Ethisch und einsatzfähig: Aufkommende und disruptive Technologien, die Bundeswehr und die Zeitenwende

Hagebölling, David; Barker, Tyson

Veröffentlichungsversion / Published Version
Sammelwerksbeitrag / collection article

Deutsche Gesellschaft für Auswärtige Politik e. V.

November 2022

DGAP BERICHT

Ethisch und einsatzfähig

Aufkommende und disruptive Technologien, die Bundeswehr und die Zeitenwende

Dr. David Hagebölling
Associate Fellow,
Programm Technologie
und Außenpolitik

Tyson Barker
Leiter, Programm
Technologie und
Außenpolitik

KAPITELÜBERSICHT

Zentrale Erkenntnisse

1 Deutschlands künftiger Beitrag zur Sicherheit Europas und seiner Verbündeten hängt davon ab, ob die Bundeswehr aufkommende und disruptive Technologien (Emerging and Disruptive Technologies, EDTs) wie künstliche Intelligenz, 5G/6G-Mobilfunktechnologie, Low Earth Orbit (LEO) Satelliten-Konnektivität sowie Quantencomputing und -kommunikation effektiv nutzen kann.

2 Selbst inmitten des russischen Angriffskriegs gegen die Ukraine bleibt Deutschland einem konzeptionellen, institutionellen und ethischen Silodenken verhaftet, das zu Entkopplungen zwischen dem Verteidigungs- und Technologiesektor ebenso wie zu Diskrepanzen mit seinen Verbündeten führt.

3 Damit Deutschland nicht nur die unmittelbaren militärischen Anforderungen erfüllen kann, sondern die Bundeswehr auch für zukünftige Einsätze gewappnet ist, sollte die Zeitenwende nicht nur eine Erhöhung des Verteidigungshaushalts bewirken, sondern auch die Basis für eine Vereinbarkeit von ethischen und militärischen Anforderungen an EDTs schaffen.

Einleitung

Der russische Angriffskrieg gegen die Ukraine hat Deutschland aufgerüttelt und dazu veranlasst, seine Verteidigungspolitik drastisch anzupassen. Nach jahrzehntelangem Stillstand füllt die Bundeswehr nun Lücken bei grundlegenden militärischen Fähigkeiten. Zudem setzt sich in der deutschen Politik zunehmend die Erkenntnis durch, dass eine stärkere Integration intelligenter Systeme, die organisatorische Ausrichtung an Hightech-Kriegsführung und die Verschmelzung von Cyber- und physischem Raum für die künftige Leistungsfähigkeit des deutschen Militärs von entscheidender Bedeutung sind.

Dennoch verharrt der deutsche politische Diskurs noch in einem konzeptionellen, institutionellen und ethischen Silodenken, das wenig Innovation zulässt und zu Entkopplungen zwischen dem Verteidigungs- und Technologiesektor ebenso wie zu Diskrepanzen zwischen Deutschland und seinen Verbündeten führt. Für die Modernisierung der deutschen Streitkräfte ist es von zentraler Bedeutung, dass ethische Bedenken mit (zukünftigen) Einsatzrealitäten abgeglichen werden und politische Entscheidungen der engen Verknüpfung zwischen Entwicklung und Nutzung militärischer und ziviler Technologien Rechnung tragen.

Status quo

Aufkommende und disruptive Technologien (Emerging and Disruptive Technologies, EDTs) wie künstliche Intelligenz, 5G/6G-Mobilfunktechnologie, Low Earth Orbit (LEO) Satelliten-Konnektivität sowie Quantencomputing und -kommunikation werden das Umfeld für Bundeswehr-Operationen nachhaltig verändern. Die Bundeswehr sieht die stärkere Integration von maschineller Intelligenz in militärische Operationen, insbesondere durch den massenhaften Einsatz unbemannter Systeme, als eine der zentralen Herausforderungen in diesem Jahrzehnt an.[1] Hochautomatisierte unbemannte Luftfahrtsysteme (Unmanned Aerial System, UAS) spielten in den jüngsten Konflikten wie dem Krieg um Bergkarabach eine wichtige Rolle.[2] Auch im Bereich der strategischen Planung und Vorausschau werden EDTs unverzichtbar, wo etwa KI-Algorithmen Erkenntnisse aus den von immer mehr Sensoren erzeugten Datenmengen gewinnen. Das Weltraumkommando der Bundeswehr setzt zum Beispiel bereits zwei Machine-Learning-Anwendungen bei der Erstellung von Lagebildern ein.[3]

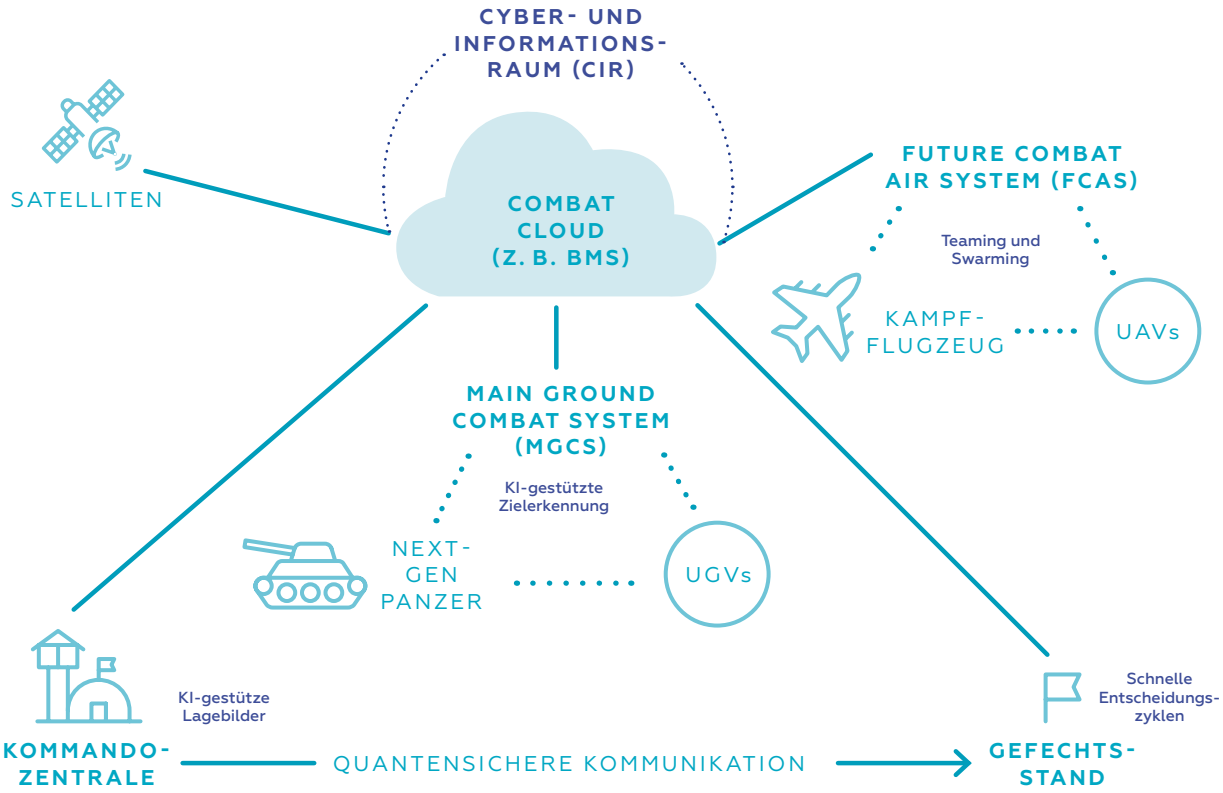
In diesem sich wandelnden Umfeld hängt die Fähigkeit der Bundeswehr, die Möglichkeiten von EDTs bei künftigen Einsätzen auszuschöpfen, entscheidend von der engen Kooperation mit Verbündeten Deutschlands in der EU und der NATO ab, und damit auch von

1 Kommando Heer, „Thesenpapier I: Wie kämpfen Landstreitkräfte künftig?“, Kommando Heer (2017) https://augengeradeaus.net/wp-content/uploads/2018/03/180327-Thesenpapier-I-Wie-ka%CC%88mpfen-LaSK-zuku%CC%88nftig.pdf (abgerufen am 18. Juli 2022).

2 Deutscher Bundestag, Zum Drohneneinsatz im Krieg um Bergkarabach im Jahre 2020, WD2-3000-113/20 (Januar 2021): https://www.bundestag.de/resource/blob/825428/5b868defc837911f17628d716e7e1e1d/WD-2-113-20-pdf-data.pdf (abgerufen am 31. Mai 2022).

3 BWI, „Künstliche Intelligenz: BWI entwickelt Lösungen für die Bundeswehr“ 24. Januar 2022: https://www.bwi.de/news-blog/blog/artikel/kuenstliche-intelligenz-bwi-entwickelt-loesungen-fuer-die-bundeswehr (abgerufen am 31. Mai 2022).

1 – WIE AUFKOMMENDE UND DISRUPTIVE TECHNOLOGIEN DIE KRIEGSFÜHRUNG VON MORGEN VERÄNDERN



Quelle: Darstellung der Autoren

der fortlaufenden Investition von politischem Kapital in gemeinsame Initiativen. Deutschlands derzeitige Bemühungen, EDTs zu nutzen, sind eng verbunden mit gemeinsamen europäischen Verteidigungsprojekten für zukünftige Kampfsysteme, darunter das Future Combat Air System (FCAS)[4] mit Frankreich und Spanien und das Main Ground Combat System (MGCS)[5] mit Frankreich. Beide Systeme werden voraussichtlich erst in den 2040er Jahren einsatzbereit sein, der Bundeswehr aber erweiterte Funktionen zur Verfügung stellen, zum Beispiel die tiefgreifende Integration in eine gemeinsame Combat Cloud und intelligente Mensch-Maschine-Kooperation.[6]

Das deutsche Verteidigungswesen sieht sich mit der Herausforderung konfrontiert, sich organisatorisch auf die High-Tech-Kriegsführung vorzubereiten. Konflikte werden zunehmend in Maschinengeschwindigkeit ausgetragen, was eine schnellere Entscheidungsfindung an der Front erfordert. Dies bedarf dezentraler Kommandostrukturen mit hochvernetzten Einheiten in der Bundeswehr. Die Bundeswehr führt auch deshalb ein Battle Management System (BMS) ein – ein neues digitales Führungssystem, das den Zugriff auf Echtzeitinformationen und somit eine digital vernetzte Kampfführung ermöglicht.[7] Sie möchte das BMS bis

4 Airbus, „Future Combat Air System (FCAS)": https://www.airbus.com/en/products-services/defence/multi-domain-superiority/future-combat-air-system-fcas (abgerufen am 31. Mai 2022) .

5 Hensoldt, „MGCS – The Smart Tank is Rolling in" (April 2021): https://www.hensoldt.net/stories/mgcs/ (abgerufen am 31. Mai, 2022).

6 „FCAS-Anforderungen festgelegt", FlugRevue, 31. August 2021: https://www.flugrevue.de/militaer/industrie-muss-sich-einigen-fcas-anforderungen-festgelegt/ (abgerufen am 31. Mai 2022); André Uzulis, „MGCS – Ein neues Kampfsystem für das Heer", *.loyal das Magazin*, (1. April 1, 2021): https://www.reservistenverband.de/magazin-loyal/mgcs-ein-neues-kampfsystem-fuer-das-heer/ (abgerufen am 31. Mai 2022).

7 Das BMS basiert auf der SitaWare-Softwarefamilie, die von vielen NATO-Partnern verwendet wird. Bundeswehr, „Battle Management System – CIR digitalisiert": https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum/auftrag/digitalisieren/gefechtsfuehrung-der-zukunft-das-battle-management-system (abgerufen am 31. Mai 2022).

2023 einsatzbereit machen, sobald sie Führungsverantwortung in der Very High Readiness Joint Task Force der NATO übernimmt.[8]

Die Bundesregierung hat außerdem wichtige Schritte unternommen, um sich auf die Verschmelzung von Cyber- und physischem Raum vorzubereiten, die mit aktuellen verteidigungstechnologischen Entwicklungen einhergeht. So hat Deutschland beispielsweise sein Netzwerk an Cyber-Institutionen erheblich ausgebaut und eine hohe Position in Ranglisten nationaler Cyber-Fähigkeiten errungen.[9] Mit der zunehmenden Nutzung digitaler Technologien in Systemen und Kommandostrukturen hat die Bundeswehr ihre Ressourcen in einem eigenen militärischen Organisationsbereich, dem Cyber- und Informationsraum (CIR), gebündelt.[10] Zudem baut das Bundesministerium der Verteidigung seine Fähigkeiten im Bereich sicherer Quantenkommunikationsnetze aus, unter anderem durch ein spezielles Labor in seinem Forschungsinstitut für Cybersicherheit, CODE.[11] Dieses Labor entwickelt MuQuaNet, einen Prototypen eines solchen Netzes.[12]

Gerade weil die Bundeswehr mit einer potenziellen militärischen Eskalation im Cyberraum umgehen muss, gewinnen auch ethische Bedenken an Relevanz. KI kann beispielsweise zur Automatisierung von Cyberaktivitäten eingesetzt werden, was einen größeren Umfang und eine höhere Häufigkeit von Cyberangriffen ermöglicht.[13] Außerdem könnte sie die Risikobereitschaft steigern, da Abwehrtechniken möglicherweise langsamer entwickelt und skaliert werden können als offensive Techniken.[14] Gleichzeitig ist die Zuordnung von Cyberangriffen kompliziert und zeitaufwändig.[15] Die Bundeswehr könnte sich beispielsweise gezwungen sehen, auf der Grundlage von uneindeutigen Informationen über Verantwortung oder Absicht (wie z. B. Spionage vs. Sabotage) gegen einen vermeintlichen böswilligen (staatlichen oder nichtstaatlichen) Akteur vorzugehen.[16] Während KI und andere EDTs die Risiken im Cyberraum erhöhen, befindet sich Deutschland noch im Prozess zur Entwicklung einer kohärenten und angemessene Antwort auf diese Herausforderungen.

Die Zusammenarbeit zwischen dem Verteidigungs- und Technologiesektor sowie die organisationale Anpassung der Bundeswehr stellen nach wie vor große Herausforderungen dar. Die erheblichen ethischen Bedenken der deutschen Gesellschaft hinsichtlich der Reduzierung menschlicher Beteiligung und Verantwortung durch die Nutzung von EDTs erschwert dies ebenfalls. Die Bundeswehr ist sich dieser Bedenken bewusst und versucht, sie mit realen Bedingungen auf dem Kampffeld, Kommandostrukturen und Entscheidungsprozessen in Einklang zu bringen. Ein Beispiel hierfür ist die explizite Abbildung ethisch-rechtlicher Implikationen in der KI-gestützten Simulationsumgebung „GhostPlay“.[17] Gleichzeitig kann die Abweichung Deutschlands von der robusteren und pragmatischeren Herangehensweise seiner Bündnispartner an Dual-Use EDTs, also EDTs mit doppeltem Verwendungszweck, die gemeinsame Planung – und insbesondere die Bestimmung der technischen Merkmale – von gemeinsamen Verteidigungsprojekten wie FCAS, die die Nutzung fortschrittlicher maschineller Intelligenz beinhalten, erschweren.

8 Bundeswehr, “Digitalisierung im Heer“: https://www.bundeswehr.de/de/organisation/heer/organisation/faehigkeiten/digitalisierung (abgerufen am 31. Mai 2022).

9 Z. B. Julia Voo, „National Cyber Power Index 2020. Methodology and Analytical Considerations“, China Cyber Policy Initiative/Belfer Center for Science and International Affairs (September 2020): https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf (abgerufen am 31. Mai 2022); Internationale Fernmeldeunion (ITU), „Global Cybersecurity Index 2020,“ (2022): https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E (abgerufen am 31. Mai 2022).

10 Bundeswehr Cyber- und Informationsraum: https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum (abgerufen am 31. Mai 2022).

11 Universität der Bundeswehr München, „CODE – Über Uns“: https://www.unibw.de/code/im-profil/ziele (abgerufen am 28. Juni 2022).

12 Universität der Bundeswehr München, „Q-Lab“: https://www.unibw.de/code/forschung/zentrallabore/q-lab (abgerufen am 31. Mai 2022).

13 James Johnson, Eleanor Krabill, „AI, Cyberspace, and Nuclear Weapons“, *War on the Rocks*, 31. Januar 2020: https://warontherocks.com/2020/01/ai-cyberspace-and-nuclear-weapons/ (abgerufen am 31. Mai 2022)

14 Garfinkel and Allan Dafoe, „Artificial Intelligence, Foresight, and the Offense-Defense Balance“, *War on the Rocks*, 19. Dezember 2019: https://warontherocks.com/2019/12/artificial-intelligence-foresight-and-the-offense-defense-balance/ (abgerufen am 31. Mai 2022).

15 Deutscher Bundestag, „Anwendbarkeit des humanitären Völkerrechts auf Computernetzwerkoperationen und digitale Kriegsführung, WD2-3000-038/15, (Februar 2015), S. 12–13: https://www.bundestag.de/resource/blob/406028/de1946480e133cf38bbee41d8d3d6898/WD-2-038-15-pdf-data.pdf (abgerufen am 31. Mai 2022).

16 James M. Action, „Cyber Warfare & Inadvertent Escalation“, *Daedalus* Nr. 149, Ausgabe 2 (April 2020), S. 133–149: https://direct.mit.edu/daed/article/149/2/133/27317/Cyber-Warfare-amp-Inadvertent-Escalation (abgerufen am 31. Mai 2022); Diese Ambivalenz ist vor allem dann problematisch, wenn verschiedene militärische Fähigkeiten in cyber-physischen Systemen verwoben sind. Die Entdeckung von Malware in Raketenfrühwarnsystemen könnte beispielsweise als Vorbereitung für einen nuklearen Erstangriff interpretiert werden, auch wenn mit der gegnerischen Intrusion eine Schwächung der konventionellen ballistischen Raketenabwehr beabsichtigt ist. James M. Acton, „Why is Nuclear Entanglement So Dangerous?“ Carnegie Endowment for International Peace (23. Januar 2019): https://carnegieendowment.org/2019/01/23/why-is-nuclear-entanglement-so-dangerous-pub-78136 (abgerufen am 31. Mai 2022).

17 Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr (dtec.bw), „GhostPlay – Simulation für KI-basierte Entscheidungsverfahren“: https://dtecbw.de/home/forschung/hsu/projekt-ghostplay (abgerufen am 31. Mai 2022).

Aktueller politischer Ansatz

Mit der Ankündigung einer sicherheits- und verteidigungspolitischen Zeitenwende durch den Bundeskanzler im Februar 2022[18] soll der jahrelange Sparkurs des deutschen Militärs umgekehrt werden. Doch das zugewiesene Sondervermögen in Höhe von 100 Milliarden Euro deckt kaum den Grundbedarf der Bundeswehr. Deutschland ist auf einen weitaus systematischeren haushaltspolitischen – und ethisch-kulturellen – Wandel angewiesen, wenn es über diesen Grundbedarf hinausgehen und sich auf zukünftige Anforderungen einstellen möchte. Zunächst muss die Bundesregierung eine einheitliche Vision für den Einsatz von EDTs in der Bundeswehr entwickeln.

Im 20. Jahrhundert wurden die Kernkraft und die Tarnkappentechnik, ja sogar das Internet, für militärische Zwecke entwickelt. Zivile Nutzungsmöglichkeiten folgten dem. Inzwischen hat sich dieser Trend umgekehrt: Zivile Technologien entwickeln sich zu einer zentralen Dimension militärischer Leistungsfähigkeit. Das Weißbuch (2016) zur Sicherheitspolitik und Zukunft der Bundeswehr[19] und das jüngste Positionspapier (2021) zur Zukunft der Bundeswehr[20] gehen jedoch kaum auf das disruptive Potenzial von Technologien ein, die in erster Linie von zivilen Innovationen angetrieben werden, darunter KI, Quantencomputing und 5G/6G-Konnektivität.[21]

Zudem zeigen Deutschlands wichtigste technologiepolitischen Papiere, dass die Bundesregierung selbst bei Technologien mit eindeutigem Dual-Use-Potenzial weiterhin eine künstliche Trennung zwischen ziviler und militärischer Sphäre beibehält, sowohl hinsichtlich Entwicklung als auch Regulierung. Die deutsche Hightech-Strategie 2025 (2018)[22] und die Industriestrategie 2030 (2019)[23] befassen sich mit volkswirtschaftlichen Dimensionen, verteidigungspolitische Aspekte kommen in der Hightech-Strategie jedoch überhaupt nicht und in der Industriestrategie nur am Rande vor. Das trifft auch auf die deutsche KI-Strategie (2017, 2020)[24] und 5G-Strategie (2017) zu.[25] In der deutschen Cyberstrategie (2021)[26] wird die Cybersicherheit in erster Linie aus der zivilen Perspektive der Strafverfolgung und der Justiz betrachtet.[27]

Die isolierte Betrachtung dieser Technologien im militärischen Kontext spiegelt die Dynamik schwieriger ethischer Debatten in Deutschland wider. Die politische Haltung des Landes zu militärischen Technologien war bislang überwiegend reaktiv, risikoscheu und von gesellschaftlichen Kontroversen geprägt. Mit der Entscheidung für die Bewaffnung der Heron-Drohne im April 2022[28] beendete die Bundesregierung eine fast zehnjährige Diskussion,[29] in der Begriffe wie unbemannte und autonome Systeme häufig fälschlicherweise als Substitute verwendet

18 Die Bundesregierung, „Regierungserklärung von Bundeskanzler Scholz am 27. Februar 2022“: https://www.bundesregierung.de/breg-de/suche/regierungserklaerung-von-bundeskanzler-olaf-scholz-am-27-februar-2022-2008356 (abgerufen am 31. Mai 2022).

19 Die Bundesregierung, „Weißbuch 2016 zur Sicherheitspolitik und zur Zukunft der Bundeswehr“, (13. Juli 2016): https://www.bundeswehr.de/resource/blob/4800140/fe103a80d8576b2cd7a135a5a8a86dde/download-white-paper-2016-data.pdf (abgerufen am 31. Mai 2022).

20 Bundesministerium der Verteidigung, „Positionspapier – Gedanken zur Bundeswehr der Zukunft (9. Februar 2021): https://augengeradeaus.net/wp-content/uploads/2021/02/20210209_AKK_GI_Bundeswehr_der_Zukunft.pdf (abgerufen am 31. Mai 2022).

21 Dies spiegelt sich auch darin wider, dass in dem 143-seitigen Weißbuch fast keine direkten Verweise auf EDTs mit doppeltem Verwendungszweck enthalten sind (künstliche Intelligenz: 1 Verweis; 5G oder 6G: 0 Verweise; Quantentechnologie: 0 Verweise).

22 Verweise auf Sicherheitsherausforderungen beschränken sich auf die zivile (IT-)Sicherheit. Bundesregierung, „Forschung und Innovation für die Menschen: Die High-Tech Strategie 2025“, (September 2018): https://www.hightech-strategie.de/SharedDocs/Publikationen/de/hightech/pdf/forschung-und-innovation-fuer-die-menschen.pdf?__blob=publicationFile&v=4 (abgerufen am 19. Juni 2022).

23 Bundesministerium für Wirtschaft und Energie (BMWi), „Made in Germany: Die Industriestrategie 2030“ (November 2019): https://www.bmwi.de/Redaktion/DE/Dossier/industriestrategie-2030.html (abgerufen am 31. Mai 2022).

24 Die Bundesregierung, „Nationale Strategie für Künstliche Intelligenz“: https://www.ki-strategie-deutschland.de/home.html (abgerufen am 31. Mai 2022).

25 Bundesregierung, „5G-Strategie für Deutschland“ (Juli 2017): https://www.bmvi.de/blaetterkatalog/catalogs/350336/pdf/complete.pdf (abgerufen am 31. Mai 2022).

26 Bundesministerium des Innern und für Heimat, „Cybersicherheitsstrategie für Deutschland 2021“, (August 2021): https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/09/cybersicherheitsstrategie-2021.pdf;jsessionid=1ABEA4EB553C692E35A59577B182FCC4.2_cid287?__blob=publicationFile&v=1 (abgerufen am 31. Mai 2022).

27 Themen wie Desinformationskampagnen und Cyberkriminalität stehen im Vordergrund.

28 Bundesministerium der Verteidigung, „Weg frei zur Bewaffnung der Drohne Heron TP mit Präzisionsmunition“, (6. April 2022): https://www.bmvg.de/de/aktuelles/bewaffnung-der-heron-tp-drohnen-mit-praezisionsmunition-5389376 (abgerufen am 31. Mai 2022).

29 Nina Werkhäuser, „No armed drones for the German army — for now“, Deutsche Welle, 4. Dezember 2020: https://www.dw.com/en/no-armed-drones-for-the-german-army-for-now/a-55936615 (abgerufen am 31. Mai 2022).

2 – DIE TRENNUNG ZIVILER UND MILITÄRISCHER SPHÄREN IN DEUTSCHLANDS WACHSENDEM ÖKOSYSTEM VON INNOVATIONS-INSTITUTIONEN

INSTITUTION	GRÜNDUNG	FÖRDERUNG	BEREICH	PRIORITÄTEN
INNOVATIONS-INSTITUTIONEN IM SICHERHEITS- UND VERTEIDIGUNGSBEREICH				
Cyber Innovation Hub (CyberHub)	2017	€ 200 Mio. 2019–2023	Verteidigung (BMVg)	Förderung Soldatinnen- und Soldaten-zentrierter digitaler Innovationen, einschließlich KI- und Virtual Reality-Anwendungen; Funktion als Schnittstelle zwischen der Bundes-wehr und dem Start-up-Ökosystem
Agentur für Innovation in der Cybersicherheit (Cyberagentur)	2020	€ 350 Mio. 2020–2023	Sicherheit/ Verteidigung (BMVg und BMI)	Unterstützung ehrgeiziger und innovativer FuE auf dem Gebiet der Cybersicherheit, auch in angrenzenden Bereichen wie Mensch-Technik-Interaktion und KI
Zentrum für Digitalisierungs- & Technologieforschung der Bundeswehr (dtec.bw)	2020	€ 500 Mio. 2020–2024	Verteidigung (BMVg)	Bündelung von Forschung der Bundeswehr zu kritischen und neuen Technologien; Förderung der Forschungskooperation mit Wirt-schaft, Verwaltung und Gesellschaft
INNOVATIONS-INSTITUTIONEN IM ZIVILEN BEREICH				
Bundesagentur für Sprunginnovation (SPRIND)	2019	≈€ 1 Mrd. 2019–2029	Zivil (BMBF und BMWK)	Unterstützung disruptiver Innovationen, u.a. in den Bereichen optische Prozessoren, Mikrooptik und Augmented Reality
Deutsche Agentur für Transfer und Innovation (DATI)	2022 (geplant)	€ 15 Mio. Startfinan-zierung	Zivil (BMBF)	Förderung technischer Innovationen, insbesondere an Fachhochschulen; Verstärkung der Zusammenarbeit mit Start-ups, KMUs sowie öffentlichen Einrichtungen
Sovereign Tech Fund (STF)	2022 (geplant)	€ 3,5 Mio. jährlich	Zivil (BMWK, Open Knowledge Foundation)	Unterstützung des Open-Source-Software-Ökosystems; Erhöhung der Sicherheit von grundlegenden Inter-nettechnologien; Verbesserung von Interoperabilität und Stärkung der digitalen Souveränität

Quelle: Eigene Darstellung

wurden.[30] Gleichzeitig schließt Deutschland den Einsatz von vollautonomen Drohnen weiterhin aus und gehört zu den entschiedensten Befürwortern eines völkerrechtlichen Verbots solcher Systeme.[31]

Die jüngsten Bemühungen, die Wettbewerbsfähigkeit in der Verteidigungstechnologie zu stärken, bedeuten einen Bruch mit der üblichen Praxis, künstliche Grenzen zwischen militärischer und ziviler Sphäre zu ziehen. Das Strategiepapier der Bundesregierung aus dem Jahr 2020 zur Stärkung der Sicherheits- und Verteidigungsindustrie[32] verdeutlicht die zunehmende Bedeutung von ziviler Forschung und Entwicklung (FuE) als treibende Kraft für militärische EDT-Anwendungen.[33] Deutschland hat in den vergangenen fünf Jahren auch beträchtliche Summen in neue Institutionen investiert, deren Aufgabe es ist, Forschung und Innovation im Verteidigungsbereich zu fördern (siehe Tabelle).

Dennoch ist die Kluft zwischen ziviler und militärischer FuE in Deutschland nach wie vor größer als in verbündeten Staaten wie Frankreich, dem Vereinigten Königreich und den USA. Obwohl die US-amerikanische Defense Advanced Research Projects Agency im deutschen politischen Diskurs häufig erwähnt wird, hält die deutsche Regierung an einer klaren Trennung zwischen ihren eigenen neuen Innovationsinstitutionen im Sicherheits- und Verteidigungsbereich und der zivilen Innovationsagentur SPRIND fest.[34] Außerdem ist es vielsagend, dass die Unterstützung des Bundesministeriums für Verteidigung für Hochschulforschung bei derzeit rund 50 Millionen Euro jährlich stagniert.[35]

Schwierigkeit, seine umfangreichen FuE-Tätigkeiten zu EDTs für das Verteidigungswesen zu nutzen, untergräbt seine Bemühungen, zu einem zukunftsfähigen europäischen Verteidigungssektor beizutragen. Die Debatte über die militärische Nutzung von EDTs auf EU-Ebene ist zukunftsorientiert, aber es besteht dennoch weiterhin eine Umsetzungslücke. Der von der deutschen EU-Ratspräsidentschaft 2020 initiierte Strategische Kompass der EU (2022)[36] unterstreicht die zentrale Bedeutung einer starken gemeinsamen technologisch-industriellen Basis Europas. Die industrielle Fragmentierung entlang nationaler Grenzen behindert jedoch weiterhin die stärkere Skalierung von Verteidigungstechnologie und damit verbundene Vorteile.

Auch gelingt es den EU-Mitgliedstaaten nicht, ausreichende Ressourcen zu mobilisieren. Der „Koordinierte Jahresbericht zur Verteidigung“ (CARD, Coordinated Annual Review on Defence) der EU aus dem Jahr 2020 warnt davor, dass der Verteidigungstechnologie unzureichende Mittel zugewiesen werden.[37] Initiativen wie der Europäische Verteidigungsfonds (European Defence Fund, EDF), die disruptive Technologien fördern, sind wichtige Schritte zur Stärkung verteidigungsbezogener Forschung.[38] Der ursprünglich für den Zeitraum 2021 bis 2027 vorgesehene EDF-Haushalt in Höhe von 13 Milliarden Euro wurde jedoch um fast die Hälfte auf 8 Milliarden Euro gekürzt.[39] Zudem halten sich lediglich zwei EU-Mitgliedstaaten an die Vereinbarung, zwei Prozent ihres Verteidigungshaushalts in Forschung und Technologie zu investieren.[40]

Angesichts dieser Einschränkungen bleibt die Koordinierung der EU mit der umfangreichen Arbeit der NATO im Bereich der EDTs ein zentraler Bestandteil der deutschen Politik. Im Mittelpunkt des Strategischen Konzepts 2030 der NATO stehen

30 Während autonome Systeme in der Lage sind, bis zu einem gewissen Grad unabhängig von menschlichen Bedienenden zu agieren, bezieht sich der Begriff „unbemannte Systeme“ lediglich auf die fehlende physische Präsenz menschlicher Bedienenden (z. B. Fernsteuerung).

31 Bundesregierung „Rede der Bundesministerin der Verteidigung, Dr. Ursula von der Leyen, in der Aktuellen Stunde zum Beschaffungsprogramm von Drohnen für die Bundeswehr vor dem Deutschen Bundestag am 2. Juli 2014 in Berlin“, (2. Juli 2014): https://www.bundesregierung.de/breg-de/service/bulletin/rede-der-bundesministerin-der-verteidigung-dr-ursula-von-der-leyen--793046 (abgerufen am 31. Mai 2022).

32 Bundesregierung, „Strategiepapier der Bundesregierung zur Stärkung der Sicherheits- und Verteidigungsindustrie“ (Februar 2020): https://www.bmwk.de/Redaktion/DE/Downloads/S-T/strategiepapier-staerkung-sicherits-und-verteidigungsindustrie.pdf?__blob=publicationFile&v=4 (abgerufen am 31. Mai 2022).

33 Das Strategiepapier hebt die strategische Bedeutung von Sicherheit und Verteidigung in der allgemeinen Technologie- und Industriepolitik hervor und bezeichnet den Transfer von (grundlegenden) Forschungs- und Entwicklungsergebnissen in beschaffungsfähige Sicherheits- und Verteidigungsprodukte und -dienstleistungen als eine zentrale Herausforderung.

34 SPRIND, „Lernen Sie SPRIND kennen“: https://www.sprind.org/en/we/ (abgerufen am 31. Mai 2022).

35 Die Finanzierung belief sich 2017 auf 42 Mio. Euro, 2018 auf 63 Mio. Euro und 2019 auf 53 Mio. Euro. Armin Himmelrath, „Unis erhalten weniger Geld vom Verteidigungsministerium“, *Spiegel Online*, 15. Juni 2021: https://www.spiegel.de/panorama/bildung/ruestungsforschung-unis-erhalten-weniger-geld-vom-verteidigungsministerium-a-0bec8b22-6269-4224-b620-a689b085fd43 (abgerufen am 31. Mai 2022).

36 European Union External Action Service (EEAS), „A Strategic Compass for Security and Defence“: https://eeas.europa.eu/headquarters/headquarters-homepage/106337/towards-strategic-compass_en (abgerufen am 31. Mai 2022).

37 European Defense Agency, „2020 CARD Report Executive Summary“ (2020), S. 7: https://eda.europa.eu/docs/default-source/reports/card-2020-executive-summary-report.pdf (abgerufen am 31. Mai 2022).

38 European Defence Fund, „Research on disruptive technologies for defence“, Europäische Kommission (2021): https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/edf-2021-open-rdis-open (abgerufen am 18. Juli 2022).

39 Europäische Kommission, „The EU budget powering the recovery plan for Europe. Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions“, COM(2020) 44 final (27. Mai 2020): https://ec.europa.eu/info/sites/default/files/about_the_european_commission/eu_budget/1_en_act_part1_v9.pdf (abgerufen am 31. Mai 2022).

40 European Defence Agency, „Defence Data 2019-2020. Key findings and analysis“ (2021), S. 12–13: https://eda.europa.eu/docs/default-source/brochures/eda---defence-data-report-2019-2020.pdf (abgerufen am 31. Mai 2022).

EDTs und die Widerstandsfähigkeit gegen Cyber-, weltraumbasierte und hybride Bedrohungen.[41] Die NATO-Verteidigungsminister haben im vergangenen Jahr zudem einen Strategieplan verabschiedet, der die Entwicklung von EDTs durch das Bündnis in sieben Kernbereichen leiten soll, darunter KI, Autonomie und Quantentechnologie.[42] Ferner treiben Deutschland und andere Mitgliedstaaten im Rahmen der NATO-Agenda 2030 ein transatlantisches Ökosystem für Verteidigungstechnologie und -industrie voran. Sie haben vereinbart, einen Defence Innovation Accelerator for the North Atlantic (DIANA)[43] zu etablieren und einen NATO-Innovationsfonds (NIF)[44] einzurichten, über den in den nächsten 15 Jahren mindestens eine Milliarde Euro investiert werden soll.[45]

Handlungs-empfehlungen

Die vom Bundeskanzler angekündigte Zeitenwende muss einen Ausgleich zwischen den ethischen Bedenken und militärischen Erfordernissen in Bezug auf EDTs in der Bundeswehr vorantreiben, wenn diese ein starker Pfeiler der europäischen Sicherheit sein soll. Um dies zu erreichen, sollte die Bundesregierung:

Zwei Prozent des 100-Milliarden-Euro-Sondervermögens für die Förderung disruptiver Verteidigungstechnologien bereitstellen. Die Bundesregierung sollte die Möglichkeit nutzen, mit dem Sondervermögen einen zukunftsfähigen verteidigungstechnologischen Sektor aufzubauen. Obwohl künftige Kampfsysteme wie das FCAS einen beträchtlichen Teil des 100-Milliarden-Euro-Budgets ausmachen, sind derzeit nur 422 Millionen Euro direkt für FuE im Bereich der EDTs, insbesondere für KI-Fähigkeiten, veranschlagt.[46] Die Bundesregierung sollte mindestens 2 Prozent des Sondervermögens für die Förderung disruptiver Verteidigungstechnologien bereitstellen, um Anreize für den Zufluss von Risikokapital in neue Start-ups im Verteidigungssektor und höhere FuE-Ausgaben etablierter deutscher Verteidigungsunternehmen zu setzen.

Die ethische Debatte über militärische Anwendungen von EDTs mit Einsatzrealitäten verbinden. In Deutschland werden Diskussionen rund um das Thema Ethik häufig stark abstrahiert von der Realität militärischer Einsätze geführt. Dabei sollten sich Diskussionen auf die Bestimmung eines angemessenen Maßes an maschineller Autonomie und die Festlegung von vertretbaren Zwecken für den Einsatz von EDTs konzentrieren. Denkbar wären interaktive Workshops, bei denen sich politische Entscheidungsträgerinnen und Entscheidungsträger und/oder Bürgerinnen und Bürger mit wahrscheinlichen Szenarien – zum Beispiel dem Einsatz von Drohnenschwärmen – befassen. Dies könnte die Diskussion über mögliche Gegenmaßnahmen fördern, einschließlich Methoden zur Auswahl von Zielobjekten, wenn die menschliche Reaktionszeit zu langsam ist.

Dual-Use Implikationen von EDTs mit innovationsorientierter Industriepolitik verknüpfen. Ministerien, die Innovations- und Industriepolitik gestalten, insbesondere das Bundesministerium für Digitales und Verkehr (BMDV), das Bundesministerium für Wirtschaft und Klimaschutz (BMWK) und das Bundesministerium für Bildung und Forschung (BMBF), sollten mit dem Bundesministerium der Verteidigung (BMVg) zusammenarbeiten, um das Dual-Use-Potenzial von EDTs wie KI und Quantum in ihren Strategien zu berücksichtigen. neue Nationale Sicherheitsstrategie sollte einen Abschnitt enthalten, der die technologie- und innovationsbezogene Industriepolitik, einschließlich ihrer für die Verteidigung relevanten Aspekte, zusammenführt – und zwar im Rahmen einer regierungsübergreifenden Bewertung zentraler Bedrohungen für die nationale Sicherheit.

41 NATO, „Strategic Concepts" (29. November 2021): https://www.nato.int/cps/en/natohq/topics_56626.htm (abgerufen am 31. Mai 2022).

42 NATO, „Emerging and disruptive technologies", (7. April, 2022): https://www.nato.int/cps/en/natohq/topics_184303.htm (abgerufen am 31. Mai 2022).

43 Ziel des DIANA ist es, die Zusammenarbeit der Allianz im Bereich der EDTs zu fördern und weiterhin Interoperabilität zu gewährleisten. Er wird ein Accelerator-Programm für Start-ups anbieten, das Zugang zu vorqualifizierten Investoren bietet, und Testzentren in Europa und Nordamerika verbinden, um gemeinsam militärische EDT-Anwendungen zu entwickeln, zu validieren und zu testen. NATO, „Emerging and disruptive technologies", (7. April, 2022): https://www.nato.int/cps/en/natohq/topics_184303.htm (abgerufen am 31. Mai 2022).

44 NATO, „NATO Allies take the lead on the development of NATO's Innovation Fund", (22. Oktober 2021): https://www.nato.int/cps/en/natohq/news_187607.htm (abgerufen am 31. Mai 2022).

45 Vivienne Machi, „NATO hopes to launch new defense tech accelerator by 2023", Defense News, 22. Juni 2021: https://www.defensenews.com/global/europe/2021/06/22/nato-hopes-to-launch-new-defense-tech-accelerator-by-2023/ (abgerufen am 31. Mai 2022).

46 Bundesministerium der Verteidigung, „Ministerin: Wir sorgen für eine voll einsatzbereite Bundeswehr", (3. Juli 2022): https://www.bmvg.de/de/aktuelles/ministerin-wir-sorgen-fuer-voll-einsatzbereite-bundeswehr-5438596 (abgerufen am 14. August 2022).

Wissenstransfer zwischen militärischer und ziviler FuE verbessern. Zivile Forschung und Entwicklung im technologischen Bereich bestimmt zunehmend den militärischen Vorsprung. Dem sollte die Bundesregierung Rechnung tragen, indem sie das Münchner Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr (dtec.bw) stärker mit den bayerischen Hightech-Start-ups vernetzt. Die Regierung sollte eine separate Track-II-Plattform einrichten, die Innovatoren bei der Entdeckung von Dual-Use-Anwendungen von EDTs unterstützt, welche mit der Förderung von Innovationsagenturen wie SPRIND und dem Cyber Innovation Hub entwickelt werden. Außerdem sollte sie Anreize für deutsche und europäische Risikokapitalinvestitionen in Start-ups im Bereich der Verteidigungstechnologie setzen, etwa durch Ko-Finanzierungen.

Die Beschaffung von Verteidigungsgütern an technologische Innovationszyklen anpassen. Schwankungen im Verteidigungshaushalt erschweren die Unterstützung längerer EDT-Innovationszyklen. Die Regierung sollte einen bis 2030 laufenden Spezial-Fonds für disruptive Verteidigungstechnologien mit jährlichen Mindestbudgetgarantien einrichten. Der Verteidigungsausschuss des Bundestages sollte außerdem ein Mitglied benennen, das über die Projektergebnisse berichtet, die Debatte über Ausgaben für Verteidigungsinnovationen fördert und Möglichkeiten der Zusammenarbeit mit anderen Ausschüssen, einschließlich des Auswärtigen Ausschusses und des Ausschusses für Digitales, ermittelt.[47]

Die Interoperabilität mit Verbündeten durch gemeinsame Grundsätze und militärische Formationen aufrechterhalten. Die Bundesregierung muss sicherstellen, dass die EDT-bezogene Transformation der Bundeswehr nicht die Interoperabilität mit verbündeten Streitkräften untergräbt. Sie sollte die Entwicklung gemeinsamer ethischer Grundsätze und Verhaltenskodizes fördern, wie etwa in der KI-Strategie der NATO geschehen. Deutschland sollte auch die Einführung experimenteller Technologien in binationalen Verbänden und Einheiten (z. B. im Rahmen der Deutsch-Französischen Brigade oder des Deutsch-Niederländischen Korps) fördern und seine Rolle als Teilnehmer am Rahmennationenkonzept der NATO nutzen, um Testumgebungen für militärische Innovationen in multinationalen Formationen zu schaffen.

47 Für ein ähnliches Argument für einen „Defense Innovation and Experimentation Ambassador", siehe: Torben Schütz et al., "Beware of Potemkin: Germany's Defense Rethink Risks Reinforcing Old Habits", War on the Rocks, 11. April 2022: https://warontherocks.com/2022/04/beware-of-potemkin-germanys-defense-rethink-risks-reinforcing-old-habits (abgerufen am 31. Mai 2022).

DGAP

Advancing foreign policy. Since 1955.

Rauchstraße 17/18
10787 Berlin
Tel. +49 30 254231-0
info@dgap.org
www.dgap.org
@dgapev

Die Deutsche Gesellschaft für Auswärtige Politik e.V. (DGAP) forscht und berät zu aktuellen Themen der deutschen und europäischen Außenpolitik. Dieser Text spiegelt die Meinung der Autorinnen und Autoren wider, nicht die der DGAP.

Die DGAP ist gefördert vom Auswärtigen Amt aufgrund eines Beschlusses des Deutschen Bundestages.

Herausgeber
Deutsche Gesellschaft für
Auswärtige Politik e.V.

ISSN 2198-5936

Übersetzung executive english

Redaktion Jana Idris

Layout Luise Rombach

Design Konzept WeDo

Fotos Autorinnen und Autoren © DGAP