

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 Informationsraum	69
(1) Betrieb und Schutz streitkräfteeigener Informationsinfrastrukturen	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 Parlaments- vorbehalt	193
1. Die Dogmatik des wehrverfassungsrechtlichen Parlamentsvorbehalts	194
a) Die Rechtsgrundlagen des wehrverfassungsrechtlichen Parla- mentsvorbehalts	194
b) Die Teleologie des wehrverfassungsrechtlichen Parlamentsvorbe- halts	196
aa) Kompensationsfunktion	196
bb) Friedenssicherung und Schutz der Soldaten	198
2. Die Anwendung des wehrverfassungsrechtlichen Parlamentsvorbe- halts auf Operationen der Streitkräfte im Cyberraum	199
a) Anwendungsvoraussetzungen	199
b) Ausnahme bei Gefahr im Verzug	201
3. Anpassung des wehrverfassungsrechtlichen Parlamentsvorbehalts 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 Not-	
standsbefugnisse	243
cc) Zusammenfassende Erwägungen	245
b) Voraussetzungen und Ermächtigungsumfang der ungeschriebe-	
nen 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 Grundlagenversor-	
gung	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 Cybernot-	
stand	267
(2) Keine vorrangige Zuständigkeit der Länder	268
bb) Einsatz der Streitkräfte und der Bundespolizei	269
cc) Einwirkungsmöglichkeit auf die Betreiber kritischer Infra-	
strukturen	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