

Das Recht der inneren und äußeren Sicherheit

Band 11

Streitkräfteeinsatz zur Verteidigung gegen Cyberangriffe

Von

Maximilian L. Knoll



Duncker & Humblot · Berlin

MAXIMILIAN L. KNOLL

Streitkräfteeinsatz zur Verteidigung gegen Cyberangriffe

Das Recht der inneren und äußeren Sicherheit

Herausgegeben von Prof. Dr. Dr. Markus Thiel, Köln

Band 11

Streitkräfteeinsatz zur Verteidigung gegen Cyberangriffe

Von

Maximilian L. Knoll



Duncker & Humblot · Berlin

Die Juristische Fakultät der Universität Passau
hat diese Arbeit im Jahr 2019 als Dissertation angenommen.

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in
der Deutschen Nationalbibliografie; detaillierte bibliografische Daten
sind im Internet über <http://dnb.d-nb.de> abrufbar.

D 739

Alle Rechte vorbehalten

© 2020 Duncker & Humblot GmbH, Berlin

Satz: L101 Mediengestaltung, Fürstenwalde

Druck: CPI buchbücher.de GmbH, Birkach

Printed in Germany

ISSN 2199-3475

ISBN 978-3-428-15830-0 (Print)

ISBN 978-3-428-55830-8 (E-Book)

Gedruckt auf alterungsbeständigem (säurefreiem) Papier
entsprechend ISO 9706 ☺

Internet: <http://www.duncker-humblot.de>

Meinen Eltern

Respice finem!

Vorwort und Danksagung

Die vorliegende Dissertation wurde im Sommersemester 2019 an der Juristischen Fakultät der Universität Passau als Dissertation angenommen. Tag der Disputation war der 21. Juni 2019.

Eine Reihe von Personen waren auf dem Weg hierher wesentlich, weshalb ich ihnen im Folgenden gleichermaßen Dank und Anerkennung aussprechen möchte.

Ein herzlicher Dank gebührt in erster Linie meinem Doktorvater Prof. Dr. Meinhard Schröder. Er ließ mir nicht nur im Zusammenhang mit der Erstellung des Werkes, sondern auch bei der Ausgestaltung des Betreuungsverhältnisses weitgehend freie Hand, gleichwohl war er bei Bedarf stets ein äußerst konstruktiver Gesprächspartner. Daneben bin ich Prof. Dr. Hans-Georg Dederer zu Dank verpflichtet, der ebenso rasch wie unbürokratisch das Zweitgutachten erstellte.

Die Aufnahme in die Schriftenreihe „Das Recht der inneren und äußeren Sicherheit“ erfüllt mich gleichermaßen mit Stolz und Dankbarkeit. Letztere gebührt dem Herausgeber der Reihe, Prof. Dr. Dr. Markus Thiel.

Für die Gewährleistung der unabdingbaren geistigen Freiheit ist zu einem nicht unwesentlichen Teil die Konrad-Adenauer-Stiftung verantwortlich, von der ich als Promotionsstipendiat aufgenommen und während der Bearbeitung finanziell unterstützt wurde. Hierfür bin ich ihr zu Dank verpflichtet, was einschließt, ihr ideell verbunden zu bleiben.

Nicht hinwegzudenken für die Realisierung des Projekts in der vorliegenden Gestalt ist mein engstes familiäres und privates Umfeld, dem ich für die fortwährende Unterstützung danke und das ich – im Lichte des vollendeten Werkes – bitte, mir die eine oder andere Verstimmung nachzusehen.

Berlin, im Februar 2020

Maximilian L. Knoll

Inhaltsverzeichnis

Einführung und Gang der Untersuchung	19
I. Die sicherheitspolitische Ausgangslage	19
II. Einführung in die Fragestellung und Relevanz der Thematik	20
III. Erkenntnisinteresse	22
IV. Gang der Untersuchung	22
Kapitel (1): Die Bedrohungslage im und aus dem digitalen Raum	22
Kapitel (2): Status quo der Sicherheitsarchitektur mit Fokus auf den digitalen Raum	23
Kapitel (3): Die Verwendung der Streitkräfte zur Verteidigung im digitalen Raum	24
Kapitel (4): Inhalt und Ablauf der Verteidigung	26
V. Neue wissenschaftliche Erkenntnisse	27

Kapitel 1

Die Bedrohungslage im und aus dem digitalen Raum	28
A. Der Cyberraum als Ort von Auseinandersetzungen	29
I. Der Cyberraum – Ein Raum ohne Grenzen?	30
1. Begriffliche Abgrenzungen	30
a) Cyber-, digitaler und analoger Raum	31
b) Aufschlüsselung des Cyber-Raums – Was umfasst die Informationstechnik?	31
aa) (Computer-)Netzwerke	32
bb) Internet	32
cc) Eingebettete Systeme	33
2. Rückkopplung in die analoge Welt	34
a) Vermeintliche Flüchtigkeit des Cyberraums	34
b) Klare Bezugspunkte im analogen Raum	35
3. Zwischenergebnis	36
II. Kategorisierung der Auseinandersetzungen im Cyberraum	37
1. Cyber-War, Cyber-Terrorismus und Cyber-Kriminalität	37
a) Cyber-War – Ein Krieg im klassischen Sinne?	37
aa) Krieg als Begriff im Grundgesetz	38
bb) Die Begrifflichkeit <i>Krieg</i> und das kodifizierte Völkerrecht	40
cc) Verständnis des sogenannten Cyberwars	41
dd) Zwischenergebnis	43

b)	Cyber-Terrorismus	44
c)	Cyber-Kriminalität	45
2.	Computernetzwerkoperationen	45
a)	Cyber-Angriff	46
b)	Cyber-Intrusion	47
c)	Auf den Cyberraum abzielende Informationsoperationen	49
aa)	Vom Mittel zur Aufklärung zur modernen Desinformationskampagne	49
bb)	Begriffliches Verständnis	53
cc)	Betrachtungsgegenstand im Rahmen des Sammelbegriffs <i>Informationsoperationen</i>	55
d)	Cyber-Exploitation	57
e)	Zwischenergebnis zu den Computernetzwerkoperationen	59
3.	Mischphänomene: „Hybride Konflikte“ und „Hybride Kriegsführung“	59
a)	Verwischung der Grenze zwischen Krieg und Frieden	60
b)	Kombination des Einsatzes verschiedener Mittel und Methoden	60
c)	Die Rolle der Computernetzwerkoperationen im Rahmen der hybriden Kriegsführung	62
d)	Rechtliche Einordnung und Zwischenergebnis	63
B.	Gegenstand und Durchführung von Computernetzwerkoperationen	63
I.	Ziele und Methoden der Angriffe	64
1.	Nichtverfügbarkeit von Diensten und Anlagen	64
a)	Angriffsziele	65
b)	Methoden	65
aa)	Überlastung des Zielsystems	65
bb)	Schadsoftware und Ransomsoftware	68
(1)	Vielfalt der Schadprogramme	69
(a)	Viren	69
(b)	Würmer	69
(c)	Trojaner	70
(d)	Logische Bomben	71
(2)	Einschleusung von Schadsoftware	71
(a)	(Spear-)Phishing	71
(b)	Backdoor	73
2.	Beschädigung und Zerstörung	73
3.	Informationsunterdrückung, -verbreitung und Falschinformation	75
a)	Angriffsziele	75
b)	Methoden	75
aa)	Website-Defacement	75
bb)	False Amplifiers und Social Bots in sozialen Netzwerken	76
cc)	Überlastung	78
dd)	Schadprogramme	79
c)	Einzelbeispiele	79

4. Informationsbeschaffung	82
a) Bandbreite und Absicht	82
b) Angriffsziele und Methoden	82
c) Einzelbeispiele	83
5. Fremdsteuerung	85
6. Klassifizierung und Zwischenergebnis	86
II. Die Protagonisten	87
1. Staatliche Akteure	87
2. Nichtstaatliche Akteure	89
C. Ergebnis zur Bedrohungslage	90

*Kapitel 2***Status quo der Sicherheitsarchitektur
mit Fokus auf den digitalen Raum** 93

A. Der zivile Arm der Sicherheitsarchitektur	94
I. Polizeien	94
1. Landespolizei	96
a) Räumlicher Tätigkeitsbereich im digitalen Raum	97
b) Gefahrenabwehr im digitalen Raum	99
2. Polizeibehörden des Bundes	100
a) Bundeskriminalamt	100
aa) Erweiterte Zuständigkeit im Bereich der Strafverfolgung von Computerkriminalität	101
bb) Cyberterrorismus nunmehr Gegenstand der Gefahrenabwehr/ Straftatenverhütung	103
b) Bundespolizei	104
aa) Sicherung der physischen Bundesgrenzen	106
bb) Schutz der Verfassungsorgane – auch im digitalen Raum? ..	107
cc) Ausgewählte Einsatzmöglichkeit in Notlagen	110
dd) Einsatz über die Landesgrenzen hinaus	110
c) Polizei beim Deutschen Bundestag	112
II. Nachrichtendienste	115
1. Bundesamt für Verfassungsschutz (BfV)	116
a) Beobachtungsauftrag nach innen	117
b) Gesetzliche Anpassung an die Sicherheitslage	118
aa) Ausbau der Zentralstellenfunktion für den Cyberraum ..	118
bb) Erweiterung der Fernmeldeaufklärung auf Computer- straftaten	118
2. Bundesnachrichtendienst (BND)	119
a) Umfassender Beobachtungsauftrag nach außen	120
b) Gesetzgeberische Reaktion auf die doppelte Entgrenzung ..	121

III.	Bundesamt für Sicherheit in der Informationstechnologie	123
1.	Mobile Incident Response Teams (MIRTs)	124
2.	Computer Emergency Response Teams (CERT)	124
IV.	Sonstige Einrichtungen mit thematischem Bezug	125
1.	Bundesebene	125
a)	Nationales Cyber-Abwehrzentrum (NCAZ)	125
b)	Nationaler Cyber-Sicherheitsrat	127
c)	Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS)	127
d)	Agentur für Innovation in der Cybersicherheit	128
2.	Landesebene	128
V.	Gemeinsame Erkenntnisse aus den Zuständigkeiten der zivilen Sicherheitsbehörden	129
1.	Mit Blick auf die Zuständigkeitsverteilung: Verlagerung auf den Bund, im Kern jedoch Ländersache	129
2.	Mit Blick auf die Bundesbehörden: Eingeschränkt einsatzfähig im digitalen Raum	130
3.	Mit Blick auf den Einsatzraum: Beschränkung auf das Staatsgebiet der Bundesrepublik Deutschland	130
B.	Die Streitkräfte	131
I.	Der <i>Einsatz</i> als die zentrale Begrifflichkeit zur Verwendung der Streitkräfte	131
1.	Der Einsatz als Auslöser des Parlamentsvorbehalts	132
2.	Der Einsatzbegriff als Begrenzung der inländischen Verwendung der Streitkräfte	132
a)	Das eingriffsrechtliche Element – Grundrechtsbetroffenheit durch das spezifisch „Militärische“	134
b)	Das föderale Element – Wahrung der Länderhoheit	135
3.	Der Cyberangriff als Herausforderung für beide Dimensionen des Einsatzbegriffs	136
II.	Die einzelnen Verwendungsmöglichkeiten der Streitkräfte	137
1.	Die Verwendung der Streitkräfte zur Verteidigung im Aus- und Inland	137
2.	Die Verwendung der Streitkräfte im Ausland im Übrigen	139
3.	Die Verwendung der Streitkräfte im Innern	140
a)	Amtshilfe	140
b)	Regionale und überregionale Ausnahmesituation	140
c)	Qualifizierter innerer Notstand	141
III.	Thematisch relevante Komponenten der Streitkräfte	142
1.	Bundeswehr und Streitkräfte, zwei synonym zu verwendende Begriffe?	142
2.	Kommando Cyber- und Informationsraum (CIR)	143
3.	Militärischer Abschirmdienst (MAD)	145

Kapitel 3

Die Verwendung der Streitkräfte zur Verteidigung im digitalen Raum	147
A. Das historische Angriffsverständnis	
I. Wesen des Angriffs als Ausgangspunkt	148
II. Der Ost-West-Konflikt als Keimzelle der Wehrverfassung	149
1. Die Bedrohungslage quo ante	150
a) Territoriale Bedrohung	151
b) Ideologische Bedrohung	151
2. Die Bedrohungslage im Spiegel der bundesverfassungsgerichtlichen Rechtsprechung	152
3. Fortbestand trotz sich verändernder Sicherheitslage	153
III. Die konkrete Fassung des historischen Angriffsverständnisses	153
B. Das klassische Angriffsverständnis im Lichte des Cyberraums	155
I. Der Mythos der Rückverfolgbarkeit im Cyberraum	155
1. Begriffliche Einführung und klassische Relevanz	155
2. Zwecke der Rückverfolgbarkeit	157
3. Die (Un-)Möglichkeit der Rückverfolgung im Cyberraum	158
4. Akzeptanzdefizit des Wehrenden	161
5. Unzureichende Lösungsansätze	163
a) Vermutungsregelung	164
b) Vorsorgeprinzip	165
6. Zwischenergebnis	167
II. Das spezifisch „Militärische“ – Kein Differenzierungskriterium im Cyberraum	167
1. Grundlegendes	167
2. Traditionelles Verständnis	168
a) Status <i>Soldat</i> nicht maßgebend	168
b) Kein wesentlicher Unterschied beim Führungs- und Entscheidungsprozess	169
c) Die Ausrüstung als Differenzierungskriterium	170
3. In Ansehung des Cyberraums	171
III. Ergebnis zum klassischen Angriffsverständnis im Lichte des Cyberraums	172
IV. Konsequenz für die Abgrenzung der Streitkräfte zu den (Bundes-)Polizeien	172
1. Historische Abgrenzungsschwäche: Der Bundesgrenzschutz – Polizeieinheit oder militärischer Verbund?	173
2. Kein stichhaltiges Exklusivitätsverhältnis auf dem Boden des gesetzlichen Auftrags	174
a) Untaugliche Abgrenzung anhand des Auftrags zur Gefahrenabwehr	174

b)	Untaugliche Abgrenzung anhand der strafrechtlichen Tatbestandsmäßigkeit	174
c)	Zwischenergebnis	175
3.	Reflexion auf den Cyberraum	176
C.	Der verfassungsrechtliche Umgang mit der Rückverfolgungsproblematik ..	177
I.	Parameter für den Einsatz zur Verteidigung	177
1.	Die (Un-)Beachtlichkeit der Herkunft – Verteidigung auch im Innern?	178
a)	Grundgesetzlicher Ausgangspunkt des Inlandseinsatzes	178
b)	Bundesverfassungsgerichtliche Maßgaben	180
aa)	Inneneinsatz bei Angriff auf die „staatliche Rechts- und Freiheitsordnung“?	180
bb)	Gebot der „strikten Texttreue“ – auch für <i>Verteidigung</i> ? ..	182
c)	Umkehrschluss aus § 8 BPolG	184
d)	Art. 87a Abs. 4 GG abschließend für den militärischen Inneneinsatz zur (Cyber-)Gefahrenabwehr?	184
e)	Bundesstaatsprinzip	186
aa)	Die grundsätzliche Eigenstaatlichkeit der Länder	186
bb)	Exot: Verteidigungsauftrag	187
cc)	Lösung vom Grundsatz bei Cyberbezug	187
dd)	Technisch-praxisbezogene Betrachtung	188
f)	Relativierung des „Droh- und Einschüchterungspotentials“ durch die Streitkräfte im Cyberraum	188
g)	Zwischenergebnis	189
2.	Die (Un-)Beachtlichkeit des Urhebers – Verteidigung gegen jeden?	190
a)	Exkurs: Verhältnis nationales Recht/Völkerrecht	190
aa)	Gegenstand des Völkerrechts	191
bb)	Allgemeines Rangverhältnis	191
cc)	Besonderes, auf Verteidigung bezogenes Rangverhältnis ..	193
dd)	Auswirkung mangelnder Rückverfolgbarkeit	195
b)	Die (Un-)Beachtlichkeit staatlicher Urheberschaft	195
aa)	Qualitative und quantitative Zunahme nichtstaatlicher Akteure	196
bb)	Vorhalten einer „militärähnlichen Struktur“?	197
cc)	Verlagerung vom „Ob“ auf das „Wie“ der Verteidigung ..	198
3.	Zwischenergebnis	199
II.	Die Fassung des Verteidigungsobjekts	199
1.	Verständnis in Literatur und Rechtsprechung	200
2.	Verteidigung als staatliche Schutzpflicht?	202
a)	Herleitung der Schutzpflichten	202
b)	Erstreckung der Schutzpflicht auf den Verteidigungssektor ..	203
c)	Erstreckung der Schutzpflicht auf den digitalen Raum	205
d)	Der Staat in Ausübung seiner Schutzpflicht	208

e) Grund und Grenze eigenverantwortlichen Schutzes	208
f) Zwischenergebnis	210
3. Art. 87a GG als normativer Ausgangspunkt	211
a) Art. 115a GG Bestandteil der Notstandsverfassung	211
b) Keine Deckungsgleichheit von Verteidigung und Verteidigungsfall	212
c) Einzug des Verteidigungsbegriffs in das Grundgesetz	214
d) Ergebnis und Ausblick	214
4. Normbezogene Konkretisierung des Verteidigungsobjekts	215
a) Konkretisierung anhand von Art. 115a Abs. 1 GG	215
aa) Kein Widerspruch mit dem Verhältnis zwischen Art. 87a und Art. 115a GG	215
bb) Konkretisierung anhand des <i>Bundesgebiets</i>	215
b) Konkretisierung anhand von Art. 87a Abs. 3 GG	216
aa) Verteidigungsobjekt nur unter Vorbehalt?	217
bb) Inhaltliches Verständnis	217
5. Konkretisierung anhand grundgesetzlicher Kollektivschutzgüter ..	218
a) Grundlegendes und Zweck	218
aa) Bedürfnis nach Konkretisierung	218
bb) Art. 87a Abs. 4 GG als Ausschlussgrund?	219
b) Bestand des Bundes oder eines Landes	219
aa) Staatsgebiet	220
bb) Staatsvolk	221
cc) Staatsgewalt	222
dd) Funktionsfähigkeit des Staates	222
c) Freiheitliche demokratische Grundordnung	224
aa) Inhaltliches Verständnis	224
bb) Abgrenzung zum Bestand des Staates	225
cc) Verteidigungsobjekt oder reines Organisationsprinzip? ..	226
(1) Verteidigung als Ausprägung streitbarer Demokratie? ..	226
(2) Taugliches Angriffsobjekt?	227
(a) Rein geistige Auflehnung gegen die bestehende Ordnung tatbestandlich für die FDGO?	227
(b) Bekämpfung der FDGO auch von außen möglich? ..	229
5. Zwischenergebnis zur Fassung des Verteidigungsobjekts	230
III. Die Intensität der Schutzgutbetroffenheit	231
1. Grundgesetzliche Herleitung	232
2. Die einzelnen Verteidigungsobjekte im Fokus	232
a) Bestandsgefährdung	233
aa) Die Perspektive des inneren Notstandes	233
bb) Das Maß der Bestandsgefährdung im einfachen Recht	234
b) Gefährdung der freiheitlichen demokratischen Grundordnung ..	235

3.	Bewertung der Intensität im digitalen Raum	237
a)	Analogie zur Typizität analoger Angriffe	237
b)	Allokation der Mittel und Ort der Zuständigkeit	238
aa)	Tatsächliche Eignung (Haushaltsallokation)	238
bb)	Rechtliche Eignung (örtliche Zuständigkeit)	239
4.	Völkerrechtlicher Einfluss auf die Bewertung der Intensität	240
a)	Der Cyberraum – Regelungsgegenstand im Völkerrecht?	240
b)	Konsens im Cyberraum? – Bisher überschaubarer Erfolg	241
c)	Auslegung der UN-Charta	245
aa)	Gewaltverbot und bewaffneter Angriff im digitalen Raum ..	245
(1)	Verhältnis der Vorschriften zueinander	246
(2)	Inhaltliches Verständnis	246
(3)	Das Prinzip der Wirkungsäquivalenz	247
(4)	Zwischenergebnis	249
bb)	Gewalt-/Angriffsverständnis im Lichte der Zurechenbarkeit	249
cc)	Gesamtschau von Angriffs- und Verteidigungshandlung ..	250
dd)	Interventionsverbot	251
d)	Zwischenergebnis zum völkerrechtlichen Einfluss auf die Inten- sität	253
IV.	Subsumtion	254
1.	Kategorie der Beschädigung und Zerstörung	254
a)	Netzwerkexterne Schäden	254
b)	Exkurs: Kritische Infrastrukturen im Sinne des BSIG	255
c)	Netzwerkinterne Schäden	256
2.	Kategorie der Nichtverfügbarkeit von Diensten und Anlagen	257
a)	Belästigend für die Bevölkerung oder funktionsbeeinträchtigend für den Staat?	258
b)	Wahrung des rechtlichen Regel-Ausnahme-Verhältnisses	261
3.	Kategorie der Informationsunterdrückung, -verbreitung und Falsch- information	261
a)	Potentielle Strafbarkeit auf subordinativer Ebene	262
b)	Intervention auf der koordinativen Ebene?	263
c)	Informationskampagnen als Verteidigungsobjekt	265
d)	Gegenstand staatlicher Schutzwürdigkeit	267
4.	Kategorie der Informationsbeschaffung	268
a)	Kein zwischenstaatliches Spionageverbot	268
b)	Spionage als Intervention	269
c)	Spionage als bestandsgefährdend?	270
V.	Kapitelabschließende Bemerkungen	271

*Kapitel 4***Inhalt und Ablauf der Verteidigung** 273

A. Inhalt und Grenzen der Verteidigung	273
I. Offensive und defensive Verteidigung im Cyberraum	273
1. Die Kategorie der defensiven Cyberfähigkeiten	274
2. Schwerpunkt: Gegenstand offensiver Cybermaßnahmen	275
II. Die Art und Weise der Verteidigungsmaßnahme im engeren Sinne	276
1. Maßnahmen mit physischer Wirkung	276
a) Konflikt mit Rückverfolgungsproblematik und dem Prinzip der Unterscheidung	277
b) Praktische Konkordanz mit dem staatlichen Sicherheitsinteresse	279
2. Sonstige Maßnahmen und Grenzen derselben	280
a) Das Gebot der Verhältnismäßigkeit	280
b) Herausforderungen an das Unterscheidungsprinzip	281
c) Verbot des Angriffskrieges	282
B. Die Streitkräfte im digitalen Raum im Lichte des Parlamentsvorbehalts	284
I. Einführung und Abgrenzung	284
II. Grundsätzliche Maßgaben nach dem ParlBG	285
1. Territorialer Maßstab	285
2. Weniger Bewaffnung als Zweck des Einsatzes entscheidend	285
3. Grundsatz der vorherigen Zustimmung	286
III. Anwendbarkeit und Zweckmäßigkeit des Parlamentsvorbehalts im digitalen Raum	287
1. Anwendbarkeit	287
a) Maßstab: Ort der militärischen Erfolgsverwirklichung	287
b) Unbeachtlichkeit des konkreten Einsatzmittels	288
2. Zweckdienlichkeit	289
a) Einsatzbeginn	289
b) Zeitmoment	290
3. De lege ferenda	291
C. Einsatz zur Verteidigung im Innern im Konflikt mit dem „Trennungsgebot“?	293
I. Trennung von Nachrichtendiensten und Polizei	294
1. Verfassungsrang des „Trennungsgebots“	296
a) Der „Polizei-Brief“	297
b) Normativer Ursprung im Grundgesetz	298
c) Herleitung aus dem Rechtsstaatsprinzip	300
d) Recht auf informationelle Selbstbestimmung	301
2. Ergebnis zur verfassungsrechtlichen Verankerung des „Trennungs- gebots“	302
II. Konsequenz für etwaige Informationsbeschaffungen durch die Streit- kräfte	303

1. Hinreichende informationelle Trennung im Nationalen Cyber- Abwehrzentrum?	303
2. Hürde bei der Erstellung eines Cyber-Lagebildes	304
3. Verteidigungsauftrag als Legitimation zur Informationsgewinnung? .	305
4. Klarstellende Ergänzung im Wehrverfassungsrecht?	305
Schlussbetrachtung	307
Literaturverzeichnis	309
Sachverzeichnis	330

Einführung und Gang der Untersuchung

I. Die sicherheitspolitische Ausgangslage

Die Weltordnung, wie sie sich derzeit darstellt, verdient das Wort „Ordnung“ im eigentlichen Sinne nur bedingt. Sie hat mit der zum Ende des Kalten Krieges bestehenden Lage nur noch insoweit etwas gemeinsam, als sich die militärischen Konflikte der Gegenwart zunehmend als solche offenbaren, bei denen sich die einstigen Blöcke wiederum (mittelbar) gegenüberstehen, mindestens aber ihre Interessen projizieren. Von einer Renaissance des Kalten Krieges zu sprechen wäre gleichwohl verkürzt, nicht zuletzt, weil es der (wieder) erstarkenden und auf ubiquitären Einfluss zielenden Großmacht China nicht gerecht würde. Die provozierende These von Francis Fukuyama, wonach sich mit dem Fall der Sowjetunion die Demokratie nun abschließend durchgesetzt habe,¹ sieht sich angesichts der Bündelung klassischer staatlicher Machtinstrumente (natürliche, wirtschaftliche und militärische Ressourcen) in den Händen maximal bedingt demokratisch verfasster, mitunter aber gleichzeitig wirtschaftlich prosperierender Staaten sowie der horizontal hierzu verlaufenden Nutzung des Cyber- und Informationsraums herausgefordert. Wenn dabei von multipolarer Weltordnung gesprochen wird, dann ist der Cyber- und Informationsraum gleichzeitig als ein Grund und eine Ausprägung derselben anzuführen. Sein Potential verhält sich zu dieser neuen, multipolaren Weltordnung geradezu komplementär. Weder konnte jemals zuvor mit vergleichbar geringem Einsatz von Ressourcen ein derart hoher Wirkungsgrad erzielt werden, noch war es denkbar, dass sich Verantwortlichkeit und Haftbarkeit (im weiteren Sinne) bis zur Unkenntnis voneinander trennen lassen. Vor allem das Gewaltmonopol des Staates ist im Kern herausgefordert, wenn Angriffe ohne nennenswerte finanzielle Ressourcen von jedem vernetzten Ort der Welt, auf jeden vernetzten Ort der Welt unter Verschleierung der eigenen Identität durchgeführt werden können.

¹ Rezipiert von Williams/Sullivan/Matthews, Francis Fukuyama and the end of history, 2016, S. 87 f.

II. Einführung in die Fragestellung und Relevanz der Thematik

Die Begleiterscheinungen unserer in sämtlichen Facetten des täglichen Privat- und Wirtschaftslebens sowie in staatlicher Hinsicht zunehmend vernetzten Welt sind vermehrt sowohl Regelungsgegenstand in Gesetzen und Verordnungen als auch Anlass für die Anpassung staatlicher Institutionen. Parallel dazu hat das Bundesverfassungsgericht bekräftigt, dass grundrechtliche Freiheiten in den digitalen Raum hineinwirken und damit Gegenstand staatlicher Schutzverpflichtung sind.²

Von dieser anlassbezogenen Um- und Neustrukturierung werden auch die Streitkräfte als staatliche Organisationseinheit nicht ausgenommen, sondern mit der Einrichtung von Computer Emergency Response Teams sowie im Wege der Aufstellung eines militärischen Organisationsbereichs für den Cyber- und Informationsraum als sechste Teilstreitkraft seit dem 5. April 2017³ strukturell auf die sicherheitspolitischen Herausforderungen der Digitalisierung eingestellt. In diesem Zusammenhang betonten staatliche Entscheidungsträger, dass einerseits weder eine Differenzierung in Krieg und Frieden, noch eine solche in Äußere und Innere Sicherheit im Zeitalter der sogenannten Cyber-Bedrohungen bzw. Cyber-Kriegsführung möglich sei, andererseits, Verteidigung sich auch auf den Cyberraum erstrecke und die Freiheit der Bundesrepublik Deutschland auch in diesem verteidigt würde.⁴ Gleichwohl ist völlig ungeklärt, ob und inwieweit Militär zur Verteidigung gegen unter-

² Siehe hierzu BVerfGE 120, 274, 319; dazu auch *Johannes/Roßnagel*, Der Rechtsrahmen für einen Rechtsrahmen der Grundrechte in der digitalen Welt, S. 18 ff.

³ Tag der Indienststellung; Verantwortlich für den Aufbau war der Aufbaustab CIR im Bundesverteidigungsministerium im Zuge des Tagesbefehls der Bundesverteidigungsministerin v. 17. September 2015, abrufbar unter: <https://www.bmvg.de/de/aktuelles/projekt-von-herausragender-bedeutung-11458>.

⁴ Vgl. Ministerin von der Leyen bei der Vorstellung des aktuellen Weißbuchs zur Sicherheitspolitik und Zukunft der Bundeswehr im Jahr 2016, Zitat abrufbar unter: http://www.deutschlandfunk.de/bundeswehr-offensive-im-cyberwar.684.de.html?dram:article_id=360331. Die ehemalige Staatssekretärin des BMVg Suder (Verantwortungsbereich Planung, Ausrüstung, Informationstechnik und Nutzung) sagte auf der Koblenzer IT-Tagung zum Thema „Das neue digitale Gefechtsfeld – Auswirkungen auf Sicherheit und Souveränität“ am 07.09.2017, an der auch der Autor teilgenommen hat, dass der Staat nicht nur politisch, sondern auch digital aktiv handeln können müsse. Beachtlich ist auch der Satz „Deutschlands Sicherheit wird auch im Cyberraum verteidigt. Mach, was wirklich zählt“, der Gegenstand einer Werbekampagne der Bundeswehr beginnend im Jahr 2016 war, um der im Zuge der Aussetzung der Wehrpflicht andauernden Personalnot zu begegnen; das Weißbuch zur Sicherheitspolitik und Zukunft der Bundeswehr aus dem Jahr 2016 verweist zudem auf die Verteidigung von Cyberangriffen mit „offensive[n] Hochwertfähigkeiten“ (S. 93); siehe auch den Tagesbefehl vom 17.9.2015, in dem die Ministerin statuiert, dass die Bun-

schiedliche Formen digitaler Angriffe auf die Bundesrepublik Deutschland eingesetzt werden darf und wo hierbei die Kompetenzlinien zwischen allgemeinem Gefahrenabwehrrecht als Bestandteil originär polizeilicher Zuständigkeit und Verteidigung als ausschließlich militärische Zuständigkeit verlaufen.⁵

Es entsteht der Eindruck, als würden zwar Strukturen geschaffen, tatsächliche und rechtliche Fragen aber nur unzureichend beantwortet oder ganz außen vorgelassen werden. Die Notwendigkeit, die Verwendung der Streitkräfte zur Verteidigung von den Aufgaben anderer Sicherheitsbehörden abzgrenzen, erschließt sich nicht ohne weiteres und mag zunächst als redundant aufgefasst werden. Gleichwohl ist dies die Konsequenz aus der Bedrohungslage im Cyberraum, die sich nicht vergleichbar des analogen Raumes anhand von eher plakativen Merkmalen einem bestimmten Aufgabenträger zuordnen lässt. So lässt sich im analogen Raum typischerweise anhand der spezifischen Form der Bewaffnung eine Zuordnung der Zuständigkeit vornehmen. Wenn der Einsatz von – typischerweise dem Militär vorbehaltenen – Waffen dann auch noch von einem anderen Staat auf Befehl der jeweiligen politischen Führung ausgeht, erschiene eine Diskussion über die behördliche Aufgabenzuweisung gar überflüssig und wäre es im Ergebnis auch, ganz unabhängig davon, dass es eine klassische Kriegserklärung als formales Abgrenzungskriterium nicht mehr gibt.

Sind die eingesetzten Medien und Mittel dagegen weder dem Militär und damit typischerweise staatlicher Kernkompetenz vorbehalten, lässt sich der Einsatz und die Zielrichtung der Attacke gleichsam unter einen Straftatbestand des StGB subsumieren und ist insbesondere eine Rückverfolgung nur eingeschränkt oder aber nicht einmal ansatzweise möglich, eröffnen sich plötzlich Fragen nach der behördlichen Zuordnung. Wenn dann das Grundgesetz, wie in Art. 73 Abs. 1 Nr. 1 und 87a GG für die *Verteidigung*, die entsprechende Aufgabenzuweisung explizit dem Bund und hier den Streitkräften zuweist, also von einer gemeinsamen Kompetenz bzw. Zuständigkeit von Bund und Ländern sowohl in formeller als auch materieller Hinsicht absieht, drängt sich eine inhaltliche Auseinandersetzung mit dem *Gegenstand von Verteidigung* und damit einhergehend die Abgrenzung zu anderen Sicherheitsbehörden geradezu auf. Erschwerend kommt hinzu, dass das Grundge-

deswehr „zur erfolgreichen Operationsführung im gesamten Informationsraum“ befähigt werden müsse, zitiert aaO.

⁵ So statuiert die Cyber Sicherheitsstrategie des BMI 2016 auf S. 33, dass Cyber-Verteidigung als militärischer Teil der Gesamtverteidigung verfassungsmäßiger Auftrag der Bundeswehr sei; im neuen Weißbuch der Bundeswehr von 2016 heißt es: „Verteidigungsaspekte der gesamtstaatlichen Cybersicherheit sind originäre Aufgaben des Bundesministeriums der Verteidigung und der Bundeswehr“ (S. 11).