Bundesministerium der Verteidigung

Strategisch-politisches Dokument

Strategische Leitlinie Digitalisierung

Zweck des Dokumentes:	Die konsequente Umsetzung der Digitalisierung ist eine Aufgabe für den gesamten Geschäftsbereich des Bundesministeriums der Verteidigung, über alle Führungsebenen hinweg, die über den Bereich der Technik hinausgeht und sowohl Organisation und Prozesse als auch militärische Fähigkeiten beeinflussen wird.
Herausgegeben durch:	Bundesministerium der Verteidigung
Gebilligt durch:	Bundesministerin der Verteidigung
Herausgebende Stelle:	BMVg CIT I 1
Geltungsbereich:	Geschäftsbereich des Bundesministeriums der Verteidigung
Einstufung:	Offen
Gültig ab:	31.03.2017
Frist zur Überprüfung:	31.12.2020
Version:	1
Ersetzt:	Entfällt
Aktenzeichen:	62-00-00

Inhaltsverzeichnis

1 Vorbemerkung

„Die Digitalisierung des GB BMVg ist mehr als nur die Umsetzung von IT-Projekten, sie wird einen Mehrwert für die Organisation und den einzelnen Nutzer erzielen!“

101. Die Digitalisierung ist in nahezu allen Bereichen des Lebens angekommen und treibt Veränderungsprozesse mit rasanter Geschwindigkeit voran. Digitalisierung ist zum Motor der Transformation zu einer „Digitalen Gesellschaft“ geworden. Informationstechnik (IT) ist dabei sowohl ein Werkzeug, um Prozesse zu unterstützen und innovative Geschäftsmodelle zu entwerfen, als auch Abläufe und Organisationsformen einschließlich der dazugehörigen Kultur zu ermöglichen, neu zu gestalten und dadurch einen Mehrwert für die Organisation zu erzielen. Auf Informationen kann zunehmend ortsunabhängig, mobil und nahezu in Echtzeit zugegriffen werden. Reale und virtuelle Welt rücken immer näher zusammen und erreichen einen immer höheren Grad der digitalen Vernetzung. Damit eröffnen sich ungeahnte Chancen für Gesellschaft und Staat. Neue Möglichkeiten der Kommunikation, des Zugangs zu Wissen und der innovativen Gestaltung von Zusammenarbeit in allen Bereichen führen zu völlig neuen Modellen sozialer Interaktion und Betätigungsfeldern für Forschung und Entwicklung.

102. Digitalisierung birgt jedoch auch Risiken. Verwundbarkeiten einer weitestgehend digitalisierten staatlichen Organisation und des gesellschaftlichen Umfeldes bieten Angriffspunkte für staatlich gesteuerte sowie hybride Bedrohungen. Cyberattacken gehören bereits heute zum Alltag. Die Sicherheit im Umgang mit IT und die Nutzung des Cyber- und Informationsraumes werden mehr und mehr zu einer strategischen Herausforderung. Dies betrifft sowohl die Härtung von Systemen nach dem vorhandenen Stand der Technik als auch die Schaffung aktiver Verteidigungselemente (bspw. durch Nutzung von Sicherheitsinformations- und Ereignis-Management Systemen (SIEMS) und von Security Operation Centres (SOC)). Innere und äußere Sicherheit lassen sich nicht mehr trennscharf voneinander abgrenzen. Vielmehr stehen sich die gegenseitigen Interessen konkurrierend gegenüber: auf der einen Seite die Forderung nach immer tiefgreifenderer Vernetzung und auf der anderen Seite die Sicherung der eigenen IT-Infrastruktur. Cyber-Sicherheit und Cyber-Verteidigung sind damit zu einer strategischen Aufgabe der gesamtstaatlichen Sicherheitsvorsorge geworden.

103. Der sich stetig beschleunigende technische Fortschritt im Bereich der IT mit raschen Innovationszyklen erfordert auch für den Geschäftsbereich des Bundesministeriums der Verteidigung (GB BMVg) klare eigene Wege im Erkennen, Beschaffen und Einführen von Neuerungen. Kompetenz im Bereich des Aufbaus einer flexiblen und sicheren IT-Architektur aus IT-Infrastruktur und darüber zur Verfügung gestellten IT-Services gewinnt an Bedeutung und ist entscheidend dafür, Zukunftsperspektiven zu gestalten und zu beherrschen.

104. Das BMVg hat auf diese Herausforderung reagiert. Die Verantwortlichkeiten für die Themen Cyber- und Informationstechnik sind durch die Aufstellung der Abteilung Cyber/IT (CIT) im BMVg im Oktober 2016 unter Leitung eines Ressort CIO gebündelt worden. Sie werden über die Leistungsprozesse „Cyber-/IT-Governance gewährleisten“ und „IT-Services bereitstellen“ im GB BMVg präzisiert und durch den Abteilungsleiter bzw. die Abteilungsleiterin CIT als Prozesseigner bzw. Prozesseignerin verantwortet. Neben der neuen ministeriellen Abteilung ist ein neuer militärischer Organisationsbereich mit einem Kommando Cyber- und Informationsraum (KdoCIR) eingerichtet worden, der mit einem Inspekteur bzw. einer Inspekteurin an der Spitze einen eigenständigen Beitrag zur „Operationsführung“ im Cyber- und Informationsraum leisten wird. Mit dem Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAAINBw) als zentralem Bedarfsdecker auch für IT-Produkte und IT-Dienstleistungen sowie der von der Präsidentin bzw. vom Präsidenten des BAAINBw wahrgenommenen Materialverantwortung für die Einsatzreife auch für IT-Produkte ist zudem die Basis für eine einheitliche, standardisierte Beschaffung und Bereitstellung innovativer Lösungen, bei gleichzeitiger Berücksichtigung der bereits etablierten IT, für den GB BMVg gegeben. Darüber hinaus steht mit der BWI Informationstechnik GmbH (BWI IT) eine Inhouse-Gesellschaft als leistungsstarker Partner und Provider mit Best Practice Ansätzen zur Verfügung.

105. Die Strategischen Leitlinie Digitalisierung (StratLL Digitalisierung) im GB BMVg zeigt auf, wie das hohe Innovationstempo und die querschnittliche Bedeutung der IT aufgenommen und mit den Erfordernissen und Rahmenbedingungen im GB BMVg in Einklang gebracht und wirksam für die Weiterentwicklung sowie für den Markenkern „Einsatz“ genutzt werden kann.

106. Wesentliche Elemente der Digitalisierung sind das Erkennen, die Einsteuerung und das Management von IT-Innovationen, die eine zielgerichtete Weiterentwicklung der Bundeswehr ermöglichen. Um solche Innovationen zu erkennen, zu fördern und gezielt für die Weiterentwicklung der Fähigkeiten der Bundeswehr nutzbar zu machen, müssen neue Kooperationsmöglichkeiten und Partnerschaften mit der Wirtschaft erschlossen werden. Eine Abkopplung von Innovationen gefährdet die Zukunftsfähigkeit der Bundeswehr.

Die Digitalisierung als Querschnittsaufgabe wird den GB BMVg mit zunehmender Geschwindigkeit weiter verändern. Die Maßnahmen zur Digitalisierung sind kein Selbstzweck und mehr als nur bloße Beschaffung und Nutzung von Technologie. Um die Chancen der Digitalisierung im gesamten (Fähigkeits-)Spektrum nutzen und die Risiken minimieren zu können, bedarf es eines Paradigmenwechsels. Dies ist ein Prozess, der mit weit reichenden Anpassungen verbunden sein wird. Digitalisierung ist nicht nur isolierte Aufgabe einer einzelnen Abteilung im BMVg, sondern muss auf allen Ebenen und in allen Bereichen der Bundeswehr durchgängig mitgedacht und gelebt werden – beginnend bei der Leitung, über alle militärischen und zivilen Führungsebenen hinweg bis hin zu jeder Mitarbeiterin und jedem Mitarbeiter. Digitalisierung ist damit mehr als nur eine Frage der Technologie – es geht um die Änderung der Denk- und Handlungsweise, um das „Digitale Selbstverständnis der Bundeswehr“.

2 Strategischer Kontext

201. Die Digitalisierung im GB BMVg ist unter Berücksichtigung von Vorgaben aus übergeordneten strategischen Dokumenten zu gestalten.

202. Das **Weißbuch zur Sicherheitspolitik Deutschlands und zur Zukunft der Bundeswehr** ist das oberste sicherheitspolitische Grundlagendokument Deutschlands und verlangt konkret den Ausbau von Fähigkeiten insbesondere zur Konsolidierung und Härtung der Sicherheitsarchitektur des IT-Systems der Bundeswehr (IT-SysBw) mit dem Ziel einer gestärkten Resilienz. Multinationalität bleibt leitendes Prinzip der Fähigkeitsentwicklung der Bundeswehr.

203. Ergänzend gibt die **Strategische Leitlinie Cyber-Verteidigung** Handlungsfelder zur Entwicklung und Umsetzung von Grundsätzen für die Cyber-Verteidigung der Bundeswehr vor. Die Konzeption der Bundeswehr und das Fähigkeitsprofil der Bundeswehr detaillieren und konkretisieren die Fähigkeitsbeiträge im Cyber- und Informationsraum.

204. Die **Digitale Agenda der Bundesregierung** gibt die Leitlinien der Digitalpolitik der Bundesregierung vor und bündelt Maßnahmen auf zentralen Handlungsfeldern. Mit der Umsetzung der Digitalen Agenda sollen die Chancen der Digitalisierung genutzt werden, Deutschlands Rolle als innovative und leistungsstarke Volkswirtschaft in der Europäischen Union und der Welt auszubauen.

205. Das **Regierungsprogramm Digitale Verwaltung** schafft die Rahmenbedingungen für die Verwaltung der Zukunft. Diese nutzt die Potenziale der Digitalisierung, ist effektiv, transparent, effizient, barrierefrei sowie bürger- und unternehmensfreundlich. Die Agilität der Verwaltung, aber auch die Finanzierbarkeit der notwendigen Maßnahmen und die Informationssicherheit des Bundes sollen langfristig gesichert werden.

206. Für die IT-Steuerung und IT-Konsolidierung des Bundes werden die übergreifenden Ziele und Handlungsfelder in der **IT-Strategie der Bundesverwaltung** definiert. Diese umfassen Konsolidierung, Standardisierung, Nachfragebündelung, Digitalisierung, Förderung von Innovationen, Erhöhung der Informationssicherheit, Aufbau und Entwicklung von IT-Personal und Ausbau der IT-Steuerung des Bundes.

207. Mit Kabinettbeschluss vom 20. Mai 2015 zur „**IT-Konsolidierung Bund**“ wurde die IT-Steuerung des Bundes hinsichtlich einer effizienteren Steuerungsstruktur angepasst. Die gemeinsamen Ziele der bzw. des Beauftragten der Bundesregierung für Informationstechnik und der vorhandenen IT-Gremien (IT-Rat/Konferenz der IT-Beauftragten der Ressorts) sind es, die Informationssicherheit vor dem Hintergrund steigender Komplexität zu gewährleisten, die Hoheit und Kontrollfähigkeit über die eigene IT dauerhaft zu erhalten, auf innovative technologische Trends flexibel reagieren zu können, einen leistungsfähigen, wirtschaftlichen, stabilen und zukunftsfähigen Betrieb sicherzustellen und ein attraktiver Arbeitgeber für IT-Fachpersonal zu bleiben. Die Daten der Bundesverwaltung sollen umfassend geschützt und gegen Missbrauch gesichert werden.

208. Die **Cyber-Sicherheitsstrategie für Deutschland 2016** bildet den ressortübergreifenden strategischen Rahmen und schreibt die Cyber-Sicherheitsstrategie aus dem Jahr 2011 fort. Ihr Anspruch, die Gewährleistung der Handlungsfähigkeit und Souveränität Deutschlands im Zeitalter der Digitalisierung zu gewährleisten, 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 die aktive Positionierung Deutschlands in der europäischen und internationalen Cyber-Sicherheitspolitik erreicht werden.

209. Die in der Erstellung befindliche **Konzeption der Bundeswehr** 2017 und das Fähigkeitsprofil der Bundeswehr 2017 detaillieren und konkretisieren die Fähigkeitsbeiträge im Cyber- und Informationsraum.

210. Die **IT-Strategie für den Geschäftsbereich BMVg** beschreibt als Fachstrategie und übergreifende konzeptionelle Grundlage die Fähigkeitsentwicklung zur optimalen IT-Unterstützung aller Prozesse im GB BMVg, u. a. durch Vorgaben zum Zielbild der Systemarchitektur des IT-SysBw, und setzt einen Rahmen für die Ausgestaltung und die Ausrichtung der IT des Verteidigungsressorts mit besonderem Blick auf dessen Einsatzorientierung.

211. In konsequenter Umsetzung der technologischen Entwicklungen und in Reaktion auf die Gefährdungen im und durch den Cyberraum wurden 2016 im Rahmen des NATO-Gipfels in Warschau umfassende Maßnahmen zur Stärkung der gemeinsamen Verteidigungsfähigkeit beschlossen (Cyber Defence Pledge) und der Cyberraum als eigenständiger Operationsraum bestätigt. Die Weiterentwicklung der Fähigkeiten der NATO wird in der **Roadmap for the Implementation of Cyberspace as a Domain of Operations** beschrieben.

212. Diese **Strategische Leitlinie ergänzt** die politisch-strategischen Ziele um Aspekte der Digitalisierung für das Verteidigungsressort. Sie bildet damit den Startpunkt eines mittel- bis langfristigen Migrationsprozesses zur Ausgestaltung eines durchgängigen digitalen Fähigkeitsspektrums im GB BMVg.

3 Ziele der Digitalisierung

- Die strategischen Rahmenbedingungen für die Digitalisierung im GB BMVg weisen Gemeinsamkeiten mit anderen Ressorts des Bundes hinsichtlich der Modernisierung im Rahmen der Digitalen Verwaltung und der IT-Konsolidierung des Bundes auf.
- Die hohe und weiter zunehmende Bedeutung IT-gestützter, standardisierter und automatisierter Abläufe sowie mobiler Arbeitsverfahren als elementare Bestandteile zur digitalen Abbildung komplexer Verwaltungsprozesse und Aufgaben erfordert eine Anpassung der Planungs-, Beschaffungs- und Betriebsprozesse für IT und die Bereitstellung anforderungsgerechter, nutzerorientierter IT-Services zur effizienten Umsetzung.
- Alleinstellungsmerkmal und Markenkern des GB BMVg sind jedoch die Aufstellung und der Einsatz von Streitkräften. Einsatzorientierung, Bundeswehrgemeinsamkeit und Bündnisorientierung einschließlich der Option, als Rahmennation in multinationalen Einsätzen wirken zu können, sind folglich in besonderem Maße prägend für die Zielsetzung der Digitalisierung der Bundeswehr.
- Voraussetzung für die Befähigung der Bundeswehr zur Vernetzten Operationsführung (NetOpFü) ist ein durchgängiger und leistungsfähiger Informations- und Kommunikationsverbund. Dazu ist die Bereitstellung der erforderlichen IT-Services sowie die Anbindung und Vernetzung der relevanten Dienststellen im In- und Ausland, der stationären und verlegefähigen Einrichtungen sowie der mobilen Elemente in den Einsatzgebieten nach standardisierten Verfahren sicherzustellen.
- Ziel ist es, auf Grundlage eines Bundeswehrgemeinsamen digitalen Lagebildes Informationsüberlegenheit als Grundlage für Führungsüberlegenheit durch bessere und schnellere Planungs- und Führungsprozesse zu ermöglichen und mithilfe echtzeitgesteuerter Datenanalyse letztendlich zur Wirkungsüberlegenheit beizutragen.
- Die Bereitstellung eines digitalen sowie bedarfsorientiert mobilen Arbeitsplatzes mit modernen Formen der Kommunikation und Kollaboration sowie des endgeräteunabhängigen Zugriffs auf alle relevanten Informationen gehört heute zu einem zeitgemäßen Arbeitsumfeld.

4 Ebenen und Anwendungsfelder der Digitalisierung

4.1 Ebenen

401. Im Fokus der Leistungsfähigkeit des IT-SysBw steht die Einsatzorientierung als Kernauftrag der Bundeswehr. Heutige und zukünftige Einsätze sowie der Grundbetrieb erfordern ein IT-SysBw, das

- die Einsatzfähigkeit und Einsatzbereitschaft in stationären, verlegefähigen und mobilen Einheiten gewährleistet,
- durchgängig, belastbar, skalierbar, nutzerorientiert, sicher, zuverlässig und flexibel in nahezu Echtzeit und bei Bedarf in Teilen autark betrieben werden kann und
- spezielle Fähigkeiten verzugslos integrieren kann und dabei Aspekte wie die Übernahme der Verantwortung als Rahmennation und Anpassungsfähigkeit im multinationalen Rahmen sowie mit Blick auf staatliche und nicht staatliche Organisationen sowie weitere Partnern unterstützt.

402. Die Digitalisierung im GB BMVg und der durchgängige und leistungsfähige Informations- und Kommunikationsverbund sind auf drei aufeinander aufbauenden Ebenen aktiv zu gestalten:

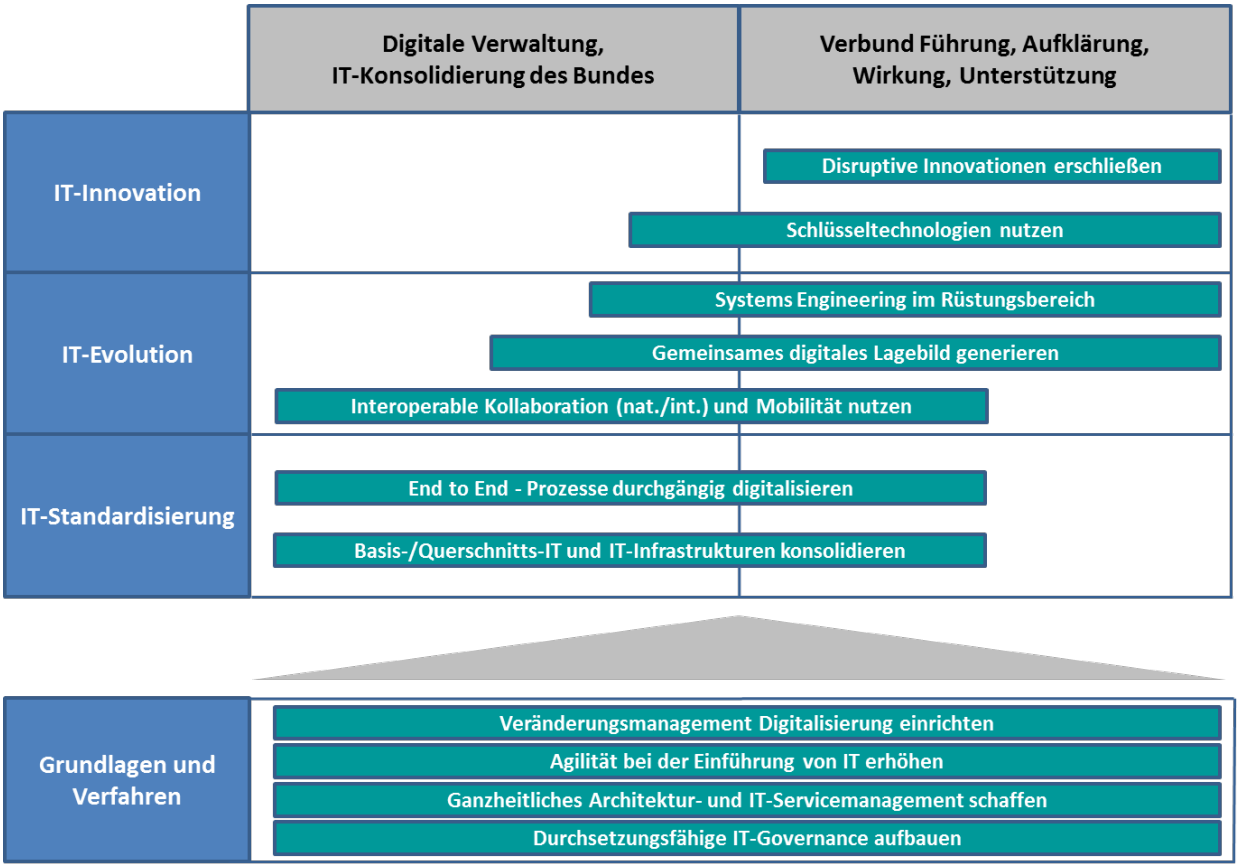

Abb. 1: Wesentliche Anwendungsfelder im Fokus der Digitalisierung

IT-Innovation erschließt Neuerungen und Schlüsseltechnologien, um dem GB BMVg mit der zeitnahen Einführung digitaler Technologien zu einem Vorsprung im Einsatz und letztendlich auch im Grundbetrieb zu verhelfen und diesen zu erhalten.

IT-Evolution baut die bestehenden IT-Services weiter aus mit dem Ziel, technologische Fortschritte zu nutzen, die Interoperabilität zu erhöhen und die IT-Steuerung effizient auszugestalten.

IT-Standardisierung schafft modular aufgebaute, deterministische, effiziente, agile und skalierbare IT-Strukturen im GB BMVg, in denen Prozesse flexibel, umfassend und auch in der Mobilität digital unterstützt werden können.

403. Bezüglich der Ausgestaltung der Digitalisierung im GB BMVg stehen dabei die nachfolgend dargestellten elf Anwendungsfelder im besonderen Fokus, die neben den Ebenen der Digitalisierung zusätzlich den zugrunde liegenden Verfahren zugeordnet sind.

404. Die Steuerung der Weiterentwicklung vom Ist- zum Sollzustand für die mittel- und langfristige Ausgestaltung der einzelnen Anwendungsfelder erfolgt fähigkeitsbezogen im Rahmen der jährlichen Überprüfung und der Fortschreibung der IT-Strategie des GB BMVg.

4.2 IT-Standardisierung

4.2.1 Basis-/Querschnitts-IT und IT-Infrastrukturen konsolidieren

405. Die aktuell unterschiedlichen Systemplattformen und Basistechnologien erschweren die Integration neuer digitaler IT-Services und können eine systemübergreifende Datenverfügbarkeit und -analyse als Voraussetzung weiterer Digitalisierung behindern. Sie sind zudem anfälliger für Cyberangriffe. Ziele der Konsolidierung unter Rückgriff auf bestehende IT-Infrastruktur sowie Basis- und Querschnitts-IT (ressortintern, ressortübergreifend, multinational) sind:

- die Cyber-/IT-Sicherheit vor dem Hintergrund steigender Komplexität zu gewährleisten,
- die Hoheit und Kontrollfähigkeit über die eigene IT dauerhaft zu erhalten,
- auf innovative technologische Trends flexibel reagieren zu können,
- einen leistungsfähigen, wirtschaftlichen, stabilen und zukunftsfähigen Betrieb sicherzustellen und
- ein attraktiver Arbeitgeber für IT-Fachpersonal zu bleiben.

406. Die IT-Leistungen für das Verteidigungsressort sind sehr eng mit den Kernprozessen „Einsätze der Bundeswehr sicherstellen“ und „Einsatzbereite Kräfte bereitstellen“ verflochten. Zukünftig sind hierbei Basis-IT, Querschnitts-IT und zentrale IT-Infrastrukturen als Core Services (CS), auf denen spezifische Community of Interest Services (COIS) aufsetzen, zu konsolidieren und an einem Zielbild für die Systemarchitektur des IT-SysBw auszurichten.

407. Basierend auf dem Gestaltungsprinzip serviceorientierter Architekturen (SOA) können mit Umsetzung der Methode Architektur komplexe Abhängigkeiten zwischen IT-Prozessen und Anforde-

rungen sowie IT-Systemen, IT-Services und IT-Projekten sichtbar gemacht. Dadurch werden komplexe IT-Systeme und IT-Services skalierbar und deren Wiederverwendbarkeit im Gesamtsystem unterstützt sowie die Identifizierung von Redundanzen, Inkonsistenzen, Risiken und organisatorischen Handlungsbedarfen ermöglicht. Langfristiges Ziel ist es, die Produkt- und Systemvielfalt im IT-SysBw sinnvoll zu reduzieren. Ein besonderer Schwerpunkt liegt dabei auf der übergreifenden Spezifikation und – durch Einbinden des Prozessmanagements – der Harmonisierung operationeller Architekturansichten als Bindeglied zwischen den Fähigkeiten der Bundeswehr und der Bereitstellung der dafür erforderlichen IT-Services.

4.2.2 End-to-End (E2E) Prozesse durchgängig digitalisieren

408. Der Mehrwert der Digitalisierung erschließt sich im Bereich des Prozessmanagements erst durch eine durchgängige digitale Gestaltung der Prozesse des GB BMVg. Ziel ist es, strukturierte Abläufe digital unterstützt, End-to-End, umgebungsunabhängig, effizient und medienbrucharm über Organisationsgrenzen hinweg zu gestalten. Dadurch wird die Organisation ihre Effektivität und vor allem Effizienz steigern.

409. Mit Blick auf die Einsatzorientierung sind insbesondere die Kernprozesse der Prozesslandkarte für den GB BMVg („Einsatzbereite Kräfte bereitstellen“ und „Einsätze der Bundeswehr sicherstellen“), aber auch der Managementprozess „Integrierte Planung durchführen“ konsequent und bedarfsgerecht zu digitalisieren und weitestgehend miteinander zu vernetzen. Damit wird die Grundlage für eine übergreifende, standardisierte Informationsbereitstellung geschaffen, die auch die Bundeswehr-spezifischen Anforderungen an Interoperabilität, Mobilität, IT-Sicherheit und Verfügbarkeiten für Einsätze oder einsatzgleiche Verpflichtungen, Dauereinsatzaufgaben, Daueraufgaben, Ständige Aufgaben und aktuelle Aufträge sowie im Grundbetrieb im Inland unterstützt.

410. Dies schließt auch die über Ressortgrenzen hinausgehende Prozessgestaltung unter Einbindung externer und multinationaler Partner, z. B. im Bereich von Amtshilfeverfahren mit anderen Ressorts, die Bereitstellung von Geoinformationen für ausländische Krisenregionen und Einsatzgebiete oder die Zusammenarbeit mit der Wirtschaft über alle Phasen der Produktentwicklung und Serviceerbringung hinweg ein.

411. Im Verwaltungsbereich kommt das Verteidigungsressort den Vorgaben zur elektronischen Aktenführung aus dem e-Government-Gesetz und dem Regierungsprogramm Digitale Verwaltung (DiV) 2020 nach und wird diese technisch und organisatorisch bis 2020 umsetzen. Zudem werden insbesondere bedarfsgerechte Dokumenten-Management-Systeme sowie spezifische Vorgangsbearbeitungssysteme ressortweit implementiert.

4.3 IT-Evolution

4.3.1 Interoperable Kollaboration (national/international) und Mobilität nutzen

412. Der Erfolg der militärischen Führung, des ministeriellen Handelns und die Effektivität und Effizienz des Verwaltungshandelns hängen wesentlich von der Qualität der genutzten Informationen ab. Qualität bedeutet hier die Integrität, Vertraulichkeit und Verfügbarkeit der Informationen, auf deren Basis Entscheidungen getroffen werden. Die weiter zunehmende Bedeutung Deutschlands im multinationalen Umfeld umfasst u. a. folgende Bereiche:,

- Einsatz- und einsatzgleiche Verpflichtungen,
- Framework Nations Concept (FNC) der NATO,
- Szenarien, wie enhanced Forward Presence (eFP) oder der Very High Readiness Joint Task Force (VJTF) im Rahman der enhanced NATO Response Force (eNRF) sowie
- Host-Nation für stationierte oder für verlegende ausländische Truppen.

413. Daher sind interoperable, möglichst ortsunabhängige Kollaborationsformen die Voraussetzung für eine effiziente elektronische Zusammenarbeit sowohl in der Bundeswehrverwaltung und in der militärischen Einsatz- und Operationsführung als auch zwischen diesen Bereichen. Die Kollaborationsformen umfassen unter anderem die Operationsplanung auf Grundlage gemeinsamer oder zumindest interoperabler Führungsinformationssysteme mit einem gemeinsamen Lagebild, die Erstellung und Bearbeitung gemeinsamer Dokumente durch örtlich getrennte Anwender oder die flexible und effiziente Planung und Durchführung von Arbeitsabläufen, Lagevorträgen, Besprechungen und Arbeitsgruppensitzungen.

414. Für mobile Elemente ist hierfür eine einheitliche und gesicherte Sprach- und Datenübertragung auf der taktischen Ebene („Digitalisierung der letzten Meile“) sowie eine Anbindung über verlegefähige Elemente im Einsatzland an die Basis im Inland über weitreichende Kommunikationsmittel erforderlich.

415. Eine informationszentrierte Arbeitsweise erfordert ein Informationsmanagement, das eine nahtlose Kollaborationsfähigkeit auch mit multinationalen Partnern über sichere Netz- und Sicherheitsdomänenübergänge ermöglicht. Das Wissensmanagement der Bundeswehr fördert dazu den bewussten und systematischen Umgang mit der strategischen Ressource Wissen querschnittlich in allen Gestaltungsbereichen.

4.3.2 Gemeinsames digitales Lagebild generieren

416. Durch Vernetzung und damit durch Verfügbarkeit ständig aktualisierter Daten und darauf aufbauender Informationen können Entscheidungsabläufe besser unterstützt und beschleunigt werden. Weiterhin eröffnet die Auswertung großer Datenmengen im digitalen Zeitalter das Gewinnen

neuer Erkenntnisse, welche für die Auftragswahrnehmung der Bundeswehr erschlossen, zielgerichtet aufbereitet und zur Auswertung bereitgestellt werden müssen.

417. Alle im Rahmen von Projekten erhobenen, erfassten und gespeicherten Daten bilden bereits heute das „Digitale Gedächtnis der Bundeswehr“. Die Nutzung der Daten innerhalb eng gefasster Projektrahmen hemmt allerdings die Entwicklung von innovativen und disruptiven Services. Ziel ist es, ein Verständnis zu erzeugen, die digital gespeicherten Daten als integralen Bestandteil der Bundeswehr zu verstehen und nicht als Teil eines Projektes. Dieses bisher nicht genutzte Potenzial ist zu aktivieren und, soweit keine anderslautenden gesetzlichen Regelungen oder vergleichbare Schutzanforderungen dagegenstehen, im Sinne von „Open Data“ innerhalb der Bundeswehr für Projekte verfügbar zu machen (Share-by-Default). Das übergreifende Prozessmanagement entscheidet abschließend über die Verwendung von Daten innerhalb des Geschäftsbereiches.

418. Im Rahmen von Big Data Analytics können Echtzeitanalysen durchgeführt werden, um aktuelle digitale Lagebilder zu erstellen. Neben Auswertungen für Lagebilder (z. B. für die Einsatzbereitschaft, den Ausbildungsstand oder die Logistik) lassen sich verschiedenartigste Datenströme, z. B. Sensor-Daten oder GPS-Daten, für eine gemeinsame Lagebeurteilung durch Verknüpfung mit Geoinformationen aufbereiten, so dass Entscheidungen auf gesicherten, validen Grundlagen getroffen werden können. Vorhandene und ggf. redundante, unabhängige und nicht widerspruchsfreie Lagen sind zu harmonisieren.

419. Die Methoden der GeoInformations-Unterstützung in der Bundeswehr bilden hierbei Basis und Brücke zwischen der neuen Dimension Cyber- und Informationsraum und den bisherigen Dimensionen, indem beispielsweise unstrukturierte Daten aus dem Informationsraum mit geografischen Referenzdaten überlagert, analysiert, dargestellt und wiederum zielgerichtet bereitgestellt werden können. Des Weiteren wird mit der Integration verschiedener Quellen die Leitung des BMVg in die Lage versetzt, Entscheidungen treffen zu können, die auf umfassenden und validen Informationen beruhen. Damit wird die Handlungsfähigkeit auf gesamtstaatlicher Ebene erhöht. Der Dreiklang „Informationsüberlegenheit führt zu Führungsüberlegenheit und schafft Wirkungsüberlegenheit“ ist der Motor für die aktive Ausgestaltung von digitalen Fähigkeiten.

420. Die Dimension Cyber- und Informationsraum erweitert den Operationsraum der Bundeswehr. In Ergänzung zu den bisherigen Lagebildern (u. a. Ausrüstungslage, Einsatzbereitschaftslage, Fähigkeitslage, Lagebilder der bisherigen Dimensionen) sind Cyber-relevante fachliche Lagen u. a. aus den Bereichen Betrieb und Schutz des IT-SysBw sowie Aufklärung und Wirkung im Cyber- und Informationsraum in eine Lage Cyber- und Informationsraum zu fusionieren und Bedarfsträgern im GB BMVg sowie im Rahmen der gesamtstaatlichen Sicherheitsvorsorge ressortübergreifend bereit zu stellen.

421. Für die Erstellung eines einheitlichen und konsistenten Lagebildes ist die Vernetzung von Einrichtungen, Plattformen und Waffensystemen notwendig, durch die ein umfassender, sicherer und unterbrechungsfreier Zugriff auf integre, eindeutige und qualitativ hochwertige Daten und Informatio-

nen ermöglicht wird. Die Realisierung der dazu notwendigen Digitalisierungsprojekte in der Bundeswehr wird hierfür die notwendigen Voraussetzungen schaffen.

4.3.3 Systems Engineering im Rüstungsbereich

422. Industrie 4.0 bzw. das Internet of Things (IoT) wird auch militärische Systeme, Abläufe und die Aufgabenbearbeitung verändern. Die Planung und Kollaboration mit Entwicklungspartnern über ein „strategisches Systems Engineering“ mittels „Product Lifecycle Management“ (PLM) unterstützt kurze Innovationszyklen und verändert – auch disruptiv – die Sicherheits- und Verteidigungsökosysteme. Hierbei stehen cloud-basierte PLM-Systeme im Mittelpunkt. Sie verbinden Planung, Konzeption, Entwicklung und Design, Herstellung, Beschaffung, Abnahme, Betrieb und Weiterentwicklung im Lifecycle Prozess im Sinne einer Rüstung 4.0.

423. Systems Engineering bei Rüstungsvorhaben ist die Grundlage für schnellere, innovative und transparente Rüstungsvorhaben. Zusammenhänge zwischen anspruchsvollen Rüstungsvorhaben, komplexen militärischen Infrastrukturen, Personal und Waffensystemen werden bei der Betrachtung aller Projektelemente in allen Planungskategorien sichtbar und können frühzeitig auf Risiken im Integrierten Planungsprozess sowie im Ausrüstungs- und Nutzungsprozess untersucht sowie dadurch besser beherrschbar gemacht werden. Dies ermöglicht, IT-Services plattformübergreifend zu nutzen.

4.4 IT-Innovation

4.4.1 Schlüsseltechnologien nutzen

424. Die Bundesregierung hat sich im Rahmen der wachsenden Europäisierung der Verteidigungsindustrie zum Erhalt nationaler verteidigungsindustrieller Schlüsseltechnologien bekannt. Diese Technologien sind besonders wichtig und erhaltenswert, deren Verfügbarkeit ist aus nationalem Sicherheitsinteresse zu gewährleisten, ggf. auch in Abstimmung und Zusammenarbeit mit den europäischen Partnern. Es gilt, definierte Schlüsseltechnologien im Schulterschluss mit anderen Ressorts und der Wirtschaft zu entwickeln oder zu erhalten. Hierdurch können eine eigene „digitale Souveränität“ erreicht und erhalten sowie die erforderlichen militärischen Fähigkeiten und die Versorgungssicherheit der Bundeswehr sowie die Rolle Deutschlands als zuverlässiger Kooperations- und Bündnispartner technologisch und wirtschaftlich gesichert werden.

425. Für die IT umfassen diese nationalen Schlüsseltechnologien aktuell die Bereiche der NetOpFü, insbesondere einer Datenintegration und -analyse, sowie Verschlüsselung (Kryptologie), deren Verfügbarkeit aus nationalem Sicherheitsinteresse zu gewährleisten ist. Nationale Unternehmen in diesen Bereichen mit ausreichender Relevanz in Deutschland bzw. im Umfeld der Bündnispartner sollen gezielt gefördert werden.

426. Zum Erhalt bzw. der Förderung von Schlüsseltechnologien sind im Rahmen der Ressortforschung und insbesondere im Bereich Forschung & Technologie (F&T) Schwerpunkte zu setzen. Neben den Schlüsseltechnologien sind hierbei insbesondere Dual-Use-Aspekte sowie die Förderung im Rahmen des Konzeptes zur Mittelstandsförderung zu beachten.

4.4.2 Disruptive Innovationen erschließen

427. Durch die rasante Entwicklung des technischen Fortschritts im IT-Bereich und die damit einhergehenden Veränderungen in der Gesellschaft besteht auch für die Bundeswehr die Notwendigkeit, sich einerseits gegen daraus resultierende Gefahren zu schützen und Risiken weitestgehend zu mindern, andererseits jedoch auch Chancen für die Weiterentwicklung eigener Fähigkeiten nutzbar zu machen. Hierbei ist disruptiven Innovationen eine besondere Bedeutung beizumessen, die zunehmend im Umfeld des „Start-up Ökosystems“ entstehen. Die Bundeswehr muss hierzu stärker an Innovationen außerhalb der eigenen Forschungsergebnisse partizipieren, auf neue Innovationstreiber wie Start-ups und die gesamte Wirtschaft zugehen und Mittel auch für solche Forschungsbereiche bereitstellen, die nicht auf einzelne konkrete Entwicklungen ausgerichtet sind. Es geht damit auch um die Erforschung neuer Zusammenhänge und Ursachen.

428. Ziel ist es, eine höhere Innovationsgeschwindigkeit zu erzielen, eine beschleunigte Einführung von neuen Technologien und Innovationen zu ermöglichen, dabei wo immer möglich nationale Entwicklungen zu fördern und die wirtschaftliche Erschließung von „Dual-Use“-Aspekten mit wehrtechnischen Anwendungsmöglichkeiten zu unterstützen.

429. Ein wichtiger Aspekt hierbei ist die Schaffung einer Plattform für den regelmäßigen Dialog mit Verantwortlichen aus den Bereichen Forschung, Wissenschaft, Wirtschaft und Industrie einschließlich dem Start-Up Ökosystem, um disruptive Technologien rasch zu identifizieren, hinsichtlich eines Mehrwerts für die Bundeswehr zu bewerten und auf Grundlage eigener Bedarfe gegebenenfalls schnell einführen und als IT-Service anbieten zu können.

430. Der Dialog mit allen relevanten Stakeholdern im Bereich Cyber/IT bedarf eines darauf zugeschnittenen Wissensmanagements, welches das verfügbare öffentliche Wissen schnell und flexibel nutzbar macht. Der Austausch von Erfahrungen, Kenntnissen und Fähigkeiten muss durch den Ausbau von Netzwerken weiter unterstützt werden. Hierdurch können Bedrohungen und Entwicklungen, die die bestehenden Rahmenbedingungen grundlegend bzw. wesentlich verändern, frühzeitig erkannt und bei Bedarf abgewehrt oder nutzbar gemacht werden. Dazu sind die bereits implementierten Schritte wie bspw. der Aufbau des Cyber-Clusters an der Universität der Bundeswehr München konsequent fortzusetzen. Darüber hinaus ist der Aufbau eines Cyber Innovation Hub umzusetzen, der als Schnittstelle zu Innovationsakteuren fungiert und auch Mittel zur Beteiligung an Studien oder Start-ups steuert.

431. Diese Ansätze sind konsequent in ein gesamtplanerisches Innovationsmanagement einzubeziehen, um die daraus entstehenden Auswirkungen auch in alle anderen betroffenen Innovationsbereiche einfließen zu lassen. Im Rahmen der Digitalisierung wird es daher in allen Innovationsbereichen darauf ankommen, ein durchgängiges Informations- und Wissensmanagement verfügbar zu machen.

5 Grundlagenverfahren im Fokus der Digitalisierung

501. Für die vorgenannten Anwendungsfelder der Digitalisierung schafft der GB BMVg konsequent die Grundlagen. Dabei werden die ressortspezifischen Verfahren an die Erfordernisse der Digitalisierung angepasst bzw. neue Verfahren eingeführt.

5.1 Durchsetzungsfähige IT-Governance aufbauen

502. Die Verantwortung für IT-Governance im GB BMVg liegt beim Ressort CIO. Sein Aufgabenspektrum umfasst dabei sowohl die Digitalisierung als auch IT-spezifische Aspekte der Planungs-, Entwicklungs-, Beschaffungs- und Betriebsprozesse. Es gilt die Wertschöpfung der IT für die Auftragserfüllung der Bundeswehr angemessen zu berücksichtigen und mögliche Risiken zu minimieren.

503. Dieses Aufgabenspektrum erfordert die Kenntnis über Rolle und Auswirkung der IT auf die Bundeswehr und den verantwortungsvollen Umgang mit Ressourcen, die Definition von möglichen Einschränkungen, die Befähigung zur Messung der (IT-Service-)Leistungserbringung und ein umfassendes Verständnis über Risiken und deren angemessene Überwachung entlang der Prozesse sowie die Gewährleistung der Cyber-/IT-Sicherheit.

504. In seiner Verantwortung, die Übereinstimmung des Einsatzes von IT mit den politischen, strategischen und operativen Zielen des GB BMVg und den IT-Festlegungen der Bundesregierung in Deckung zu bringen, gestaltet der Ressort CIO einen Leistungsprozess „IT-Governance gewährleisten“, schreibt federführend die IT-Strategie GB BMVg fort und führt bei wesentlichen Abweichungen hinsichtlich der Zielerreichung die notwendigen Leitungsentscheidungen herbei.

5.2 Ganzheitliches IT-Architektur- und IT-Servicemanagement schaffen

505. Die Einführung eines standardisierten, übergreifenden und entscheidungsbefugten IT-Architektur- und durchgängigem IT-Servicemanagements in die Bundeswehr – aufbauend auf bzw. in Wechselwirkung mit dem Prozessmodell GB BMVg – ist eine zentrale Voraussetzung für die effektive strategische Steuerung der zukunftsorientierten Ausrichtung des IT-SysBw.

506. Die Entwicklung und dynamische Fortschreibung einer „Enterprise Architecture“ wird mit Nachdruck vorangetrieben. Nur so lassen sich die in den strategischen Vorgaben definierten Ziele zur Einbindung der Streitkräfte in multinationale Strukturen und multinationale Interoperabilität realisieren.

507. Die Beherrschung der zunehmenden Komplexität und Kurzlebigkeit der Technologie im Bereich Cyber/IT erfordert einen breit angelegten, nachhaltigen und wirkungsvollen Fähigkeitsaufbau in allen Bereichen der Bundeswehr, der einheitlichen Architektur- und IT-Servicemanagementvorgaben folgt.

5.3 Agilität bei der Einführung von IT erhöhen

508. Im Gegensatz zu „klassischen“ Rüstungsgütern wird die Informationstechnik im Wesentlichen vom zivilen Markt geprägt und unterliegt deutlich kürzeren Innovationszyklen. Um dieser Entwicklung Rechnung zu tragen, gilt es sich eines zwischen Spezifikations- und Realisierungsseite iterativen Entwicklungsmodells als Kennzeichen einer agilen Organisation zu bedienen. Dazu sind Prozesse, Produkte und Leistungen integrativ statt nach einem traditionellen „V-“ oder „Wasserfallmodell“ auszuplanen. Kurzfristigen politischen Ereignissen und einer sich schnell ändernden Sicherheitslage kann damit besser Rechnung getragen werden. Grundsätzlich ist so eine schnelle Anpassungsfähigkeit an veränderte Rahmenbedingungen möglich, Fehler können frühzeitig erkannt und zeitnah korrigiert werden.

509. Zur Beschleunigung bei der Einführung von CGM-Produkten[1] wurden die bestehenden Prozesse für Planung und Beschaffung bereits modifiziert. Die kurzen Innovationszyklen in der IT erfordern dennoch – wie oben beschrieben – eine kontinuierliche Überprüfung der bestehenden Verfahren hinsichtlich der notwendigen Agilität.

5.4 Veränderungsmanagement Digitalisierung einrichten

510. Zentraler Erfolgsfaktor für die Umsetzung von Digitalisierung im GB BMVg ist die adäquate Einbindung und Berücksichtigung der Belange der beteiligten Nutzer im GB BMVg und eine transparente Fortschrittsmessung unter Einbindung von Fachaufsicht und Nutzung von IT-Systemen.

511. Digitalisierung der Bundeswehr ist mehr als nur die Umsetzung von IT-Projekten, sie soll einen Mehrwert für die Organisation und den einzelnen Nutzer erreichen. Zur Nutzung des gesamten Potenzials müssen Maßnahmen in allen Planungskategorien koordiniert ineinander greifen. Es wird ein Veränderungsmanagement etabliert, um die zentrale Steuerung adressatengerechter Kommunikationsmaßnahmen vor und während der Umsetzung von Digitalisierungsmaßnahmen zu steuern und zu gestalten.

512. Ziel ist die Schaffung einer dauerhaften Akzeptanz für die Anwendungen der Digitalisierung durch ein einheitliches Verständnis über Inhalte, Umsetzungsgrad (IST) und Zielzustand (SOLL) bei Nutzer und Nutzergruppen. Darüber hinaus soll das Veränderungsmanagement zur bedarfsgerechten, den Anwendungen der Digitalisierung entsprechenden Qualifizierung des Personals beitragen. Diese Maßnahmen reichen von der Aus-, Fort- und Weiterbildung, über die Prozessanpassung und die Personalgewinnung bis zur Sensibilisierung und Schulung von vorhandenem Schlüsselpersonal der Bundeswehr (z. B. Vorgesetzte aller Führungsebenen, IT-Verantwortliche, IT-Sicherheitsbeauftragte, etc.).

[1] CGM: COTS, GOTS, MOTS (Commercial Off-The-Shelf; Governmental Off-The-Shelf; Military Off-The-Shelf)

513. Im Ergebnis begleitet das Veränderungsmanagement aktiv die Konzeption und Umsetzung der Anwendungen der Digitalisierung. Es sensibilisiert für die Dringlichkeit dieser Anwendungen, vermittelt Inhalte für eine Identifikation mit dem Thema Digitalisierung („Digital Awareness“) und kommuniziert mit den entsprechenden Zielgruppen über Strategien, Ziele und Zwischenergebnisse der Digitalisierung. Darüber hinaus sind die daraus resultierenden Folgen für den Menschen in einer digitalisierten Arbeitsumwelt konsequent zu berücksichtigen. Hier wird es Aufgabe sein, jeden Einzelnen bzw. jede Einzelne mitzunehmen, durch Schulung und Training konsequent auf sein bzw. ihr Arbeitsumfeld vorzubereiten und insgesamt die sich eröffnende Veränderung von Arbeit im Gleichklang mit der voranschreitenden Digitalisierung auszugestalten. Nur so kann ein Mehrwert für den GB BMVg als Ganzes und den Menschen innerhalb der Organisation erzielt werden.

6 Schlusswort

601. Der GB BMVg hat die Chancen und Risiken der Digitalisierung erkannt und wird den weiteren Digitalisierungsprozess aktiv gestalten und damit für den GB BMVg einen Mehrwert bei der Auftragserfüllung erzielen. IT ist der strategische „Enabler“ (Impulsgeber) für die Befähigung der Streitkräfte und der Bundeswehrverwaltung zur Erfüllung ihrer Kernaufträge.

602. Die Bundeswehr nutzt Chancen der Digitalisierung und begegnet den Risiken aktiv. Dies geschieht zukünftig nicht sequenziell, sondern muss aufgrund der hohen Entwicklungsdynamik auf drei Ebenen parallel stattfinden.

603. Die Anwendungsfelder der Ebene der IT-Standardisierung steigern die Effizienz des Handelns. Dazu steigert der Einsatz einheitlicher Methoden und Standards die Interoperabilität und Bündnisfähigkeit der Bundeswehr. Die Bundeswehr nutzt dieses Vorgehen aktiv und stärkt ihre Rolle im multinationalen Umfeld bei der NATO und der Europäischen Union.

604. Zur Unterstützung der Fähigkeitsentwicklung der Bundeswehr in allen Bereichen muss auch das IT-SysBw im Kontext der Ebene der IT-Evolution stetig weiterentwickelt werden.

605. Informationstechnik wandelt sich vom „Systemunterstützer“ zur „Triebfeder“ für Veränderungen. Auf der Ebene der IT-Innovation wird die Bundeswehr eine führende Rolle bei der Entwicklung von Schlüsseltechnologien für die Bundeswehr einnehmen. Durch die gezielte Vernetzung von Bundeswehr, Wissenschaft und Wirtschaft sowie auf der Basis eines strukturierten Dialogs mit der Industrie werden Innovationen und Trends in der Informationstechnologie frühzeitig erkannt und für die Bundeswehr nutzbar gemacht.

606. Wesentliche Erfolgsfaktoren für die Umsetzung von Digitalisierung sind die Akzeptanz und Umsetzung durch den Nutzer, eine durchsetzungsfähige IT-Governance, ein ganzheitliches IT-Architektur- und IT-Servicemanagement, Agilität bei der Einführung von IT, die Digitalisierung der Mobilität sowie ein übergreifendes, begleitendes Veränderungsmanagement und eine umfassende Ausbildung.

607. Die konsequente Umsetzung der Digitalisierung ist eine Aufgabe für den gesamten GB BMVg, über alle Führungsebenen, die über die Technik hinausgeht und sowohl Organisation und Prozesse als auch militärische Fähigkeiten beeinflussen wird. Dies gilt es gemeinsam zu gestalten.

„Das Ausschöpfen der digitalen Möglichkeiten und das Ausbilden eines digitalen Selbstverständnisses werden die militärischen Fähigkeiten der Zukunft prägen.“

7 Anlagen

7.1 Glossar

Big Data Analytics

Big Data Analytics steht für die Untersuchung von großen Mengen an Daten unterschiedlicher Arten (Big Data), um darin (versteckte) Muster, unbekannte Korrelationen und andere nützliche Informationen zu erkennen. Solche Informationen können Einsatz-/Wettbewerbsvorteile gegenüber anderen bringen. Das Hauptziel von Big Data Analytics besteht darin, dem GB BMVg in allen Bereichen zu besseren Entscheidungen zu verhelfen.

Core Services

Core Services (CS) bieten generische, domänenunabhängige, technische Funktionen, die den Betrieb und die Nutzung von IT-Ressourcen ermöglichen und erleichtern. Hierbei handelt es sich meist um Infrastrukturdienstleistungen (inkl. Leistungen der Informationssicherung), Service-orientierte Architektur Plattformleistungen sowie generelle Unternehmensunterstützungsleistungen.

Community of Interest Services

Community of Interest (COIS) Services unterstützen eine oder mehrere kollaborative Gruppen von Nutzern mit gemeinsamen Zielen, Interessen, Missionen oder Geschäftsprozessen.

Dual-Use Innovationspotenzial

Dual-Use bezeichnet Fähigkeiten, Güter oder Dienste, welche neben ihrer beabsichtigten, originären Verwendung direkt oder mit minimaler Anpassungszeit auch anders eingesetzt werden können. Während der Primärzweck häufig ziviler oder militärisch-defensiver Natur ist, können Dual-Use-Technologien auch für militärisch-offensive Zwecke verwendet werden. Beispiele für Dual-Use-Innovationen sind Forschungen im Bereich der Abwehr von biologisch-chemischen Waffen, der Nutzung von Nukleartechnologie, insbesondere der Anreicherung, aber auch Technologien im Bereich der Cyberverteidigung.

End-to-End Prozesse

Ein End-to-end-Prozess ist ein Prozess, der aus sämtlichen zeitlich-logisch aufeinander folgenden Teilprozessen besteht, die zur Erfüllung eines Kundenbedürfnisses/Auftrages notwendig sind. Die Betonung auf „End-to-end“ soll verdeutlichen, dass sich dieser Prozess vom ursprünglichen Bedarf bis zur Leistungserbringung erstreckt und mit Blick auf den GB BMVg in der Regel abteilungsübergreifend wahrgenommen wird.

Enterprise Architecture

Enterprise Architecture oder auch „Unternehmensarchitektur“ beschreibt im Bereich Cyber/IT das Zusammenspiel von Elementen der Informationstechnologie und der Tätigkeiten im GB BMVg. Die IT-Strategie GB BMVg ist dabei ein Lenkungsdokument, macht Vorgaben und wird in der Unternehmensarchitektur detailliert. Eine Enterprise Architecture-/Unternehmensarchitekturinitiative geht immer vom Ressort CIO aus.

Industrie 4.0

Die Bezeichnung „Industrie 4.0“ bringt das Ziel zum Ausdruck, eine vierte industrielle Revolution einzuleiten. Die industrielle Produktion soll dabei mit moderner Informations- und Kommunikationstechnik verzahnt werden. Technische Grundlage hierfür sind intelligente und digital vernetzte Systeme, mit deren Hilfe nicht mehr nur einen Produktionsschritt, sondern eine gesamte Wertschöpfungskette optimiert werden soll.

Internet of Things (IoT)

Unter Internet of Things (Internet der Dinge) wird die zunehmende Einbeziehung von Alltagsgegenständen (Infrastruktur, Autos, Häuser, Küchengeräte etc.) in den Cyberraum verstanden.

IT-Governance

IT-Governance dient der Steuerung der IT, so dass diese die Strategie und die Ziele des GB BMVg optimal unterstützt. Sie besteht aus Führung, Organisationsstrukturen und Prozesse und liegt in der Verantwortung des Ressort CIO.

IT-Rat

Der IT-Rat ist auf politisch-strategischer Ebene das zentrale Gremium für ressortübergreifende IT-Fragestellungen in der Bundesverwaltung und zuständig für die strategische Steuerung des ressortübergreifenden Projekts IT-Konsolidierung des Bundes. Die Besetzung des IT-Rats erfolgt durch die für IT zuständigen beamteten Staatssekretäre bzw. Staatssekretärinnen aller Bundesministerien, die für Informationstechnik zuständigen Abteilungsleiter bzw. Abteilungsleiterinnen des Bundeskanzleramtes, sowie die Beauftragte bzw. den Beauftragten der Bundesregierung für Kultur und Medien und des Presse- und Informationsamtes der Bundesregierung. Vorsitzender bzw. Vorsitzende des IT-Rats ist der bzw. die Beauftragte der Bundesregierung für Informationstechnik.

Konferenz der IT-Beauftragten der Ressorts

Die Konferenz der IT-Beauftragten der Ressorts ist verantwortlich für die operative IT-Steuerung der Bundesverwaltung und entscheidet über alle Fragen des Betriebs der Bundes-IT auf der Basis der Beschlüsse des IT-Rats. Mitglieder der Konferenz sind die IT-Beauftragten der Bundesressorts. Die anderen Verfassungsorgane, der bzw. die Beauftragte für die Wirtschaftlichkeit in der Verwaltung, der

Bundesrechnungshof und die bzw. der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit werden in die Arbeit der Konferenz eingebunden. Der Vorsitz liegt bei der bzw. dem IT-Beauftragten des Bundesministeriums des Innern (BMI).

Private Cloud Bundeswehr

Umschreibt den Ansatz, abstrahierte Services (z. B. Datenspeicher, Rechenkapazitäten, Netzwerkkapazitäten oder auch Software) dynamisch an den Bedarf angepasst über eine eigene Infrastruktur zur Verfügung zu stellen. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei über definierte Schnittstellen und Protokolle.

Product Lifecycle Management

Beim Product Lifecycle Management handelt es sich um einen Ansatz zur ganzheitlichen, unternehmensweiten Verwaltung und Steuerung aller Daten und Prozesse des gesamten Lebenszyklus‘ eines Produktes – von der Entwicklung und Produktion über den Vertrieb bis hin zur Verwertung. Ziel dabei ist es, den Produktentstehungsprozess durch Datenmanagement zu unterstützen und die Entwicklungsproduktivität zu erhöhen. Zur Unterstützung dieses Ansatzes stehen IT-basierende PLM-Lösungen zur Verfügung, die mit ihren Funktionen die Umsetzung des PLM-Ansatzes in großen Teilen erst ermöglichen.

Ressort CIO

Der Chief Information Officer (CIO) nimmt die Aufgaben der strategischen und operativen Führung der Informationstechnologie und -technik wahr. Die Spezifizierung auf Ressort CIO verdeutlicht die Zuständigkeit für ein ausgewähltes Ressort der Bundesregierung, im vorliegenden Fall dem GB BMVg.

Die Aufgaben der Ressort CIO werden im Konzept IT-Steuerung Bund beschrieben und umfassen u. a.:

- Gewährleistung der Übereinstimmung des IT-Einsatzes mit den politischen, strategischen und operativen Zielen des Ressorts und den IT-Festlegungen der Bundesregierung
- entscheidungsbefugte Vertretung der IT des Ressorts nach außen sowie
- Wahrnehmung der Funktion in engem Zusammenwirken mit den Aufgaben der Verwaltungsorganisation und Verwaltungsmodernisierung.

Der Ressort CIO ist der jeweiligen Leitung des Ressorts in dieser Funktion grundsätzlich unmittelbar unterstellt.

Serviceorientierte Architekturen

Eine Serviceorientierte Architektur (SOA) ist ein Rahmenwerk zur Strukturierung verteilter heterogener Informationssysteme und kann als Methode verstanden werden, vorhandene EDV-Komponenten wie Datenbanken, Server und Websites in Dienste zu integrieren und so zu koordinieren, dass Leistungen durch unterschiedliche Anwender genutzt werden können. Ziel ist die höhere Flexibilität und Agilität der Geschäftsprozesse.

Sicherheits- und Verteidigungsökosystem

Der Begriff Ökosystem soll in diesem Zusammenhang verdeutlichen, dass eine Vielzahl von Akteuren zu berücksichtigen ist, diese netzwerkartig miteinander verknüpft sind und die Gestaltung der Verbindung zwischen den einzelnen Elementen für den Erfolg oder auch Misserfolg des gemeinsamen Ziels verantwortlich ist. Im Fall des Sicherheits- und Verteidigungsökosystems sind dies alle Akteure, die direkt oder indirekt mit der Sicherheits- und Verteidigungspolitik und der Umsetzung dieser Politik befasst sind.

Start-up Ökosystem

Unter dem Begriff Ökosystem werden hier alle Stakeholder zusammengefasst, deren Zusammenspiel für den Erfolg oder Misserfolg des Gesamtsystems verantwortlich ist. Das Start-up Ökosystem ist dabei als Teilsegment des Innovationssystems insgesamt zu verstehen, da Gründungen von Unternehmen zur Verfolgung einer technologischen Idee eine Möglichkeit der Innovationsverwertung darstellen. Der Begriff „Start-up Ökosystem“ umfasst daher alle Akteure, die direkt oder indirekt mit Start-ups im Zusammenhang stehen.

Systems Engineering

Systems Engineering ist ein interdisziplinärer Ansatz, um komplexe technische Systeme zu entwickeln und zu realisieren. Im Mittelpunkt stehen die gewünschten Anforderungen an das fertigzustellende System, die innerhalb eines Kosten- und Zeitrahmens zu erfüllen sind. Das System wird hierfür in Subsysteme, Geräte und Software heruntergebrochen und spezifiziert. Die Implementierung wird über alle Ebenen hinweg kontinuierlich über alle Lebensphasen eines Projektes, einschließlich der Übergabe des Lebenszyklusmanagements, kontrolliert.

Vernetzte Operationsführung (NetOpFü)

NetOpFü bedeutet die Führung und den Einsatz von Streitkräften auf der Grundlage eines bundeswehrgemeinsamen, Führungsebenen übergreifenden und interoperablen Informations- und Kommunikationsverbundes, der durch das IT-SysBw übergreifend bereitgestellt wird und der alle beteiligten Personen, Dienststellen, Truppenteile und Einrichtungen sowie Sensoren und Effektoren miteinander verbindet.

7.2 Änderungsjournal

Version	Gültig ab	Geänderter Inhalt
1	31.03.2017	• Erstveröffentlichung