Dokumentation

Cyberoperationen der Bundeswehr

Cyberoperationen der Bundeswehr

Aktenzeichen:	WD 2 - 3000 - 012/22
Abschluss der Arbeit:	25. Februar 2022 (zugleich letzter Zugriff auf Internetlinks)
Fachbereich:	WD 2: Auswärtiges, Völkerrecht, wirtschaftliche Zusammenarbeit und Entwicklung, Verteidigung, Menschenrechte und humanitäre Hilfe

Inhaltsverzeichnis

1. Cyberrelevante Dokumente

Die Federführung im Bereich von **Cybersicherheit und Cyberabwehr** obliegt dem **Bundesinnenministerium (BMI),** insb. dem **Bundesamt für Sicherheit in der Informationstechnik (BSI)**. Die Bundeswehr wirkt nur in bestimmten Fällen an der gesamtstaatlichen Cyberverteidigung mit.[1] Zu den zentralen Dokumenten für Cyberaktivitäten der Bundeswehr gehören u.a. das **Weißbuch zur Sicherheitspolitik und zur Zukunft der Bundeswehr** (2016),[2] die **Konzeption der Bundeswehr** (2018)[3] sowie die **Strategische Leitlinie Cyber-Verteidigung** (2015).[4] Im August 2021 hat das BMI die **Cybersicherheitsstrategie für Deutschland 2021**[5] erlassen, die den strategischen Rahmen für das Handeln der Bundesregierung im Bereich der Cybersicherheit für die nächsten fünf Jahre abbildet.[6]

2. Speziell mit Cyberaktivitäten befasste Behörden der Bundeswehr

Das 2017 in Dienst gestellte **Kommando Cyber- und Informationsraum (KdoCIR)** ist das Führungskommando des Cyber- und Informationsraums, der als eigenständiger militärischer Organisationsbereich aufgestellt ist. Der Aufgabenbereich des Kommandos umfasst den Schutz der IT-Sicherheit der Bundeswehr im In- und Ausland sowie die Aufklärung im Cyber- und Informationsraum.[7]

---

1 *Matthias Schulze*, „Militärische Cyber-Operationen – Nutzen, Limitierungen und Lehren für Deutschland“, SWP-Studie 15, August 2020, S. 7, https://www.swp-berlin.org/publications/products/studien/2020S15_she_CyberOperationen.pdf.

2 „Weißbuch 2016 zur Sicherheitspolitik und zur Zukunft der Bundeswehr“, https://www.bmvg.de/resource/blob/13708/015be272f8c0098f1537a491676bfc31/weissbuch2016-barrierefrei-data.pdf; Kurzbericht zum Weißbuch 2016 unter https://www.bmvg.de/de/themen/dossiers/weissbuch.

3 BMV, Konzeption der Bundeswehr, 20. Juli 2018, https://www.bmvg.de/resource/blob/26544/9cedddf6df2f48ca87aa0e3ce2826348d/20180731-konzeption-der-bundeswehr-data.pdf.

4 Netzpolitik.org, „Geheime Cyber-Leitlinie, Verteidigungsministerium erlaubt Bundeswehr ‚Cyberwar‘ und offensive digitale Angriffe“, 30. Juli 2015, https://netzpolitik.org/2015/geheime-cyber-leitlinie-verteidigungsministerium-erlaubt-bundeswehr-cyberwar-und-offensive-digitale-angriffe/.

5 BMI, Cybersicherheitsstrategie für Deutschland 2021, August 2021, https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/09/cybersicherheitsstrategie-2021.pdf;jsessionid=1FF58003448900C2E8B74604953CABEE.1_cid364?__blob=publicationFile&v=1#page120.

6 Die Strategie basiert auf der Grundlage von vier übergreifenden Leitlinien, namentlich (1.) „Cybersicherheit als eine gemeinsame Aufgabe von Staat, Wirtschaft, Wissenschaft und Gesellschaft etablieren“, (2.) „Digitale Souveränität von Staat, Wirtschaft, Wissenschaft und Gesellschaft stärken“, (3.) „Digitalisierung sicher gestalten“ und (4.) „Ziele messbar und transparent ausgestalten“.

7 Nähere Informationen unter: https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum/auftrag.

Das **Militärische Nachrichtenwesen (MilNW)** ist eines der Führungsgrundgebiete der Bundeswehr. Zu den Aufgaben des MilNW gehören Nachrichtengewinnung, -verarbeitung und Aufklärung für die Streitkräfte im Auslandseinsatz.[8]

3. Rechtsgrundlagen für Bundeswehroperationen im Cyberraum

Im Gegensatz zum BND, der auf der Grundlage des sog. BND-Gesetzes arbeitet, operiert die **Bundeswehr im Cyberraum** nur auf Grundlage der **allgemeinen verfassungsrechtlichen Vorschriften für Bundeswehreinsätze**.[9] Eine einfachgesetzliche Regelung für Cyberoperationen der Bundeswehr existiert nicht.[10]

Auch für das MilNW bestehen keine einfachgesetzlichen Regelungen. Die verfassungsrechtlichen Grundlagen für das MilNV finden sich in Art. 87a Abs. 1 und 2 GG. Als integraler Bestandteil der Streitkräfte unterfällt das MilNW keinem speziellen Rechtsrahmen. Es unterliegt aber der parlamentarischen Kontrolle durch den Verteidigungsausschuss und die Wehrbeauftragte des Deutschen Bundestages.[11]

Cyberverteidigung (als Teil der Landesverteidigung) findet eine Rechtsgrundlage in Art. 87a Abs. 2 GG. Einsätze der Bundeswehr „zur Verteidigung" setzen einen **„bewaffneten Angriff"** i.S.d. Art. 51 VN-Charta voraus. Wann die Intensitätsschwelle zum „Cyberangriff" überschritten ist, wird in der Literatur seit langem diskutiert.

> „Neuartige Formen der **Kriegsführung im Cyber-Raum** (Cyber-Attacken, IT-Angriffe bzw. Computernetzwerk-Operationen), durch welche die Funktionsweise der zivilen und militärischen Informationseinrichtungen und Computernetzwerke eines Staates gezielt

---

8 Vgl. Antwort der Bundesregierung vom 25. Januar 2021 auf die Kleine Anfrage der Fraktion BÜNDNIS 90/ DIE GRÜNEN, „Rechtsgrundlage und Kontrolle des Militärischen Nachrichtenwesens der Bundeswehr", BT-Drs. 19/26114, https://dserver.bundestag.de/btd/19/261/1926114.pdf.
Marek Krüger, „Das Militärische Nachrichtenwesen der Bundeswehr", in: Europäische Sicherheit und Technik Nr. 6, 2. Juni 2019, S. 5861, https://esut.de/2019/06/fachbeitraege/streitkraefte-fachbeitraege/12921/das-militaerische-nachrichtenwesen-der-bundeswehr/.

9 Zur Einordnung der Durchführung von Cybermaßnahmen durch Militär oder Nachrichtendienste siehe auch: Gutachten der Wissenschaftlichen Dienste „Verfassungsmäßigkeit von sog. ‚Hackbacks' im Ausland" vom 8. Juni 2018, dort insb. S. 5, https://www.bundestag.de/resource/blob/560900/baf0bfb8f00a6814e125c8fce5e89009/wd-3-159-18-pdf-data.pdf.

10 Vgl. dazu näher die Antwort der Bundesregierung auf die Kleine Anfrage der FDP-Fraktion vom 5. November 2018, „Hackbacks als aktive digitale Gegenwehr", BT-Drs. 19/5472, S. 3, https://dserver.bundestag.de/btd/19/054/1905472.pdf.

11 Antwort der Bundesregierung vom 25. Januar 2021 auf die Kleine Anfrage der Fraktion BÜNDNIS 90/ DIE GRÜNEN, „Rechtsgrundlage und Kontrolle des Militärischen Nachrichtenwesens der Bundeswehr", BT-Drs. 19/26114, https://dserver.bundestag.de/btd/19/261/1926114.pdf (dort insb. Vorbemerkung der Bundesregierung und Frage 29).

> ge-/zerstört bzw. infiltriert werden soll (vgl. zB „Stuxnet"-Attacke auf das iranische Atomprogramm 2010), sind nach überwiegender Auffassung als „bewaffneter Angriff" zu qualifizieren, wenn sie mit Blick auf **Umfang und Wirkung** (scale and effects) dem Einsatz kinetischer Waffen und kriegerischen Handlungen gleichkommen, also den Tod vieler Menschen bzw. weitreichende physische Zerstörungen von Sachwerten nach sich ziehen (vgl. näher Dittmar, Angriffe auf Computernetzwerke, 2005, 153 f.; Zielkowski HuV-I 2008, 202 (206); Heintschel v. Heinegg in Schmidt-Radefeldt/Meissler, Automatisierung und Digitalisierung des Krieges, 2012, 159 (162 f.); Schmitt, Tallinn Manual 2.0 on the international law applicable to cyber operations, 2017, 339; Knoll, Streitkräfteeinsatz zur Verteidigung gegen Cyberangriffe, 2020). Die **bloß vorübergehende Beeinträchtigung der Funktionsfähigkeit** (Neutralisierung) ziviler Infrastruktur bzw. Zerstörung von Daten dürfte dagegen regelmäßig unterhalb der Schwelle zum bewaffneten Angriff bleiben (tendenziell weiter Döge AVR 2010, 486 (492)). Ebenso verhält es sich mit **Computernetzwerk-Operationen gegen Telekommunikationseinrichtungen** (sog. Denial-of-Service-Attacks) oder gegen das Banken- und Finanzsystem, was regelmäßig (nur) der Ausübung wirtschaftlichen Zwangs gleichkommt (Krieger AVR 2012, 1, 10)."[12]

Nur ein Bruchteil der **offensiven militärischen Cyberoperationen (OMCO)** der Bundeswehr erfüllt die Merkmale einer „Einbeziehung in bewaffnete Unternehmungen", was eine Zustimmungspflicht des Bundestages für entsprechende Auslandsoperationen der Bundeswehr auslösen würde.[13] Obgleich die Trennung zwischen „Inland" und „Ausland" im Cyberraum schwerfällt, unterscheidet *Marxsen*[14] rechtlich zwischen **Cyberaktivitäten der Bundeswehr im Inland und bei Auslandseinsätzen.** Einen Überblick über das Spektrum an Cyberoperationen der Bundeswehr findet sich auch in einem **Arbeitspapier der Bundesakademie für Sicherheitspolitik**.[15]

3.1. Auslandseinsätze

Militärische Maßnahmen im Cyberraum unterliegen den gleichen rechtlichen Rahmenbedingungen wie andere militärische Operationen. Bewaffnete Einsätze der Streitkräfte außerhalb des Geltungsbereichs des Grundgesetzes unterliegen nach dem Parlamentsbeteiligungsgesetz grundsätzlich der vorherigen konstitutiven Zustimmung des Deutschen Bundestages. Im Rahmen von

---

12 BeckOK GG/*Schmidt-Radefeldt*, 49. Ed., Art. 115a Rn. 4 m.w.N. (als **ANLAGE**).
Ebenso Dürig/Herzog/Scholz/*Volker Epping*, 95. EL Juli 2021, GG Art. 115a Rn. 43-44;
v. Mangoldt/Klein/Starck/*Rainer Grote*, 7. Aufl. 2018, GG Art. 115a Rn. 17.

13 *Matthias Schulze*, „Militärische Cyber-Operationen – Nutzen, Limitierungen und Lehren für Deutschland", SWP-Studie 15, August 2020, S. 8, https://www.swp-berlin.org/publications/products/studien/2020S15_she_CyberOperationen.pdf.

14 *Christian Marxsen*, JZ 2017, S. 543 ff., https://www.mohrsiebeck.com/artikel/verfassungsrechtliche-regeln-fuer-cyberoperationen-der-bundeswehr-aktuelle-herausforderungen-fuer-einsatzbegriff-und-parlamentsvorbehalt-101628002268817x14845739077254?no_cache=1 (als **ANLAGE**).

15 Bundesakademie für Sicherheitspolitik, BAKS-Arbeitspapier, *Carolin Busch,* „Von Firewall bis Hackback: Das Spektrum militärischer Cyberoperationen", 1/2020, https://www.baks.bund.de/sites/baks010/files/arbeitspapier_sicherheitspolitik_2020_1.pdf (als **ANLAGE**).

Auslandseinsätzen kann die Bundeswehr im Einklang mit dem jeweiligen **Bundestagsmandat** auch Cyberoperationen vornehmen. Als verfassungs- und völkerrechtliche Grundlage rekurriert das Bundestagsmandat in der Regel auf Art. 24 Abs. 2 GG i.V.m. dem jeweiligen VN-Sicherheitsratsmandat. Bei Auslandseinsätzen kann es auf der Basis des Amtshilfegrundsatzes (Art. 35 Abs. 1 GG) zur Kooperation zwischen der Bundeswehr und dem BND kommen. Nach einem seitens der Bundesregierung nicht bestätigten Bericht aus dem September 2016 ist im Jahr 2015 die erste offensive *Cyber Network Operation* in Afghanistan durchgeführt worden.[16]

3.2. Einsatz der Bundeswehr im Inland

Im Inland sind Cyberoperationen der Bundeswehr nur in den **engen Grenzen der Verfassung**, d.h. im **Inneren Notstand** (Art. 87a Abs. 4 GG) oder im **Katastrophennotstand** (Art. 35 Abs. 2 und 3 GG) möglich, sofern dabei die Schwelle zu einem „Einsatz“ im Rechtssinne überschritten wird. Ansonsten bleibt nur die **Amtshilfe** (Art. 35 Abs. 1 GG). Eine Abgrenzung ist nicht immer trennscharf möglich.[17] Unterhalb der sog. „Einsatzschwelle“ erfolgen z.B. Maßnahmen der Bundeswehr zur Sicherung der eigenen IT-Infrastruktur.[18]

3.3. Völkerrecht im Cyberraum

Völkerrechtliche Regeln sind grundsätzlich auch im Cyberraum anwendbar. Die **Bundesregierung** hat dazu im März 2021 ein **Positionspapier** vorgelegt.[19] Das Positionspapier spiegelt allerdings nur die deutsche Sicht auf das Thema wieder; andere Staaten haben eigene, zum Teil abweichende Regelungen für Cyberoperationen ihrer Streitkräfte. Das Thema „Anwendung des Völkerrechts im Cyberraum“ ist bislang noch im Fluss. Es existiert **kein international verbindlicher Vertrag über militärische Cyberoperationen**. **Gewohnheitsrechtliche Regeln** werden sich nur langsam herausschälen; Vorarbeiten dazu leistet das „Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations“.[20]

***

---

16 Damals drangen Bundeswehrexperten der Einheit „Computer Netzwerk Operationen“ in die internen Computersysteme eines afghanischen Mobilfunkbetreibers ein, um Informationen über die Entführung einer Entwicklungshelferin zu beschaffen. Vgl. *Christian Marxsen*, JZ 2017, S. 543 ff., 549 (als **ANLAGE**).

17 Vgl. zum Ganzen *Schmidt-Radefeldt*, in: Kischel/Kielmansegg (Hrsg.) 2018, „Rechtsdurchsetzung mit militärischen Mitteln – Inlandseinsätze der Armee und Militarisierung der Polizei – Landesbericht Deutschland“, S. 1–55 (S. 25–26), https://www.mohrsiebeck.com/uploads/tx_sgpublisher/produkte/leseproben/9783161563720.pdf (als **ANLAGE**)

18 *Christian Marxsen*, JZ 2017, S. 543 ff., 546 (als **ANLAGE**).

19 „On the Application of International Law in Cyberspace”. Position Paper – March 2021, https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf.

20 Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge Univ. Press, 2. Aufl. 2017, https://www.cambridge.org/core/books/tallinn-manual-20-on-the-international-law-applicable-to-cyber-operations/E4FFD83EA790D7C4C3C28FC9CA2FB6C9.