Digitalisierung führt aufgrund ihrer Querschnittlichkeit und breiten Anwendungen die Wissenschaften notwendigerweise zusammen. Die militärische Anwendung ist dabei kein Sonderfall, benötigt aber besondere Betrachtungen zu Verantwortung, Ethik und Führung. Der Mensch, die Technologie und die Ethik werden hierdurch aufeinander hingeordnete „Bereiche". Datenzentriertheit und ein Cyber-Umfeld erfordern eine neue Form der Resilienz. Zugleich ist Führung – bei Erhalt einer Auftragstaktik – an ein digitales Umfeld deutlich zu verändern.

Digitalisierung der Streitkräfte – Ein (nicht nur) technischer Blick

Generalleutnant Dr. Ansgar Rieks

Prolog: Von der Dominanz der Perspektive

Öffentliche Diskussionen leben vom Diskurs. Bei Fernsehdiskussionen werden die Diskutantinnen und Diskutanten ausgewählt, um „unterschiedliche“ Perspektiven mit- und einzubringen. Im besten Fall entsteht ein interessanter Schlagabtausch, der es den Zuschauerinnen und Zuschauern ermöglicht, Argumente zu sammeln und sich eine eigene Meinung zu bilden. Ein allzu starker Schlagabtausch kann aber auch darin münden, dass man sich angesichts von fehlender Kongruenz abwendet. Übrigens gilt dies nicht nur für Fernsehdiskussionen, sondern auch für Veranstaltungspanels, Katholikentage oder Foren, wer auch immer sie wirklich offen organisiert.

Angenehmer ist es, Fachleute „vom gleichen Schlage“ einzuladen und sie vor einem Publikum mit gleicher Zielrichtung und gleichem Interesse vortragen zu lassen. Die schon vorher gefühlte Dominanz der eigenen Perspektive wird als Ergebnis bestätigt, gestärkt und als „gesetzt“ fixiert. Das ist angesichts von Fachlichkeit, komplexen Wissenschaften und Detailtiefe wichtig. Die Wissenschaften scheinen immer weiter auseinanderzudriften, sind zunehmend nur „in sich“ schlüssig und wirken oft gekapselt. Zudem wird es schwerer, sich anderen Wissenschaften zuzuneigen und sie zu durchdringen. Das gilt für Technologie, Geisteswissenschaft, und ich zähle dazu auch die Militärwissenschaft und die Ethik, will man sie als „Wissenschaften“ mit verstehen – was sicher weder Soldatinnen und Soldaten noch Ethikerinnen und Ethiker verneinen würden.

Herausforderungen oder Probleme kommen auf, wenn ein zu bewertendes Thema nicht klassisch aus einer dieser Wissenschaften stammt, sondern querschnittliche Bedeutungen bekommt oder hat.

Digitalisierung und all die damit verbundenen Elemente stellen ein solches Thema dar. Sie ist zu einem übergroßen Thema der technologischen Weiterentwicklung geworden (das Zeitalter der Daten ist angebrochen); sie ist für die Fähigkeitsentwicklung der Streitkräfte ein unabdingbarer Baustein geworden (um gegen einen potenten Gegner bestehen zu können); sie eröffnet neue Forschungsfelder (von der Künstlichen Intelligenz über die Automatisierung bis hin zu Quantentechnologien); und sie erzeugt neue ethische Fragen (Wo bleibt der Mensch in einer digitalisierten Welt?). Digitalisierung bedarf des Diskurses. Dieses Buch trägt dazu bei.

Eine zusätzliche Herausforderung entsteht, wenn am Ende eines Diskurses ein Ergebnis stehen muss. Dies ist bei der Entwicklung und Realisierung von Fähigkeiten der Streitkräfte der Fall. Diese Fähigkeiten besitzen „ein scharfes Ende", einen möglichen Waffeneinsatz. Sie sind sogar daraufhin ausgerichtet. Das macht es nicht nur in allen zum Tragen kommenden Wissenschaften kompliziert, es verhindert auch eine zeitlich ausufernde oder unbegrenzte Diskussion. Am Ende – und dieses Ende ist immer absehbar – bedarf es eines „Ja", gegebenenfalls mit einigen Rahmenbedingungen, oder eines „Nein" – letztlich eines politischen Entscheids. Um einen solchen herbeizuführen, bedarf es der Befassung mit allen oben aufgeführten Perspektiven, eines zumindest „verstehenden Sachverstands" sowie der Akzeptanz und Einbeziehung aller beteiligten Wissenschaften.

Es gibt nur wenige Menschen, die das wirklich leisten können. Als technisch ausgebildeter Soldat ist es „angenehm", über die „technische Umsetzung im militärischen Bereich" in diesem Kapitel zu schreiben. Ich bin mir aber bewusst, dass viele andere Perspektiven dabei nur berührt werden können. Deshalb wird das Weitere nur partiell und persönlich sein, aber vielleicht gerade dadurch „ein" Beitrag.

Die digitale Transformation für die Streitkräfte

Jede militärische Perspektive geht vom Auftrag aus. Dieser wiederum leitet sich bei der Landes- und Bündnisverteidigung von der Bedrohung ab, bei friedensschaffenden und -sichernden Aufträgen von weiteren Rahmenbedingungen. Ganz generell ist die

Der Mensch wird in ein neues Zusammenwirken mit der Technik auch im militärischen Bereich eintreten. Er wird „in the Loop“ bleiben, auch wenn sich der Loop verändert. Technik, Führung und der Mensch bleiben aufeinander hingeordnet.

Notwendigkeit einer modernen Bundeswehr – und damit der Verwendung von Digitalisierung – heute davon abhängig, dass wir es mit modernen und fähigen Gegnern zu tun haben. Führen, Aufklären, Wirken und Unterstützen (FAWU, wie wir die Fähigkeitskategorien zusammengefasst nennen) sind zweifellos von der Digitalisierung betroffen. Sie waren es bereits in der Vergangenheit bei der Entwicklung neuer Technologien. Aber die Digitalisierung ermöglicht mehr als diese Entwicklungen eine ganzheitliche Durchdringung und vielfältige Anwendung. Das ist der Fall, da Digitalisierung in sich selbst vielfältig ist. So sehen wir sie etwa als „Allheilmittel" und sind hoffnungsfroh, dass sie uns „das Problem schon lösen wird". Ein gewisses Maß an Euphorie geht damit einher. Das leitet zumeist in ein intensives Nachdenken über, wenn das „Wie" – jenseits der *Buzzwords* – und zugleich der „Umgang" mit der Digitalisierung bestimmt werden müssen. Die Herausforderung liegt darin, aus dem Baukasten der digitalen Technologien das richtige Werkzeug herauszufinden und es zielgerichtet in die Fähigkeitsentwicklung einzubeziehen, sodass der Operateur seinen Auftrag besser erfüllen kann. „Besser" kann dabei mit Adjektiven beschrieben werden. Sie sind: durchsetzungsfähiger, präziser, schneller, mit besserem Lagebild, effizienter, über weitere Entfernungen und sicherer für die Soldatinnen und Soldaten im Einsatz –, alles in einem Cyberumfeld. Bei Letzterem kann man feststellen, dass die digitale Entwicklung nicht nur Probleme löst, sondern auch neue Herausforderungen schafft.

Die militärische Anwendung – ein Sonderfall?

All diese „verbesserten" Eigenschaften in der militärischen Auftragserfüllung sind bei unterschiedlichen Anwendungen im zivilen Bereich ebenfalls zu finden oder anzustreben. Es gibt zunächst keine grundlegenden Unterschiede, ob die Digitalisierung in den zivilen oder militärischen Bereich Einzug hält. Schließlich unterstützt sie die angestrebte Verbesserung der Fachlichkeit. Und in beiden Bereichen erzeugt sie einen enormen „Transformationssprung", der technisch, prozessual und mit Blick auf die Menschen große Veränderungen bringt. Das betrifft auch die Qualifizierung und Zulassung sowie alle Rahmenbedingungen, die ungewollte Effekte ausschließen. Dennoch sind militärische Anwendungen ein Sonderfall, weil sie bis in den

Waffeneinsatz reichen und damit letale Wirkung haben. Die Bandbreite der Anwendungen reicht von der Auswertung großer Mengen von Daten für administrative Zwecke bis hin zur Schaffung Letaler Autonomer Waffensysteme (LAWS). Der „Sonderfall der militärischen Anwendung" muss also eingeordnet werden, ob, wann und wie die Digitalisierung in der Anwendung hilfreich und sinnvoll ist, sie ethisch akzeptabel, gesetzlich konform und politisch durchsetzbar ist.

Diese vier Perspektiven (militärisch, ethisch, gesetzlich und politisch) führen nicht immer zu gleichen Ergebnissen. Sie werden sogar oft miteinander verschränkt und gegenseitig verwendet. Ein klares Bild entsteht nur, wenn man diszipliniert unterscheidet und am Ende vor diesem Hintergrund eine Entscheidung fällt. Diese besteht nicht aus einer Ja-Nein-Alternative, sondern aus gesetzten Rahmenbedingungen, unter denen eine Anwendung stattfinden kann. Zwei Rahmenbedingungen bei der Anwendung von technischen Entwicklungen im militärischen Bereich sind in unserer Ausrichtung, dass autonome Waffensysteme ohne den Einfluss eines menschlichen Entscheiders oder einer menschlichen Entscheiderin in Deutschland ebenso abgelehnt werden wie ein gezieltes Töten von Menschen, ohne dass von ihnen Gefahr ausginge. Bei der Anwendung und Zulassung neuer Technologien im militärischen Bereich – insbesondere der Digitalisierung – gilt daher eine besondere Sorgfalt. Sie wird zusätzlich mit einer weiteren politischen *Firewall* versehen, da das Parlament den Einsatz und die zugehörigen Einsatzregeln im jeweiligen Fall billigt.

Der autonom wirkende Mensch und die intelligente Automatisierung

Diese grundsätzlichen Überlegungen führen unmittelbar zu der Frage, wie der Mensch einer fortschreitenden Digitalisierung und (dadurch) Automatisierung gewachsen bleibt und sie weiterhin dominieren kann. Zugleich ist zu beantworten, wie sehr die Digitalisierung der Streitkräfte die Führungsphilosophie verändern darf oder gar soll. Hierbei liegen die grundsätzlichen Meinungen innerhalb und außerhalb der Streitkräfte weit auseinander. Sie variieren von einem Festhalten an allen Elementen der Inneren

Führung bis zur Notwendigkeit einer weitgehenden Neufassung. Und zugleich liegen oft geäußerte Deklarationen und Beurteilungen von Details auseinander.

Es geht um folgende vier Fragen:

- Muss der Mensch immer die Entscheidung haben, oder kann ein *Ethical Design* ihn übersteuern? – Wären viele Gräueltaten von Menschen überhaupt vorgekommen, wenn der Mensch gerade nicht der Allentscheider gewesen wäre?

- Wo liegt der Grad der Automatisierung, selbst wenn der Mensch durch ein *In the loop*-Sein der Letztentscheider ist? Wenn ein automatisches Starten und Landen eines Luftfahrzeugs mit einem Piloten oder einer Pilotin an Bord, der/die jederzeit eingreifen kann, heute akzeptiert ist, kann dieses auf einen Waffeneinsatz übertragen werden?

- Wie verändern sich Führungsprozesse, wenn Informationen schneller, umfangreicher, ausgewerteter und präziser sind als bisher? – Wie viel Entscheidungsautonomie kann hierdurch auf die taktische Ebene delegiert werden und welche Entscheidungen bleiben höheren Führungsebenen (mit welchen Zyklen) überlassen? (Diese Frage ist besonders angesichts einer Multi-Domain-Führungsphilosophie zu stellen, die alle Dimensionen einbezieht.)

- Und letztlich: Bleibt der Mensch in einer immer komplexer werdenden Daten- und Digitalisierungswelt überhaupt in der Lage, diese steuernd zu bewältigen?

Diese Fragen sind bisher nicht ausreichend diskutiert worden, um hier eine Antwort in einem „gemeinsamen Zielkreis“ geben zu können. Zugleich darf eine andauernde Diskussion nicht den Fortschritt verhindern, will man die eigene Entwicklung nicht unterbrechen oder so verlangsamen, dass sie nicht mehr Schritt hält. Daher ist auch jeder subjektive substanzielle Einzelbeitrag wichtig, bevor in jeder Frage deutlich gegeneinanderstehende Pole eine Lösung erschweren oder unmöglich machen. Es ist stets dasselbe Ziel

zu verwirklichen: Am Ende ist eine Lösung mit Rahmenbedingungen anzustreben. Diese leiten sich aus Kriterien ab, die möglichst auf der Grundlage eines breiten Konsenses zu Forschung und Technologie zu entwickeln sind.

Bei allen vier Fragen ist festzustellen, dass in den letzten Jahren je eine Entwicklung stattgefunden hat. Es gibt autonom fahrende Bahnen und Autos. Fahrzeugsysteme übersteuern Menschen, zum Beispiel bei Unfällen. Führung findet in manchen Fällen über Ebenen hinweg bereits unmittelbar statt. Und der Mensch hat sich an eine so große Menge und Qualität an Digitalisierung gewöhnt, dass er sich gar nicht mehr vorstellen kann, ohne diese zu leben.

Haben nicht schon unsere Eltern angesichts unserer Technisierung und Digitalisierung die Hände über dem Kopf zusammengeschlagen? Haben wir nicht unsere Welt ganz anders gestaltet als die Vorgängergeneration? Wie viel Vertrauen und Zuversicht setzen wir in die nächste und übernächste Generation? Digitalisierung verändert sehr viel in kurzer Zeit. Aber die neue Generation lebt in und mit ihr. Der autonom wirkende Mensch wird daher ebenso bleiben, wie er die künstlich intelligente Automatisierung für sich nutzen wird. Eine positive Sicht auf eine denkbare Zukunft ermöglicht, dass wir diese technologiebegleitend gestalten und verhindert zugleich, dass diese ungesteuert aus der Bahn bricht.

Resilienz – eine sich erweiternde Begrifflichkeit

Die Abhängigkeit in einer globalen Welt von ebensolchen Märkten hat in konfliktfreien Zeiten zu mehr Effizienz und zu vielfältigen Wertschöpfungsketten geführt. Der russische Angriffskrieg gegen die Ukraine und die Sanktionen gegen den Aggressor Russland sind dabei nicht folgenlos geblieben; die Corona-Pandemie führt bis heute zu einem Lieferengpass von Teilen, die unter Covid-19 nur eingeschränkt oder gar nicht mehr produziert werden konnten. Resilienz ist zu einem wichtigen Faktor für das Funktionieren nicht nur unserer Volkswirtschaft, sondern der gesamten Gesellschaft geworden.
Die Forderung nach Resilienz ist überall hörbar. Über die Ebene der Resilienz besteht allerdings wenig Einvernehmen: Ist sie in der

Allianz (NATO), in der EU, national oder gar für einzelne Ressorts oder Produktionsbereiche herzustellen? Es hat also etwas mit „Sicherheit und Vertrauen“ zu tun, dass im Falle eines Engpasses die Bereiche eine mögliche Autarkie ohne innere Egoismen entwickeln. Resilienz ist davon abhängig, ob wir diese Autarkie selbst schaffen und ob wir denjenigen im Krisenfall vertrauen können, die mit uns diese Autarkie gemeinsam begründen. Ist das bei einer EU-Resilienz mehr gegeben als bei einer NATO-Resilienz? Was ist zu tun, wenn die „sicherste Variante“, Resilienz national herzustellen, aufgrund fehlender Rohstoffe nicht zu verwirklichen ist?

Bei der Technisierung und Digitalisierung von Streitkräften kommt es besonders darauf an, resilient zu sein. Darum gilt es, starke Partner einzubeziehen, mit all ihrer Leistungsfähigkeit. Trotz manchen Wissensvorsprungs auch in Deutschland ist daher das transatlantische Bündnis essenziell.

Zugleich wandelt sich der Resilienzbegriff in ein weites Feld, wenn wir die oben genannten Rahmenbedingungen für das Führen, Aufklären, Wirken und Unterstützen (FAWU) in einer neuen digitalisierten Welt zu garantieren haben. Die genannte politische *Firewall* einer Bundestagsentscheidung vor jedem Einsatz, die Einbindung der Streitkräfte als Parlamentsarmee sowie die ethische Bildung und Verpflichtung in den Streitkräften sind ein starker Resilienzanker in dieser Hinsicht. Dennoch sind beste Absichten und entsprechende Ausbildung nicht immer ein Garant. Daher kommt der wissenschaftlichen Entwicklung eines *Ethical Design* eine immer stärker werdende Bedeutung zu. In der Arbeitsgruppe „Technikverantwortung“ zum Future Combat Air System (FCAS), das derzeit mit Frankreich und Spanien entwickelt wird, steht ein solches *Ethical Design* im Vordergrund. Auf den Punkt gebracht, lautet die Frage: Wie kann ein ethischer Waffensystemeinsatz durch Digitalisierung und Technik resilient garantiert werden? Es ist absehbar, dass dabei klare Fortschritte entwickelt und einbezogen werden können und drei Aspekte eine besondere Rolle spielen:

- Die „Ethik“ eines *Ethical Design* muss bestimmt werden.
- Die Funktionsfähigkeit von FCAS darf nur bei unethischem Einsatz eingeschränkt werden.

→ Ethische Resilienz muss technisch sinnvoll und funktionsfähig realisierbar sein.

Ähnlich wie sich die Umstellung auf Resilienz bei wirtschaftlichen Fragen nach den neuerlichen Krisen und dem russischen Angriffskrieg auf die Ukraine schrittweise vollzieht, ist sie auch in dieser Blickrichtung schrittweise anzugehen. Die ersten Schritte werden gerade unternommen: mit Zuversicht, aber noch mit ungewissem Ausgang und unklarer Prägung. Es lohnt sich in jedem Fall, „das Feld zu beackern".

Ein dritter, eigentlich immer schon bedeutsamer Aspekt, ist die militärische und insbesondere die operative Resilienz in einer stark technisierten Umgebung. Um es auf den Punkt zu bringen: Technik in Waffensystemen, die zwar die Präzision und Durchsetzungskraft deutlich erhöht, aber bei der ersten Einflussnahme von außen nicht mehr funktioniert, ist nicht „einsatztauglich". Umfassende, aus einer Vielzahl von Daten zusammengefügte Lagebilder sind nur hilfreich und verfügbar, wenn die Daten auch bei einer Cyberbedrohung unverfälscht und vollständig vorliegen. Ein System der Systeme – oder ein *Multi Domain Warfighting* – mögen als operative Idee gegenüber einem militärisch gut und modern aufgestellten Gegner notwendig sein, hinreichend sind sie nur, wenn sich eingesetzte Technik und Digitalisierung als ausreichend resilient beweisen.

Über alle Zeiten der Kriegsführung gab es die Diskussion um die Frage der notwendigen Einfachheit und Funktionsfähigkeit der Ausrüstung und der Waffensysteme versus Exzellenz, aber zugleich auch der Anfälligkeit, die durch Technik entsteht. Angesichts der Spanne vom „Infanteristen der Zukunft" bis hin zum modernen Kampfflugzeug ist von dieser Diskussion keine Ebene mehr ausgenommen. Mit Blick auf die Digitalisierung der Bundeswehr entsteht eine notwendige Resilienz aus einer Vielzahl von Ansätzen, die von Beginn an Beachtung verdienen. Fünf solcher Ansätze sind:

→ **Bewusstsein**

Das Wissen der Operateurin beziehungsweise des Operateurs um eine Cyberbedrohung, die nicht nur Daten „unterdrückt", sondern auch verändert oder hinzufügt, ermöglicht ihr oder ihm, bei Anomalien eine besondere Sorgfalt oder ergänzende Prüfungen bei

ihrem oder seinem Handeln und ihren oder seinen Entscheidungen einzubeziehen.

Mehrfache Auslegung und Übertragungswege

Daten an mehreren Orten abzulegen – im Sinne einer *Cloud* als *System of Systems* – beziehungsweise Auswertungen und Rechenleistung mehrfach abzubilden, garantiert die Funktionsfähigkeit auch bei gegnerischem Einwirken auf eines der Elemente. Gleiches gilt, wenn mehrfache Übertragungswege eingerichtet werden.

Sichere Datenübertragung

Die Datenwege zwischen den Komponenten eines *System of Systems* – also zwischen *Command Fightern* und *Remote Carriern*, zwischen *Cloud* und *Edge*, oder auch zwischen den *Combat Clouds* eines Multi-Domain-Gesamtsystems – müssen auch in einer cyberbedrohten Umwelt funktionieren. Laserkommunikation, Verschlüsselung und Boostübertragungen von vorausgewerteten Daten sind Ansätze.

Offensive elektronische Mittel

Eigene digitale Funktionsfähigkeit wird erheblich gestärkt, wenn die gegnerischen Einflussmöglichkeiten aktiv unterdrückt werden können. Die *Electronic Order of Battle* hat in der Zukunft einen viel höheren Stellenwert als in den letzten Jahrzehnten. Das reicht von eigenen Cyber- über begleitende *Airborne Electronic Attack*-Fähigkeiten bis hin zur Fähigkeit, gegnerische Mittel und Kräfte zu identifizieren und klassisch durch Waffenwirkung auszuschalten.

Auftragstaktik und Automatisierung

Bei allen notwendigen und Erfolg versprechenden Ansätzen einer cloudbasierten Datenverarbeitung mit entsprechenden zentralen Ansätzen für eine Datenfusion und -verteilung, ist die Rückfallposition einer Unterbrechung der Datenversorgung planerisch einzubeziehen. Hierzu sind sowohl vorgesehene und programmierte Automatismen eine Lösung (Fortsetzen des Auftrags mit den vorhandenen Informationen), als auch die klassische Auftragstaktik für den menschlichen Operateur – gegebenenfalls in Kombination der beiden Ansätze.

Resilienz kostet. Sie erfordert technische Ansätze, gegebenenfalls Mehrfachauslegung und ergänzende operative Überlegungen.

In den letzten Jahrzehnten ist die Operationsführung weitestgehend von technischen Fortschritten angepasst worden. Heute muss Technik auch die operativen Notwendigkeiten realisieren oder unterstützen, die sich aus dem Gefährdungspotenzial des Gegners ergeben.

Resilienz ist der Preis, der in einer immer stärker technisierten Welt zu zahlen ist, will man mit Exzellenz und Durchsetzungsfähigkeit – bei Präzision, Reaktionsfähigkeit und Flexibilität – den Auftrag erfüllen. Daher gilt es, in sie zu investieren, sie von vornherein in alle Planungen einzubeziehen. Interessanterweise kommt hier der Verbindung zwischen Mensch und Maschine wiederum eine besondere Bedeutung zu. Genau betrachtet, schaffen sich beide gegenseitig Resilienz, der Mensch als „Überwacher" der Maschine und Anwender der Auftragstaktik – die Maschine als Garant einer Auftragserfüllung (oder sicheren Rückkehr), wenn der Mensch in einer technisierten Welt überlastet ist, falsche Entscheidungen trifft oder gar ausfällt. Die Einstellung dieser Zweierbeziehung im Sinne von Resilienz ist eine herausfordernde Aufgabe, die es anzugehen gilt.

Datenzentriertheit in einer Cyberwelt – eine Sackgasse oder der Schlüssel für zukünftige Herausforderungen?

Zweifellos leben wir in einer Welt voller Daten. Sie kommen aus einer Vielzahl von Sensoren, deren Technologie sich in den letzten Jahren deutlich weiterentwickelt hat. Das gilt auch für den militärischen Bereich. Daten tragen Informationen in sich, die – richtig ausgewertet und beurteilt – zu einer militärischen Überlegenheit beitragen. Digitalisierung besitzt mit all ihren Anwendungen die Fähigkeit dazu. Wir alle stimmen dieser Analyse zu; allein die Folgerungen daraus sind sehr unterschiedlich. Am Beispiel des neu zu entwickelnden *System of Systems* beim FCAS kann dieses an zwei Linien deutlich gemacht werden:

- Im Eurofighter gibt es bereits eine Vielzahl frei programmierbarer Rechner, die mit den Sensordaten ein Lagebild und weitere Funktionen bieten, um das Waffensystem erfolgreich wirken zu lassen. Moderne Digitalisierung ermöglicht es, dieses im Sinne eines ausgefeilten *Edge Computing* zu optimieren.

- Massive Rechenleistung wird für die Auswertung einer Vielzahl an Daten benötigt. Diese kann in einem Flugzeug auch mit neuen IT-Systemen nicht erzeugt werden,

insbesondere, wenn es um die Anwendung Künstlicher Intelligenz geht. Daher sind die Daten in einer Cloud – jenseits der Waffensysteme selbst – zu ver- beziehungsweise bearbeiten. Eine Cloud ermöglicht darüber hinaus auch mehr als nur die Sensoren des Flugzeugs einzubeziehen. Zugleich können andere Nutzer mit auf die Daten in der Cloud zugreifen.

Die Geister scheiden sich hierbei an der Frage, ob die Ergebnisse von *Cloud Computing* in eine Cyberumgebung übertragen werden können oder ob das Umfeld als zu unsicher oder gar als „völlig unbrauchbar" gewertet werden muss. Die Suche nach der richtigen Position des Schiebereglers zwischen *Edge* und *Cloud* in diesem Anwendungsfall ist schwer festzulegen. In jedem Fall gilt, dass nicht überall dieselben digitalen Funktionalitäten abgebildet und eingerichtet werden können. Das wäre nicht nur unwirtschaftlich, sondern auch militärisch sinnlos. Übertragungstechnologie in einem cyberdominierten Umfeld spielt die entscheidende Rolle. Daher sind sowohl die Fortschritte bei Laserkommunikation, programmierbaren Funkgeräten, Kryptografie und Quantentechnologie wichtig, aber auch operative und taktische Entwicklungen, um in einer Cyberwelt erfolgreich sein zu können. Obwohl wir bisher einen *All Out Cyber War* nicht erlebt haben, wissen wir um die Möglichkeiten eines potenziellen Gegners. Widerspricht also eine Cyberbedrohung der Datenzentriertheit und Digitalisierung der Zukunft? Aus drei Gründen wird die Frage absehbar mit „Nein" zu beantworten sein:

- Erstens ist ein vollständiges Ausschalten des elektromagnetischen Spektrums für alle Streitkräfte – also auch für den Angreifer – selbstabschreckend. Es wird also ein kaum realistisches Szenario sein. (Ein Vergleich mit der Nutzung des Weltraums ist hier zulässig.)

- Zweitens werden Clouds auch in einem *System of Systems* so verteilbar sein, dass in der Nähe der *Edge* entsprechende Rechenleistung und Datenhaltung sowie die Übertragung im nahen Umfeld weiter sichergestellt werden kann. (Eine Cloud in ein mitfliegendes Transportflugzeug oder mehrere *Remote Carriers* zu integrieren, wäre denkbar, gegebenenfalls auch als Back-up zu einer Cloud am Boden).

→ Und drittens ist es heute möglich, die Daten von Sensoren bereits vorauszuwerten, sodass größere Datenströme gar nicht versendet werden müssen. Gleiches gilt für die Daten, die aus einer Cloud an ein Waffensystem übertragen werden. Auch hier kann eine zeitlich begrenzte Boostübertragung bereits alle nötigen Daten beinhalten.

Daher stoßen wir nicht auf eine Entweder-oder-Frage, sondern vielmehr auf die Notwendigkeit, eine intelligente Lösung zu finden. Hierbei sind Technik und Operationsführung aufeinander abzustimmen. Interessanterweise mischt sich in diese Diskussion immer wieder die Frage nach der Auftragstaktik. Sie war bisher die Grundlage aller Führungsüberlegungen: Der Pilot in seinem Waffensystem kann auch ohne Kommunikation weiterkämpfen und seinen Auftrag erfüllen, weil er die Absicht der Führung kennt und es zugleich gewohnt ist, eigene Entscheidungen auf dieser Basis zu treffen. Erste Versuche, dieses technisch zu fassen und auch in der Systematik fliegender Waffensysteme in einem Verbund zu integrieren, sind bereits gemacht worden. Neben den oben genannten *Ethics by Design* entsteht gerade folgerichtig ein *Task-based Command and Control by Design*.

Datenzentriertheit ist also selbst in einer Cyberwelt keine Sackgasse, sondern eine Grundlage für die Zukunft – unter bestimmten gesetzten Rahmenbedingungen.

Fazit: Technik und Führung – zwei aufeinander hin geordnete Bereiche zur Unterstützung des Menschen

Aus dieser eher technischen Perspektive ist der Blick auf die Bundeswehr im Zeitalter der Digitalisierung und Künstlichen Intelligenz weiterhin sowohl vom technologischen Fortschritt und seiner Anwendung in den Waffensystemen und Fähigkeiten der Bundeswehr geprägt, als auch von den operativen Strategien und den menschlichen Führern und Entscheidern. (Innere) Führung wird sich verändern. Sie hat sich bereits dadurch verändert, dass die Vernetzung der Menschen auch im Dienst umfassend geworden ist und bei der Informationsweitergabe die Hierarchiegrenzen kaum zu

halten sind. Damit einher geht eine Veränderung des Mindsets, einerseits Technologie umfassend nutzen zu wollen, andererseits aber auch operative Notwendigkeiten in den Vordergrund zu stellen oder stellen zu müssen.

In den letzten Jahrzehnten ist die Operationsführung weitestgehend von technischen Fortschritten angepasst worden. Heute muss Technik vor allem die operativen Notwendigkeiten realisieren oder unterstützen, die sich aus dem Gefährdungspotenzial des Gegners ergeben. Die Reihenfolge dreht sich gegenüber der Vergangenheit also um.

Technik und Führung sind weiterhin zwei aufeinander hin geordnete Bereiche zur Unterstützung des Menschen – im militärischen Bereich der Führer und Operateure. Wenn Technik – und in ihr vor allem Digitalisierung und Künstliche Intelligenz – die Auftragserfüllung des Menschen unterstützen, ist zugleich die Herangehensweise an diese Verbindung zwischen Technik, Operationsführung und dem Menschen zu klären. Um es auf den Punkt zu bringen: Wer macht und entscheidet eigentlich was, und wie sehr soll der Mensch sich auf die Technik verlassen – und wie wir gesehen haben, wohl auch die Technik gegebenenfalls auf den Menschen. Einige grundsätzliche Fragen sind zu klären, um nicht in eine Lose-Lose-Situation zu geraten. Fünf Beispiele:

- Was ist, wenn die KI Vorschläge macht, die absehbar der Analyse des militärischen Führers beziehungsweise der militärischen Führerin nicht entsprechen und seine oder ihre abweichende Entscheidung zu negativen Ergebnissen führt?

- Was ist, wenn der militärische Führer beziehungsweise die militärische Führerin der KI folgt und es zu negativen Ergebnissen kommt, obwohl er oder sie es gegebenenfalls hätte besser wissen können?

- Muss der militärische Führer beziehungsweise die militärische Führerin in jedem Fall die Datenlage selbst noch einmal analysieren und auswerten, auch wenn die KI das schon gemacht hat?

- Was sind Abbruch- oder Nutzungskriterien eines KI-Ratschlags?

- Wie lernen wir die KI kontinuierlich und breit an, wenn wir nicht genügend Daten beziehungsweise Testfälle haben?

Die Anwendung und Einführung von KI erfordert – neben konkreten ersten erfolgreichen Fällen – sehr grundsätzliche Überlegungen. Diese sind parallel zu den technischen und operativen Entwicklungen anzugehen.

Inmitten einer Welt, in der wir gerade sowohl eine technologisch rasante Entwicklung erleben, in der wir uns wieder zeitgleich auf die Landes- und Bündnisverteidigung ausrichten müssen, in der operative Ideen die Technikentwicklung bestimmen, in der das Verhältnis von Mensch und Maschine neu bestimmt wird – in dieser Welt kann man ängstlich die Vielzahl an neuen Parametern beklagen oder euphorisch gestaltend nach vorn schauen. Es ist Entwicklungszeit, viel weniger als Entscheidungszeit. Keine Ja-Nein-Fragen stehen an, vielmehr Gestaltungsfragen. Tiefe Fachlichkeiten sind zu einem Ganzen mit dem übergeordneten Ziel einer zukünftig erfolgreichen Auftragserfüllung zu verbinden.

Führung wird sich dabei und dazu verändern. Sie ist bereits auf dem Weg dahin. Der Mensch wird in ein neues Zusammenwirken mit Technik auch im militärischen Bereich eintreten. Er wird *in the Loop* bleiben, auch wenn sich der *Loop* verändert. Technik, Führung und Mensch bleiben aufeinander hingeordnet.