so muss bei der Zuordnung der Führung, für Einsätze zur Bewältigung eines Angriffes, der nächste Entscheidungsfaktor herangezogen werden.

9.2.2.2 Intensität als sekundärer Entscheidungsfaktor

Hier ist der Fokus auf das Ausmaß des Angriffs gerichtet. Wird der Angriff so geführt, dass Elemente des Gemeinwesens mit großer Kritikalität angegriffen werden, ist die Bedingung für die Übernahme der Führung durch das Militär erfüllt. Es ist hier davon auszugehen, dass durch die hohe Kritikalität eine breite Wirkung im Gemeinwesen gegeben ist. Der in der Literatur viel zitierte Blackout in der Stromversorgung, hervorgerufen durch eine Cyber Attacke, sei hier beispielhaft erwähnt.

Der Angriff auf dieses, zunächst nicht oder nur indirekt souveränitätsrelevante System, kann auf Grund des flächendeckenden Ausfalls nicht nur die Intensität erreichen, die die Attacke einem kriegerischen Akt im Cyberspace annähert, sondern, auf Grund einer andauernden Beeinträchtigung, auch eine entsprechende Souveränitätsrelevanz erreichen.

Ein Beispiel aus der jüngeren Vergangenheit illustriert dies vielleicht noch deutlicher. Estland wurde Ziel einer umfassenden Cyber Attacke als Reaktion auf die Versetzung eines russischen Kriegerdenkmals. Diese sichtlich politisch motivierten Angriffe erreichten ein Ausmaß, welches die gesamte netzgestützte Verwaltung des Landes zusammenbrechen ließ. Da Estland über einen hohen Grad an netzgestützter Verwaltung, sogenannter e-Governance, verfügt, waren die Auswirkungen und damit die Intensität eine sehr hohe.

Ungeachtet der Motivation, die hinter diesen Angriffen stand, ist allein auf Grund der Auswirkungen eine Führungsverantwortung beim Militär zu suchen. Je breiter und je länger die Wirkung eines solchen Angriffs ist, umso mehr ist das Militär mit seinen Ressourcen gefragt. Sowohl im Umfang, als auch in der Qualität der Leistungen kann nur das Militär einem solchen Angriff entgegentreten.

Es verfügt in der Regel über Kräfte, die zumindest in begrenztem Rahmen ein autarkes Netz zur Wiedererlangung eines Mindestmaßes an Kommunikationsfähigkeit errichten und betreiben können. Weiter sind Militärs in der Lage nicht nur defensiv und reaktiv zu agieren, sondern haben auch die offensiven Kapazitäten⁹⁹⁰ zur Verfügung.

Ist die Ordnung nicht mehr vorhanden, muss diese erst für ein Handeln der Polizei wiederhergestellt werden. Dies gilt also auch für ein Ausweichnetz, welches durch Führungsunterstützungskräfte des Militärs eingerichtet werden kann. Es ist daher nur logisch, dass, bei einem massiven

⁹⁹⁰ Anm. d. Verf.: Dazu zählen vor allem Verfahren und Denken des Personals.

Angriff auf der Informationsebene, diejenige Institution die Führungsverantwortung trägt, deren Ressourcen zum Einsatz kommen. Eine hohe Intensität erfordert einen hohen Einsatz dieser Ressourcen und damit den Einsatz des Militärs.

Ist weder die Relevanz für die Souveränität noch die Intensität in einem hohen Ausmaß (im Sinne von breiter Wirkung, hohem Schadensausmaß oder langer Dauer) gegeben, muss der Beurteilungskreislauf weiter durchschritten werden und der nächste Faktor untersucht werden, die Intention eines Angriffs.

9.2.2.3 Intention als tertiärer Entscheidungsfaktor

Dieser Faktor ist der mit großer Wahrscheinlichkeit am schwierigsten festzustellende Parameter. Die Motivation, die hinter einem Cyber Angriff steht, ist nur bedingt im Moment des Angriffs feststellbar. Auch danach ist man vielfach auf die Äußerung des Angreifers angewiesen, welches Motiv er damit verfolgt hat. Im Gegensatz dazu sind die beiden ersten Faktoren im Augenblick des Angriffs durch eine Beurteilung der verantwortlichen Entscheidungsträger feststellbar.

Im Zusammenhang mit der Intention kann allerdings am Ergebnis des Angriffes abgelesen werden, ob es sich um die Ausnutzung des angegriffenen Systems handelt oder ob die Zerstörung das Ziel der Angriffshandlung war. Die Intention lässt sich somit einerseits am dahinterliegenden Motiv und andererseits am Ergebnis des Angriffs ablesen. Eine politische Intention muss nicht immer die Zerstörung eines Systems zur Folge haben und die Zerstörung eines Systems muss nicht immer politisch motiviert sein.

Diese Tatsache macht die Suche und das Erkennen des Motivs schwierig. Bei der Intention sind Zusatzinformationen in die Beurteilung miteinzubeziehen. Eine Kontextanalyse muss erfolgen und bedingt hier einen gewissen Zeitverzug in der Reaktion auf Angriffe aus dem und im Netz. Zur Verdeutlichung lässt sich hier, neben dem Angriff in Estland, ein weiteres sehr bekanntes Beispiel anführen. Dies ist, da es klar von der Souveränitätsrelevanz und der Intensität abgrenzbar ist, hervorragend zur Darstellung des letzten Faktors geeignet.

Der Angriff auf die Uran-Zentrifugen im Iran zeigt hier besonders eindeutig die Intention. Im Augenblick des Angriffs war nicht klar was eigentlich passierte. Nach dem Angriff, der weder die Handlungs- bzw. Entscheidungsfähigkeit des Iran betraf, noch von einem solchen Ausmaß war, dass das Gemeinwesen möglichst breit bewirkt worden wäre, konnte die politische Intention klar erkannt werden. Hier decken sich auch Motiv und Ergebnis. Die politische Intention war die Behinderung oder Unterbindung eines möglichen militärischen Atomprogrammes und das Ergebnis war die Zerstörung einer großen Anzahl von Uran-Zentrifugen. Diese charakterisiert eindeutig einen Cyberwar bzw. kriegesischen Akt im Cyberspace.

Es kann hier eine Verbindung der Faktoren zu den Formen des Cyberwar hergestellt werden. Handelt es sich um einen Kleinen Cyberwar, ist die Entscheidung über die Führungsverantwortung an Hand dieses

Kreislaufes sehr einfach. Ziel ist ein souveränitätsrelevantes System, das Militär oder die militärische bzw. politische Entscheidungsebene. Die Intensität für den angegriffenen Teilbereich ist als hoch einzustufen, wenngleich die breite Wirkung beim Kleinen Cyberwar nicht vorhanden ist. Die Intention hinter einem Cyber Angriff zur Unterstützung konventioneller Streitkräfte in einer Operation ist als politisch einzustufen.

Beim Großen Cyberwar ist die Identifikation ungleich schwieriger. Um einen Angriff, der nicht direkt auf souveränitätsrelevante Systeme wirkt, eindeutig zu klassifizieren, ist ein hoher Beurteilungsaufwand zu betreiben. Es besteht die Gefahr, erst viel zu spät einen Angriff als solchen zu erkennen. Die jüngsten Ereignisse um die Abhöraktivitäten der National Security Agency (NSA) zeigen, dass erst durch Insiderinformationen diese Angriffe auf fremde Informationen aufgedeckt werden konnten. Auf Grund der schlechten Wahrnehmbarkeit von Aktionen im Großen Cyberwar ist die Zuordnung einer Führungsverantwortung auch hinsichtlich der Intensität schwer bis gar nicht möglich.⁹⁹¹

Die drei dargestellten Faktoren dürfen und können nicht isoliert betrachtet werden, sondern beeinflussen sich stets gegenseitig. Ist zum Beispiel die Intensität hoch und man kann von einem kriegsähnlichen Zustand sprechen, bedingt dies, auf der Seite der Intention die Absicht des Angreifers, Systeme zu schwächen oder zu zerstören. Sind dies für das Gemeinwesen existenzielle Systeme, liegt auch eine hohe Souveränitätsrelevanz vor.

Ein weiteres Indiz für die Zuordnung der Führungsverantwortung sind die, zur Begegnung von Cyber Attacken, einzusetzenden Mittel. Diese sind zum großen Teil in den Streitkräften verfügbar. Ein weiteres Argument findet sich in der Asymmetrie zwischen Wirkung der Attacke und Reaktion darauf. Da die Wirkung stets schneller ist, als die Reaktion darauf, liegt im schlimmsten Fall die höchste Eskalationsstufe vor. Ein Cyber Angriff ist also auf den ersten Blick, in Bezug auf Umfang und Auswirkung, nicht abschätzbar.

So können Kaskadeneffekte schneller wirken als darauf reagiert werden kann. Hinsichtlich der operativen Führungsverantwortung bedeutet dies, dem Militär die Erstverantwortung zu übertragen und diese nach Beurteilung zu deeskalieren. Diese Deeskalation verhindert Schwachstellen, welche bei einer Eskalation der Führungsverantwortung an den Schnittstellen der Übergabe, von einem zum anderen Verantwortungsträger, entstehen können.

Um dennoch eine handlungsfähige Cyber Abwehr des Gemeinwesens zu ermöglichen, muss das Wesen von Führung, in Bezug auf die Verantwortung im Cyberspace, näher betrachtet werden. In der Auseinandersetzung im Cyberspace ist die Führungsüberlegenheit entscheidend. Um diese zu erzielen und sie nicht durch die genannten Reibungsverluste hinsichtlich der Zuständigkeiten zu verspielen, soll eine

⁹⁹¹ Anm. d. Verf.: Die wahrgenommene Intensität muss nicht mit der tatsächlichen Intensität übereinstimmen.

These zur Eskalation bzw. Deeskalation von Führungsverantwortung im Folgenden dargestellt werden.

Unter Berücksichtigung, dass Cyber Angriffen nur dann mit Erfolg begegnet werden kann, wenn die Führungsverantwortung klar geregelt ist, wird der These, dass es leichter ist Führungsbereitschaft bzw. – verantwortung zu deeskalieren als zu eskalieren, nachgegangen. Der Argumentation werden dabei die Physik und die militärische Führungslehre zu Grunde gelegt. Vorab werden jedoch zunächst die verwendeten Begriffe, klar zueinander abgegrenzt, dargestellt.

9.2.3 Die Abgrenzung zwischen Verantwortung, Koordinierung und Führung

Die Kompetenz oder Verantwortung ist die Zuständigkeit für einen bestimmten Aufgabenbereich und beinhaltet auch die Ermächtigung bzw. Verpflichtung zum Handeln.⁹⁹² Diese Ermächtigung bzw. Verpflichtung, das Führen, zeigt sich auf den verschiedenen Ebenen der Führung in unterschiedlicher Ausprägung. Dieses Handeln bezieht sich in der gegenständlichen Thematik auf den Cyberspace und hier im Speziellen auf Angriffe im und aus diesem Raum.⁹⁹³ Die Führung, um einem solchen Angriff zu begegnen, wird durch Einsatz entsprechender personeller und materieller Ressourcen umgesetzt. Diese müssen geplant und geführt werden.⁹⁹⁴

Es muss davon ausgegangen werden, dass je tiefer die Führungsebene angesiedelt ist, die Ausprägung des Führungsbegriffes sich umso unmittelbarer darstellt. Obwohl jeder Ebene eine bestimmte Ausprägung von Führung eigen ist, sind alle Ausprägungen in der jeweiligen Führungsebene enthalten. Führung ist multidimensional und wird im Folgenden in seinen drei wesentlichen Ausprägungen dargestellt.

Jede Ebene hat eine entsprechende Führungsverantwortung, wobei für die Forschungsfrage die strategisch/operative Ebene und der damit verbundene Führungsbegriff von Bedeutung sind, es geht somit um Koordinierung und Führung. Die Führungsverantwortung, die im Zuge der Abhandlung betrachtet wird, ist, wie bereits in der Einleitung festgehalten, als Verantwortung für die Führung des Einsatzes oder anders formuliert als Einsatzverantwortung zu verstehen. Die Begriffe werden in der Literatur nicht synonym verwendet, so spricht Lätsch von zwei durchaus unterschiedlichen Bedeutungen, welche er den Begriffen zuordnet:

„Während bei der Unterstützung der zivilen Behörden die Einsatzverantwortung bei den zivilen Behörden und die

⁹⁹² Vgl. Erpenbeck, John; von Rosenstiel, Lutz (Hrsg.): Handbuch der Kompetenzmessung, Schäffer-Poeschel Verlag, Stuttgart 2003, S. Xf.

⁹⁹³ Anm. d. Verf.: Es geht hier um Angriffe, die in einem der drei oben genannten Faktoren den Schwellenwert überschritten haben. Dies ist der Fall, wenn entweder ein oder mehrere Faktoren des Beurteilungskreislaufes zutreffen.

⁹⁹⁴ Vgl. Lautsch, Siegfried: Zur Entwicklung der Militärwissenschaften in der Russischen Föderation-Teil 1, Grundzüge des militärischen Denkens und Handelns in der Gegenwart. In: Österreichische Militärische Zeitschrift, 5/2019, S. 575.

Führungsverantwortung für militärische Kräfte bei der militärischen Führung liegt, trägt im Verteidigungsfall die Armeeführung die Einsatz- und die Führungsverantwortung.“⁹⁹⁵

Dies weist auf eine Differenzierung hin, da aber die Verantwortung für die Führung eines Einsatzes auch eine Führungsverantwortung darstellt, wird in der Abhandlung lediglich zwischen Koordinierung und Führung unterschieden. Koordinierung meint die Abstimmung zwischen den Akteuren durch eine übergeordnete Stelle, welche jedoch keine Führungsagenden, im Sinne eines konkreten Mitteleinsatzes, wahrnimmt. Die Koordinierungsaufgabe besteht darin die Ziele vorzugeben, welche durch die führungsverantwortlichen Stellen zu erreichen sind.

Koordination ist eine Ausprägung von Führung, sie ist die

„[...] Abstimmung verschiedener Vorgänge, Dinge oder Faktoren, um diese miteinander in Einklang bringen, und zwar im Sinne eines geordneten Zusammenwirkens zur Gewährleistung einer an die jeweiligen Gegebenheiten angepaßten [sic] Funktion.“⁹⁹⁶

Da die strukturellen Voraussetzungen für die Koordination auf operativer Ebene noch zu schaffen sind, gilt es darzustellen bei wem die Einsatzverantwortung im Falle einer Cyber Attacke liegen sollte.⁹⁹⁷ Die Beantwortung der Forschungsfrage fokussiert sich auf die operative Führungsebene, bezogen auf das gesamtstaatliche Handeln.

Die These, die den abschließenden Betrachtungen zu Grunde liegt, ist jene, dass das Militär grundsätzlich die Führungsverantwortung und damit die Einsatzverantwortung übernehmen sollte, da eine Deeskalation der Führungsverantwortung bei Wegfall bzw. Prüfung der Parameter leichter und sicherer zu bewerkstelligen ist, als eine Eskalation dieser Verantwortung.

Nach dem Begriff der Koordination ist nun zu klären was Führung überhaupt ist. Führung ist

„[...] ein richtungsweisendes, steuerndes und motivierendes Einwirken [...], um eine Zielvorstellung zu verwirklichen und die Organisation zu optimieren. Sie [Führung] setzt Kräfte, Mittel und Information zielgerichtet nach Zeit und Raum ein.“⁹⁹⁸

Führung bedeutet also Ressourceneinsatz zur Zielerreichung. Führung kann durchaus als Trinität von Denken (Koordinierung), Führen (Planen) und Tun (Durchführen) verstanden werden. Sie bewegt sich zwischen den extremen Ausprägungen: dem Denken und der Aktion. Je nach Ebene ist Führung einer der drei Ausprägungen am nächsten.

⁹⁹⁵ Lätsch, Daniel: Innere Sicherheit und Armee. In: Military Power Revue der Schweizer Armee, Nr.2/2012, S. 19.

⁹⁹⁶ <http://www2.informatik.hu-berlin.de/ki/lehre/ws0102/VLKogRob/Lexikon/Koordination/koordination.html>.

⁹⁹⁷ Vgl. Republik Österreich: Aus Verantwortung für Österreich. Regierungsprogramm 2020-2024, Wien 2020, S. 154f.

⁹⁹⁸ BMLV, Dienstvorschrift für das Bundesheer, Taktischer Führungsprozess, 2019, S. 15.

Im Gegensatz zu anderen Arten der Führung ist die militärische Führung dadurch gekennzeichnet, dass sie unter außergewöhnlichen Belastungen zu erfolgen hat.⁹⁹⁹ Ein Merkmal, das auf Angriffe aus dem Cyberspace zutrifft.¹⁰⁰⁰ Bedeutend, um die Fragestellung, die dieser Arbeit zu Grunde liegt, zu verstehen, ist dabei ein Merkmal effizienter Führung¹⁰⁰¹ deren Unteilbarkeit.

Es kann in einem bestimmten Raum, zu einer bestimmten Zeit eines Einsatzes, nur einer die Verantwortung für die Führung tragen. Diese Grundregel der Führung, auch als Einheit der Führung verstanden, ist der Dreh- und Angelpunkt in der Beantwortung der Forschungsfrage.¹⁰⁰² Diese Verantwortung ist nur bedingt an den Faktoren eines Angriffes oder an der Einstufung der kritischen Systeme festzumachen. All dies trägt zur Bestimmung der Führungsverantwortung bei, kann sie jedoch nicht allein definieren. Die Europäische Union führt dazu in dem Cyber Defence Policy Framework aus, dass eine

„[...] unified chain of command could be considered with the aim to improve the resilience of networks [...]“¹⁰⁰³.

Eine klare Führungsverantwortung trägt somit zur Widerstandsfähigkeit von Netzen bei. Da, bedingt durch das Wesen des Cyberspace, ein Angriff in seinen Auswirkungen nie genau bestimmt werden kann, muss, um einen hohen Grad an Führungsbereitschaft zu haben, das Gemeinwesen die Führung jener Organisation im Erstansatz übergeben, die über das höchste Maß an Führungsfähigkeit verfügt. Da in der zivilen Führung die Zuständigkeiten oftmals verteilt werden und dadurch die Führungsfähigkeit herabgesetzt wird, ist eine Ausgangsverantwortung des Militärs angezeigt.¹⁰⁰⁴ Unter Führungsfähigkeit wird dabei das Vermögen verstanden Führungsaufgaben wahrzunehmen.¹⁰⁰⁵

Im Gegensatz zur zivilen Führung ist die militärische Führung darauf ausgerichtet in Situationen zu handeln, in denen es um die Existenz des Gemeinwesens geht. Hier lässt sich ein höherer Bereitschaftsgrad erkennen. In unübersichtlichen Lagen, wie einem Cyber Angriff, ist dies von großer Bedeutung. Hier sind, wie bereits angeführt, die Asymmetrie zwischen Aktion und Reaktion, die Unvorhersehbarkeit der Auswirkungen und die Ungewissheit insgesamt von entscheidender Bedeutung für die Führung und wirken auf diese ein.

Die militärische Führung ist darauf trainiert ein effektives Führungssystem zu betreiben. Auch Störungen und anderen

⁹⁹⁹ Vgl. ebd., S. 17.

¹⁰⁰⁰ Vgl. Lautsch, 2019, S. 576.

¹⁰⁰¹ Anm. d. Verf.: Im Sinne von die richtigen Dinge richtig tun.

¹⁰⁰² Vgl. Joint Chiefs of Staff, Cyberspace Operations, Joint Publication 3-12, 2013, S. III-1.

¹⁰⁰³ Political and Security Committee, EU Cyber Defence Policy Framework, 2014, S. 6.

¹⁰⁰⁴ Vgl. BMLV, Dienstvorschrift für das Bundesheer, Taktischer Führungsprozess, 2019, S. 21.

¹⁰⁰⁵ Vgl. ebd., S. 40.

Beeinflussungen kann durch militärische Führung begegnet werden.¹⁰⁰⁶ Durch den Grundsatz der Einheit der Führung hat militärische Führung eine ganz andere Führungsleistung. Diese Führungsleistung ist der wesentliche Punkt bei der Argumentation, neben dem bisher dargestellten, warum dem Militär in Erstverantwortung die Führung bei Angriffen im Cyberspace zugeordnet werden sollte.

Führungsleistung wird definiert als

„[...] die Qualität und Quantität der Führungsentscheidungen [...] über einen bestimmten Zeitraum hinweg.“¹⁰⁰⁷

Dieser Wert gibt allerdings noch keinen Aufschluss darüber, ob die Entscheidungen auch zielgerichtet sind. Dies wird durch die sogenannte Durchführungsleistung ausgedrückt, die Auskunft über die „[...] die Qualität und Quantität der zielorientierten Ressourcenfreisetzung [...]“¹⁰⁰⁸ gibt.

Der Bereitschaftsgrad oder physikalisch ausgedrückt das Energieniveau auf dem sich die militärische Führung abspielt, ist die Summe beider Leistungen. Dieses Niveau ist auch als Potential der Führungsebene zu fassen und ist direkt proportional zur Führungsfähigkeit.¹⁰⁰⁹ Militärische Führung ist auf das Handeln in besonders kritischen Situationen ausgerichtet. Gerade in nicht offensichtlich festlegbaren Situationen, wie sie im Cyberspace vorherrschen, muss verhindert werden, dass durch zu geringe Führungsfähigkeit¹⁰¹⁰ ein Nachteil für das Gemeinwesen entsteht.

Will man das Potential der Führung erhöhen, ist eine gewisse „Energiezufuhr“ (Hervorhebung durch den Verfasser.) nötig, um das Führungsvermögen steigern zu können.¹⁰¹¹ Hier geht in dem sehr zeitkritischen Umfeld des Cyberspace wertvolle Zeit verloren, die in Summe die Führungsleistung minimiert. Eskalation der Führung, wie dieser Vorgang bezeichnet werden kann, wäre also mit der Zufuhr von Ressourcen verbunden und führte zu einem Nachteil im Kampf um die Führungsüberlegenheit mit einem Angreifer.

Ist die potentielle Führungsenergie hoch, das heißt das Vermögen eine hohe Führungsleistung und Durchführungsleistung zu erbringen hoch, so kann nach Durchlauf des „Drei-Faktoren-Beurteilungsverfahren“ ein niedrigeres Energieniveau eingenommen werden. Dabei können Ressourcen freigesetzt werden, die anderwärtig zum Einsatz gelangen können. Dieser Vorgang ist als Deeskalation der Führungsverantwortung zu fassen.

In der Physik muss Arbeit aufgewendet werden, um von einem niedrigeren Energieniveau auf ein höheres zu gelangen, und es wird Energie

¹⁰⁰⁶ Vgl. ebd., S. 24.

¹⁰⁰⁷ Ebd., S. 41.

¹⁰⁰⁸ Ebd., S. 42.

¹⁰⁰⁹ Vgl. ebd., S. 43.

¹⁰¹⁰ Vgl. ebd., S. 40f.

¹⁰¹¹ Vgl. BMLV, Bedrohungsbild 2030, Trends, Konfliktbild, Ableitungen, GZ S92000/98-GStb/2018, Wien 2018, S. 33.

freigesetzt, wenn der umgekehrte Vorgang durchlaufen wird.¹⁰¹² Dieses Prinzip ist auch auf die Führung anwendbar. Es liefert ein Argument für den Einsatz des Militärs als erstverantwortlicher Organisation bei Angriffen im Cyberspace. Kritisch hinterfragt werden muss in diesem Zusammenhang ein präventives Sammeln von Daten im großen Stil, wie es die National Security Agency durchführt. Die NSA folgt dabei zwar dem beschriebenen Prinzip der Deeskalation der Führung, greift dabei aber massiv in die Privatsphäre der Nutzer des Cyberspace ein.¹⁰¹³

Dies stellt eine große Herausforderung für die dargestellte These dar. Es geht hier nicht nur um die Grenze, die Schwelle, zwischen Kriminalität und Krieg, sondern auch um eine ethische Dimension in der Vorbereitung und der Reaktion auf Angriffe im Cyberspace. In diesem Zusammenhang eröffnet sich ein weiteres Untersuchungsfeld im Zusammenhang mit der Forschungsfrage, welches in der vorliegenden Abhandlung jedoch nicht tiefergehend zu beantworten ist.

In Zusammenschau mit der Einstufung der Kritischen Infrastruktur und den einen Cyber Konflikt charakterisierenden Faktoren (Souveränitätsrelevanz, Intensität und Intention) ergibt sich zusammen mit der These von der Deeskalation der Führungsverantwortung ein Instrumentarium, welches es einem Gemeinwesen ermöglicht, seinen Cyberspace zu schützen und auf Angriffe zu reagieren.

Wie bereits angeführt verfügt das Militär über Ressourcen, die der Justiz- und Polizei fehlen bzw. diese gar nicht benötigen. Als Beispiel genannt seien Führungsunterstützungskräfte, die für das Militär in einem Einsatz autarke Kommunikationsnetze errichten können. Diese sind als Substitution für ausgefallene zivile Netze mehr als brauchbar einzusetzen. Die militärischen Nachrichtendienste verfügen über Kapazitäten in der Cyberforensik oder im Schutz von hochsensiblen Netzen. Die Kapazitäten in den Computer Network Operations, welche nicht nur passive Schutzmaßnahmen, wie im zivilen Umfeld üblich, beinhalten, können auch zur Informationsgewinnung genutzt oder für offensives Agieren eingesetzt werden.

Diese Ressourcen¹⁰¹⁴, die generisch dem Militär unterstehen, einer zivilen Führung, im operativen Sinn, zu unterstellen, würde schon vom Denken und Verstehen her Friktionen hervorrufen. Als Beispiel sei hier die Luftraumüberwachung angeführt, welche eine luftpolizeiliche Maßnahme darstellt. Da die Abfangjäger und Radaranlagen eine Ressource des Militärs sind, obliegt nicht nur die Durchführung, sondern auch die Führung demselben. Die Führungsverantwortung an das Militär zu übertragen heißt nicht automatisch, dass mit konventionellen Mitteln auf Cyber Angriffe

¹⁰¹² Vgl. Krikava, Franz; Ruhswurm, Hans; Seiser, Josef: Grundlagen der Elektrotechnik, Band 1, Oldenbourg Verlag, Wien, 1983, S. 102f.

¹⁰¹³ Vgl. Hersh, Seymour M.: Cyberwar: Die neue Front. In: Blätter für deutsche und internationale Politik, 1/2011, S. 52f.

¹⁰¹⁴ Vgl. BMLVS, Cyber Defence, GZ S90000/86-SII/2013, Grundsatzweisung für das Military Computer Emergency Readiness Team (milCERT), Wien 2013, S. 3ff.

reagiert wird.¹⁰¹⁵ Es geht hier um den Einsatz im Cyberspace gegen Angriffe aus und in ihm.

Eine Zusammenfassung der Cyber Abwehrkapazitäten unter eine eigens dafür geschaffene Institution, einem Cyber Amt oder Cyber Kommando, löst die momentane Problematik der operativen Führungsverantwortung und Zuständigkeit nur bedingt auf.¹⁰¹⁶ Die Frage bleibt schließlich, ob es sich bei dem Angriff um einen kriminellen oder kriegserischen Akt handelt. Im Erstansatz wäre ein solches Amt für Cyberangelegenheiten operativ sowohl für kriminelle als auch für kriegserische Angriffe zuständig.

Auf strategischer Ebene mag dies sinnvoll sein, birgt aber auf operativer Ebene Probleme in sich. So ist in Österreich die Koordinierung im Fall eines Cyber Angriffs auf strategischer Ebene beim Bundeskanzleramt angesiedelt, Koordinierung heißt Zuweisung von Kompetenzen, Vorgabe von Effekten (Zielen) und Zuweisung von Mitteln, aber nicht konkreter Einsatz von Mitteln.

Operativ geführt werden die konkreten Ressourcen, die auch dem Verantwortlichen unterstellt sein müssen, er muss direkt darauf zugreifen können. Hier ist die Verbindung zwischen Ressourcen und operativer Führung immanent.¹⁰¹⁷ Ein eigenes Cyber Amt müsste, um die Frage der operativen Führungsverantwortung zu beantworten, über eigene Mittel verfügen.¹⁰¹⁸ Hier wäre eine Duplizierung von Kapazitäten angezeigt. Trotzdem bleiben die Bedrohungen im und aus dem Cyberspace eine gesamtstaatliche Aufgabe. So muss darüber nachgedacht werden ob es nicht möglich ist, eine integrierte, gemeinsame Führungseinrichtung zu schaffen.

Die Effektoren – das heißt die konkreten Mittel zur Umsetzung – blieben getrennt, jedoch von einer Einrichtung geführt. Die derzeit abgebildete operative Führung ist nicht vereint und birgt die Gefahr durch unklare Verantwortungszuordnung im Falle einer Krise, eines Cyber Angriffes, durch Reibungsverluste zu spät wirken zu können.¹⁰¹⁹ Die Auflösung eines Cyber Defence Centers und eines Cyber Security Centers in einem Cyber Center wäre hier ein Lösungsansatz. Dieses könnte dann rasch und unter Abstützung auf das aus allen relevanten Ressorts bestehenden Personals die am besten geeigneten Mittel zum Einsatz bringen.¹⁰²⁰ Die Forderung „Leadership on the political, economic and military fronts must be integrated.“¹⁰²¹, die Alexander Swetschin hier für die strategische Führungsebene aufgestellt hat, soll in dieser Thematik auch auf der

¹⁰¹⁵ Vgl. Rolofs, Oliver: Digital abwehrbereit? Cybersicherheit ist eine globalpolitische Aufgabe. Europäische Sicherheit, 60. Jg., Nr. 12, 2011, S. 52ff.

¹⁰¹⁶ Vgl. Schmidt/Cohen, 2013, S. 162.

¹⁰¹⁷ Vgl. BMLV, Dienstvorschrift für das Bundesheer, Taktischer Führungsprozess, 2019, S. 15.

¹⁰¹⁸ Vgl. § 3 Ziff. 4 NISG.

¹⁰¹⁹ Vgl. Republik Österreich, Cyber Sicherheit Steuerungsgruppe, Bericht Cyber Sicherheit 2018, Wien 2018, S. 31ff.

¹⁰²⁰ Vgl. Statement of Admiral Michael S. Rogers Commander United States Cyber Command before the Senate Committee on Armed Services, March 2015, S. 2.

¹⁰²¹ Swetschin, Alexander: Strategy, Minneapolis 2004, S. 100.

operativen Ebene umgesetzt werden. Dabei darf aber nicht „[...] so etwas wie ein Parlament der Behörden, das alle zentrifugalen Bestrebungen widerspiegelt [...]“¹⁰²² entstehen.

Während die Zentralisierung auf Ebene der operativen Führung notwendig erscheint, ist die Zentralisierung der Effektoren nicht ratsam.¹⁰²³ Die verschiedenen Probleme im Cyberspace bedürfen einer durchaus unterschiedlichen Reaktion darauf. Jedes der Instrumente, die einem vereinten Cyber Kommando oder Cyber Center untergeordnet sind, hat seine spezifischen Stärken und Schwächen. Auch ist die Denkweise einer Strafverfolgungsbehörde anders als die von militärischen Cyberkräften.

Die aktuelle Sicherheitsstrategie gibt einen Hinweis auf die Kompetenzzuordnung hinsichtlich Terror und Cyber Angriffen.

„Die Bewältigung von subkonventionellen Bedrohungen oder von neuen Gefährdungen in Folge von Cyber-Angriffen kann zu einem neuen militärischen Aufgabenfeld werden.“¹⁰²⁴

Hier wird explizit die mögliche operative Verantwortung bzw. Zuständigkeit für Cyber Angriffe, ohne diese näher zu spezifizieren, beim Militär gesehen. Dennoch ist gerade der Terrorismus oft von Kriminalität begleitet und somit nicht alleinige Aufgabe des Militärs. Auch das ist ein Indiz dafür die operative Führungsverantwortung in einer militärisch, aber auch polizeilich denkenden operativen Führungseinrichtung zu vereinen. Nach der Klärung der Begriffe Kompetenz, Koordinierung und Führung, sowie der Darstellung der These von der Deeskalation von Führung ist klar, dass es sich in der Forschungsfrage um die operative Führungsverantwortung (Planung und Führung) im Hinblick auf Cyber Angriffe handelt.

Die Führungsverantwortung soll im ersten Ansatz bei Angriffen im Netz, nicht bei Einzelaktionen, sondern bei systematischem Vorgehen gegen hochkritische Systeme mit entsprechend großer Wirkung, beim Militär liegen. Die Ressourcen und Verfahren (um zu verteidigen, muss man angreifen können) stehen dem Militär umfassender zur Verfügung. Nichtsdestotrotz bleibt Cyber Sicherheit eine gesamtstaatliche bzw. gemeinschaftliche Aufgabe, vor allem auf strategisch-politischer Ebene.

Die Grenze der Zuständigkeit zwischen Polizei und Militär liegt seitens der Intensität am Übergang von der Cyberkriminalität zur Cyberspionage/-sabotage, seitens der Relevanz für die Souveränität ist der Übergang zwischen indirekter und direkter Relevanz gegeben. Bei der Intention liegt die Grenze am Übergang von der Ausnutzung zur Schwächung und Störung der Systeme, welche angegriffen werden. Daraus ergeben sich die Zuständigkeitsbereiche der beiden Träger des Gewaltmonopols.¹⁰²⁵

¹⁰²² Schaposchnikow, Boris: Das Hirn der Armee, Berlin 1987, S. 437.

¹⁰²³ Vgl. Ramsden, Robert: What and where? Considerations for Command and Control of Cyberspace Operations, Newport 2010, S. 9f.

¹⁰²⁴ BKA, Österreichische Sicherheitsstrategie (ÖSS), 2013, S. 11.

¹⁰²⁵ Vgl. Hofstetter, 2019, S. 69.

Um dem Grundsatz der Einheit der Führung gerecht zu werden und eine hohe Führungs- und Durchführungsleistung zu gewährleisten, ist die operative Einsatz- und Führungsverantwortung des Militärs, unter Mitwirkung der Strafverfolgungsbehörden, angezeigt, denn es verfügt letztlich über alle relevanten Möglichkeiten und Verfahren, sowohl defensiv, investigativ als auch offensiv. Eine Deeskalation der Führung, nach Prüfung der relevanten Faktoren, ist unter Freisetzung von Kapazitäten leichter durchführbar als umgekehrt.

Dies ist umso mehr von Bedeutung, da vielfach nicht klar ist, was sich im Falle eines Angriffs, falls dieser als solcher erkannt wird, im Cyberspace wirklich abspielt. Dabei muss ein ausgewogenes und kontrolliertes Verhältnis zwischen Anlassfall, Vorbereitung und Reaktion darauf erfolgen.¹⁰²⁶ Die Kritischen Infrastrukturen sind viel zu verwundbar und für das Gemeinwesen viel zu bedeutend, als dass hier auf Experimente vertraut werden sollte.

9.3 Ausblick

Wie in der Abhandlung bereits mehrmals festgehalten wurde, sehen wir uns einer zunehmenden Vernetzung gegenüber. Die Digitalisierung aller Gesellschaftsbereiche schreitet voran. Für die Gemeinwesen ergeben sich viele Chancen, aber es entstehen dadurch neue Bedrohungen für diese. Ein Faktor, der mit dieser Entwicklung in Zusammenhang steht, ist die zunehmende Verstädterung. Diese Entwicklung hat für alle Akteure in kriegesischen Auseinandersetzungen eine große Bedeutung.

Die Vielzahl an möglichen Angriffsvektoren und die gesteigerte Verwundbarkeit der hochtechnologischen Kommunikationsrelationen macht Städte zu lohnenden Zielen. Terroranschläge, wie sie in den letzten 20 Jahren rund um den Globus stattfanden, spielen sich zumeist in den großen Metropolen ab. Dieser Trend dürfte weiter anhalten. Zudem sind Städte auch aus militärischer Perspektive interessant.

Viele Konflikte der jüngeren Vergangenheit spielten sich im urbanen Umfeld ab. Die Rolle der Städte wird vor allem in Verbindung mit dem durch den Cyberspace erweiterten Handlungsraum der Menschen weiter zunehmen. Sogenannte „Smart Cities“ werden im Zeitalter der Digitalisierung zu neuen Konflikträumen, in denen sich das Militär zum Schutz der staatlichen Souveränität zu bewegen lernen muss.

„Je smarter ein Land oder eine Stadt, je digitaler die Infrastruktur, je größer das Internet der Dinge und je ausgeprägter die Umstellung auf die von KI [Künstlicher Intelligenz] gesteuerten Produktionsabläufe von Industrie 4.0 ist, je mehr Daten und Prozesse in die Cloud, also in Rechenzentren, ausgelagert werden, desto anfälliger werden sie auch für Cyberangriffe und Cyberwar.“¹⁰²⁷

¹⁰²⁶ Vgl. ebd., S. 249.

¹⁰²⁷ Rötzer, Florian: Smart Cities im Cyberwar, Westend, Frankfurt 2015, S. 10f.

Zwei Drittel aller Haushalte haben schon Zugang zum Internet, welches zur Verbindung der verschiedenen Dienste genutzt wird.¹⁰²⁸ Die Zahl der Angriffspunkte steigt somit stetig an. Hier ist es nun notwendig sich nicht nur organisatorisch mit der Kompetenzzuordnung innerhalb der Gemeinwesen, in Bezug auf die operative Führungsverantwortung, auseinanderzusetzen, sondern sich begrifflich klar darüber zu werden, was denn das Phänomen Cyberwar ausmacht. Diese Begriffsbasis leistet den wesentlichen Beitrag, um in Zukunft diese Verwundbarkeit der Gesellschaft auch rechtlich eindeutig fassbar zu machen.

Die Entstehung neuer Rechts- bzw. Normenkomplexe ist eine Generationenaufgabe und daher ist, ausgehend von einer klaren Sicht auf dieses Phänomen, mit der Aufgabe zu beginnen.¹⁰²⁹ Es ist wichtig, eine auf einem entsprechenden Rechtsrahmen basierende Kompetenzzuordnung in diesem – Raum und Zeit schrumpfenden – Umfeld zu treffen. Dies deshalb, weil rasche Entscheidungsfindung eine Voraussetzung für die Abwehr und Eindämmung der Bedrohungen im und aus dem Cyberspace ist. Das drückt sich in einem Zitat aus dem Thesenpapier der Deutschen Bundeswehr zur Digitalisierung der Landstreitkräfte folgendermaßen aus:

„Der eigene Führungsprozess ist zu dynamisieren, um die Reaktionsschnelligkeit der Entscheidungen zu erhöhen. Dies stellt bewährte Aspekte des deutschen Führungsprozesses nicht in Frage, sondern erweitert diese sinnvoll entsprechend der neuen komplexeren Bedrohungen und Möglichkeiten. Der Einsatz autonomer und teilautonomer Waffensysteme ist dabei zu berücksichtigen.“¹⁰³⁰

Rasch entschieden werden kann nur dann, wenn klar ist, wer wann zu entscheiden hat. Diese Festlegung ist Aufgabe der politischen Führung, welche hier, im Angesicht der zukünftigen Entwicklungen, den Rahmen zu schaffen hat.

¹⁰²⁸ Vgl. <https://de.statista.com/statistik/daten/studie/187116/umfrage/anteil-der-haushalte-mit-internetzugang/>, [12.05.2020].

¹⁰²⁹ Vgl. Hofstetter, 2019, S. 201.

¹⁰³⁰ Kommando Heer (Hrsg.), Thesenpapier I, Wie kämpfen Landstreitkräfte künftig?, o.J., S. 15.

10 Abstract

10.1 Kurzbeschreibung

In der vorliegenden Abhandlung mit dem Titel „Der Krieg im Cyberspace und seine normativen Grundlagen“, wird ein Blick auf den Krieg und seinen neuesten Spross, den Cyberwar geworfen. Kriege sind die ultimative Einsatzform der bewaffneten Staatsgewalt. In der realen Welt lässt sich, neben vielen anderen Mitwirkenden das Militär als Hauptakteur, ausmachen. Im Cyberspace, als einem Raum, in dem sich Vieles der Wahrnehmbarkeit entzieht, unter anderem auch die Austragung bewaffneter Virtueller Kriege, ist die Frage nach dem Hauptakteur im Konflikt nicht so offensichtlich beantwortbar.

Die Dissertation geht dieser Frage nach und analysiert, welche Bedingungen erfüllt sein müssen, um eine Attacke im Cyberspace als Krieg zu klassifizieren. Darauf aufbauend wird die Schwelle für den Übergang der Führungsverantwortung bei Konflikten im Cyberspace von einem Träger der Staatsgewalt auf den anderen definiert. Die Abhandlung führt dabei vom klassischen Kriegsbegriff mit einer Typologisierung des Krieges über die Auseinandersetzung mit dem Cyberraum und dem Cyberwar selbst hin zu den rechtlichen Normen, die im Cyberspace zur Anwendung kommen, um letztlich aus den Ableitungen heraus die Forschungsfrage *„Wann muss das Militär die Führungsverantwortung bei Angriffen im und aus dem Cyberspace übernehmen?“* zu beantworten.

Der Schlüssel zur Antwort liegt in der Betrachtungsweise des virtuellen Raumes. Die Definition von innen und außen, bezogen auf die Souveränität des Staates, ist nicht mehr territorial, sondern systemisch und funktional zu fassen. Angriffe auf die souveränitätsrelevanten Systeme des Staates sind zum einen immer Angriffe von außen, und zum anderen sind diese immer darauf ausgerichtet, die Handlungsunfähigkeit des Gemeinwesens herbeizuführen. Dies führt zur Auflösung des Ordnungsrahmens und bedingt daher die Führungsverantwortung des Militärs. Vorbedingung für die Festlegung der Führungsverantwortung ist die Festlegung einer Schwelle, basierend auf einer Kategorisierung der souveränitätsrelevanten Systeme eines Gemeinwesens. Damit lässt sich der Übergang der Führungsverantwortung definieren.

10.2 Abstract

In the present dissertation titled „The War in Cyberspace and its normative Foundations“ emphasis is put on war and its latest addition, the cyberwar. Wars are the ultimate application of the armed state authority. In the real world the military, among many other participants, can be identified as the key player. Whereas in cyberspace, an area in which a lot is beyond perceptibility (e.g. among others the conduct of armed virtual conflicts), the question concerning the main actor in the conflict is not so obvious to answer.

This dissertation examines this question and analyses which conditions have to be met to classify an attack in cyberspace as a war. Based on this, the threshold for the transition of leadership responsibility from one carrier of government authority to the other governmental actor for conflicts in the cyberspace is defined. The paper leads from war and a typologization of war via the concept of cyberspace to the cyberwar itself towards the specific law in cyberspace with the aim to finally answer the following research question: "When do the military have to assume leadership responsibilities for attacks in and out of cyberspace?"

The key to the answer lies in the approach to virtual space. The definition of "inside" and "outside", based on the sovereignty of the state, is no longer territorial, but has to be understood as systemic and functional. Attacks on systems relevant for the sovereignty of the state, are *on the one hand* always attacks from the outside and *on the other hand* always aimed to lead to complete acting inability of the community. This cause leads to disorganization and disintegration of the regulatory framework and therefore requires the leadership responsibility of the military. Precondition for the definition of leadership responsibility is the establishment of a threshold based on a categorization of sovereignty relevant systems of a community; hence it is possible to define the transition of leadership responsibility.

11 Literaturverzeichnis

11.1 Primärliteratur

11.1.1 Gesetze, Vorschriften, Positionspapiere

Entschließung des Europäischen Parlaments vom 21. Mai 2015 zur Umsetzung der Gemeinsamen Sicherheits- und Verteidigungspolitik (nach dem Jahresbericht des Rates an das Europäische Parlament zur Gemeinsamen Außen- und Sicherheitspolitik) 2014/2220(INI) ABl. C 353/12.

Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union ABl. L 194.

Australian Government, Cyber Security Strategy, 2009.

Australian Government, Cyber Security Strategy, 2016.

BKA, Österreichische Strategie für Cyber Sicherheit (ÖSCS), Wien 2013.

BKA, Österreichische Sicherheitsstrategie (ÖSS), Sicherheit einer neuen Dekade – Sicherheit gestalten, Wien, Juli 2013.

BKA, Vortrag an den Ministerrat, BKA-406.200/0002-IV/6/2011, Österreichische Sicherheitsstrategie (ÖSS), Wien, März 2011

BKA, Vortrag an den Ministerrat, BKA-406.300/0001-IV/6/2008, Das österreichische Programm zum Schutz kritischer Infrastrukturen, Masterplan APCIP, Wien, März 2008.

BMI, Cyber-Sicherheitsstrategie für Deutschland, 2011.

BMI, Cyber-Sicherheitsstrategie für Deutschland, 2016.

BMI, Richtlinie über die Zusammenarbeit zwischen Sicherheitsexekutive und Bundesheer im Assistenzeinsatz (RLAsSE), Zl. BMI-EE2510/0004-II/2/b/2017.

BMLV, Bedrohungsbild 2030, Trends, Konfliktbild, Ableitungen, GZ S92000/98-GStb/2018, Wien 2018.

BMLV, Dienstvorschrift für das Bundesheer, Taktischer Führungsprozess, 2019.

BMLVS, Begleitschreiben zum Ministerratsbeschluss 180/8, GZ S92100/6-MilStrat/2013, Wien 2013.

- BMLVS, Cyber Defence, GZ S90000/86-SII/2013, Grundsatzweisung für das Military Computer Emergency Readiness Team (milCERT), Wien 2013.
- BMLVS, Dienstvorschrift für das Bundesheer, Operative Führung, 2009.
- BMLV, DVBH Führungsbegriffe, Wien, November 2005.
- BMLV, DVBH (zur Erprobung) Truppenführung, Wien, August 2004.
- BMLVS, Erlass zur Neuregelung des Begleitschutzes, GZ S92000/199-GStbAbt/2010, Verfügung, Wien, Februar 2010.
- BMLVS, Intensität von Auslandseinsätzen, GZ S92107/10-MilStrat/2013, Festlegung der Begriffe, Wien 2013.
- BMLV, Merkblatt für das Bundesheer, Raumschutz, 2000.
- BMLVS, Militärische Cyber Handlungen und Verfahren (Cyber Operations), Anlage zum Militärstrategischen Konzept, Entwurf, August 2013.
- BMLV, Militärstrategisches Konzept des Österreichischen Bundesheeres, Bundesheer 2010, (Beilage zu GZ. 92150/3-MilStrat/2006), Wien, Fassung 2006.
- BMLVS, Netzwerkorientierte Verfahren Austria, Grundkonzept, 2006.
- BMLVS, Operatives Fachkonzept Führungsunterstützung im ÖBH, 2012.
- BMLVS, ÖSCS, GZ S91018/14-GrpRechtLeg/2012, Ersuchen um rechtliche Würdigung, Stellungnahme, 2012.
- BMLVS, Rechtliche Rahmenbedingungen der Abwehr von Cyber-Angriffen durch das Bundesheer, GZ S91018/17-GrpPräsRechtLeg/2017, Rechtsgutachten, 2017.
- BMLVS, Teilstrategie Verteidigungspolitik 2014, Wien, Oktober 2014.
- BMLVS, Terrorabwehr und Eventschutz, Operatives Fachkonzept, Wien, Juli 2009.
- Bundes-Verfassungsgesetz (B-VG) BGBl. Nr. 1/1930 idF BGBl. I Nr. 22/2018.
- Bundesgesetz über die Zahl, den Wirkungsbereich und die Einrichtung der Bundesministerien (Bundesministeriengesetz 1986 – BMG) BGBl. Nr. 76/1986 idF BGBl. I Nr. 61/2018.
- Bundesgesetz über Aufgaben und Befugnisse im Rahmen der militärischen Landesverteidigung (Militärbefugnisgesetz – MBG) BGBl. I Nr. 86/2000 idF BGBl. I Nr. 102/2019.

- Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG) BGBl. I Nr. 111/2018.
- Bundesgesetz über die Organisation der Sicherheitsverwaltung und die Ausübung der Sicherheitspolizei (Sicherheitspolizeigesetz – SPG) BGBl. Nr. 566/1991 idF BGBl. I Nr. 56/2018.
- Bundesgesetz vom 23. Jänner 1974 über die mit gerichtlicher Strafe bedrohten Handlungen (Strafgesetzbuch – StGB) BGBl. Nr. 60/1974 idF BGBl. I Nr. 70/2018.
- Bundesgesetz über die Waffenpolizei (Waffengesetz 1996 – WaffG) BGBl. I Nr.12/1997 idF BGBl. I Nr. 97/2018.
- Bundesministerium für Inneres (Hrsg.): Mehr Freiheit. Mehr Sicherheit. Die Sicherheitsdoktrin des BMI für Österreich 2017 - 2020, Wien 2017.
- Bundesverfassungsgesetz über Kooperation und Solidarität bei der Entsendung von Einheiten und Einzelpersonen in das Ausland (KSE-BVG) BGBl. I Nr. 38/1997 idF BGBl. I Nr. 35/1998.
- Cabinet Office, National Cyber Security Strategy 2016-2021, Progress Report, 2019.
- Cabinet Office, The UK Cyber Security Strategy, 2011.
- Department of Defense, Cyber Strategy, 2015.
- Department of Defense, Directive Number 3000.07, 01. December 2008.
- Department of Defense, Strategy for Operating in Cyberspace, July, 2011.
- DHS, National Cyber Incident Response Plan (NCIRP), 2010.
- DHS, National Cyber Incident Response Plan (NCIRP), 2016.
- DHS, The Cybersecurity Strategy for the Homeland Security Enterprise, 2012.
- DHS, Cybersecurity Strategy, 2018.
- Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS, Programm zum Schutz Kritischer Infrastrukturen, Methode zur Erstellung des SKI-Inventars, Oktober, 2010.
- EUMS, EU Concept for Computer Network Operations in EU-led Military Operations, 2009.
- EUMS, EU Concept for Cyber Defence for EU-led Military Operations, 2012.

Europäische Kommission, Cybersicherheitsstrategie der Europäischen Union, 2013.

Europäische Kommission, Gemeinsame Mitteilung an das europäische Parlament und den Rat, Abwehrfähigkeit, Abschreckung und Abwehr: die Cybersicherheit in der EU wirksam erhöhen, 2017.

Verordnung (EU) 2019/881 des europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit) ABI. L 151/15.

European Union, Political and Security Committee, EU Cyber Defence Policy Framework, 2014.

Federal Ministry of Defence of the Republic of Austria: Handbook on Cybersecurity, The Common Security and Defence Policy of the European Union, 2019.

French Network and Information Security Agency (ANSSI), Information systems defence and security, France's strategy, 2011.

Government of Canada, Canada's Cybersecurity Strategy, 2010.

HM Government, National Cyber Security Strategy 2016-2021, 2016.

International Committee of the Red Cross (Hrsg.): Handbook on international Rules governing military Operations, Genf 2013.

ITU, National Cybersecurity Guide, 2011.

Joint Chiefs of Staff, Cyberspace Operations, Joint Publication 3-12, 2013.

Kommando Heer (Hrsg.), Thesenpapier I, Wie kämpfen Landstreitkräfte künftig?, o.J.

MOD, Joint Doctrine Publication 01, 2008.

NATO, Allied Joint Doctrine for Land Operations, 2009.

NATO, Allied Joint Maritime Operations, 2004.

NATO, Comprehensive Operations Planning Directive, 2010.

NATO, Defending the networks, The NATO Policy on Cyber Defence, 2011.

NATO, Joint Air and Space Operations Doctrine, 2002.

NATO, Strategic Concept, 2010.

- Public Safety of Canada, National Cyber Security Strategy, 2018.
- Rat der Europäischen Union, EU-Politikrahmen für die Cyberabwehr (Aktualisierung 2018), 2018.
- Republik Österreich: Aus Verantwortung für Österreich. Regierungsprogramm 2020-2024, Wien 2020.
- Republik Österreich, Beilagen zu den stenographischen Protokollen des Nationalrates, 15. Band, Wien, 1974.
- Republik Österreich, Cyber Sicherheit Steuerungsgruppe, Bericht Cyber Sicherheit 2018, Wien 2018.
- Royal Army, Army Field Manual, Volume 1, Combined Arms Operations, Part 10, Counter Insurgency Operations, (Strategic and Operational Guidelines) Revised and updated Version, 2007.
- Secrétariat général de la Défense et de la Sécurité nationale (SGDSN), French National Digital Security Strategy, 2015.
- Statement of Admiral Michael S. Rogers Commander United States Cyber Command before the Senate Committee on Armed Services, March 2015.
- The North Atlantic Treaty, 1949. In: NATO, Towards the new Strategic Concept, 2010, S. 3-20.
- The White House, International Strategy for Cyberspace, 2011.
- The White House, National Cyber Strategy of the United States of America, 2018.
- The White House, The National Strategy to Secure Cyberspace, 2003.
- United Kingdom Cabinet Office, Cyber Security Strategy, 2009.
- United Nations, General Assembly, Resolution 53/70, 1999.
- United Nations Regional Information Centre for Western Europe (Hrsg.): Charta der Vereinten Nationen, 2009.
- United States Joint Force Command, Doctrinal Implications of Operational Net Assessment, 2004.
- USAF, Air Force Doctrine Document, Cyberspace Operations, 2010.
- Verordnung der Bundesregierung vom 9. Jänner 1979 über die Allgemeinen Dienstvorschriften für das Bundesheer (ADV) BGBl. Nr. 43/1979 idF BGBl. II Nr. 362/2014.
- Wehrgesetz 2001 – WG 2001 BGBl. I Nr. 146/2001.

11.1.2 Bücher (Monographien und Sammelbände)

Clausewitz, Carl von u.a.: Vom Kriege, Reinbek bei Hamburg 1963.

Clausewitz, Carl von: Meine Vorlesungen über den kleinen Krieg. In: Hahlweg, Werner: Lehrmeister des Kleinen Krieges. von Clausewitz bis Mao Tse-Tung und (Che) Guevara, Darmstadt 1968, S. 46-52.

Decker, Carl: Der kleine Krieg im Geist der neueren Kriegführung. Abhandlung über die Verwendung und den Gebrauch aller drei Waffen im kleinen Kriege, Berlin, Poßen und Bromberg 1844.

Douhet, Giulio: Luftherrschaft, Berlin 1935.

Eimannsberger, Ludwig: Der Kampfwagenkrieg, München 1934.

Galula, David: Counterinsurgency Warfare. Theory and Practice, 1964.

Gehlen, Reinhard: Der Dienst, München 1973.

Kant, Immanuel: Kritik der reinen Vernunft, Reclam, Stuttgart 1966.

Kirchmann, J. H. (Hrsg.): Des Hugo Grotius drei Bücher über das Recht des Krieges und Friedens, Erster Band, Berlin 1869.

Hobbes, Thomas: Leviathan, Suhrkamp, Berlin 1966.

Lilienstern, August Rühle von: Handbuch für den Offizier zur Belehrung im Frieden und zum Gebrauch im Felde, Berlin 1818.

Machiavelli, Niccolò: Die Kunst des Krieges. In: Ulfig, Alexander (Hrsg.): Machiavelli, Niccolò. Gesammelte Werke, Frankfurt am Main, 2006, S. 709-856.

Machiavelli, Niccolò: Discorsi. Gedanken über Politik und Staatsführung, 2. Aufl., Stuttgart 1977.

Machiavelli, Niccolò: Geschichte von Florenz. In: Ulfig, Alexander (Hrsg.): Machiavelli, Niccolò. Gesammelte Werke, Frankfurt am Main, 2006, S. 381-708.

Machiavelli, Niccolò: Mensch und Staat, tredition Verlag, Hamburg 2012.

Machiavelli, Niccolò; Zorn, Rudolf: Der Fürst. Il principe, 6. Aufl., Stuttgart 1978.

Mahan, Alfred Thayer: Der Einfluss der Seemacht auf die Geschichte, überarbeitet und herausgegeben von Gustav-Adolf Wolter, Koehlers Verlagsgesellschaft mbH, Herford 1967.

Platon: Sämtliche Werke. Lysis, Phaidon, Kleitophon, Politeia, Phaidros, 33. Aufl., Reinbek bei Hamburg 2011.

Platon: Sämtliche Werke. Timaios, Kritias, Minos, Nomoi, 23. Aufl., Reinbek bei Hamburg 2009.

Schaposchnikow, Boris: Das Hirn der Armee, Berlin 1987.

Schmitt, Carl: Politische Theologie, Duncker u. Humblot, Berlin 1985.

Shannon, Claude: A Mathematical Theory of Communication, 1948.

Spinoza: Ethik. In geometrischer Weise behandelt in fünf Teilen, Leipzig 1975.

Spinoza, Benedikt; Bartuschat, Wolfgang: Politischer Traktat. Lateinisch - deutsch = Tractatus politicus, 2. Aufl., Hamburg 2010.

Swetschin, Alexander: Strategy, Minneapolis 2004.

Tse-tung, Mao: Theorie des Guerillakrieges oder Strategie der Dritten Welt, Reinbek bei Hamburg 1966.

Ulfig, Alexander (Hrsg.): Machiavelli, Niccolò. Gesammelte Werke, Frankfurt am Main, 2006.

Wiener, Norbert: Kybernetik. Regelung und Nachrichtenübertragung im Lebewesen und in der Maschine, 1948.

11.2 Sekundärliteratur

Andress, Jason; Winterfeld, Steve: Cyber Warfare, Techniques, Tactics and Tools for Security Practitioners, 1. Aufl., 2011.

Assange, Julian u.a.: Cypherpunks. Unsere Freiheit und die Zukunft des Internets, 1. Aufl., s.l 2013.

Arquilla, John; Ronfeldt, David: The Advent of Netwar, Santa Monica 1996.

Aust, Stefan; Ammann, Thomas: Digitale Diktatur, Econ Verlag, Berlin 2014.

Barnett, Thomas: The Pentagon's New Map, War and Peace in the Twenty-First Century, New York 2004.

Beauchamp, K. G.: History of telegraphy, London 2001.

Benz, Arthur: Der moderne Staat. Grundlagen der politologischen Analyse, 2. Aufl., München 2008.

Bilban, Christoph; Grininger, Hanna (Hrsg.): Mythos „Gerasimov-Doktrin“, Ansichten des russischen Militärs oder Grundlage hybrider Kriegsführung?, Schriftenreihe der Landesverteidigungsakademie, Wien 2019.

- Boltenkov, Dimitry, Gayday, Aleksey, u.a.: Russia's New Army, Centre for Analysis of Strategies and Technologies, Moskau 2011.
- Bonacker, Thorsten; Imbusch, Peter: Zentrale Begriffe der Friedens- und Konfliktforschung. In: Imbusch, Peter; Zoll, Ralf (Hrsg.): Friedens- und Konfliktforschung. Eine Einführung, Wiesbaden 2010, S. 67-80.
- Bowden, Mark: Worm. Der erste digitale Weltkrieg, Berlin 2012.
- Clarke, Richard: World Wide War. Angriff aus dem Internet, Hamburg 2011.
- Edlinger, Karl: Die völkerrechtliche Klassifizierung bewaffneter Konflikte. Konflikttypen, Abgrenzungen sowie Rechtsfolgen und deren Auswirkungen auf die Planung und Durchführung militärischer Operationen, Frankfurt am Main 2016.
- Erpenbeck, John; von Rosenstiel, Lutz (Hrsg.): Handbuch der Kompetenzmessung, Schäffer-Poeschel Verlag, Stuttgart 2003.
- Eppler, Erhard: Auslaufmodell Staat?, 1. Aufl., Frankfurt am Main 2005.
- Fazal, Tanisha M.: [Kein] Recht im Krieg? Nicht intendierte Folgen der völkerrechtlichen Regelung bewaffneter Konflikte, Hamburg 2019.
- Feichtinger, Walter: Differenzierung von Asymmetrie im Kontext bewaffneter Konflikte. In: Schröfl, Josef; Pankratz, Thomas (Hrsg.): Asymmetrische Kriegführung. Ein neues Phänomen der internationalen Politik?, 1. Aufl., Baden-Baden 2004, S. 117-120.
- Forgò, Nikolaus; Helfrich, Marcus; Schneider, Jochen: Betrieblicher Datenschutz. Rechtshandbuch, 3. Auflage, München 2019.
- Freudenberg, Dirk: Theorie des Irregulären. Partisanen, Guerillas und Terroristen im modernen Kleinkrieg, 1. Aufl., Wiesbaden 2008.
- Gareis, Sven; Klein, Paul (Hrsg.): Handbuch Militär und Sozialwissenschaft, 1. Aufl., Wiesbaden 2004.
- Gaycken, Sandro: Cyberwar. Das Internet als Kriegsschauplatz, 1. Aufl., München 2011.
- Gaycken, Sandro: Cyberwar. Das Wettrüsten hat längst begonnen; vom digitalen Angriff zum realen Ausnahmezustand, 1. Aufl., München 2012.
- Geers, Kenneth: Demystifying Cyber Warfare. In: Schröfl, Josef; Muhr, Dieter; Rajae, Bahram M. (Hrsg.): Hybrid and cyber war as consequences of the asymmetry. A comprehensive approach answering hybrid actors and activities in cyberspace: political social and military responses, Frankfurt am Main, New York 2011, S. 119-126.

- Geers, Kenneth: Strategic Cyber Security: Evaluating Nation-State Cyber Attack Mitigation Strategies with DEMATEL, Tallinn University of Technology, Dissertation, 2011.
- Geis, Anna (Hrsg.): Den Krieg überdenken. Kriegsbegriffe und Kriegstheorien in der Kontroverse, Schriftenreihe der DVPW-Sektion Politische Theorien und Ideengeschichte, Baden-Baden 2006.
- Glenn, Russell W. (Hrsg.): Capital preservation. Preparing for Urban Operations in the Twenty-First Century, Santa Monica 2001.
- Glenny, Misha: Cybercrime. Kriminalität und Krieg im digitalen Zeitalter, 1. Aufl., München 2012.
- Griffith, B. Samuel: Sun Zi. Die Kunst des Krieges. Die neue illustrierte Ausgabe, Kerkdriel 2019.
- Haffner, Sebastian: Der neue Krieg. In: Tse-tung, Mao: Theorie des Guerillakrieges oder Strategie der Dritten Welt, Reinbek bei Hamburg 1966, S. 5-34.
- Hahlweg, Werner: Lehrmeister des Kleinen Krieges. Von Clausewitz bis Mao Tse-Tung und (Che) Guevara, Darmstadt 1968.
- Haltiner, Karl: Vom Landesverteidiger zum militärischen Ordnungshüter. In: Gareis, Sven; Klein, Paul (Hrsg.): Handbuch Militär und Sozialwissenschaft, 1. Aufl., Wiesbaden 2004, S. 476-484.
- Hansel, Mischa: Stuxnet und die Sabotage des iranischen Atomprogramms: Ein neuer Kriegsschauplatz im Cyberspace? In: Jäger, Thomas; Beckmann, Rasmus: Handbuch Kriegstheorien, Wiesbaden 2011, S. 564-576.
- Hartmann, Uwe: Carl von Clausewitz: Erkenntnis, Bildung, Generalstabsausbildung, Olzog Verlag, München 1998.
- Hathaway, Oona u.a.: The Law of Cyber-Attack, 2011.
- Hähnel, Martin: ...um einer Vielheit statt. In: Schlitte, Annika; Hünefeldt, Thomas (Hrsg.): Ort und Verortung. Beiträge zu einem neuen Paradigma interdisziplinärer Forschung, Bielefeld 2017, S. 31-44.
- Heydte, Friedrich August Freiherr von: Völkerrecht, Verlag für Politik und Wirtschaft, Köln, 1958.
- Heuser, Beatrice: August Rühle von Lilienstern. In: Jäger, Thomas; Beckmann, Rasmus: Handbuch Kriegstheorien, Wiesbaden 2011, S. 206-213.
- Hofstetter, Yvonne: Der unsichtbare Krieg. Wie die Digitalisierung Sicherheit und Stabilität in der Welt bedroht, Droemer Verlag, München 2019.

- Holischka, Tobias: Zur Philosophie des virtuellen Ortes. In: Schlitte, Annika; Hünefeldt, Thomas (Hrsg.): Ort und Verortung. Beiträge zu einem neuen Paradigma interdisziplinärer Forschung, Bielefeld 2017, S. 199-213.
- Hülsmann, Thorsten: Geographie des Cyberspace. Wahrnehmungsgeographische Studien, Band 9, 2000.
- Imbusch, Peter; Zoll, Ralf (Hrsg.): Friedens- und Konfliktforschung. Eine Einführung, Wiesbaden 2010.
- Jäger, Thomas; Beckmann, Rasmus: Handbuch Kriegstheorien, Wiesbaden 2011.
- Jäger, Thomas; Beckmann, Rasmus: Carl von Clausewitz' Theorie des Krieges. In: Jäger, Thomas; Beckmann, Rasmus: Handbuch Kriegstheorien, Wiesbaden 2011, S. 214-226.
- Johnson, Brian: Streng Geheim. Wissenschaft und Technik im 2. Weltkrieg, Stuttgart 1983.
- Jung, Matthias: Hermeneutik zur Einführung, Junius Verlag, Hamburg 2001.
- Kahn, Herman: On escalation. Metaphors and scenarios, New Brunswick, N. J. 2010.
- Keegan, John: Die Kultur des Krieges, 2. Aufl., Reinbek bei Hamburg 2001.
- Kleemeier, Ulrike: Grundfragen einer philosophischen Theorie des Krieges. Akademie Verlag, Berlin 2002.
- Klimburg, Alexander: Gesamtstaatliche Ansätze zur Cybersicherheit. Erfahrungen aus Österreich. In: Pucher, Johann; Frank, Johann (Hrsg.): Strategie und Sicherheit 2012. Der Gestaltungsspielraum der österreichischen Sicherheitspolitik, 2012, S. 463-472.
- Kohlweg, Markus: Militärisches Denken in den Streitkräften der Russländischen Föderation-Ist Stand und Entwicklungstendenzen, Militärwissenschaftliche Arbeit, Universität Wien, April 2010.
- Konegen, Norbert: Zum Staatsverständnis von Hugo Grotius. in: IFS-Nachrichten, Vol. 1998.
- Krech, Hans: Der russische Krieg in Tschetschenien (1994-1996), Ein Handbuch, 2. unveränderte Auflage, Verlag Dr. Köster, Berlin, 2000.
- Krech, Hans: Der Zweite Tschetschenien-Krieg (1999-2002), Ein Handbuch, 1. Auflage, Verlag Dr. Köster, Berlin, 2002.
- Krikava, Franz; Ruhswurm, Hans; Seiser, Josef: Grundlagen der Elektrotechnik, Band 1, Oldenbourg Verlag, Wien, 1983.

- Kurz, Constanze; Rieger, Frank: Cyberwar. Die Gefahr aus dem Netz, Bertelsmann, München 2018.
- Lau, Torsten: Cyber-Crime und Cyber-Crime-Kontrolle. Zum möglichst rationalen Umgang mit weltweiten Bedrohungsszenarien: Cyber-Kriege und Cyber-Terror, Bonn 2003.
- Lessig, Lawrence: The Laws of Cyberspace. Essay presented at the Taiwan Net 98 conference, Taipei 1998.
- Libicki, Martin C.: What Is Information Warfare? National Defense University, August 1995.
- Liessmann, Konrad Paul: Lob der Grenze. Kritik der politischen Urteilskraft, Wien 2012.
- Linares, Filadelfo: Einblicke in Hugo Grotius' Werk, Vom Recht des Krieges und des Friedens, Hildesheim, New York 1993.
- Lücke, Friedrich (Hrsg.): Hermeneutik und Kritik mit besonderer Beziehung auf das Neue Testament von Dr. Friedrich Schleiermacher; Berlin 1838.
- Maresch, Rudolf; Rötzer, Florian: Cyberhypes. Möglichkeiten und Grenzen des Internet, 1. Aufl., Frankfurt 2001.
- Mey, Holger: Zur Entwicklung der modernen Kriegführung. In: Reiter, Erich: Jahrbuch für internationale Sicherheitspolitik 2001, S. 15-25.
- Minkwitz, Olivier: Ohne Hemmungen in den Krieg? Cyberwar und die Folgen, Frankfurt 2003.
- Montgomery of Alamein, Bernard Law Montgomery: Kriegsgeschichte. Weltgeschichte der Schlachten und Kriegszüge, Sonderausg. Aufl., Frechen 1999.
- Münkler, Herfried: Die neuen Kriege, 4. Aufl., Reinbek bei Hamburg 2010, (zit. 2010a).
- Münkler, Herfried: Der Wandel des Krieges. Von der Symmetrie zur Asymmetrie, [Unveränd. Nachdr.] Aufl., Weilerswist 2010, (zit. 2010b).
- Münkler, Herfried: Machiavelli. Die Begründung des politischen Denkens der Neuzeit aus der Krise der Republik Florenz, 10. Aufl., Frankfurt / Main, Fischer, 1984.
- Münkler, Herfried: Über den Krieg. Stationen der Kriegsgeschichte im Spiegel ihrer theoretischen Reflexion, 5. Aufl., Weilerswist 2008.
- Neisser, Heinrich; Windhager, Fritz (Hrsg.): Wie sicher ist Österreich? Beiträge zu einer konzeptiven Sicherheitspolitik, Wien 1982.

- Neuhold, Hanspeter u.a.: Österreichisches Handbuch des Völkerrechts, 2. Aufl., Wien 1991.
- Neuhold, Hanspeter u.a.: Österreichisches Handbuch des Völkerrechts, 2. Aufl., Band 2, Wien 1991.
- Nohlen, Dieter; Schultze, Rainer-Olaf: Lexikon der Politik. in: Lexikon der Politik (op. 1995).
- Nye, Joseph S.: Macht im 21. Jahrhundert. Politische Strategien für ein neues Zeitalter, München 2011.
- Olson, Parmy: Inside Anonymous. Aus dem Innenleben des globalen Cyber-Aufstands, München 2012.
- Pesendorfer, Wolfgang: Staat und äussere Sicherheit. In: Neisser, Heinrich; Windhager, Fritz (Hrsg.), Wie sicher ist Österreich? Beiträge zu einer konzeptiven Sicherheitspolitik, Wien 1982, S. 92–104.
- Pucher, Johann; Frank, Johann (Hrsg.): Strategie und Sicherheit 2012. Der Gestaltungsspielraum der österreichischen Sicherheitspolitik, 2012.
- Ramsden, Robert: What and where? Considerations for Command and Control of Cyberspace Operations, Newport 2010.
- Rasche, Michael: Der topographische Beginn der Philosophie: Anaximander. In: Schlitte, Annika; Hünefeldt, Thomas (Hrsg.): Ort und Verortung. Beiträge zu einem neuen Paradigma interdisziplinärer Forschung, Bielefeld 2017, S. 16-30.
- Rid, Thomas: Cyberwar will not take place, Hurst & Company, London 2013.
- Riedel, Siegfried: Vorwort zur deutschen Übersetzung der Militärstrategie von Sokolowski. In: Hahlweg, Werner: Lehrmeister des Kleinen Krieges. Von Clausewitz bis Mao Tse-Tung und (Che) Guevara, Darmstadt 1968, S. 14-16.
- Riemer, Andrea: Der Strategos 21. In Umbruchszeiten erfolgreich führen, Verlag Holzhausen, 2010.
- Rosenbach, Marcel; Stark, Holger: Der NSA Komplex. Edward Snowden und der Weg in die totale Überwachung, München 2014.
- Rötzer, Florian: Smart Cities im Cyberwar, Westend, Frankfurt 2015.
- Saalbach, K.: Cyberwar. Grundlagen-Methoden-Beispiele Version 4.0, 2012.
- Schadenböck, Dieter: Von der Taktik der Landstreitkräfte, Landesverteidigungsakademie, Wien 2013.
- Schmidt, Eric; Cohen, Jared: Die Vernetzung der Welt. Ein Blick in unsere Zukunft, Rowohlt, Reinbek bei Hamburg, 2013.

- Schmidt, Manfred G.: Wörterbuch zur Politik, 2. Aufl., Stuttgart 2004.
- Schmitt, Michael N. (Hrsg.): Tallinn Manual 2.0 on the International Law applicable to Cyber Operations, Cambridge University Press, New York 2017.
- Schröfl, Josef; Pankratz, Thomas (Hrsg.): Asymmetrische Kriegführung. Ein neues Phänomen der internationalen Politik?, 1. Aufl., Baden-Baden 2004.
- Schröfl, Josef; Muhr, Dieter; Rajaei, Bahram M.(Hrsg.): Hybrid and cyber war as consequences of the asymmetry. A comprehensive approach answering hybrid actors and activities in cyberspace: political social and military responses, Frankfurt am Main, New York 2011.
- Schwartzmann, Rolf: Der Vertrag von Lissabon. EU-Vertrag, Vertrag über die Arbeitsweise der EU - konsolidierte Fassungen, 3., überarb. und erw. Aufl., Stand: 1. Dezember 2009. Aufl., Heidelberg; München ; Landsberg [u.a.] 2010.
- Seiffert, Wolfgang: Wladimir W. Putin, Wiedergeburt einer Weltmacht?, Langen Müller, München 2000.
- Singer, Peter; Friedman Allan: Cybersecurity and Cyberwar. What everyone needs to know, New York 2014.
- Sommer, Peter; Brown, Ian: Reducing Systemic Cybersecurity Risk 2011.
- Stadler, Christian: Krieg, 1. Aufl., Wien 2009.
- Stahel, Albert A.: Klassiker der Strategie. Eine Bewertung, 4. Aufl., Zürich 2004.
- Strachan, Hew: Hew Strachan über Carl von Clausewitz, Vom Kriege, Dt. Erstausg. Aufl., München 2008.
- Strauss, Leo; Kojève, Alexandre; Kittler, Friedrich: Kunst des Schreibens, Merve Verlag, Berlin 2009.
- Stupka, Andreas: Strategie denken, Wien 2008.
- Stupka, Andreas: Militärwissenschaften. Ihre Grundlagen und ihr System, Wien 2011.
- Torkler, Rene: Einen Ort in der Welt haben. In: Schlitte, Annika; Hünefeldt, Thomas (Hrsg.): Ort und Verortung. Beiträge zu einem neuen Paradigma interdisziplinärer Forschung, Bielefeld 2017, S. 45-72.
- Vego, Milan: Operational Warfare, 2000.

11.3 Internetquellen

Dörrmann, Knut: Applicability of the Additional Protocols to Computer Network Attacks, Genf 2004.
<https://www.icrc.org/eng/resources/documents/misc/68lg92.htm>,
[12.05.2020].

Klauninger, Bert: Cyberspace als ein selbstorganisierendes System, o.J.
http://archive.gpi-online.de/files/_klauninger_cyberspace.pdf,
[12.05.2020].

Reilly, Jeffrey M.: Multidomain Operations, A Subtle but Significant Transition in Military Thought. In: Air & Space Power Journal (ASPJ), Volume 30, Issue 1, Spring 2016, S. 61-73.
https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-30_Issue-1/V-Reilly.pdf, [12.05.2020].

Schmitt, M.; Harrison Dinniss, H.; Wingfield, T.: Computers and War: The Legal Battlespace, Cambridge 2004.
<http://www.hpcresearch.org/sites/default/files/publications/schmittetal.pdf>, [12.05.2020].

<https://de.statista.com/statistik/daten/studie/187116/umfrage/anteil-der-haushalte-mit-internetzugang/>, [12.05.2020].

<https://richtervereinigung.at/justiz/rechtssystem/staatsgewalten-und-gewaltentrennung/>, [12.05.2020].

<https://www.faz.net/aktuell/politik/politische-buecher/terrorismus-und-souveraenitaet-auch-auf-fremdem-territorium-14117751.html>,
[12.05.2020].

http://www.internet4jurists.at/strafrecht/recht_oe1a.htm, [12.05.2020].

<https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/090000168008157a>, [12.05.2020].

<http://www2.informatik.hu-berlin.de/ki/lehre/ws0102/VLKogRob/Lexikon/Koordination/koordination.html>, [01.01.2014].

11.4 Zeitschriften, Fachjournale, Studien

Albright, David u.a.: Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? In: Institute for Science and International Security Report, 2010.

Arquilla, John; Ronfeldt, David: Cyberwar is coming! In: Comparative Strategy, Vol. 12, 1993, S. 141–165.

Bendrath, Ralf: Militärpolitik, Informationstechnologie und die Virtualisierung des Krieges. In: Forschungsgruppe Informationsgesellschaft und Sicherheitspolitik FoG:IS, Texte zur

- Sicherheitspolitik in der Informationsgesellschaft, 1997-99, FoG:IS
Arbeitspapier Nr. 1, November 1999, S. 24-40.
- Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK),
Abschätzung der Verwundbarkeit gegenüber Hochwasserereignissen auf
kommunaler Ebene, Band 4, 2010.
- Bundesgerichtshof, Neue Juristische Wochenschrift, 1995.
- Byung-Chul Han: Clausewitz im Drohnenkrieg. In: Die Zeit vom 15.11.2012.
S. 60.
- Bings, Felix u.a.: HIK Conflict Barometer 2011. disputes, non-violent crises,
violent crises, limited wars, wars, Campus Bergheim 2012.
- Council of the European Union (Hrsg.): Independent International Fact-
Finding Mission on the Conflict in Georgia (IIFMCG), Volume II,
September 2009.
- Center for Security Studies: CSS Analysen zur Sicherheitspolitik: Cyberwar:
Konzept, Stand und Grenzen, 2010.
- Falliere, Nicolas u.a.: W32.Stuxnet Dossier 2011.
- Frank, Johann; Pucher, Johann: Österreichische Sicherheits- und
Verteidigungspolitik unter geänderten Rahmenbedingungen – Chance zur
Profilschärfung des Bundesheeres. In: Österreichische Militärische
Zeitschrift, 5/2012, S. 552-567.
- Hersh, Seymour M.: Cyberwar: Die neue Front. In: Blätter für deutsche und
internationale Politik, 1/2011, S. 45-56.
- Klimburg (Hrsg.): National Cyber Security Framework Manual, NATO CCD
COE Publication, Tallinn 2012.
- Kuster, Matthias: Der Georgien-Krieg 2008 aus militärstrategischer Sicht. In:
Military Power Revue der Schweizer Armee, Nr.1/2011, S. 46-60.
- Ladinig, Udo; Saurugg, Herbert: Black Out. Nichts geht mehr. In:
Truppendienst, Nr. 326, 2/2012, S. 128-136.
- Lautsch, Siegfried: Zur Entwicklung der Militärwissenschaften in der
Russischen Föderation-Teil 1, Grundzüge des militärischen Denkens und
Handelns in der Gegenwart. In: Österreichische Militärische Zeitschrift,
5/2019, S. 573-583.
- Lätsch, Daniel: Innere Sicherheit und Armee. In: Military Power Revue der
Schweizer Armee, Nr.2/2012, S. 18-21.
- Lenz, Susanne: Vulnerabilität Kritischer Infrastrukturen, Bundesamt für
Bevölkerungsschutz und Katastrophenhilfe (BBK), Band 4, 2009.

- Rolofs, Oliver: Digital abwehrbereit? Cybersicherheit ist eine globalpolitische Aufgabe. Europäische Sicherheit, 60. Jg., Nr. 12, 2011.
- Schaller, Christian: Internationale Sicherheit und Völkerrecht im Cyberspace, Für klarere Regeln und mehr Verantwortung, Stiftung Wissenschaft und Politik, Deutsches Institut für Internationale Politik und Sicherheit, Berlin 2014.
- Shackelford, Scott J.: From Nuclear War to Net War: Analogizing Cyber Attacks in International Law. In: Berkeley Journal of International Law, 2009, S. 192–251.
- Stadler, Christian: Clausewitz zwischen Morsetelegraph und IFMIN. In: FMTSforum, 5. Jahrgang, 1/1995, S. 16-20.
- Stoll, Oliver: Gemeinschaft in der Fremde. Xenophons "Anabasis" als Quelle zum Söldnertum im klassischen Griechenland? In: Göttinger Forum für Altertumswissenschaft (Hrsg.), Göttinger Forum für Altertumswissenschaft 5, Heidelberg 2002, S. 123–183.
- Ziolkowski, Katharina: Computernetzwerkoperationen und die Zusatzprotokolle zu den Genfer Abkommen. In: Humanitäres Völkerrecht Informationsschriften. Journal of International Law of Peace and Armed Conflict, Vol. 21, 2008, S. 202–213.

12 Abkürzungsverzeichnis

A	
Abb.	Abbildung
ABl.	Amtsblatt
Abs.	Absatz
ACD	Active Cyber Defence
ADV	Allgemeine Dienstvorschrift für das Bundesheer
AEUV	Vertrag über die Arbeitsweise der EU
Anm. d. Verf.	Anmerkung des Verfassers
ANSSI	Nationale Agentur für Sicherheit der Informationssysteme
APCIP	Austrian Program for Critical Infrastructure Protection
Art.	Artikel
ASD	Australian Signals Directorate
Aufl.	Auflage
B	
Bd.	Band
BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
BKA	Bundeskanzleramt
BMG	Bundesministeriengesetz
BMI	Bundesministerium des Inneren
BMLV(S)	Bundesministerium für Landesverteidigung (und Sport)
B-VG	Bundes Verfassungsgesetz
bzw.	beziehungsweise
C	
CCD COE	Cooperative Cyber Defence Centre of Excellence
CERT	Computer Emergency Response Team
CERT	Computer Emergency Readiness Team
CNA	Computer Network Attack
CND	Computer Network Defence
CNE	Computer Network Exploitation
CNO	Computer Network Operations
CPCC	Civilian Planning and Conduct Capability
CPOE	Comprehensive Preperation of Operational Environment
CMPD	Crisis Management and Planning Directorate
CSS	Center for Security Studies
CW	Cyberwar

D	
d.h.	das heißt
DHS	Department for Homeland Security
DoD	Department of Defence
DoDIN	Department of Defence Information Network
DVBH	Dienstvorschrift für das Bundesheer
E	
Ebd.	Ebenda
EEAS	European External Affairs Services
ENISA	Europäische Agentur für Netz- und Informationssicherheit
EU	Europäische Union
EUMS	EU Militärstab
EUV	Vertrag über die Europäische Union
F	
F	folgende Seite
Ff	folgende Seiten
FMTS	Fernmeldetruppschule
FSB	russischer Inlandsgeheimdienst
G	
GCHQ	Government Communications Headquarters
GenLt	Generalleutnant
GSVP	Gemeinsame Sicherheits- und Verteidigungspolitik
GUS	Gemeinschaft unabhängiger Staaten
GZ	Geschäftszahl
H	
HIK	Heidelberg Institut für Internationale Konfliktforschung
HNS	Host Nation Support
Hrsg.	Herausgeber
HVR	Humanitäres Völkerrecht

I	
idF	in der Fassung
IIFMCG	Independent International Fact-Finding Mission on the Conflict in Georgia
IFMIN	Integrierte Fernmeldeinfrastruktur
IK	Irreguläre Kräfte
IKT	Informations- und Kommunikationstechnologie
inkl.	inklusive
IO	Internationale Organisationen
IT	Informationstechnologie
ITU	International Telecommunication Union
IW	Information War
J	
JOA	Joint Operations Area
K	
KI	Künstliche Intelligenz
KSchG	Konsumentenschutzgesetz
KSE-BVG	Bundesverfassungsgesetz über Kooperation und Solidarität bei der Entsendung von Einheiten und Einzelpersonen in das Ausland
L	
lit.	litera, Buchstabe
LOAC	Law of Armed Conflict
M	
MBG	Militärbefugnisgesetz
MDR	Managing Directorate for Resources
Mil	militärisch
MilStrat	Militärstrategie
MOD	Ministry of Defence
N	
NATO	North Atlantic Treaty Organisation
NCIRP	National Cyber Incident Response Plan
NCSS	National Cyber Security Strategy
NEMP	Nuklearelektromagnetischer Puls
NGO	Non Governmental Organisation
NIS	Netz- und Informationssystemssicherheit
NISG	Netz- und Informationssystemssicherheitsgesetz
Nr.	Nummer
NSA	National Security Agency
NS	Nationalsozialismus

O	
ÖBH	Österreichisches Bundesheer
o. J.	ohne Jahr
OK	Organisierte Kriminalität
ÖSCS	Österreichische Strategie für Cyber Sicherheit
ÖSS	Österreichische Sicherheitsstrategie
P	
PMC	Private Military Company
PMESII	Political Military Economic Social Infrastructure Information
Q	
R	
RBN	Russian Business Network
RF	Russische Föderation
RIS	Rechtsinformationssystem
RL	Richtlinie
S	
S.	Seite
SGDSN	Secrétariat général de la Défense et de la Sécurité nationale
Sic	so, wirklich so
SK	Streitkräfte
SPG	Sicherheitspolizeigesetz
SPS	Speicherprogrammierbare Steuerung
StGB	Strafgesetzbuch
SVN	Satzung der Vereinten Nationen
T	
TSK	Teilstreitkräfte
U	
u. a.	und andere
UK	United Kingdom
UN	United Nations
U.S.	United States
USA	United States of America
USAF	United States Airforce
USV	Umfassende Sicherheitsvorsorge

V	
VBS	Verteidigung, Bevölkerungsschutz und Sport
Vgl.	Vergleiche
VN	Vereinte Nationen
VR	Virtuelle Realität
W	
WaffG	Waffengesetz
WG	Wehrgesetz
WMD	Weapons of Mass Destruction
WoNA	Whole of Nation Approach
X	
Y	
Z	
Z	Ziffer
z.B.	zum Beispiel
Ziff.	Ziffer
Zl.	Zahl

13 Abbildungsverzeichnis

Abbildung 1: Kategorisierung des Krieges	26
Abbildung 2: Momente des bewaffneten Konfliktes	32
Abbildung 3: Akteure im Krieg	45
Abbildung 4: Die Trinität des Krieges	73
Abbildung 5: Intensität von Konflikten	86
Abbildung 6: Intensität des Krieges	87
Abbildung 7: Einteilung der Waffen im Cyberspace	119
Abbildung 8: Das Konzept der virtuellen Kriegführung	121
Abbildung 9: Beziehung zwischen den Aktionen im Cyberspace	136
Abbildung 10: Einordnung des Cyberwar	138
Abbildung 11: Intensität der Aktionen im Cyberspace	146
Abbildung 12: Die Trinität des Cyberwar	148
Abbildung 13: Die Teilbereiche der Cyber Security	152
Abbildung 14: Einfluss des Vernetzungsgrades	156
Abbildung 15: Einordnung des Cyberwar in den Kriegsbegriff	174
Abbildung 16: Anwendungsbereich des HVR	201
Abbildung 17: Verfahren zur Abschätzung der Verwundbarkeit	235
Abbildung 18: Beurteilungskreislauf zur Zuordnung der Führungsverantwortung	237

14 Lebenslauf

Name: Georg KUNOVJANEK

Geburtsdatum: 10.03.1971

Schulbildung: 1977-1981 Volksschule Bad Kleinkirchheim
1981-1985 Bundesrealgymnasium Spittal/Drau
1985-1990 HTL Nachrichtentechnik und
Elektronik Klagenfurt

Abschluss: Mai 1990 Reifeprüfung

Akademischer Werdegang:

03/2000 - 09/2003 Offiziersausbildung an der Theresianischen
Militärakademie, Wr. Neustadt
Abschluss: Mag.(FH) Militärische Führung

08/2009 – 04/2010 Ausbildung zum Bataillonskommandanten an der
Landesverteidigungsakademie, Wien
Abschluss: MSD, Master of Security- and
Defense Management

09/2010 – 06/2013 Hörer des 19. Generalstabslehrgangs

07/2013 – 09/2018 Lehrtätigkeit an der Theresianischen
Militärakademie im FH-Bachelorstudiengang
Militärische Führung, Wr. Neustadt

10/2018 – dato Leiter der Direktion an der Theresianischen
Militärakademie im FH-Bachelorstudiengang
Militärische Führung, Wr. Neustadt

Wissenschaftliche Arbeiten:

Das Handwerk des Krieges, Seminararbeit aus anthropologischen Theorien,
Wiener Neustadt 2000.

Die elektronische Kampfführung im II. Weltkrieg, Seminararbeit aus
Militärgeschichte, Wiener Neustadt 2000.

Führungsgrundsatz Handlungsfreiheit am Beispiel Galatas - Abwehr eines
Gegenangriffes - KRETA 24. Mai 1941, Seminar aus Führungs- und
Organisationslehre, Wiener Neustadt 2000.

Militär – Kultur – Identität, Seminararbeit aus Grundlagen der
pädagogischen Soziologie, Wiener Neustadt 2000.

Mit wehender Fahne und klingendem Spiel, Seminararbeit aus
Zeitgeschichte, Wiener Neustadt 2001.

Controlling als Führungsunterstützung - ÖBH spezifische Ausprägung, Seminararbeit aus Betriebswirtschaftslehre, Wiener Neustadt 2003.

Die Österreichische Garde - Zwischen Tradition und neuem Weg, Diplomarbeit, FH-Diplomstudiengang „Militärische Führung“, Wiener Neustadt 2003.

Die Führungsunterstützung im Bereich Luftunterstützung in Bezug auf eine Aviation Task Force und ein Brigade Aviation Element im In- und Auslandseinsatz, Seminararbeit, Wien 2007.

Das Planungsverfahren Führungsunterstützung eines multinationalen Bataillons in der Einsatzart Angriff im urbanen Umfeld im Szenario S&R, Seminararbeit, Wien 2010.

Darstellung des Close Air Supports (CAS) während der Operation Anaconda anhand der Fähigkeitsbereiche und ihre Auswirkungen auf das Gefecht, Seminararbeit, Wien 2010.

Einsatz eines verstärkten Führungsunterstützungsbataillons zur Errichtung des Führungsnetzes einer Framework-Brigade im Rahmen einer SOPF-Operation am afrikanischen Kontinent unter besonderer Berücksichtigung des Bereiches der Netzplanung und Netzsteuerung, Master Thesis, Lehrgang universitären Charakters „Sicherheitsmanagement“, Wien 2010.

Die russischen Interventionen in Tschetschenien und Georgien mit dem Fokus auf die Operativen Ziele und die Phase des Manövers - Russlands Kampf um den Kaukasus, Seminararbeit aus operativer Führung, Wien 2012.

Il Principe & Discorsi sopra la prima deca di Tito Livio, Die Strategie des Niccolo Machiavelli, Seminararbeit aus Militärstrategie, Wien 2012.

Die Panzergrenadierbrigade in der Verzögerung, Die multinationale gemischte Panzergrenadierbrigade als Teil einer multinationalen Division der EUFOR im Verzögerungskampf gegen irregulären Gegner innerhalb eines SOPF-Szenarios, Militärwissenschaftliche Arbeit aus Taktik, Wien 2012.

Militärstrategische Analyse von Kernländern - Die Militärstrategie der Russischen Föderation, Seminararbeit aus Militärstrategie, Wien 2013.