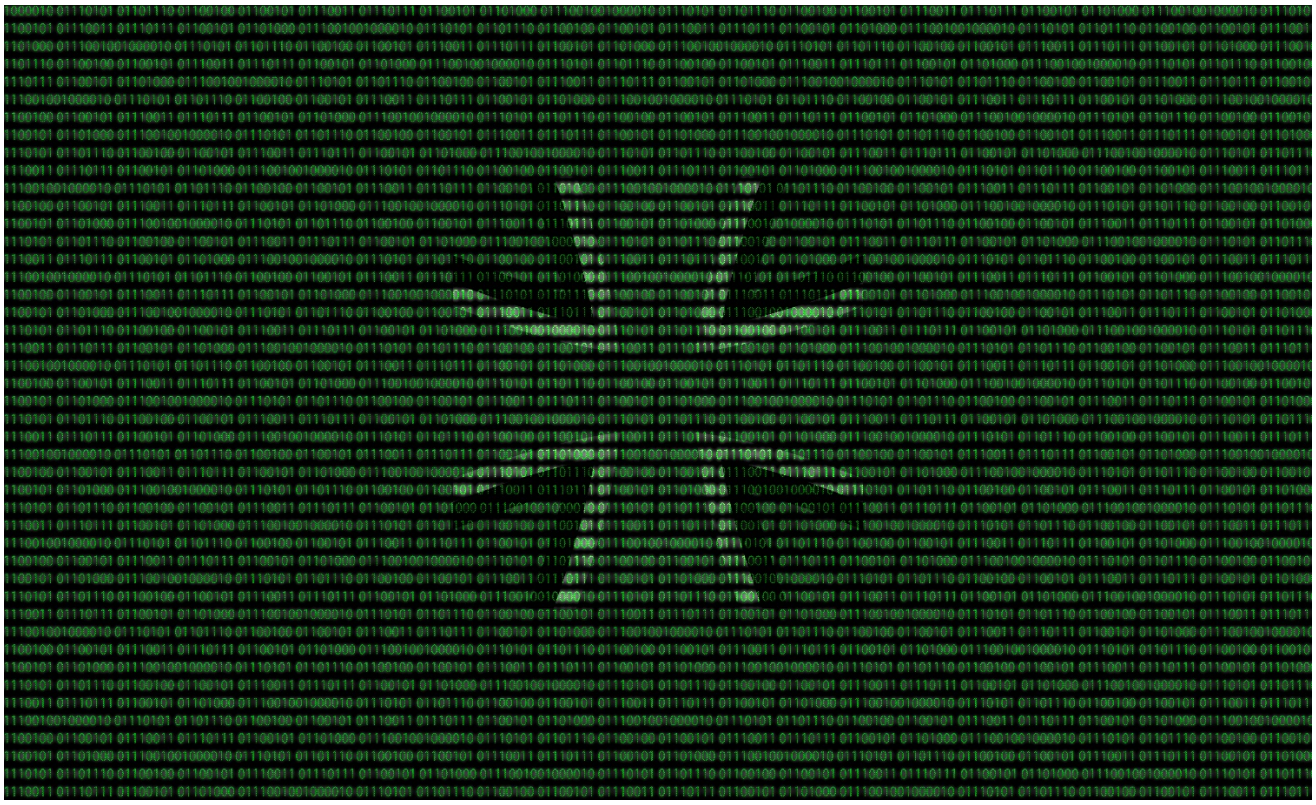
Bundesministerium
der Verteidigung

Erster Bericht zur Digitalen Transformation des Geschäftsbereichs des Bundesministeriums der Verteidigung

Berlin, Oktober 2019



Inhaltsverzeichnis

Kurzzusammenfassung 1

1. Einleitung 2

2. Chancen und Herausforderungen der Digitalen Transformation des Geschäftsbereichs BMVg 3

3. Rahmenbedingungen 4

4. Strategischer Ansatz der Digitalen Transformation des Geschäftsbereichs BMVg 8

   4.1. Strategische Grundlagendokumente 8

   4.2. Organisatorischer Aufbau 9

   4.3. Vorgehensmodell 14

5. Stand der Digitalen Transformation des Geschäftsbereichs BMVg 19

   5.1. Portfolio Digitalisierungsaktivitäten 20

   5.2. Maßnahmen zur Erhöhung der Digitalisierungsfähigkeit 24

   5.3. Innovationsthema künstliche Intelligenz 27

6. Ausblick 29

Kurzzusammenfassung

Digitalisierung ist richtungsweisend für die Zukunftsfähigkeit des Geschäftsbereichs des Bundesministeriums der Verteidigung (BMVg). Erste, wichtige Schritte sind bereits getan: Mit der „Strategischen Leitlinie Digitalisierung“ und der „Umsetzungsstrategie Digitale Bundeswehr“ wurden im Geschäftsbereich BMVg die notwendigen konzeptionellen Voraussetzungen geschaffen, um die Digitale Transformation des Geschäftsbereichs zielgerichtet anzustoßen. Auch organisatorisch hat sich der Geschäftsbereich auf die Digitale Transformation ausgerichtet und weitreichende strukturelle Veränderungen durchgeführt: Es wurde ein neuer Organisationsbereich Cyber- und Informationsraum aufgestellt und eine Abteilung Cyber/Informationstechnik im BMVg eingerichtet.

Leitprinzip der Digitalen Transformation ist die zentrale Steuerung bei dezentraler Umsetzung. Dafür wurden neben der Einrichtung eines Steuerungspanels und Leitungsboards auf höchster Leitungsebene in allen Abteilungen und Stäben im Ministerium sowie in allen Organisationsbereichen sogenannte Koordinatoren benannt, welche die Digitale Transformation in ihrem Verantwortungsbereich fördern. Zudem wurden ein Digitalrat BMVg als Beratungsgremium der Bundesministerin der Verteidigung initiiert und eine Vielzahl an Digitalisierungsaktivitäten sowie Maßnahmen zur Erhöhung der Digitalisierungsfähigkeit auf den Weg gebracht. Um Innovationen systematisch zu fördern, wurden unterschiedliche Innovationselemente ins Leben gerufen. Der Cyber Innovation Hub identifiziert Entwicklungen aus der Start-Up-Szene und soll sie für die Bundeswehr nutzbar machen. Eine „Cyberagentur“ ist, in Zusammenarbeit mit dem Bundesministerium des Innern, für Bau und Heimat, im Entstehen begriffen, um mittel- und langfristige technologische Entwicklungen in der Cybersicherheit frühzeitig erkennen und beauftragen zu können. Die Universität der Bundeswehr in München trägt schließlich mit dem Forschungsinstitut CODE die Perspektive universitärer Grundlagenforschung im Bereich Cyber bei und erweitert zugleich die wissenschaftlichen Ausbildungskapazitäten in einschlägigen Fachdisziplinen.

Gleichwohl steht die Digitale Transformation des Geschäftsbereichs BMVg noch vor wesentlichen Herausforderungen, wie etwa der Personalgewinnung und -bindung im Fachbereich IT. Auch hier wurden bereits erste Schritte, wie z.B. die Einführung von IT-relevanten Zulagen, eingeleitet, um die Bedarfsdeckung von IT-Personal zu verbessern. Unter der Überschrift „Umsetzen, Systematisieren und Ausprobieren“ bilden z.B. die Stärkung digitaler Kompetenzen und Förderung eines digitalen Mindsets, der Aufbau einer Digitalisierungsplattform oder die Erarbeitung von Grundlagen für ein bundeswehr- und streitkräftegemeinsames „Systemzentrum Digitalisierung Land“ die wesentlichen Schwerpunkte der derzeitigen Umsetzungsphase bis Ende 2020.

1. Einleitung

Der Koalitionsvertrag für die 19. Legislaturperiode bezeichnet die Digitalisierung als eine der großen Chancen für unser Land und seine Menschen. Zugleich wird festgestellt, dass angesichts der Dynamik der mit der Digitalisierung verbundenen Veränderungen große Schritte gewagt werden müssen, um an die Spitze zu kommen und unser Land in allen Bereichen zu einem starken Digitalland zu entwickeln.[1]

Diese mit der Digitalisierung verbundenen Veränderungen sind richtungsweisend für die Zukunftsfähigkeit des Geschäftsbereichs des BMVg. Digitalisierung ist für die Bundeswehr nicht grundsätzlich neu. Gleichwohl bleibt viel zu tun, um mit der „digitalen Revolution" Schritt halten zu können. Daher wurde durch die Leitung des BMVg die Digitale Transformation des Geschäftsbereichs BMVg nicht nur als „Megathema der Bundeswehr in der nächsten Dekade" und als einer der Arbeitsschwerpunkte gesetzt, sondern auch als „Führungsaufgabe" zur **Chefsache** erklärt.[2]

Unter Digitalisierung versteht der Geschäftsbereich BMVg die zielgerichtete Identifikation und das konsequente Ausschöpfen von Potenzialen, die sich aus digitalen Technologien ergeben. Folglich geht Digitalisierung über die Einführung technischer Innovationen weit hinaus. Sie beeinflusst die gesamte Handlungs- und Denkweise im Geschäftsbereich BMVg. Die mit der Digitalen Transformation verbundenen Maßnahmen reichen daher von Anpassungen in Bereichen der Führung, Ausbildung und Organisation über die konsequente Nutzung digitaler Technologien in Rüstungsvorhaben und die Digitalisierung von Arbeitsprozessen bis hin zu Etablierung von Innovationselementen einschließlich Anbindung an die Startup-Szene. Strategische Grundlagen, Organisationsstrukturen, Verfahren, Personalentwicklung, Beschaffung aber auch das „digitale Selbstverständnis" der Bundeswehr werden hierbei ganzheitlich schrittweise angegangen.

Dem Anspruch „Transparenz als strategisches Prinzip" folgend wird hiermit der erste Bericht zur Digitalen Transformation des Geschäftsbereichs BMVg vorgelegt. Der halbjährlich fortzuschreibende Bericht wird übergreifend über die Inhalte, Fortschritte und Risiken der Digitalen Transformation des Geschäftsbereichs BMVg wie auch über die Kerninhalte des jeweiligen Leitungsboards Digitalisierung informieren. Er wird zusätzlich zum Bericht des Bundesministeriums der Verteidi-

1 „Ein neuer Aufbruch für Europa. Eine neue Dynamik für Deutschland. Ein neuer Zusammenhalt für unser Land", Koalitionsvertrag zwischen CDU, CSU und SPD, 19. Legislaturperiode, 12. März 2018, Kapitel IV.5., S. 37.

2 Vgl. Eröffnungsworte der Bundesministerin der Verteidigung zum 1. Leitungsboard Digitalisierung am 9. November 2018, BMVg, „Digitalisierung der Bundeswehr: „Tempo machen!"" vom 12. November 2018, https://www.bmvg.de/de/aktuelles/digitalisierung-der-bundeswehr-tempo-machen--28986.

gung zu Rüstungsangelegenheiten erscheinen und die der Projektkategorie A zugeordneten Programme mit Schwerpunkt IT nach der gleichen Methodik darstellen.[3] Er wird den für das vierte Quartal 2019 geplanten Bericht zum Cyber- und Informationsraum nicht ersetzen.[4]

2. Chancen und Herausforderungen der Digitalen Transformation des Geschäftsbereichs BMVg

Digitalisierung ermöglicht die Durchsetzungsfähigkeit der Streitkräfte auf dem digitalisierten Gefechtsfeld und optimiert das unterstützende Verwaltungshandeln. Damit trägt sie entscheidend zur Auftragserfüllung der Bundeswehr bei.

Für die **Streitkräfte** ist die Digitalisierung der Schlüssel zur Informations-, Führungs- und Wirkungsüberlegenheit wie auch zur Verbesserung der Durchsetzungs- und Reaktionsfähigkeit. Zu bedenken ist dabei, dass auch potenzielle Gegner digitale Innovationen für neue Ansätze und Fähigkeiten bereits nutzen oder zukünftig nutzen werden, so dass zumindest eine entsprechende Reaktionsfähigkeit erforderlich ist. Im Rahmen des **Verwaltungshandelns** verspricht die Nutzung digitaler Technologien eine Steigerung der Effizienz und damit das Freisetzen personeller Ressourcen für den Kernauftrag. Darüber hinaus schafft die Digitale Transformation die Voraussetzung für eine umfassende Modernisierung der Arbeitswelt im Geschäftsbereich BMVg und trägt somit auch zur Attraktivität des Arbeitgebers Bundeswehr bei. Digitalisierung wirkt sich auch auf die Führungs- und Ausbildungskultur der Bundeswehr aus und stellt daher einen bedeutsamen Aspekt bei der Weiterentwicklung der Inneren Führung dar.

Die Digitalisierung des Geschäftsbereichs BMVg birgt nicht nur Chancen, sondern auch Risiken. Angesichts der ständig wachsenden Cybergefahren ist der Schutz der Informationstechnologie (IT) der Bundeswehr sowie die Gewährleistung der Informationssicherheit zwingend erforderlich. Die **Informationssicherheit** im Geschäftsbereich BMVg besteht aus einer flächendeckenden Informationssicherheitsorganisation mit definierten Rollen, eingespielten Prozessen, Meldewegen und Handlungsanweisungen.

Damit wird innerhalb des Geschäftsbereichs BMVg der Forderung und Umsetzung eines steuernden Informationssicherheitsmanagementsystems der Bundeswehr (ISMS Bw) nachgekommen.

---

3 Dies sind die-Programme „Harmonisierung der Führungsinformationssysteme“ (HaFIS) und „Digitalisierung landbasierter Operationen“ (D-LBO). Da die Programme im 9. Bericht des Bundesministeriums der Verteidigung zu Rüstungsangelegenheiten vom Juni 2019 im Detail vorgestellt wurden, wird in diesem Bericht aufgrund der zeitlichen Nähe der Veröffentlichungen auf eine Wiederholung verzichtet.

4 Der Bericht zum Cyber- und Informationsraum resultiert aus dem Maßgabebeschluss vom 20. Oktober 2016, siehe Haushaltsausschuss Ausschussdrucksache 18/3719.

Durch das ISMS Bw werden die Planung, Umsetzung, Gewährleistung und Überwachung von technischen Maßnahmen bzw. Maßnahmen an der IT selbst (Technische Informationssicherheit) sowie von personellen, infrastrukturellen und organisatorischen Maßnahmen im Einsatzumfeld der IT (Sicheres IT-Umfeld) erreicht.

Der 2017 im Organisationsbereich Cyber- und Informationsraum eingeführte „Chief Information Security Officer“ der Bundeswehr (CISOBw) verantwortet zentral die Lage, Kontrolle und Steuerung der Informationssicherheit in der Bundeswehr. Dem CISOBw arbeitet das Zentrum für Cybersicherheit (ZCSBw) mit dem zum 24/7-Dienst befähigten Cyber Security Operation Center (CSOCBw) mit Schwerpunkt Incident Management, IT-Forensik, Netzüberwachung und Hotline zu. Zur Durchführung von Schwachstellenanalysen und „Red Teaming“ kann er neben den weiteren Kräften des ZCSBw auch auf Kräfte des Zentrums für Cyber Operationen (ZCO) zugreifen. Im Bereich der zentralen Überwachung der Informationssicherheit in der Bundeswehr stehen dem CISOBw vier Regionalzentren des ZCSBw (Wilhelmshaven, Köln/Wahn, Berlin (zurzeit in Storkow), Ulm) zur Verfügung, die bis zum Erreichen der Full Operational Capability auf insgesamt 20 Prüfteams aufwachsen werden.

Darüber hinaus unterstützt das Zentrum für Softwarekompetenz der Bundeswehr (ZSwKBw) als weiterer Baustein im Cyber- und Informationsraum und zentraler Kompetenzträger für Innovation und Weiterentwicklung der Softwarelandschaft die Entwicklung und Integration digitalisierter und resilienter IT-Services für das IT-System der Bundeswehr.

Zur Informationssicherheitslage wird auf den Bericht zum Cyber- und Informationsraum verwiesen.[5]

Um der Informationssicherheit als Enabler der Digitalisierung umfassender gerecht zu werden, ist für den nachgeordneten Bereich des BMVg die Zusammenlegung der Bereiche Informationssicherheit, administrativer Datenschutz, Geheimschutz und militärische Sicherheit in einem Organisationselement „Sicherheitsmanagement“ angewiesen.

3. Rahmenbedingungen

Den **nationalen politischen Rahmen** für die Digitale Transformation des Geschäftsbereichs BMVg bildet die aktuelle Umsetzungsstrategie der Bundesregierung „Digitalisierung gestalten“ vom März 2019. In dieser konzentriert sich die Bundesregierung auf Schwerpunktvorhaben, die die einzelnen

5 Der Bericht zum Cyber- und Informationsraum ist bisher VS-NfD (Verschlusssache – Nur für den Dienstgebrauch) eingestuft.

Bundesministerien identifiziert haben. Ziel ist es, sowohl in der Zusammenarbeit zwischen den Bundesministerien als auch in Kooperation mit Wirtschaft und Wissenschaft Synergieeffekte zu nutzen. Das BMVg hat zehn Schwerpunktvorhaben in diese Umsetzungsstrategie gemeldet, die den Handlungsfeldern „Innovation und digitale Transformation“, „Gesellschaft im digitalen Wandel“ und „Moderner Staat“ zugeordnet sind (vgl. Abbildung 1).

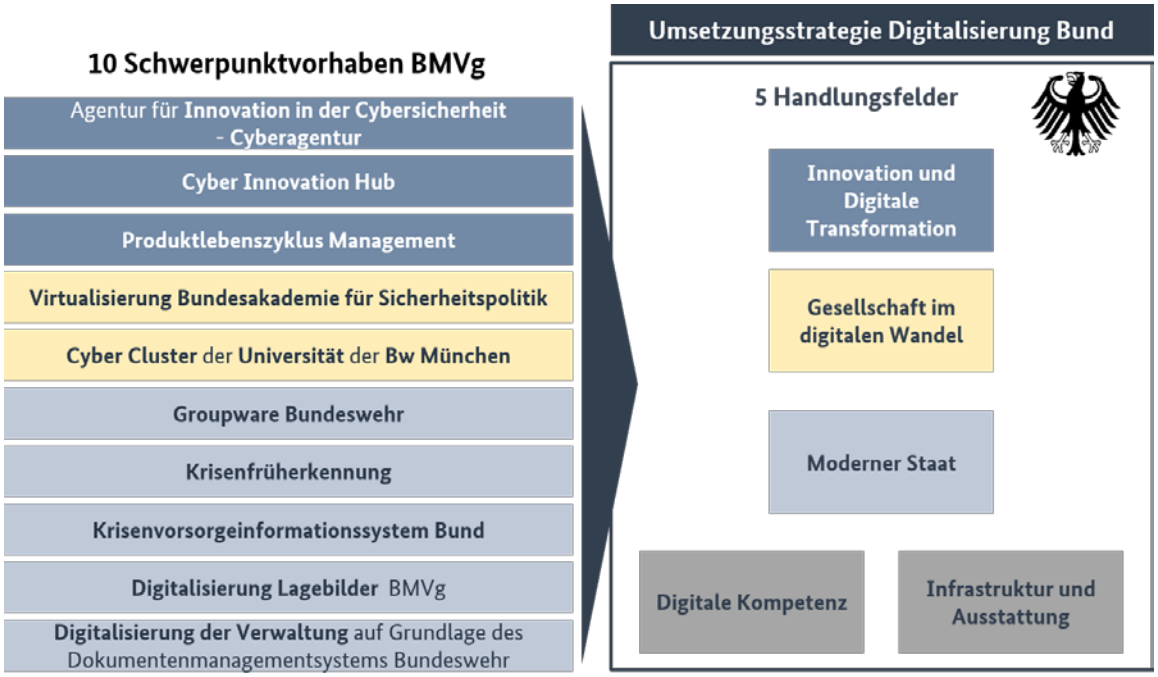


Abbildung 1: Schwerpunktvorhaben BMVg in der Umsetzungsstrategie der Bundesregierung „Digitalisierung gestalten“ vom März 2019

Beispielhaft für diese Schwerpunktvorhaben sei das beim 2. Leitungsboard Digitalisierung am 11. Juni 2019 vorgestellte „Krisenvorsorgeinformationssystem Bund“ (KVInfoSysBund) genannt:

Beispiel: Krisenvorsorgeinformationssystem Bund

Die Bewältigung der gesamtstaatlichen Aufgabe des Nationalen Risiko- und Krisenmanagement zum Schutz deutscher Staatsangehöriger im Ausland (NatRKM) bei zunehmender Komplexität erfordert ein ressortgemeinsam nutzbares, von stationär bis mobil einsetzbares sowie flexibel erweiterbares KVInfoSysBund. Es soll dem gestiegenen Bedarf des BMVg und anderer zuständiger Ressorts an einem umfassenden Informations- und Datenaustausch sowie modernen Kommunikationsformen zur Unterstützung gemeinsamer Prozessabläufe bei der Bewältigung von Krisenlagen gerecht werden.

Aufgaben und Funktionen eines IT-gestützten Systems zur Unterstützung aller Maßnahmen im Rahmen NatRKM sind:

- prozedurale, organisatorische und technische Grundlage eines ressortübergreifend zugänglichen „Informationsraum für das NatRKM“,
- weltweit und unmittelbar sowie ohne Zeitverzug nutzbares System,
- Einsatz moderner Werkzeuge und Kommunikationsformen für die Vorbereitung, Planung, Durchführung und Nachbereitung aller Maßnahmen im Rahmen des NatRKM,
- effiziente Suche und Analyse vorhandener Informationen und Bearbeitungsmöglichkeit auf Basis moderner Kollaborations-Werkzeuge,
- schnelles Erzeugen eines gemeinsamen Lagebildes sowie differenzierte Lagedarstellung und -bearbeitung mit hohem Aktualisierungsgrad,
- Unterstützung der Lagefeststellung und des Entscheidungsprozesses der jeweiligen Krisenstäbe der Bundesregierung, Lagezentren und Einsatzstäbe.

Ziel ist es, in 2020 mit der Realisierung zu beginnen, um Anfang 2022 Anwendungen bzw. Funktionen auf Basis einer gemeinsamen Plattform für die ressortübergreifende Zusammenarbeit im Rahmen NatRKM bereitstellen zu können.

Neben den politischen Rahmenbedingungen spielen die **rechtlichen Rahmenbedingungen** für die Digitale Transformation des Geschäftsbereichs BMVg eine zentrale Rolle. Sie ergeben sich insbesondere aus dem am 25. Juli 2013 erlassenen E-Government-Gesetz. Im Zuge der Umsetzung verfügt der Geschäftsbereich BMVg seit März 2016 über ein zentrales Postfach, das einen Zugang über De-Mail ermöglicht. Seit Juli 2017 wird die elektronische Akte in der Bundeswehr über das Projekt „Dokumentenmanagement und elektronische Archivierung im IT-gestützten Geschäftsgang der Bundeswehr“ (DokMBw) in der ersten Ausbaustufe ausgerollt. Der geplante Rollout umfasst bis Dezember 2020 das BMVg und die Dienststellen der ersten nachgeordneten Ebene.[6] Zur Umsetzung des elektronischen Rechtsverkehrs mit den Gerichten und den Dienststellen, die Ordnungswidrigkeitenangelegenheiten bearbeiten, wurden im Geschäftsbereich BMVg seit Dezember 2018 – im Sinne einer Erstbefähigung – elektronische Gerichts- und Verwaltungspostfächer (eGVP) für die Truppendienstgerichte und besondere elektronische Behördenpostfächer (beBPo) für relevante Dienststellen eingerichtet. In diesem Zusammenhang wurde auch eine erste Möglichkeit der Verifikation qualifizierter elektronischer Signaturen an elektronischen Dokumenten geschaffen. Bis Ende 2019 werden Lösungsvorschläge für eine bedarfsdeckende Ausstattung sowohl

6 Dies gilt, soweit die personellen Ressourcen für die Einführung und Nutzung von DokMBw zeitgerecht in den vom Rollout betroffenen Dienststellen geschaffen werden können.

im Bereich der De-Mail als auch der eGVP/beBPo erarbeitet. Der Rollout der Ziellösung ist für 2021 geplant.

Auch im Kontext **internationaler Verpflichtungen**, vorrangig in der Europäischen Union (EU) und der Organisation des Nordatlantikvertrages (NATO), gestaltet das BMVg durch eine deutsche Teilhabe an Digitalisierungsvorhaben aktiv mit. Die übergeordneten Trends der Digitalisierung (z.B. künstliche Intelligenz, 5G) werden aktuell durch zivil geprägte Entwicklungen gesetzt. Aus militärischer Sicht ist hier ein enger Austausch zwischen EU- und NATO-Aktivitäten elementar. Generell bietet die Digitalisierung die Möglichkeit, Streitkräfte multinational zu verzahnen und vertiefend zu integrieren. Etwaige Interoperabilitätsherausforderungen können durch die Digitalisierung überwunden werden.

Die **EU** hat die herausgehobene Bedeutung der Digitalisierung als eine zentrale Herausforderung und Chance für die Gesellschaft wie auch für die Mitgliedstaaten erkannt. Das „European Cybersecurity Competence Network and Center“ (Europäisches Kompetenzzentrum für Cybersicherheit in Industrie, Technologie und Forschung und Netzwerk nationaler Koordinierungszentren) ist ein Vorschlag der Europäischen Kommission, mit dem Ziel, die Anstrengungen zur Erforschung und Entwicklung von Cybersicherheitstechnologien innerhalb der EU zu bündeln. Für den Geschäftsbereich BMVg bietet sich hier die Möglichkeit zivil-militärische Forschung und Entwicklung von „Dual-Use“ Cybersicherheitstechnologien auf europäischer Ebene voranzutreiben und so Synergien nutzen zu können. Außerdem soll das ressorteigene Forschungsinstitut „Cyber Defence und Smart Data“ (CODE) der Universität der Bundeswehr (UniBw) München innerhalb des Netzwerks nationaler Koordinierungszentren eine wichtige Rolle einnehmen. CODE koordiniert mit dem Projekt CONCORDIA einen Piloten des zukünftigen „European Cybersecurity Competence Network and Center“. Im Zuge der Deutschen EU-Ratspräsidentschaft in der 2. Jahreshälfte 2020 plant das BMVg das Thema der Digitalisierung der Streitkräfte im Rahmen des GSVP-Ziels „Einheitliche europäische Digital- und Cyber-Kompetenz“ inhaltlich auszugestalten. Auch im Hinblick auf Cybersicherheit und Cyberverteidigung gilt es, die Kohärenz von auswärtigem Handeln und anderen Politikbereichen zu wahren. Hierdurch wird das Risiko verringert, dass die Schnittstelle zwischen intergouvernementalem und supranationalem politischen Handeln der EU zu einer Sollbruchstelle wird.

Die **NATO** beschäftigt sich aktiv mit Chancen wie auch Risiken der Digitalisierung, ohne diese jedoch einem zentralen Digitalisierungsbegriff unterzuordnen. Der Arbeitsschwerpunkt liegt hier auf

„Cyber Defence“. Deutschland unterstützt im Rahmen der Vorbereitungs- und Entscheidungsprozesse in NATO-Gremien Maßnahmen zur Implementierung des Cyber- und Informationsraums als Domäne der Operationsführung und des „Cyber Defence Action Plan“, insbesondere in den Bereichen organisatorischer Anpassungen, der Aktualisierung von Doktrinen, aber auch bei der Modernisierung der IT-Umgebung und Stärkung der Resilienz im Cyberraum. So kündigte die Bundesministerin der Verteidigung während des Treffens der NATO-Verteidigungsminister am 13.-14. Februar 2019 in Brüssel an, dass Deutschland unter Beibehaltung nationaler, politischer und rechtlicher Vorbehalte grundsätzlich bereit ist, nach Einzelfallentscheidung NATO Operationen mit souveränen nationalen Cyber-Operationen zu unterstützen. Auch bringt sich Deutschland mit hochqualifiziertem Fachpersonal und in der konzeptionellen Grundlagenarbeit in das SHAPE Cyberspace Operationscenter ein, das die NATO derzeit implementiert.

Weitere Beispiele der aktiven Teilhabe Deutschlands an Digitalisierungsvorhaben der NATO sind das Vorantreiben der Bestrebungen zur Schaffung einer NATO Innovationsstrategie oder die aktive Unterstützung der beabsichtigten Schaffung einer Position eines „NATO Chief Information Officer“ auf höchster Ebene, um dem Erfordernis einer sinnvollen Bündelung von Innovations-, Implementierungs- und Regelungskompetenzen wie auch Verantwortlichkeiten gerecht zu werden. Ferner unterstützt Deutschland den Ansatz, auf strategischer Ebene neuen Entwicklungen Rechnung zu tragen und sich der Thematik „Daten als strategische Ressource“ anzunehmen.

4. Strategischer Ansatz der Digitalen Transformation des Geschäftsbereichs BMVg

Der strategische Ansatz der Digitalen Transformation des Geschäftsbereichs BMVg umfasst neben den erarbeiteten strategischen Grundlagendokumenten und organisatorischen Anpassungen auch ein Vorgehensmodell, das auf einer zentralen Steuerung bei gleichzeitiger dezentraler Umsetzung der Digitalisierung basiert.

4.1. Strategische Grundlagendokumente

Mit der „Strategischen Leitlinie Digitalisierung“ und der „Umsetzungsstrategie Digitale Bundeswehr“ wurden die strategischen Grundlagen der Digitalen Transformation des Geschäftsbereichs BMVg geschaffen.

Die „**Strategische Leitlinie Digitalisierung“** vom 31. März 2017 zeigt auf, wie das hohe Innovationstempo und die querschnittliche Bedeutung der Informationstechnik aufgenommen, mit den Erfordernissen und Rahmenbedingungen des Geschäftsbereichs BMVg in Einklang gebracht und wirksam für die Auftragserfüllung genutzt werden können.

Die „**Umsetzungsstrategie Digitale Bundeswehr**“ vom 14. Juni 2019 schließt an die „Strategische Leitlinie Digitalisierung“ an, konkretisiert das dort enthaltene Zielbild und beschreibt das Vorgehen und die konkreten Schritte zur Umsetzung und Steuerung der Digitalen Transformation des Geschäftsbereichs BMVg. Darüber hinaus wurden den ministeriellen Abteilungen und Stäben sowie den militärischen und zivilen Organisationsbereichen der Bundeswehr konkrete Aufgabenpakete zur Umsetzung zugeordnet. Die in der Umsetzungsstrategie beschriebene „**Roadmap Digitale Bundeswehr**“ gibt einen Überblick über den geplanten Weg der Digitalen Transformation des Geschäftsbereichs BMVg. Die derzeitige Phase bis Ende 2020 steht unter der Überschrift „Umsetzen, Systematisieren und Ausprobieren“ (vgl. Abbildung 2).

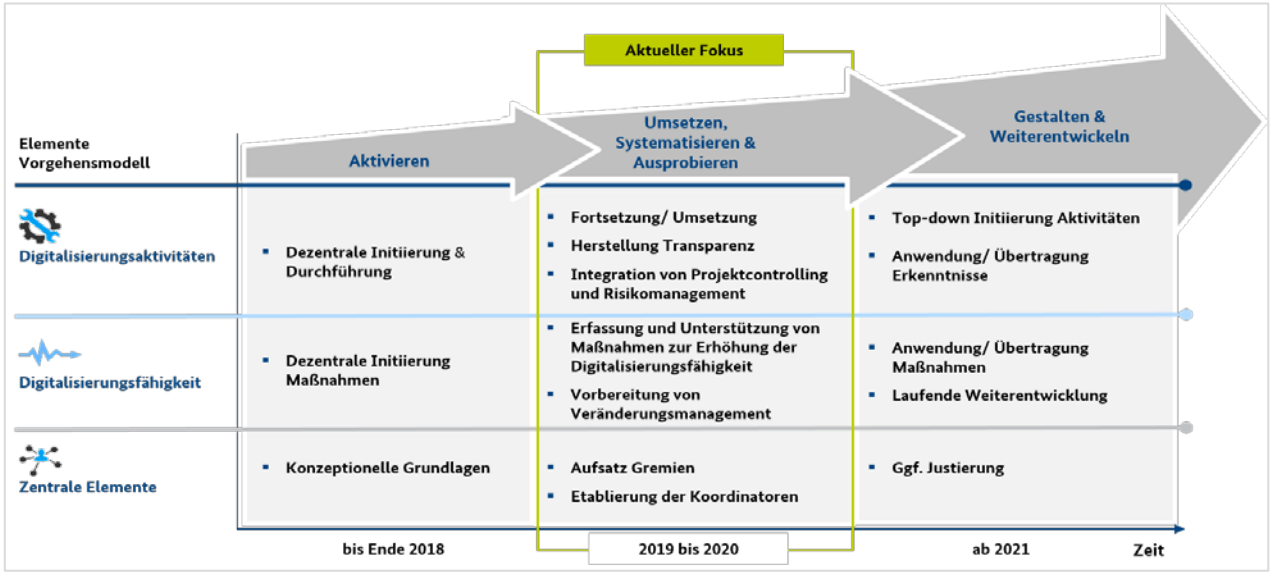


Abbildung 2: Roadmap Digitale Bundeswehr, „Umsetzungsstrategie Digitale Bundeswehr“ 2019

Angesichts der Dynamik der mit der Digitalisierung verbundenen Veränderungen ist eine regelmäßige Anpassung der strategischen Grundlagendokumente geplant. Die „Umsetzungsstrategie Digitale Bundeswehr“ wird in spätestens zwei Jahren überarbeitet.

4.2. Organisatorischer Aufbau

Der Geschäftsbereich BMVg hat die Konsequenzen der Digitalen Transformation erkannt und entsprechende Maßnahmen eingeleitet. Zum 1. Oktober 2016 wurde die **Abteilung Cyber/Informa-**

tionstechnik (CIT) im BMVg eingerichtet. In dieser wurden die bis dahin über mehrere Abteilungen verteilten Zuständigkeiten im Bereich Cyber/Informationstechnik in weiten Teilen gebündelt.[7] Sie werden durch den Abteilungsleiter CIT, der zugleich die Funktion des „Chief Information Officer" des Geschäftsbereichs BMVg inne hat, aus einer Hand gesteuert.

Dabei verantwortet das Referat CIT I 1 unter anderem den Themenbereich **„Cyber- und Digitalpolitik"** und stellte bis zum 1. Juli 2019 das **„Sekretariat Digitalisierung"**. Im Zuge der konsequenten Stärkung der Digitalisierung wurde zum 1. Juli 2019 ein neues Referat eingerichtet, das die **„Strategische Steuerung der Digitalisierung"** unterstützt.

Zugleich wurde ein neues Referat eingerichtet, das den Aufbau, die Unterstützung und Weiterentwicklung der **Digitalisierungsplattform** im Geschäftsbereich BMVg koordiniert.

Die Digitalisierungsplattform soll wesentliche IT-Services in eine einheitliche IT-Architektur einbinden und damit der Bundeswehr in einer standardisierten Form zur Verfügung stellen. Derzeit werden vergleichbare IT-Services vielfach in unterschiedlicher Ausprägung gerüstet, was zu hohem Betriebsaufwand und Zeitbedarf für den Planungs- und Ausrüstungsprozess sowie zu mangelnder Interoperabilität führt. Durch die Digitalisierungsplattform sollen IT-Services schneller bereitgestellt werden. Hierbei ist beabsichtigt, Programme und Projekte architekturgetrieben vorausschauend aufzusetzen. Als ersten Schritt zur Umsetzung der Digitalisierungsplattform hat BMVg CIT – neben der Einrichtung der oben genannten, neuen Referate – ebenfalls zum 1. Juli 2019 eine neue Struktur eingenommen. Es wurden sieben **Clusterreferate** gebildet, die als **„Baukastensystem"** weitgehend überschneidungsfrei IT-Services und IT-Projekte verantworten (vgl. Abbildungen 3 und 4).

7 Unberührt bleiben Zuständigkeiten der Abteilung Recht für bestimmte Rechtsfragen im Zusammenhang mit Cyber- und Informationstechnik und der Abteilung Strategie und Einsatz für Einsatzaspekte von Cyber-Operationen sowie für einsatzbedingte operative Belange im Zusammenhang mit IT-Services.

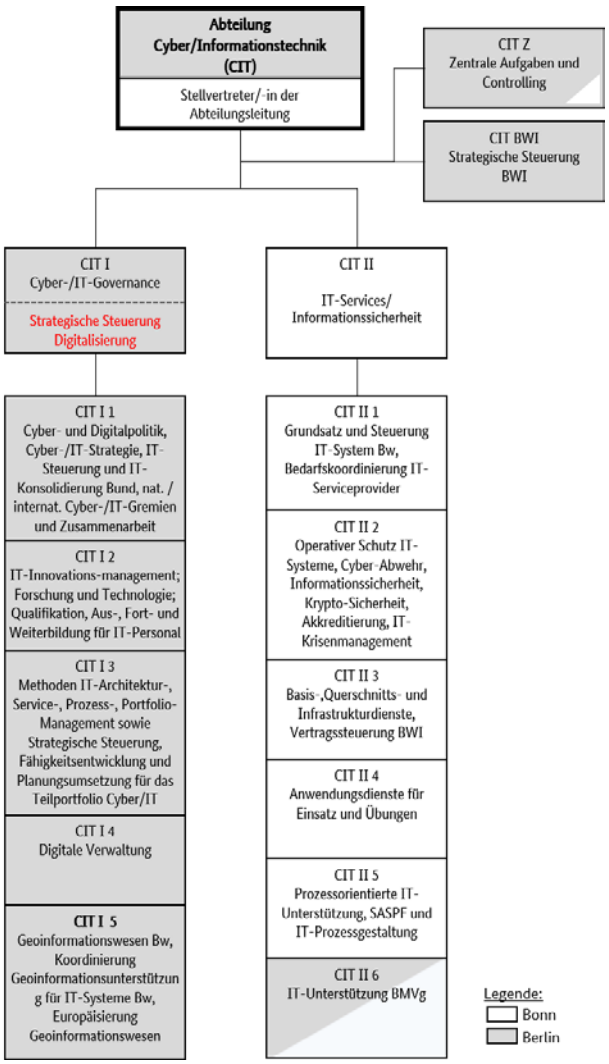


Abbildung 3: Organigramm BMVg CIT bis 30. Juni 2019

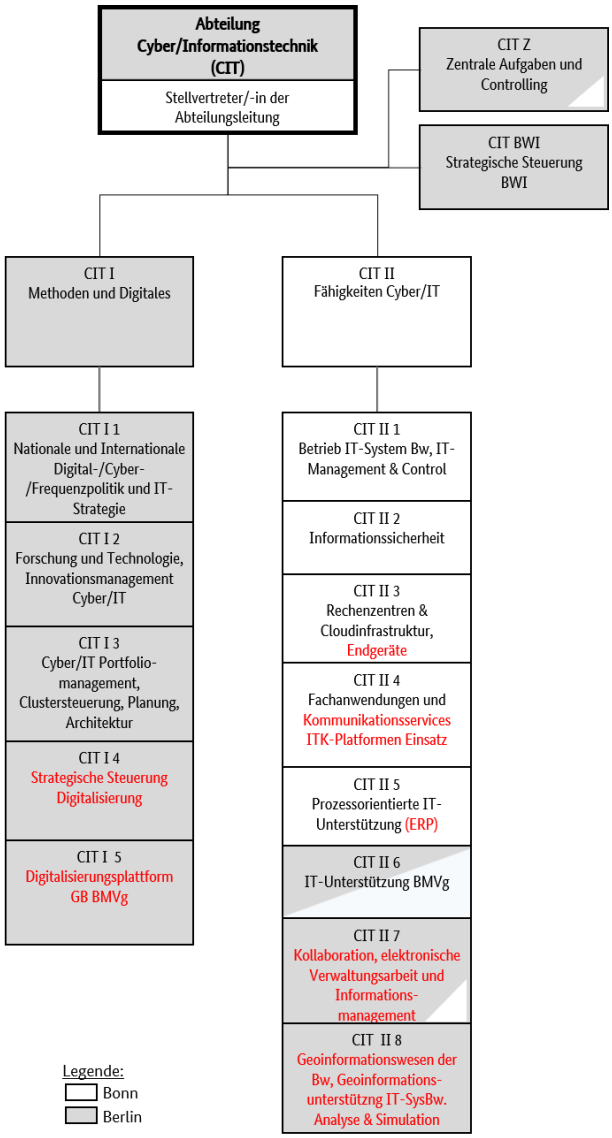


Abbildung 4: Organigramm BMVg CIT seit 1. Juli 2019

Die Cluster steuern die jeweils zugeordneten IT-Projekte auf ministerieller Ebene. Sie setzen clusterspezifisch Vorgaben und Standards für die jeweils zugeordnete IT bzw. die zugeordneten Services und Projekte im Geschäftsbereich BMVg. Die Realisierung von IT-Services folgt dabei künftig einem zentral gesteuerten ganzheitlichen Ansatz bezüglich Planung, Realisierung, Betrieb und Weiterentwicklung (vgl. Abbildung 5). Grundlage dafür ist ein architekturgetriebener, übergreifender Bebauungsplan für das Teilportfolio Cyber/IT. Die durch Nutzerforderungen bestimmten Integrationsprojekte sollten die IT-Serviceprojekte der Cluster als Standardbausteine nutzen. Mit diesem Ansatz sollen Planungs- und Rüstungsprozesse und damit die Bereitstellung innovativer IT-Lösungen beschleunigt und die IT-Services im Geschäftsbereich BMVg standardisiert werden. In der Folge werden Anpassungen und ggf. Erweiterungen der etablierten Prozesse, Rollen und

Gremien sowie organisatorische Anpassungen im Kommando Cyber- und Informationsraum (Kdo CIR), im Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr und bei der BWI GmbH nötig.

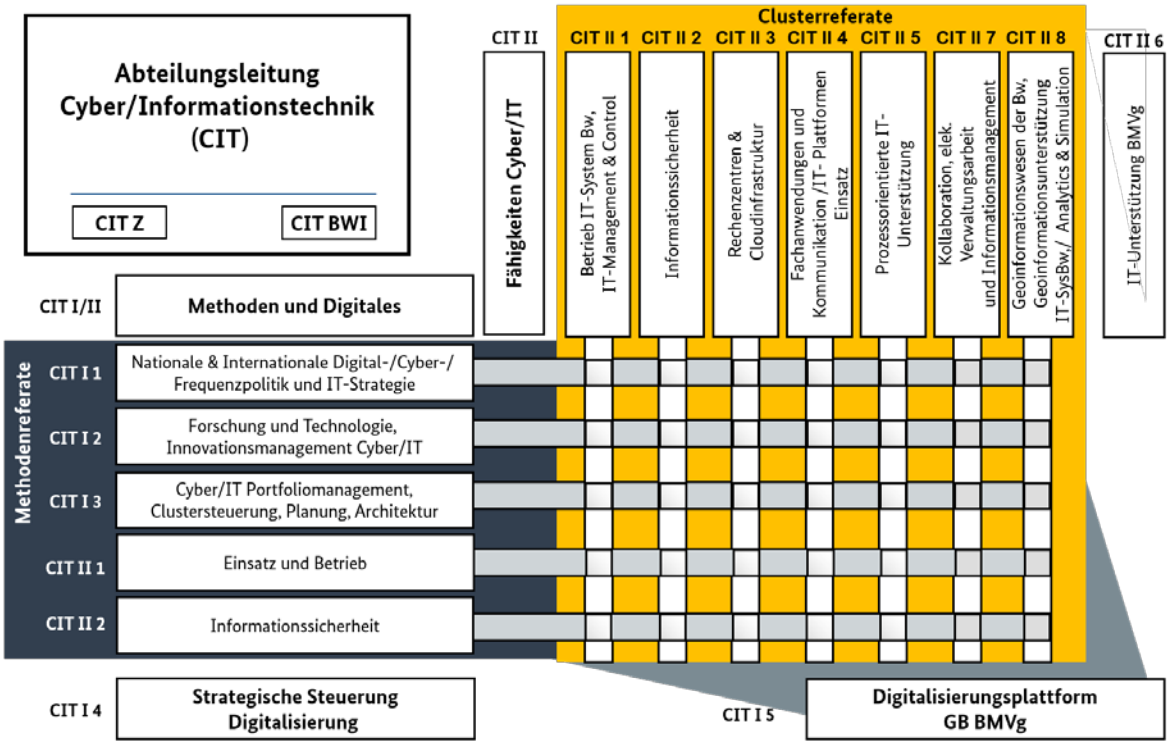


Abbildung 5: Matrixorganisation Abteilung Cyber/Informationstechnik (CIT)

Ebenfalls zum 1. Juli 2019 wurde in der Abteilung Führung Streitkräfte im BMVg in direkter Zuordnung zum Leitungsboard Digitalisierung die Projektorganisation „Digitalisierung Lagebilder BMVg“ als eigenständiges Referat eingerichtet. Damit wird dieses Schwerpunktvorhaben des Ressorts durch den Aufbau weiterer digitaler Kompetenz konsequent vorangetrieben.

Unterhalb des BMVg wurde am 1. April 2017 ein neuer **militärischer Organisationsbereich Cyber- und Informationsraum** aufgestellt. In Ergänzung zu den Dimensionszuständigkeiten von Heer, Luftwaffe und Marine, verantwortet dieser Organisationsbereich ganzheitlich die Dimension Cyber- und Informationsraum. Die Bündelung der Zuständigkeiten im Cyber- und Informationsraum und damit die Stärkung des Bereiches ist die Antwort auf die sicherheitspolitischen Herausforderungen in Folge der zunehmenden Digitalisierung. Sie setzt konsequent das Verständnis des Cyber- und Informationsraumes als eigenständige Domäne von Operationen durch die Staats- und

Regierungschefs aller Mitgliedstaaten der NATO auf dem Gipfeltreffen vom 9. Juli 2016 in Warschau um.[8] Die ca. 11.600 zivilen und militärischen Angehörigen[9] des Organisationsbereiches Cyber- und Informationsraum (Stichtag: 1. Juni 2019) stellen zum einen den Einsatz, Schutz und Betrieb des IT-Systems der Bundeswehr im Inland und im Einsatz sicher. Zum anderen stärken sie Fähigkeiten zur Aufklärung und Wirkung im Cyber- und Informationsraum und entwickeln diese weiter. Der Inspekteur des Cyber- und Informationsraums führt den Organisationsbereich aus dem Kdo CIR in Bonn. Der Organisationsbereich Cyber- und Informationsraum wird kontinuierlich weiter aufgebaut, mit seinen umfangreichen Fähigkeiten weiterentwickelt und soll ab dem Jahr 2021 seine volle Einsatzbereitschaft erreichen.

Um die benötigte Expertise in einem sich schnell und ständig wandelnden Bereich aktuell zu halten und die Fähigkeiten der Bundeswehr im Cyber- und Informationsraum durch fachlichen Austausch und Wissenstransfer zu verbessern, wurde eine **„Cyber-Reserve“** eingerichtet. Der Generalinspekteur der Bundeswehr zeichnete am 3. März 2017 das „Konzept für die personelle Unterstützung der Cyber Community der Bundeswehr“ („Cyber-Reserve“). Die „Cyber-Reserve“ steht nicht nur für ehemalige Soldaten mit Cyber- und IT-Expertise offen, sondern ist einem weiteren Personenkreis zugänglich, z.B. Wissenschaftlern, Geschäftsführern von IT-Unternehmen oder Angehörigen von Nicht-Regierungsorganisationen. Diese können sich auf unterschiedlichen Wegen, z.B. im Rahmen ehrenamtlichen, bürgerschaftlichen oder vertraglichen Engagements, „ungedient“ und ohne Soldatenstatus einbringen. Zum 26. Juni 2019 lagen dem Kommando Cyber- und Informationsraum 829 Interessenbekundungen für die „Cyber Reserve“ vor, 253 Reservistendienste wurden bereits durchgeführt.

In anderen Organisationsbereichen der Bundeswehr wurden unterschiedliche Organisationselemente bestimmt, geschaffen oder sind in Planung, die dem Themenkomplex der Digitalisierung zugeordnet sind.

So soll beispielsweise zukünftig ein „Systemzentrum Digitalisierung Land“ wesentliche Aufgaben im Zuge der Digitalisierung der Landstreitkräfte wahrnehmen. Im „Systemzentrum Digitalisierung Land“ sollen alle mit der Digitalisierung der Landstreitkräfte verbundenen Maßnahmen an einer Stelle zusammengeführt werden. Das „Systemzentrum Digitalisierung Land“ wird in Federführung

8 Warsaw Summit Communiqué, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016, Ziff. 70, https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

9 Ohne Personal im Ausbildungsstatus (zusätzlich ca. 1.500 Angehörige).

des Heeres gemeinsam durch verschiedene Organisationsbereiche der Bundeswehr betrieben werden.

Im Bundesamt für das Personalmanagement der Bundeswehr wird das Human Resources Laboratory „Modernes Personalmanagement" (HR Lab) in eigener Verantwortung aufgebaut. Eine dort geschaffene Testumgebung bietet die Möglichkeit, Innovationen unter Zuhilfenahme moderner Methoden, Verfahren und Technologien zeitlich begrenzt und lokal auf eine Umsetzung für das Personalmanagement der Bundeswehr hin zu testen und in den Wirkbetrieb zu überführen. Erfolgreich erprobte Technologien und Verfahrensweisen bilden dann den Ausgangspunkt für die Beschleunigung von Prozessanpassungen und die weitere Digitalisierung von Prozessen.

4.3. Vorgehensmodell

Zur Strukturierung der Umsetzung der Digitalen Transformation des Geschäftsbereichs BMVg wurde ein **Vorgehensmodell** (vgl. Abbildung 6) erarbeitet und in der „Umsetzungsstrategie Digitale Bundeswehr" verankert. Es beschreibt die für das Grundprinzip „zentrale Steuerung bei dezentraler Umsetzung" erforderlichen Elemente.

Die dezentralen Umsetzungselemente treiben die Umsetzung einzelner **Digitalisierungsaktivitäten** und Maßnahmen zur Erhöhung der **Digitalisierungsfähigkeit** im Rahmen der bestehenden Verfahren und Verantwortlichkeiten voran. Die **Strategische Steuerung und Unterstützung** der Digitalen Transformation erfolgt durch die **zentralen Elemente** Leitungsboard Digitalisierung und Steuerungspanel Digitalisierung. Diese werden durch die Einrichtung eines Digitalen Campus, bestehend aus Digitalrat, Digitallabor und Digitalgalerie, komplementiert und durch das Referat „Strategische Steuerung Digitalisierung" operativ unterstützt.

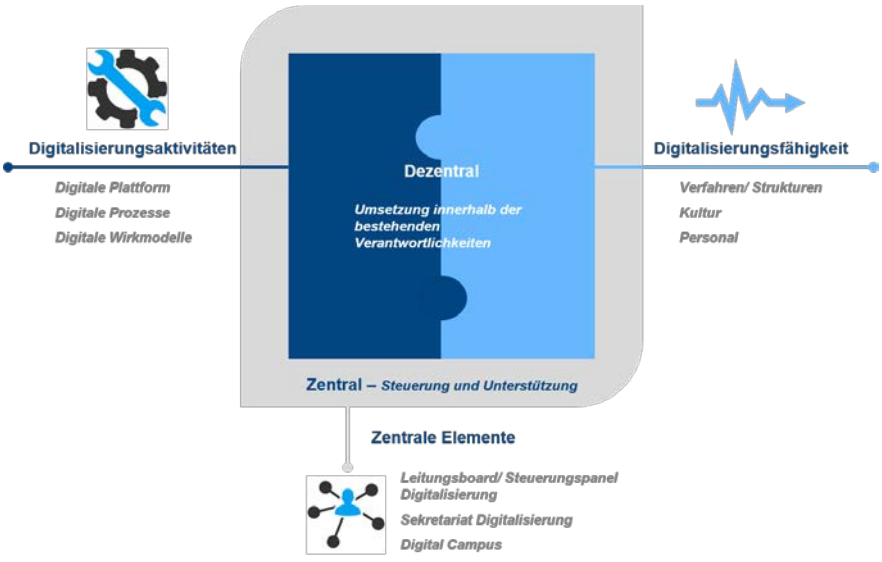


Abbildung 6: Vorgehensmodell der Digitalen Transformation des Geschäftsbereichs BMVg, „Umsetzungsstrategie Digitale Bundeswehr" 2019

4.3.1. Strategische Steuerung und Dezentrale Umsetzung

Das **Leitungsboard Digitalisierung** wurde am 12. Dezember 2017 als Steuerungs- und Entscheidungsgremium auf höchster Leitungsebene eingerichtet. Es tagt unter der Leitung der Bundesministerin der Verteidigung. Ständige Teilnehmer sind neben den beamteten Staatssekretären der Generalinspekteur der Bundeswehr, die ministeriellen Abteilungsleiterinnen bzw. Abteilungsleiter sowie der Leiter des Stabes Organisation und Revision im BMVg. Bislang wurden weitere Teilnehmer, wie beispielsweise die Inspekteure der militärischen Organisationsbereiche, die Präsidentinnen des Bundesamtes für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr, des Bundesamtes für das Personalmanagement der Bundeswehr, des Bundesamtes für Infrastruktur, Umweltschutz und Dienstleistungen der Bundeswehr und der Amtschef des Planungsamtes der Bundeswehr hinzugezogen. Das 1. Leitungsboard Digitalisierung fand am 9. November 2018 statt, das **2. Leitungsboard Digitalisierung** wurde am 11. Juni 2019 durchgeführt. Zur Vorbereitung auf das Leitungsboard tagte jeweils das **Steuerungspanel Digitalisierung** unter Leitung des zuständigen Staatssekretärs.

Das in der Abteilung CIT eingerichtete **Referat „Strategische Steuerung Digitalisierung“** ist der operative Arm des Leitungsboards und des Steuerungspanels. Es schafft Transparenz über laufende Digitalisierungsaktivitäten und Maßnahmen zur Erhöhung der Digitalisierungsfähigkeit, berät die Durchführenden und gibt zukünftig auch Impulse zur Initiierung neuer Vorhaben.

Um die **dezentrale Umsetzung** der Digitalen Transformation sicherzustellen, haben alle ministeriellen Abteilungen und Stäbe sowie die militärischen und zivilen Organisationsbereiche der Bundeswehr auf Kommando- und Ämterebene sogenannte „**Koordinatoren Digitalisierung**“ benannt. Deren Aufgabe ist es, eigenständig und aktiv die Digitalisierung in ihrem jeweiligen Verantwortungsbereich zu gestalten. Mit dem **Tag der Koordinatoren**, der erstmalig am 4. April 2019 stattfand, wurde ein Format initiiert, das den Austausch der Koordinatoren untereinander im Sinne einer „Digital Community“ fördert. Weiterhin besteht ein Netzwerk von „Points of Contact“ in jeder Abteilung und jedem Stab des BMVg sowie in jedem Organisationsbereich der Bundeswehr. Dieses Netzwerk wird vom Referat „Strategische Steuerung Digitalisierung“ orchestriert.

4.3.2. Digitaler Campus

Der Digitale Campus soll durch das Zusammenwirken eines Digitalrates, eines Digitallabors und einer Digitalgalerie zur systematischen Identifikation und Nutzbarmachung von Digitalisierungsaktivitäten und -fähigkeiten beitragen und die Innovationsgeschwindigkeit des Geschäftsbereichs BMVg insgesamt erhöhen.

Der **Digitalrat** berät die Bundesministerin bzw. den Bundesminister der Verteidigung als Expertengremium hinsichtlich der Digitalen Transformation des Geschäftsbereichs BMVg. Dabei soll der Rat u.a. den strategischen Ansatz der Digitalen Transformation des Geschäftsbereichs BMVg wie auch konkrete Innovationen bewerten und insbesondere als Impulsgeber agieren. Er besteht aus sechs, jeweils für zwei Jahre benannten, ständigen Mitgliedern aus Wissenschaft, Wirtschaft, Gesellschaft sowie aus dem Geschäftsbereich BMVg. Zusätzlich werden bei Bedarf themenbezogen zwei sogenannte Springer (Bundeswehr, Startup-Szene) herbeigezogen. Der Digitalrat wurde am 16. April 2019 eingerichtet. Die **konstituierende Sitzung** der ständigen Mitglieder des Digitalrates für die Sitzungsperiode 2019-2021 fand am 15. Mai 2019 statt. Diese ständigen Mitglieder sind:

- aus der Wissenschaft: Univ.-Prof.'in Dr. Cristina Besio, Professur für Soziologie mit Schwerpunkt Organisationssoziologie, Helmut-Schmidt-Universität / UniBw Hamburg; Univ.-Prof.'in Dr. Gabi Dreo Rodosek, Lehrstuhl für Kommunikationssysteme und Netzsicherheit, Leitende Direktorin FI CODE / UniBw München,
- aus der Wirtschaft: Martin Kaloudis, Chief Executive Officer, BWI GmbH; Matthias Moeller, Chief Executive Officer, Arvato Systems GmbH / Chief Information Officer, Bertelsmann SE & KGaA,
- aus der Zivilgesellschaft: Lena-Sophie Müller, Geschäftsführerin, Initiative D21 e.V.,
- aus dem BMVg: Ministerialdirigent Ralf Schnurr, BMVg, Abteilung Ausrüstung, Unterabteilungsleiter II und Direktor „Forschung & Technologie".

Das **Digitallabor** soll die im Geschäftsbereich BMVg bereits vorhandene digitale Expertise und entsprechende Produkte im Geschäftsbereich BMVg (z.B. Studien, Prototypen) systematisch mit Bedarfsträgern der Bundeswehr zusammenführen und als zentrale Anlaufstelle für innovative Technologien dienen. Dazu soll das Digitallabor als virtuelle Organisation die Innovationsakteure und Innovationselemente der Bundeswehr miteinander verknüpfen.

Die **wesentlichen Innovationselemente** stellen das Forschungsinstitut „Cyber Defence und Smart Data" (FI CODE) an der UniBw München, der Cyber Innovation Hub der Bundeswehr (CIH), die im Aufbau befindliche Agentur für Innovation in der Cybersicherheit (Cyberagentur) sowie die digitalen „Test- und Versuchsstrukturen" dar.

Forschungsinstitut CODE

Das an der UniBw München am 23. Juni 2017 eröffnete ressorteigene Forschungsinstitut CODE verfolgt das Ziel, technische Neuerungen und Konzepte zum Schutz von Daten, Software sowie

IT-Systemen integrativ und interdisziplinär in einem universitären Umfeld zu erforschen und prototypisch entwickeln zu lassen. Seit dem 1. Januar 2018 läuft der Studienbetrieb im neuen Master-Studiengang „Cyber-Sicherheit“ an der Universität neben dem schon bestehenden Bachelor- und Master-Studiengang „Informatik“, der hinsichtlich seiner Kapazitäten erweitert worden ist. Beide werden die professionelle wissenschaftliche Aus-, Fort- und Weiterbildung der eigenen Fach- und Führungskräfte mithilfe von elf zusätzlichen Professuren, von denen zum 1. Juli 2019 vier besetzt waren, nachhaltig stärken. Die UniBw München soll zu einem der zentralen Forschungs- und Entwicklungsorte für die IT-Sicherheitsforschung des Bundes ausgebaut werden und die Kooperation mit einschlägigen Ressorts, anderen (Sicherheits-)Behörden des Bundes und der Länder, der Wirtschaft und Wissenschaft sowie weiteren gesellschaftlichen Institutionen bei der Befassung mit Sicherheitstechnologien und Sicherheitsanwendungen systematisch ermöglichen. Für das Wintertrimester 2018 hatten sich acht Bachelor-Studierende der UniBw München für den Master-Studiengang „Cyber-Sicherheit“ immatrikuliert. Im aktuellen Wintertrimester 2019 haben sich 14 Bachelor-Studierende der UniBw München für den Masterstudiengang „Cyber-Sicherheit“ eingeschrieben, darüber hinaus fünf Externe, wobei vier davon dem Geschäftsbereich des Bundesministeriums des Inneren, für Bau und Heimat (BMI) angehören (Zentrale Stelle für Informationstechnik im Sicherheitsbereich sowie Bundesamt für Verfassungsschutz). Aktuell hat sich das FI CODE als Projektkoordinator und Führer eines Konsortiums mit 46 Partnern aus 18 Nationen „CONCORDIA“ bei einer europäischen Ausschreibung für das zivile EU-Forschungsrahmenprogramm „Horizont 2020“ erfolgreich beworben. Die EU beabsichtigt mit der Förderung von insgesamt vier Pilotprojekten („Competence Networks“) den Aufbau eines „European Cybersecurity Competence Networks and Center“ voranzutreiben und somit die Weiterentwicklung einer europäischen Cybersicherheitsstrategie zu unterstützen.

Cyber Innovation Hub

Das BMVg entschied im März 2017 im Rahmen eines Pilotprojekts den CIH aufzubauen. Die strategische Steuerung des CIH erfolgt über ein Steuerungspanel unter dem Vorsitz von Herrn Staatssekretär Zimmer. Der CIH soll als „Digital Innovation Unit“ (DIU) der Bundeswehr durch gezielte Marktbeobachtung und Innovations-Scouting neue Ideen und existierende Lösungen identifizieren, experimentell in Zusammenarbeit mit Nutzern validieren und entwickeln lassen mit dem Ziel, diese digitalen Innovationen der Bundeswehr kurzfristig verfügbar zu machen. Ferner soll er für Startup-Unternehmen und andere innovative Marktteilnehmer als Schnittstelle zur Bundeswehr und „Marktplatz“ fungieren. Er führt u.a. Studien, Pilotprojekte und Ideenwettbewerbe durch. Dabei soll der CIH nach agilen Prinzipien unter Startup-ähnlichen Bedingungen arbeiten. Er orientiert

sich an „Best Practices" ähnlicher Einheiten in der Wirtschaft und anderer Streitkräfte (z.B. USA, Israel). Der CIH ist die erste DIU eines Bundesministeriums und kann auch im internationalen Vergleich als wegweisend bezeichnet werden. Die Haushaltsmittel für den Grundbetrieb des CIH sowie für die (Weiter-) Entwicklung von Innovationen im Bereich Cyber/IT betragen in 2019 jeweils 5 Mio. Euro. Der CIH hat 36 Beschäftigte (Stichtag: 1. Juli 2019). Dabei stehen 19 Personen der Belegschaft in einem Arbeitsverhältnis mit der BWI GmbH. Hinzu kommen 14 Reservistendienst Leistende und drei Soldaten. Das Pilotprojekt soll spätestens am 31. Dezember 2019 enden. Es wurde im Jahr 2018 evaluiert. Zwecks Verstetigung wurde eine Wirtschaftlichkeitsuntersuchung durchgeführt und im März 2019 abgeschlossen. Im Ergebnis wird das BMVg den CIH ab 2020 als eine Abteilung der BWI GmbH verstetigen.

Cyberagentur

Um die Entwicklung innovativer Lösungen im Bereich der Cybersicherheit voranzutreiben, hat die Bundesregierung am 29. August 2018 beschlossen, eine Agentur für Innovation in der Cybersicherheit (Cyberagentur) unter der Leitung von BMVg und BMI zu gründen. Die Einrichtung der Cyberagentur ist notwendig, weil nationale und europäische Schlüsseltechnologien für die Verteidigung im Cyberraum nicht ausreichend zur Verfügung stehen. Gleichzeitig entwickelt sich dieser Bereich exponentiell. Das Handeln der Cyberagentur wird in die Zukunft gerichtet sein. Sie wird nach Lösungen für Herausforderungen suchen, deren Tragweite wir heute noch nicht abschätzen können. Die Cyberagentur wird Forschungsvorhaben fokussieren, die im Rahmen der gesamtstaatlichen Sicherheitsvorsorge einen strategischen Vorteil für die Technologiesouveränität bieten können, z.B. Quantentechnologie, künstliche Intelligenz oder alternative Rechnerarchitekturen. Aufgabe der Agentur wird sein, bahnbrechende Innovationen zu identifizieren und konkrete Aufträge für die Entwicklung von Lösungsmöglichkeiten zu vergeben. Sie wird die einzelnen Programme planen, steuern, priorisieren und zusammenführen. Nach Fertigstellung eines Programms wird die Agentur die Ergebnisse der Bundesregierung zur Verfügung stellen und verwalten. Die Cyberagentur soll 2019 in der Region Leipzig/Halle gegründet werden. Dort werden bis zum Jahr 2022 bis zu 100 neue Arbeitsplätze entstehen. Die Auswahl des Standortes ist Bestandteil der Heimatstrategie der Bundesregierung.

Test- und Versuchsstrukturen

Um iterativ und der Innovationsgeschwindigkeit angepasst digitale Technologien zu testen und für die Streitkräfte so schnell wie möglich zu adaptieren, wurde der Aufbau eines ersten digitalen

„TestBed“ im Kontext der „Digitalisierung Landbasierter Operationen“ (= „Systemzentrum Digitalisierung Land“) in der „Umsetzungsstrategie Digitale Bundeswehr“ beauftragt. Den Anforderungen des Gefechtsfelds der Zukunft werden die Streitkräfte nur gerecht, wenn Lösungen in enger Zusammenarbeit zwischen Operateuren und Technologie-Kompetenzträgern erarbeitet und auf Effektivität sowie Robustheit in Operationen getestet und realisiert werden. Die zahlreichen Erfahrungen der Truppe fließen unmittelbar ein. Die Test- und Versuchsstrukturen sollen künftig auch Produkte des CIH oder der Cyberagentur testen und so den Kreis der Innovationelemente des Geschäftsbereichs BMVg schließen.

Als weiteres Element des Digitalen Campus soll die **Digitalgalerie** künftig technische Innovationen für die Nutzer innerhalb aber auch außerhalb des Geschäftsbereichs BMVg erlebbar machen, zum Ausprobieren bereitstellen und das Feedback in die Weiterentwicklung der Innovationen spiegeln.

Die Zusammenarbeit und wechselseitige Förderung der vorgenannten drei Elemente[10] des Digitalen Campus wird zukünftig durch das Referat „Strategische Steuerung Digitalisierung“ gesteuert. Die Konzepte für das Digitallabor, die Digitalgalerie und das Zusammenwirken der Elemente befinden sich derzeit in der Erarbeitung.

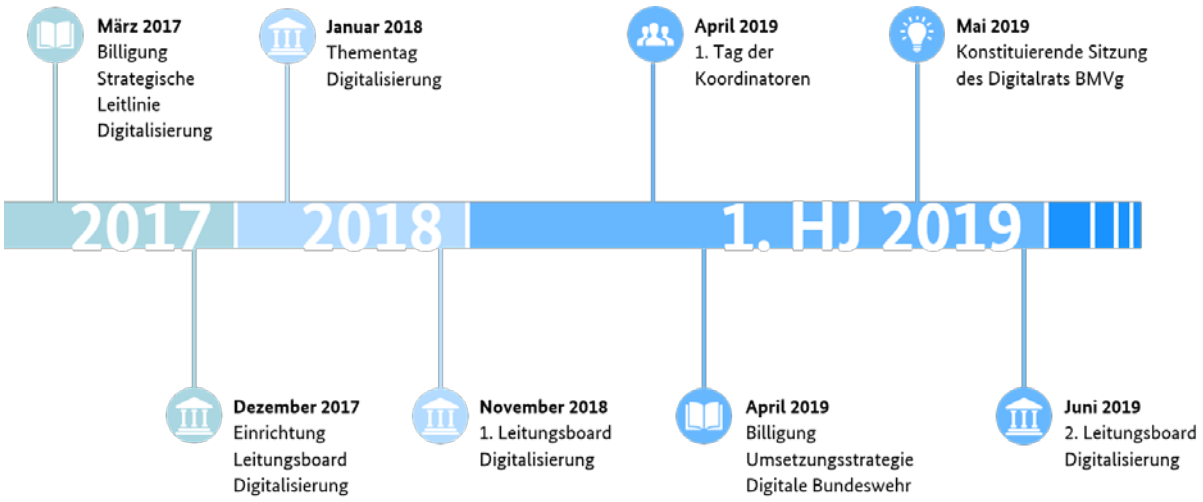


Abbildung 7: Überblick über bisherige Meilensteine der Digitalen Transformation des Geschäftsbereichs BMVg

5. Stand der Digitalen Transformation des Geschäftsbereichs BMVg

Digitalisierung findet im gesamten Geschäftsbereich BMVg in allen Facetten im täglichen Dienstbetrieb Berücksichtigung und durchdringt somit alle Organisationsbereiche und Planungskategorien. Eine klare Differenzierung einzelner Projekte oder Vorhaben nach Digitalisierung oder Nicht-

10 Digitalrat BMVg, Digitallabor und Digitalgalerie.

Digitalisierung ist demnach nicht möglich. Die „Umsetzungsstrategie Digitale Bundeswehr“ führt nur einen kleinen Ausschnitt einer Vielzahl an Vorhaben auf, die der fortschreitenden Digitalisierung des gesamten Geschäftsbereichs BMVg direkt oder indirekt dienen. Dies sind ausgewählte Digitalisierungsaktivitäten und Maßnahmen zur Erhöhung der Digitalisierungsfähigkeit, die von den ministeriellen Abteilungen und Stäben sowie den militärischen und zivilen Organisationsbereichen gemeldet wurden. Das Referat „Strategische Steuerung Digitalisierung“ schafft Transparenz über die Umsetzung der gemeldeten Vorhaben gegenüber der Leitung des BMVg.

5.1. Portfolio Digitalisierungsaktivitäten

Unter Digitalisierungsaktivitäten im Sinne der „Umsetzungsstrategie Digitale Bundeswehr“ werden Aktivitäten im Geschäftsbereich BMVg verstanden – von der Idee über die Planung und Realisierung bis hin zur Nutzung –, die durch den Einsatz von digitalen Technologien eine höhere Wirkung und/oder einen effizienteren Ressourceneinsatz anstreben.

Der Stand und Fortschritt derjenigen Digitalisierungsaktivitäten, die den IT-Programmen/-Projekten der Kategorie A[11] zugeordnet sind (namentlich „Harmonisierung der Führungsinformationssysteme“ (HaFIS) und „Digitalisierung landbasierter Operationen“ (D-LBO)), werden nach der für vergleichbare Rüstungsprojekte im Bericht des BMVg zu Rüstungsangelegenheiten regelmäßig dargelegten Methodik des Projektcontrollings und Risikomanagements nachgehalten. Andere Aktivitäten, einschließlich Ideen, werden in Anlehnung an diese Methodik durch Steckbriefe erfasst.

Das Portfolio der Digitalisierungsaktivitäten umfasst derzeit 74 gemeldete Vorhaben (Stichtag: 22. Mai 2019). Die Veränderung im Vergleich zum Stand der „Umsetzungsstrategie Digitale Bundeswehr“ erklärt sich durch die Dynamik und Weiterentwicklung im Rahmen der Digitalen Transformation des Geschäftsbereichs BMVg. Rund ein Fünftel der Vorhaben weist einen Ideenstatus auf (z.B. Entwicklung eines „digitalen Lagetisches“ für Operationsübungen an der Führungsakademie der Bundeswehr), während rund die Hälfte sich bereits in der Phase der Entwicklung, Beschaffung bzw. Realisierung befindet (vgl. Abbildung 8). Unter „Sonstiges“ werden Digitalisierungsaktivitäten u.a. aus den Bereichen „komplexe Dienstleistungen“ (z.B. Herkules Folgeprojekt) oder „Architekturen“ (z.B. Digitalisierung der Gesundheitsversorgung der Bundeswehr) zusammengefasst.

11 Die Zentrale Dienstvorschrift A-1500/3 „Customer Product Management“ (CPM) unterscheidet zwischen Projekten der Kategorien A bis D. Projekte, die der Kategorie A zugeordnet werden, stehen wegen ihrer besonderen Bedeutung im Fokus der Leitung des BMVg.

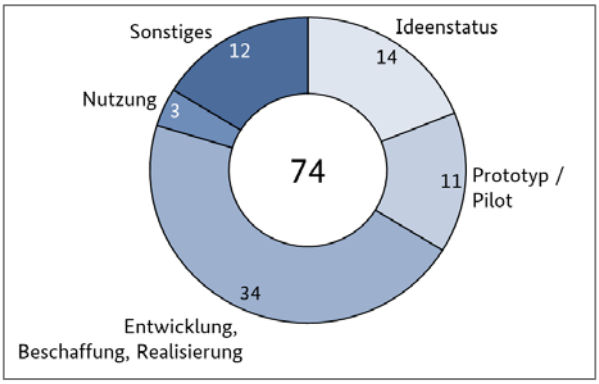


Abbildung 8: Umsetzungsstand der Digitalisierungsaktivitäten

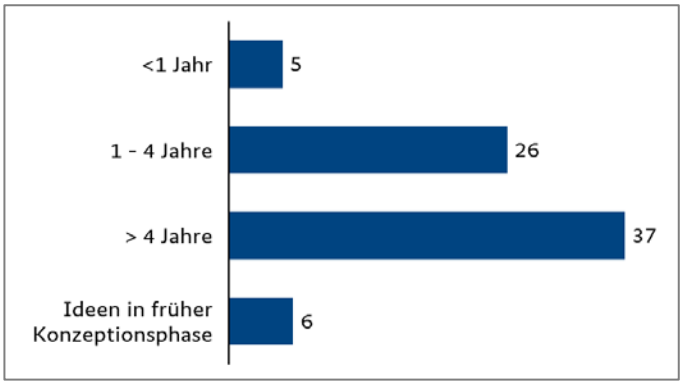


Abbildung 9: Umsetzungszeitraum der Digitalisierungsaktivitäten

Den schnellen Innovationszyklen digitaler Technologien steht bei einer Mehrzahl der gemeldeten Digitalisierungsaktivitäten ein Umsetzungszeitraum von mehr als vier Jahren gegenüber (vgl. Abbildung 9). Perspektivisch muss sich die Umsetzung aber stärker an die Dynamik und Agilität der technologischen Entwicklung anpassen. Dafür werden in einem Aufgabenpaket im Rahmen der Maßnahmen zur Erhöhung der Digitalisierungsfähigkeit die bestehenden Verfahren und Strukturen in den Bereichen Forschung, Entwicklung und Beschaffung geprüft und bewertet.

Beim 2. Leitungsboard Digitalisierung am 11. Juni 2019 wurde – neben anderen Digitalisierungsaktivitäten – die „Digitalisierung der Gesundheitsversorgung der Bundeswehr“ (GesVersBw) vorgestellt. Diese besitzt insbesondere wegen des konsequenten Architekturansatzes Beispielscharakter für die Digitale Transformation des Geschäftsbereichs BMVg.

Beispiel: Digitalisierung der Gesundheitsversorgung der Bundeswehr

Übergeordnetes Ziel der Digitalisierungsaktivität ist es, das Digitalisierungspotenzial für die GesVersBw systematisch zu erschließen und für die weitere Verbesserung in allen Bereichen der Patientenversorgung sowie zur Entlastung der Mitarbeiterinnen und Mitarbeiter des Sanitätsdienstes nutzbar zu machen.

Die Umsetzung erfolgt strukturiert auf der Grundlage der Prozess- und Architekturmodelle der GesVersBw, aus denen konkrete Digitalisierungsschritte abgeleitet werden. Auf diese Weise wurden z.B. bereits die Tele-Sonografie etabliert und eine Videosprechstunde pilotiert. Weitere geplante Projekte, wie geschlossenes Medikationsmanagement in den Bundeswehrkrankenhäusern, Anbindung derselben an die zivile Telematikinfrastruktur, Digitalisierung der truppenärztlichen Versorgung oder Teilhabe der Soldatinnen und Soldaten an der zivilen elektronischen Patientenakte passen sich in die strategische Gesamtforderungslage ein.

Die Digitalisierungsschritte folgen dem Ziel einer durchgehenden, prozessorientierten IT-Unterstützung der GesVersBw und fügen sich zur umfassenden Realisierung der elektronischen Gesundheitsakte der Bundeswehr (eGABw) zusammen. Konzeption und Einführung der eGABw machen den Sanitätsdienst der Bundeswehr zu einem Vorreiter in der digitalen Gesundheitsversorgung. Die rechtliche Grundlage dafür wurde mit dem Bundeswehr-Einsatzbereitschaftsstärkungsgesetz geschaffen.

Mit der Digitalisierung der GesVersBw wird der Grundgedanke der Realisierung verschiedener Digitalisierungsaktivitäten über eine Gesamtarchitektur erstmals umgesetzt. Dabei werden alle Einzelprojekte über die Architektur gesteuert und ihre wechselseitigen Abhängigkeiten transparent gemacht.

Von besonderer Bedeutung für die Digitalisierung der Streitkräfte sind auch die Programme **„Harmonisierung der Führungsinformationssysteme“ (HaFIS)** und **„Digitalisierung landbasierter Operationen“ (D-LBO)**. Beide Programme leisten u.a. einen wesentlichen Beitrag für die Fähigkeit zur Durchführung von nationalen und multinationalen Einsätzen sowie im Fall von **HaFIS** zum Nationalen Risiko- und Krisenmanagement zum Schutz deutscher Staatsangehöriger im Ausland (NatRKM). Durch die Einführung von **HaFIS** wird dem Erfordernis, harmonisierte und serviceorientierte Führungs- und Kommunikationssysteme sowie -verfahren bereitzustellen, umfassend Rechnung getragen. Mit **HaFIS** sollen georedundante, stationäre sowie verlegefähige Rechenzentren realisiert werden, die verschiedene Sicherheitsdomänen bereitstellen. HaFIS reduziert die Produktvielfalt, implementiert NATO-Applikationen und verbessert so die Führungsfähigkeit der Bundeswehr. Der Austausch von eingestuften Informationen kann so zwischen unterschiedlichen Nutzern bis auf die Ebene BMVg und bei Bedarf ressortübergreifend erfolgen und stellt somit die Kernführungsfähigkeit sicher.

Das Programm **D-LBO** schafft für die Streitkräfte einen in sich verzahnten Informations- und Kommunikationsverbund auf der mobilen taktischen Ebene und erhöht hierdurch die Interoperabilität. Es dient der Modernisierung der mobilen taktischen Kommunikation sowie der Informationsverarbeitung der Landstreitkräfte. Das Programm D-LBO / Tactical Edge Networking (TEN) beschreibt das binationale Vorgehen in enger Verzahnung mit den Niederlanden (NLD); es wird das übergeordnete Ziel der vollständigen und uneingeschränkten Interoperabilität der Landstreitkräfte beider Nationen im Bereich der vernetzten Operationsführung verfolgt, d.h. IT- Services werden vom Soldaten bis hin zur Ebene der verlegefähigen Gefechtsstände bereitgestellt.

Ein diesbezügliches DEU–NLD Memorandum of Understanding (MoU) wurde am 26. Juni 2019 durch beide Verteidigungsministerinnen gezeichnet.

Operatives Beispiel der Digitalen Transformation: Digitalisierung der Landstreitkräfte

Die Digitalisierung eröffnet neue Möglichkeiten der Operationsführung in zukünftigen Einsätzen der Bundeswehr und übt somit einen großen Einfluss auf die Landstreitkräfte aus. Abgeleitet aus der Analyse aktueller Entwicklungen und den Erfordernissen zukünftiger Gefechtsfelder, werden sich Landstreitkräfte der Zukunft auf ein neues – auf digitalen Technologien basierendes – Wirkmodell abstützen müssen. Kennzeichen des neuen Wirkmodells ist vor allem die schnellere und operativ skalierbare Wirkung von Landstreitkräften und die Fähigkeit zum präzisen Kampf, bei gleichzeitig größtmöglichem Schutz unserer Soldatinnen und Soldaten und der Bevölkerung.

Die Digitalisierung ermöglicht eine optimierte Kampfweise der Landstreitkräfte („verteiltes Operieren“). Das bedeutet, aus der streitkräfteübergreifenden weitreichenden Überwachung großer Räume kommend, durch Verknüpfung aller Sensoren in einem gemeinsamen Lagebild („gläsernes Gefechtsfeld“) und abgestützt auf eine umfassende Vernetzung aller Sensoren und Wirkmittel („Sensor to Shooter Konzept“), können digitalisierte Landstreitkräfte stets eine zeitgerechte und angemessene Gegenkonzentration streitkräfteübergreifend abrufen.

Mit anderen Worten: Die Digitalisierung ist eine Voraussetzung dafür, dass es den Landstreitkräften ermöglicht wird, mit dem gleichen Kräfteansatz von „heute“ ihre Aufträge von „morgen“ bzw. „übermorgen“ effizienter und effektiver erfüllen können.

Aktuell liegt der Schwerpunkt auf der Bereitstellung einer Lösung zur Digitalisierung der Führungsmittel für die „Very High Readiness Joint Task Force Land“ (VJTF (L)) 2023. Hier gilt es, vorhandene Insellösungen so miteinander zu verknüpfen, dass der Einstieg in die vertikal und horizontal durchgängige Digitalisierung der Landstreitkräfte gelingt. Dieses soll durch Beschaffung eines modernen taktischen Battle Management Systems (BMS) und entsprechender Anzeigegeräte für nahezu alle Waffensysteme und Fahrzeuge der VJTF (L) 2023 erreicht werden. Eine der Rahmen- bzw. Leadnation angemessene Führungsfähigkeit sowie Befähigung zur multinationalen Interoperabilität stehen dabei im Fokus. Unter Federführung des Heeres wurde gemeinsam mit dem Kommando Cyber- und Informationsraum, dem Kommando Streitkräftebasis, dem Zentralen Sanitätsdienst der Bundeswehr sowie dem Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr ein erstes digitales „TestBed“ („Test- und Versuchsstrukturen“) geschaffen und ein BMS erfolgreich getestet.

Auf Basis dieser Erfahrungen ist das übergeordnete und langfristige Ziel die stetige und explorative Digitalisierung der Landstreitkräfte in einem iterativen Prozess von abwechselnder Konzeptentwicklung und experimenteller Überprüfung auf operationellen Nutzen und Innovationspotenzial. In diesem Zusammenhang ist es notwendig, dass die digitalen Technologien und Werkzeuge – möglichst einsatznah – vor einer Beschaffung durch Soldatinnen und Soldaten getestet und erprobt werden. Wesentliche Elemente hierbei sind die „Test- und Versuchsstrukturen", der Aufbau eines bundeswehrgemeinsamen Systemzentrums „Digitalisierung Land" und die Einbindung des – in diesem Falle – niederländischen Partners, um die Interoperabilität in einem multinationalen Umfeld sicherstellen zu können.

Wie im **9. Bericht des Bundesministeriums der Verteidigung zu Rüstungsangelegenheiten vom Juni 2019** erwähnt, wird die Berichterstattung zu HaFIS und D-LBO künftig im Digitalbericht erfolgen. Da die Programme im vorgenannten Bericht im Detail vorgestellt wurden, wird in diesem Bericht aufgrund der zeitlichen Nähe der Veröffentlichungen auf eine Wiederholung verzichtet.

5.2. Maßnahmen zur Erhöhung der Digitalisierungsfähigkeit

Die Digitale Transformation des Geschäftsbereichs BMVg basiert zwar auf der Beschaffung und Nutzung moderner Technologien (vgl. Kap. 5.1), geht aber über diese weit hinaus. Die Chancen der Digitalisierung können nur dann vollständig ausgeschöpft werden, wenn die Digitalisierungspotenziale von Verfahren und Strukturen, die Befähigung von Personal, sowie eine digitale Kultur im Sinne eines strategischen Wandels gleichzeitig im gesamten Geschäftsbereich BMVg angegangen werden.

Hierzu beinhaltet die „Umsetzungsstrategie Digitale Bundeswehr" insgesamt 60 Aufträge zur Durchführung von Maßnahmen zur Erhöhung der Digitalisierungsfähigkeit an die ministeriellen Abteilungen und Stäbe und an die militärischen und zivilen Organisationsbereiche der Bundeswehr.[12] Stand und Fortschritt der Maßnahmen werden in Anlehnung an die Methodik des Projektcontrollings und Risikomanagements durch Steckbriefe erfasst. Zum Stichtag 22. Mai 2019 lagen 17 Steckbriefe für konkret geplante oder in Durchführung befindliche Maßnahmen vor. Ferner wurden sechs zusätzliche Maßnahmen in Form eines Steckbriefs gemeldet, die nicht in der „Umsetzungsstrategie Digitale Bundeswehr" enthalten sind. Damit erhöht sich das Portfolio auf insgesamt 66 Maßnahmen zur Erhöhung der Digitalisierungsfähigkeit. Von den 23 in Steckbriefen erfassten Maßnahmen befinden sich ca. 40% bereits in der Umsetzungsphase (z.B. Überprüfung und ggf. Anpassung bestehender Inhalte der IT-fachbezogenen Ausbildung) (vgl. Abbildung 10). Rund

12 Maßnahmen zur Erhöhung der Digitalisierungsfähigkeit sind: Verfahren, Strukturen, Kultur und Personal.

die Hälfte der Maßnahmen wirken übergreifend auf mehrere Bereiche der Digitalisierungsfähigkeit ein (vgl. Abbildung 11). Insgesamt steht der Geschäftsbereich BMVg bei der Umsetzung der Maßnahmen zur Erhöhung der Digitalisierungsfähig eher am Anfang.

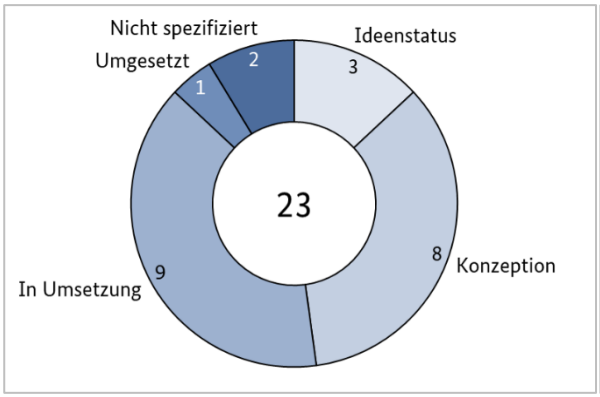


Abbildung 10: Umsetzungsstand Maßnahmen zur Erhöhung der Digitalisierungsfähigkeit

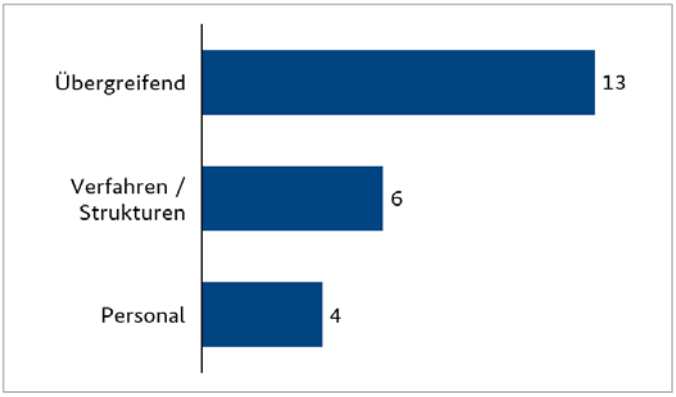


Abbildung 11: Wirkebene der Maßnahmen zur Erhöhung der Digitalisierungsfähigkeit

Eine besondere Herausforderung stellt die alle Organisationsbereiche übergreifende **Personalgewinnung und -bindung im Fachbereich IT** dar, insbesondere in der Konkurrenz zu anderen attraktiven Arbeitgebern. Beispielhaft stellt sich der Dienstpostenbesetzungsgrad bei IT-relevantem Fachpersonal für den Organisationsbereich Cyber- und Informationsraum mit Stand vom 31. März 2019 über die militärischen und zivilen Laufbahngruppen ab IT-Feldwebeln bzw. dem mittleren Dienst aufwärts wie folgt dar:

Laufbahn	Stabsoffiziere	Offiziere Truppendienst	Offiziere militärfachlicher Dienst	Feldwebel allg. Fachdienst	Beamte höherer Dienst	Beamte gehobener Dienst	Beamte mittlerer Dienst
Besetzungsgrad	84 %	77 %	79 %	65 %	77 %	70 %	82 %

Tabelle 1: Dienstpostenbesetzungsgrad der Laufbahngruppen im Organisationsbereich Cyber- und Informationsraum

Im engen Zusammenwirken mit den Bedarfsträgern wurden bereits vielfältige, teilweise ineinandergreifende Ansätze entwickelt, um die personelle Bedarfsdeckung **IT-Personal** zu verbessern. Die Einführung von IT-relevanten Zulagen, die Gewährung von Personalbindungsprämien, die Entfrachtung von Werdegängen und die Erhöhung der Einstellungsumfänge sind nur einige dieser Maßnahmen. Allerdings wirken sich kurzfristig erhöhte Einstellungsumfänge in den militärischen Laufbahnen i.d.R. nicht *ad hoc* auf die Dienstpostenbesetzung und die Einsatzbereitschaft aus, da

mehrjährige Ausbildungszeiten zu berücksichtigen sind. Hier ist prognostisch eine verbesserte Besetzungslage bei militärischem Personal zu erwarten. So wird sich der Dienstposten-Besetzungsgrad bei den IT-Feldwebeln im militärischen Organisationsbereich Cyber und Informationsraum auf ca. 83% erhöhen. Vergleichbar wird für die in Rede stehenden zivilen Laufbahnen kurz- und mittelfristig eine entsprechende Verbesserung der Personalbedarfsdeckung angestrebt, z.B. über den beruflichen Direkteinstieg von fachlich qualifiziertem Personal ohne allgemeine Laufbahnanteile beginnend zum 1. Oktober 2019. Darüber hinaus beabsichtigt das Kdo CIR in Zusammenwirkung mit dem Bundesamt für das Personalmanagement der Bundeswehr mittelfristig mit einem „**Cyber/IT Evaluation Center**" (CITEC) eine Stelle einzurichten, an der hochqualifiziertes Fachpersonal gezielt angesprochen und geprüft werden soll, um mittels innovativer Testverfahren deren fachliche Qualifikationen für Verwendungen im Cyber/IT-Dienst der Bundeswehr festzustellen und zu validieren. Zukünftige Verfahren einschließlich Möglichkeiten eines Einstiegs von Personen mit non-formalen Kompetenzen in eine Fachkarriere werden derzeit untersucht. In 2019 wird zunächst in einer Pilotphase Bestandspersonal getestet. Durch ergänzende Etablierung einer attraktiven Fachkarriere können die auf diese Weise gewonnenen IT-Experten langfristig an die Bundeswehr gebunden werden.

Neben der rein quantitativen Ausstattung mit personellen Ressourcen ist die Qualifizierung der Beschäftigten im Hinblick auf **„digitale Kompetenzen“** für die Digitale Transformation des Geschäftsbereichs entscheidend. Konzepte und Maßnahmen zur Stärkung dieser Kompetenzen befinden sich derzeit in Erarbeitung.

Die Digitalisierung stellt einen gesellschaftlichen Wandel dar, der auch das **Dienst- und Arbeitsumfeld** der Angehörigen des Geschäftsbereichs BMVg grundlegend verändern wird. Ein wesentlicher Aspekt der Digitalisierung ist daher die Förderung und Stärkung einer Digitalkultur. Eingeleitete Maßnahmen im Geschäftsbereich BMVg zur Förderung eines „digitalen Selbstverständnisses“ wie Informationsveranstaltungen, Qualifizierungsmaßnahmen oder das Einrichten von Informationsmöglichkeiten für Mitarbeiter und Mitarbeiterinnen mittels kooperativer Formate, wie z.B. der Bundeswehr Wiki-Plattform und des Prozessportals, zeigen erste Wirkung. Sie fördern die Transparenz, binden Nutzer eng in den Prozess ein und bieten so die Möglichkeit, Ideen, konstruktive Rückmeldungen, Erwartungen und natürlich auch Sorgen und Herausforderungen jedes Einzelnen in den Veränderungsprozess einzubringen.

Das Referat „Strategische Steuerung Digitalisierung“ entwickelt eine übergreifende Anleitung zur **Förderung und Stärkung der Digitalkultur** und eines **„digitalen Selbstverständnisses“** für alle

Bereiche des Geschäftsbereichs BMVg. Hierzu ist ein Konzept zum Veränderungsmanagement Digitalisierung sowie zur Digitalkultur in Erarbeitung, die im Sinne einer dezentralen Umsetzung allen ministeriellen Abteilungen und Stäben sowie allen militärischen und zivilen Bereichen der Bundeswehr zur Verfügung gestellt werden. Erste Ergebnisse werden noch in 2019 erwartet.

Greifbarer ist der Bereich der Anpassung von Verfahren und Strukturen an die Anforderungen der technologischen Entwicklung und Innovation. Die „Umsetzungsstrategie Digitale Bundeswehr" enthält mehrere Aufträge in Bezug auf die Prüfung und Bewertung einer möglichen Beschleunigung bestehender Verfahren und Strukturen in den Bereichen Forschung, Entwicklung und Beschaffung. Beim 2. Leitungsboard Digitalisierung am 11. Juni 2019 wurde ein erster „Vorschlag der Abteilung CIT zur beschleunigten Einführung von IT-Innovationen" eingebracht, der geprüft wird.

5.3. Innovationsthema künstliche Intelligenz

Die Digitale Transformation des Geschäftsbereichs BMVg lebt auch von einer schnellen Adaption von Innovationen. Eines der für den Geschäftsbereich bedeutsamen Innovationsthemen ist die Entwicklung und Nutzung künstlicher Intelligenz (KI).

Besonders die verschiedenen, auf maschinellem Lernen basierenden Anwendungen schwacher KI bieten in den Bereichen einen Vorteil, bei denen große Datenmengen ausgewertet und zu Empfehlungen für menschliche Entscheider verdichtet werden können. Für die Bundeswehr wird KI einen wichtigen Beitrag zur Erfüllung des Auftrages leisten. Dies gilt speziell dort, wo KI zur Steigerung der Effektivität oder Effizienz in der Auftragserfüllung beiträgt sowie dort, wo sie das militärische und zivile Personal von unterstützenden und administrativen Aufgaben entlastet.

In den absehbaren Einsatzmöglichkeiten ist KI aber keine universelle Lösung für jede Problemstellung. Vielmehr müssen diese Systeme auf eine spezifische Einsatzmöglichkeit hin entwickelt und trainiert werden. Voraussetzung ist dabei der Zugang zu großen Datenmengen, die Automatisierung von Prozessen sowie ein Human-Machine-Interface, um eine wechselseitige Kommunikation zwischen Mensch und KI zu ermöglichen. Die Zukunft von KI in den Streitkräften liegt dabei nicht in der Entscheidung Mensch oder KI, sondern in einer effektiven und skalierbaren Kombination von Mensch und KI, um eine bestmögliche Aufgabenerfüllung zu gewährleisten.

Bezüglich der Thematik der letalen autonomen Waffensysteme ist es zum Erhalt einer umfassenden Bewertungsfähigkeit erforderlich, sich weiter mit allen Aspekten einer möglichen militärischen Anwendung und den damit verbundenen Auswirkungen zu befassen. Dies gilt insbesondere für die

Aspekte möglicher Gegenmaßnahmen sowie des Schutzes der Soldatinnen und Soldaten der Bundeswehr in künftigen Einsatzszenarien. Die Bundeswehr verfügt über keine letalen autonomen Waffensysteme und beabsichtigt auch nicht deren Einführung.

Beim 2. Leitungsboard Digitalisierung am 11. Juni 2019 wurde die Digitalisierungsaktivität „Gemeinsames Lagezentrum Cyber- und Informationsraum“ (GLZ CIR) als ein Beispiel der Anwendung von KI vorgestellt.

Beispiel: Gemeinsames Lagezentrum Cyber- und Informationsraum

Das GLZ CIR dient der Lagefeststellung und Operationsführung im Cyber- und Informationsraum. Unterschiedlichste Lagen aus dem gesamten Cyber- und Informationsraum werden korreliert und bewertet. Daraus werden individuelle Informationsprodukte – zugeschnitten auf spezifische Bedarfsträger – im Geschäftsbereich BMVg und auch außerhalb des Ressorts bereitgestellt. So stellt das GLZ CIR zukünftig z.B. dem nationalen Cyber-Abwehrzentrum beim Bundesamt für Sicherheit in der Informationstechnik die Lage der Bundeswehr im Cyber- und Informationsraum zur Verfügung.

Zugleich stehen im GLZ CIR die erforderlichen Informationen zur Erarbeitung von Handlungsoptionen für militärische Operationen im Cyber- und Informationsraum bereit. Zur Erstellung der Lage ist die Analyse einer Vielzahl ständig eingehender, strukturierter und unstrukturierter Daten notwendig. Hier kommen auch Methoden der „künstlichen Intelligenz“ und „Big Data“ zur Anwendung. Um beispielsweise fremdsprachige öffentliche Informationen zum Cyber- und Informationsraum analysieren zu können, werden diese im GLZ CIR mittels Unterstützung durch KI automatisch übersetzt. Diese Art der Übersetzung liefert bessere Übersetzungsergebnisse, als die bisher übliche phrasenbasierte statistische Übersetzung, bei der einzelne Satzelemente wörtlich übersetzt werden.

Intelligente und automatisierte Systeme sind die Basis zukünftiger Führungs-, Informations- und Wirkungsüberlegenheit. Die Menge der zur Verfügung stehenden Informationen kann weder vom Umfang noch in einer akzeptablen Zeit durch Analysten ausgewertet werden. Der Einsatz automatisierter Verfahren ist unerlässlich. Durch die Ablösung analoger Prozessschritte sowie die Einführung neuer digitaler Arbeitsabläufe schafft es das GLZ CIR, die Chancen der Digitalisierung gewinnbringend zu nutzen.

6. Ausblick

In der derzeitigen Phase der „**Roadmap Digitale Bundeswehr“** steht der Fokus der Digitalen Transformation des Geschäftsbereichs BMVg bis Ende 2020 unter der Überschrift „Umsetzen, Systematisieren und Ausprobieren“ (vgl. Kap. 5).

In diesem Zusammenhang stehen folgende kurz- bis mittelfristige Vorhaben im Fokus:

- Stärkung der strategischen Steuerung Digitalisierung durch Aufbau eines hierfür zuständigen Fachreferates und das Nachhalten der Aufträge aus der „Umsetzungsstrategie Digitale Bundeswehr“,
- Aufbau einer Digitalisierungsplattform beginnend mit der Umgliederung innerhalb der Abteilung CIT,
- Erstellung der Konzepte für den Aufbau eines Digitallabors und einer Digitalgalerie sowie für das Zusammenwirken der Elemente des Digitalen Campus,
- Fortführung der Test- und Versuchsstrukturen, Exprimentierfähigkeit und Erarbeitung der Grundlagen zum Aufbau eines bundeswehr- und streitkräftegemeinsamen „Systemzentrums Digitalisierung Land“ am Standort Munster,
- Stärkung des Projektcontrollings und des Risikomanagements von Digitalisierungsaktivitäten und Maßnahmen zur Erhöhung der Digitalisierungsfähigkeit in Anlehnung an das Leitungsboard Rüstung,
- Zweite Sitzung des Digitalrates BMVg, um die strategischen Ansätze der Digitalen Transformation der Bundeswehr zu analysieren.

Die in der „Umsetzungsstrategie Digitale Bundeswehr“ definierten Steuerungsinstrumente werden weiter etabliert. So finden im 2. Halbjahr 2019 neben dem dritten Leitungsboard Digitalisierung auch der zweite Tag der Koordinatoren sowie die zweite Sitzung des Digitalrats statt. Die Herausgabe des zweiten Digitalberichts BMVg ist für das erste Quartal 2020 geplant.

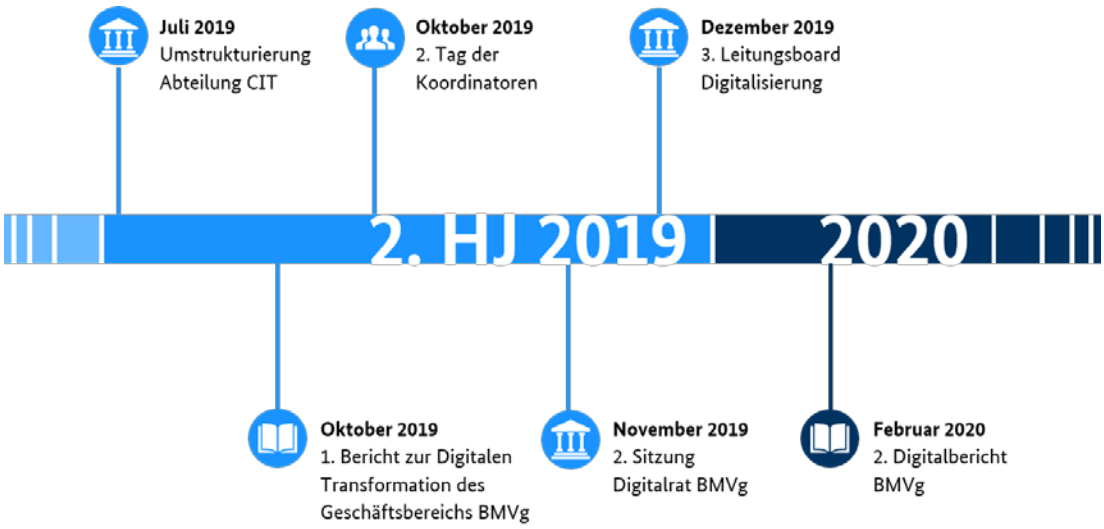


Abbildung 12: Überblick über zukünftige Meilensteine der Digitalen Transformation des Geschäftsbereichs BMVg

Abbildungsverzeichnis

Abbildung 1: Schwerpunktvorhaben BMVg in der Umsetzungsstrategie der Bundesregierung „Digitalisierung gestalten“ vom März 2019 5

Abbildung 2: Roadmap Digitale Bundeswehr, „Umsetzungsstrategie Digitale Bundeswehr“ 9

Abbildung 3: Organigramm BMVg CIT bis 1. Juli 2019 10

Abbildung 4: Organigramm BMVg CIT seit 1. Juli 2019 10

Abbildung 5: Matrixorganisation Abteilung Cyber/Informationstechnik (CIT) 11

Abbildung 6: Vorgehensmodell der Digitalen Transformation des Geschäftsbereichs BMVg 14

Abbildung 7: Überblick über bisherige Meilensteine der Digitalen Transformation des Geschäftsbereichs BMVg 19

Abbildung 8: Umsetzungsstand der Digitalisierungsaktivitäten 21

Abbildung 9: Umsetzungszeitraum der Digitalisierungsaktivitäten 21

Abbildung 10: Umsetzungsstand Maßnahmen zur Erhöhung der Digitalisierungsfähigkeit 25

Abbildung 11: Wirkebene der Maßnahmen zur Erhöhung der Digitalisierungsfähigkeit 25

Abbildung 12: Überblick über zukünftige Meilensteine der Digitalen Transformation des Geschäftsbereichs BMVg 30

Tabellenverzeichnis

Tabelle 1: Dienstpostenbesetzungsgrad der Laufbahngruppen im Organisationsbereich Cyber- und Informationsraum 25

Impressum

Herausgeber

Bundesministerium der Verteidigung

Stauffenbergstraße 18

10785 Berlin

Redaktionsschuss

25. September 2019

Herausgabe

Oktober 2019

Gestaltung

Bundesministerium der Verteidigung

Bildnachweis

Titelbild: Bundeswehr / Roland Alpers

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