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

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

Kapitel 3

Die Verwendung der Streitkräfte zur Verteidigung im digitalen Raum 147

Kapitel 4

Inhalt und Ablauf der Verteidigung 273

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 2017[3] 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 abzugrenzen, 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).