

Das Recht der inneren und äußeren Sicherheit

Band 22

Die deutschen Streitkräfte im Cyberraum

Eine Untersuchung der wehr- und
notstandsverfassungsrechtlichen Herausforderungen
eines neuen militärischen Operationsraums

Von

Fabian Walden



Duncker & Humblot · Berlin

FABIAN WALDEN

Die deutschen Streitkräfte im Cyberraum

Das Recht der inneren und äußeren Sicherheit

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

Band 22

Die deutschen Streitkräfte im Cyberraum

Eine Untersuchung der wehr- und
notstandsverfassungsrechtlichen Herausforderungen
eines neuen militärischen Operationsraums

Von

Fabian Walden



Duncker & Humblot · Berlin

Der Fachbereich Wirtschaft und Recht der EBS Law School Wiesbaden
hat diese Arbeit im Jahre 2022 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.

Alle Rechte vorbehalten
© 2023 Duncker & Humblot GmbH, Berlin
Satz: L101 Mediengestaltung, Fürstenwalde
Druck: CPI books GmbH, Leck
Printed in Germany

ISSN 2199-3475
ISBN 978-3-428-18793-5 (Print)
ISBN 978-3-428-58793-3 (E-Book)

Gedruckt auf alterungsbeständigem (säurefreiem) Papier
entsprechend ISO 9706 ☺

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

Vorwort

Die vorliegende Arbeit wurde im Sommertrimester 2022 von der juristischen Fakultät der EBS Universität für Wirtschaft und Recht als Dissertation angenommen. Tag der Disputation war der 8. August 2022. Rechtsprechung und Literatur konnten bis Juni 2021 berücksichtigt werden.

Einige Personen, die zum erfolgreichen Abschluss des Dissertationsvorhabens entscheidend beigetragen haben, möchte ich gerne namentlich erwähnen und ihnen meinen Dank aussprechen.

Mein herzlicher Dank gilt zunächst meinem Doktorvater Herrn Prof. Dr. Dr. Martin Will für die engagierte und konstruktive Betreuung. Von seinen wertvollen Hinweisen und Anmerkungen hat die Arbeit wesentlich profitiert. Herrn Prof. Dr. Steffen Detterbeck danke ich für die rasche Erstattung des Zweitgutachtens.

Danken möchte ich ferner meinem Freund, Kommilitonen und Mitstreiter Dr. Sebastian Tetzlaff, mit dem ich an vielen Bibliothekstagen Freud und Leid eines Dissertationsvorhabens geteilt habe. Der fachliche Austausch mit ihm hat die Arbeit bereichert.

Weiterer Dank gebührt meiner Frau Hanna Henrike Walden, die durch ihren bedingungslosen Rückhalt während des Dissertationsvorhabens erheblich zum Gelingen der Arbeit beigetragen hat.

Schließlich gilt mein besonderer Dank meinen Eltern Ina und Hartmut Walden, die meine Ausbildung stets unterstützt und gefördert haben. Mein akademischer Werdegang und die Realisierung der Dissertation wäre ohne ihren Beitrag nicht denkbar. Ihnen ist diese Arbeit daher gewidmet.

Ahrensburg, im Oktober 2022

Fabian Walden

Inhaltsübersicht

A. Einführung und Bestimmung des Untersuchungsgegenstands	23
I. Überblick	23
II. Der Cyberraum	26
1. Der Begriff des Cyberraums	26
2. Die Bedeutung des Cyberraums	28
3. Die Verwundbarkeit im und durch den Cyberraum	31
4. Die militärische Dimension des Cyberraums	58
III. Erkenntnisinteresse und Forschungsstand	74
IV. Gang der rechtlichen Untersuchung	77
B. Der Cyberangriff als Waffe	82
I. Die Waffe als zentraler Begriff der Wehr- und Notstandsverfassung	82
II. Der Waffenbegriff der Verfassung	83
1. Die hergebrachte Waffendefinition	83
2. Der wehrverfassungsrechtliche Waffenbegriff	86
III. Die Qualifikation von Cyberangriffen als Waffe	106
1. Die Qualifikation von Cyberangriffen in der Literatur	106
2. Die Beurteilung nach dem wehrverfassungsrechtlichen Waffenbegriff	112
IV. Ergebnisse in Thesen	124
C. Die Wehrverfassung im Cyberraum	125
I. Die verfassungsrechtliche Stellung der Streitkräfte	125
1. Die Streitkräfte als rechtlich gebundener Garant äußerer Souveränität	125
2. Die Cyberstreitkräfte als wesentlicher Bestandteil der Streitkräfte	128
II. Die Cyberstreitkräfte und der Verfassungsvorbehalt	129
1. Der Anwendungsbereich des Verfassungsvorbehalts	130
2. Der Einsatz der Cyberstreitkräfte	134
III. Der Verteidigungsauftrag der Streitkräfte im Cyberraum	173
1. Der Verteidigungsbegriff	173
2. Die Mittel der Verteidigung	185
3. Zwischenergebnis	192
IV. Die Cyberstreitkräfte und der wehrverfassungsrechtliche Parlamentsvorbehalt	193
1. Die Dogmatik des wehrverfassungsrechtlichen Parlamentsvorbehalts	194
2. Die Anwendung des wehrverfassungsrechtlichen Parlamentsvorbehalts auf Operationen der Streitkräfte im Cyberraum	199

3. Anpassung des wehrverfassungsrechtlichen Parlamentsvorbehalts für Operationen im Cyberraum	202
4. Zwischenergebnis	209
V. Ergebnisse in Thesen	210
D. Der Notstand im Cyberraum	212
I. Die Definition des Notstands	212
1. Die ordnende Funktion der Verfassung	212
2. Normalität als Grundlage normativer Geltungskraft	213
3. Der Notstand als Durchbrechung der vorausgesetzten Normallage ..	215
II. Die Notstandsverfassung des Grundgesetzes	217
1. Die Notwendigkeit einer verfassungsrechtlichen Regelung des Notstands	217
2. Die Implementierung der Notstandsverfassung	218
3. Die rechtliche Ausgestaltung der Notstandsverfassung	224
4. Die ungeschriebenen Notstandsbefugnisse	235
5. Zwischenergebnis	247
III. Der Cybernotstand und seine rechtliche Bewältigung	247
1. Die Möglichkeit des Cybernotstands	248
2. Voraussetzungen der rechtlichen Bewältigung des Cybernotstands	266
3. Die rechtliche Bewältigung des Cybernotstands in der bestehenden Notstandsverfassung	273
4. Die gebotene Weiterentwicklung der Notstandsverfassung	305
IV. Ergebnisse in Thesen	316
E. Schlussbetrachtung	318
Literaturverzeichnis	320
Stichwortverzeichnis	340

Inhaltsverzeichnis

A. Einführung und Bestimmung des Untersuchungsgegenstands	23
I. Überblick	23
II. Der Cyberraum	26
1. Der Begriff des Cyberraums	26
2. Die Bedeutung des Cyberraums	28
3. Die Verwundbarkeit im und durch den Cyberraum	31
a) Grundlagen der Verwundbarkeit durch den Cyberraum	32
aa) Physische Abschirmung vom Cyberraum	33
bb) Sicherheitslücken	34
cc) Menschliches Fehlverhalten	37
b) Ausnutzung der Verwundbarkeit durch Cyberangriffe	38
aa) Angriffsformen	39
(1) Schadsoftware	39
(a) Verbreitung und Aktivierung der Schadfunktion	40
(b) Nutzlast und Wirkung	41
(2) DoS/DDoS-Angriff	43
bb) Praxisbeispiele für Cyberangriffe	45
(1) Stuxnet	45
(2) BlackEnergy	48
(3) WannaCry	50
(4) NotPetya	52
(5) Estland 2007	53
(6) Hack des Bundestags	55
4. Die militärische Dimension des Cyberraums	58
a) Der Cyberraum als eigenständiger Operationsraum	58
aa) Wirkungsvielfalt im Cyberraum	59
bb) Verfügbarkeit und globale Wirkungsmöglichkeit	61
cc) Non-Attribution	63
b) Die Bundeswehr im Cyberraum	67
aa) Die Digitalisierung der Bundeswehr	67
bb) Das Kommando Cyber- und Informationsraum	69
cc) Die Aufgaben des Kommandos Cyber- und Informations- raum	69
(1) Betrieb und Schutz streitkräfteeigener Informationsinfra- strukturen	70
(2) Aufklärung und Wirkung im Cyberraum	72

III. Erkenntnisinteresse und Forschungsstand	74
IV. Gang der rechtlichen Untersuchung	77
B. Der Cyberangriff als Waffe	82
I. Die Waffe als zentraler Begriff der Wehr- und Notstandsverfassung ..	82
II. Der Waffenbegriff der Verfassung	83
1. Die hergebrachte Waffendefinition	83
2. Der wehrverfassungsrechtliche Waffenbegriff	86
a) Notwendigkeit eines einheitlichen Waffenbegriffs	86
b) Historischer Ausgangspunkt	90
c) Entwicklungsfähigkeit und Einflussfaktoren	91
aa) Entwicklungsfähigkeit	91
bb) Völkerrechtlicher Einfluss	93
(1) Völkerrechtsfreundlichkeit der Verfassung	94
(2) Auswirkungen für den Waffenbegriff	96
d) Allgemeine Merkmale des wehrverfassungsrechtlichen Waffenbe-	
griffs	98
aa) Physisches Schädigungspotenzial	98
bb) Unmittelbarkeit der Wirkung	100
cc) Erkennbarkeit der Wirkung	102
dd) Träger des unmittelbaren physischen Schädigungspotenzials	103
ee) Erheblichkeit der Wirkung	103
e) Die Definition der Waffe	105
III. Die Qualifikation von Cyberangriffen als Waffe	106
1. Die Qualifikation von Cyberangriffen in der Literatur	106
a) Cyberangriffe im Völkerrecht	106
b) Cyberangriffe im Verfassungsrecht	109
c) Zusammenfassende Erwägungen	111
2. Die Beurteilung nach dem wehrverfassungsrechtlichen Waffenbe-	
griff	112
a) Der virtuelle Befehl als Wirkmittel	113
b) Unmittelbares physisches Schädigungspotenzial von Cyberangrif-	
fen	113
aa) Funktionsstörung mit physischem Schaden am Gesamtsys-	
tem	113
bb) Vorübergehende Beeinträchtigungen der Funktionsfähigkeit	115
(1) Ausgeschlossene Funktionsfähigkeit als physischer	
Schaden?	115
(2) Unmittelbarkeitszusammenhang zwischen Cyberangriff	
und Schaden	116
cc) Die Grenze physischen Schädigungspotenzials	120
c) Qualifikation gegenwärtiger Cyberoperationen als Waffengewalt	122
IV. Ergebnisse in Thesen	124

C. Die Wehrverfassung im Cyberraum	125
I. Die verfassungsrechtliche Stellung der Streitkräfte	125
1. Die Streitkräfte als rechtlich gebundener Garant äußerer Souveränität	125
2. Die Cyberstreitkräfte als wesentlicher Bestandteil der Streitkräfte ..	128
II. Die Cyberstreitkräfte und der Verfassungsvorbehalt	129
1. Der Anwendungsbereich des Verfassungsvorbehalts	130
2. Der Einsatz der Cyberstreitkräfte	134
a) Der Einsatzbegriff des Art. 87a Abs. 2 GG	135
aa) Der Einsatz im Innern	136
bb) Der Einsatz nach Außen	138
(1) Dualistisches Verständnis des Einsatzbegriffs	138
(2) Die Definition des Außeneinsatzes	142
b) Die Verwendung der Cyberstreitkräfte als Einsatz	145
aa) Der Inneneinsatz der Cyberstreitkräfte	145
(1) Eingriffszusammenhang durch Waffengewalt im Cyberraum	145
(2) Eingriffszusammenhang durch Eingriff in die Vertraulichkeit und Integrität informationstechnischer Systeme	146
(3) Eingriffszusammenhang durch Droh- und Einschüchterungspotenzial im Cyberraum?	147
(4) Verwendungen unterhalb der Einsatzschwelle	148
(a) Schutz streitkräfteeigener Informationsinfrastrukturen	149
(b) Öffentlichkeitsarbeit	149
(c) Amtshilfe	150
(d) Beteiligung am Nationalen Cyber-Abwehrzentrum	151
(aa) Aufgabe des Nationalen Cyber-Abwehrzentrums	151
(bb) Einsatzqualität der Beteiligung	152
(5) Zwischenergebnis	153
bb) Der Außeneinsatz der Cyberstreitkräfte	154
(1) Anwendbarkeit des äußeren Einsatzbegriffs	154
(2) Die unmittelbare Einbeziehung in bewaffnete Unternehmungen	155
(a) Cyberoperationen als Waffengewalt	156
(b) Cyberoperationen unterhalb der Schwelle zur Waffengewalt	157
(aa) Notwendigkeit der Erfassung unbewaffneter Cyberoperationen	158
(bb) Konkrete Einbeziehungserwartung in bewaffnete Unternehmungen	159
(cc) Einbeziehung in bewaffnete oder von <i>ähnlicher militärischer Gewalt</i> geprägte Unternehmungen	161

	(α) Definition der militärischen Gewalt	162
	(β) Militärische Gewalt im Cyberraum	163
	(3) Die mittelbare Einbeziehung	165
	(4) Einsatzqualität des militärischen Nachrichtenwesens im Cyberraum	166
	(5) Zwischenergebnis	172
III.	Der Verteidigungsauftrag der Streitkräfte im Cyberraum	173
1.	Der Verteidigungsbegriff	173
a)	Militärischer Angriff von außen	173
b)	Urheber des militärischen Angriffs von außen	177
aa)	Angriff durch nichtstaatliche Akteure	177
bb)	Notwendigkeit der Identifizierbarkeit des Angreifers	179
(1)	Das Gebot strikter Texttreue	179
(a)	Die Herleitung des Gebots strikter Texttreue	179
(b)	Anknüpfungspunkt der strikten Texttreue	181
(2)	Völkerrechtsfreundlichkeit der Verfassung	181
(3)	Bestimmung der Verteidigungsbefugnis als Prognoseent- scheidung	182
2.	Die Mittel der Verteidigung	185
a)	Beschränkung der Verteidigungsmittel durch den Grundsatz der Verhältnismäßigkeit	185
b)	Art und Umfang der Verteidigung im Cyberraum	187
aa)	Vorrang der Cyberverteidigung	187
bb)	Identifizierbarkeit des Angreifers	189
(1)	Nicht identifizierbarer Angreifer	190
(2)	Indiziell identifizierbarer Angreifer	191
(3)	Eindeutig identifizierbarer Angreifer	192
3.	Zwischenergebnis	192
IV.	Die Cyberstreitkräfte und der wehrverfassungsrechtliche Parla- mentsvorbehalt	193
1.	Die Dogmatik des wehrverfassungsrechtlichen Parla- mentsvorbehalts	194
a)	Die Rechtsgrundlagen des wehrverfassungsrechtlichen Parla- mentsvorbehalts	194
b)	Die Teleologie des wehrverfassungsrechtlichen Parla- mentsvorbehalts	196
aa)	Kompensationsfunktion	196
bb)	Friedenssicherung und Schutz der Soldaten	198
2.	Die Anwendung des wehrverfassungsrechtlichen Parla- mentsvorbehalts auf Operationen der Streitkräfte im Cyberraum	199
a)	Anwendungsvoraussetzungen	199
b)	Ausnahme bei Gefahr im Verzug	201
3.	Anpassung des wehrverfassungsrechtlichen Parla- mentsvorbehalts für Operationen im Cyberraum	202

a)	Spannungsverhältnis zwischen militärischer Wirksamkeit und öffentlicher parlamentarischer Kontrolle	202
b)	Parlamentarische Kontrolle bei gleichzeitiger Sicherung von Geheimhaltungsinteressen	204
aa)	Cyberoperationen als genereller Fall von Gefahr in Verzug	204
bb)	Cyberoperationen als Kommandooperationen	205
cc)	Ausschuss als parlamentarisches Kontrollgremium	207
4.	Zwischenergebnis	209
V.	Ergebnisse in Thesen	210
D.	Der Notstand im Cyberraum	212
I.	Die Definition des Notstands	212
1.	Die ordnende Funktion der Verfassung	212
2.	Normalität als Grundlage normativer Geltungskraft	213
3.	Der Notstand als Durchbrechung der vorausgesetzten Normallage	215
II.	Die Notstandsverfassung des Grundgesetzes	217
1.	Die Notwendigkeit einer verfassungsrechtlichen Regelung des Notstands	217
2.	Die Implementierung der Notstandsverfassung	218
a)	Parlamentarischer Rat und Notstandsverfassung	218
b)	Wehrverfassung von 1956	220
c)	Notstandsverfassung von 1968	220
3.	Die rechtliche Ausgestaltung der Notstandsverfassung	224
a)	Die Unterscheidung des inneren und äußeren Notstands	224
b)	Der innere Notstand	225
aa)	Staatsnotstand	225
bb)	Katastrophennotstand	226
(1)	Erscheinungsformen des Katastrophennotstands	226
(2)	Handlungsbefugnisse im Katastrophennotstand	227
cc)	Grundrechte im inneren Notstand	228
c)	Der äußere Notstand	228
aa)	Verteidigungsfall	229
(1)	Voraussetzung	229
(2)	Auswirkungen auf das Gesetzgebungsverfahren	229
(3)	Verlängerung von Wahlperioden und Amtszeiten	231
(4)	Verhältnis von Bund und Ländern	231
(5)	Stellung des Bundesverfassungsgerichts	231
(6)	Grundrechte im äußeren Notstand	232
(7)	Beendigung des Verteidigungsfalls	232
bb)	Spannungsfall, Zustimmungsfall und Bündnisfall	232
d)	Die wesentlichen Merkmale der Notstandsverfassung	233
aa)	Kasuistisches Modell	234
bb)	Notstand als Effektivitätsproblem	234

4. Die ungeschriebenen Notstandsbefugnisse	235
a) Rechtliche Herleitung ungeschriebener Notstandsbefugnisse	236
aa) Ablehnung ungeschriebener Handlungsbefugnisse	236
(1) Strenge Normativität der Verfassung	236
(2) Missbrauchsgefahr	238
(3) Zusammenfassende Erwägungen	242
bb) Die verfassungsrechtliche Begründung ungeschriebener Notstandsbefugnisse	243
cc) Zusammenfassende Erwägungen	245
b) Voraussetzungen und Ermächtigungsumfang der ungeschriebenen Notstandsbefugnisse	245
5. Zwischenergebnis	247
III. Der Cybernotstand und seine rechtliche Bewältigung	247
1. Die Möglichkeit des Cybernotstands	248
a) Bewaffnete Cyberangriffe	248
b) Cyberangriffe unterhalb der Schwelle zur Waffengewalt	249
aa) Die Integrationsfähigkeit der Normallage	249
bb) Die Integration des Cyberraums in Normallage	251
(1) Abhängigkeit von Staatsorganen	251
(a) Abhängigkeit der Verwaltung	251
(b) Abhängigkeit der Streitkräfte	255
(2) Grundlage der Freiheitsverwirklichung der Bürger	255
(a) Kommunikationsfreiheiten	256
(b) Freie Persönlichkeitsentfaltung	257
(c) Wirtschaftsfreiheit	258
(3) Der Cyberraum als Bestandteil der Grundlagenversorgung	259
(a) Bestandteil der Grundlagenversorgung	259
(b) Staatliche Gewährleistungsverantwortung aus Art. 87f GG	260
(4) Zusammenfassende Erwägungen	262
c) Die allgemeine Definition des Cybernotstands	263
2. Voraussetzungen der rechtlichen Bewältigung des Cybernotstands	266
a) Die tatbestandliche Gesamterfassung des Cybernotstands	266
b) Die Stärkung der Reaktionsfähigkeit des Staats	266
aa) Funktionskonzentration der Exekutive	267
(1) Zuständigkeit der Bundesexekutive für den Cybernotstand	267
(2) Keine vorrangige Zuständigkeit der Länder	268
bb) Einsatz der Streitkräfte und der Bundespolizei	269
cc) Einwirkungsmöglichkeit auf die Betreiber kritischer Infrastrukturen	270
(1) Notwendigkeit einer Einwirkungsmöglichkeit	270

(2) Rechtliche Ausgestaltung der Einwirkungsmöglichkeit	272
c) Zusammenfassende Erwägungen	273
3. Die rechtliche Bewältigung des Cybernotstands in der bestehenden Notstandsverfassung	273
a) Systematische Integration des Cybernotstands in die Notstandsverfassung	274
aa) Realisierungsort der Notstandsgefahr	274
bb) Herkunft der Notstandsgefahr	277
cc) Zusammenfassende Erwägungen	281
b) Cybernotstand als äußerer Notstand	282
aa) Tatbestandliche Erfassung	282
(1) Bewaffneter Angriff auf das Bundesgebiet	282
(2) Erheblichkeit der Waffengewalt	282
(3) Zugehörigkeit des Angreifers	284
(4) Zusammenfassende Erwägungen	285
bb) Rechtsfolgen	286
(1) Umgestaltung der Verfassungsordnung	286
(2) Einsatz der Streitkräfte	287
cc) Zusammenfassende Erwägungen	287
c) Cybernotstand als innerer Notstand	288
aa) Cybernotstand als Staatsnotstand	288
(1) Tatbestandliche Erfassung	288
(a) Bestand des Bundes oder eines Landes	289
(b) Freiheitliche demokratische Grundordnung	290
(c) Der Störer	292
(2) Rechtsfolgen	293
(a) Art. 91 GG	293
(b) Art. 87a Abs. 4 GG	294
(aa) Einsatzvoraussetzungen	294
(bb) Einsatzbefugnisse	294
(α) Schutz ziviler Objekte	294
(β) Organisierte und militärisch bewaffnete Aufständische	295
(c) Das Eskalationsmodell im Cybernotstand	296
(3) Zusammenfassende Erwägungen	297
bb) Cybernotstand als Katastrophennotstand	298
(1) Tatbestandliche Erfassung	298
(a) Naturkatastrophe	298
(b) Besonders schwerer Unglücksfall	298
(2) Rechtsfolgen	300
(a) Art. 35 Abs. 2 S. 2 GG	300
(b) Art. 35 Abs. 3 GG	301
(c) Das Eskalationsmodell im Cybernotstand	301

(3) Zusammenfassende Erwägungen	302
d) Cybernotstand und ungeschriebene Notstandsbefugnisse	302
e) Zusammenfassende Erwägungen	303
4. Die gebotene Weiterentwicklung der Notstandsverfassung	305
a) Vorschlag zur rechtlichen Bewältigung des Cybernotstands	306
aa) Tatbestandliche Gesamterfassung des Cybernotstands	306
bb) Keine Differenzierung nach Gefahrherkunft und Auswirkungsort	307
cc) Zuständigkeit der Bundesexekutive	308
dd) Einsatz der Cyberstreitkräfte und der Bundespolizei	309
ee) Weisungsrecht gegenüber kritischen Infrastrukturen	311
ff) Einstellungsverlangen des Bundesrats und des Bundestags	313
gg) Integration in die bestehende Notstandsverfassung des Grundgesetzes	314
b) Zum Erfordernis eines Tätigwerdens des verfassungsändernden Gesetzgebers	315
IV. Ergebnisse in Thesen	316
E. Schlussbetrachtung	318
Literaturverzeichnis	320
Stichwortverzeichnis	340

Abkürzungsverzeichnis

Dieses Abkürzungsverzeichnis konzentriert sich auf wichtigere und auf wenig bekannte Abkürzungen. Im Übrigen sei auf die gängigen Abkürzungsverzeichnisse verwiesen.

a. A.	andere Ansicht
Abg.	Abgeordneter
Abs.	Absatz
a. F.	alte Fassung
AfP	Zeitschrift für Medien- und Kommunikationsrecht
AK	Alternativkommentar
Aktual.	Aktualisierung
Amerik.	Amerikanisch
Anl.	Anlage
Anm.	Anmerkung
AöR	Archiv des öffentlichen Rechts
APT	Advanced Persistent Threat
Art.	Artikel
Aufl.	Auflage
AVR	Archiv des Völkerrechts
AWACS	Airborne Warning and Control System
BaföG	Bundesgesetz über individuelle Förderung der Ausbildung (Bundesausbildungsförderungsgesetz)
BB	Der Betriebs-Berater
Bd.	Band
BeckOK	Beck'scher Onlinekommentar
BeckRS	Elektronische Entscheidungsdatenbank in beck-online
BGB	Bürgerliches Gesetzbuch
BGBI.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BGHSt	Entscheidungen des Bundesgerichtshofes in Strafsachen
BGHZ	Entscheidungen des Bundesgerichtshofs in Zivilsachen
BMVg	Bundesministerium der Verteidigung
BND	Bundesnachrichtendienst
Bot	Robot

BPolG	Gesetz über die Bundespolizei
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
BSI-KritisV	Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz
BT	Bundestag
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungen des Bundesverfassungsgerichts
BVerfGG	Gesetz über das Bundesverfassungsgericht (Bundesverfassungsgerichtsgesetz)
BVerfGK	Kammerentscheidungen des Bundesverfassungsgerichts
bzw.	beziehungsweise
CERT	Computer Emergency Response Team
CIR	Cyber- und Informationsraum
CR	Computer und Recht
DDoS	Distributed Denial of Service
ders.	derselbe
Diss.	Dissertation
DoS	Denial of Service
DÖV	Die öffentliche Verwaltung
DRiZ	Deutsche Richterzeitung
Drs.	Drucksache
dt.	deutsch
DVBl.	Deutsches Verwaltungsblatt
ebda.	ebenda
EGovG SH	Gesetz zur elektronischen Verwaltung für Schleswig-Holstein (E-Government-Gesetz)
EL.	Ergänzungslieferung
EloKa	elektronischer Kampfführung
EMP	elektromagnetischer Impuls
EuGH	Europäischer Gerichtshof
EuGRZ	Europäische Grundrechte-Zeitschrift
f.	folgende
F.A.S.	Frankfurter Allgemeine Sonntagszeitung
FAZ	Frankfurter Allgemeine Zeitung
FDP	Freie Demokratische Partei
Fn.	Fußnote
FS	Festschrift

gem.	gemäß
GG	Grundgesetz für die Bundesrepublik Deutschland
ggf.	gegebenenfalls
GO-BT	Geschäftsordnung des Deutschen Bundestages
GSZ	Zeitschrift für das Gesamte Sicherheitsrecht
HBStR	Handbuch des Staatsrechts der Bundesrepublik Deutschland (hrsgg. von Josef Isensee und Paul Kirchhof)
HChEntw	Herrenchiemseer Entwurf
Hrsg.	Herausgeber
hrsgg.	herausgegeben
HuV-I	Humanitäres Völkerrecht – Informationsschriften
INPOL	Informationssystem Polizei
i. S. d.	im Sinne des
IT	Informationstechnik
IT-NetzG	Gesetz über die Verbindung der informationstechnischen Netze des Bundes und der Länder – Gesetz zur Ausführung von Arti- kel 91c Absatz 4 des Grundgesetzes
i. V. m.	in Verbindung mit
JöR	Jahrbuch des öffentlichen Rechts der Gegenwart
JuS	Juristische Schulung
JZ	JuristenZeitung
Kap.	Kapitel
KdoStratAufkl	Kommando Strategische Aufklärung
km	Kilometer
KPD	Kommunistische Partei Deutschlands
krit.	kritisch
KrWaffKontrG	Ausführungsgesetz zu Artikel 26 Abs. 2 des Grundgesetzes (Kriegswaffenkontrollgesetz)
KSK	Kommando Spezialkräfte
KSM	Kommando Spezialkräfte der Marine
KTS	Zeitschrift für Insolvenzrecht
LG	Landgericht
Lit.	Literatur
LuftSiG	Luftsicherheitsgesetz
MADG	Gesetz über den militärischen Abschirmdienst
MIRT	Mobile Incident Response Team
MMR	MultiMedia und Recht
m. w. N.	mit weiteren Nachweisen
NATO	North Atlantic Treaty Organization

NCAZ	Nationales Cyber-Abwehrzentrum
Neudr.	Neudruck
n. F.	neue Fassung
NJW	Neue Juristische Wochenschrift
Nr.	Nummer
NSA	National Security Agency
NVwZ	Neue Zeitschrift für Verwaltungsrecht
NWVBl.	Nordrhein-Westfälische Verwaltungsblätter
NZWehrr	Neue Zeitschrift für Wehrrecht
ParlBG	Gesetz über die parlamentarische Beteiligung bei der Entscheidung über den Einsatz bewaffneter Streitkräfte im Ausland (Parlamentsbeteiligungsgesetz)
PTSG	Gesetz zur Sicherstellung von Postdienstleistungen und Telekommunikationsdiensten in besonderen Fällen
RAF	Rote Armee Fraktion
Res.	Resolution
Rn.	Randnummer
Rspr.	Rechtsprechung
S.	Seite
SAR	Search and Rescue
SchlHVerf	Verfassung des Landes Schleswig-Holstein
Slg.	Sammlung der Rechtsprechung des Gerichtshofes und des Gerichts Erster Instanz
std.	ständige
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
u.	und
UN	Vereinte Nationen
UN-Charta	Charta der Vereinten Nationen
UN Doc.	United Nations Document
unveränd.	unverändert
USA	Vereinigte Staaten von Amerika
UZwGBw	Gesetz über die Anwendung unmittelbaren Zwanges und die Ausübung besonderer Befugnisse durch Soldaten der Bundeswehr und verbündeter Streitkräfte sowie zivile Wachpersonen
Verf.	Verfasser
vgl.	vergleiche
Vorb.	Vorbermerkung
VVDStRL	Veröffentlichungen der Vereinigung der Deutschen Staatsrechtslehrer

VwVfG	Verwaltungsverfahrensgesetz
WEU	Westeuropäische Union
WRV	Weimarer Reichsverfassung
ZaöRV	Zeitschrift für ausländisches öffentliches Recht und Völkerrecht
z.B.	zum Beispiel
ZParl	Zeitschrift für Parlamentsfragen
ZRP	Zeitschrift für Rechtspolitik

A. Einführung und Bestimmung des Untersuchungsgegenstands

I. Überblick

Durch Tagesbefehl vom 5. April 2017 hat die damalige Bundesministerin der Verteidigung *von der Leyen* das Kommando Cyber- und Informationsraum als neuen militärischen Organisationsbereich der Bundeswehr in Dienst gestellt.¹ Die Bundeswehr bündelt damit die Teile der Streitkräfte, deren originärer Operationsraum der Cyberraum ist. Sie erhalten den Charakter einer eigenen Teilstreitkraft. Ähnlich wie Heer, Luftwaffe und Marine umfassend für ihre Dimensionen Land, Luft und See zuständig sind, ist das Kommando Cyber- und Informationsraum ganzheitlich für die Dimension des Cyberraums verantwortlich.² Der neue Organisationsbereich und seine Angehörigen stellen zum einen den Schutz und den Betrieb der informationstechnischen Systeme der Bundeswehr – sowohl im Inland als auch im Einsatz – sicher. Zum anderen stärken sie die Fähigkeiten zur Aufklärung und Wirkung im Cyberraum und entwickeln diese weiter.

Doch woraus ergibt sich die Notwendigkeit der Aufstellung? Generalleutnant *Leinhos* – der erste Inspekteur des Kommandos Cyber- und Informationsraum – nennt den Grund: „Staat, Wirtschaft und Gesellschaft sind in dieser zunehmend vernetzten, digitalisierten Welt für Angriffe im Cyber- und Informationsraum verwundbarer geworden. Die Zahl und Qualität der Cyber-Angriffe und Maßnahmen im Informationsumfeld durch staatliche wie nicht-staatliche Akteure nehmen mit exponentieller Geschwindigkeit zu“.³ Auftrag der Bundeswehr ist, die von außen bedrohte Souveränität der Bundesrepublik

¹ *Die Bundesministerin*, Tagesbefehl vom 05.04.2017, S. 1.

² Hier und im Folgenden *Bundesministerium der Verteidigung*, Entwicklung des Organisationsbereichs bei der Bundeswehr, abrufbar unter <https://www.bmvg.de/de/themen/cybersicherheit/cyber-verteidigung/entwicklung-des-org-bereich-bei-der-bw>, Internetquellen, die sich stets ändern können, wurden zuletzt im Mai 2021 geprüft soweit nicht abweichend gekennzeichnet; *Bundesministerium der Verteidigung* (Hrsg.), Strategische Leitlinie Cyber-Verteidigung im Geschäftsbereich BMVg, 2015 (unveröffentlicht); *Bundesministerium der Verteidigung* (Hrsg.), Abschlussbericht Austausch Cyber- und Informationsraum, 2016, S. 1.

³ *L. Leinhos*, Neue Bedrohungen aus dem Cyber- und Informationsraum – die Bundeswehr stellt sich modern und schlagkräftig auf, in: Clausewitz Gesellschaft Jahrbuch 2016, S. 128 [128].

zu garantieren und zu bewahren.⁴ In der Sicherung der von außen bedrohten Souveränität liegt die „staatliche Urfunktion“ der Streitkräfte,⁵ denn „wo eine nach Innen und Außen sich selbst behauptende Staatsgewalt nicht gewollt wird, da entsteht und da besteht auch kein Staat“.⁶ Ihre Urfunktion nimmt die Bundeswehr nun auch im Cyberraum wahr und leistet damit „einen Beitrag zur gesamtstaatlichen Sicherheitsvorsorge“.⁷

Die Bundeswehr hat den Cyberraum militärisch erschlossen. Doch welche rechtlichen Rahmenbedingungen gelten für die Aufstellung, das Verhalten und die Gefahrenabwehr der Streitkräfte im Cyberraum? Diese Frage ist aus Sicht des Verfassungsrechts weitgehend ungeklärt. So heißt es in der strategischen Leitlinie Cyber-Verteidigung des Bundesministeriums der Verteidigung: „Technische Komplexität und Wechselwirkungen führen meist zu einer komplexen Rechtslage im Cyberraum. Der rechtlichen Beratung kommt somit eine besondere Bedeutung zu. Entsprechende juristische Fachexpertise ist auszubauen“.⁸ Demnach besteht das Ziel der vorliegenden Arbeit darin, einen Beitrag zur Einordnung des Kommandos Cyber- und Informationsraum in das Wehrverfassungsrecht zu liefern.

Doch sie bleibt nicht auf diesen Aspekt beschränkt. Die Aufstellung des Kommandos Cyber- und Informationsraum ist eine Reaktion auf die Gefahren, die durch den Cyberraum drohen: „Moderne Gesellschaften und Volkswirtschaften sind in hohem Maße auf die gesicherte und freie Nutzung des grenzenlosen Cyber- und Informationsraumes angewiesen. Durch die zunehmende digitale und informationsseitige Vernetzung von Staat, Wirtschaft und Gesellschaft sind diese jedoch auch für Angriffe im Cyber- und Informationsraum verwundbarer geworden“.⁹ Es ist unerlässlich, diese Verwundbarkeit in den Blick zu nehmen, wird doch inzwischen beinahe wöchentlich über neue Cyberangriffe mit teils weitreichenden Folgen berichtet. Angreifer

⁴ F. Kirchhof, Verteidigung und Bundeswehr, in: HBStR IV, 3. Aufl. 2006, § 84, Rn. 2; K. Stern, Staatsrecht II, 1980, S. 852; vgl. auch E.-W. Böckenförde, Die Organisationsgewalt im Bereich der Bundesregierung, 1964, S. 155; Bundesministerium der Verteidigung (Hrsg.), Abschlussbericht Aufbaustab Cyber- und Informationsraum, S. 5; Die Bundesregierung (Hrsg.), Weißbuch 2016, S. 89 ff.

⁵ K. Stern, Staatsrecht II, 1980, S. 844; vgl. auch O. Depenheuer, in: Maunz/Dürig GG, 93. EL. 2020, Art. 87a, Rn. 8.

⁶ H. Heller, Staatslehre, 4. unveränd. Aufl. 1970, S. 202.

⁷ Bundesministerium der Verteidigung (Hrsg.), Strategische Leitlinie Cyber-Verteidigung im Geschäftsbereich BMVg, 2015 (unveröffentlicht); Bundesministerium der Verteidigung (Hrsg.), Abschlussbericht Aufbaustab Cyber- und Informationsraum, 2016, S. 5.

⁸ Bundesministerium der Verteidigung (Hrsg.), Strategische Leitlinie Cyber-Verteidigung im Geschäftsbereich BMVg, 2015 (unveröffentlicht).

⁹ Bundesministerium der Verteidigung (Hrsg.), Abschlussbericht Aufbaustab Cyber- und Informationsraum, 2016, S. 3.

beeinflussen Wahlen,¹⁰ zerstören Urananreicherungsanlagen,¹¹ schneiden Banken vom europäischen Zahlungssystem ab,¹² stören Krankenhäuser¹³ sowie die Stromversorgung in ihrer Funktionsfähigkeit,¹⁴ bedrohen den Weltmarkt¹⁵, spähen staatliche Institutionen aus¹⁶ oder attackieren in kriegerischen Auseinandersetzungen Kommunikationsinfrastrukturen.¹⁷ Eine Liste, die sich beliebig erweitern lässt. Schwerwiegende Angriffe sind der Bundesrepublik Deutschland bisher erspart geblieben. Sicherheit für die Zukunft bietet dies jedoch keinesfalls. So betont auch die Cyber-Sicherheitsstrategie des Bundesministeriums des Innern, dass Cyberangriffe „weite Bereiche des öffentlichen und privaten Lebens zum Erliegen bringen“ oder die „Funktionsfähigkeit von Verwaltung, Streitkräften und Sicherheitsbehörden erheblich beeinträchtigen und damit Auswirkungen auf die öffentliche Sicherheit und Ordnung in Deutschland haben“ können.¹⁸ Doch welche Handlungsmöglichkeiten und -befugnisse hat der Staat, um auf Gefahren zu reagieren, sollte sich eine solche exzeptionelle Lage durch Ausnutzung der Verwundbarkeit im Cyberraum ergeben? Die Antwort darauf könnte im Notstandsrecht liegen. Dieses sieht besondere Reaktionsmöglichkeiten für Situationen vor, die sich mit Mitteln der Normallage nicht mehr bewältigen lassen. Auch die

¹⁰ heise online, CIA, FBI und NSA: Putin ließ US-Wahl durch Hacker beeinflussen, vom 7. Januar 2017, abrufbar unter <https://www.heise.de/newsticker/meldung/CIA-FBI-und-NSA-Putin-liess-US-Wahl-durch-Hacker-beeinflussen-3590722.html>.

¹¹ Spiegel Online, Stuxnet-Virus könnte tausend Uran-Zentrifugen zerstört haben, vom 26. Dezember 2010, abrufbar unter <http://www.spiegel.de/netzwelt/netzpolitik/angriff-auf-irans-atomprogramm-stuxnet-virus-koennte-tausend-uran-zentrifugen-zerstoert-haben-a-736604.html>; dazu auch S.-H. Schulze, Cyber-„War“ – Testfall der Staatenverantwortlichkeit, Diss. 2015, S. 16 f.

¹² S. Aust/T. Amman, Digitale Diktatur, 2016, S. 324.

¹³ WELT Online, Weltweite „Wanna-Decryptor“-Attacke legt britische Krankenhäuser lahm, vom 12. Mai 2017, abrufbar unter <https://www.welt.de/politik/ausland/article164521094/Weltweite-Wanna-Decryptor-Attacke-legt-britische-Krankenhaeuser-lahm.html>.

¹⁴ Zeit Online, Malware führt zum Blackout, vom 5. Januar 2016, abrufbar unter <http://www.zeit.de/digital/internet/2016-01/stromausfall-hacker-ukraine-blackenergy>.

¹⁵ heise online, Nach NotPetya-Angriff: Weltkonzern Maersk arbeitete zehn Tage analog, vom 26. Januar 2018, abrufbar unter <https://www.heise.de/newsticker/meldung/Nach-NotPetya-Angriff-Weltkonzern-Maersk-arbeitete-zehn-Tage-lang-analog-3952112.html>.

¹⁶ F.A.S., Cyber-Attacke war gezielter Angriff auf das Auswärtige Amt, vom 3. März 2018, abrufbar unter <http://www.faz.net/aktuell/politik/inland/hacker-angriff-war-gezielter-angriff-auf-das-auswaertige-amt-15476826.html>.

¹⁷ MIT Technology Review, Russia hacked an American satellite company one hour before the Ukraine invasion, vom 10. Mai 2022, abrufbar unter <https://www.technologyreview.com/2022/05/10/1051973/russia-hack-viasat-satellite-ukraine-invasion/>.

¹⁸ Bundesministerium des Innern (Hrsg.), Cyber-Sicherheitsstrategie 2016, S. 7.