Die Grundzüge der Inneren Führung der Bundeswehr sind heute relevanter denn je. Erfolg im Systemwettstreit hat, wer die Potenziale der Digitalisierung versteht und unter Berücksichtigung der gesellschaftlichen Grundwerte orchestrieren kann. KI-Anwendungen stellen dabei einen Teilaspekt dar. Der Beitrag betont, dass Innovationszyklen immer schnelllebiger sind. Das erfordert agile Strukturen und ein digitales Mindset in Politik, Verwaltung, Wirtschaft und Bundeswehr, um die Werteordnung zu verteidigen.

Innere Führung vor dem Hintergrund der Digitalisierung

Dr. Bernhard Rohleder, Stephan Ursuleac

Ausgangslage

Die internationale Politik erlebt erneut einen Wettstreit der Wertesysteme zwischen Demokratien und Autokratien. Herausforderungen bieten sich durch klassische militärische Antagonisten, hybride Angriffe auf die Demokratie – insbesondere durch Desinformation und Cyberangriffe – sowie unterschwellige militärische und nachrichtendienstliche Operationen, die die politische Ordnung unterlaufen. In besonderem Maße wirkt sich die voranschreitende Digitalisierung auf die Gesellschaft und die Streitkräfte aus. Die Abläufe in der Kommunikation und Produktion sowie ein durch digitale Anwendungen immer schnellerer technologischer Fortschritt betreffen die Sphären von Gesellschaft, Politik, Wirtschaft und Bundeswehr.

Der Zweite Weltkrieg prägt bis heute das politische Wesen der Bundesrepublik Deutschland. Am 5. Januar 1950 besprachen die ehemaligen Wehrmachtsgeneräle Hermann Foertsch, Adolf Heusinger und Hans Speidel die Grundzüge des Aufbaus neuer deutscher Streitkräfte. Ihnen war klar, dass es nicht mehr nur um Strukturen, Ausrüstung und politische Leitlinien gehen konnte. Auch das innere Gefüge dieser Streitkräfte, ihr innerer Kompass, sei für die kommenden Konflikte zwischen den Wertesystemen entscheidend. Diese Grundüberlegungen prägten die im Oktober 1950 verfasste „Himmeroder-Denkschrift“ eines 15-köpfigen Militärexpertenrates, eingesetzt von Bundeskanzler Konrad Adenauer. Das Grundverständnis der Soldaten sollte sich fortan auf die Wahrung der Menschenrechte und die Bejahung der freiheitlich-demokratischen Grundordnung stützen. Ihr Handeln beruhe nicht auf Loyalität zum Vaterland oder zu einem politischen Anführer, sondern auf

persönlicher Überzeugung und Einsicht gegenüber dem Rechtsstaat und der Werte und Normen der Gesellschaft. Diese manifestieren sich im Grundgesetz der Bundesrepublik Deutschland. Die Streitkräfte unterliegen dem alleinigen Primat der Politik aus Parlament und Regierung. Im Grunde waren dies bereits die Impressionen, die der preußische Reformer Gerhard von Scharnhorst im 19. Jahrhundert für die Armee ersann. Das Gründungsdatum der Bundeswehr am 12. November 1955 ist daher nicht zufällig der 200. Geburtstag von Gerhard von Scharnhorst.

Sachstand der Digitalisierung – Impressionen für die Bundeswehr

Wir leben im Zeitalter der vierten Industriellen Revolution. Nachdem die ersten beiden Industriellen Revolutionen noch durch mechanischen Fortschritt ausgelöst wurden, ermöglichen technische Innovationen, vor allem in der IT, seit den 1960er-Jahren eine ganz neue Form wirtschaftlicher und sozialer Prozesse, die mit einer zunehmenden, überregional und letztlich übergreifenden Vernetzung einhergehen. Daraus hat sich in den 1980er-Jahren der Trend der Globalisierung entwickelt: Unternehmen nutzen IT, um ihre Effizienz durch Standardisierung und globale Arbeitsteilung zu steigern. Die wirtschaftspolitischen und rechtlichen Rahmenbedingungen haben diesen Trend verstärkt. Seit den 2000er-Jahren sehen wir durch die Digitalisierung die zunehmende Nutzung von IT in allen Bereichen. Diese bisher letzte Phase der Industriellen Revolution hat in kürzester Zeit zu völlig neuen Produkten, Dienstleistungen und Geschäftsmodellen geführt.[1]

Die erfolgreiche Umsetzung der Digitalisierung benötigt klare Verantwortlichkeiten und Strategien. Mehr als die Hälfte der Unternehmen setzt dazu auf agiles Projektmanagement und auf ein kontinuierliches Change- und Wissensmanagement.[2] Daten werden meist in privaten Cloudstrukturen verwaltet. Großes Potenzial sieht die Wirtschaft bei der Automatisierung von Geschäfts- und Verwaltungsprozessen. So sehen 43 Prozent die größten Potenziale bei der automatischen Erkennung von eingehenden Dokumenten und Informationen.[3]

Erfolg im Systemwettstreit hat, wer die Potentiale der Digitalisierung versteht und zu orchestrieren vermag, unter Berücksichtigung der gesellschaftlichen Grundwerte, für die die Innere Führung der Bundeswehr eintritt.

Ein zunehmender Engpass bei der Umsetzung von Digitalisierungsprojekten sind das verfügbare Personal und gestörte Lieferketten für IT-Bauteile. Deutschlandweit fehlen über 96.000 IT-Fachkräfte. Um Mängeln zu begegnen, investieren im Durchschnitt 71 Prozent der Unternehmen und 56 Prozent der Verwaltung in Fort- und Weiterbildungen zur Digitalisierung.[4] Weiterhin fordern 78 Prozent der Unternehmen ein Pflichtfach Informatik, um den Bedarfen zu begegnen.[5] Auch qualifizierte Zuwanderung kann ein Weg sein, diesen Bedarf teilweise zu decken. Allein durch den russischen Angriffskrieg gegen die Ukraine kommt es zu einem Braindrain von russischen IT-Spezialistinnen und -Spezialisten, die dem Regime den Rücken kehren. Über 170.000 von ihnen haben ihr Heimatland verlassen.[6] Diese Fachkräfte, die sogar oft von deutschen Unternehmen stammen, könnten auch in Deutschland Anschluss finden.

Die größten Chancen bei der Digitalisierung sehen 70 Prozent der Unternehmen in der Steigerung der Transparenz, aber auch der deutlichen Senkung von Verwaltungskosten.

Hürden bei der Digitalisierung liegen für 73 Prozent der Unternehmen beim nach wie vor hohen Investitionsbedarf. Weiterhin bemängeln über 50 Prozent zu hohe rechtliche Standards, unter anderem Anforderungen an den Datenschutz oder die IT-Sicherheit. Dazu kommt: 65 Prozent fürchten einen unberechtigten Zugriff auf sensible Unternehmensdaten.[7] Dies verwundert nicht, da allein 2022 in der deutschen Wirtschaft durch Cyberangriffe oder Spionage und Sabotage ein Schaden von über 203 Milliarden Euro entstanden ist.[8]

Im militärischen Kontext bietet die Digitalisierung den Streitkräften große Chancen. Sie liefert einen entscheidenden Beitrag zur Stärkung ihrer Einsatzbereitschaft. Digitalisierung gilt als Schlüssel zur Informationsüberlegenheit. Sie kann die Führungs- und Reaktionsfähigkeiten, aber auch die Attraktivität der Bundeswehr stärken und somit entscheidende Vorteile verschaffen. Dazu gehören vor allem Maßnahmen wie das ortsunabhängige Arbeiten, datenzentrierte Prozesse in der Verwaltung und im Führungsprozess, die Patientenakte im Sanitätsdienst, aber auch der Einsatz unbemannter Systeme und bei Abwehrsystemen und vieles mehr im Dreiklang Aufklärung – Führung – Wirkung.

Die stetig steigenden Innovationsprozesse bei technologischen Anwendungen stellen längst einen Wettlauf der Armeen dar. Zwar sind westliche Armeen – vor allem die der USA aber auch Israels – in Sachen Militärtechnologie noch führend, jedoch holen andere Nationen wie China rasant auf. Hinzu kommt eine zunehmende Komplexität der internationalen Politik. Innenpolitische und fiskalische Herausforderungen in den USA zwingen diese, neue Schwerpunkte zu setzen. Das erfordert mehr Eigenverantwortung durch Europa, wobei Deutschland aufgrund seines politischen und wirtschaftlichen Gewichts mehr Engagement abverlangt wird.

Moderne Streitkräfte sind dafür essenziell. Die Bundesregierung verfolgt das Ziel, die Bundeswehr zur besten konventionellen Streitmacht Europas zu machen, was durch die Zeitenwende und das 100 Milliarden Euro Sondervermögen sowie steigende Wehretats erreicht werden soll. Dazu benötigt es jedoch agilere Strukturen, durchhaltefähige Logistik und Technik, die State of the Art ist. Auch sind ein gefestigtes Mindset der Soldatinnen und Soldaten in Bezug auf Werte und Normen, aber auch die Fähigkeit, gesellschaftliche, politische und technologische Veränderungen zu adaptieren und Innovationen zu fördern und umzusetzen, nötig. Eine enge Zusammenarbeit und Austausch auf Augenhöhe zwischen Politik und Bundeswehr sowie mit der Wirtschaft und Wissenschaft sind dafür erforderlich.

Dabei ist die Verteidigungsbereitschaft der Streitkräfte nicht mehr nur durch schwere Waffen gegeben, sondern zunehmend durch digitale Aspekte im Cyber- und Informationsraum. Im 20. Jahrhundert waren Panzer, Schiffe und Flugzeuge reine Hardware, denen ein wenig Technik zum Funktionieren implementiert wurde. Die technologische Abstimmung dieser Systeme musste lediglich taktisch in den Einsatzdoktrinen berücksichtigt werden, sodass die Teilstreitkräfte zwar im Verbund dachten, jedoch in eigenen Silostrukturen technische Entwicklungen umsetzten. Heute sind diese Plattformen fahrende, schwimmende und fliegende Rechenzentren, die national und im Verbund mit NATO und EU interoperabel funktionieren müssen. Dies erfordert abgestimmte IT-Technologien. Die Fähigkeit zur Digitalisierung ist somit entscheidend für den Erfolg.

Die Trendtechnologien der deutschen Verteidigungsindustrie für die kommenden fünf Jahre werden regelmäßig durch den Bitkom und

andere Verbände für das Bundesministerium für Verteidigung (BMVg) erhoben. In Abbildung 1 sind die Trendtechnologien 2022 zu sehen, die in einer repräsentativen Umfrage unter 70 Unternehmen der Verteidigungsindustrie erstellt wurde. KI-Anwendungen sehen über 50 Prozent der Unternehmen als entscheidende Trendtechnologie.

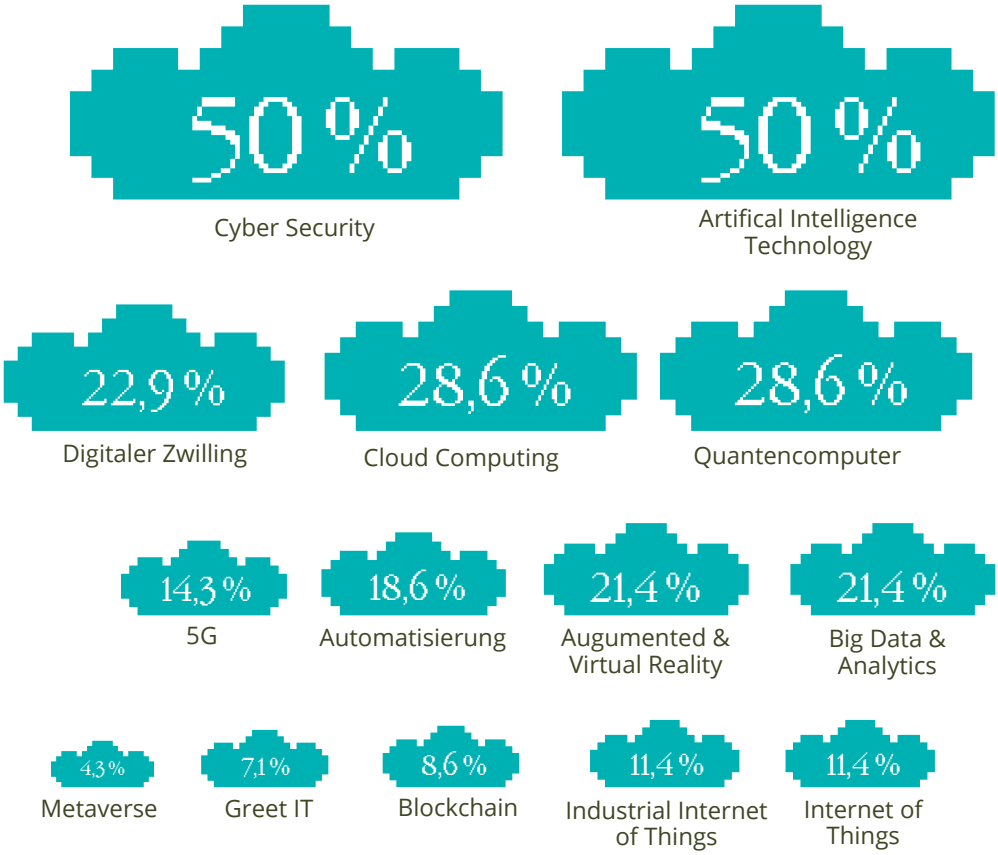


Abbildung 1: Umfrage zu Trendtechnologien der Sicherheits- und Verteidigungsbranche 2022. Quelle: bitkom e. V.

KI-Sachstand und Anwendungsmöglichkeiten im Militär

Um Nutzen, Chancen und Risiken der Künstlichen Intelligenz (KI) diskutieren zu können, ist es zunächst notwendig, die wichtigsten Begriffe der KI zu verstehen und den historischen und aktuellen Kontext zu beleuchten. Künstliche Intelligenz ist als Begriff nicht einheitlich definiert. Vor allem, da sie sich schon seit der Begriffsbildung

Ende der 1950er-Jahre als interdisziplinäre Forschungsrichtung entwickelt und sich in ihrer Deutung stets an die technischen Möglichkeiten angepasst hat. Für die praktische Anwendung hat sich folgende Definition als nützlich erwiesen: Künstliche Intelligenz beschreibt Informatikanwendungen, deren Ziel es ist, intelligentes Verhalten zu zeigen. Dazu sind in unterschiedlichen Anteilen bestimmte Kernfähigkeiten notwendig: Wahrnehmen, Verstehen, Handeln und Lernen. Diese vier Kernfähigkeiten stellen die größtmögliche Vereinfachung eines Modells zur modernen KI dar: Wahrnehmen – Verstehen – Handeln erweitern das Grundprinzip aller EDV-Systeme: Eingabe – Verarbeitung – Ausgabe. Das Neue ist das Lernen. Heutige echte KI-Systeme haben gemeinsam, dass sie in der Verarbeitungsfähigkeit auch trainiert werden und damit lernen können. So erzielen sie bessere Ergebnisse als herkömmliche Verfahren, die nur auf starren, klar definierten und fest programmierten Regelwerken basieren. Heute spricht man von der schwachen KI, bei der es darum geht, den Menschen intelligent beim Erreichen seiner Ziele zu unterstützen, also um smarte Mensch-Maschine-Interaktion und -Kollaboration. Die starke KI ist eher philosophisch relevant. Sie zielt auf eine Imitation des Menschen ab, die eher als Science-Fiction-Vision taugt.

Die neueste Phase von KI-Systemen versucht daher, Lernverfahren mit Expertenwissen zu verbinden, um das Beste aus beiden Welten zu nutzen: Kontrolle und explizites Wissen mit der Kraft von Lernalgorithmen, die dann auch bei unsicherer Faktenlage ähnlich gut wie ein Mensch handeln können.[9] In Zusammenarbeit mit wissenschaftlichen Vertreterinnen und Vertretern sowie seinen Mitgliedern hat der Bitkom das Periodensystem der KI entwickelt.

Dieses hilft, systematisch über die Einsatzzwecke, Chancen und Risiken von Künstlicher Intelligenz zu reflektieren, ohne sich dabei in Diskussionen über ihre technische Umsetzung zu verlieren.[10] Die Aktualisierung dieses Systems befindet sich in der Planung. Für die Bundeswehr ergibt dies verschiedene Herausforderungen und Chancen in Bezug auf KI-Anwendungen. Daten in guter Qualität sind die Grundlage für erfolgreiche KI-Anwendungen und erfordern ein intelligentes Datenmanagement als solides Fundament. Das Datenmanagement muss die Daten so orchestrieren und zur Verfügung stellen, dass die jeweilige KI-Anwendung optimal darauf zugreifen

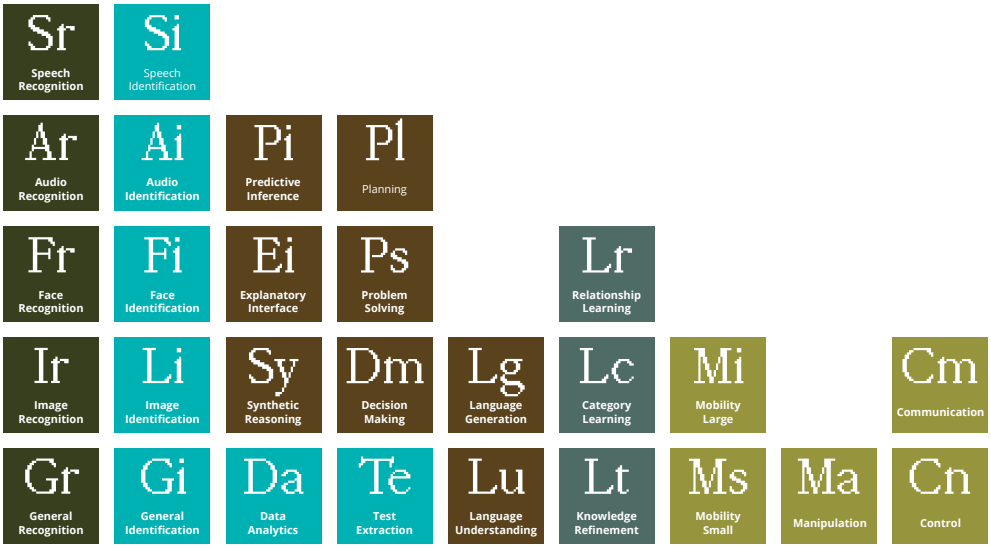
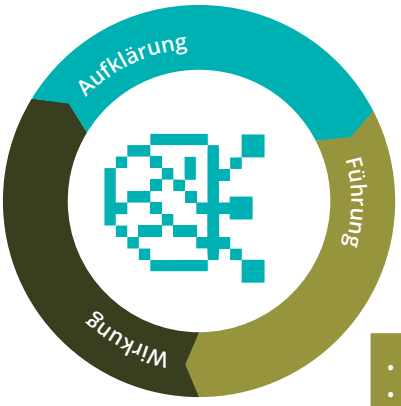


Abbildung 2: Periodensystem der Künstlichen Intelligenz. Quelle: bitkom e. V.

kann. Daher müssen Datenmanagement und KI-Anwendung gut aufeinander abgestimmt sein. Die Komplexität von Prozessen und der sie abbildenden Verfahren nehmen dabei stetig zu. Dies umfasst unter anderem die Menge der gespeicherten und übermittelten Daten. Auch die Wichtigkeit von Informationen zur und während der Verarbeitung nimmt durch immer bessere Sensoren weiter zu. Dabei sind die Personalressourcen für Verfahrensbearbeitungen begrenzt und werden zunehmend geringer. Daraus gewonnene Ergebnisse müssen gleichzeitig immer schneller bewertet werden und bedürfen analytischer und kognitiver Unterstützung beim Entscheidungsfindungsprozess. Schließlich werden sogenannte Robotics-Szenarien und damit einhergehende automatisierte und autonome Anwendungen diskutiert beziehungsweise befinden sich diese weltweit in der Erprobung. Somit besteht die Gefahr, technologisch abgehängt zu werden und einen taktischen Nachteil im Gefecht zu erhalten. Die Bundeswehr beziehungsweise die sie führenden politischen Vertreterinnen und Vertreter müssen daher grundsätzliche Überlegungen für Arbeitsabläufe und Verfahren für KI-Technologien definieren. Dies bedarf der Erarbeitung entsprechender Cluster, um Priorisierungen zum Einsatz von KI-Technologien vorzunehmen und das intelligente Datenmanagement danach auszulegen. Auf der Fachebene erarbeitete Standards sollten auch die



- Lagezentrum / Systeme zur Entscheidungsunterstützung: Automatisierte Lagebilderstellung und -bewertung auf Gefechtsfeldern
- Gegnersimulation
- Systeme zur Entscheidungsunterstützung in der Operationsführung

- Krisenfrüherkennung
- Bild- und Mustererkennung
- Automatisierte Aufklärungssysteme inkl. Sensorfusion
- Gegneranalyse
- Automatisierte und autonome Aufklärungssysteme inkl. Sensorfunktion
- Prädikative Gegneranalyse

- Schutzsysteme; z.B.: Luftverteidigung, aktive Land-Schutzsysteme, Counter-IED, Drohnenabwehr, Feldlagerschutz
- Verbesserte Zieldiskriminierung
- Kampfmittelräume
- Manned-Unmanned Teaming; z.B.: FCAS, UAV und MGCS
- Sensor-to-Shooter-Verbund
- Schwarmsysteme

Abbildung 3: KI-Anwendungen in der Bundeswehr Aufklärung – Führung – Wirkung. Quelle: bitkom e. V.

Nachvollziehbarkeit und Transparenz von Algorithmen einbeziehen, wobei nötige ethische, datenschutzrechtliche und beschaffungsrelevante Standards Berücksichtigung finden. Eine Übersicht möglicher KI-Anwendungen in der Bundeswehr bieten Abbildung 3 und Abbildung 4, die der Arbeitskreis Verteidigung des Bitkom 2019 erarbeitete.[11]

Insbesondere auf dem Gefechtsfeld werden Anfragen an die Automatisierung und der Einsatz von KI-Anwendungen immer aktueller, entgegen derzeitigen politischen Entscheidungen. In der analogen Welt erfolgte der Informationsaustausch für eine nötige Lageanalyse und daraus folgenden Handlungen über Menschen. Somit war die Reaktion auf Ereignisse eine Frage von Entfernungen, Ausbildung und der Kommunikationstechnik. Moderne Gefechtsführung

Abbildung 4: KI-Anwendungen im Unterstützungsbereich der Bundeswehr.
Quelle: bitkom e. V.

umfasst eine sehr hohe Informationsdichte, die automatisiert von diversen Sensoren erfasst wird. Die Informationsüberlegenheit und die Schnelligkeit bei der Auswertung von Daten beziehungsweise die Überführung der Daten in Aktionen, sind entscheidend für den Erfolg.

Menschen sind zunehmend nicht mehr in der Lage, diese Informationsflut der Sensoren zu erfassen und auszuwerten, um zeitnah Handlungsanweisungen an Effektoren, wie zum Beispiel die Artillerie oder Abwehrsysteme, zu übermitteln. Zukünftig kann eine automatisierte Auswertung erforderlich sein, um die nötige Geschwindigkeit zu erreichen. KI-Anwendungen spielen hier eine

entscheidende Rolle, vor allem bei Abwehrsystemen. So bräuchten zum Beispiel herkömmliche Atomraketen aus Russland gerade einmal 106 Sekunden bis nach Berlin. Hyperschallwaffen brauchen einen Bruchteil dieser Zeit. Menschliches Reaktionsvermögen kann dies, vorausgesetzt die dazu nötige Technologie steht zur Verfügung, nicht bewältigen.

Der Aufbau solcher Wirkungsketten, sogenannter Sensor-Effektor-Ketten, ist nicht leicht, jedoch technisch möglich. Zunächst gilt es, eine Zielaufklärung auszuwerten. Dazu müssen Sensoren Objekte richtig erkennen und identifizieren können. Im zweiten Schritt erfolgt eine Sensordatenfusion, wobei Informationen für ein Lagebild aufbereitet beziehungsweise verworfen werden. Die heutige Technik ist dabei weit fortgeschritten. KI-basierte Bildanalysen haben mittlerweile eine Fehlerquote von unter drei Prozent. Die menschliche Fehlerquote liegt bei circa fünf Prozent. Insgesamt sind Sprach-, Bild- und Videoanalyse mittlerweile so gut, dass sie real eingesetzt werden können. Im zivilen Bereich ist dies in den USA zu sehen, wo autonome Fahrzeuge einen weit fortgeschrittenen Teststand haben. In Deutschland fokussieren sich die Kritisierenden meist auf spezifische Szenarien, die natürlich auch ethischer Überlegungen bedürfen. Der Mehrwert, den KI jedoch leisten kann, sollte hier auch berücksichtigt werden. Wir benötigen dazu eine Chancen- und keine Risikodebatte. So wird unter anderem die Frage gestellt, wie sich KI bei einem Ausweichmanöver entscheidet. Die Tatsache, dass dies ein moralisches Dilemma ist, was nicht einmal Menschen lösen können, wird dabei vernachlässigt. Die Basis bietet die Programmierung und nicht eine freie Entscheidung der KI.

Sind das militärische Ziel erkannt und das Lagebild erfasst, folgt eine Zielzuweisung für das gerade verfügbare Wirkmittel. Diese Schritte erfolgen automatisiert. Der danach folgende Einsatz von Waffen bietet die Möglichkeit einer menschlichen Kontrolle, dem *Human in the Loop*. Abwehrsysteme, die eine Reaktion innerhalb von Sekunden verlangen, bieten wenig Spielraum für menschliche Beteiligung. Abwehrsysteme wie Grenzsicherungsanlagen, die zeitliche Spielräume erlauben, lassen den *Human in the Loop* jedoch zu. Es geht somit um die Dringlichkeit einer Entscheidung. Der Einsatz von Offensivwaffen für die Bekämpfung eines Ziels bietet hingegen einen gebotenen Einsatz eines menschlichen Entscheidenden. Jedoch

ist auch hier zu berücksichtigen, dass es auf das Szenario ankommt. Entwicklungen bei Drohnen auf dem Gefechtsfeld spiegeln dieses Dilemma wider. Heutige Szenarien umfassen den Einsatz einzelner Drohnen, die durch Operierende gesteuert und somit kontrolliert werden. Zukünftige Szenarien sehen vor, dass der Erfolg auf dem Gefechtsfeld nur durch eine Überforderung der gegnerischen Abwehrsysteme möglich ist. Dies können unter anderem Drohnenschwärme sein, die mehrere Dutzend oder gar Hunderte Drohnen umfassen. Die Steuerung einzelner Drohnen durch Operierende wird somit zu einem komplexen und nicht koordinierbaren Unterfangen. Dazu nötige Militärstrukturen, wie Kommandozentralen, sind durch ihre digitalen Spuren leichte Ziele für Gegner. Wann und ob Menschen in den Entscheidungsprozess involviert werden, muss durch das Primat der Politik geklärt werden. Festzuhalten ist: Das technisch Machbare hat bereits den Sachstand der theoretischen Debatte zum Einsatz von KI-Anwendungen, zumindest beim Einsatz von Waffengewalt, überholt. Im Wettstreit der Wertesysteme ist fraglich, ob autoritäre Staaten diese Debatte ebenso führen.

KI und Ethik – eine Gegenüberstellung mit den Grundsätzen der Inneren Führung

Die Grundsatzfrage lautet: Gibt es eine Abwägung zwischen der Schlagfertigkeit im Verteidigungsfall und einer soliden Ethik von KI?

Intelligente Systeme werden zukünftig in vielen Lebensbereichen Entscheidungen (selbstständig) treffen und damit die Handlungsfähigkeit und Handlungsmächtigkeit jedes und jeder Einzelnen beeinflussen. Die zentrale ethische Herausforderung wird sein, intelligente Systeme humangerecht und werteorientiert zu gestalten. Das heißt, das Ziel der technologischen Entwicklung sollte sein, nicht nur Prozesse zu optimieren und ökonomische Effizienz zu erzielen, sondern auch, die Lebenssituation der Menschen zu verbessern, ihre Handlungsmöglichkeiten zu erweitern und ihre Autonomie zu wahren. Eine humangerechte Einbindung intelligenter Systeme in hochkomplexen Gesellschaften ist keine individuelle Angelegenheit, sondern eine gesamtgesellschaftliche Aufgabe. Deshalb braucht es einen gesellschaftlichen Konsens darüber, wie die

Mensch-System-Interaktion kontrollier- und steuerbar ist. Hilfreich hierfür ist die Digitale Ethik, da sie als Navigationsinstrument diesen Prozess durch Reflexion, Orientierung und Moderation steuern kann. Praktisch gesehen kann sie Empfehlungen für (selbst-)regulative Vorgaben und ethische Kodizes zur Verfügung stellen.[12] Dazu gehören im Wesentlichen folgende gesamtgesellschaftliche Fragen:

Chancengleichheit
Wie kann sichergestellt werden, dass durch automatisierte Entscheidungen keine Diskriminierung von Personen aufgrund ihres Geschlechts, ihrer ethnischen Herkunft, religiösen Zugehörigkeit, ihrer sexuellen Orientierung und politischen Überzeugungen erfolgt? Automatisierte Entscheidungen können beispielsweise Auswirkungen auf Einzelne nehmen. KI-Systeme im Personalbereich der Bundeswehr können zum Beispiel Einfluss auf Lebenswege et cetera nehmen.

Informationsfreiheit, Informationsvielfalt und freie Meinungsbildung
Wie kann ein freier Zugang zu Informationen garantiert werden und wie können Personen vor Falschmeldungen und Manipulation geschützt werden? Beispielsweise könnten KI-Anwendungen zur Unterstützung von Ausbildungsmaßnahmen in der Bundeswehr, wie bei der politischen Bildung, die freie Meinungsbildung ermöglichen aber auch verhindern. Zweckdienliche Informationen der politischen und militärischen Führung könnten so aufbereitet werden, dass ein erwünschtes Verhalten initiiert wird. Dies würde den Prozess der freien Meinungsbildung als Basis der Inneren Führung unterlaufen.

Privatsphäre und Datenschutz
Wie soll der Eingriff intelligenter Systeme in die Privatsphäre geregelt werden? Wie kann Transparenz über Datenerhebung und Nutzung sichergestellt werden? Wie können Mensch-Maschine-Interaktionen durch Daten verbessert werden? Intelligente Systeme sind kontextsensitiv, verhalten sich adaptiv und erfassen Nutzeridentitäten. Beispielsweise benötigen intelligente Systeme in der medizinischen Versorgung sensible Daten. Soldatinnen und Soldaten könnten somit

einfach als Nummer im System behandelt werden beziehungsweise bei einer medizinischen Versorgung. Das Individuum rückt so in den Hintergrund.

Arbeitsplätze und Arbeit 4.0
Was kann die Bundeswehr tun, damit die Attraktivität mit New Work gesteigert wird, es aber nicht zu einem sozialunverträglichen Abbau von Verwaltungsstellen kommt, die dank der Digitalisierung eingespart werden könnten.

Bildung
Welche Digitalkompetenzen braucht es, um souverän und verantwortungsbewusst mit den vielfältigen Möglichkeiten digitaler Technologien umgehen zu können?

Die zentrale ethische Herausforderung ist es, intelligente Systeme humangerecht und werteorientiert zu gestalten, damit sie die Lebenssituation der Menschen verbessern, ihre Handlungsoptionen erweitern und ihre Autonomie wahren.

Die durch Big Data und KI im Gange befindlichen und bevorstehenden Veränderungen sind fundamental und unumkehrbar. Mit diesem Algorithmic Turn sind sowohl Narrative der Risiken als auch der Chancen (zum Beispiel Effizienzsteigerung, Fortschritt in der medizinischen Diagnostik, Entlastung von mühseliger Arbeit, Effektivitätsvorteile auf dem Schlachtfeld et cetera) verknüpft. Um in der Praxis intelligente Systeme humangerecht zu gestalten, bedarf es einer Verständigung darüber, welche Prinzipien gelten sollen, wie sie entwickelt werden können und wie eine Systemkontrolle möglich ist.

Bezogen auf das Militär bringt die Digitalisierung und mit ihr die Anwendung von KI-Lösungen ein altes Dilemma der Inneren Führung der Bundeswehr zum Tragen. Der Fokus auf Effizienz und Effektivität im Kampf bringt stark vereinfacht das Spannungsfeld zwischen Wolf von Baudissin und Heinz Karst, zwei Vordenkern der Inneren Führung der Bundeswehr, zum Vorschein. Von Baudissin setzte Bürgerinnen und Bürger voraus, die sich zur Wahrung des Friedens und zur Verteidigung der Freiheit einsetzen würden, wobei die Bundeswehr

einen Beitrag zur politischen Formung von Staatsbürgern in Uniform leistet und die Bundeswehr eher als Behörde betrachtet wurde. Karst stellte eher den „Kämpfer" in den Vordergrund, der durch die Streitkräfte geformt werde, mit dem Zweck, dass diese Armee kriegstauglich sei. Diesem Ziel sollte sich alles andere unterordnen. Eine ethische Debatte zum Einsatz von KI-Anwendungen im Militär sollte beide Aspekte beinhalten: den Einsatz letaler automatisierter Waffen mit Beteiligung von KI, um im Systemwettstreit physisch bestehen zu können sowie KI-Lösungen im Bereich des Arbeitsalltags in der „Behörde Bundeswehr". Ethik muss dabei normative Standards und moralisches Handeln begründen und das Handeln nach dem inneren Kompass steuern können. Dabei müssen je nach Anwendungsfällen von KI-Lösungen verschiedene Perspektiven berücksichtigt werden. Im Zentrum dieser Überlegungen stehen die Begriffe Fürsorge, Autonomie des Handelns, Nichtdiskriminierung und Transparenz für diese Anwendungen. Hier könnte zum Beispiel eine Ethikkommission aus Bundestag, Bundeswehr, Wirtschaft und Wissenschaft die Grundlagen legen und somit endlich Fakten schaffen, da das Thema bereits seit Jahren ohne Ergebnis diskutiert wird. Dies könnte die Innovation maßgeblich beschleunigen.

Innovation beschleunigen – Digitales Mindset entwickeln

Eine Organisationskultur lässt sich nicht ohne Weiteres ändern. Dabei erstellen Organisationen oft Leitbilder, Strategien und Gremien zur Implementierung und Begleitung eines Kulturwandels. In der Regel erfolgt dies mit einem Top-down-Ansatz. Das kann jedoch nur ein erster Schritt sein. Organisationskulturen bestehen aus einem komplexen Geflecht von Regelungen, Gewohnheiten, offiziellen und informellen Netzwerken. Eine Organisation wie die Bundeswehr ist eingebettet in diverse Stakeholder-Strukturen aus Politik, Recht und Gesellschaft sowie internen Subkulturen, die man durch die Begriffe „Kämpfende" und „Beamte" kennzeichnen könnte. Diese ließen sich noch weiter aufteilen. Hinzu kommen in jeder Organisation menschliche Verhaltensweisen, die meist auf individueller Wahrnehmung, persönlichen Zielen und Werten basieren. Es gilt somit, einen Rahmen zu setzen, der die individuellen Bedürfnisse einer Person vor dem Hintergrund der strategischen Ziele der Organisation

anspricht und zur Mitarbeit an Organisationsvisionen anregt. Es bedarf daher einer Analyse vorhandener Kulturen innerhalb der Bundeswehr und die Festlegung einer Zielkultur, die zum Beispiel mit der S.M.A.R.T-Methode (Spezifisch, Messbar, Attraktiv, Realistisch, Terminiert) angegangen werden kann. Hier bieten die Innere Führung und abgeleitete Konzepte wie die Auftragstaktik (*Management by Objectives*) sehr gute Ansätze. Die Grundzüge einer agilen Unternehmenskultur, die Innovationen zulässt, sind bereits dort angedacht. Die Gründerväter des Konzepts der Inneren Führung haben somit vor über 70 Jahren eine moderne Kultur erschaffen. Diese muss jedoch auch gelebt und weiterentwickelt werden, denn auch die Gesellschaft ist im Wandel. Der Digitalbericht des BMVg 2022 skizziert die Grundsätze eines digitalen Mindsets auf Basis einer Bundeswehr internen Befragung mit den Schlagworten Innovationsfreude, Technologieaffektivität, Agilität, Eigenverantwortung, Risikofreude, Veränderungsbewusstsein, Vernetzung, Digital Leadership, Sicherheitsbewusstsein und Ethik.[13] Diese Punkte lassen sich ohne Weiteres auf den Soldatenberuf, für die Subkultur der Kämpfenden, übertragen, da diese in agilen Situationen genau diese Eigenschaften benötigen. Dabei muss jedoch klar sein, dass moderne Streitkräfte umfassend gebildet sein sollten. Dazu gehören wirtschaftliche, politische und technologische Aspekte. Die reine Fokussierung auf das Militärhandwerk führt in eine Sackgasse. Der Militärhistoriker Prof. Sönke Neitzel postuliert in seinem Werk „Deutsche Krieger“ unter anderem, dass einer der Gründe für die Niederlage im Ersten Weltkrieg war, dass die Armee gesellschaftliche, wirtschaftliche und politische Aspekte nicht adaptieren konnte und sich nur auf das Militärische fokussierte. So warnte bereits General Moltke Ende des 19. Jahrhundert im Reichstag, dass der kommende Krieg ein Krieg der Volkswirtschaften werde, bei dem die Seite siegt, die wirtschaftlich am durchhaltefähigsten ist. Adaptiert auf die Zeitenwende 2022 in der Verteidigungspolitik stellt sich auch heute die Frage, wie leistungsstark die jeweiligen Industrien der Antagonisten der Wertesysteme sind. Deutschland ist traditionell in hohem Maße abhängig von Rohstoffen und aufgrund seiner globalen Verflechtungen anfällig für die Störung von Lieferketten. Es gilt daher, zunehmend in einer Kreislaufwirtschaft zu denken, die nachhaltig agiert. Technologisch steht Deutschland gut da, gerät jedoch insbesondere bei der Digitalisierung zunehmend ins Abseits. Über 60.000 IT-Unternehmen in Deutschland liefern Innovationen, jedoch

gelingt es ihnen kaum, zu Großkonzernen zu wachsen. Insbesondere auf dem international wichtigsten IT-Markt, den USA, haben sie es schwer, da Made in Germany eher mit Hardware verbunden wird. Hier bedarf es politischer Initiativen und vor allem Visionen seitens der Politik, die der Digitalisierung einen entscheidenden Schub verleihen. Ein engerer Verbund aus Politik, Wirtschaft und Wissenschaft, wobei ein Agieren auf Augenhöhe erfolgt, ist hierbei nötiger als je zuvor. Technologieführerschaft kann auch andere Schwächen in Deutschland, zum Beispiel die Alterung der Gesellschaft und deren Folgen, entscheidend begegnen. Bezogen auf die Bundeswehr muss die Digitalisierung nicht nur als Top-down-Ansatz nach Fähigkeitsbedarfen erfolgen. Es benötigt auch eine Einbindung der Nutzerinnen und Nutzer, Soldatinnen und Soldaten bei der Eingabe von Bedarfen und von Innovationsideen. Dabei stehen auch die Interoperabilität zur EU und NATO sowie gängige Industriestandards im Fokus. Kooperationsformate wie der „Cyberinnovation Hub“ der Bundeswehr, mit Industrievertreterinnen und -vertretern sowie Start-ups und KMU sollen dies stärken und den Austausch zu relevanten State-of-the-Art- und Zukunftslösungen fördern. Der Bitkom unterhält daher zum Kommando Cyber- und Informationsraum sowie zum entstehenden Zentrum Digitalisierung, Dimension Land sowie zu weiteren Formaten der Sicherheitsbehörden Kooperationsformate, um Bedarfe der Amtsseite auf neutralem Boden mit Wirtschaft und Wissenschaft gemeinsam zu diskutieren. Beim Bottom-up-Ansatz sollte auch die Forschungslandschaft stärker eingebunden werden. Die Bundeswehr verfügt mit ihren Universitäten und anderen Laboren et cetera über sehr gute Ideenstätten. Diese sollten noch mehr praxisorientiert mit der Wirtschaft verzahnt werden, was in Ansätzen bereits geschieht.

Im 19. Jahrhundert prägte das Militär Innovationen für die Zivilgesellschaft. Heute ist dies in Deutschland umgekehrt. Dabei werden die Innovationszyklen immer schneller. Dies erfordert Anpassungen von Kommunikations-, Innovations- und Vergabestrukturen von Streitkräften hin zu agilen Strukturen. Dazu ist auch eine interne Abstimmung von Politik, der Behörde Bundeswehr und der Bundeswehr als Armee nötig, bevor die Kooperation mit externen Akteuren verbessert werden kann. Dort agieren oftmals viele Projekte und Ansprechpartner parallel. Das Denken in Silos der eigenen Teilstreitkräfte und Organisationsbereiche muss zu einem vernetzten

Denken verbunden werden. Insbesondere bei der IT sind einheitliche Strukturen wesentlich effizienter. Aufseiten der Wirtschaft bedarf es der Fähigkeit, sich an die speziellen Herausforderungen des Militärs anzupassen, Transparenz der Lieferketten zu klären und auch bei der Software keine Blackboxes zu schaffen, zum Beispiel bei der Nutzung von Open Software zugänglichen Source-Code-Control-Systemen wie Git oder Subversion, unterschiedliche Code-Stränge für stabile Releases und die laufenden Entwicklungen, klare Releases, öffentlich verfügbare Mailinglisten, Bugtrackingsysteme, Wikis und so weiter. Ein gutes Open-Source-Software-Projekt wird mithin in der Öffentlichkeit entwickelt, nicht hinter verschlossenen Türen.[14] Gegenseitiges Vertrauen sowie Vertraulichkeit und Sensibilität für die gegenseitigen Bedürfnisse sind der Schlüssel zum Erfolg. Nur wenn alle vom gleichen digitalen Mindset und dem Willen zur Innovation sprechen, mit dem Anspruch auf Augenhöhe zu agieren, lassen sich Innovationen wie KI-Anwendungen für das Militär zeitnah erschließen. Erfolg im Systemwettstreit hat, wer die Potenziale der Digitalisierung versteht und zu orchestrieren vermag, unter Berücksichtigung der gesellschaftlichen Grundwerte, für die die Innere Führung der Bundeswehr eintritt.

1 Bitkom (2017). Künstliche Intelligenz Wirtschaftliche Bedeutung, gesellschaftliche Herausforderungen, menschliche Verantwortung. Bitkom e. V., Berlin, S. 25.

2 Ebd., S. 21.

3 Ebd., S. 36.

4 Ebd., S. 18.

5 Bitkom (2022b). Kampf gegen Fachkräftemangel: Drei Viertel der Unternehmen brauchen IT-Spezialistinnen. In: Bitkom.org. https://www.bitkom.org/Presse/Presseinformation/Kampf-gegen-Fachkraeftemangel-mit-IT-Spezialistinnen (letzter Aufruf: 29.9.2022.)

6 RND (2022). Ukraine-Krieg: Russland fehlen wegen Abwanderung 170.000 IT-Kräfte. In: *rnd.de*. https://www.rnd.de/wirtschaft/ukraine-krieg-russland-fehlen-wegen-abwanderung-170-000-it-kraefte-2OQPDVWR4HOW5CRJZDBEDPBLDI.html (letzter Aufruf: 29.9.2022.)

7 Bitkom (2022b), S. 58ff.

8 Bitkom (2022). 203 Milliarden Euro Schaden pro Jahr durch Angriffe auf deutsche Unternehmen. In: Bitkom.org. https://www.bitkom.org/Presse/Presseinformation/Wirtschaftsschutz-2022 (letzter Aufruf: 29.9.2022.).

9 Bitkom (2017), S. 14ff.

10 Bitkom (2022c). Das Periodensystem der Künstlichen Intelligenz. In: Periodensystem-ki.de. https://www.periodensystem-ki.de/ (letzter Aufruf: 29.9.2022.).

11 Bitkom (2022d). Aktualisierter Technologiesteckbrief Künstliche Intelligenz. Bitkom e. V., Berlin.

12 Intelligente Systeme können dem Wohl des oder der Einzelnen und der Gesellschaft dienen – vorausgesetzt, dass die Risiken frühzeitig und kontinuierlich in den Blick genommen werden.

13 BMVg (2022). Vierter Bericht zur Digitalen Transformation des Geschäftsbereichs des Bundesministeriums der Verteidigung. Bundesministerium für Verteidigung, Berlin, S.18.

14 Bitkom (2022e). Open-Source-Leitfaden. Praxisempfehlungen für Open-Source-Software Version 3.0. In: Bitkom.org. https://www.bitkom.org/sites/main/files/2022-06/220624-Bitkom-Leitfaden-Open%20Source-3.0_0.pdf (letzter Aufruf: 29.9.2022), S. 18.