Krieg der Zukunft?!

Operative Herausforderungen des Multi-Domain Battlefield für die Bundeswehr

Hintergrundinformation Presse

Lehrgang Generalstabs-/Admiralstabsdienst (LGAN) 2020 – Studienphase

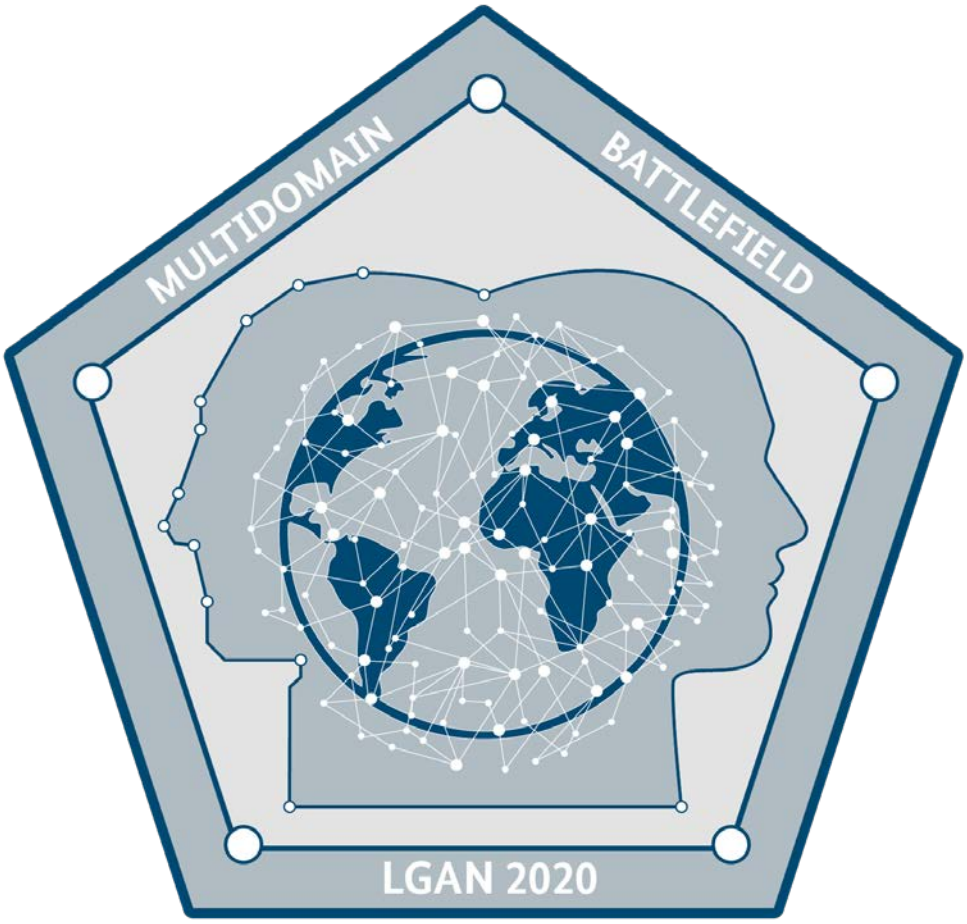
Diese Hintergrundinformation ist im Lehrgang Generalstabs-/Admiralstabsdienst National 2020 an der Führungsakademie der Bundeswehr entstanden.

Diese Hintergrundinformation gibt die Meinung der AutorInnen wieder und stellt nicht zwangsläufig den Standpunkt der Führungsakademie dar.

Redaktion: KKpt Alexander Heinrich und Oberstlt Michael Jappsen
Erscheinungsjahr: 2022

Führungsakademie der Bundeswehr
Manteuffelstraße 20 · 22587 Hamburg
Tel.: +49 (0)40 8667 0
https://www.bundeswehr.de/de/organisation/weitere-bmvg-dienststellen/fuehrungsakademie-der-bundeswehr

Lehrgang
Generalstabs-/Admiralstabsdienst 2020 –
Studienphase



Krieg der Zukunft?!

Operative Herausforderungen des Multi-Domain Battlefield für die Bundeswehr
Hintergrundinformation Presse

Lehrgang
Generalstabs-/Admiralstabsdienst 2020 –
Studienphase

Krieg der Zukunft?!

Operative Herausforderungen des Multi-Domain Battlefield für die Bundeswehr

Hintergrundinformation Presse

Inhalt

1 Einleitung – Auftrag 1
2 Wandel der Konfliktbilder 2
3 Methodik 3
4 Handlungsfelder für die Bundeswehr 4
4.1 Digitalisierung und Vernetzung – „Einfach mal machen“ 4
4.2 Multi-Domain-Effects – Flexibel und effizient 4
4.3 Resilienz – Verteidigung im Frieden 5
4.4 Siegfähigkeit – Vom Gegner her denken 6
4.5 Funktionale Robustheit – ganzheitlich denken 6
4.6 Innovation – Ermöglichen statt administrieren 7
5 Herausforderungen auf dem Gefechtsfeld der Zukunft 8
6 Wie wir bestehen – Zielbild 10

1 Einleitung – Auftrag

Das durch den Generalinspekteur festgelegte Thema der Studienphase der Lehrgangsteilnehmerinnen und -teilnehmer des 17. streitkräftegemeinsamen General- und Admiralstabslehrgang National (LGAN) lautet: „Krieg der Zukunft?! – Operative Herausforderungen des Multi-Domain Battlefield für die Bundeswehr“.

Das selbst definierte Ziel lautet dabei:

> *LGAN 2020 leitet kurz-, mittel- und langfristige operative Herausforderungen des Multi-Domain Battlefield für die Bundeswehr in einem Zeithorizont bis maximal in das Jahr 2045 aus möglichen Konfliktszenarien und in der Entwicklung befindlichen Technologien ab und erarbeitet konkrete Handlungsempfehlungen für den Geschäftsbereich des BMVg, die dazu beitragen, die Bundeswehr zukunftsfähig aufzustellen und zu verhindern, dass wesentliche Entwicklungen in ihrer Ausrichtung unberücksichtigt bleiben.*

Diese Hintergrundinformation informiert über die Herangehensweise im Rahmen der Erarbeitung der Studienphase und gibt einen Überblick über die wesentlichen Inhalte und Ergebnisse.

Dafür wird zunächst ein Blick auf das Multi-Domain Battlefield (MDB) geworfen und die Methodik der Studienphase kurz skizziert, um anschließend die Kernbotschaften aus insgesamt sechs identifizierten Handlungsfeldern darzustellen. Den Abschluss bildet ein Überblick über die, während der Studienphase aufgezeigten Problemstellungen des MDB und den als Zielbild formulierten Notwendigkeiten. Hieraus werden Lösungsideen mit konkreten Handlungsempfehlungen abgeleitet, um so eine siegfähige Bundeswehr für das Multi-Domain Battlefield zu schaffen.

2 Wandel der Konfliktbilder

Ein Blick in die Geschichtsbücher reicht aus, um festzustellen, dass Kriegs- und Konfliktbilder veränderlich sind. Die Gründe dafür sind vielfältig. Sicherheitspolitische Polaritäten können beispielsweise in Dynamik geraten, die Großmächte zu Stellvertreterkriegen oder zu direkter Konfrontation bewegen. Ausgeglichene Kräfteverhältnisse erlauben eine offene Auseinandersetzung, während Unterlegenheit die Asymmetrie von Kriegsführung befördert. In jüngster Vergangenheit sind es vor allem das Informationszeitalter, umfassende Technologiesprünge sowie das Erschließen neuer Dimensionen, die weitere Möglichkeiten der Kriegsführung eröffnen beziehungsweise neue Räume der Auseinandersetzung entstehen lassen.

Vor uns liegt demnach ein neuer, hoch technologisierter Kriegsschauplatz: das Multi-Domain Battlefield (MDB), welches die seit Jahrzehnten etablierte Konzentration auf die „klassischen“ Dimensionen Land, Luft und See mehr als nur herausfordert. Der Weltraum und der Cyberraum sind de facto bereits neue Gefechtsfelder. Dies hat zum einen zur Folge, dass wortwörtlich eine neue physische Sphäre mitgedacht werden muss. Zum anderen fördert die Nutzung des virtuellen Raums – verbunden mit den gesamtgesellschaftlichen Phänomenen eines Informations- und Digitalisierungszeitalters – neue Verwundbarkeiten und Ziele zu Tage. Unser Operationsraum ist damit komplexer geworden.

Wesentlicher Treiber dieses sich bereits vollziehenden Wandels, ist der zum Teil gar quantensprungartige technologische Fortschritt. Nur wer diesen mit seinen vielschichtigen Konsequenzen nachvollziehen, bewerten und nutzen kann, wird auf dem neuen Gefechtsfeld bestehen. Beispielweise verkürzen Digitalisierung und Künstliche Intelligenz Entscheidungsprozesse und beschleunigen so das Gefecht. Führungsfähigkeiten müssen daher nicht mehr nur erhalten bleiben, sondern leistungsfähiger und effizienter werden. Beim dafür notwendigen Rückgriff auf neueste Informationstechnik ist die Verwundbarkeit gegenüber Angriffen aus dem Cyberraum und elektromagnetischen Spektrum zu berücksichtigen. Systeme sind daher widerstandsfähiger, autonomer und möglichst autark zu konzipieren. Immer weiter reichende, schwer detektier- oder abwehrbare Waffensysteme sind als facettenreiche Herausforderung für die eigene Sicherheit, aber auch als Chance zu begreifen, das eigene Fähigkeitsspektrum zu erweitern. Teil- und Vollautonomie bieten darüber hinaus domänenübergreifend Möglichkeiten, um Streitkräfte auf dem MDB in vielerlei Hinsicht effizienter einzusetzen.

Es ist jedoch nicht nur das Militär, das sich auf diesen neuen Kriegsschauplatz vorzubereiten hat. Stattdessen sind auch gesamtstaatliche Ansätze notwendig, um einerseits als Nation gewappnet zu sein und andererseits die eigenen Streitkräfte in die Lage zu versetzen, ihrem verfassungsmäßigen Auftrag nachzukommen. So muss ein gesellschaftliches Bewusstsein von einem ganzheitlich ausgestalteten MDB geschaffen werden, auf dem eben nicht mehr nur die Streitkräfte im Fokus stehen, sondern auch die Zivilgesellschaft zum Ziel wird. Darüber hinaus braucht es mindestens einer national vernetzten Innovationsstrategie, um das erhebliche technologische Potential auch hinreichend ausschöpfen zu können. Und nicht zuletzt sind mit der Implementierung von Hochtechnologie mehr und mehr auch bundes- sowie völkerrechtliche Fragen verbunden, die für den nachhaltig legitimen Einsatz von Streitkräften sowie ihrer Mittel und Methoden zweifelsfrei durch eine Legislative zu beantworten sind.

Dennoch: zuallererst bleiben es die Streitkräfte, die das MDB verstehen und sich diesem anpassen müssen, um zukünftig siegfähig zu sein. Im Kern gilt es, alle operativen Dimensionen miteinander zu verbinden, die daraus erwachsenden eigenen Handlungsmöglichkeiten komplementär zur klassischen Gefechtsführung auszugestalten und in diese zu integrieren.

3 Methodik

Ausgangspunkt der Untersuchung waren die zentralen Begrifflichkeiten der Fragestellung. Dazu war zunächst zu klären, wie im Rahmen dieser Arbeit operative Herausforderungen[1] definiert werden und wie das MDB[2] zu verstehen ist. Insbesondere die Definition des MDB wurde in einem iterativen Prozess erarbeitet, da keine passende Definition vorlag.
Ein dritter wesentlicher Bestandteil der Arbeit war der Zukunftsaspekt. Um valide Szenare zu schaffen, wurden zwei Schritte zunächst getrennt voneinander durchgeführt. Eine Gruppe untersuchte eingehend aktuelle Technologieentwicklungen, während sich eine andere mit gesellschaftlichen und sicherheitspolitischen Trends auseinandersetze. Die Erkenntnisse beider Gruppen wurden anschließend zunächst in vier, später in drei Zukunftsszenarien zusammengefasst. Diese Szenare decken den Einsatz der Bundeswehr mit einer Bandbreite von Landes- und Bündnisverteidigung (LV/BV) über eine unterstützende Rolle im Rahmen eines ad hoc-Bündnisses bis hin zur Teilnahme an einem Szenar des Internationalen Krisen- und Konfliktmanagements (IKM) im Rahmen eines etablierten Bündnissystems ab. Sie berücksichtigen damit geographische Unterschiede, gesellschaftliche sowie sicherheitspolitische Entwicklungen, setzen die Schwerpunkte auf verschiedene Teilstreitkräfte und nehmen unterschiedliche technologische Entwicklungsstände auf Seiten des Gegners auf.
Parallel zur Technologierecherche und der anschließenden Erstellung der Szenare, begannen weitere Arbeitsgruppen mit der Grundlagenrecherche zu den Themen: operative Konzepte, Human Dimension, Fähigkeiten sowie Command and Control. In einem Zwischenschritt wurde jedes Szenar durch die jeweilige Arbeitsgruppe überprüft, geschärft sowie auf Ableitungen für die Bundeswehr hin geprüft. Abschließend wurden arbeitsgruppenübergreifend die Erkenntnisse zusammengeführt, um basierend auf den zukünftigen Herausforderungen des MDB Lösungsideen und Zielbilder für eine siegfähige Bundeswehr zu entwickeln. Dadurch wurde die Arbeit wie folgt gegliedert:

Kapitel 2 „Herausforderungen auf dem Gefechtsfeld der Zukunft“
- Darstellung der zukünftigen Herausforderungen,

Kapitel 3 „Wie wir bestehen – Zielbild“
- Entwicklung eines Zielbildes für die Bundeswehr mit einem operativen Konzept und der Ableitung zukünftig notwendiger Fähigkeiten,

Kapitel 4 „Handlungsfelder für die Bundeswehr“
- Ableitung von zur Erreichung des Zielbildes notwendigen kurz- und mittelfristigen Maßnahmen

1 Ein operatives Konzept ist die Vorstellung, wie deutsche Streitkräfte auf dem Gefechtsfeld der Zukunft agieren müssen, um siegfähig zu sein. Es berücksichtigt militärstrategische Vorgaben, gesellschaftliche und technologische Trends sowie mögliche Konfliktszenarien und daran beteiligte Akteure.
2 Das MDB umfasst den operativen Einsatzraum von Streitkräften – schon in der Vorbereitung auf ihren Einsatz. Das MDB schließt neben dem klassischen Gefechtsfeld in den Dimensionen Land –– Luft –– See in allen Domänen gemäß FAWU, die Dimensionen Cyber-/ Informationsraum (CIR) und Weltraum (WR) gleichrangig ein, um die eigenen operativen Fähigkeiten skalierbar über den Verlauf einer Operation hinweg projizieren zu können.

4 Handlungsfelder für die Bundeswehr

4.1 Digitalisierung und Vernetzung – „Einfach mal machen“

Im Handlungsfeld „Digitalisierung und Vernetzung“ lassen sich für das Multi-Domain Battlefield und die Bundeswehr der Zukunft die folgenden operativen Kern-Herausforderungen ableiten:

- Die Sicherstellung eines dimensionsübergreifenden Datenaustauschs auf allen Führungsebenen (insb. der taktischen und operativen),
- das Minimieren der Verwundbarkeit der Führungseinrichtungen,
- die Abhängigkeit vom elektromagnetischen Spektrum,
- das Beherrschen der zur Verfügung stehenden, großen Datenmengen
- und das Sicherstellen der Datenintegrität in Zeiten von Quanten-Computing.

Im Zielbild ist die Bundewehr in der Lage Daten auf allen Ebenen und dimensionsübergreifend schnell, effizient und plattformunabhängig auszutauschen. Diese Daten werden dabei in einer einheitlichen Bundeswehr-Combat-Cloud gespeichert, verarbeitet und in einem einheitlichen, durch Künstliche Intelligenz (KI) gestützten, Battle-Management-System dem Nutzer aufbereitet dargestellt, um ein effizientes Sensor- und Effektoren-Management sicherzustellen. Die Übertragung der Daten erfolgt durch Quanten-Schlüssel-Verteilung und ist damit sicher sowie durch die Nutzung neuer Übertragungswege (z. B. Unterwasser- und Laserkommunikation) redundant und zuverlässig. Zudem existieren nur noch kleine, dezentrale und hochmobile Gefechtsstände. Briefings und Befehlsausgaben werden in den virtuellen Raum verlagert. Im Endzustand ist die Bundeswehr durch die Digitalisierung und zunehmende Automatisierung im Einsatz sowie im Grundbetrieb gestärkt.
Digitalisierung und Vernetzung sind die Voraussetzung und der Schlüssel für den Erfolg auf dem MDB!

4.2 Multi-Domain-Effects – Flexibel und effizient

Die ukrainischen Streitkräfte haben mit „GIS Arta“ ein automatisiertes Command and Control-System zur Nutzung gebracht, das mit einfachsten Mitteln private IT und damit die gesamte Bevölkerung zu einem Aufklärungs- und Wirkungsverbund integriert. Ein System, das selbstständig in der Lage ist, eine Vielfalt von Wirkungsketten (System of Systems) – auch in Zusammenarbeit mit anderen Systemen (Network of Networks) – auszuführen, bietet den Führerinnen und Führern vor Ort flexible Möglichkeiten einen Effekt zu erzielen und damit gegenüber gegnerischen Kräften einen signifikanten Entscheidungsvorteil.
Planung und Rüstung müssen sich auf modulare Wirkungsketten (sog. „kill-chains“ oder „kill-webs“, also die Gesamtheit der Systeme und Einheiten, die einen bestimmten Effekt erzielen sollen), statt auf monolithische Plattformen wie Kampfpanzer, Kampfhubschrauber, Kampfflugzeuge oder Fregatten konzentrieren. Dieser modulare Aufbau ermöglicht es der Bundeswehr, Fähigkeiten einfacher zu modernisieren, Interoperabilität herzustellen und somit schnell an veränderte Bedrohungslagen anzupassen. Funktionen werden nicht in einzelne teure Plattform integriert, sondern auf eine Vielzahl von bemannten und unbemannten Systemen verteilt, die Daten und Verarbeitungsfunktionen gemeinsam nutzen. Ein dazu befähigtes Netzwerk ist so zu konzipieren, dass es flexibel gebildet und schnell angepasst werden kann, um dem militärischen Vorgesetzen eine Auswahl an Effekten anzubieten.

Zunächst sollte geprüft werden, ob eigene Systeme[3] zu ähnlichen Fähigkeiten in der Lage sind und ggf. ertüchtigt werden können. Auf dieser Basis gilt es für Übungsvorhaben eine experimentelle Multi-Domain Task Force aufzustellen und Elemente von Mosaic Warfare[4] auszuprobieren, neue taktische Verfahren zu entwickeln und flexible Wirkketten zu beüben. Die Elemente von Mosaic Warfare erfordern hohe Flexibilität im Denken und Handeln und sind damit in einer Bundeswehr, die bereits mit Auftrag führt, perspektivisch sehr gut umsetzbar.

4.3 Resilienz – Verteidigung im Frieden

Um schon im Frieden ein resilientes und gesamtheitliches Lagebild zu schaffen, müssen in einem ersten Schritt die Teillagebilder verschiedener Ressorts zusammengefasst werden. So kann ein, nicht nur militärisch fokussiertes, Gesamtlagebild zur Krisenfrüherkennung generiert werden.
Blickt man auf die Erweiterung von Fähigkeiten im Cyberraum darf sich auch im Frieden nicht nur auf die Abwehr gegnerischer Angriffe konzentriert werden.
Der uneingeschränkte Zugang zum Cyber- und Informationsraum für Jedermann birgt Risiken. Hier muss eine umfassende Refokussierung auf die Themen Informationssicherheit, (personeller) Geheimschutz und Militärische Sicherheit im Kontext sozialer Medien, aber auch privat genutzter IT erfolgen.
Die verschiedenen Möglichkeiten zur Auswertung riesiger Datenmengen ermöglichen die frühzeitige Aufklärung gegnerische Narrative im öffentlichen Informationsumfeld. In Zusammenhang mit dem zu schaffenden ressortübergreifenden Lagebild sollten die Streitkräfte schnellstmöglich diese Chancen für sich nutzen und könnten mit der Schaffung eines Organisationselementes für strategische Kommunikation im BMVg aktiv-offensiv gegen diese Narrative wirksam werden.
Abschließend muss für die Truppenteile der Bundeswehr wieder eine nationale Notfallplanung geschaffen werden, um über eine resiliente Handlungssicherheit in Krise und Krieg zu verfügen. Dies umfasst ebenso materielle Reserven. Eine Überarbeitung des Schutzkonzeptes kritischer Infrastruktur (KRITIS), welche für die Operationsfreiheit der Streitkräfte notwendig ist, muss vorangetrieben werden. Daraus kann der tatsächliche Bedarf an Objektschutzkräften ermittelt werden.

3 Als Beispiel seien hier das Lagebilddarstellungssystem MESE (Militärische Erweiterbare Software-Entwicklung) oder der Artillerie-, Daten-, Lage- und Einsatz-Rechnerverbund (ADLER) III genannt.
4 Bei Mosaic Warfare werden eine Vielzahl einzelner Waffen- oder Sensorplattformen verschiedener Klassen, Größen und Typen - wie Kacheln in einem Mosaik - in einem Systemverbund ad-hoc zusammengeführt, um flexibel und missionsangepasst gegnerische Kräfte überwinden zu können.

4.4 Siegfähigkeit – Vom Gegner her denken

Als wichtigste, neu zu erwerbende Fähigkeit der Streitkräfte wird der Schutz von Truppenkörpern vor Bedrohungen aus der Luft betrachtet. Dabei müssen mobile Kapazitäten für C-RAM[5] sowie Abwehr von Drohnen/-schwärmen und Loitering Munition im Nah- und Nächstbereich fokussiert und kosteneffiziente Methoden der Bekämpfung wie Directed-Energy-Weapons, wie z. B. Laser, priorisiert werden. Überall dort, wo Drohnen ressourcenschonender denselben Effekt wie ein bisheriges Waffensystem erzielen können, sind diese mindestens ergänzend zu beschaffen.
Kern von Multi Domain Operations (MDO) ist das Überwinden gegnerischer A2/AD-Wirkverbünde. Systeme wie Artillerie und Raketenartillerie sind dazu zu befähigen, in einem modernen Wirkverbund koordinierte Effekte innerhalb kürzester Zeit zu erzielen, während sie durch Drohnen zur Aufklärung, für ECM und zur Erhöhung der Abstandsfähigkeit ergänzt werden.
Es ist unabdingbar, offene Quellen effizient auszuwerten, um Rückschlüsse auf reelle gegnerische Truppenbewegungen oder Propaganda ziehen zu können. Mittelfristiges Ziel muss daher eine KI-gestützte Fähigkeit zur Open Source Aufklärung sein.
Der Weltraum als Operationsraum erlaubt es, sich relativ frei über gegnerischem Gebiet zu bewegen. Zu beschaffende Kleinstsatelliten sind schnell einsetzbare und relativ günstig zu ersetzende Aufklärungsmittel, die mit verschiedensten Sensoren ausgestattet werden können.
Die systematische, maschinenlesbare Speicherung von Informationen und Rohdaten sowie eine anschließende Nutzung durch KI-Systeme versprechen in Zukunft eine Erhöhung des operativen Nutzens und die Unterfütterung des militärischen Echtzeitlagebilds mit bereits vorhandenen Informationen. Um dieses Ziel zu erreichen, muss die Bundeswehr kurzfristig die Entwicklung von Verfahren zur KI-gestützten Big-Data-Analyse beauftragen.
Aber auch im Bereich des Battle-Damage-Managements gibt es Potential: Über die Einbindung von beispielsweise Augmented Reality-Technologie könnte die Truppe gezielt in der Fehlersuche und -behebung unterstützt werden, indem Baupläne oder Anleitungen als virtuelle Objekte computergeneriert in die Umgebung eingeblendet werden. Die zusätzliche Implementierung von 3D-Druck beziehungsweise additiver Fertigung in die Bundeswehr muss Truppenteile zukünftig in zunehmendem Maße autark von vorgehaltenen Ersatz- und Austauschteilen werden lassen und bedarfsgerechtes Battle-Damage-Repair ermöglichen.

4.5 Funktionale Robustheit – ganzheitlich denken

Vor dem Hintergrund der zunehmenden Komplexität und Geschwindigkeit auf dem Gefechtsfeld, der steigenden Ansprüche an zukünftige Entscheidungsträger, dem steigenden Spezialisierungsgrad sowie der Herausforderungen der demografischen Entwicklung, werden zukünftig grundsätzlich Human Performance Optimisation (HPO)-Maßnahmen zum Ausschöpfen des individuellen biologischen Potentials und diese als Basis möglicher Human Performance Enhancement (HPE)-Maßnahmen notwendig sein. Kurz: Der Mensch muss bis an seine biologische Leistungsgrenze und gegebenenfalls darüber hinaus geführt werden.
Um gegenüber den zukünftigen Anforderungen zu bestehen, sind singuläre Maßnahmen nicht mehr erfolgsversprechend. Vielmehr ist das abgestimmte und kohärente Zusammenwirken von bereits bestehenden und additiven Maßnahmen zur Ausschöpfung

5 Counter Rocket, Artillery, and Mortar (C-RAM) sind Systeme zum Detektieren und Abfangen von anfliegenden Raketen und Artilleriegranaten kurzer Reichweite sowie Mörsergranaten.

des individuellen biologischen Potentials, welche das physische, psychische und kognitive Leistungsniveau adressieren, der Schlüssel zum Erfolg einer funktionalen Robustheit.
In diesem Zusammenhang müssen daher eine individuelle Betrachtung und Begleitung der/des Einzelnen, mittels Unterstützung durch Wearables und Apps erfolgen sowie Programme zur Steigerung der kognitiven Leistungsfähigkeit und der mentalen Widerstandsfähigkeit entwickelt und implementiert werden. Aufgrund der bisher wenig untersuchten Aspekte von HPE-Maßnahmen sowie deren ethischen und rechtliche Implikationen sollten Möglichkeiten der Nutzung von HPE wie Medikamente, Exoskelette, Implantate, Brain-Machine-Interfaces zeitnah gezielt analysiert werden. Dabei sollte der Fokus darauf gerichtet werden, wie mittels HPE der Nachteil gegenüber autonomen Systemen ausgeglichen werden kann.

4.6 Innovation – Ermöglichen statt administrieren

Innovatives Denken und Handeln ermöglichen jene Adaptivität und Flexibilität, die taktisch-operatives Führen besser macht und eine stetige organisatorische und technische Erneuerung der Gesamtorganisation schafft. Damit wird Innovation unter anderem Katalysator und Voraussetzung für das operative Konzept des Mosaic Warfare.
Innovation ist hierbei immer auf ein lösungsorientiertes Umsetzen ausgerichtet. In einem zivil-militärischen Innovationsökosystem müssen Eigenkreativität und Innovationsideen in und aus der Truppe sowie weiteren militärischen und zivilen Innovationstragenden berücksichtigt und gefördert werden.
Der Maßstab für die Leistungsfähigkeit des Innovationsökosystems bleibt die zeitliche Komponente, Idea-Ownership des Innovators und schlussendlich der Nutzen für die Streitkräfte. Hierzu ist eine strategische Neuausrichtung notwendig, die eine Schwerpunktsetzung, Priorisierung und Ressourcensteuerung für Innovationsvorhaben vorgibt. Die für Innovationsmanagement verantwortlichen Institutionen müssen entlang einheitlicher aber maximal flexibel gehandhabter Kriterien im Umgang mit Innovation vor allem bestrebt sein, Innovationen frühzeitig zu identifizieren, Synergieeffekte und Wissenspotentiale zu nutzen und unter der Akzeptanz von Fehlschlägen eine schnelle und skalierbare Implementierung anzustreben.
Exemplarisch ist dafür die Sichtbarkeit von Innovationsvorhaben innerhalb der Bundeswehr zu erhöhen und diese explizit durch interne Kommunikation sichtbar zu machen. Darüber hinaus sollten Test- und Versuchsstrukturen der jeweiligen Teilstreitkräfte und Organisationsbereiche zu streitkräftegemeinsamen Zentren überführt werden, um ein Denken in Dimensionsgrenzen bereits bei Test und Evaluierung zu erkennen und diesem vorzubeugen.

5 Herausforderungen auf dem Gefechtsfeld der Zukunft

Die Herausforderungen auf dem MDB werden vielfältig sein. Die Technologisierung des Gefechtsfeldes sowie hybride Bedrohungen und die damit einhergehende Verlagerung in den Welt-, Cyber- und Informationsraum werden stetig an Bedeutung gewinnen. Dies verhindert eine eindeutige Abgrenzung zwischen Frieden, Krise und Krieg noch weiter. Dabei wird der konventionellen Kriegsführung, mit Schwerpunkt auf urbanem Gebiet, dennoch weiter Beachtung geschenkt werden müssen. Die daraus resultierenden künftigen operativen Herausforderungen für die Bundeswehr in Bezug auf das MDB werden in Kapitel 2 „Herausforderungen auf dem Gefechtsfeld der Zukunft“ dargestellt.
Ein Großteil zukünftiger Herausforderungen wird durch den technologischen Fortschritt und die damit verbundenen Innovationszyklen bestimmt werden. Ihre Handhabbarkeit, ihr Einsatz bzw. die Nutzung ihrer Vorteile waren und sind seit jeher ausschlaggebend für den Erfolg militärischer Operationen. In Kapitel 2 werden die folgenden Technologiefelder beleuchtet, aus welchen sich militärisch nutzbare Fähigkeiten für die Bundeswehr ergeben, oder sich ableiten lassen:

- Informationstechnik,
- Zukünftige kinetische Effekte und Waffensysteme,
- Automatisierung von Waffen- und Assistenzsystemen,
- Human Performance Enhancement.

Die Abhängigkeit vom Elektromagnetischem Spektrum (EMS), ortsfesten und leicht aufzuklärenden Führungseinrichtungen und einer hohen Vulnerabilität von Netzwerkinfrastruktur und Kommunikation fordern die militärische Organisation weiter heraus. Die Nutzung von KI und Quantentechnologie der zweiten Generation in der Operationsplanung und -führung sind auf dem künftigen MDB „Gamechanger“ und bieten Lösungsansätze für vorhandene Problemstellungen, bergen aber auch neue Herausforderungen.
Kinetische Effektoren und Waffensysteme der Zukunft sind Mittel, die Streitkräfte einsetzen werden, um dem Feind durch Erzeugung multipler Dilemmas überlegen und somit siegreich zu sein. Diese umfassen u. a. hypersonische Fluggeräte, Direct Energy Weapons (DEW, z. B. Laser), Anti-Satellite Weapons (ASAT), High Power Electromagnetics und die Anpassung und Modernisierung von derzeitigen Effektoren an die Herausforderung des MDB. Diese Harmonisierung bei gleichzeitiger Implementierung bilden signifikante Aufgabenstellungen für Operationen auf dem MDB.
Das MDB erfordert ein effizientes Zusammenbringen von Sensoren und Effektoren verschiedener Dimensionen, um zur richtigen Zeit den gewünschten militärischen Effekt zu erzeugen. Das Potential automatisierter Prozesse und Entscheidungen bleibt derzeit weitgehend ungenutzt. Die zunehmende Entwicklung von Unmanned Aerial Systems und KI wird die Automatisierung von Waffensystemen bis hin zur vollständigen Autonomisierung ermöglichen und damit die Effizienz und die Koordination untereinander signifikant erhöhen. Eine der größten Herausforderungen auf diesem Gebiet entsteht durch die unterschiedliche ethische wie rechtliche Bewertung innerhalb der Allianz, wie auch bei potentiellen Gegnern.
Die Dimension Cyber- und Informationsraum (CIR) durchdringt mittlerweile nahezu alle Lebensbereiche, von der kontinuierlichen Gewährleistung der Social Media Plattformen für Smartphones bis hin zur automatisierten Überwachung von Umspannwerken, Kläranlagen oder Ölpipelines. Daher birgt die Dimension CIR neben vielen Chancen auch große Risiken für die gesamtstaatliche Verteidigung. Potentielle Gegner können in der

Anonymität des Cyber- und Informationsraumes derzeit, ohne substantielle Gegenwehr, unbemerkt und permanent Effekte erzielen.
Der uneingeschränkte Zugang, die Nutzung und die Kontrolle der Dimension Weltraum sind wesentliche Elemente für die Durchführung militärischer Operationen, humanitären Einsätzen und Logistik bis hin zum hochintensiven Gefecht. In einem Peer-to-peer Konflikt ist davon auszugehen, dass Gegner zu einem sehr frühen Zeitpunkt in der Dimension Weltraum wirken werden. Dafür stehen schon heute Effektoren für offensive Weltraumoperationen wie ASAT Raketen, Deorbiting-Manöver und DEW zur Verfügung. Der freie Zugang und die friedliche Nutzung des Weltraumes sind somit bedroht.
Der aktuelle Megatrend „Urbanisierung“ setzt sich unverändert fort. Im dicht besiedelten Europa fehlen große rurale Räume, in denen ohne die Gefahr von Kollateralschäden gekämpft werden könnte. Eine zwangsläufige Herausforderung ist es daher, Kämpfe aus urbanen Räumen herauszuhalten und dem Gegner den Zugriff auf die Zivilbevölkerung zu verwehren.
Hybride Kriegsführung bedeutet die gesamtstaatliche Verschränkung von militärischen und nicht-militärischen Akteuren. Eingebettet in Propaganda, staatliche Narrative, nicht-attribuierende Cyberangriffe, die Anwendung von „Weaponized Law und Ethics“ und Maßnahmen im EMS, wirken diese unterhalb der Schwelle einer militärischen Auseinandersetzung, um koordiniert außen- und sicherheitspolitische Effekte zu erzielen. Das Zusammenspiel von militärischen und nicht-militärischen Mitteln fordert daher insbesondere demokratische und föderale Staatstrukturen heraus.
Die zukünftig steigenden Anforderungen an Soldatinnen und Soldaten und insbesondere militärische Vorgesetzte, vor allem im Hinblick auf die zunehmende Komplexität, müssen in Einklang gebracht werden. Körperliche Fitness und das Niveau grundlegender Stressresilienz von Bewerbern gehen zurück, während Technikaffinität nicht generell vorausgesetzt werden kann. Zusätzlich müssen Soldatinnen und Soldaten aufgrund der technologischen Entwicklung auf immer stärker spezialisierte Aufgabenfelder vorbereitet werden. Human Performance Modification (HPM) eröffnet die Möglichkeiten, die Grenze der individuellen, physischen, psychischen und kognitiven Leistungsfähigkeit zu optimieren und ggf. zu überwinden. Dies ist notwendig, um mit den steigenden Herausforderungen der technologischen Entwicklungen Schritt halten zu können. HPM bietet in diesem Zusammenhang eine weitere Möglichkeit im Umgang mit autonomen, leistungsfähigen Waffensystemen. Dieses umfasst Maßnahmen, die bestehenden Einschränkungen des menschlichen Organismus zu überwinden. Bereits heute sind unterschiedliche Technologien verfügbar, die den Menschen bei vielfältigen Herausforderungen unterstützen können. Die unterschiedlichen ethischen Bewertungen von HPE innerhalb unserer Allianzen und auf dem Gefechtsfeld der Zukunft bergen eine der größten zukünftigen Herausforderungen.
Unter Human Performance Degradation (HPD) werden alle Maßnahmen subsumiert, welche die menschliche Leistungsfähigkeit beeinträchtigen. Dies kann gezielt durch Mikrowellen, Schall, Nervenkampfstoffe oder ähnliches erfolgen und durch potentielle Gegner operationalisiert werden. Auf dem Gefechtsfeld der Zukunft wird der Mensch noch mehr als Ziel zu verstehen sein.

6 Wie wir bestehen – Zielbild

In allen Überlegungen hinsichtlich der Frage nach dem „Wie bestehen wir?“ werden zwei wesentliche Linien erkennbar: ein eher hybrides Vorgehen, um die technologische Überlegenheit des Westens zu umgehen sowie konventionelle Konflikte hoher Intensität zwischen staatlichen Akteuren mit modernen Technologien und Fähigkeiten (bspw. A2/AD- und Cyber-Fähigkeiten).
Im hier zusammengefassten Kapitel „Wie wir bestehen“ wird aus den Erkenntnissen und Herausforderungen des vorherigen Kapitels ein „Zielbild Bundeswehr“ von MDO- und zukunftsfähigen Streitkräften skizziert sowie Lösungsideen, Prüffragen und Denkanstöße aufgezeigt, die auf dem Weg dorthin zwingende Berücksichtigung erfahren müssen.
Ausgehend von einer Definition des Begriffs „Operatives Konzept“ wird der Blick auf neue operative Konzepte geworfen. Dabei wird herausgearbeitet, dass staatlich koordiniertem, aggressiven Verhalten, welches die Destabilisierung der Bundesrepublik zum Ziel hat, mit dem bestehenden Rechtsrahmen nicht zielgerichtet begegnet werden kann. Gerade wenn Zivilpersonen und zivile Einrichtungen zur Zielscheibe des „hybriden Krieges“ werden, muss der Verteidigungsfall im Sinne des Grundgesetzes auch „Multi-Domain“ gedacht werden. Gesamtstaatliche Verteidigung muss bereits im Frieden unterschwellige hybride Angriffe, vor allem im Cyber- und Informationsraum, erkennen, angemessen reagieren und Antworten finden, die potentielle Gegner zukünftig abschrecken.
Ein operatives Konzept für künftige Kriege kann der Mosaic Warfare des Strategic Technology Office der amerikanischen Defense Advanced Research Projects Agency (DARPA) für die Entwicklung von Streitkräften und Operationen sein, welches eine überlegene manövrierfähige Kriegsführung im 21. Jahrhundert sicherstellen soll. Ein „Mosaik“-System ist so konzipiert, dass es flexibel vernetzt und schnell konfiguriert werden kann, um dem Nutzer belastbare Fähigkeiten zu bieten. Wie die Teile eines Mosaiks kann jedes System (oder jede Einheit), das bestimmte funktionale Merkmale aufweist, mit anderen kombiniert werden. Neu ist die Geschwindigkeit, Variabilität und Komplexität, die Mosaic Warfare ermöglicht. Durch Vernetzung und Datenaustausch bietet dieses Konzept das Potential, auch in unvorhergesehenen Lagen die Initiative zu gewinnen und den Gegner konstant in seinem Führungsprozess zu stören.
Der Kampf um Informationsüberlegenheit, als Basis für Führungs- und Wirküberlegenheit, wird in einer sehr frühen Phase eines Konfliktes aufgenommen und erfolgt oft unterhalb der Schwelle einer kriegerischen Auseinandersetzung. Dafür muss in einem ersten Schritt das Zusammenfließen der Informationen von etablierten Systemen mit den immer wichtiger werdenden Dimensionen CIR und Weltraum erfolgen. Mit den vorliegenden, ausgewerteten Informationen wird aus einem Effektoren-Mix das nach allen bisher bekannten Kriterien geeignetste und auch effizienteste Mittel ausgewählt. Der geforderte Effekt wird damit zu einem Service eines aktiv unterstützenden BMS.
Die in diesem Zusammenhang notwendigen Implikationen und Ableitungen hinsichtlich der Command and Control-Strukturen sowie aufzubauenden Fähigkeiten werden im Kapitel „Multi-Domain Command and Control“ dargestellt. Eine Überlegung besteht darin, zukünftig eine größere Interoperabilität zwischen den Dimensionen zu schaffen, welche durch flachere Strukturen und einen schnelleren Entscheidungsfindungsprozess flankiert wird. Die umfassende Vernetzung der Streitkräfte erfordert Protokolle und Verfahren, um beliebige Hardware zu integrieren. Statische Hardwarestandards und monolithische Fähigkeitsträger hemmen die Vernetzung.

Darüber hinaus sind die Voraussetzungen zu schaffen, Truppenteile aus dem Stand in eine einsatz- oder effektorientierte, individuell angepasste operative Struktur zu überführen, die auch multinational sein kann. Auch an der bewährten Führungsphilosophie „Führen mit Auftrag“ kann festgehalten werden, ihre Grundsätze passen wie kein zweites Konzept zu den Gedanken von MDO.
Militärischen Führungskräften wird künftig ein einheitlich aggregiertes Lagebild zur Verfügung stehen, welches alle Dimensionen und Führungsebenen umfassen kann. Dazu müssen sie von automatisierten und teilautonomen Systemen unterstützt werden, die auf KI-Unterstützung zurückgreifen und den man-on-the-loop-Gedanken unterstützen.
Technologien, operative Konzepte und mögliche Konfliktformen sind Treiber von Fähigkeiten, die die Bundeswehr benötigt, um zukünftig bestehen zu können.
Trotz aller technologischen Innovationen wird das Wesen der modernen Kriegsführung auch weiterhin von Menschen bestimmt werden. Für das Kapitel „Human Dimension“ wird zum einen zugrunde gelegt, dass der Mensch ein multispektrales, militärisches Ziel bleibt, welches auch auf kognitiver Ebene beeinflusst werden kann. Zum anderen ist der Mensch ein limitierender Faktor, da ihn immer schnellere Datenverarbeitungszyklen über die Grenzen seiner Verarbeitungsfähigkeit bringen.
Die im Anteil „Human Dimension“ getroffenen Schlussfolgerungen reichen dabei von der lebenslangen Steigerung beziehungsweise Aufrechterhaltung der individuellen Leistungsfähigkeit bis hin zu den Möglichkeiten der Weiterentwicklung von Human Performance. Dabei werden die vielfältigen organisatorischen und technischen Lösungen betrachtet, mit denen die Leistungsfähigkeit des Menschen gesteigert werden kann und die Diskussion angestoßen, wie weit man dabei gehen möchte.
Insgesamt ist die physische, psychische, kognitive und ethisch-moralische „Fitness“ hinsichtlich der Einsatzbereitschaft der Streitkräfte für MDO von essentieller Bedeutung. Ziel ist daher die Implementierung und Umsetzung eines Konzeptes „Funktionale Robustheit der SK“, womit eine individuelle, präventive, ebenengerechte und adäquate Ausnutzung des individuellen Potentials gewährleistet wird.
Diskutiert wird weiterhin die Nutzung von Automation und KI in Waffensystemen und die offene Frage von neuen völkerrechtlichen Regelungen. Auf dem Weg dahin werden je nach Situation, System und technischen Möglichkeiten verschiedene Stufen durchlaufen, die von der Unterstützung des menschlichen Bedieners „man-in-the-loop“ hin zu einem teilweise eigenständig durchzuführendem Einsatz „man-on-the-loop“, beispielsweise zur Selbstverteidigung, reichen. Für die, bis dahin notwendigen Diskussionen werden durch die Arbeit Impulse geliefert und Begriffe erläutert.
Eine MDO-befähigte Bundeswehr bietet die Chance, im Rahmen der Verteidigung des NATO- und EU-Bündnisgebiets einen wesentlich höheren Beitrag zu leisten, als es heute der Fall ist. In den drei Kurzportraits ‚So könnte es aussehen‘ wird anhand möglicher Einsatzszenarien der Bundeswehr sowie mittels fiktiver Erfahrungen einzelner Personen während möglicher Operationen gezeigt, wie ein erfolgreiches Operieren auf dem MDB aussehen könnte:

1. Multi Domain Coalition und Homeland Defense – Deutschland in einer Führungsrolle in einem Peer-to-peer-Konflikt im Kampf um Europa.
2. Multi Domain Expeditionary Force – Deutschland als Führungs- bzw. Anlehnungsnation im Einsatz außerhalb des NATO/ EU-Bündnisgebiets.
3. Multi Domain Supporting Role – Deutschland als unterstützende Nation ohne Führungsrolle in einem Einsatz weit außerhalb des NATO/EU-Bündnisgebiets.

In den skizzierten Szenarien finden sich die bereits dargestellten wesentlichen Ableitungen zukünftiger Anforderungen an Command and Control sowie notwendige Fähigkeiten in entsprechenden Bildern als mögliches Anwendungsbeispiel wieder.
Zum Abschluss des gesamten Kapitels werden noch einige strategische Überlegungen angestellt. Sie sind aus unserer Sicht jedoch sowohl innerhalb der Bundeswehr als auch gesamtstaatlich notwendig, um in Zukunft bestehen zu können, wenn bereits durch Propaganda, Desinformationskampagnen, nicht-attribuierbare Cyberangriffe, die Anwendung von „Weaponized Law und Ethics“ und wirtschaftspolitische Maßnahmen konstant Druck auf Staat und Gesellschaft ausgeübt wird.
Eine Reaktion auf Augenhöhe kann nur durch Etablierung und Durchführung von passiven-defensiven und aktiv-offensiven Maßnahmen im Rahmen einer ressortübergreifenden Cognitive Warfare auf strategischer Ebene erfolgen. Dabei geht es im Wesentlichen um die Stärkung von Moral, Vertrauen, persönlicher Resilienz oder „Kampfeswillen“. Für alle Bundeswehrangehörigen sollten in ausgewählten Ausbildungsabschnitten Module zu „Propaganda-Awareness“, „Informationssicherheit“ und „Mentale Fitness/Stressresistenz“ absolviert werden. Dazu kommt passiv-defensive Cognitive Warfare, die auf die eigene Bevölkerung fokussiert und deren mentale Resilienz gegenüber gegnerischer Desinformation und Propaganda stärkt. Technische Unterstützung zur Erkennung, Attribuierung und der Richtigstellung gegnerischer Narrative durch deren Kennzeichnung als Fake-News werden dabei genauso betrachtet wie die Schaffung eines gemeinsamen Verständnisses innerhalb der Ressorts der Bundesregierung bezüglich geregelter Zuständigkeiten, Verfahren und Abläufe für eigene aktiv-offensive Cognitive Warfare.
Des Weiteren müssen Vorschriften und Prozesse innerhalb der Bundeswehr wieder auf ihre Notwendigkeit oder Verkürzung/Aussetzung im Spannungs-/Verteidigungsfall hin geprüft werden, um einen „Kaltstart“ realisieren zu können. Verantwortlichkeiten und Zuständigkeiten für Beschaffung und Rüstung müssen bereits vorab gedacht werden und festgelegt sein, um im Verteidigungsfall reibungsarm wirksam zu werden.
Im Rahmen hybrider Maßnahmen ist die KRITIS Cyberangriffen und Sabotageakten ausgesetzt. Im Verteidigungsfall fehlt gesamtstaatlich jedoch die Kapazität, KRITIS zu schützen. Dafür ist neben der Erhebung von Grundlagendaten zu KRITIS in Kooperation mit anderen Ressorts insbesondere zu kalkulieren, mit welchem regional notwendigen Kräfteansatz diese rudimentär zu schützen ist. In den ressortgemeinsamen Anstrengungen ist zunächst eine dem Stand der Technologie angemessene Vernetzung sicherzustellen. Notwendige Arbeitsbeziehungen müssen institutionalisiert werden und jederzeit funktional sein. Insbesondere für Einsätze im Rahmen des IKM könnte so auch der Comprehensive Approach gestärkt werden.
Im Sinne der gesamtstaatlichen Verteidigung ist auch die aktuelle Praxis der Arbeitsbeziehungen von Streitkräften, Wehrverwaltung und Industrie untereinander zu prüfen und zu erörtern, wie durch gezielte Personalabstellungen oder Reservestrukturen mit anderen Ressorts kooperiert werden kann. Dazu sind auch Anpassungen des Beschaffungsprozesses notwendig, um diesen an die künftigen Herausforderungen anzupassen und im Konfliktfall die Versorgung sicherstellen zu können.

Platz für Ihre Innovationen:

Platz für Ihre Innovationen