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.

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

Inhaltsverzeichnis

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
BGBl.	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 Kritischwer 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 Artikel 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 nichtstaatliche 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 Aufbaustab 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 Krankenhäuser[13] sowie die Stromversorgung in ihrer Funktionsfähigkeit,[14] bedrohen den Welthandel[15], spähen staatliche Institutionen aus[16] 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.