Das Recht der inneren und äußeren Sicherheit

Band 26

Verfassungsrechtliche Grundlagen für Cyberoperationen der Streitkräfte

Von

Thomas Hintzen

Duncker & Humblot · Berlin

THOMAS HINTZEN

Verfassungsrechtliche Grundlagen für Cyberoperationen der Streitkräfte

Das Recht der inneren und äußeren Sicherheit

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

Band 26

Verfassungsrechtliche Grundlagen für Cyberoperationen der Streitkräfte

Von

Thomas Hintzen

Duncker & Humblot · Berlin

Die Rechtswissenschaftliche Fakultät
der Christian-Albrechts-Universität zu Kiel hat diese Arbeit
im Jahre 2023 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 978-3-428-19078-2 (Print)
ISBN 978-3-428-59078-0 (E-Book)

Gedruckt auf alterungsbeständigem (säurefreiem) Papier
entsprechend ISO 9706 ♾

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

Vorwort

Die vorliegende Arbeit wurde im Januar 2023 von der juristischen Fakultät der Christian-Albrechts-Universität zu Kiel als Dissertation angenommen. Tag des Rigorosums war der 30. August 2023. Rechtsprechung und Literatur wurden bis einschließlich September 2023 eingearbeitet.

An erster Stelle bedanke ich mich ganz herzlich bei meinem Doktorvater Herrn Professor Dr. Sebastian Graf von Kielmansegg für die herausragende Betreuung und die wertvollen Anregungen. Auf Fragen antwortete er mir stets zuverlässig, umfassend und innerhalb kürzester Zeit. Durch seine wertvollen Ratschläge hat er maßgeblich zum erfolgreichen Abschluss dieser Arbeit beigetragen.

Herrn Professor Dr. Christoph Brüning danke ich für die rasche Erstellung des Zweitgutachtens. Für die unkomplizierte Aufnahme der Arbeit in die Schriftenreihe „Das Recht der inneren und äußeren Sicherheit“ danke ich Herrn Professor Dr. Dr. Markus Thiel.

Bedanken möchte ich mich ferner bei der Studienstiftung des deutschen Volkes, die mich sowohl als Student als auch während meiner Doktorandenzeit mit einem Stipendium unterstützte. Die finanzielle Förderung ermöglichte mir die nötige geistige Freiheit, um mein Dissertationsvorhaben zügig zu beenden. Der fachliche und akademische Austausch mit den anderen Stipendiaten im Rahmen der ideellen Förderung war für mich eine enorme persönliche Bereicherung.

Weiterer Dank gebührt meiner Freundin Jessica Gallander, meiner Schwester Christina Hintzen und meinem Bruder Stephan Baur, weil sie mir bei meinem Vorhaben den Rücken gestärkt haben und ich mich immer auf sie verlassen kann.

Abschließend möchte ich mich besonders bei meinen Eltern Claudia und Hubert Hintzen dafür bedanken, dass sie mich auf meinem bisherigen Lebensweg stets mit so viel Hingabe und Engagement unterstützt haben. Ohne ihren starken Rückhalt wären meine akademische Laufbahn und die Fertigstellung dieser Dissertation nicht möglich gewesen. Aus diesem Grund widme ich Ihnen diese Arbeit.

Düsseldorf, im September 2023 *Thomas Hintzen*

Inhaltsverzeichnis

Kapitel 3

Kapitel 4

Kapitel 6

Abkürzungsverzeichnis

a. A.	andere Ansicht
ABl.	Amtsblatt der Europäischen Union
Abs.	Absatz
ACM	Association for Computing Machinery
ACT	Allied Command Transformation
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
a. F.	alte Fassung
AFLR	Air Force Law Review
A.F.L. Rev.	Air Force Law Review
AFS	Armed Forces & Society
AGS	Alliance Ground Surveillance
a.i.	ad interim
AIVD	Algemene Inlichtingen- en Veiligheidsdienst
AK	Avtomat Kalaschnikowa
AöR	Archiv des öffentlichen Rechts
APARNET	Advanced Research Projects Agency Network
Army Law.	Army Lawyer
Art.	Artikel
ASPJ	Air and Space Power Journal
ATP	Advanced Persistent Threat
AU Press	Air University Press
AVR	Archiv des Völkerrechts
AWACS	Airborne Early Warning & Control System
Az.	Aktenzeichen
BAE Systems	British Aerospace Electronic Systems
BAKS	Bundesakademie für Sicherheitspolitik
BayVBl.	Bayrische Verwaltungsblätter
BBC	British Broadcasting Corporation
BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
BC-Waffen	Biologische und Chemische Waffen
Begr.	Begründer
BfV	Bundesamt für Verfassungsschutz

BGBl.	Bundesgesetzblatt
BKA	Bundeskriminalamt
BMI	Bundesministerium des Innern und für Heimat
BMVg	Bundesministerium der Verteidigung
BND	Bundesnachrichtendienst
BR	Bundesrat
BRJ	Bonner Rechtsjournal
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Bundesamt für Sicherheit in der Informationstechnik Gesetz
BT-Drucks.	Drucksache des Deutschen Bundestages
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungen des Bundesverfassungsgerichts
BVerfGG	Bundesverfassungsgerichtsgesetz
BVerwG	Bundesverwaltungsgericht
BVerwGE	Entscheidungen des Bundesverwaltungsgerichts
CCDCOE	NATO Cooperative Cyber Defence Centre of Excellence
CDU	Christlich Demokratische Union
CEO	Chief Executive Officer
CIO	Chief Information Officer
CIR	Cyber- und Informationsraum
CISO	Chief Information Security Officer
CJTL	Columbia Law Journal of Transnational Law
CMS	Critical Military Studies
CNO	Computernetzwerkoperation
COE	Centres of Excellence
COVID-19	Coronavirus Disease 2019
CQISS	China Quarterly of International Strategic Studies
CR	Computer und Recht
CSU	Christlich-Soziale Union
DDoS	Distributed Denial of Service
d. h.	das heißt
DNC	Democratic National Committee
Doc.	Document
DoD	Department of Defense
DoS	Denial of Service
DÖV	Die öffentliche Verwaltung
Drucks.	Drucksache

DS	Der Sachverständige
DVBl.	Deutsches Verwaltungsblatt
ENISA	European Network and Information Security Agency
ESIL	European Society of International Law
EU	Europäische Union
EU CyCLES	EU Cyber Crisis Linking Exercise on Solidarity
EuR	Zeitschrift Europarecht
EUV	Vertrag über die Europäische Union
EuZW	Europäische Zeitschrift für Wirtschaftsrecht
e. V.	eingetragener Verein
f.	folgende
FAQ	Frequently Asked Questions
FAZ	Frankfurter Allgemeine Zeitung
FDP	Freie Demokratische Partei
ff.	fortfolgende
FG	Finanzgericht
FIfF	Forum Informatiker:innen für Frieden und gesellschaftliche Verantwortung
Fn.	Fußnote
FR	Frankfurter Rundschau
GA	UN Generel Assembly
GASP	Gemeinsame Außen- und Sicherheitspolitik der Europäischen Union
GG	Grundgesetz
GGE	Group of Governmental Experts
GIZ	Deutsche Gesellschaft für Internationale Zusammenarbeit
GJIA	Georgetown Journal of International Affairs
GJIL	Georgetown Journal of International Law
GMBl	Gemeinsames Ministerialblatt
GOBT	Geschäftsordnung des Deutschen Bundestages
GPS	Global Positioning System
GRCh	Charta der Grundrechte der Europäischen Union
GSVP	Gemeinsame Sicherheits- und Verteidigungspolitik
GSZ	Zeitschrift für das Gesamte Sicherheitsrecht
HFR	Humboldt Forum Recht
Hrsg.	Herausgeber
HuV-I	Humanitäres Völkerrecht – Informationsschriften
IAEO	Internationale Atomenergie-Organisation

IANA	Internet Assigned Numbers Authority
ICANN	Cooperation for Assigned Names and Numbers
ICJ	International Court of Justice
ICT	Information and Communications Technologies
IGH	Internationaler Gerichtshof
InfoOP	Informationsoperation
IP	Internet Protocol
IS	Islamischer Staat
i. S. d.	im Sinne des
ISF	Information Systems Frontiers
ISIS	Islamischer Staat im Irak und Syrien
ISR	Intelligence, Surveillance and Reconnaissance
IT	Informationstechnik/Informationstechnologie
i. V. m.	in Verbindung mit
JA	Juristische Arbeitsblätter
JCCJ	Journal of Contemporary Criminal Justice
JCR	Journal of Conflict Resolution
JCSL	Journal of Conflict and Security Law
JNCA	Journal of Network and Computer Applications
JR	Juristische Rundschau
JSS	Journal of Strategic Security
JURA	Juristische Ausbildung
JuS	Juristische Schulung
JuWissBlog	Junge Wissenschaft im öffentlichen Recht – Blog
JZ	JuristenZeitung
Kfz	Kraftfahrzeug
KrWaffKontrG	Gesetz über die Kontrolle von Kriegswaffen
KSK	Kommando Spezialkräfte
Ls.	Leitsatz
LTO	Legal Tribune Online
LuftSiG	Luftsicherheitsgesetz
MAD	Militärischer Abschirmdienst
MADG	Militärischer Abschirmdienst Gesetz
MMR	MultiMedia und Recht
MüKo	Münchener Kommentar
m. w. N.	mit weiteren Nachweisen
NATO	North Atlantic Treaty Organization
NCAZ	Nationales Cyber-Abwehrzentrum

NDR	Norddeutscher Rundfunk
n. F.	neue Fassung
NJW	Neue Juristische Wochenzeitschrift
NMRZ	Nürnberger Menschenrechtszentrum
No.	Numero
NPT	Non-Proliferation Treaty
NVwZ	Neue Zeitschrift für Verwaltungsrecht
NZWehrr	Neue Zeitschrift für Wehrrecht
NZZ	Neue Züricher Zeitung
OEWG	Open-Ended Working Group
OK	Online-Kommentar
OSZE	Organisation für Sicherheit und Zusammenarbeit in Europa
OVCW	Organisation für das Verbot chemischer Waffen
ParlBG	Gesetz über die parlamentarische Beteiligung bei der Entscheidung über den Einsatz bewaffneter Streitkräfte im Ausland
PESCO	Permanent Structured Cooperation – Ständige Strukturierte Zusammenarbeit gemäß Art. 42 Abs. 6, Art. 46 EUV
Rn.	Randnummer
S.	Seite
SAR	Synthetic Aperture Radar
Sci Eng Ethics	Science and Engineering Ethics
sog.	sogenannte
SoldatenG	Soldatengesetz
SPD	Sozialdemokratische Partei Deutschlands
S/RES	Resolution des Sicherheitsrates
SSQ	Strategic Studies Quarterly
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
SWP	Stiftung Wissenschaft und Politik
SWR	Südwestrundfunk
Taz	Die Tageszeitung
TCP	Transmission Control Protocol
u. a.	unter anderem
UAbs.	Unterabsatz
UAS	Unmanned Aircraft Systems
UdSSR	Sowjetrepubliken
UN	United Nations
USA	United States of America

USB	Universal Serial Bus
UZwG	Gesetz über den unmittelbaren Zwang bei Ausübung öffentlicher Gewalt durch Vollzugsbeamte des Bundes
UZwGBw	Gesetz über die Anwendung unmittelbaren Zwanges und die Ausübung besonderer Befugnisse durch Soldaten der Bundeswehr und verbündeter Streitkräfte sowie zivile Wachpersonen
v.	von
VerfEU	Verfassung der EU
vgl.	vergleiche
VJTL	Vanderbilt Journal of Transnational Law
VMBl	Ministerialblatt des Bundesministeriums der Verteidigung
VN	Vereinte Nationen
Vorb.	Vorbemerkungen
VwVfG	Verwaltungsverfahrensgesetz
WD	Wissenschaftliche Dienste des Deutschen Bundestages
WDR	Westdeutscher Rundfunk
WEU	Westeuropäische Union
Wi-Fi	Wireless Fidelity
WiWo	Wirtschaftswoche
WRV	Weimarer Reichsverfassung
ZaöRV	Zeitschrift für ausländisches öffentliches Recht
z. B.	zum Beispiel
ZG	Zeitschrift für Gesetzgebung
ZöR	Zeitschrift für öffentliches Recht
ZP	Zusatzprotokoll
ZParl	Zeitschrift für Parlamentsfragen
ZRP	Zeitschrift für Rechtspolitik
ZSE	Zeitschrift für Staats- und Europawissenschaften
Zusatzprotokoll I	Zusatzprotokoll zu den Genfer Abkommen vom 12. August 1949 über den Schutz der Opfer internationaler bewaffneter Konflikte

„Wir haben als Bundesverteidigungsministerium und als Bundeswehr frühzeitig erkannt, dass der Cyber- und Informationsraum eine Dimension auch mit militärischer Relevanz ist, in der und für die wir uns entsprechend aufstellen müssen."[1]

Kapitel 1

Einführung, Forschungsstand und Gang der Untersuchung

Im Zuge der fortschreitenden Digitalisierung hat sich die Bundesrepublik Deutschland in den letzten Jahren grundlegend verändert. Neue Möglichkeiten der Kommunikation und Vernetzung führen zu mehr sozialer Interaktion, neuen Geschäftsbereichen sowie neuen Forschungsfeldern. Vernetzte elektronische Geräte prägen dabei immer stärker das Leben der Menschen. Fast alle relevanten Vorgänge werden heutzutage auf informationstechnischem Wege und insbesondere über das Internet getätigt.[2] Diese Entwicklung wurde durch die COVID-19-Pandemie zusätzlich beschleunigt.[3]

Die wachsende digitale Vernetzung hat aber nicht nur positive Auswirkungen auf Gesellschaft, Staat und Wirtschaft. Mit der steigenden Abhängigkeit von digitalen Infrastrukturen wächst auch deren Verwundbarkeit im Cyber- und Informationsraum.[4] Beinahe wöchentlich werden Netze der deutschen Verwaltung von staatlichen und nicht-staatlichen Akteuren angegriffen.[5] Den bislang größten Erfolg hatte ein solcher Angriff auf das Intranet des Bundestages im Jahr 2015. Über Monate hinweg haben Hacker dieses Netzwerk

---

[1] Generalleutnant *Michael Vetter*, Abteilungsleiter Cyber- und Informationstechnik und CIO im Bundesministerium der Verteidigung, https://background.tagesspiegel.de/cybersecurity/wir-muessen-die-hemmschwelle-wieder-hoeher-legen (diese sowie alle im weiteren Verlauf dieser Untersuchung zitierten Internet-Fundstellen wurden zuletzt am 01.01.2023 abgerufen).

[2] *Schulze*, Cyber-„War" – Testfall der Staatenverantwortlichkeit, S. 2.

[3] *BMI*, Cybersicherheitsstrategie für Deutschland, 2021, S. 8, 24.

[4] *Kurz/Rieger*, Cyberwar – Die Gefahr aus dem Netz, S. 7; https://crisis-prevention.de/kommunikation-it/neue-bedrohungen-aus-dem-cyber-informationsraum.html.

[5] https://www.lto.de/recht/nachrichten/n/hackback-cyber-gegen-angriff-abwehr-bnd-bfv-mad-geheimdienste-bundeswehr/.

infiltriert und konnten dadurch hochsensible Daten erlangen.[6] Darüber hinaus war der Landkreis Anhalt-Bitterfeld im Juli 2021 das Ziel einer umfassenden Cyberattacke. Im Rahmen dieses Angriffs wurden mehrere Server des Landkreises mit einer Ransomware infiziert, die zahlreiche Daten verschlüsselte.[7] Die Täter erklärten sich nur gegen die Zahlung eines Lösegeldes bereit, die Daten wieder freizugeben.[8] Der Landrat verweigerte dies und rief daraufhin den Katastrophenfall aus, weil die Verwaltung nahezu lahmgelegt war.[9]

Die Folgen von Cyberangriffen beschränken sich inzwischen nicht mehr allein auf den Cyber- und Informationsraum, sondern sie wirken auch in die analoge Welt hinein. Solche Angriffe können die Funktionsfähigkeit von Verwaltung, Streitkräften und zivilen Sicherheitsbehörden erheblich beeinträchtigen und damit die öffentliche Sicherheit und Ordnung in Deutschland nachhaltig gefährden.[10] Im Extremfall können sie sogar kritische Infrastrukturen lahmlegen und zerstören.[11] In diesem Szenario wäre mit erheblichen Personenschäden und sogar mit Todesopfern zu rechnen. Die Angriffe werden dabei stets komplexer und professioneller.[12]

Zwar fand bisher noch kein Krieg i. S. d. Völkerrechts statt, der sich ausschließlich auf Maßnahmen im Cyber- und Informationsraum beschränkte.[13] Allerdings werden Cyberoperationen immer häufiger als begleitende Maßnahme innerhalb eines mit konventionellen Waffen geführten zwischenstaatlichen Konflikts eingesetzt und sind damit Teil einer hybriden Kriegsführung geworden.[14]

So zeigte sich der flankierende Einsatz von Cyberoperationen zuletzt beim russischen Angriffskrieg auf die Ukraine. Bevor die russischen Bodentruppen am 24. Februar 2022 mit der Invasion begannen, führte Russland bereits einige Tage zuvor Cyberangriffe gegen kritische Infrastrukturen der Ukraine

---

6 https://taz.de/Cyberangriff-auf-den-Bundestag-2015/!5682997/.

7 Zu den technischen Hintergründen und das Vorgehen der Erpresser bei einer Ransomware siehe unten Kapitel 2 A. III. 2.

8 https://www.zeit.de/news/2021-08/27/bundeswehr-beendet-amtshilfe-nach-cyberangriff?utm_referrer=https%3A%2F%2Fwww.google.com%2F.

9 https://www.wiwo.de/politik/deutschland/hackerangriff-erste-cyber-katastrophenfall-in-deutschland-landkreis-lahmgelegt/27409940.html.

10 *BSI*, Die Lage der IT-Sicherheit in Deutschland, 2018, S. 10.

11 *Bundesregierung*, Weißbuch zur Sicherheitspolitik und zur Zukunft der Bundeswehr, 2016, S. 37; https://www.industry-of-things.de/kritische-nationale-infrastruktur-in-gefahr-a-841461/.

12 *BSI*, Die Lage der IT-Sicherheit in Deutschland, 2021, S. 88.

13 *Dornbusch*, Das Kampfführungsrecht im internationalen Cyberkrieg, S. 19 f.

14 *BMVg*, Abschlussbericht Aufbaustab Cyber- und Informationsraum, S. 13; *Spies-Otto*, in: Hornung/Schallbruch, IT-Sicherheitsrecht, § 19 Rn. 1 f.; https://www.deutschlandfunk.de/cyberangriffe-russland-ukraine-putin-kreml-100.html.

durch und legte die Homepage des ukrainischen Parlaments sowie der Regierung lahm. Infolgedessen waren die Webseiten für die Bürger über mehrere Stunden nicht erreichbar.[15] Auch während des Krieges führt Russland regelmäßige Cyberangriffe gegen Stromnetzwerke durch, um Schäden in der zivilen Bevölkerung anzurichten.[16]

Zeitgleich mit dem russischen Einmarsch erfolgte außerdem ein gezielter Cyberangriff auf das Satellitennetzwerk KA-SAT, das die ukrainischen Sicherheitskräfte unter anderem für die Kommunikation verwenden.[17] Dieser Cyberangriff war auch in anderen Ländern zu spüren, weil die Satelliten weltweit für Kommunikation im zivilen Bereich genutzt werden. So verwendet beispielsweise der deutsche Windkraftanlagenhersteller Enecron das Satellitennetzwerk zur Überwachung und Fernsteuerung seiner Windparks.[18] Aufgrund des Cyberangriffs fielen am 24. Februar 2022 die Satellitenverbindungen bei über 5.800 Anlagen in ganz Zentraleuropa aus, was zu massiven Störungen führte.[19]

Ein ähnliches Vorgehen seitens Russlands konnte bereits 2008 im Rahmen der militärischen Auseinandersetzung mit Georgien beobachtet werden.[20] Die damalige russische Invasion wurde ebenfalls von koordinierten und massiven DDoS-Attacken[21] auf die Webseiten von Regierung, Nachrichtenwesen und Banken von Georgien begleitet.[22] Teilweise wurde es der georgischen Regierung unmöglich gemacht, Informationen über den stattfindenden Konflikt sowohl mit der eigenen Bevölkerung als auch mit der internationalen Gemeinschaft zu teilen.[23] Durch die Nichterreichbarkeit der Homepages der

---

15 https://www.zeit.de/politik/ausland/2022-02/russland-hackerangriffe-ukraine-krieg-westen.

16 https://www.tagesschau.de/investigativ/swr/cyberkrieg-ukraine-101.html.

17 https://www.nzz.ch/technologie/ein-cyberangriff-legte-zu-beginn-der-invasion-die-kommunikation-der-ukraine-lahm-er-verursacht-kollateralschaeden-in-ganz-europa-ld.1675044.

18 https://www.ndr.de/nachrichten/niedersachsen/Nach-Cyberangriff-Stoerung-bei-Windkraft-Fernwartung-behoben,windkraftanlagen124.html.

19 https://www.handelsblatt.com/unternehmen/energie/erneuerbare-energien-massive-stoerung-der-satellitenverbindung-enercon-meldet-fast-6000-betroffene-windanlagen/28114360.html.

20 Siehe dazu umfassend *Keber/Roguski*, AVR 2011, 399 (402).

21 Für eine umfassende Definition und den Ablauf eines DDoS-Angriffs siehe unten Kapitel 2 B. V. 2.

22 *Dornbusch*, Das Kampfführungsrecht im internationalen Cyberkrieg, S. 33.

23 Der Grund dafür war, dass die georgische Internetanbindung fast ausnahmslos von Russland und der Türkei abhing. Nahezu alle der sich dort befindenden Router, welche die Datenpakete nach Georgien weiterleiteten, wurden mit Anfragen derart überflutet, dass von Georgien aus keine Daten mehr in andere Länder übertragen werden konnten. Auf diese Weise wurde auch das Senden von E-Mails ins Ausland