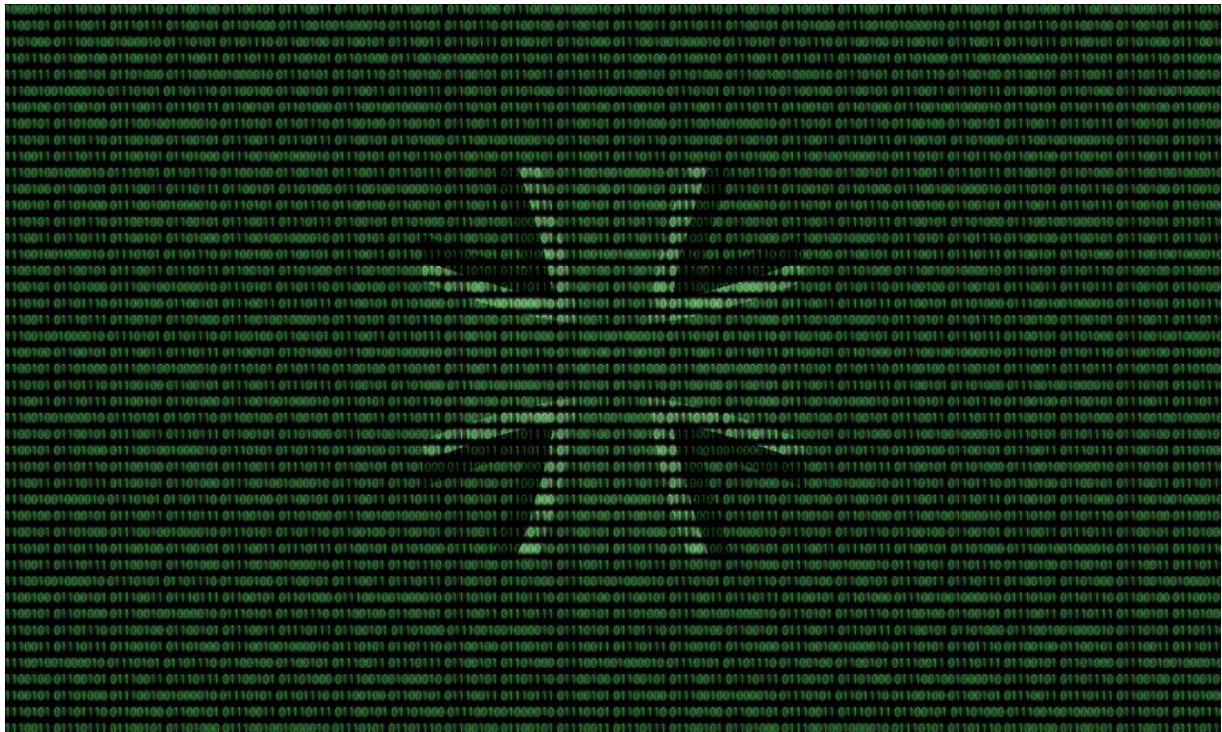




Dritter Bericht zur Digitalen Transformation des Geschäftsbereichs des Bundesministeriums der Verteidigung

Berlin, Februar 2021



Inhaltsverzeichnis

1.	Vorwort.....	3
2.	Einleitung	4
3.	Aktuelle Schwerpunktthemen des Leitungsboards Digitalisierung	7
3.1.	Auswirkungen von COVID-19 auf die Digitalisierung: Erhöhung der Resilienz der Bundeswehr durch Digitalisierung	7
3.2.	Fortschritte beim digitalen ortsunabhängigen und kollaborativen Arbeiten.....	9
3.3.	Innovative virtuelle Arbeitsumgebungen	13
3.4.	Analyse und Auswertung von Daten auf Basis SASPF.....	16
3.5.	Infrastrukturdatenmanagement.....	20
3.6.	Digitalisierung der Verwaltungsarbeit.....	22
4.	Stand der Digitalen Transformation des GB BMVg.....	24
4.1.	Zentrale Elemente.....	24
4.2.	Digitalisierungsaktivitäten.....	31
4.3.	Digitalisierungsfähigkeiten.....	37
5.	Ausblick	49
6.	Abkürzungsverzeichnis	50
7.	Abbildungsverzeichnis	53
8.	Anlage Eckpunktepapier	54

1. Vorwort

Die Digitale Transformation des Geschäftsbereiches des Bundesministeriums der Verteidigung (GB BMVg) schreitet weiter voran. Der erstellte dritte Digitalbericht stellt nach Herausgabe des zweiten Digitalberichts im Mai 2020 eine Fortschreibung zum Stand der Digitalisierung der Bundeswehr im Zeitraum bis Ende Dezember 2020 dar. Am 26. Juni 2020 wurde das vierte Leitungsboard Digitalisierung unter Leitung der Bundesministerin erstmals weitgehend digital durchgeführt. Die zentrale Steuerung wurde weiter gefestigt. Die Bilanz an dezentral umgesetzten Digitalisierungsaktivitäten ist beachtlich. Insgesamt standen und stehen die Digitalisierungsaktivitäten des GB BMVg unter dem Eindruck der COVID-19-Pandemie als einem bestimmenden Faktor.

Für die Bundeswehr galt und gilt es, auch unter den Bedingungen von COVID-19, ihren originären Auftrag zu erfüllen und die ständige Einsatzbereitschaft und Einsatzfähigkeit sicherzustellen. Der GB BMVg war gefordert, schnell aufzulockern und die Aufträge ortsunabhängig und „dezentral“ zu erfüllen. Ortsunabhängiges und kollaboratives Arbeiten unter Nutzung digitaler Arbeitsmittel und Werkzeuge war und ist ein Mittel, um Gesundheitsschutz für die Mitarbeitenden und Auftragserfüllung gewährleisten zu können. Gleichzeitig unterstützt die Bundeswehr die zivilen Gesundheitsbehörden im Kampf gegen die Pandemie.

Die Erfahrungen der Bundeswehr in der Pandemielage haben deutlich unterstrichen, dass Digitalisierung heute eine wesentliche Grundlage für die Aufrechterhaltung der Arbeitsfähigkeit und Einsatzbereitschaft der Bundeswehr ist.

Resilienz durch Digitalisierung – so lautet eine klare Erkenntnis aus der Corona Krise.

2. Einleitung

Digitalisierung bleibt – nicht nur vor dem Hintergrund der aktuellen COVID-19-Pandemie – weiterhin eine der vordringlichsten Herausforderungen für Staat und Gesellschaft. Die Bedeutung wurde auf Seiten der Bundesregierung erkannt und zu einem Schwerpunktthema der Legislaturperiode gemacht. Daher ist die konsequente Umsetzung der Digitalisierung eine Aufgabe für den gesamten GB BMVg. Sie hat zudem herausragende Relevanz für die Zukunftsfähigkeit der Bundeswehr.

Die Digitale Transformation betrifft weitaus mehr als nur technische Aspekte: Das Denken und Handeln im gesamten GB BMVg sind von der Digitalisierung betroffen. Vor diesem Hintergrund setzt das Leitungsboard Digitalisierung periodische Schwerpunkte, um ausgewählte Themen intensiv und umfassend zu betrachten.

Das vierte Leitungsboard Digitalisierung, dessen Inhalte und Entscheidungen Kern des vorliegenden Berichts sind, befasste sich im Schwerpunkt mit den Auswirkungen der COVID-19-Pandemie sowie in diesem Zusammenhang mit Digitalisierungsaktivitäten für digitales, mobiles und virtualisiertes Arbeiten.

In Anbetracht der aktuellen Lage durch die COVID-19-Pandemie wurde die Notwendigkeit von Veränderungen des Arbeitsplatzes deutlich aufgezeigt: Ortsunabhängiges Arbeiten und mobile, auch für die Ausbildung geeignete Kommunikations- und Kollaborationsmöglichkeiten sind nun mehr denn je ein hoch relevantes Thema für die Bundeswehr und werden mit Nachdruck verfolgt. Resilienz durch aufgelockertes Arbeiten und Ausbilden steht im Fokus. Daraus erwachsen Chancen und Herausforderungen gleichermaßen.

Das Beschleunigen der Digitalisierung der Bundeswehr durch das Sonderprogramm „Resilienz der Bundeswehr durch Digitalisierung“ dient einem übergeordneten Ziel: Das konsequente Verbessern der Einsatzbereitschaft der Bundeswehr – unabhängig von jeder Lageentwicklung.

Vorhaben mit unmittelbarem Bezug zu den Schwerpunktthemen Resilienz und digitaler, mobiler und virtualisierter Arbeits- und Ausbildungsplatz sind in diesem Bericht im Abschnitt 3 vorangestellt, bevor zu Fortschritten in weiteren Feldern der Digitalisierung im Abschnitt 4 ausgeführt wird.

Aus dem Berichtszeitraum ebenfalls hervorzuheben ist die seit dem 1. Juli 2020 für sechs Monate übernommene EU-Ratspräsidentschaft (EU-RP) der Bundesrepublik Deutschland. Auch das BMVg hat unter dem übergeordneten Ziel „Resilienz der EU“ die Digitalisierung als einen Themenschwerpunkt identifiziert. Ziel war es, im Rahmen der Gemeinsamen Sicherheits- und Verteidigungspolitik die digitalen Kompetenzen und Cyberverteidigungsfähigkeiten der europäischen Streitkräfte weiter zu stärken. Die Grundlagen hierfür wurden u.a. durch einen institutionalisierten Dialog (Defence CIO-Council) mit den europäischen Partnern, die Zeichnung eines multinationalen Konzeptes des Cyber and Information Domain Coordination Centre (CIDCC) und verschiedene Ausbildungsmodule geschaffen. Im Deutschen EU-RP Programm wurde digitale Souveränität in einer globalisierten Welt als Leitmotiv der europäischen Digitalpolitik verankert.

Zur Einordnung des Digitalberichts ist anzumerken, dass die weitere Berichterstattung zu den Rüstungsprojekten des Teilportfolios Cyber/IT, so auch der beiden der Kategorie A zugeordneten Rüstungsprogramme Digitalisierung Landbasierte Operationen (D-LBO) und Harmonisierung der Führungsinformationssysteme (HaFIS), gemäß den Maßgaben des Haushaltsausschusses des Deutschen Bundestages ab dem dritten Sachstandsbericht des BMVg zum „Cyber- und Informationsraum“ (CIR) dort zusammengeführt wird. Der Sachstandsbericht CIR enthält auch weitere haushaltsrelevante Informationen, auf diese wird im Digitalbericht daher verzichtet. Da die Digitalisierung der Bundeswehr über die Dimension CIR hinaus alle Dimensionen betrifft und bundeswehrgemeinsam im Leitungsboard Digitalisierung gestaltet wird, führt das BMVg die Berichterstattung zur Digitalen Transformation des GB BMVg im Digitalbericht fort, um das in der Öffentlichkeit und der Bundeswehr vorliegende hohe Informationsinteresse zu decken.

Chancen und Risiken

Chancen, Herausforderungen und Risiken der Digitalen Transformation aus der übergeordneten Perspektive wurden im ersten und zweiten Bericht zur Digitalen Transformation beschrieben und behalten weiter Gültigkeit.

Rahmenbedingungen und strategischer Ansatz

Grundlagendokumente für die Digitale Transformation im GB BMVg bilden weiterhin die *Strategische Leitlinie Digitalisierung* sowie die *Umsetzungsstrategie Digitale Bundeswehr* mit dem darin beschriebenen Vorgehensmodell der zentralen Steuerung bei dezentraler Umsetzung. Beide Dokumente sind neben der *Umsetzungsstrategie der Bundesregierung „Digitalisierung gestalten“* maßgeblicher Bestandteil des nationalen politischen Rahmens.

Darüber hinausgehende Einordnungen im nationalen politischen Rahmen sowie die Betrachtung rechtlicher Rahmenbedingungen der Digitalen Transformation und internationaler Verpflichtungen des GB BMVg wurden im ersten und zweiten Bericht zur Digitalen Transformation vorgenommen und behalten ebenfalls Gültigkeit.

3. Aktuelle Schwerpunktthemen des Leitungsboards Digitalisierung

Das Leitungsboard Digitalisierung ist das zentrale Steuerungs- und Entscheidungsgremium der Digitalen Transformation im GB BMVg unter Leitung des BMVg. Um eine zielgerichtete, fokussierte und umfassende Betrachtung zu gewährleisten, sind die jeweiligen Sitzungen des Leitungsboards und des vorbereitenden Steuerungspanels auf Schwerpunktthemen ausgerichtet, die sich aus den in der Umsetzungsstrategie Digitale Bundeswehr aufgeführten Zielen ergeben.

Aufgrund der besonderen Relevanz und Aktualität fokussierte sich das vierte Leitungsboard Digitalisierung am 26. Juni 2020 auf die Auswirkungen der COVID-19-Pandemie auf die Digitalisierung im Allgemeinen sowie auf die Maßnahmen zur Erhöhung der Resilienz und die Fortschritte beim digitalen ortsunabhängigen und kollaborativen Arbeiten im Besonderen.

3.1. Auswirkungen von COVID-19 auf die Digitalisierung: Erhöhung der Resilienz der Bundeswehr durch Digitalisierung

Die COVID-19-Pandemie ist für die Bundeswehr, genauso wie für weite Teile des gesellschaftlichen Lebens, Treiber und Bewährungsprobe der Digitalisierung zugleich. Die laufende Digitalisierung der Bundeswehr konnte wesentliche Beiträge zu Resilienz und Einsatzbereitschaft leisten. Insbesondere die kurzfristige Umwandlung einer großen Anzahl bis dato fester bürogebundener in flexible ortsunabhängige Arbeitsplätze stellt auch den GB BMVg vor Herausforderungen – sowohl beispielsweise im Hinblick auf die Bereitstellung notwendiger Hard- und Software als auch auf veränderte Arbeits- und Kommunikationsweisen. Die auf Antriebe zur Verfügung stehenden sowie die kurzfristig erreichten Digitalisierungslösungen haben gezeigt, dass der GB BMVg gut aufgestellt war und die Digitalisierungsstrategie der Bundeswehr wirkt. So konnte schnell und zielgerichtet reagiert werden.

Hinsichtlich der Systemarchitektur und der Kapazitäten bedurfte es einer schnellen strategischen Anpassung, denn selbst wenn mobile Endgeräte zur Verfügung standen, waren die Netze und Zugänge zunächst nicht darauf ausgelegt. Eine ganzheitliche Planung unter Berücksichtigung der vollständigen Servicekette vom Endgerät, über das sichere Netzwerk bis zu den Rechenzentren ist entscheidend. Die Digitalisierung gewinnt durch zusätzliche Mittel aus dem Konjunktur- und Zukunftspaket der Bundesregierung an Tempo und es gilt, diese Entwicklung in den nächsten Jahren fortzusetzen und das Erreichte zu verstetigen.

Die Aktivitäten zur Erhöhung der Resilienz durch Digitalisierung zielen ab auf eine Beschleunigung der Digitalisierung der Bundeswehr auf unterschiedlichen Ebenen – im Einsatz- und Grundbetrieb, in der Truppe, auf der Ämter- und Kommandoebene, in den Akademien, in Ausbildung und Qualifizierung, Forschung und Verwaltung für alle Aufgaben der Bundeswehr im Rahmen der Landes- und Bündnisverteidigung, des Internationalen Krisenmanagements, des Heimatschutzes und der Cybersicherheit und -verteidigung. Fokus des Programms ist der Ausbau und die Verstetigung der Möglichkeiten zum ortsunabhängigen Arbeiten.

Ziele des Sonderprogramms „Resilienz durch Digitalisierung“ im Einzelnen sind

- langfristige Durchhalte- und Einsatzfähigkeit der Bundeswehr, angepasst an Lageentwicklungen in allen Bereichen – Ausbildung, Qualifizierung, Grundbetrieb einschließlich Gesundheitsversorgung und ressortübergreifender und multinationaler Einsatz von Bundeswehr-Kräften,
- qualitativ und quantitativ bestmögliche Verfügbarkeit von IT zum digitalen ortsunabhängigen und kollaborativen Arbeiten zum Schutz der Angehörigen der Bundeswehr,
- vertrauenswürdige IT-Services auch unter den Bedingungen des dislozierten Arbeitens.

Das Sonderprogramm listet daher 42 Maßnahmen auf zur

- Erhöhung der Anzahl der Endgeräte für mobiles und ortsunabhängiges Arbeiten,
- Steigerung des Ausbaus der IT-Services für kollaboratives Arbeiten,
- digitalen Ausbildung und Qualifizierung,
- Digitalisierung der Gesundheitsversorgung,
- Anpassung der Backend-IT-Infrastruktur für mobiles Arbeiten,
- Verbesserung der IT-Sicherheit und des Datenschutzes,
- Verbesserung der internationalen Zusammenarbeit im Kontext EU und NATO,
- Verbesserung der ressortübergreifenden Zusammenarbeitsfähigkeit und
- Verbesserung der Führungs- und Arbeitsfähigkeit und damit der Einsatzbereitschaft der Bundeswehr.

3.2. Fortschritte beim digitalen ortsunabhängigen und kollaborativen Arbeiten

Die Bereitstellung eines digitalen, mobilen und virtualisierten Arbeitsplatzes ist eine Grundvoraussetzung für die Digitale Transformation und beinhaltet sowohl infrastrukturelle, technische sowie kulturelle Aspekte. Die Hardwareausstattung des Arbeitsplatzes ist ebenso darunter gefasst wie die Bereitstellung und Nutzung moderner Kommunikations- und Kollaborationstools und die Möglichkeit des sicheren und endgeräteunabhängigen Zugriffs auf alle für die Arbeit relevanten Informationen.

Die Fortschritte in diesem Schwerpunktthema sind daher eng verknüpft mit den Maßnahmen und Erfolgen aus dem Resilienzprogramm. Erste Maßnahmen wurden bereits in 2020 als Sofortmaßnahmen eingeleitet und umgesetzt.

Die Fähigkeit zum Arbeiten im Homeoffice konnte wesentlich gesteigert werden:

- die Bandbreite der zentralen Internetübergänge wurde von 10 GB/s auf 100 GB/s verzehnfacht,
- eine CISCO WebEx Lösung (OFFEN) für zunächst ca. 7.000 Nutzer (ohne dienstliche mobile IT) im Homeoffice eingerichtet,
- mehr als 10.000 Notebooks beschafft und
- die Infrastruktur zum gesicherten mobilen Zugriff für bis zu 30.000 gleichzeitige Nutzer ertüchtigt.

Mit der vorgezogenen Beschaffung von 5.000 Handfunkgeräten für das ressortübergreifende Funknetz Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben wurde die Fähigkeit der Truppe zum ressortgemeinsamen Einsatz rasch gesteigert. Softwarelösungen für mobilen Zugriff und eine COVID-19 Lagedarstellung wurden im Laufe des Jahres 2020 entwickelt. Derzeit werden die notwendigen Vorbereitungen zur Umsetzung der weiteren Maßnahmen ab 2021 getroffen. Maßgeblich ist dafür eine geplante Leistungserweiterung des HERKULES-Folgeprojektes. Die parlamentarische Behandlung ist für die 20. Kalenderwoche 2021 geplant.

Ein kurzfristiger Schwerpunkt lag in der Steigerung von Kapazitäten für Anwendungen im Bereich des Messagings.

Beispiel: Messenger in der Bundeswehr

Im Rahmen eines Innovationsvorhabens des Cyber Innovation Hubs der Bundeswehr (CIHBw) wurde seit 2018 der kommerziell verfügbare Messenger „stashcat“ im Pilotbetrieb auf freiwilliger Basis ausschließlich auf privaten Endgeräten pilotiert. Infolge der COVID-19-Pandemie wurde temporär das Lizenzkontingent „stashcat“ (BwChat) erhöht. Auf Grundlage der durch die BWI GmbH (BWI) bis Ende 2020 geschlossenen Verträge konnten zunächst 20.000 Nutzer teilnehmen. Durch die von dem zivilen Anbieter im Rahmen seines „Disaster Response Programs“ eingeräumten – auf maximal 6 Monate befristeten Unternehmenslizenz – konnten bis zu maximal 50.000 Nutzer mit BwChat unterstützt werden.

Um die vorhandene Fähigkeitslücke beim Messaging auch auf dienstlichen Endgeräten schnellstmöglich zu beseitigen, wird seit Mitte 2019 gemeinsam mit der BWI und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) an der Umsetzung einer für VS-NfD zulassungsfähigen Messenger-Lösung für mobile Endgeräte in der Bundeswehr unter der Bezeichnung BwMessenger gearbeitet. Der Lösungsansatz (auf der Basis der Open-Source-Lösung MATRIX) wird im „On-Premise“ Betrieb durch die BWI in Bundeswehreigenen Rechenzentren betrieben.

Inzwischen wurde der BwChat Messenger weitgehend durch den BwMessenger MATRIX abgelöst und steht aktuell für 80.000 Endgeräte (50.000 private sowie 30.000 dienstliche Endgeräte) für die „Offene“ Kommunikation zur Verfügung. Darüber hinaus ist der Pilot des BwMessenger MATRIX für die VS-NfD Kommunikation Ende 2020 gestartet. Der Übergang erfolgt bruchfrei (Abbildung 1)



Abbildung 1: Messenger-Nutzung in der Bundeswehr - Wechsel von BwChat zu BwMessenger

Durch die Aktivitäten zur Erhöhung der Resilienz wird ebenso die Umsetzung bereits bestehender Vorhaben beschleunigt, um ortsunabhängiges Arbeiten in der Breite zu ermöglichen. Die qualitative und quantitative Verfügbarkeit von IT zum ortsunabhängigen Arbeiten wird u.a. durch die sogenannte Mobilitätsquote gemessen.

Ziel ist es, die Mobilitätsquote von 4% (Ende 2019) über 11% (Juni 2020) auf 66% in 2024 zu erhöhen. Dies bedeutet, 66% aller IT-Nutzer im GB BMVg sollen in der Lage sein, ab 2024 komplett ortsunabhängig arbeiten zu können.

Die Resilienzmaßnahmen sowie inhaltliche und quantitative Erweiterungen des HERKULES-Folgeprojektes unter Berücksichtigung der durch das Konjunktur- und Zukunftsprogramm zurätzlich zur Verfügung gestellten Finanzmittel tragen wesentlich dazu bei, dieses Ziel zu erreichen.

Eine weitere im Leitungsboard Digitalisierung nachgehaltene Maßnahme zur Unterstützung des ortsunabhängigen Arbeitens ist die Einführung von Groupware Bw als bundeswehrgemeinsame Kollaborationsplattform.

Beispiel: Groupware Bw

Mit Groupware Bw wird eine technische und organisatorische Klammer über bereits existierende Insellösungen im IT-System der Bundeswehr (IT-SysBw) bereitgestellt. Das Ziel ist eine einheitliche Plattform für die verschiedensten Arten der Kollaboration (gemeinsame Arbeit an Dokumenten, E-Mail, Terminplanung, Video- und Webkonferenzen, Chat, Telefonie), in der Mitarbeiter/-innen eingebunden sind und das Wissen geteilt werden kann. Die Plattform unterstützt ein flexibles Arbeitsumfeld und ermöglicht sowohl die traditionelle Arbeitsweise im Büro als auch zu Hause oder von unterwegs mit Mobilgeräten. Die Zusammenarbeit wird gefördert, ohne dabei die Informationssicherheit und den Schutz persönlicher Daten außer Acht zu lassen. Die Harmonisierung, funktionale Erweiterung und Modernisierung erfolgt im Wesentlichen durch Standard-Softwarelösungen, vorrangig von Microsoft und Cisco, und löst auf der IBM-Produktfamilie basierende Lösungen, wie z.B. IBM Notes ab (Abbildung 2).

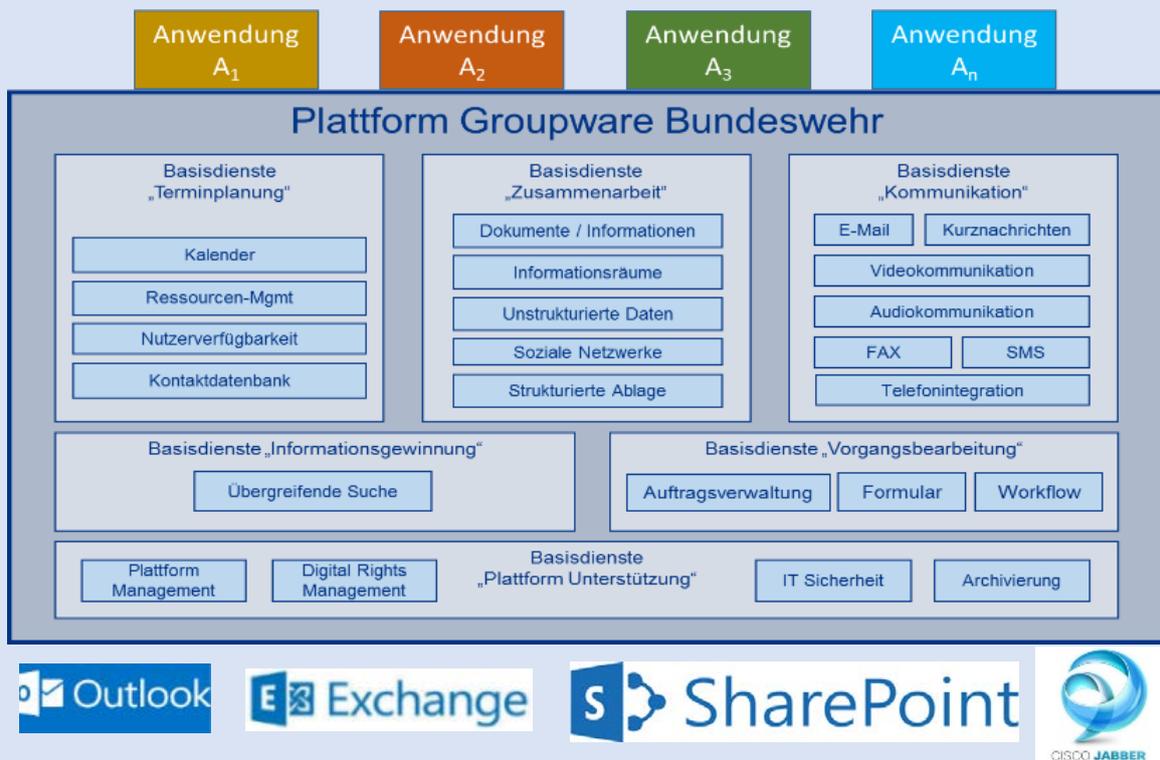


Abbildung 2: Groupware Bw

Die laufende erste Phase deckt die Fortführung der Realisierung mit Aufbau, Einrichtung und Rollout der Groupware Bw ab. Die organisatorische Einrichtung, Öffnung und Besetzung der Dienstposten für die zentralen Unterstützungselemente –

Programmorganisation im Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAAINBw) und das Kompetenzzentrum „Elektronische Verwaltungsarbeit/Collaboration, Digital Administration, Information Management“ (eVA/CDI) im Kommando Cyber- und Informationsraum (KdoCIR) sowie die Gruppe Stabs- und Verwaltungshandeln im Streitkräfteamt (SKA) – wurde veranlasst. Mit Beginn der Realisierung ist mit dem Schwerpunkt der „Mitwirkungshandlungen“ der ablauf- und aufbauorganisatorische Aufbau personeller Kapazitäten in allen Organisationsbereichen/Bereichen parallel zur zeitnahen Einrichtung, Öffnung und priorisierten Besetzung der Dienstposten dringend erforderlich. Der Pilot-Rollout Groupware Bw wird im Zeitraum Oktober 2021 bis November 2021, der Flächenrollout dann ab Dezember 2021 erfolgen.

Das Sonderprogramm Resilienz und die weiteren beispielhaft dargestellten Vorhaben bieten den Einstieg in den digitalen, mobilen und zunehmend auch virtualisierten Arbeitsplatz der Zukunft.

3.3. Innovative virtuelle Arbeitsumgebungen

Neben der Ausweitung der Möglichkeiten zum ortsunabhängigen Arbeiten werden innovative Formen der dislozierten Zusammenarbeit und interaktiven Kollaboration mit Hilfe von Virtual Reality (VR) und die damit verbundenen disruptiven Veränderungen von Arbeitsweisen experimentell untersucht.

Beispiel: VR-Lage – Experimentelle Realisierung VR-gestützter Lageraum für die Lw

Das Innovationsexperiment VR-Lage untersucht die technologischen Fähigkeiten von Virtual Reality (VR) in der dislozierten Zusammenarbeit, im Umfeld der Planung, der Vor- und Nachbesprechung von Missionen bei der Luftwaffe. Es wurde ein experimenteller virtueller Raum geschaffen, ausgestattet mit einem virtuellen Lagetisch in 4D (räumliche und zeitliche Zuordnung von Objekten) und vielen Kollaborationsfunktionen wie z.B. Whiteboards, Gruppengesprächsfunktion, Haft- u. Sprachnotizen, etc..

Um den Bezug zur realen Nutzung im Experiment herzustellen, wurden – über das Kommando Luftwaffe – das Zentrum für Luftoperationen, das Zentrum für Softwarekompetenz der Bundeswehr, das Luftwaffentruppenkommando und das Taktische Luftwaffengeschwader 31 eingebunden. Die Ergebnisse der Untersuchungsgegenstände und der zu überprüfenden Hypothesen wurden nach dem Abschluss des Experiments Ende Mai 2020 im Studienbericht zusammengefasst.

Seit Oktober 2020 wird das Experiment in einer Phase II mit einer erweiterten Zielsetzung zur Erprobung fortgesetzt. Schwerpunkte sind die Durchführung des vollständigen Missionsplanungsprozesses mit einem erweiterten Teilnehmerkreis und eine erste Bewertung der Lösungsbausteine hinsichtlich der Realisierungsmöglichkeit unter Einhaltung der Vorgaben zur Informationssicherheit bei einer Nutzung im IT-SysBw. Der Abschluss der Phase II ist für April 2021 geplant.

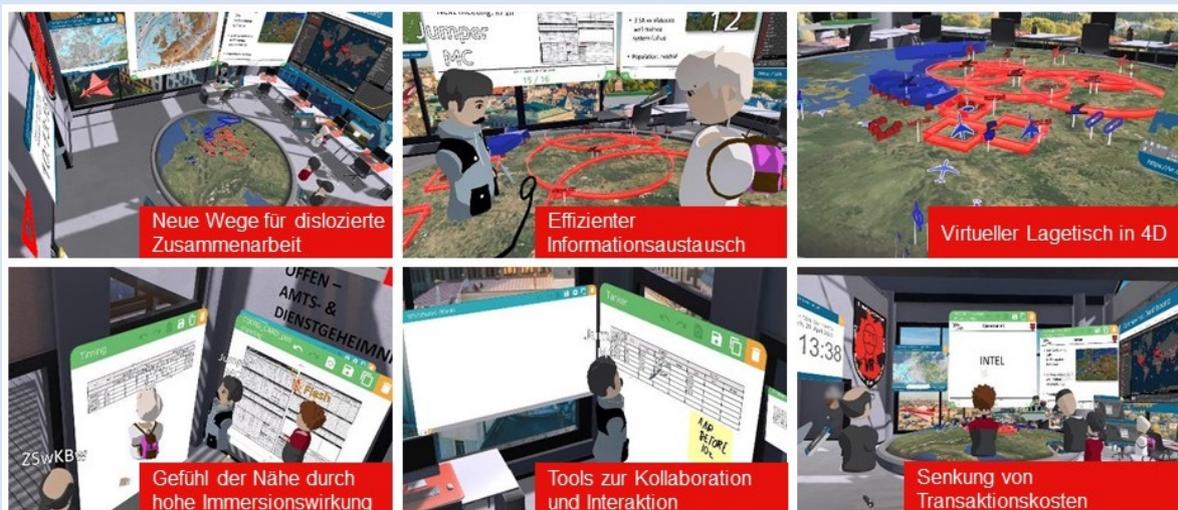


Abbildung 3: Experiment VR-gestützter Lageraum – ein Schritt in Richtung Zukunft

Ein weiteres experimentelles Vorhaben unter Einsatz der VR-Technologie stellt das Virtual Reality-Truppenbesuchszentrum (VR-TrBesZ) im Bereich der Personalgewinnung als ein Innovationsvorhaben des Cyber Innovation Hubs der Bundeswehr (CIHBw) dar.

Beispiel: Virtual Reality-Truppenbesuchszentrum

Das virtuelle Truppenbesuchszentrum bietet die Möglichkeit für Bewerberinnen/Bewerber und Interessierte, alltägliche Arbeitssituationen der Bundeswehr orts- und zeitunabhängig in einer virtuellen Realität (Cave Automatic Virtual Environment – CAVE) im Umfeld der Personalgewinnung zu erleben und in Mangelberufe/außergewöhnliche Berufsbilder „reinzuschnuppern“.

Das VR-TrBesZ verhindert die hohe Ressourcenbindung der Truppe (personell, materiell, finanziell) bei klassischen Truppenbesuchen und ermöglicht Aktivitäten, die rechtlichen bzw. sicherheitspolitischen Einschränkungen unterliegen (z.B. das Mitfahren im U-Boot).

Das Pilotprojekt ist am 1. Januar 2020 gestartet und befindet sich derzeit in der Evaluationsphase. Ein Prototyp der CAVE mit einem Content zum Berufsbild „Sonarmaat“ U-Boot befindet sich im Bundesamt für das Personalmanagement der Bundeswehr (BAPersBw) in Köln-Gremberghoven.

Das BAPersBw leistet hier in enger Zusammenarbeit mit dem CIHBw, der Marine und einer engagierten vertragsgebundenen Firma (in Kooperation mit einem weiteren Unternehmen) einzigartige Pionierarbeit. Das Projekt wird mit der Umsetzung zwei weiterer Contents zu Berufsbildern der Luftwaffe und des Heeres prototypisch fortgesetzt.



Abbildung 4: VR-TrBesZ – Berufsbilder zum virtuellen (Er-)Leben erwecken

3.4. Analyse und Auswertung von Daten auf Basis SASPF

Im GB BMVg wurde die herausgehobene Bedeutung der Analyse- und Nutzungsmöglichkeiten komplexer Daten und großer Datenmengen als weitere Grundlage digitaler Arbeits- und Entscheidungsprozesse erkannt. Wesentlicher Anknüpfungspunkt hierfür ist das Programm zur Einführung und Nutzung von Standardsoftware SASPF¹.

Beispiel: Analyse-, Auswertemöglichkeiten in SASPF - Bedeutung von Daten

Seit 2016 steht das SASPF Business Warehouse mit der In-Memory-Datenbank SAP HANA für Analyse- und Auswertemöglichkeiten in SASPF als Plattform in (nahe) Echtzeit zur Verfügung.

Die SASPF Business Analytics Plattform unterstützt das strukturierte Speichern und Abrufen von relevanten Daten aus allen Bereichen – von Personal und Finanzen über Ausrüstung bis hin zu Logistik, Infrastruktur und IT, verknüpft und harmonisiert sie und erlaubt auch den direkten Zugriff auf transaktionale Daten des SASPF Enterprise Resource Planning (ERP) Systems und Systemen in Nutzung (SinN) sowie weiterer externer Quellen (Abbildung 5).

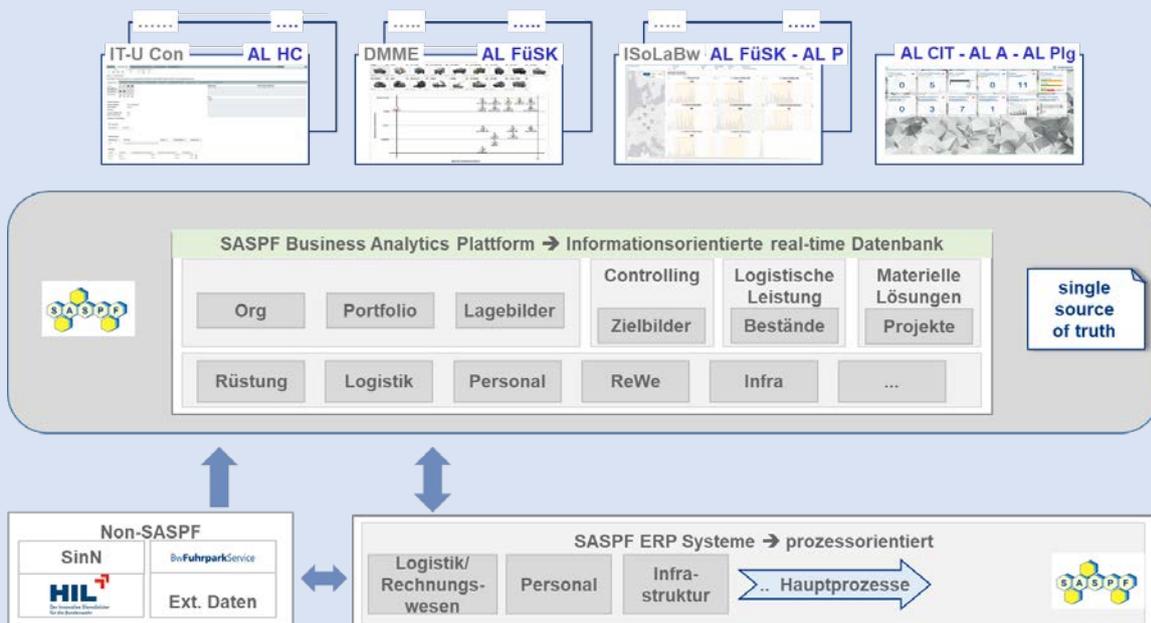


Abbildung 5: SASPF Plattform und Übersicht Lagebilder/Dashboards

Ferner bietet sie Funktionalitäten, die nicht nur den Blick in die Vergangenheit („was ist passiert“) richten, sondern zusätzlich die Vorhersage zukünftiger Ereignisse („was wird voraussichtlich passieren und unter welchen Voraussetzungen“) in den Vordergrund rücken.

¹ SASPF = Standard-Anwendungs-Software-Produktfamilien

Erste Ergebnisse zeigen eine hohe Genauigkeit der Prognose von Haushaltsmittelabflüssen im Bereich der IT-Titel.

Das hierauf aufsetzende SASPF-Projekt IT-Unterstützung Controlling unterstützt die strategische Steuerung des GB BMVg. Inhaltlich bildet das Projekt dazu alle notwendigen Informationen ab und leistet mit seinen Analyse- und Anwendungswerkzeugen einen wesentlichen Beitrag zur zentralen Steuerungsfähigkeit des BMVg, auch unter zeitkritischen Bedingungen.

Mittels der IT-Unterstützung Controlling (IT-U Con) werden verschiedene Lage-/Zielbilder, wie z.B. Digitalisierung Meldewesen Materielle Einsatzbereitschaft (DMME), Haushalt, Innere und Soziale Lage der Bundeswehr (ISoLaBw) sowie ein Dashboard zur Verfügung gestellt. Das Dashboard ermöglicht einen schnellen Überblick über Projektstände, Personal- und Haushaltslagen, Projektrisiken und weitere Leistungskennzahlen (Abbildung 6) und bietet weitere detaillierte Sichten und Filterfunktionen in speziellen Themengebieten eines Projektes.

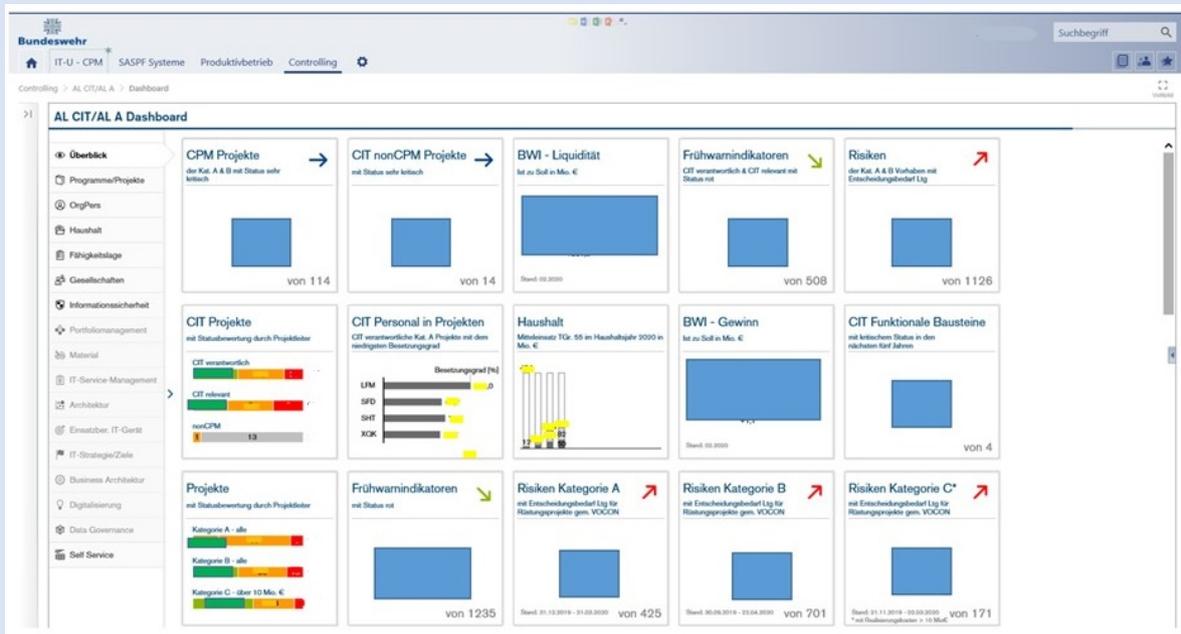


Abbildung 6: Dashboard, Ansicht Überblick

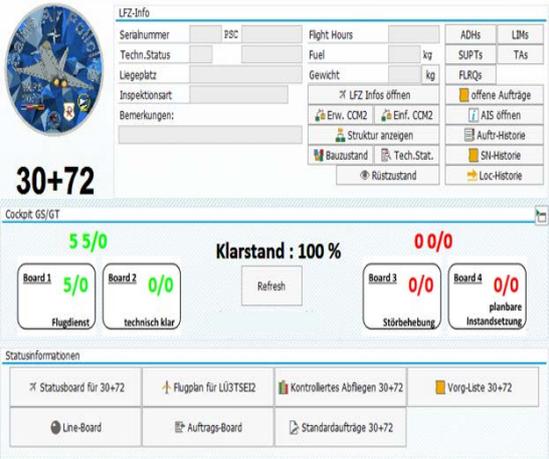
In einem Dashboard wird aktuell z.B. die Digitalisierung Meldewesen Auslieferung Material (DMAM) realisiert, mit dem der vertraglich vereinbarte und aktuell abgestimmte Stand der Auslieferungsplanung von Material sowie die tatsächlichen Auslieferungen erfasst werden,

um eine Gegenüberstellung zwischen SOLL und IST der Auslieferung von Material zu visualisieren.

Aktuell hervorzuheben ist ferner das SASPF-Projekt „IT-Unterstützung Digitalisierung Lagebilder“ (IT-U DigLage), für das am 23. März 2020 die Auswahlentscheidung (AWE) durch Herrn GenInspBw getroffen wurde und aktuell die Realisierung der Engpassmateriallage begonnen hat.

Ein weiteres SASPF-Projekt steigert die Attraktivität von SASPF durch die Bereitstellung moderner Benutzeroberflächen. Zeitgemäße Benutzeroberflächen-„Apps“ erleichtern die Einarbeitung in SASPF, steigern die Produktivität und erhöhen durch Fehlervermeidung die Datenqualität. Die Bereitstellung von ersten Apps aus diesem Projekt soll 2021 erfolgen und wird zum Projektabschluss an die BWI überführt. Der Start dieser „App-Factory“ soll im Januar 2022 erfolgen.

Als Grundlage dienen die von der Luftwaffe eigenentwickelten und bereits in den Eurofighterengeschwadern ausgerollten nutzerorientierten graphischen Benutzeroberflächen (Graphical user interface Extended kurz: GuiXT). Die Luftwaffe kann mit diesen Oberflächen bereits heute die IT-Unterstützung SASPF in den fliegenden Verbänden erheblich vereinfachen und damit einen Beitrag zur Steigerung der Einsatzbereitschaft der Luftwaffe leisten. Vorteile durch diese Vereinfachung sind insbesondere zeitliche Ersparnisse in der Bearbeitung und eine Erhöhung der Datenqualität durch die Vermeidung von Fehleingaben. Um die Nutzerorientierung technologieunabhängig strategisch zu verstetigen, wurde durch die Luftwaffe für das Programm SASPF eine User Experience Strategie SASPF erarbeitet.



The screenshot shows a digital cockpit interface for aircraft 30+72. It includes a top-left logo, a central 'Cockpit GS/GT' section with 'Klarstand : 100 %' and '5 5/0', and a bottom 'Statusinformationen' section. The interface is clean and organized, with clear data points and navigation options.

- ✓ Auf den Nutzer zugeschnittene Übersichtlichkeit
- ✓ Beachtliche zeitliche Ersparnis
- ✓ Bestmögliche Vermeidung von Fehleingaben
- ✓ Erhöhung der Datenqualität
- ✓ Vereinheitlichung der Betriebs- und Arbeitsabläufe (Flottenweit)

→ **Zusammenfassend:**
Signifikante Steigerung der Anwenderfreundlichkeit

Abbildung 7: Digitalisierungsprojekt GuiXT Luftwaffe – Optimierte Benutzeroberflächen

Mit steigenden Anforderungen hinsichtlich Autarkie, Schnelligkeit, Verfügbarkeit und Informationssicherheit werden Trendthemen wie Advanced Analytics, Internet of Things, Machine Learning, Augmented Reality und insbesondere auch prädiktive Anteile („schwache Künstliche Intelligenz (KI)“ in SASPF weiter ausgebaut und damit innerhalb des zentralen Programms für den strukturierten Umgang mit administrativ-logistischen Daten neue Qualitäten der Informationsbereitstellung zur Folge haben.

Die stetig wachsende Verfügbarkeit von Daten ist dabei nicht nur zu managen, sondern deren Potenzial als eigener „Unternehmenswert“ in der bei SASPF verfügbaren „Business Analytics Plattform“ zu nutzen. Dazu sind die verfügbare Menge von Daten, die Datenqualität und deren Nutzung die Werttreiber für eine „Daten-Wertschöpfungskette“. Für das Gesamtsystem SASPF stellte bei einschlägiger Bewertung auch der Bundesrechnungshof die Sinnhaftigkeit eines zentralen Business Warehouse heraus. Ein weiterer Ausbau der SASPF Business Analytics Plattform trägt dem Rechnung und verhindert – wenn konsequent genutzt – so einen unstrukturierten Aufbau von parallelen Daten- und Analysetools.

Das BMVg erarbeitet derzeit eine Datenstrategie, die auf die konkreten Mehrwerte der Datennutzung innerhalb des GB BMVg ausgerichtet ist. Die Etablierung einer Data Governance zur Verbesserung der eigenen Organisation, Sicherung einer hohen Datenqualität und Steigerung der Datenkompetenz sind dabei drei wichtige Handlungsfelder. Eine schlagkräftige Data Governance Organisation basiert auf der bereits

etablierten Rolle des Chief Data Officer (stellvertretender Abteilungsleiter CIT) sowie den bereits in Teilen umgesetzten Strukturen im nachgeordneten Bereich (z.B.: Data Governance Office SASPF, Data Governance Office Hauptprozess Rechnungswesen und Logistik).

3.5. Infrastrukturdatenmanagement

Einen konkreten Anwendungsbereich in der Analyse und Nutzung komplexer Daten und großer Datenmengen stellt das Infrastrukturdatenmanagement dar, das bereits seit 2017 eine ganzheitliche Lebenszyklusbetrachtung der Bundeswehrinfrastruktur vorsieht. Aufgrund der Vielzahl und Komplexität der Daten, die nicht nur durch ca. 6.000 aktuelle Baumaßnahmen der Bundeswehr, sondern auch durch den rechtskonformen Betrieb in der langjährigen Nutzungs- und Betriebsphase von Infrastruktur entstehen, ist ein zentraler, gesicherter Informationsaustausch unerlässlich. Dies ist Betrachtungsfokus des Projektes **Digitales Infrastrukturdatenmanagement**.

Beispiel: Digitales Infrastrukturdatenmanagement

Die Methode „Building Information Modeling“ (BIM) bietet mit dem kollaborativen Arbeiten auf cloud-basierten Plattformen die Möglichkeit, organisationsübergreifend eine erhöhte Transparenz und Qualität von Infrastrukturdaten zu erreichen.

Um das strukturierte Erstellen und den Transfer dieser Daten in die SASPF-Umgebung der Bundeswehr zu ermöglichen, wird seit 2018 die marktverfügbare Softwarelösung CoPIN im Rahmen eines BIM-Pilotprojekts in Neuburg/Donau erprobt. Weitere Pilotprojekte wurden bereits in 2019 begonnen, zum Ende 2020 werden mit voraussichtlich mehr als 60 Pilotprojekten bundesweit Erfahrungen auf der Demonstrationsumgebung gesammelt. Hervorzuheben ist hierbei die agile Entwicklung sowie die Berücksichtigung der Bedarfe aller am Infrastrukturprozess beteiligten Parteien innerhalb und außerhalb der Bundeswehr. Das Projekt hat am 22. September 2020 beim 19. eGovernment-Wettbewerb den ersten Preis als bestes Infrastrukturprojekt und zudem den Publikumspreis gewonnen.



Abbildung 8: Erste Preise für das Cloudbasierte Gebäudemanagement mit BIM

3.6. Digitalisierung der Verwaltungsarbeit

Ziel der digitalen Verwaltungsarbeit ist es, die Aufgaben im GB BMVg effizienter zu erfüllen. Um einen ganzheitlichen Fortschritt erzielen zu können, müssen moderne, digitale Arbeitsformen konsequent etabliert werden. Bisherige analoge Arbeitsabläufe lassen sich allerdings nicht einfach eins zu eins digitalisieren, sondern müssen vom Verwaltungsziel her neu gedacht und entsprechend der digitalen Möglichkeiten umstrukturiert werden. Neben den technischen Grundlagen geht es daher vor allem um veränderte Arbeitsabläufe, die einen umfassenden kulturellen Wandel erfordern. Im Wesentlichen bedeutet das, dass die digitale Verwaltungsarbeit so organisiert und strukturiert ist, dass es den Beschäftigten möglich ist, selbstständig zeit- und ortsunabhängig zu arbeiten. Informationen und Wissen sind dabei entsprechend zugänglich und digitale Kommunikations- sowie Kollaborationsstrukturen verlässlich verfügbar. Durch die COVID-19-Pandemie wurde der Bedarf moderner, digitaler Arbeitsformen zudem noch deutlicher sichtbar als zuvor.

Wie dargestellt, gehören die flächendeckende Ausstattung mit zeitgemäßer Informationstechnik (mobile Arbeitsplätze), der geräteunabhängige Zugang zu Daten und Informationen sowie das Sicherstellen einer Digitalen Grundbefähigung in der Ausbildung und Qualifizierung durch die Vermittlung eines digitalen Grundverständnisses zu digitalen Technologien und digitaler Kompetenzen in den Fachprozessen zu den Voraussetzungen für die digitale Verwaltungsarbeit. Ebenso muss eine dienststellen- bzw. ressortübergreifende sichere, digitale Kommunikation künftig selbstverständlich sein. Für den Ausstieg aus der papiergebundenen Kommunikation stehen deshalb Vertrauensfunktionalitäten (elektronische Signatur, elektronische Dienstsiegel) und geschützte Kommunikationswege über die Einstufung Verschlussache hinaus im Fokus.

Seit Februar 2020 sind die ministeriellen Aufgaben zur „Digitalen Verwaltung / Digitalisierung Verwaltungshandeln“ im BMVg Stab Organisation und Revision zur Harmonisierung der Ablauforganisation bei der Einführung und Nutzung digitaler Lösungen, sowie zum Erreichen einer höheren Steuerungsfähigkeit und Durchsetzungskraft gebündelt.

Darüber hinaus wurde zur Weiterentwicklung und Professionalisierung der bundeswehrgemeinsamen Verwaltungsarbeit und deren angemessene Überführung in die digitale Arbeitsweise/-welt zum 1. April 2020 die Gruppe Stabs- und Verwaltungshandeln im Streitkräfteamt eingerichtet.

Beispiel: Digitalisierungsvorhaben „USG-Online App“

Ein beispielhaftes Digitalisierungsvorhaben ist das **Projekt „USG-Online App“**. Reservistendienst Leistende (RDL) sind für die Zeit des Dienstes finanziell durch die Leistungen nach dem Unterhaltssicherungsgesetz (USG) abgesichert. Die Leistungen sind antragsgebunden. Derzeit werden die dafür erforderlichen Anträge per Post oder E-Mail und ggf. in Mischform eingereicht. Lange Postlaufzeiten, unvollständige Angaben und/oder das Fehlen von Nachweisen etc. führen zu einem erhöhten Kommunikationsbedarf und Bearbeitungsaufwand.

Mit dem Projekt des BAPersBw in Zusammenarbeit mit der BWI GmbH und dem BAAINBw wird beabsichtigt, das Leistungsverfahren zur Unterhaltssicherung für RDL zu digitalisieren, zu vereinfachen und zu vereinheitlichen. Damit wird nicht nur eine zeitgerechte Ansprache an die RDL unterstützt, sondern ebenso die Attraktivität der Reserve gesteigert. Im Zuge der Refokussierung auf die Landes- und Bündnisverteidigung und dem damit verbundenen Aufwuchs der Reservistenstellen (StellenRes) soll die Bearbeitung steigender Antragszahlen mit modernen Data-Management Methoden unterstützt werden. Die durch USG-Online automatisierten und kumulierten Prozessabläufe eröffnen innovative Möglichkeiten der weiteren Ausgestaltung eines digitalen ortsunabhängigen Arbeitsplatzes und beschleunigen allgemein die Vorgangsbearbeitung.

Die Realisierung des Projekts erfolgt in zwei Ausbaustufen. In der Ausbaustufe 1 wurde das Leistungsverfahren nach dem USG erfolgreich in einem funktionalen Prototyp abgebildet und Anfang Oktober 2020 auf der diesjährigen Tagung der Reserve vorgestellt. Nach dessen Weiterentwicklung zur fertigen Anwendung ist ein Go-live für das Frühjahr 2021 angestrebt. Die Ausbaustufe 2, die die Anbindung an das Personalwirtschaftssystem der Bundeswehr und die elektronische Personalakte vorsieht, wurde durch die Beschreibung der Fähigkeitslücke vorbereitet und läuft bereits parallel zur App-Entwicklung als Initiative im Prozess Customer Product Management (CPM).

4. Stand der Digitalen Transformation des GB BMVg

Das in der Umsetzungsstrategie Digitale Bundeswehr beschriebene Vorgehensmodell zur Digitalen Transformation des GB BMVg differenziert nach dem Leitsatz „zentrale Steuerung – dezentrale Umsetzung“ in zentrale Elemente zur Steuerung sowie umsetzungsbezogene Digitalisierungsaktivitäten und -fähigkeiten.

Im Folgenden werden die wesentlichen Entwicklungen und Meilensteine seit dem vergangenen Digitalbericht vom März 2020 beschrieben.

4.1. Zentrale Elemente

Die wesentlichen Steuerungsgremien sind mittlerweile fest etabliert. Das **vierte Leitungsboard Digitalisierung** als höchstes, strategisches Steuerungsgremium der Digitalen Transformation des GB BMVg hat unter Leitung von Frau Bundesministerin Kramp-Karrenbauer am 26. Juni 2020 getagt.

Um die digitale Vorreiterrolle auszufüllen, stand auch die Sitzung selbst sowohl unter dem politischen Willen zur unbedingten (i.S. von „raschen“) Digitalisierung als auch der erstmaligen Anwendung dementsprechender Verfahren: So wurde das Leitungsboard ausschließlich auf Basis digitaler Unterlagen („papierlos“) und als Multipoint-VTC durchgeführt. Das vorbereitende **Steuerungspanel Digitalisierung** fand am 7. Mai 2020 unter Vorsitz von Herrn Staatssekretär Zimmer statt.

Die zweite ordentliche Sitzung des **Digitalrat BMVg** fand am 19. Mai 2020 statt. In diesem Rahmen diskutierte der Digitalrat BMVg mit Frau Bundesministerin Kramp-Karrenbauer sowie Herrn Staatssekretär Zimmer die derzeitigen Schwerpunktthemen. Die inhaltlichen Schwerpunkte wurden im weiteren Verlauf weiter differenziert, ergänzt und umfassen derzeit folgende Themenstellungen (Abbildung 9).



Abbildung 9: Schwerpunktthemen Digitalrat des BMVg

Die **Digitalgalerie** befindet sich in der Realisierungsphase mit dem Ziel, bis April 2021 im Intranet der Bundeswehr die Fortschritte und Erfolge der Digitalen Transformation für alle Beschäftigten des GB BMVg anhand von „Ausstellungsstücken“ erlebbar zu machen. Zusätzlich werden die Beschäftigten die Möglichkeit haben, ihre eigenen Ideen zur Gestaltung der Digitalen Transformation direkt über die Digitalgalerie zu melden, um somit einen Beitrag zur Innovationsfähigkeit des GB BMVg zu leisten. Damit wollen wir auch die Nutzung von „Best Practices“ fördern.

Der **Cyber Innovation Hub der Bundeswehr (CIHBw)** wurde zum 1. Januar 2020 nach einer fast dreijährigen Pilotierungsphase als neue Abteilung mit eigener Geschäftsordnung in der BWI GmbH für zunächst drei weitere Jahre verankert. Die strategische Steuerung des CIHBw erfolgt weiterhin durch das BMVg. Die strategischen Zielvorgaben werden mittels Key Performance Indicators verfolgt, um den Erfüllungsgrad der strategischen Vorgaben zu messen, für entsprechende Transparenz zu sorgen und ggf. nachzusteuern. Der CIHBw identifiziert und validiert durch gezielte Marktbeobachtung und Innovation-Scouting neue Ideen und existierende Lösungen und lässt diese experimentell in Zusammenarbeit mit Nutzern (weiter-)entwickeln. Ziel ist es, diese digitalen Innovationen der Bundeswehr zur Einführung vorzuschlagen und damit für die Bundeswehr kurzfristig verfügbar zu machen. Des Weiteren dient der CIHBw als Schnittstelle der Bundeswehr zu Startup-Unternehmen und anderen innovativen Marktteilnehmern. Zudem trägt er durch den Bereich Intrapreneurship und nutzerzentrierte Innovationsmethoden wie „User Experience Design“ und „Design Thinking“ zu einem Kulturwandel in der Bundeswehr hin zu mehr Innovationsbereitschaft bei. Innovationsvorhaben des CIHBw wie z.B. die „Online-Videosprechstunde“ sowie die „Pflege-App“ in Zusammenarbeit mit dem Bundeswehrkrankenhaus Berlin haben insbesondere während der Corona-Lage zu einer spürbaren Erleichterung geführt. Sichtbares Produkt des CIHBw ist die „Bw-eToken-App“. Mit diesem Innovationsvorhaben ist es dem CIHBw mit dem Projektteam gelungen, dass Soldatinnen und Soldaten der Bundeswehr im Rahmen des kostenfreien Bahnfahrens in Uniform jederzeit und überall über private Smartphones und Tablets die zur Buchung von Bahnreisen notwendigen digitalen Zugangscodes, sogenannte eToken, flexibel nutzen können. Der CIHBw hat sich damit als fester Bestandteil des „Innovations-Ökosystem“ etabliert.

Der Prozess der Gründung der **Agentur für Innovation in der Cybersicherheit GmbH** (Cyberagentur) konnte am 12. August 2020 abgeschlossen werden. Als ressortübergreifende

Inhouse-Gesellschaft des Bundes, vertreten durch das BMVg und das Bundesministerium des Innern, für Bau und Heimat (BMI), detektiert, stimuliert, finanziert und bewertet die Cyberagentur mittel- und langfristige Forschungs-, Entwicklungs- und Innovationsvorhaben zur Sicherheit im CIR und diesbezüglicher Schlüsseltechnologien für den Bereich der Inneren und Äußeren Sicherheit. Die Cyberagentur will die besten Köpfe Deutschlands für die gemeinsame Forschung zu Cybersicherheitsthemen gewinnen, um die technologische Innovationsführerschaft und damit einen Beitrag zur digitalen Souveränität Deutschlands sicherzustellen. Dazu wird sie bundesweit eng mit der deutschen Forschungslandschaft, Industrie, Wirtschaft, sowie der Startup- und Gründerszene zusammenarbeiten.

Derzeit werden durch die zwei Geschäftsführer die Voraussetzungen für die Geschäfts- und Betriebsfähigkeit geschaffen. Die Personalgewinnung wurde eingeleitet. Es konnte bereits erstes Personal aus dem Bereich der Wissenschaft, dem Wissenschafts- und Innovationsmanagement sowie aus Digital-Startups gewonnen werden. Erste konkrete Forschungsaufträge sollen Anfang 2021 vergeben werden.

Das **Zentrum für Digitalisierungs- und Technologieforschung** (DTEC.Bw) ist ein – durch Zeichnung einer entsprechenden universitären Kooperationsvereinbarung – von beiden Universitäten der Bundeswehr getragenes und vom GB BMVg mit Forschungsmitteln aus dem Konjunktur-, Krisenbewältigungs- und Zukunftsprogramm im Einzelplan 14 ausgestattetes wissenschaftliches Zentrum an der Universität der Bundeswehr München, das seit dem 11. August 2020 seinen Betrieb aufgenommen hat.

Übergeordnetes Ziel ist es, die universitäre Forschung der Universitäten der Bundeswehr in den Bereichen Digitalisierung sowie damit verbundener Schlüssel- und Zukunftstechnologien strategisch zu bündeln und zu stärken, in einem sicheren Umfeld noch besser zu verknüpfen und neue Forschungsk Kooperationen mit Wissenschaft, Wirtschaft, Verwaltung und Gesellschaft zu ermöglichen. Insbesondere soll die Forschung im DTEC.Bw stärker auf Innovationsbereiche ausgerichtet werden. Exemplarisch sind folgende Forschungsfelder zu nennen:

- Aufbau von Forschungsinfrastruktur und Grundlagenforschung im Bereich Raketen- und Satellitentechnologie,
- Forschungen zu Nanoschichtsensoren,
- Aufbau von Forschungsinfrastruktur und Grundlagenforschung im Topos "Gestaltung der Mobilität der Zukunft" und „Autonomes Fahren“,

- Forschungen im Bereich Quantenkommunikation und Computersimulationen,
- Forschungen im Bereich der Digitalisierung des Energiesektors und Produktionsabläufen und
- Forschungen im Bereich Additive Manufacturing (3D-Druck).

Zum Ausbau und zur Stärkung nationaler, digitaler sowie technologischer Souveränität ist zudem vorgesehen, dass das DTEC.Bw einen Gründungsinkubator etabliert, der potenzielle Gründerinnen und Gründer aktiv dabei unterstützt, aus Ideen marktreife Produkte und Dienstleistungen zu entwickeln, deren Rechte am geistigen Eigentum national verfügbar bleiben.

Im Kontext Netzwerke und Veranstaltungen haben der 6. und 7. **Fachgesprächskreis** (FGK) am 30. Juni 2020, 7. Juli 2020 und 1. Dezember 2020 stattgefunden. Im Unterschied zu vergangenen Veranstaltungen wurden sie vollkommen digital durchgeführt. Der fachliche Austausch wurde auch in diesem Format durch digitale Break-Out-Sessions, d.h. thematische Diskussionen in virtuellen Kleingruppen, sichergestellt. Das Schwerpunktthema des 6. FGK war die Analyse und Bewertung der Auswirkungen von COVID-19 auf die Digitale Transformation des GB BMVg. Dabei wurden Handlungsempfehlungen für die Leitung des BMVg entlang mehrerer Themenfelder erarbeitet und ein Leitfaden zur Durchführung virtueller Workshops erstellt. Der 7. FGK befasste sich im Thema "Digitalkultur-Digitales Mindset-Digitale Führung" mit Kernpunkten Digitaler Führung. Aus den Arbeitsergebnissen wurde eine Handreichung mit Hilfestellungen zur Umsetzung Digitaler Führung erstellt.

Die Netzwerkveranstaltung **Tag der Koordinatoren** fand am 8. September 2020 zum dritten Mal statt. Unter dem thematischen Schwerpunkt „Digitalisierung und der Faktor Mensch“ haben die „Koordinatorinnen/Koordinatoren Digitalisierung“ und die „Points of Contact Digitalisierung“ (POC Digitalisierung) der einzelnen Organisationsbereiche den Austausch gepflegt und innerhalb verschiedener Paneldiskussionen über die Bedeutung des „Faktors Mensch“ im Rahmen der Digitalisierung diskutiert. Dabei wurde ein neues, hybrides Format genutzt: Im Rahmen einer Präsenzveranstaltung für die Koordinatoren mit gleichzeitiger Übertragung als Online-Konferenz für die POC hatten alle Teilnehmer der Veranstaltung die Möglichkeit, den Panels vollumfänglich zu folgen und mitzudiskutieren.

Das vierte **Veränderungsmanagement-Meeting** (VM-Meeting) wurde am 9. September 2020 ausgerichtet. Das Meeting gab die Möglichkeit, inhaltliche Entwicklungen der Digitalen Transformation in Bezug auf Veränderungsmanagement (VM) vorzustellen und gleichzeitig Impulse

der POC Digitalisierung aufzunehmen. Darüber hinaus diente die Veranstaltung der Förderung des Austauschs der POC sowohl intern als auch mit externen Impulsgebern und der Vermittlung methodischer Anreize, um diese durch die POC in die jeweiligen Bereiche zu tragen. Als Ergebnis wurde u.a. die Einführung eines agilen Projekt- und Prozesscoachings vor Ort festgehalten – hierbei sollen versierte Reservistendienst Leistende (RDL) Projekte mit Digitalisierungsbezug im Rahmen des VM unterstützen. Der Pilot des VM-Projektcoachings startete im November 2020 unter Hinzuziehung von drei RDL Corona bedingt als virtuelle dreitägige Veranstaltung mit dem Projektteam der Führungsakademie der Bundeswehr (FüAkBw). Das VM-Projektcoaching soll in 2021 fortgesetzt werden.

Mit den Fachgesprächskreisen, dem Tag der Koordinatoren, den VM-Meetings und dem VM-Projektcoaching ist es gelungen, ein Netzwerk aufzubauen, das den Prozess der Digitalen Transformation aktiv unterstützt und in alle Bereiche der Bundeswehr hineinwirkt.

Die Governance der Digitalen Transformation im GB BMVg wurde im Zeitraum Februar bis Oktober 2020 erstmalig mithilfe eines **Reviews** in Form einer Reifegradanalyse bewertet. Das Review ist ein strategisches Steuerungstool des Abteilungsleiters Cyber/Informationstechnik (CIT) und Chief Information Officer (CIO), das ihm die Möglichkeit gibt, gezielt Impulse zur Weiterentwicklung zu geben. Dies unterstützt ihn dabei, seine Verantwortung für die Umsetzung der Digitalen Transformation im GB BMVg wahrzunehmen. Über eine regelmäßige Wiederholung im Jahres-Turnus sollen Fortschritte nachvollziehbar und transparent aufgezeigt und gezielte Hebel zur Weiterentwicklung identifiziert werden.

Für die ganzheitliche Betrachtung der Digitalen Transformation im GB BMVg wurden die zu betrachtenden neun Dimensionen und 18 Teildimensionen (Abbildung 10) maßgeblich aus der *Umsetzungsstrategie Digitale Bundeswehr* abgeleitet.



Abbildung 10: Betrachtete Dimensionen und Teildimensionen des Reviews

Für das Review wurde eine fünfstufige Bewertungsskala entwickelt. Für jede Teildimension wurden die fünf Bewertungsstufen operationalisiert und mit spezifischen Kriterien hinterlegt. Die gewählte Abstufung gibt die Möglichkeit, eine einheitliche Skalierung auf alle Dimensionen anzuwenden und Vergleichbarkeit herzustellen (Abbildung 11).

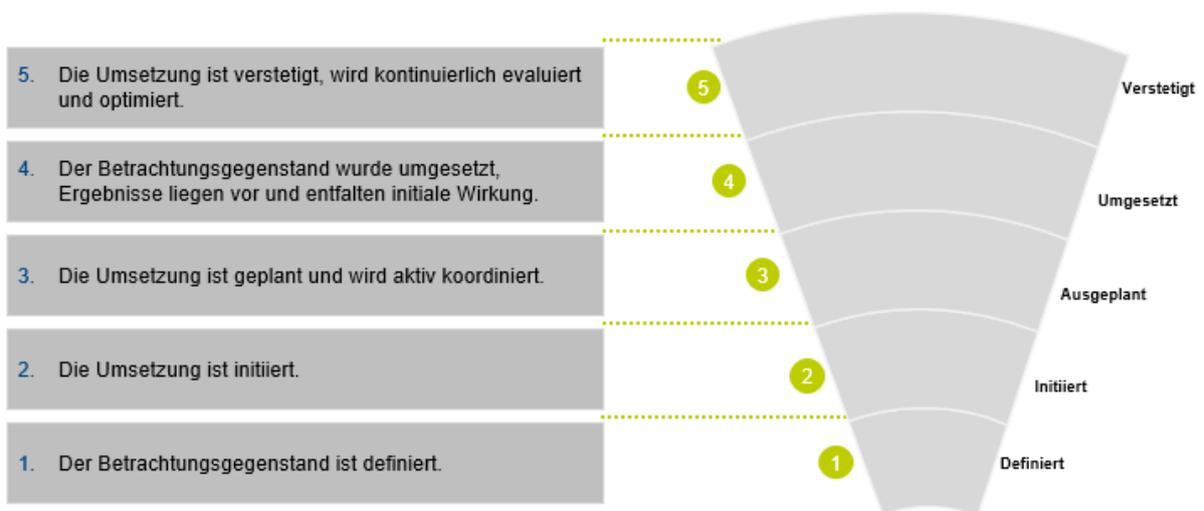


Abbildung 11: Fünfstufige Bewertungsskala

Die Erhebung erfolgte in einem dreistufigen Vorgehen:

1. Analyse der bereits vorhandenen Dokumentenlandschaft zu den einzelnen Teildimensionen,
2. Workshops zur Erfassung aller laufenden Maßnahmen und Aktivitäten pro Teildimension, inklusive Einordnung der Erkenntnisse anhand des Bewertungsrasters für eine Lagefeststellung und vorläufige Reifegradbewertung nach einem strengen Maßstab,
3. Expertengespräche zur Validierung, Ergänzung und Festlegung des Reifegrades.

Die im Rahmen der Erhebung gesammelten Erkenntnisse bilden die Grundlage für die Ableitung von Handlungsempfehlungen, die als Ansatzpunkte zur Erreichung der nächsten Reifegradstufe in der (Teil-)Dimension zu verstehen sind. Entwicklungen und Aktivitäten sind in allen Dimensionen erkennbar – einige Teildimensionen stehen bereits kurz vor dem „Sprung“ in einen höheren Reifegrad. Bei der Bewertung der Reifegradstufe wurde ein strenger Maßstab angelegt. Dadurch ergibt sich für 2020 das erwartete heterogene Gesamtbild in den Reifegraden. In 14 Teildimensionen (78%) sind die zugehörigen Maßnahmen definiert und initiiert (Reifegrad Stufe 2). Bei fünf dieser Teildimensionen ist darüber hinaus die Umsetzung ausgeplant und wird koordiniert umgesetzt (Reifegrad Stufe 3). Für jede Teildimension wurden Ansatzpunkte für die systematische Weiterentwicklung identifiziert.

4.2. Digitalisierungsaktivitäten

Digitalisierung findet im gesamten GB BMVg auf allen Ebenen des täglichen Dienstbetriebs statt und durchdringt damit alle Organisationsbereiche und Planungskategorien. Wie bereits in den bisherigen Berichten zur Digitalen Transformation des GB BMVg dargelegt, führt die *Umsetzungsstrategie Digitale Bundeswehr* nur einen kleinen Ausschnitt einer Vielzahl an Vorhaben auf, die der fortschreitenden Digitalisierung des gesamten GB BMVg direkt oder indirekt dienen.

Unter Digitalisierungsaktivitäten werden Aktivitäten im GB BMVg verstanden – von der Idee über die Planung und Realisierung bis hin zur Nutzung – die durch den Einsatz digitaler Technologien eine höhere Wirkung oder einen effizienteren Ressourceneinsatz anstreben.

Das Portfolio der Digitalisierungsaktivitäten umfasste zum Zeitpunkt der vierten Sitzung des Leitungsboards 81 gemeldete Digitalisierungsaktivitäten, welche durch BMVg Abteilung Cyber/Informationstechnik (CIT) nachgehalten werden. Im Vergleich zum vorherigen Bericht zur Digitalen Transformation des GB BMVg wurden vier Aktivitäten neu angemeldet.

Rund 20 % der Vorhaben weisen einen Ideen- bzw. Konzeptionsstatus aus, während sich fast 50 % in den CPM-Phasen der Entwicklung, Realisierung bzw. in (Teil-)Nutzung befinden und rund 35 % außerhalb IPD/CPM u.a. in den Bereichen „komplexe Dienstleistungen“ oder „Architekturen“ verfolgt werden (Abbildung 12). Den schnellen Innovationszyklen digitaler Technologien steht hinsichtlich des verbleibenden Umsetzungszeitraums der gemeldeten Digitalisierungsaktivitäten eine differenzierte Lage mit weniger als einem Jahr, eine Zeitspanne zwischen einem und vier Jahren und mehr als vier Jahren gegenüber (Abbildung 13). Bei den letztgenannten Aktivitäten handelt es sich regelmäßig um komplexe Beschaffungsprogramme, die mehrjährig konzipiert werden.

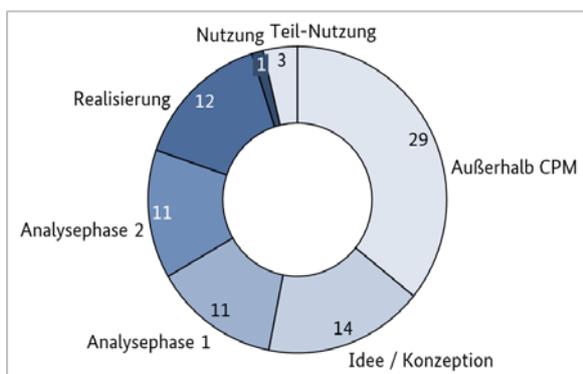


Abbildung 12: Digitalisierungsaktivitäten – Überblick Phasen

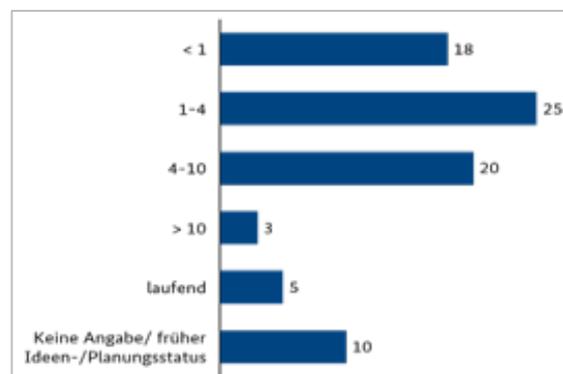


Abbildung 13: Digitalisierungsaktivitäten – Umsetzungszeitraum

Neben der rein quantitativen Darlegung des Fortschritts werden im folgenden Abschnitt ausgewählte Beispiele zur Entwicklung der Digitalisierungsaktivitäten veranschaulicht.



Abbildung 14: Digitalisierungsaktivitäten – Übersicht ausgewählte Beispiele

Die Digitalisierung im Bereich der Streitkräfte ist aufgrund der Weiterentwicklungen und dem zunehmenden Einsatz neuer Technologien von höchster Relevanz. Neben der reinen Einführung neuer Technologien ist der Ausbau von Kommunikations- und Informationssystemen elementar für den Erfolg der Streitkräfte auf dem digitalisierten Gefechtsfeld. Aufbau und Nutzung einheitlicher, sicherer und leistungsfähiger Informations- und Kommunikationssysteme inkludiert sämtliche Vorhaben, die Datenverarbeitung und Datenübertragungssysteme zum Gegenstand haben sowie die vernetzte Operationsführung ausbauen.

Beispiel: Führungsfähigkeit Nationaler Territorialer Befehlshaber

Der Inspekteur der Streitkräftebasis (InspSKB) hat in seiner Funktion als „Nationaler Territorialer Befehlshaber“ (NatTerrBefh) Planungs- und Führungsaufgaben in der Bandbreite von ‚subsidiärer Hilfeleistung‘ über ‚Host Nation Support‘ bis hin zur Nationalen Territorialen Verteidigung im Rahmen der Landes- und Bündnisverteidigung (LV/BV).

Für die Aufgabenwahrnehmung stützt sich der InspSKB hierbei im Wesentlichen auf die Arbeitsplatzausstattung BWI ab. Fähigkeitslücken bestehen insbesondere bei IT-Services sowie IT-Funktionalitäten im Bereich der Lageerfassung, -darstellung und -führung von der operativen bis zur taktischen Ebene.

Aktuelle Erkenntnisse aus DEFENDER EUROPE 2020 und COVID-19-Pandemie verdeutlichen die erkannten Defizite.

Das im Leitungsboard vorgestellte Vorhaben setzt auf einer Erstbefähigung auf und treibt die Ausweitung zur Grund- und Zielbefähigung im Rahmen einer Digitalisierungsaktivität voran. Die Beauftragung einer Vorhabenskizze in Federführung BMVg CIT I 3 für den Anteil „Grundbefähigung“ wurde am 9. Juni 2020 planerisch initiiert. Die Vorhabenskizze wurde am 4. Dezember 2020 durch das Planungsamt der Bundeswehr übermittelt und wird gegenwärtig im BMVg auch im Hinblick auf eine zukünftige Einplanbarkeit geprüft.

Die Fähigkeitslücke soll in zwei parallel laufenden Handlungssträngen geschlossen werden:

- Handlungsstrang 1: Erstbefähigung auf Grundlage vorhandener HaFIS-Infrastruktur/IT-Services sowie Schaffen der Voraussetzungen für den Betrieb;
- Handlungsstrang 2: Grund- und Zielbefähigung mit eigenständigen Rüstungsprojekten im Sinne eines „Integrationsprojektes für IT-Services“ in zwei Hauptschritten (Grundbefähigung frühestens ab 2023 und Zielbefähigung erst nach erfolgter Entscheidung zur Nationalen Führungsorganisation frühestens ab 2027). Im Rahmen des Handlungsstrangs 2 werden außerdem zusätzliche Bedarfe, insbesondere in der Planungskategorie Infrastruktur, mit zu bewerten sein.

Das Vorhaben „**Realisierung der elektronischen Gesundheitsakte Bundeswehr (eGABw)**“ des Sanitätsdienstes der Bundeswehr ist ein weiteres Beispiel für Initiativen zum Aus- und Aufbau verbesserter Informations- und Kommunikationssysteme in der Bundeswehr. Das

komplexe und abteilungsübergreifende Vorhaben forciert die digitalisierte Gesundheitsversorgung der Bundeswehr (GesVersBw).

Die Realisierung erfolgt stufenweise durch Ausbringen verschiedener einrichtungs- und aufgabenspezifischer Informationssysteme.

Um ein erstes funktionales Ergebnis der eGABw bis 2025 zu erzielen, konzentriert sich das Vorhaben im Rahmen der bestehenden Rüstungsverfahren (Schwerpunkt Programmstrategie SASPF) auf die Realisierung einer Anfangsbefähigung.

Der wesentliche Bedarf für diese operative Anfangsbefähigung ist in sechs SASPF-Teilprojekten und einem weiteren Projekt WLAN in den Einrichtungen der GesVersBw hinterlegt, die in Abstimmung mit BMVg und dem nachgeordneten Bereich bis 2025 realisiert werden sollen. Parallel dazu ist die strategische Grundlage und Bedarfsanerkennung für Realisierung und Betrieb der zukünftigen IT Serviceerbringung GesVersBw zu schaffen.

Aufbauend auf der fertig zu stellenden Soll-Architektur GesVersBw sind die bedarfs- und haushaltsbegründenden Dokumente zur Realisierung der **Digitalisierung der Gesundheitsversorgung der Bundeswehr** (Digit GesVersBw) zu erarbeiten.

Dieses komplexe und abteilungsübergreifende Thema wird im Rahmen einer neu eingerichteten ministeriellen Sonderorganisation AG Digit GesVersBw vorangetrieben.

Neben den im Leitungsboard vorgestellten Digitalisierungsvorhaben wird eine hohe Anzahl weiterer Digitalisierungsaktivitäten umgesetzt.

So wird über das Projekt **IT-Unterstützung Controlling, Zielbild ISoLaBw** ein aggregiertes Lagebild zur inneren und sozialen Lage in der Bundeswehr erhoben.

Die Analyse- und Bewertungsunterstützung der Inneren Lage der Bundeswehr wird dabei mit einer SASPF basierten IT-Unterstützung umgesetzt. Seit Juli 2018 befindet sich die Applikation in der Nutzungsphase.

Die bisherige Zwischenlösung wurde um eine umfängliche Nutzbarkeit der IT-gestützten Erfassung von Meldungen auf Einheitsebene sowie die Möglichkeit des Zugriffs berechtigter Anwender der Teilstreitkräfte/Organisationsbereiche in ihrem jeweiligen Zuständigkeitsbereich für eine eigene Bewertung der Inneren Sozialen Lage ergänzt. Nach einer

umfangreichen Testphase mit Nutzern aus allen OrgBereichen konnte die Anwendung am 3. September 2020 in den technischen Produktivbetrieb gehen.

Mit dem ab Oktober 2020 begonnenen Rollout der Anwendung als Ziellösung wurden das bisherige Eingabeformular aus dem Formularwesen der Bundeswehr in die integrative IT-U ISoLaBw überführt und Arbeitsvorgänge vom Erfassen der Meldung am „Entstehungsort“ bis hin zur Darstellung der ISoLaBw auf Leitungsebene implementiert.

Durch Reduzierung des manuellen Aufwandes für die meldenden Dienststellen bis zur Bereitstellung leitungsrelevanter Informationsbedarfe auf Grundlage einer besseren Datenqualität und -verfügbarkeit wird die Effizienz deutlich gesteigert.

Die flächendeckende Nutzung in der Bw ist wie geplant zum 5. Januar 2021 gestartet.

Zugleich wird auf Grundlage bestehender IT-Umsetzungen zur Abbildung von weiteren Zielbildern („Dashboard“) der IT-U Controlling ein integrierter und ganzheitlicher Ansatz zur strategischen Entscheidungsunterstützung und Steuerungsunterstützung umgesetzt.

Ein bedeutender Entwicklungsschritt wurde in diesem Jahr auch bei der **Virtualisierung der Bundesakademie für Sicherheitspolitik (BAKS)** erreicht.

Personell wurde die BAKS bereits durch das Einrichten von vier Dienstposten für den Bereich Kommunikation gestärkt, welche insbesondere die professionelle Nutzung von Social Media Diensten sicherstellen werden. Um die Mitarbeiterinnen und Mitarbeiter der BAKS zum mobilen Arbeiten zu befähigen, wurde die BAKS mit mobilen Endgeräten (Smartphones und Tablets) ausgestattet. Die Durchführung digitaler Veranstaltungsangebote wird durch die Ausstattung mit modernen Videokonferenzenanlagen ermöglicht. Die Einrichtung eines leistungsfähigen Gäste-WLAN soll im Jahr 2021 abgeschlossen werden. Darüber hinaus soll der Akademiebetrieb zukünftig durch die Beschaffung zeitgemäßer „Campus-Management- und E-Learning Software“ weiter optimiert werden.

Die Virtualisierung der BAKS hat zum Ziel die Präsenz und Reichweite im digitalen Raum zu erhöhen und die Lehr- und Veranstaltungsangebote um digitale Elemente zu erweitern. Das Vorhaben folgt dabei dem 2018 beschlossenen Koalitionsvertrag, womit unter anderem auch die BAKS – als sicherheitspolitisches Kompetenzzentrum und erstrangige sicherheitspolitische Weiterbildungsstätte der Bundesregierung – gestärkt werden soll. Gleichsam wird

hierdurch der gesamtgesellschaftliche Dialog zu den Erfordernissen künftiger Sicherheitsvorsorge unterstützt.

Die veränderten Ansprüche an Arbeit und Führung erfordern eine Kulturveränderung, die auf vernetztes, selbstorganisiertes Lernen, Kommunizieren und Arbeiten ausgerichtet ist. Die FüAkBw entwickelt in einem umfassenden Transformations- und Veränderungsprojekt bis Ende 2021 die **„Digitale Ausbildungsakademie für lebenslanges Lernen“**. Die Zielsetzung ist eine signifikante Erweiterung flexibler, digitaler Lehr-/Lernangebote sowie verbesserte Lernunterstützung durch Lernbegleitung und das Ermöglichen selbstgesteuerten Lernens. Durch fünf Projektgruppen (Kultur, Organisation, Personal, Informationstechnologie und Infrastruktur) wurden zunächst 130 Ideen entwickelt, die in einem Ideenforum vorgestellt, diskutiert und bis September 2020 zu 50 Ideen konsolidiert wurden. Im weiteren Prozess der Konzepterstellung erfolgt die Ausgestaltung konkreter Maßnahmen mit Zeitplan. Seit Beginn 2020 wurden zwei Pilotprojekte auf den Weg gebracht: die FüAkBw als Pilotdienststelle der „Virtuellen Lernumgebung der Bundeswehr“ und das Infrastrukturprojekt „iLab/modernes Lernen“ in der Graf-von-Baudissin-Kaserne in Hamburg. Das Gesamtprojekt ist auf maximale Transparenz und Beteiligung angelegt und kann auf der Internetseite der FüAkBw nachverfolgt werden.

Darüber hinaus wird auch die Initiierung neuer Digitalisierungsvorhaben mit Nachdruck betrieben. Mit dem Gesetz zur Einführung der elektronischen Akte in der Justiz und zur weiteren Förderung des elektronischen Rechtsverkehrs vom 5. Juli 2017 ist auch der GB BMVg verpflichtet, ab dem 1. Januar 2026 Verfahrens- und Gerichtsakten nach der Wehrdisziplinarordnung (WDO) und nach der Wehrbeschwerdeordnung (WBO) elektronisch zu führen. Da diese Fähigkeit bislang in der Bundeswehr nicht vorhanden ist, erarbeitet der fachliche Bedarfsträger BMVg R II 1 derzeit zusammen mit CIT II 7 und CIT I 3 die Grundlagen zur Initiierung des Projekts **„Einführung einer elektronischen Verfahrens- und Gerichtsakte (eVGA)“** für Wehrdisziplinaranwaltschaften und Truppendienstgerichte.

4.3. Digitalisierungsfähigkeiten

Die Digitale Transformation geht weit über Themen zu Beschaffung und Nutzung von Technologien hinaus – daher sind Maßnahmen zur Erhöhung der Digitalisierungsfähigkeiten der Bundeswehr elementar. Diese umfassen neben kulturellen und personellen Fragestellungen auch Verfahren und Strukturen. Damit betreffen diese Themen in der Regel die gesamte Organisation, was sie ausgesprochen relevant und gleichzeitig sehr vielschichtig macht.

Das Portfolio der Digitalisierungsfähigkeiten umfasste zum Zeitpunkt der vierten Sitzung des Leitungsboards 40 Maßnahmen. Insgesamt wurden im Vergleich zum vorherigen Bericht zur Digitalen Transformation des Geschäftsbereichs BMVg zwei Maßnahmen neu angemeldet und folgende drei Maßnahmen abgeschlossen:

- „Beschleunigte Einführung von IT-Innovationen mittels Prototypen“ (siehe Detaildarstellung auf Seite 39),
- „Aufbau von Digitalkompetenzen, einer Wissensplattform Digitalisierung und eines zentralen Managements der Digitalisierungsmaßnahmen im Organisationsbereich IUD im Rahmen der AG Leitlinie IUD 2030“ (siehe Detaildarstellung auf Seite 48),
- „Bedarfsträgerforderungen für ein Verwendungsaufbaumodell (mil)“ (BMVg FüSK I 3).

Von den laufenden Maßnahmen befinden sich ca. ein Drittel in der Konzeptionsphase und ca. die Hälfte in der Umsetzungsphase (Abbildung 15). Dementsprechend steht der GB BMVg bei der Umsetzung der Maßnahmen zur Erhöhung der Digitalisierungsfähigkeit noch eher am Anfang. Mit 18 Maßnahmen wirkt knapp die Hälfte übergreifend auf mehrere Bereiche der Digitalisierungsfähigkeit ein (Abbildung 16).

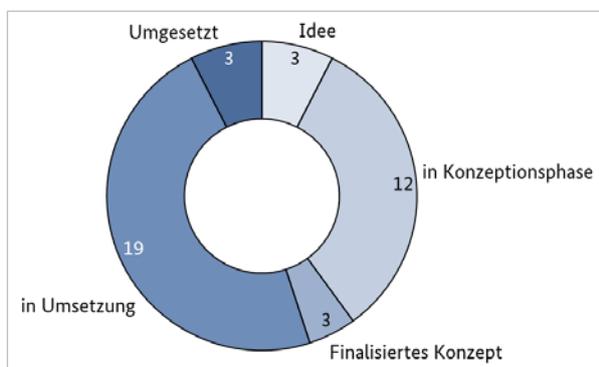


Abbildung 15: Digitalisierungsfähigkeiten – Überblick Phasen

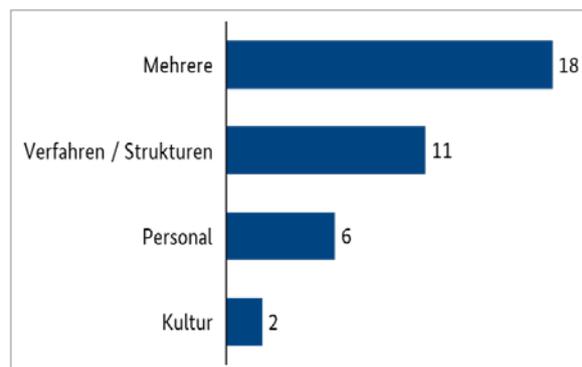


Abbildung 16: Digitalisierungsfähigkeiten – Überblick Wirkebenen

Neben der quantitativen Erfassung des Fortschritts werden im folgenden Abschnitt ausgewählte Beispiele zur voranschreitenden Digitalisierung mit Bezug zur Erhöhung der Digitalisierungsfähigkeiten dargelegt.



Abbildung 17: Digitalisierungsfähigkeiten: Übersicht ausgewählte Beiträge

Schnelle technologische Veränderungen im Rahmen der Digitalisierung, kürzere Produktlebenszyklen sowie nicht zuletzt die Notwendigkeit zur Aufrechterhaltung der Effektivität auf dem Gefechtsfeld zwingen die Bundeswehr, sich mit Innovationen auseinander zu setzen. Optionen zur Beschleunigung von IT-Innovationen wurden bereits im 2. Leitungsboard Digitalisierung im Juni 2019 erstmalig vorgestellt. Seitdem haben Weiterentwicklungen mit unterschiedlichen Prozessverantwortlichen stattgefunden – eine finale Abstimmung zur Handreichung mit Bezug auf die **beschleunigte Einführung von innovativen IT Prototypen** aus F&T der Stufe 2 (anwendungsnahe Forschung und Technologie) in der Fallgruppe II (Maßnahmen mit IT-Anteil ohne militärische Fähigkeiten) fand am 31. Oktober 2019 statt.

Die Handreichung gibt entlang der bestehenden Leistungsprozesse „Integrierte Planung durchführen“ (IPD) und „Materielle Lösungen nach CPM bereitstellen“ (CPM) den Rollenträgern im KdoCIR und BAAINBw Handlungssicherheit, innovative IT mittels anwendungsnaher IT-Prototypen beschleunigt in die Bundeswehr zu überführen.

Beispiel: Beschleunigte Einführung von IT-Innovationen mittels Prototypen

Um Erfahrungen bei der Anwendung der „Handreichung zur beschleunigten Einführung von innovativen IT-Prototypen aus F&T der Stufe 2 in der Fallgruppe II“ zu sammeln, wurden fünf anwendungsbezogene IT-Prototypen aus dem Zuständigkeitsbereich der Abteilung CIT identifiziert, die aufgrund ihres Reifegrades und absehbarer Nutzerforderungen für eine zeitnahe Überführung in IPD und CPM in Frage kommen.

Drei der fünf IT-Prototypen (DCR, MEGA, MiTeRa) wurden mit Messpunkten versehen, eng begleitet und haben aktuell folgenden Sachstand:

- Der Demonstrator **„Distributed Cyber Reconnaissance as a Service (DCR)“** soll Lösungsmöglichkeiten aufzeigen, wie ständige Cyberaufklärung kostengünstig und wirtschaftlich zu gewährleisten ist. Die Durchführung der Studie hat begonnen, der Demonstrator ist in Betrieb. Ein Zwischenbericht ist in Erarbeitung. Die bisherig erzielten Ergebnisse übertreffen die Erwartung des Nutzers.
- Das **„Multisensorische und echtzeitaugliche Gefechtsmanagementsystem auf einem ad hoc-Meshnetwork (MEGA)“** hat in ersten Praxistests bei Gebirgsjägern und Spezialkräften eine hohe Akzeptanz erfahren und Potential für unterschiedlichste Anwendungen gezeigt. Das Abstellen der festgestellten IT-Sicherheitsmängel führt allerdings zu Verzögerungen im Innovationsvorhaben.
- Der Prototyp **„Militärisches Technologie Radar Cyber/IT (MiTeRa)“** wurde im Rahmen eines F&T-Vorhabens zwischen BAAINBw und dem Fraunhofer-Institut FKIE entwickelt. Er kann unterschiedliche Sichten auf wehrtechnische F&T-Vorhaben basierend auf der bisherigen VOCON/2-F&T Datenbank visualisieren, die eine zielgerichtete Forschungsplanung und -steuerung für den Bereich Cyber/IT ermöglichen. Der Prototyp wurde erfolgreich entlang der Handlungsempfehlungen der Handreichung entwickelt und genutzt und zeigt das Potential des Vorgehens beispielhaft auf. Im letzten Schritt wurde der Prototyp in einen Beschaffungsprozess überführt – in diesem Fall den CPM – und hat somit den Anwendungsbereich der Handreichung verlassen.

Neben der Entwicklung und Einführung von IT-Innovationen stellt das Gewinnen und Befähigen des Personals, das Innovationen und sämtliche neuen Tools und Abläufe beherrschen und nutzen soll, eine weitere Herausforderung dar.

Hier steht vor allem die Befähigung des Bestandspersonals im Fokus. Nicht nur aufgrund der hohen Anzahl an Beschäftigten im GB BMVg und somit des zu befähigenden Personals, sondern auch bedingt durch die unterschiedlichen Anforderungen von zivilem und militärischen Personal ist dieser Schritt umfassend und vielschichtig. Die COVID-19-Pandemie hat auch diesem Thema ungeplanten Nachdruck verliehen, da sich Arbeitswelt und Anforderungen an das Bildungs- und Qualifizierungsangebot schlagartig verändert haben: Mitarbeitende arbeiten disloziert aus dem Homeoffice und finden sich wieder im Umgang mit neuen Tools und bislang ungewohnten Formen der Zusammenarbeit.

Zur Befähigung („Enabling“) des Personalkörpers für diese und weitere digitale Kompetenzen sind verschiedene Vorhaben initiiert oder befinden sich bereits in der Umsetzung. So wurden zur Befähigung des zivilen Personals die Vorhaben **„Digitale Grundbefähigung“** und **„Digitale Führungskompetenzen“** initiiert.

Unter dem Stichwort „Arbeit 4.0“ hat die vierte einschneidende Transformation von Wirtschaft und Gesellschaft begonnen: Die Arbeit wird vernetzter, digitaler und flexibler. Dies gilt für alle Dimensionen von „Arbeit“ – ganz gleich ob Inhalte, Prozesse, Methoden oder Kultur betroffen sind.

Die Anforderungen an die Arbeitswelt und an das Bildungs- und Qualifizierungsangebot werden durch die COVID-19-Pandemie stärker als zuvor auf die Umsetzung der digitalen Transformation fokussiert. Dabei ist in Rechnung zu stellen, wie sehr die Digitalisierung unser aller Leben verändert (Stichworte Homeoffice, Homeschooling, Uni@home, etc.).

Das Personalmanagement hat auf Grundlage der Notwendigkeit, Menschen in der Bundeswehr zur Digitalisierung zu befähigen, im Rahmen der „Digitalen Grundbefähigung“ eine Modulreihe mit Online- und Präsenzmodulen für das zivile Bestandspersonal der Bundeswehr etabliert und für eine verpflichtende Teilnahme durch das Bildungszentrum der Bundeswehr (BiZBw) vorbereiten lassen. Die Module der „Digitalen Grundbefähigung“ werden für die Nachwuchskräfte auch in die Laufbahnausbildung der unterschiedlichen beamtenrechtlichen Vorbereitungsdienste und die Berufsausbildungen sukzessive und passgenau integriert werden.

Die Maßnahmen werden bereits ab Jahresbeginn 2021 dazu führen, dass die Beschäftigten der Bundeswehr Schritt für Schritt einen signifikanten Zugewinn digitaler Kompetenzen erfahren und damit unter den neuen Anforderungen des digitalen Arbeitens sicherer agieren werden. Zu den Schlüsselqualifikationen künftiger Führungskräfte im Rahmen der Arbeitswelt 4.0 wird gehören,

- die neuen Technologien und Arbeitsweisen zu kennen,
- die Wertschöpfung dieser Technologien im eigenen Bereich bewerten zu können,
- die Mitarbeiterinnen und Mitarbeiter zur Lösung komplexer Probleme anzuleiten und sie mit aktuellen Szenarien und Zukunftsstrategien in der digitalisierten Arbeitswelt zu führen sowie
- eine persönliche Bindung und Kommunikation mithilfe unpersönlicher Kanäle (darunter auch Social Media) aufzubauen.

Das BiZBw hat an der „Enabler“-Rolle des Zivilpersonals auch bei der zentralen Operationalisierung der Führungskräftequalifizierung einen wesentlichen Anteil bei Umsetzung und Durchführung. Zum Beispiel werden durch das BiZBw für Spitzenführkräfte der Ebene B6+ im GB BMVg sogenannte Masterclasses durchgeführt. In den Masterclasses soll ein grundlegendes Wissen über Abläufe, ggf. technische Voraussetzungen und Risiken erworben werden, die Wirkmechanismen der Digitalisierung bestimmenden Faktoren erkannt und konkrete Digitalisierungsstrategien für den eigenen Verantwortungsbereich abgeleitet werden können. Die jeweiligen Module der Masterclasses reflektieren ausgewählte Themen der Digitalisierung (Big Data Analytics, Daten-/Cybersicherheit, Künstliche Intelligenz, Blockchain, Agiles Führen und Arbeiten, Digitale Kommunikation und Kollaboration, Social Media) und stellen gezielt Instrumente und Werkzeuge im Führungsprozess für das Spitzenpersonal bereit.

Ebenfalls werden **Maßnahmen zur digitalen Befähigung des militärischen Personals** initiiert.

So konfrontiert der Arbeitsalltag jede Soldatin und jeden Soldaten mit der Automatisierung von Abläufen, der Interaktion via digitaler Medien oder dem Umgang mit Daten. Digitalisierung beeinflusst die Denk- und Handlungsweise der Streitkräfte auf allen Ebenen im Sinne

eines Digitalen Selbstverständnisses. Sie wirkt in der Weiter- bzw. Zukunftsentwicklung übergreifend über die Aspekte Fähigkeitserhalt, Fähigkeitsaufwuchs Modernisierung und Fähigkeitsentwicklung. Um die Chancen der Digitalisierung effektiv zu nutzen und deren Risiken wirksam zu begegnen, sind Soldatinnen und Soldaten adäquat zu qualifizieren. Alle Beschäftigten benötigen, über Organisations- und Fachbereiche hinweg, ein Grundverständnis digitaler Techniken und digitaler Prozesse.

Ziel der Steckbriefe Nr. 08 „Erarbeitung von Grundlagen digitaler Fähigkeiten/Fertigkeiten für militärische Führungskräfte“ und Nr. 11 „Erarbeitung von Basiselementen digitaler Fähigkeiten/Fertigkeiten für das militärische Personal“ ist es daher, in enger Abstimmung mit den Organisationsbereichen (OrgBer), den querschnittlichen Bedarf der OrgBer für eine digitale Grundbefähigung aller Soldatinnen und Soldaten als auch für militärische Führungskräfte zu erarbeiten. Diese „Digitale Grundbefähigung“ kann in der Folge für eine Deltaanalyse innerhalb der jeweiligen Trainingslandschaft genutzt werden. Der Bedarf der OrgBer dient als streitkräftegemeinsame Vorgabe.

Zunächst wurde mit einer Lagefeststellung die Auswertung bereits bestehender Projekte zu gleichen oder zumindest ähnlichen Fragestellungen durchgeführt. Als Ergebnis ist festzuhalten, dass es bereits jetzt eine Vielzahl formeller und informeller Qualifizierungsmaßnahmen mit dem Ziel der Erhöhung der Digitalisierungsfähigkeit aller Dienstgradgruppen gibt.

Eine konkrete Vorgabe, welche Fähigkeiten und Fertigkeiten im Einzelnen auf den unterschiedlichen Ebenen benötigt werden, existierte jedoch nicht. Um die Projektteammitglieder von Beginn an einzubinden, wurde eine Erhebungsschablone entwickelt, mit der die OrgBer zu ihren Bedarfen befragt wurden. Die Bedarfserhebung der Basiselemente digitaler Fähigkeiten und Fertigkeiten für das militärische Personal wurde an sechs Kompetenzdimensionen ausgerichtet. Dabei wurde sowohl nach den Bedarfen einer „Digitalen Grundbefähigung“ für alle Soldatinnen und Soldaten gefragt, als auch nach speziellen Fähigkeiten, die besonders für militärische Führungskräfte von Bedeutung sind.

Die Ergebnisse wurden ausgewertet und in den Entwurf eines Positionspapiers „Streitkräftegemeinsame Vorgaben für die Ausbildung zur Erhöhung der Digitalisierungsfähigkeit in den Streitkräften“ eingearbeitet. Für militärische Führungskräfte ist bereits jetzt festzustellen, dass neben einem steigenden Umfang digitaler Fähigkeiten und

Fertigkeiten (z.B. Anwendung neuer (Führungs-)Methoden, Kommunikation und Zusammenarbeit) auch explizit soziale Kompetenzen und ein „Digitales Mindset“ gefordert werden.

Im Kontext der Bedarfserhebung wurden eine aktuelle sowie perspektivische Relevanzeinschätzung auf einer Skala von 1 (sehr relevant) bis 5 (nicht relevant) vorgenommen.

Aktuelle Relevanz			Perspektivische Relevanz (in 10 Jahren)		
Rang	Dimension	Mittelwert	Rang	Dimension	Mittelwert
1	 Sicherheit & Ethik in der digitalen Arbeitswelt	2,04	1	 Sicherheit & Ethik in der digitalen Arbeitswelt	1,29
2	 Nutzung digitaler Technologien am Arbeitsplatz	2,17	2	 Kommunikation & Zusammenarbeit in der digitalen Arbeitswelt	1,43
3	 Kommunikation & Zusammenarbeit in der digitalen Arbeitswelt	2,41	3	 Nutzung digitaler Technologien am Arbeitsplatz	1,48
4	 Kenntnis und Verständnis digitaler Technologien	2,71	4	 Kenntnis und Verständnis digitaler Technologien	1,74
5	 Führung in der digitalen Arbeitswelt	2,92	5	 Führung in der digitalen Arbeitswelt	1,9
6	 Anwendung neuer Methoden in der digitalen Arbeitswelt	3,07	6	 Anwendung neuer Methoden in der digitalen Arbeitswelt	2,32

Abbildung 18: Bedeutung digitaler Kompetenzen (aktuell und perspektivisch)

Die in Abbildung 18 wiedergegebenen Ergebnisse weisen darauf hin, dass bereits heute digitale Fähigkeiten und Fertigkeiten dringend erforderlich sind, um der Auftragserfüllung sowie der Digitalisierung der Arbeitswelt und des Gefechtsfeldes gerecht zu werden. Von besonderer Bedeutung werden heute die Dimension „Sicherheit & Ethik in der Arbeitswelt“, gefolgt von der Dimension „Nutzung digitaler Technologien am Arbeitsplatz“ wahrgenommen. Der Blick in die 10-Jahres-Vorschau unterstreicht die bereits heute hohe Notwendigkeit einer digitalen Grundbefähigung. Während sich die aktuellen Relevanzwerte zwischen „hoher Relevanz“ und „mittlerer Relevanz“ bewegen, so steigen diese perspektivisch auf ein sehr hohes, respektive hohes Relevanzniveau an.

Nach einer weiteren Konsolidierung der sich seit September 2020 in der Mitprüfung durch die OrgBer befindlichen Ergebnisse wird der Entwurf des Positionspapiers mit den zusammengefassten Bestandteilen der „Digitalen Grundbefähigung“ und den besonderen Aspekten für militärisches Führungspersonal finalisiert und bis zum 31. Januar 2021 bei BMVg FüSK I 3 vorgelegt.

Im Rahmen des ersten und zweiten Digitalberichts wurde bereits über das Programm Cyber/IT Evaluation Centre (CITEC) berichtet. Als Maßnahme der Personalbindung und -gewinnung sollen darüber die im militärischen Personalkörper auch absehbar noch bestehenden Vakanzen im Bereich Cyber/IT weiter reduziert werden. Diesbezüglich pilotiert das KdoCIR in Zusammenarbeit mit dem BAPersBw.

Mit CITEC soll die positive Entwicklung der Personallage im Cyber/IT-Dienst durch fachliches Screening zur Identifizierung von IT-Kenntnissen sowie der Feststellung fachlicher Potentiale über den Prognosezeitraum 2022 hinaus unterstützt werden. Erste Erfahrungen belegen, dass CITEC ein geeignetes Instrument darstellt, um Potentiale für den Bereich Cyber/IT-Dienst zu identifizieren und in der Folge eine qualitativ hochwertige Bedarfsdeckung zu ermöglichen.

CITEC ist dabei in vier Piloten mit unterschiedlichen Testgruppen geclustert. Der erste Pilot fokussiert sich auf das militärische Bestandspersonal und wurde beginnend ab November 2019 durchgeführt. Dazu wurden Personen aus der Laufbahn der Offiziere des Truppendienstes (OffzTrD) mit MINT-Studium (Mathematik, Informatik, Naturwissenschaft und Technik) kurz vor ihrem Dienstzeitende hinsichtlich ihrer Bereitschaft zum Wechsel in den Werdegang Cyber/IT Dienst (bisher 255 Personen) angeschrieben, von denen 217 eine Rückmeldung an das BAPersBw gesendet haben. Davon haben 82 Personen ihr Interesse an einem Screening abgeben. Bisher wurden in drei Durchgängen 30 von 32 getesteten Personen dem BAPersBw für eine Übernahme in die Laufbahn Cyber/IT-Dienst empfohlen, wovon nach aktuellem Stand bereits neun Personen in die Laufbahn überführt wurden. Im Dezember 2020 wurde erstmalig der zweite Pilot „Screening Seiteneinsteiger“ durchgeführt. Hierzu wurden 13 Personen getestet und für eine Übernahme empfohlen. Deren Einplanung wird durch das BAPersBw geprüft. Künftige Verfahren, einschließlich Möglichkeiten eines Einstiegs von Personen mit non-formalen Kompetenzen, werden derzeit untersucht.

Gewonnenes und befähigtes Personal wird – nicht zuletzt aufgrund des veränderten Arbeitsumfeldes – neue Wege der Zusammenarbeit und Abläufe finden. Gleichzeitig befinden sich nicht nur operative Abläufe direkt am Endnutzer im Umbruch – auch Prozesse, Verfahren und Strukturen auf strategischer und planerischer Ebene werden weiterentwickelt.

Ein Schlüsselement für die Digitale Transformation und ein Beispiel, das für ein die gesamte Organisation betreffendes Vorhaben steht, ist die **Digitalisierungsplattform des GB BMVg**. Das Vorgehen orientiert sich auch an den Erfahrungswerten des HERKULES-Folgeprojekts und insbesondere der agilen Reaktionsfähigkeit bei der Anpassung des IT-Systems der Bundeswehr (bspw. mobiles Arbeiten in der COVID-19-Pandemie).

Mit dem geplanten Aufbau der Digitalisierungsplattform GB BMVg sollen die Besonderheiten bei der Bereitstellung von IT-Services im Vergleich zu anderen Rüstungsvorhaben im Beschaffungsprozess einschließlich des Integrierten Planungsprozesses verstärkt Berücksichtigung finden und sollen eine Top-Down-Steuerung erlauben. Die Digitalisierungsplattform GB BMVg ist somit nicht als rein technische Plattform zu verstehen sondern als Wirkverbund aus Prozessen, Verfahren, Arbeitsweisen und Strukturen. Mit der Top-Down-Steuerung und damit der Bereitstellung querschnittlicher IT-Services soll die Voraussetzung geschaffen werden, dass sich zukünftige Bedarfsanforderungen auf bestehende Lösungsanteile vergleichbar einem Baukastensystem abstützen und im Ergebnis damit ein erheblicher Zeitgewinn bei der Projektrealisierung erreicht werden kann.

Alle künftigen IT-Projekte nutzen wiederverwendbare Standardbausteine.

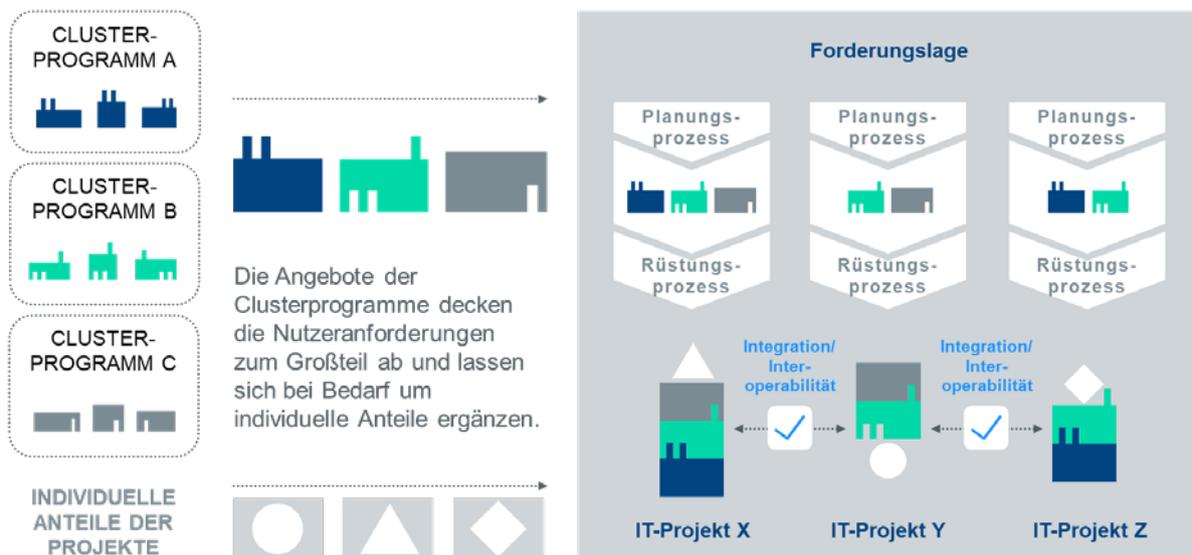


Abbildung 19: Bereitstellung von IT-Services durch Clusterprogramme

Im Jahr 2020 wurde begonnen die Prozesse, Verfahren und Arbeitsweisen im Rahmen eines Pilotvorgehens prototypisch umzusetzen. Die Bereitstellung von IT-Services aus dem ersten Pilotclusterprogramm Infrastructure & Cloud Base, User Equipment ist beginnend ab dem Jahr

2021 vorgesehen. Die damit verbundene Bereitstellung von querschnittlichen und wiederverwendbaren IT-Services ist ein Kernelement für eine schnelle und nachhaltige Digitale Transformation.

Die Nutzung von vertrauenswürdiger Informations- und Kommunikationstechnologien in sicherheitsrelevanter Umgebung ist eine essentielle und grundlegende Anforderung und Notwendigkeit der Bundeswehr. Dafür ist es wichtig, mögliche Abhängigkeiten von nicht-vertrauenswürdigen IT-Partnern zu verringern und die Datenautarkie zu fördern – um so einen Anteil der **Digitalen Souveränität** zu stärken.

Im Rahmen der digitalpolitischen Schwerpunktsetzung wurde der Ausbau der digitalen Souveränität sowohl seitens der Bundesregierung als auch des BMVg als politische Zielbestimmung ausgegeben. Die Federführung zur Ausgestaltung dieses Themas aus digitalpolitischer Sicht liegt im BMVg bei der Abteilung CIT.

Während der laufenden Arbeiten im GB BMVg zur digitalen Souveränität wurden eine Definition², folgende fünf Handlungsfelder im GB BMVg sowie Thesen zu den Handlungsfeldern auf Basis von Interviews auf ministerieller Ebene erarbeitet:

- (1) Nutzung vertrauenswürdiger IT
- (2) Aufbau und Erhalt von Schlüsseltechnologien
- (3) Erhalt der Kernführungsfähigkeit
- (4) Erhöhung der Innovationsfähigkeit
- (5) Aufbau und Erhalt digitaler Kompetenzen.

Abteilungsleiter CIT hat dazu ein politisch-strategisches Eckpunktepapier „Ausbau der digitalen Souveränität im GB BMVg“³ im August 2020 gezeichnet.

In der aktuellen Phase geht es nun um das Erarbeiten von Grundlagen für eine Operationalisierung von Maßnahmen durch:

- Identifikation des Status Quo im Themenfeld digitale Souveränität sowie ableiten von konkreten Handlungsbedarfen und

² Im GB BMVg wird unter „digitaler Souveränität“ das Vorliegen der erforderlichen Kontroll- und Handlungsfähigkeiten im Cyber- und Informationsraum verstanden, um den verfassungsgemäßen Auftrag der Bundeswehr sicher, selbstbestimmt und frei von ungewollter Einflussnahme durch Dritte ausüben zu können.

³ Siehe Anlage

- verstärkte Zusammenarbeit mit dem Digitalrat GB BMVg zur Operationalisierung.

Auch im **Deutschen EU-Ratspräsidentschaftsprogramm** war digitale Souveränität in einer globalisierten Welt als Leitmotiv der europäischen Digitalpolitik verankert. Die EU sollte sich zu digitaler Souveränität positionieren und globale Debatten hierzu mitgestalten.

Für die Sicherheit und Verteidigung Europas kommt dem Ausbau der digitalen Souveränität vor dem Hintergrund eines volatilen sicherheitspolitischen Umfelds, zunehmenden Abhängigkeiten von Informations- und Kommunikationstechnologien sowie einer kontinuierlichen Bedrohungslage im Cyber- und Informationsraum eine Schlüsselrolle zu. Die Stärkung der digitalen Souveränität in der EU – eingebettet in den Gesamtkontext der Resilienz – war daher ein wesentliches Anliegen, zu dem das BMVg in verschiedenen Konferenzen erfolgreich eine Debatte anstoßen konnte.

Auch über unsere Ratspräsidentschaft hinaus werden wir uns weiter dafür einsetzen, den Herausforderungen der digitalen Souveränität auf europäischer Ebene zu begegnen und Lösungsansätze zu entwickeln.

Die aufgeführten Beispiele zeigen, dass mit der Digitalisierung eine große Veränderung Einzug in die Bundeswehr hält – die Digitale Transformation ist ein **Veränderungsprozess**. Um die Menschen im Rahmen dieses Prozesses nicht zu verlieren, werden an vielfältigen Stellen innerhalb der Bundeswehr – in den einzelnen Organisationsbereichen wie auch zentral – Maßnahmen ergriffen, um den Veränderungsprozess einerseits zu begleiten und andererseits eine **Digitalkultur** im GB BMVg zu fördern und zu stärken.

Digitalkultur bezeichnet den Umgang mit Anforderungen, Chancen und Risiken der Digitalisierung. Bestandteil davon ist das digitale Selbstverständnis, welches das Bewusstsein für die Veränderungen, die mit der digitalen Transformation einhergehen, beschreibt. Im Rahmen der *Umsetzungsstrategie Digitale Bundeswehr* wurde vom BMVg in Zusammenarbeit mit dem Zentrum für Militärgeschichte und Sozialwissenschaften der Bundeswehr (ZMSBw) eine Studie zur „Nullmessung“ der Digitalkultur aufgesetzt. Sie soll wichtige Erkenntnisse liefern, wie die Bundeswehrangehörigen den Stand der Digitalisierung in der Bundeswehr bewerten, wo Informationsbedarf besteht und mit welchen Maßnahmen die Digitalkultur gefördert werden kann. Die hierfür unter Nutzung eines Onlineumfrage-Tools angeschriebenen 10.000 Bundeswehrangehörigen konnten im September 2020 einen Fragebogen mit insgesamt 27 Fragen zur Digitalisierung beantworten. Die Auswertung des

Datensatzes und Erstellung des Forschungsberichtes erfolgte bis Ende November 2020. Eine detaillierte ministerielle Auswertung und die Ableitung kurz- und langfristiger Maßnahmen schließt sich an. Hierzu wird im nächsten Digitalbericht vorgetragen werden.

Ein umfassendes Maßnahmenpaket zur Erhöhung der Digitalisierungsfähigkeit im Organisationsbereich IUD ist das Vorhaben zur **„Umsetzung der Maßnahmen der Unterarbeitsgruppe Digitale Transformation im Rahmen der Arbeitsgruppe Leitlinie IUD 2030 (AG IUD 2030+)“**.

Zur Weiterentwicklung des Organisationsbereiches IUD wurden im Rahmen der AG IUD 2030+ Möglichkeiten digitaler Lösungen zur Steigerung der Effizienz, Effektivität und Zufriedenheit der Bedarfsträger und Nutzer in der Leistungserbringung der IUD untersucht. Dies umfasst u.a. den Aufbau von Digitalkompetenzen und eines Wissensmanagements sowie die Nutzung von Technologietrends und Kommunikationsmaßnahmen. Hierzu wurden Ziele definiert und Maßnahmen zu deren Erreichung umgesetzt.

Um die Potentiale der Digitalisierung für die IUD zu nutzen, ist zunächst die Digitalkompetenz der eigenen Mitarbeiterinnen und Mitarbeiter zu entwickeln und durch geeignete Maßnahmen zu fördern. Durch den Aufbau einer „Wissensplattform Digitalisierung IUD“ im Wiki-Service der Bundeswehr und die Etablierung von Netzwerken für den Wissensaustausch sollen die Möglichkeiten der Digitalisierung besser erkannt und die Schaffung einer Digital-Kultur unterstützt werden.

Mit einem definierten Prozess zur Ideengenerierung für Pilotprojekte und deren anschließenden Umsetzung sollen Technologietrends genutzt werden, um die Leistungserbringung zu verbessern, Synergien zu heben und Ressourcen freizusetzen.

Zudem sollen mittels eines Leitfadens für das projektbegleitende VM von digitalen Projekten und einem Kommunikationsplan "Digitale Transformation" die Angehörigen des Organisationsbereiches IUD mit geeigneten Kommunikationsmaßnahmen für das Thema "Digitale Transformation" sensibilisiert und positiv gestimmt werden.

Durch die Konzipierung eines zentralen Managements über alle Digitalisierungsmaßnahmen des Organisationsbereiches IUD können alle relevanten Projekte unterstützt und gesteuert werden. Aktuell werden alle Maßnahmen und Ergebnisse in einer Digitalisierungsstrategie für den Organisationsbereich IUD zusammengefasst und mittels einer Reifegradanalyse unterlegt.

5. Ausblick

Die Digitalisierung in Gesellschaft und Bundeswehr wird weiter in hoher Geschwindigkeit voranschreiten. Die COVID-19-Pandemie wirkt hier wie ein Katalysator. Sicherheitspolitische Erfordernisse rücken ins Bewusstsein. Neben den laufenden Digitalisierungsaktivitäten und Maßnahmen zur Erhöhung der Digitalisierungsfähigkeit kommt daher vor allem dem Sonderprogramm Resilienz eine besondere Bedeutung zu.

Zusätzlich zu diesen Vorhaben und Programmen werden im Rahmen der strategischen Steuerung im Kern vor allem folgende Themen vorangetrieben:

- Weiterentwicklung der strategischen Ausrichtung der Digitalen Transformation durch Fortschreibung der „Roadmap Digitale Transformation“ für den Zeitraum 2021 – 2026: Die Roadmap greift den Ansatz der inhaltlichen Schwerpunktsetzung auf und rückt im Zeitverlauf gezielt Themen in den Fokus, um diese einer intensiveren Betrachtung zu unterziehen und zielgerichtet voranzutreiben.
- Neuauflage der „Umsetzungsstrategie Digitale Bundeswehr“: Die im Juni 2019 erlassene Umsetzungsstrategie wird auf Basis der bisherigen und vorgesehenen Entwicklungen bis Mai 2021 für einen Zeitraum von zwei Jahren fortgeschrieben. Dabei wird sie insbesondere die Inhalte der zuvor genannten Roadmap aufgreifen.
- Operationalisierung des Zielsystems Digitale Transformation: Die Operationalisierung des Zielsystems wird weiter vorangetrieben. Dafür werden Handlungsbedarfe konkretisiert und Ambitionen definiert. Ziel ist eine erstmalige Berichterstattung über den Stand der Zielerreichung im 6. Leitungsboard Digitalisierung.

Im Kontext des strategischen VM steht die sukzessive Befähigung der OrgBer über das Projektcoaching im Fokus sowie die Weiterentwicklung und Etablierung der VM Community. Die Ergebnisse der Studie zur Digitalkultur des GB BMVg werden als Grundlage für die Erarbeitung von Maßnahmen zur Erhöhung der Digitalkultur im GB BMVg dienen.

Der Digitale Campus mit seinen Kernelementen (Digitalrat, Digitalgalerie, Digitallabor) wird weiter ausgestaltet, implementiert bzw. verstetigt. Nächste ordentliche Sitzungen des Digitalrates des BMVg sind geplant. Die Digitalgalerie wird bis April 2021 in einer ersten Ausbaustufe im Intranet der Bundeswehr realisiert. Die Ausgestaltung des Digitallabors soll ebenfalls bis April 2021 erfolgen.

6. Abkürzungsverzeichnis

Abkürzung	Bedeutung
AG	Arbeitsgruppe
AWE	Auswahlentscheidung
BAAINBw	Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr
BAKS	Bundesakademie für Sicherheitspolitik
BAPersBw	Bundesamt für das Personalmanagement der Bundeswehr
BIM	Building Information Modeling
BiZBw	Bildungszentrum der Bundeswehr
BMI	Bundesministerium des Innern, für Bau und Heimat
BSI	Bundesamt für Sicherheit in der Informationstechnik
BWI	BWI GmbH
CAVE	Cave Automatic Virtual Environment
CIDCC	Cyber and Information Domain Coordination Center
CIHBw	Cyber Innovation Hub der Bundeswehr
CIO	Chief Information Officer
CIR	Cyber- und Informationsraum
CIT	Cyber/Informationstechnik
CITEC	Cyber/IT Evaluation Centre
CPM	Customer Product Management
DCR	Distributed Cyber Reconnaissance
Digit GesVersBw	Digitalisierung der Gesundheitsversorgung der Bundeswehr
D-LBO	Digitalisierung Landbasierte Operationen
DMAM	Digitalisierung Meldewesen Auslieferung Material
DMME	Digitalisierung Meldewesen Materielle Einsatzbereitschaft
DTEC.Bw	Zentrum für Digitalisierungs- und Technologieforschung
eGABw	Elektronische Gesundheitsakte Bundeswehr
ERP	Enterprise Resource Planning
EU	Europäische Union
eVA/CDI	Elektronische Verwaltungsarbeit/Collaboration, Digital Administration, Information Management
eVGA	Elektronische Verfahrens- und Gerichtsakte
F&T	Forschung und Technologie
FGK	Fachgesprächskreis
FüAkBw	Führungsakademie der Bundeswehr

FüSK	Führung Streitkräfte
GB BMVg	Geschäftsbereich des Bundesministeriums der Verteidigung
GenInspBw	Generalinspekteur der Bundeswehr
GesVersBw	Gesundheitsversorgung Bundeswehr
GMN	German Mission Network
GuiXT	Graphical user interface Extended
HaFIS	Harmonisierung der Führungsinformationssysteme
InspSKB	Inspekteur der Streitkräftebasis
IOCC	Interoperables Cloud Computing
IPD	Integrierte Planung durchführen
ISoLaBw	Innere und Soziale Lage der Bundeswehr
ITSysBw	Informationstechnik-System der Bundeswehr
IT-U	Informationstechnik-Unterstützung
IT-U Con	Informationstechnik-Unterstützung Controlling
IT-U ISoLaBw	Informationstechnik-Unterstützung Controlling, Zielbild Innere und Soziale Lage der Bundeswehr
IT-U DigLage	Informationstechnik-Unterstützung Digitalisierung Lagebilder
IUD	Infrastruktur, Umweltschutz und Dienstleistungen
KdoCIR	Kommando Cyber- und Informationsraum
KI	Künstliche Intelligenz
LV/BV	Landes- und Bündnisverteidigung
MEGA	Multisensorische und echtzeitnahe Gefechtsmanagementsystem auf einem ad hoc-Meshnetwork
MINT	Mathematik, Informatik, Naturwissenschaft und Technik
MiTeRa	Militärisches Technologie Radar Cyber/IT
NATO	North Atlantic Treaty Organization
NatTerrBefh	Nationaler Territorialer Befehlshaber
POC	Point of Contact
RDL	Reservistendienst Leistende
SASPF	Standard-Anwendungs-Software-Produktfamilien
SinN	Systeme in Nutzung
SKA	Streitkräfteamt
USG	Unterhaltssicherungsgesetz
VM	Veränderungsmanagement
VR	Virtual Reality
VR-TrBesZ	Virtual Reality-Truppenbesuchszentrum

WBO	Wehrbeschwerdeordnung
WDO	Wehrdisziplinarordnung
ZMSBw	Zentrum für Militärgeschichte und Sozialwissenschaften der Bundeswehr

7. Abbildungsverzeichnis

Abbildung 1: Messenger-Nutzung in der Bundeswehr - Wechsel von BwChat zu BwMessenger	10
Abbildung 2: Groupware Bw	12
Abbildung 3: Experiment VR-gestützter Lageraum – ein Schritt in Richtung Zukunft.....	14
Abbildung 4: VR-TrBesZ – Berufsbilder zum virtuellen (Er-)Leben erwecken.....	15
Abbildung 5: SASPF Plattform und Übersicht Lagebilder/Dashboards.....	16
Abbildung 6: Dashboard, Ansicht Überblick.....	17
Abbildung 7: Digitalisierungsprojekt GuiXT Luftwaffe – Optimierte Benutzeroberflächen.....	19
Abbildung 8: Erste Preise für das Cloudbasierte Gebäudemanagement mit BIM.....	21
Abbildung 9: Schwerpunktthemen Digitalrat des BMVg.....	24
Abbildung 10: Betrachtete Dimensionen und Teildimensionen des Reviews	29
Abbildung 11: Fünfstufige Bewertungsskala.....	29
Abbildung 12: Digitalisierungsaktivitäten – Überblick Phasen	31
Abbildung 13: Digitalisierungsaktivitäten – Umsetzungszeitraum	31
Abbildung 14: Digitalisierungsaktivitäten – Übersicht ausgewählte Beispiele	32
Abbildung 15: Digitalisierungsfähigkeiten – Überblick Phasen.....	37
Abbildung 16: Digitalisierungsfähigkeiten – Überblick Wirkebenen.....	37
Abbildung 17: Digitalisierungsfähigkeiten: Übersicht ausgewählte Beiträge.....	38
Abbildung 18: Bedeutung digitaler Kompetenzen (aktuell und perspektivisch).....	43
Abbildung 19: Bereitstellung von IT-Services durch Clusterprogramme.....	45

8. Anlage Eckpunktepapier

Ausbau der digitalen Souveränität im GB BMVg Eckpunktepapier

Herausgebende Stelle: BMVg CIT I 1

Stand: 28.08.2020

Version: 0.2

Inhalt

1.	Motivation	56
2.	Strategischer Kontext	57
3.	Handlungsfelder digitaler Souveränität im GB BMVg.....	58
3.1.	Nutzung vertrauenswürdiger IT	59
3.2.	Aufbau und Erhalt von Schlüsseltechnologien	60
3.3.	Erhalt der Kernführungsfähigkeit.....	60
3.4.	Erhöhung der Innovationsfähigkeit.....	61
3.5.	Aufbau und Erhalt digitaler Kompetenzen.....	61
4.	Fazit.....	62
5.	Anlagen	63

1. Motivation

Die erfolgreiche Gestaltung der Digitalen Transformation erfordert die Verfügbarkeit von verlässlicher, resilienter und sicherer Informations- und Kommunikationstechnik (IKT). Vor dem Hintergrund eines volatilen sicherheitspolitischen Umfelds, steigenden Abhängigkeiten von IKT im Geschäftsbereich (GB) BMVg und einer kontinuierlichen hohen Bedrohungslage im Cyber- und Informationsraum kommt der Bewahrung und dem Ausbau der nationalen technologischen und digitalen Souveränität (im Kontext Cyber/IT) eine Schlüsselrolle zu. Im GB BMVg wird unter „digitaler Souveränität“ das Vorliegen der erforderlichen Kontroll- und Handlungsfähigkeiten im Cyber- und Informationsraum verstanden, um den verfassungsgemäßen Auftrag der Bundeswehr sicher, selbstbestimmt und frei von ungewollter Einflussnahme durch Dritte ausüben zu können.

Aus diesem Anspruch werden als Ziele für den GB BMVg u.a. abgeleitet, Verfügbarkeit, Vertraulichkeit und Integrität der gewonnenen, gespeicherten, verarbeiteten und übertragenen Daten bzw. Informationen zu bewahren und die Handlungsfähigkeit im digitalen Umfeld sicherzustellen. Darunter fällt z.B. die aufgrund des verfassungsmäßigen Auftrags der Bundeswehr unabdingbare Fähigkeit, die eigene IT in jedem Fall, somit auch in Krisen und im Spannungs- bzw. Verteidigungsfall, selbstständig zu schützen, zu betreiben und wiederherzustellen. Aus nationalem Sicherheitsinteresse sind die hierfür notwendigen (Schlüssel-)Technologien⁴ von dauerhaft vertrauenswürdigen Herstellern zu beziehen. Einer zertifizierten, leistungsfähigen nationalen und europäischen IKT-Industrie kommt sowohl unter sicherheits- und verteidigungspolitischen als auch unter technologie- und industriepolitischen Aspekten eine strategische Bedeutung zu. Als weiterer Anspruch wird das Ziel abgeleitet, Abhängigkeiten von einzelnen IKT-Produktherstellern zu reduzieren, um den daraus resultierenden Einschränkungen der eigenen Handlungsfähigkeit zu begegnen.

Im Rahmen einer gesamtstaatlichen Sicherheitsvorsorge ist eine ressortübergreifende Vorgehensweise und darüber hinaus auch eine Zusammenarbeit auf europäischer Ebene bei den Themen der digitalen Souveränität von entscheidender Bedeutung. Positionen, wie beispielsweise jene des Eckpunktepapiers des IT-Planungsrats, IT-Rats und des Beauftragten der Bundesregierung für Informationstechnik zur „Stärkung der Digitalen Souveränität in der Öffentlichen Verwaltung“ vom 31. Januar 2020, werden entsprechend durch das BMVg unterstützt.

⁴ Schlüsseltechnologien sind Technologien, die aus den außen-, sicherheits- und europapolitischen Interessen Deutschlands, dem militärischen Bedarf der Bundeswehr, den Bündnisverpflichtungen sowie der Verantwortung Deutschlands abgeleitet und regelmäßig überprüft werden.

Ziel des vorliegenden Eckpunktepapiers ist es, das Leitbild digitaler Souveränität im GB BMVg mit bestehenden politisch-strategischen Zielen zu verknüpfen und Handlungsfelder zur Ausübung digitaler Souveränität für den GB BMVg aufzuzeigen.

2. Strategischer Kontext

Die digitale Souveränität im GB BMVg ist unter Berücksichtigung von Vorgaben der NATO, der EU sowie im nationalen Rahmen zu gestalten.

Wichtige Voraussetzungen für die Stärkung der europäischen IKT-Industrie wurden 2016 mit der **EU-Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union** geschaffen, welche erstmals einheitliche EU-Regeln festgelegt hat. Diese Richtlinie wurde 2018 mit dem **Rechtsakt zur Cybersicherheit** u.a. durch einen EU-weiten Zertifizierungsrahmen ergänzt. Der **EU-Politikrahmen für die Cyber-Abwehr** von 2018 stellt in Bezug auf den Cyberraum die Notwendigkeit heraus, einen Beitrag zur strategischen Autonomie Europas zu leisten. Dies kann z.B. durch die Erleichterung der zivil-militärischen Zusammenarbeit bei der Entwicklung von Cyberabwehr-Fähigkeiten und die Stärkung der technologischen und industriellen Basis der europäischen Verteidigung gelingen. Dazu wird u.a. die Wichtigkeit des Erschließens von Synergien zwischen der Forschung und Technologien-Anstrengungen im militärischen Bereich und den zivilen Programmen unterstrichen. In der im Februar 2020 veröffentlichten **Kommunikation der Europäischen Kommission zur „Gestaltung der digitalen Zukunft Europas“** wird zudem der Anspruch erhoben, als EU eigene digitale Schlüsselkapazitäten zu entwickeln und einzusetzen und so die Abhängigkeit von anderen Teilen der Welt bei den wichtigsten Technologien zu verringern. Mit der im März 2020 veröffentlichten **Industriestrategie der Europäischen Kommission** wird der industriepolitische Fokus der EU spezifiziert und u.a. folgende strategische, digitale Technologien („key enabling technologies“) festgelegt: Cloud-Computing, Blockchain, Quantentechnologie, Künstliche Intelligenz und der Mobilfunkstandard „5G“. Mit dem in der Entstehung befindlichen Europäischen Kompetenzzentrum für Cybersicherheit (ECCC) und dem Netzwerk nationaler Koordinierungszentren sollen Investitionen aus europäischen Digitalisierungsprogrammen gesteuert und die Fachexpertise der Mitgliedstaaten eingebunden werden.

Das **Weißbuch zur Sicherheitspolitik Deutschlands** verlangt den Erhalt festgelegter nationaler Schlüsseltechnologien aus nationalem Sicherheitsinteresse zur Bewahrung der technologischen Souveränität,

auch in Abstimmung und Zusammenarbeit mit europäischen Partnern. Zum Erreichen dieses Zieles nennt das Weißbuch die folgenden Instrumente:

- ressortübergreifende Abstimmung und Priorisierung von Forschungs- und Technologiemaßnahmen,
- gezielte Industriepolitik,
- Exportunterstützung,
- Auftragsvergabe durch das BMVg.

In dem im Februar 2020 veröffentlichten **Strategiepapier der Bundesregierung zur Stärkung der Sicherheits- und Verteidigungsindustrie** legt die Bundesregierung u.a. die folgenden sicherheits- und verteidigungsindustriellen Schlüsseltechnologien im Bereich Cyber/IT fest:

- sicherheitsrelevante Informations- und Kommunikationstechnologien (insbesondere Chip-, Netz- und Verschlüsselungstechnologien, Cyberabwehrsysteme sowie Host- und Netzforensik),
- Künstliche Intelligenz.

Analog zu den im Weißbuch genannten Instrumenten identifiziert das Strategiepapier zum Schutz und Förderung der festgelegten Schlüsseltechnologien Maßnahmen in den folgenden Bereichen: Forschung, Entwicklung und Innovation, Produktion, Beschaffung, Exportunterstützung und -kontrolle sowie Investitionskontrolle.

Die **Cyber-Sicherheitsstrategie für Deutschland 2016** bildet den ressortübergreifenden strategischen Rahmen. Ihr Anspruch, die Gewährleistung der Handlungsfähigkeit und Souveränität Deutschlands im Zeitalter der Digitalen Transformation zu sichern, soll durch sicheres und selbstbestimmtes Handeln in einer digitalisierten Umgebung, einen kooperativen Ansatz zwischen Wirtschaft und Staat, eine leistungsfähige und nachhaltige gesamtstaatliche Cyber-Sicherheitsarchitektur sowie durch eine aktive Positionierung Deutschlands in der europäischen und internationalen Cyber-Sicherheitspolitik erreicht werden.

Die **Strategische Leitlinie Digitalisierung** des GB BMVg greift die Forderung des Weißbuchs auf, definierte Schlüsseltechnologien im Schulterschluss mit anderen Ressorts und der Wirtschaft zu entwickeln oder zu erhalten, um so eine eigene „digitale Souveränität“ zu erreichen und zu erhalten.

3. Handlungsfelder digitaler Souveränität im GB BMVg

Das vorliegende Eckpunktepapier leitet aus den bestehenden politisch-strategischen Zielen eigene Handlungsfelder der digitalen Souveränität für den GB BMVg ab. Dazu zählen die Nutzung vertrauenswürdiger IT, der Aufbau und Erhalt von Schlüsseltechnologien, der Erhalt der Kernführungsfähigkeit, die

Erhöhung der Innovationsfähigkeit und der Aufbau und Erhalt digitaler Kompetenzen. Die Handlungsfelder bilden den Rahmen für unterschiedliche Themenkomplexe, welche im Zusammenwirken den Aufbau und die Stärkung der digitalen Souveränität im Verteidigungsressort ermöglichen sollen.

3.1. Nutzung vertrauenswürdiger IT

Die Nutzung vertrauenswürdiger IT-Hard- und Software (inkl. Firmware) ist eine entscheidende Grundlage für selbstbestimmtes staatliches Handeln im Cyber- und Informationsraum und somit Teil der digitalen Souveränität⁵.

Eine Stärkung der Vertrauenswürdigkeit der eingesetzten IT-Hard-, Firm- und Software ist immer Teil eines holistischen Ansatzes zur Gewährleistung der Cyber-Sicherheit mit dem Ziel, die Risiken auf ein tragbares Maß zu reduzieren.

Bei der Einführung von Technologien mit strategischer Auswirkung auf die IT der Bundeswehr (ITBw), wie z.B. die Cloud-Technologie, ist auch die Wahrung der digitalen Souveränität zu beachten. Daher wird die aufzubauende Cloud unter vollständiger Kontrolle des GB BMVg weitgehend unabhängig von externen partnerbetriebenen Diensten ausgestaltet.

Die Sicherheit der oftmals weltweiten Lieferketten der eingesetzten IT-Hard und Software muss unter Einbezug des gesamten Produktlebenszyklus und den Produktabhängigkeiten ebenfalls berücksichtigt werden. Die Förderung eigener industrieller Wertschöpfungsketten in Deutschland und der EU ist Teil der Risikominimierung und kann zur Stärkung der Vertrauenswürdigkeit beitragen.

Im Rahmen des IT-Architekturmanagements ist eine möglichst durchgängige Nutzung offener und international anerkannter Standards, Schnittstellen und Protokolle unter Beachtung der spezifischen Anforderungen der Bündnis-Interoperabilität von hoher Wichtigkeit. Dabei ist ebenfalls die Möglichkeit des uneingeschränkten Zugriffs auf den Quellcode der eingesetzten Produkte von besonderer Bedeutung. Dies dient sowohl der Vermeidung von Herstellerabhängigkeiten, sog. „Vendor lock-ins“, als auch der Informationssicherheit. Wo immer möglich, ist daher auf Open-Source basierende Lösungsansätze zu setzen. Zudem ist die Stärkung eigener Fähigkeiten zur Überprüfung der Vertrauenswürdigkeit der eingesetzten Komponenten im GB BMVg unerlässlich.

Zukünftig gilt es auch, Fragen der Vertrauenswürdigkeit der verschiedenen Hersteller in Vergabeverfahren verstärkt zu berücksichtigen, um die Vertrauenswürdigkeit der ITBw zu erhöhen und so die digitale Souveränität zu stärken.

⁵ Siehe dazu auch die Detailbetrachtung im Ideenpapier „Vertrauenswürdige IT“ des BMVg und den Industrieverbänden BDSV und Bitkom.

3.2. Aufbau und Erhalt von Schlüsseltechnologien

Ein Bestandteil zur Steigerung der Vertrauenswürdigkeit der ITBw und somit der digitalen Souveränität im GB BMVg ist der Aufbau und Erhalt der notwendigen nationalen sicherheits- und verteidigungsindustriellen Schlüsseltechnologien im Bereich Cyber/IT.⁶ Die Verfügbarkeit dieser Schlüsseltechnologien von vertrauenswürdigen Herstellern ist aus nationalem Sicherheitsinteresse zu gewährleisten, je nach Technologie in Abstimmung und Zusammenarbeit in der EU und der NATO. Um dieses Ziel zu erreichen, sind die im Weißbuch benannten Instrumente auch im Bereich Cyber/IT gezielt einzusetzen. Zudem sind die für diese Technologien vom Gesetzgeber geschaffenen vergaberechtlichen Spielräume konsequent zu nutzen. Wo derzeit Kernkompetenzen bei Schlüsseltechnologien fehlen, sollte ressortübergreifend und auf EU-Ebene durch gezielte Förderung langfristig die Leistungsfähigkeit der IKT-Industrie unterstützt werden. EU-Instrumente zur Investitionssteuerung und Schließung von Fähigkeitslücken (z.B. im Rahmen des Europäischen Verteidigungsfonds oder der Ständigen Strukturierten Zusammenarbeit) sind konsequent zu nutzen, um in der Zusammenarbeit die Effekte auf EU-Ebene zu verstärken. Der Ausgestaltung der Öffnung der jeweiligen Programme für Drittstaaten kommt dabei eine besondere Bedeutung zu.

Weiterhin wird im Rahmen der Ressortforschung des GB BMVg mittels wehrtechnischer Forschung & Technologie (F&T) kontinuierlich ein Schwerpunkt auf den Aufbau und Erhalt der Schlüsseltechnologien im Bereich Cyber/IT gelegt.

3.3. Erhalt der Kernführungsfähigkeit

Neben dem Einsatz vertrauenswürdiger IT und dem Erhalt und Ausbau von Schlüsseltechnologien beinhaltet digitale Souveränität im GB BMVg – und damit selbstbestimmtes Handeln im digitalen Umfeld – auch den Erhalt der Kernführungsfähigkeit (KFF)⁷. Um die KFF sicherzustellen, muss der GB BMVg im digitalen Umfeld handlungsfähig sein, auch und gerade wenn Kritische Infrastrukturen nicht mehr funktionsfähig sind. Dadurch entstehen besondere Ansprüche an Vertraulichkeit, Verfügbarkeit, Integrität, Resilienz und Durchhaltefähigkeit der ITBw. Zum Aufbau und Stärkung der digitalen Souveränität werden für ausgewählte IT-Anwendungen, IT-Produkte und IT-Infrastrukturen zwingend (geo-) redundante Systeme und Prozesse auf Grundlage einer Second-Source-Strategie benötigt. Die aus der KFF resultierenden Forderungen bestimmen zudem die Kernfähigkeiten IT (KFIT), definiert als die minimal notwendigen Bereitstellungen von IT-Services zum Erhalt der jeweiligen KFF. Der GB BMVg muss jederzeit in der Lage sein, die KFIT im Krisen-, Einsatz- und Verteidigungsfall im benötigten Umfang zu

⁶ Das im Februar 2020 veröffentlichte Strategiepapier der Bundesregierung zur Stärkung der Sicherheits- und Verteidigungsindustrie legt die sicherheits- und verteidigungsindustrielle Schlüsseltechnologien fest.

⁷ Kernführungsfähigkeit (KFF) beschreibt das unabdingbar erforderliche Mindestmaß an Führungsfähigkeit für den Inhaber der Befehls- und Kommandogewalt um eine durchgehende nationale Einsatz- und multinationale Operationsführung im gesamten Aufgabenspektrum sicherzustellen.

gewährleisten. Das schließt auch die Bereitstellung ergänzender Kapazitäten durch die BWI GmbH (BWI), zivilgewerbliche Dienstleister (inkl. externe IT-Serviceprovider), EU- und NATO-Agenturen oder Partnernationen mit ein.⁸ Ein weiteres wesentliches Element zur Sicherstellung der KFIT ist die Frequenzverfügbarkeit. Der Zugang zu militärisch nutzbarem elektromagnetischen Spektrum ist für die KFIT essentiell und daher für den Ausbau der digitalen Souveränität im GB BMVg zwingend erforderlich.

3.4. Erhöhung der Innovationsfähigkeit

Ein Baustein zum Ausbau der digitalen Souveränität im GB BMVg und einer zielgerichteten technologischen Weiterentwicklung sind verstärkte Investitionen in Forschung und Innovation als Grundlage für zukunftsorientierte Beschaffungen und Realisierung von IT-Services. Es sind, wo immer möglich, insbesondere nationale Entwicklungen zu fördern. Der Agentur für Innovation in der Cybersicherheit (Cyberagentur) unter der Federführung des BMVg und des BMI kommt eine hohe Bedeutung zur Stärkung der digitalen Souveränität zu. Die Cyberagentur wird in zukünftige Innovationen in der Cybersicherheit und diesbezüglicher Schlüsseltechnologien investieren. Das Zentrum für Softwarekompetenz der Bundeswehr wird mit dem Dezernat Innovationsmanagement die Innovationsfähigkeit des GB BMVg erhöhen. Des Weiteren stärkt der Cyber Innovation Hub der Bundeswehr die Schnittstelle zu Gründern und Startups, die eine wichtige Rolle beim frühzeitigen Innovations- und Praxistransfer im Bereich Cyber/IT spielen. Durch das Forschungsinstitut CODE an der Universität der Bundeswehr München wird zudem der Zugriff auf eigene universitäre Grundlagenforschung im Bereich der Cybersicherheit sichergestellt. Über das nationale Koordinierungszentrum im Rahmen des ECCC soll der europäische Austausch gestärkt werden. Um die nationale Verfügbarkeit digitaler und technologischer Innovationen kontinuierlich zu verbessern und innovative und interdisziplinäre Forschung in einem sicheren Umfeld zu betreiben, wird ein Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr aufgebaut. Ein Augenmerk des BMVg im Kontext der Stärkung der digitalen Souveränität liegt außerdem auf der Zusammenarbeit mit starken europäischen und nationalen Forschungsinstitutionen im Bereich digitaler Technologien.

3.5. Aufbau und Erhalt digitaler Kompetenzen

Das Verständnis von digitaler Souveränität des GB BMVg beinhaltet nicht nur technische Aspekte, sondern hängt auch maßgeblich vom Aufbau und Erhalt der erforderlichen digitalen Kompetenzen aller Angehörigen des Geschäftsbereichs ab. Folgerichtig wird bei der Digitalen Transformation im GB BMVg ein Schwerpunkt auf den Ausbau und die Förderung der digitalen Kompetenzen des Personals im gesamten

⁸ Die zivil-gewerbliche bzw. externe Leistungserbringung endet jedoch immer dort, wo entsprechende KFIT Bestandteil der KFF sind und die Erbringung dieser KFIT nicht in der Entscheidungsgewalt des verantwortlichen Truppenführers bzw. der verantwortlichen Truppenführerin liegen.

Geschäftsbereich gelegt. Die Förderung der Souveränität jedes Einzelnen im Umgang mit digitaler Technologien ist ein integraler Bestandteil digitaler Souveränität im GB BMVg. Da der Mensch im Mittelpunkt aller technischen Veränderungen steht, ist der Aufbau einer Digitalkultur im GB BMVg und der damit verbundenen Stärkung einer verantwortungsvollen Sicherheitskultur beim Einsatz digitaler Technologien auch im Kontext der digitalen Souveränität von besonderer Bedeutung.⁹ Die erforderliche digitale Kompetenz ist bei allen Angehörigen des GB auszubauen und über den gesamten Berufsweg weiterzuentwickeln.

4. Fazit

Mit der Digitalen Transformation sind zahlreiche Chancen, aber auch Herausforderungen und Risiken für den GB BMVg verbunden, denen u.a. durch den Ausbau der eigenen digitalen Souveränität begegnet werden muss. Das Ziel ist die Gewährleistung der notwendigen Handlungs- und Kontrollfähigkeiten im Cyber- und Informationsraum als GB BMVg und damit der Schutz nationaler Sicherheitsinteressen. Das vorliegende Eckpunktepapier deckt das weit zu fassende Themenfeld der digitalen Souveränität für den GB BMVg nicht vollständig ab. Für eine nachhaltige Umsetzung und die Entwicklung von Maßnahmen ist ein Ausbau der gesamtstaatlichen Fähigkeiten und damit ein ressortgemeinsames Vorgehen von hoher Bedeutung. Das BMVg verfolgt in den aufgeführten Handlungsfeldern zum Ausbau der digitalen Souveränität des GB einen vernetzten Ansatz, um den verfassungsgemäßen Auftrag sicher, selbstbestimmt und frei von ungewollter Einflussnahme durch Dritte ausüben zu können.

⁹ Siehe auch Umsetzungsstrategie Digitale Bundeswehr, S. 17.

5. Anlagen

5.1 Bezugsjournal

(Nr.) Bezugsdokumente	Titel
1.	EU-Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union 2016
2.	EU-Politikrahmen für die Cyber-Abwehr 2018
3.	EU-Rechtsakt zur Cybersicherheit 2019
4.	Kommunikation der Europäischen Kommission zur „Gestaltung der digitalen Zukunft Europas“ 2020
5.	Industriestrategie der Europäischen Kommission 2020
6. Die Bundesregierung vom 13.07.2016	Weißbuch 2016 zur Sicherheitspolitik und zur Zukunft der Bundeswehr
7. GB BMVg	Verteidigungspolitische Richtlinie
8. Die Bundesregierung vom 13.02.2020	Strategiepapier der Bundesregierung zur Stärkung der Sicherheits- und Verteidigungsindustrie
9.	Cyber-Sicherheitsstrategie für Deutschland 2016
10. SLL 001	Strategische Leitlinien Digitalisierung
11. SLL 006	Umsetzungsstrategie Digitale Bundeswehr
12. IT-Rat vom 24. März 2020	IT-Planungsrat, IT-Rat und der Beauftragte der Bundesregierung für Informationstechnik „Stärkung der Digitalen Souveränität in der Öffentlichen Verwaltung“.
13.	Ideenpapier „Vertrauenswürdige IT“ des BMVg und den Industrieverbänden BDSV und Bitkom 2019

5.2 Glossar

Cyber- und Informationsraum

Der CIR ist der als militärischer Operationsraum erschließbare, zugleich virtuelle, physische und kognitive Raum, der aus dem Cyberraum, dem Elektromagnetischen Umfeld sowie dem Informationsumfeld besteht.

Digitale Souveränität

Unter dem Begriff „digitale Souveränität“ versteht der GB BMVg die erforderlichen Kontroll- und Handlungsfähigkeiten im CIR, um den verfassungsgemäßen Auftrag der Bundeswehr sicher, selbstbestimmt und frei von ungewollter Einflussnahme durch Dritte ausüben zu können.

Digitale Kompetenzen

Unter Digitalen Kompetenzen wird das Wissen über und die praktische Verwendung von digitalen Anwendungen, die für die Information, Kommunikation und die Problemlösungsstrategien genutzt werden, verstanden. Ebenso wird mit Digitalen Kompetenzen das Verständnis über Chancen und potenzielle Gefahren, die das Internet und die Kommunikation über elektronische Medien mit sich bringen, beschrieben. Durch z. B. Schulungen und die regelmäßige Konfrontation mit digitalen Technologien können digitale Kompetenzen gefördert und ausgebaut werden

Digitalkultur

Digitalkultur meint den Umgang der Angehörigen der Bundeswehr mit den Anforderungen, Chancen und Risiken der Digitalisierung aufgrund eines gemeinsamen Grundverständnisses

ITBw

Die ITBw umfasst die gesamte im GB BMVg genutzte Informationstechnik (IT).

Second-Source-Strategie

Mit einer Second-Source-Strategie soll u.a. das Risiko der Abhängigkeit von einem Lieferanten sowie die Gefahr der Nichtverfügbarkeit eines Produktes verringert werden. Unter Second-Source (engl. für Zweitlieferant) werden eine oder mehrere alternative Lieferanten für ein Produkt bezeichnet, das baugleich und kompatibel mit einem anderen Produkt ist. Neben baugleichen (Lizenz-) Produkten kommen dafür auch funktionsgleiche Produkte verschiedener Hersteller in Betracht, falls diese die Anforderungen erfüllen.

5.3 Abkürzungsverzeichnis

Abkürzung	Bedeutung
IKT	Informations- und Kommunikationstechnik
GB BMVg	Geschäftsbereich Bundesministerium der Verteidigung
ECCC	Europäisches Kompetenzzentrum für Cybersicherheit
ITBw	IT der Bundeswehr
F&T	Forschung & Technologie
KFF	Kernführungsfähigkeit
KFIT	Kernfähigkeiten IT

Impressum

Herausgeber

Bundesministerium der Verteidigung

Stauffenbergstraße 18

10785 Berlin

Redaktionsschluss

5. Januar 2021

Gestaltung

Bundesministerium der Verteidigung

Bildnachweis

Titelbild: Bundeswehr / Roland Alpers

Seite 21 (Preisverleihung 19. eGovernment-Wettbewerb): BearingPoint / Andrew Graumann

Diese Publikation ist Teil der Öffentlichkeitsarbeit des Bundesministeriums der Verteidigung. Sie wird kostenlos abgegeben und ist nicht zum Verkauf bestimmt.