bitkom

Auf einen Blick

Smarte Bundeswehr – Digitalisierung neu denken

Ausgangslage

Mit der Gründung der Abteilung CIT im BMVg und der Aufstellung des Kommando CIR im Jahr 2016 wurden wichtige Schritte unternommen, um die verteilten Kompetenzen im Bereich der IT der Bundeswehr zu bündeln und eindeutige Zuständigkeiten zu schaffen. Die Bundeswehr soll so die Chancen der Digitalisierung besser nutzen und bestmöglich auf Bedrohungen aus dem Cyberraum vorbereitet sein. Aktuell sind im Geschäftsbereich des BMVg viele wichtige Digitalisierungsaktivitäten zu beobachten, die sich auch in der Gründung neuer Zentren und Innovationseinheiten widerspiegeln. Zur Steuerung dieser Aktivitäten braucht es eine konsequente Fortsetzung der Umsetzungsstrategie Digitale Bundeswehr von 2019.

Bitkom-Bewertung

Die konsequente Umsetzung der 2016 begonnenen Restrukturierung über alle Organisationsbereiche hinweg mit einer stringenten Prozessorientierung wird eine Voraussetzung für die erfolgreiche digitale Transformation der Bundeswehr sein. Damit diese gelingt, müssen aus **Sicht des Bitkom die strategischen Ziele im Bereich der Digitalisierung sowie der Aufbau der digitalen Kompetenzen im Kommando Cyber- und Informationsraum** konsequent umgesetzt und der Weg zu einer digitalen Gesamtarchitektur konsequent fortgesetzt werden. **Gelingt dies nicht, droht eine erneute Zersplitterung** der Digitalisierungslandschaft in der Bundeswehr und damit **eine Digitalisierungskonfusion**, die keine effektive und effiziente Wirkung im Ziel entfalten kann.

Das Wichtigste

- Wir erleben in der Bundeswehr eine Diskrepanz zwischen technologiefokussierten Leuchtturmprojekten und einer in Teilen noch im analogen Zeitalter verhafteten Infrastruktur
- Die Bundeswehr fokussiert auf Technologien und droht die weiteren Digitalisierungsebenen Infrastruktur, und Prozesse zu vernachlässigen, dabei lässt sich erst aus dem Zusammenspiel dieser Ebenen das Potenzial der Digitalisierung voll ausschöpfen
- Dies könnte bei den Soldaten für Frust sorgen und die Bundeswehr daran hindern, ein attraktiver Arbeitgeber, insbesondere für die so dringend benötigten Fachkräfte zu werden
- Die Bundeswehr braucht eine digitale Gesamtarchitektur, die notwendige Agilität sowie die entsprechenden Mittel, um die digitale Transformation erfolgreich zu meistern

68 Prozent der Bevölkerung glauben nicht, dass die Bundeswehr ausreichend ausgestattet ist, um Deutschland im Cyberraum zu verteidigen
(lt. einer Studie von Bitkom Research)

Stellungnahme

Smarte Bundeswehr

01.05.2021

Zusammenfassung

Die Digitalisierung der Bundeswehr sollte ganzheitlich betrachtet und gesteuert werden, damit sie ihre Wirkung effizient und effektiv entfalten kann. Hierzu braucht es eine digitale Gesamtarchitektur und eine konsequente Umsetzung der bislang noch vorrangig in strategischen Dokumenten wie der „Umsetzungsstrategie Digitale Bundeswehr“ formulierten Ziele. In diesem Papier sind Vorschläge zusammengefasst, die dazu beitragen sollen, die Digitalisierung der Bundeswehr neu zu denken und zu fördern. Zentrale Elemente sind hierbei der klare Fokus auf die Rahmenbedingungen und Ziele der digitalen Transformation der Bundeswehr, die Umsetzung der Digitalisierungsplattform im Geschäftsbereich des Bundesministeriums der Verteidigung (BMVg) und die Gestaltung einer Innovationslandschaft aus einem Guss unter Berücksichtigung der digitalen Souveränität sowie der Aufbau einer Digitalkultur, die tatsächlich gelebt wird. Exemplarisch werden zudem ausgewählte Technologien mit Schlüsselfunktion für die Bundeswehr dargestellt und deren Nutzen für den Verteidigungssektor aufgezeigt.

Bitkom
Bundesverband
Informationswirtschaft,
Telekommunikation
und Neue Medien e.V.

Dr. Christian Weber
Bereichsleiter Öffentliche Sicherheit & Verteidigung
T +49 30 27576-136
c.weber@bitkom.org

Albrechtstraße 10
10117 Berlin

Präsident
Achim Berg

Hauptgeschäftsführer
Dr. Bernhard Rohleder

Inhalt

Seite

1 Die Digitalisierung der Bundeswehr neu denken

In der Umsetzungsstrategie Digitale Bundeswehr hat sich das BMVg auf eine Definition des Begriffs „Digitale Transformation" festgelegt, die mit einer ausgeprägten Fokussierung auf neue Technologien verbunden ist:

„Unter Digitalisierung versteht das BMVg die zielgerichtete Identifikation und das konsequente Ausschöpfen von Potenzialen, die sich aus digitalen Technologien (z. B. KI, 5G, Augmented Reality, etc.) ergeben. Durch eine konsequente digitale Transformation können nicht nur erhebliche Effizienzpotenziale ausgeschöpft werden, sondern in Teilen auch angepasste oder neue Wirkmodelle und Arbeitsbeziehungen (i.S.v. Geschäftsmodellen) – d. h. grundlegend neue Ansätze zur Aufgabenerfüllung – implementiert werden."[1]

Eine erfolgreiche digitale Transformation geht jedoch über technologische Aspekte hinaus. Dies bringt die Wehrbeauftragte des Deutschen Bundestags in ihrem Jahresbericht 2020 wie folgt auf den Punkt:

„Die digitale Transformation hat eben nicht nur eine technische Seite. Einer „Kultur des Machens", wie die Bundeswehr die Digitalisierung ausdrücklich versteht, stehen viele Hürden im Wege. Über die technischen und rechtlichen Herausforderungen hinaus, müssen sich auch Handlungsweisen und Denkmuster ändern."[2]

Digitalisierung betrifft damit jeden Soldaten und Mitarbeiter im Geschäftsbereich BMVg. Nur durch eine ganzheitliche Betrachtung der Ebenen „Technologie", „Infrastruktur", und „Prozesse" können neue Wirkmodelle und Arbeitsbeziehungen entstehen. Die Digitalisierung in der Bundeswehr sollte organisationsübergreifend, vernetzt und integriert im Sinne einer „Digitalen Gesamtarchitektur" neu gedacht werden.

Eine solche digitale Gesamtarchitektur folgt im Grundsatz der Idee, moderner IT-Architekturen: Ein gesamtheitliches IT-System besteht nicht mehr aus einer monolithischen Applikation, sondern aus vielen kleinen Microservices (Dienststellen die sich mit Technologie beschäftigen) und diese Microservices leben alle selbstständig. Für die Gesamtfunktionalität gibt es aber definierte APIs (Kommunikationsschnittstellen zwischen den Dienststellen), die Netzwerkverkehr und Datenfluss steuern.

[1] https://www.bmvg.de/de/themen/ruestung/digitalisierung/umsetzungsstrategie-digitale-bundeswehr
[2] https://dip21.bundestag.de/dip21/btd/19/266/1926600.pdf, S. 97

In der Umsetzungsstrategie „Digitale Bundeswehr“ wurden in diesem Zusammenhang bereits sehr gute und zielführende Maßnahmen beschrieben, die schnellstmöglich auf die Spur gebracht werden müssen.

Dies betrifft insbesondere den „Digitalen Campus“, der mit den drei Elementen „Digitalrat“, Digitallabor“ und „Digitalgalerie“ zur systematischen Identifikation und Nutzbarmachung von Digitalisierungsaktivitäten und -fähigkeiten beitragen soll. Von diesen drei Elementen ist bislang jedoch nur der Digitalrat nach außen in Erscheinung getreten. Dessen Arbeit muss transparent erfolgen, um einen Wissensaustausch zwischen den einzelnen Akteuren aus Verteidigung, Industrie, Wissenschaft und Zivilgesellschaft zu ermöglichen.

Die Idee einer Digitalgalerie findet sich hingegen in Ansätzen im durch das Kommando Heer geplanten Systemzentrum Digitalisierung Landstreitkräfte wieder und könnte dort zur Umsetzung kommen. In den Test- und Versuchsstrukturen dieses Zentrums sollen digitale Technologien und Werkzeuge für Landstreitkräfte vor der eigentlichen Beschaffungsentscheidung getestet und erprobt werden. Die Nutzer, also Soldatinnen und Soldaten, sollen hier möglichst einsatznah eingebunden und im Mittelpunkt stehen. Bitkom begrüßt dieses Projekt als eine einzigartige Möglichkeit, die Digitalisierungskompetenz in den Landstreitkräften zu bündeln und auszubauen.[3] Dieses könnte gleichzeitig den Nukleus für den Aufbau eines Systemzentrums für die Digitalisierung der gesamten Bundeswehr im Sinne der Digitalgalerie bilden.

Diese Idee eines zentral gesteuerten „Digitalen Campus“ sollte schnellstmöglich umgesetzt werden, um das institutionelle Gefüge der verschiedenen Digitalisierungszentren und- Einheiten im Sinne der von uns geforderten digitalen Gesamtarchitektur zu steuern. Im Zuge dieses Prozesses sollte geprüft werden, den Cyber Innovation Hub der Bundeswehr (CIHBw) zu einem „Digital Innovation Hub“ im Sinne eines „Hub of Hubs“ aufzuwerten.

Die Umsetzungsstrategie fordert ferner als übergreifendes Prinzip die strategische Steuerung bei dezentraler Umsetzung. Die Praxis wird diesem Anspruch bislang noch nicht ausreichend gerecht: Aus Sicht unserer Unternehmen befassen sich immer noch zu viele Dienststellen mit vergleichbaren Themen. Für uns bedeutet eine zentrale Steuerung bei dezentraler Umsetzung, dass die zentrale Stelle einen gesamtheitlichen Blick bewahrt, die digitale Gesamtarchitektur ausbaut, grundlegende Entscheidungen trifft sowie technische, ethische und kulturelle Herausforderungen der digitalen Transformation bewertet. Die dezentralen Stellen müssen in der Lage sein, diese Vorgaben unter

[3] https://www.bitkom.org/Bitkom/Publikationen/Systemzentrum-Digitalisierung-Land

Berücksichtigung eigener Spezifika umzusetzen und etwaige Problemstellungen gebündelt an die zentrale Stelle zu kommunizieren. Digitalisierung verlangt deshalb nach flächendeckender Kompetenz in der gesamten Bundeswehr und eine Änderung des Mindsets sowie eine Fehlerkultur, die auch tatsächlich gelebt wird.

Dies ist auch deshalb wichtig, weil in den vergangenen Jahren eine Vielzahl an neuen Innovationseinheiten, Zentren und Agenturen gegründet worden ist, die noch besser miteinander vernetzt werden müssten. Je mehr Zentren gegründet werden, umso dezentraler wird die Organisation der Digitalisierung in der Bundeswehr und am Ende steht diese mit einer zersplitterten Digitalisierungslandschaft wieder vor dem gleichen Dilemma wie vor der Gründung des Kommando CIR. Dadurch droht eine Digitalisierungskonfusion, die keine ausreichende und effiziente Wirkung im Ziel entfalten kann, solange die Roadmap für die Umsetzungsstrategie nicht eingehalten wird.

2 Digitalisierung zur Wirkung bringen

Die Digitalisierung bietet sowohl Chancen als auch Risiken. Als Folge der zunehmenden Gefahren aus dem Cyberraum für die Sicherheit Deutschlands wird dieser selbst zum Austragungsort von Phänomenen wie Cyberspionage, Sabotage und Desinformationskampagnen und erhält damit eine Schlüsselrolle in hybriden Konfliktszenarien mit unmittelbaren Auswirkungen auf die nationale Sicherheit.

Advanced Persistent Threats, wie im Solarwinds-Fall zeigen, dass wir Antworten auf die Frage brauchen, wann ein Cyberkrieg beginnt und ob die Bundeswehr Cyberkriegsfähig ist, also über die Fähigkeiten verfügt, um in einem solchen komplexen Szenario zu bestehen. Die Bundeswehr muss neben einem umfassenden Cybersicherheitskonzept auch die Chancen der Digitalisierung voll ausschöpfen, um eine Wirkungsüberlegenheit im gesamten Einsatzspektrum zu erreichen. Auch im Rahmen ihrer Bündnisverpflichtungen, muss die Bundeswehr einen relevanten Beitrag leisten können und auf technischer Augenhöhe mit ihren Verbündeten agieren.

Die Digitalisierung der Bundeswehr bietet zudem die Chance, im Sinne von Dual-Use, Technologien und Anwendungen für die Öffentliche Sicherheit und die Cybersicherheit allgemein nutzbar zu machen. Hierzu ist die erfolgreiche Gründung der Cyberagentur bereits ein wichtiger Meilenstein. Nun kommt es darauf an, dass die Agentur sowohl die entsprechenden Ressourcen als auch die notwendigen Freiheiten und das politische Vertrauen erhält, um ihre Arbeit zu etablieren.

2.1 Den Anwender in den Mittelpunkt stellen

Soldaten möchten mit Systemen arbeiten, die in der Bedienbarkeit mit zivilen Anwendungen vergleichbar sind. Die Erwartungshaltung der Nutzer wird durch Technologien gefördert, die aus dem zivilen Leben bekannt sind. Diese sind in der Regel hochverfügbar, orts- und zeitunabhängig nutzbar und bieten eine positive User-Experience, mit welcher sie schnell und unkompliziert Informationen finden oder Prozesse anstoßen können. Gerade vor dem Hintergrund des Fachkräftemangels in der IT-Wirtschaft und im Öffentlichen Dienst ist es von Vorteil, wenn Systeme einfach zu bedienen sind und ihre Nutzer nicht überfordern. Das Stichwort lautet hier „Plug & Fight".

Dazu braucht es offene Schnittstellen und standardisierte Oberflächen sowie eine Abkehr von proprietären Systemen, die nicht untereinander kompatibel und meistens bei ihrer Einführung bereits veraltet sind. Ein Grund für eine solche fehlende Kompatibilität ist ein Beschaffungswesen und industrielles Ökosystem, das die Einführung von Innovationen behindert. Der bisherige „CPM-Prozess" ist nicht geeignet, schnell digitale Produkte für die Bundeswehr zu beschaffen. Hier braucht es eine schnellstmögliche Anpassung der Rahmenbedingungen und internen Abläufe, die sicherstellen, dass marktübliche Benchmarks hinsichtlich ihres Zeitbedarfs erreicht werden. Vorschläge hierzu werden aktuell in einem Expertenkreis im Rahmen des Strategischen Industriedialogs erarbeitet.

2.2 Innovationszyklen und Beschaffungswesen in Einklang bringen

Die Innovationszyklen der Digitalwirtschaft verlaufen deutlich schneller als bei klassischen Rüstungsgütern. Dabei ist die digitale Wirtschaft der Treiber für Innovationen. Anbieter des zivilen Marktes erwarten daher auch andere Rahmenbedingungen, zum Beispiel schnellere Beschaffungszyklen, inkrementelle Vorgehensweisen, frühzeitiges Obsoleszenzmanagement und konsequente Umsetzung der mit der öffentlichen Hand ausgehandelten Musterverträge wie der EVB-IT. Zudem sollten haushälterische Möglichkeiten und rechtliche Rahmenbedingungen geschaffen werden, um auch flexible „... as a service"-Modelle zu nutzen.

Zudem ist es nicht ausreichend bestehende Abläufe eins zu eins in IT-unterstützte Abläufe zu überführen. Die Bundeswehr muss ihre Vorschriften und internen Prozesse anpassen, um die Fähigkeiten der Digitalisierung vollständig nutzen zu können. Das Potenzial der Digitalisierung erschließt sich auch hier nur aus einer gemeinsamen Betrachtung und Optimierung von Technologie, Infrastruktur, Ablauf und Prozessen.

Bitkom unterstützt deshalb ausdrücklich den Aufbau der Digitalisierungsplattform im Geschäftsbereich BMVg, durch welche die Besonderheiten bei der Bereitstellung von IT-Services im Vergleich zu anderen Rüstungsvorhaben im Beschaffungsprozess inkl. des Planungsprozesses und der Haushaltsaufstellung verstärkt Berücksichtigung finden sollen. Die Zeitspanne zur Deckung eines Bedarfs ließe sich durch die gezielte Wiederverwendbarkeit von standardisierten IT-Services deutlich reduzieren und wirtschaftlicher gestalten. Eine erfolgreiche Umsetzung ist dringend notwendig, damit Bundeswehrangehörige künftig alles, was sie in ihrer täglichen IT-Arbeit benötigen, unabhängig ob im In- oder Ausland, zentral gesteuert durch die Digitalisierungsplattform zur Verfügung gestellt bekommen können. Damit die Digitalisierungsplattform ihre Wirkung entfalten kann, muss auch diese als Wirkverbund einen ganzheitlichen Ansatz verfolgen und alle relevanten Prozesse, Verfahren, Arbeitsweisen und Strukturen in ihre Arbeit einbeziehen. Dadurch kann die Bundeswehr ihre erforderliche IT-Unterstützung effizient, wirtschaftlich, modern und schnell beim Nutzer erhalten. Die bereits bei der COVID-19 Pandemie erfolgreiche angewendete Top-Down-Steuerung, mit der die Möglichkeiten zum mobilen Arbeiten in kurzer Zeit erweitert wurden, entspricht unser Forderung nach einer effektiven Realisierung bereits bestehender Lösungen.

Damit innovative Technologien frühzeitig implementiert werden können, sind Prozesse nötig, die gemeinsame Projekte mit der Digitalwirtschaft und der Rüstungsindustrie auf den Weg bringen – und das von Anfang an. Kooperationen zwischen Bundeswehr und Wirtschaft, wie im Rahmen der Kooperation des Bitkom mit dem Kommando CIR oder die Durchführung von gemeinsamen Workshops, wie beispielsweise mit dem Kommando Heer zum Systemzentrum Digitalisierung Land, müssen vertieft und ausgebaut werden. Dadurch können auch Unternehmen erreicht werden, die zwar Lösungen von hoher Relevanz für die Bundeswehr anbieten, aber aufgrund fehlender Kenntnisse über die Bedarfe im Verteidigungssektor bislang nicht erreicht werden.

2.3 Industriediversität fördern

Eine größere Industriediversität sollte dazu beitragen, innovative Lösungen auch von Startups und KMUs für die Bundeswehr nutzbar zu machen. Noch stehen den oftmals software-zentrischen Geschäftsmodellen von Unternehmen der Digitalwirtschaft die eher hardware-zentrischen Geschäftsmodelle der großen Plattformhersteller entgegen, die auf langfristig geplante oder bereits umgesetzte Entwicklungen ausgelegt sind. Dadurch richtet sich die Aktualisierung der Software nach der Aktualisierung der Plattformen mit entsprechend langen Entwicklungszyklen. Mit Erreichen der Einsatzreife sind diese oftmals bereits veraltet. Idealerweise definiert der Einsatz die software-gestützte Lösung, welche dann die Konfiguration und Konstellation der Hardware festlegt. Gemeinsam mit dem

Bedarfsträger muss eine vom Einsatz her gedachte und zukunftsfähige Innovationslandschaft gestaltet werden, welche die gesamte Industrie, vom Startup über KMU bis hin zum internationalen Großkonzern adressiert. Der Dialog zwischen BMVg und Industrie sollte sich deshalb nicht nur auf die Sicherheits- und Verteidigungsindustrie beschränken, sondern muss die gesamte Digitalwirtschaft einbeziehen.

Umfragen unter Startups zeigen, dass diese oftmals große Vorbehalte gegenüber einer Zusammenarbeit mit dem ÖAG pflegen[4]. Dies betrifft insbesondere die Erfahrung vor zu langen und komplizierten Vergabeverfahren sowie die Einschätzung aufgrund hoher Hürden bei den Vergabekriterien, z. B. durch die Forderung nach Referenzlisten ohnehin chancenlos zu sein. Dabei könnte der Öffentliche Sektor und insbesondere die Bundeswehr in hohem Maße von der Innovationsfreude, Agilität und schnellen Reaktionsfähigkeit von Startups profitieren. Bitkom hat bereits mit einem Sieben-Punkte-Papier ausführlich Vorschläge und Maßnahmen dargestellt, wie mehr Startups in der öffentlichen Vergabe berücksichtigt werden könnten[5].
Hierzu gehören die Abkehr von einer vollständigen Risikoeliminierung bei den Eignungsanforderungen und Bewertungsstrukturen bei öffentlichen Aufträgen hin zu einem angemessenen Risikomanagement genauso wie die Wertschätzung technologischer Innovationen und die Reduzierung des Bürokratieaufwandes bei Vergabeverfahren.
Um erfolgreich an öffentlichen Vergaben teilzunehmen, müssen Startups sich mit der Welt der Vergabe sowohl rechtlich als auch kulturell vertraut machen. Hier geht es nicht nur darum, die Verfahrensarten zu verstehen, sondern auch darum, ein Verständnis für die Sprache und Mentalität des öffentlichen Sektors zu entwickeln. Schulungsangebote und Workshops sollten durch den ÖAG, bspw. in Trägerschaft des CIH für Startups angeboten werden, um ihnen die Grundlagen des Vergaberechts näher zu bringen.
Aber auch die Kooperation mit etablierten Unternehmen, wie beispielsweise die Non-Traditional-Player-Initiative von Airbus mit dem BAAINBw im Rahmen von FCAS bietet ein großes Potenzial für den Verteidigungssektor. Sie sollte nachhaltig und dauerhaft institutionalisiert werden und als Vorbild für weitere Rüstungsprojekte dienen. Dazu müssen aber auch Unternehmen für Startups als potenzielle Partner präsent, sichtbar und attraktiv sein und ein entsprechendes Netzwerk aufbauen.

[4] https://www.bitkom.org/sites/default/files/2020-12/bitkom_startup_report_2020.pdf

[5] https://www.bitkom.org/Bitkom/Publikationen/7-Punkte-fuer-mehr-Startups-in-der-oeffentlichen-Vergabe

3 Digitale Souveränität fördern

In seiner 2020 veröffentlichten Stellungnahmen zum Thema Digitale Souveränität[6] weist Bitkom darauf hin, dass dieser Begriff nicht klar definiert ist, sondern unterschiedliche kontextbezogene Ausprägungen enthält. Die Selbstbestimmtheit als Ausdruck Digitaler Souveränität ist umso bedeutender, je kritischer der Einsatzbereich digitaler Technologien für eine Gesellschaft ist. Dies betrifft insbesondere den Bereich der Verteidigung. Digitale Souveränität umfasst die Fähigkeit zu selbstbestimmtem Handeln und grenzt sich damit von der Digitalen Abhängigkeit, die zu einem Kontrollverlust führt, genauso ab, wie vom Anspruch einer kompletten Digitalen Autarkie, die ausschließlich auf eigene Technologien setzt. Dieser Gedanke wurde in einer Arbeitsgruppe von Vertretern der Industrie- als auch der Amtsseite im Rahmen der Kooperation zwischen Bitkom und dem Kommando CIR weiterentwickelt. Es muss politisch entschieden werden, wie mit bestehenden digitalen Abhängigkeiten umzugehen ist, also wo zum einen eigene Entscheidungs- und Handlungsfreiheiten nicht wesentlich gefährdet sind und wo zum anderen inakzeptable Defizite bestehen und eigene Fähigkeiten aufgebaut werden müssen. Eine Prüfung unter Kosten- Nutzen- Aspekten und auch unter Beachtung der teils internationalen Lieferketten bildet die Grundlage für die Entscheidung, diese Defizite später bei Bedarf zu beheben und einem Controlling zu unterwerfen. In diesem Kontext bedeutet Digitale Souveränität nicht, dass der Staat, bzw. die Bundeswehr im Sinne der oben genannten digitalen Autarkie alles selbst macht, und eigene Technologien und selbst entwickelte Lösungen selbst dann bevorzugt, wenn diese von externen Anbietern deutlich mehr Leistung bieten würden. Vielmehr besteht der Kerngedanke einer so verstandenen Digitalen Souveränität darin, Abhängigkeiten im digitalen Raum zu erkennen und diese zu bewerten.

3.1 Die BWI braucht starke Partner

Das BMVg verfolgt mit der 2020 formulierten Eigentümerstrategie das Ziel, die BWI zum IT-Systemhaus der Bundeswehr weiterzuentwickeln. Die BWI soll als In-House Gesellschaft des Bundes als Treiber von Innovationen agieren und die Digitale Transformation der Bundeswehr unterstützen. Daher wurden auch der Cyber Innovation Hub der Bundeswehr und die neue Software-Innovationseinheit Schmiede in der BWI angesiedelt. Mit der Weiterentwicklung zum Systemhaus will das BMVg die Digitale Souveränität gegenüber privaten Providern wahren. Die Eigentümerstrategie und betriebliche Praxis der BWI kennen Aufgaben, die einen hohen Eigenfertigungsanteil der BWI vorsehen (z. B. in den Bereichen Planung und Steuerung von Aufgaben). Demgegenüber stehen Aufgaben, die

[6] https://www.bitkom.org/Bitkom/Publikationen/Digitale-Souveraenitaet-Anforderungen-an-Technologien-und-Kompetenzfelder-mit-Schluesselfunktion

dauerhaft enge Kooperationsformen mit der Privatwirtschaft im Rahmen eines Partner-Ökosystems erfordern (z. B. bei Entwicklung und Transition bis hin zum Betrieb).

In Bezug auf die Digitale Souveränität ist der Aufbau eines IT-Systemhauses der Bundeswehr, das sich im hundertprozentigen Eigentum des Bundes befindet, plausibel. Bitkom stellt diese Weichenstellung grundsätzlich nicht in Frage. Es wäre aber falsch mittels eines bundeseigenes IT-Systemhauses nahezu ausschließlich eine Leistungserbringung mit eigenen Ressourcen zu Lasten der privaten Digitalwirtschaft zu realisieren. Dies würde den Gedanken des Strategiepapieres der Bundesregierung zur Stärkung der Sicherheits- und Verteidigungsindustrie konterkarieren[7], das privatwirtschaftliche Unternehmen in Bereichen nationaler und europäischer Schlüsseltechnologien ausdrücklich fördern will. Bitkom begrüßt daher den von der BWI eingeschlagenen Weg, die Digitalisierung der Bundeswehr gemeinsam mit Industriepartnern anzupacken und fordert dessen Umsetzung. Erst das Netzwerk der Akteure trägt sinnvoll zur digitalen Souveränität bei.

4 Digitalkultur gestalten

Die Corona-Pandemie hat auch für die digitale Transformation der Bundeswehr ein Gelegenheitsfenster geöffnet. Wie zivile Unternehmen auch, musste die Bundeswehr kurzfristig ihre Soldaten und Mitarbeiter in das Home-Office senden und es wurde die Notwendigkeit verstanden, „aufgelockert“ zu arbeiten. Die Erfahrungen aus der Pandemie zeigen deutlich, dass die Digitalisierung eine wesentliche Grundlage für die Aufrechterhaltung der Arbeits- und Einsatzbereitschaft der Bundeswehr ist. Die Erkenntnis „Resilienz“ durch Digitalisierung muss auch über die Krise Bestand haben. Sie trägt nicht nur dazu bei, auch in Krisenzeiten arbeitsfähig zu sein. Der Aufbau von Remote-Arbeitsplätzen würde auch einen wichtigen Beitrag für die Attraktivität der Bundeswehr als Arbeitgeber leisten. Was bislang noch sperrig unter dem Begriff des „ortsunabhängigen Arbeitens“ firmiert und nur auf Antrag bei temporären familiären Notsituationen und persönlichen Gründen gewährt wird, sollte auch für die Mitarbeiter der Bundeswehr, die überwiegend Büroarbeit leisten, zum Normalfall werden. Für die Nutzung von Videokonferenzsystemen und Kollaborationstools muss ein Ausgleich zwischen den Anforderungen an VS-spezifische und offene Kommunikation geschaffen werden, sodass auch der Austausch mit externen Gesprächspartnern einfach und praktikabel mit einem nutzerfreundlichen und auch in ausreichender Zahl verfügbaren Angebot ermöglicht wird. Es muss unbedingt vermieden werden, dass Angehörige der

[7] https://www.bmwi.de/Redaktion/DE/Downloads/S-T/strategiepapier-staerkung-sicherits-und-verteidigungsindustrie.pdf?__blob=publicationFile&v=4

Bundeswehr aufgrund fehlender Mittel eine „Schatten-IT“ aufbauen, die mit unkalkulierbaren Sicherheitsrisiken verbunden ist.

Die Nutzung digitaler Medien erfordert den Aufbau einer Digitalkultur, die tatsächlich gelebt wird sowie die Förderung der Digitalkompetenz der Soldaten und zivilen Mitarbeiter. Jeder Angehörige des GB BMVg sollte bei Dienstantritt mit einem sicheren, persönlichen, mobilen Device ausgestattet werden Die digitale Transformation der Bundeswehr muss als Führungsaufgabe querschnittlich etabliert und agil gelebt werden. Das Konzept der Inneren Führung muss auch für das Digitale Zeitalter weiterentwickelt werden. Das Konzept des Führens mit Auftrag darf in der Praxis nicht durch das bloße Weiterleiten von E-Mails konterkariert werden. Soldaten müssen in der Digitalkompetenz geschult werden, um ihren Auftrag in hybriden Szenaren umsetzen zu können. Digitale Bildung muss auch in der Bundeswehr selbstverständlich werden!

Die Kompetenz junger digitalaffiner Soldaten, muss trotz bestehender starrer Laufbahnsysteme und Beförderungsregeln besser genutzt werden. Gleiches gilt für digitalaffine Reservisten, für deren Einsatz es eine strategische Personalplanung braucht. Eine Digitalkultur in der Bundeswehr braucht beides: Die technische Kompetenz genauso wie einen verantwortungsvollen Umgang mit digitalen Systemen und neuen Medien.

5 Zukunftstechnologien in die Gegenwart bringen

Die Bundeswehr muss über ihre Fähigkeiten präzise, zeitgerecht und flexibel verfügen, um sich im gesamten Einsatzspektrum durchzusetzen. Dieses Fähigkeitsspektrum wird sich zukünftig von von einem joint-approach über einen System-of-Systems-Ansatz bis zu einem (combined) Joint All Domain-Ansatz weiterentwickeln. Das geht nur unter durchgängiger Nutzung digitaler Technologien wie KI, Big Data, VR/AR etc.

Diese neuen Technologien müssen schnell mit dem Nutzer auf Wirkung getestet werden, die Abläufe in Führung, Aufklärung, Wirkung und Unterstützung verantwortungsübergreifend betrachtet und die digitalen Kompetenzen des Personals ergebnisorientiert auf- und ausgebaut werden. Dies betrifft insbesondere Technologien mit Schlüsselfunktion, mit denen sich der Bitkom Arbeitskreis Verteidigung bereits vertiefend auseinandergesetzt hat[8] und die im Folgenden exemplarisch anhand ausgewählter Beispiele vorgestellt werden.

[8] Siehe auch „Technologie-Steckbriefe“: https://www.bitkom.org/Bitkom/Organisation/Gremien/Verteidigung.html

5.1 Künstliche Intelligenz

Künstliche Intelligenz gehört zu den wichtigsten Zukunftstechnologien für die Bundeswehr. Die Spannbreite möglicher Einsatzfelder ist enorm und reicht von militärischen Anwendungen bei der Erfüllung hoheitlicher Aufgaben bis zum Einsatz bei der Optimierung der Verwaltung und Personal- und Materialbewirtschaftung. Eine erst im September 2020 durch den Bitkom durchgeführte Bevölkerungsumfrage zeigt, dass eine Mehrheit von 52 Prozent der Bevölkerung die Anwendung von KI im Militär kritisch sieht, wohingegen sich in fast allen Lebensbereichen eine Mehrheit den Einsatz von KI wünscht. Während im privaten Anwendungsbereich der schnelle Zugriff auf Informationen und Medien sowie die Unterstützung im Alltag durch intelligente Haushaltsgeräte oder den Autopiloten im KFZ wertgeschätzt wird, wird KI im militärischen Einsatz schnell auf intelligente Waffentechnologie und damit auf gesellschaftlich kontroverse Einsatzbereiche reduziert. Dabei kann nur mittels KI die Datenflut moderner Einsatzszenarien der Bundeswehr bewältigt und der Schutz der Soldaten gewährleistet werden. Bereits in naher Zukunft ist der Einsatz von KI als Ratgeber (recommendation engine) für den Einsatz im Militär praktikabel. Der Zugriff in Sekundenschnelle auf alle Informationen aus dem Internet, aus hunderttausenden Dokumenten, von Millionen von Sensoren, etc. ergänzt durch die Fähigkeit der KI, Änderungen in den Bedingungen blitzschnell in die Empfehlung einfließen zu lassen, Vorhersagen zu treffen und Simulationen verschiedener Szenarien zu erstellen, sind heute bereits Realität.

Bilderkennungstechnologien, Sprach- und Übersetzungsassistenten oder intelligente Wegführung in riskanten Einsatzgebieten sind weitere Beispiele für Anwendungen, welche die zügige Auftragserfüllung und die Sicherheit unserer Soldaten erhöhen. Ebenso kann durch Lösungen wie Predictive Maintenance die Verfügbarkeit und die Effizienz der technischen Hilfsmittel verbessert werden.

Aus Sicht des Bitkom brauchen wir einen vorurteilsfreien Blick auf die Anwendungsfelder von KI im Militär. Das im Bitkom weiterentwickelte „Periodensystem der KI“[9] kann dazu beitragen, eine sachgerechte Bewertung bestehender Anwendungsfälle von KI für die Bundeswehr vorzunehmen. Grundsätzlich sollte eine Regulierung bestimmter Technologien immer eine Anwendung und ihre Auswirkungen betreffen und nicht die Technologie als solche. In den Fällen, wo KI-Anwendungen in Hochrisikobereichen zum Einsatz kommen, muss konsequent an bestehende Regulierung und die bestehenden institutionellen Strukturen des jeweiligen Sektors angeknüpft werden. Dies betrifft

[9] https://www.periodensystem-ki.de/

besonders den sensiblen Bereich des Militärs und der Sicherheits- und Verteidigungsindustrie.

5.2 Quantencomputing

Quantentechnologien stellen ein querschnittliches Thema mit einem hohen Entwicklungspotenzial für die Forschung und damit auch für die Bundeswehr dar. Unter Quantencomputing (QC) versteht man grundsätzlich die Nutzung von Effekten auf Quantenebene zur Berechnung von Daten. Dadurch können Quantencomputer in bestimmten Anwendungsfällen klassischen Computern deutlich überlegen sein. Insbesondere könnten Quantencomputer, sobald ihre Einsatzreife erreicht ist, die mathematischen Probleme, auf denen asymmetrische Kryptografie beruht deutlich schneller berechnen als klassische Computer. Quantencomputer können so gängige asymmetrische Kryptografie-Verfahren brechen, deren Sicherheit auf der Laufzeit für Faktorisierungsverfahren beruht sowie die Sicherheit von symmetrischer Kryptographie halbieren. Das Brechen heute gängiger Verschlüsselungen durch QC stellt ein enormes Sicherheitsrisiko für Streitkräfte dar.

Den Vorteilen von Quantencomputern stehen gegenwärtig noch viele Probleme bei der technischen Realisierung gegenüber. Die Entwicklung ist aber keine Frage des »Ob?«, sondern des »Wann?« Brückentechnologien wie Field-Programmable Gate Arrays auf Basis des »Quanten inspired Computing« sind schon heute mit QC-Algorithmen nutzbar. Diese sind in der Lage Lösungen für signifikante Problemgrößen zu liefern und fügen sich nahtlos in bestehende Datacenter Infrastruktur ein. Auch hybride Systeme sind denkbar, welche die Vorteile beider Systeme in sich vereinen.

Es ist deshalb bereits jetzt unbedingt notwendig, sich auf einen eventuellen Technologiesprung vorzubereiten, sowohl bei der Hardware als auch bei den Algorithmen inklusive der Nutzung vorhandener Brückentechnologien. Dazu gehören die Verfügbarkeit und der Zugang zu Quantencomputern und die Intensivierung von Forschungsaktivitäten, wie beispielsweise am Forschungscluster CODE an der Universität der Bundeswehr in München sowie die Einsatzprüfung der Brückentechnologie u. a. für den Wissensaufbau in der Bundeswehr.

5.3 Blockchain

Durch die Blockchain kann ein sicherer organisationsübergreifender Datenaustauch und damit maximale Transparenz erreicht werden. Auch im Verteidigungsbereich sind verschiedene Einsatzszenarien der Blockchain Technologie denkbar. Hierzu gehört vor

allem die deutliche Erhöhung der Datensicherheit und des Datenschutzes. In der Logistik bietet sich die Nutzung von Blockchain Technologie zur Vermeidung von Missbrauch oder Verlust und zur Gewährleistung der Fälschungssicherheit an. Naheliegend erscheint die Anwendung damit für sicherheitsrelevante Güter, aus dem Bereich der Rüstung, wie Waffen und Munition oder der Chemie. Deren Herstellung, Einsatz, und Verfügbarkeit könnten durch die Blockchain transparent abgebildet werden. Auch könnte dies mit der Möglichkeit, diese Daten für das „Predictive Maintenance" nutzbar zu machen, verbunden werden. Auch die eindeutige Zuordnung digitaler Fahraufträge bei der Bundeswehr wäre ein konkreter Use-Case und möglicher Ansatzpunkt für einen sinnvollen Einsatz der Blockchain. Bei größeren, koordinierten Einsätzen im internationalen Rahmen wäre die Technologie zudem zur Steuerung der Personal- und der Einsatzkontingente denkbar.

Der Zugriff auf vertrauliche Informationen, Gesundheitsdaten, der Zugang zu sensiblen Gebäuden oder Fahrzeugen, die Benutzung von Verteidigungssystemen kann weiterhin durch die SSI (Self-sovereign identity) protokolliert und dezentral organisiert werden. Die SSI nutzt hierbei die Blockchain-Technologie um eine eindeutige, selbstbestimmte Identität Personen, Organisationen wie auch Maschinen zuzuweisen. So wie die Bundeswehr als Aussteller einmalig dem Benutzer diese Rechte zur Verfügung stellt, so kann er diese auch jederzeit wieder entziehen. Die Blockchain-Technologie liefert so die unumstößliche Beglaubigung von Daten, die der Bundeswehr helfen, sich dezentral zu organisieren und damit ihre Resilienz zu steigern.

5.4 Virtual und Augmented Reality

Durch Virtual Reality werden dem Nutzer in einem Headset computergenerierte Inhalte angezeigt. Seine reale Umgebung sieht er nicht. Ideal ist dies immer dann, wenn komplett in eine virtuelle Umgebung eingetaucht werden soll, etwa zur Schulung, Aus- und Weiterbildung. Per VR können Angehörige der Bundeswehr kostengünstig und gefahrlos die Bedienung komplexer Waffensysteme und Maschinen trainieren, Arbeitsabläufe lernen, Vorträge üben, aber auch soziale Fähigkeiten stärken. Möglich ist außerdem, ortsübergreifend zusammenzuarbeiten.

Augmented Reality funktioniert bereits mit Smartphone und Tablet, umfassender als mit AR-Brillen. Bei AR sieht der Nutzer in seiner realen Umwelt virtuelle Inhalte, und zwar idealerweise so, dass sie in Bezug zur realen Umwelt stehen. AR eignet sich im technischen Bereich insbesondere für Schritt-für-Schritt-Anleitungen. So können bei Wartungen und Reparaturen etwa Hinweise und Warnungen eingeblendet werden, einzelne Maschinenteile lassen sich hervorheben. Im medizinischen Bereich lassen sich während

OPs CT- oder MRT-Bilder auf den Patienten projizieren. Auch AR-Lernanwendungen existieren.

Den Nutzen für das Militär haben viele Nationen bereits erkannt. Bei der Bundeswehr besteht hingegen Nachholbedarf. Dabei ließe sich durch den Einsatz von VR und AR die Effizienz der Ausbildung deutlich steigern. Dies gilt nicht nur für die bereits skizzierten Anwendungsmöglichkeiten, die sowohl zivil als auch militärisch nutzbar sind. Auch originär militärische Einsatzmöglichkeiten bieten sich für AR/ und VR-Anwendungen an. So lässt sich der Wirkungsgrad der eigenen Waffensysteme durch die Verbindung von AR und Künstlicher Intelligenz in den Optiken und Visiereinrichtungen erhöhen. Eine intelligente Zielerkennung hilft zudem die Treffgenauigkeit zu optimieren und Kollateralschäden zu vermeiden. Nicht zuletzt tragen moderne Ausbildungs- und Simulationsmöglichkeiten maßgeblich zur Attraktivität der Ausbildung in der Bundeswehr bei. In diese sollten auch die spezifisch militärischen Anforderungen an die Belastbarkeit der Ausrüstung aber auch an die notwendigen Sicherheitsanforderungen integriert werden.

6 Fazit

Damit das Ziel der digitalen Transformation gelingt und neue Technologien für die Bundeswehr nutzbar gemacht werden, müssen der Weg zu einer digitalen Gesamtarchitektur der Bundeswehr konsequent fortgesetzt werden und die Erfahrungen der Digitalwirtschaft als Treiber von Innovationen genutzt werden.

Aus organisatorischer und prozessualer Sicht müssen Aufgaben, Arbeitsbeziehungen und damit einhergehende Abhängigkeiten innerhalb der Bundeswehr identifiziert, analysiert und auf das Digitalisierungspotenzial hin bewertet werden. Dabei sollten auch die Akzeptanz, Erwartungshaltung und Bereitschaft der Bundeswehrangehörigen in Bezug zur Digitalisierung berücksichtigt und gefördert werden.

Hierzu braucht es eine iterative Vorgehensweise, die Unsicherheiten akzeptiert und Geschwindigkeit vor Perfektion stellt. Dieser Grundgedanke ist richtig in der Umsetzungsstrategie Digitale Bundeswehr festgehalten und muss konsequent umgesetzt werden.

Auch in der Digitalisierung gilt das Pareto Prinzip: 80 Prozent der Leistung wird mit 20 Prozent des Einsatzes erreicht. In diesem Sinne kann ein Großteil der durch die Digitalisierung bereits heute angestrebten Wirkung durch den Einsatz bereits bestehender Technologie und Infrastruktur umgesetzt werden, während gleichzeitig die langfristigen

Ziele durch die Entwicklung zukunftsorientierter Schlüsseltechnologien weiter vorangetrieben werden. Dazu müssen die organisatorischen Einschränkungen und Richtlinien, die sich im Wesentlichen noch an den Handlungsmodellen papierorientierter Vorgehensweisen orientieren, an die bestehenden, verfügbaren Technologien und deren Möglichkeiten angepasst werden.

Gleichzeitig benötigt die Bundeswehr die entsprechenden personellen, materiellen und Ressourcen, damit sie ihren Auftrag erfüllen kann. Eine solide finanzielle Planbarkeit ist hierfür unabdingbar. Zur strukturellen Sicherung von Hochtechnologie sollte diese auch über den Einzelplan 14 hinaus gefördert werden.

Dies ist Grundvoraussetzung für einsatzbereite Streitkräfte und eine leistungsfähige Bundeswehrverwaltung im digitalen Zeitalter, die auf Bedrohungen aus dem Cyberraum bestmöglich vorbereitet ist und die Chancen der Digitalisierung umfassend und effizient nutzt.