

Computer sagt Nein

Lehren für die Bundeswehr aus dem ukrainischen Battle Management System



Max Becker
Policy Fellow, Center for
Security and Defense



Sebastian Schwartz
Associate Fellow, Center
for Security and Defense

Die Ukraine zeigt im Abwehrkampf gegen Russland, dass moderner Krieg auch eine softwaretechnische Herausforderung ist: Wie schnell Daten aus Drohnen, Satelliten und Aufklärung zu militärischer Wirkung gebracht werden, zeigt das Battle Management System (BMS) Delta eindrucklich. Die Bundeswehr setzt primär mit SitaWare auf ein vergleichbares System. Doch fehlende Digitalisierung, Verzögerungen bei D-LBO (Digitalisierung landbasierter Operationen der Bundeswehr) und eine zu wenig agile Entwicklungskultur verhindern noch, dass sie im Ernstfall ähnlich schnell und vernetzt handeln kann wie die Ukraine.

- Ein Battle Management System vernetzt Gefechtsfelddaten aus heterogenen Quellen in Echtzeit zu einem einheitlichen Lagebild. Es beschleunigt die Kill Chain, also den Zeitraum von der Detektion bis zur Bekämpfung eines Ziels, und wird durch KI sehr zentral zur Voraussetzung verantwortbarer militärischer Entscheidungen.
- Ukraines System Delta zeigt, wie dies gelingt: niedrigschwellig zugänglich, leicht bedienbar und ständig durch Feedback vom Schlachtfeld weiterentwickelt, ist es die fortschrittlichste verfügbare BMS-Lösung.
- Die Bundeswehr setzt seit 2019 schrittweise auf das BMS SitaWare und hat es seither auf Heer, Marine, Luftwaffe und den Sanitätsdienst ausgeweitet – konzeptionell vergleichbar mit dem ukrainischen Delta-Ansatz.
- Drei zentrale Lücken verhindern volle Wirksamkeit: fehlende Digitalisierung der Altsysteme, Verzögerungen im Programm D-LBO bei Funkgeräten sowie eine Beschaffungskultur ohne agile, kontinuierlichere Feedbackschleifen zwischen Entwicklung und Truppe.

Der Abwehrkampf der Ukraine gegen die russische Vollinvasion zeigt, was moderne Kriegsführung bedeutet. Was seit 2014, spätestens aber seit Februar 2022, auf ukrainischem Boden erprobt, verworfen und weiterentwickelt wird, betrifft jedoch nicht nur die veränderte Kriegsführung durch unbemannte Systeme: Es berührt die Frage, wie Informationen möglichst schnell in militärische Wirkung übersetzt werden können. Die Antwort, die die Ukraine auf diese Frage entwickelt hat, ist nicht primär taktischer oder operativer Natur. Sie ist eine softwaretechnische.

Das ukrainische Delta-System ist hierfür das prominenteste Beispiel. Als integrierte Lagedarstellungsplattform aggregiert es Daten aus Drohnen, Satelliten, Bodenaufklärung, dem Cyberraum und menschlichen Quellen in Echtzeit, stellt sie verschiedenen Nutzer:innengruppen auf unterschiedlichen Führungs- bzw. Operationsebenen und auf verschiedenen Endgeräten zur Verfügung und verkürzt damit den Weg von der Aufklärung bis zur tatsächlichen Bekämpfung des Gegners drastisch. Delta ist damit kein technisches Detail am Rande des Kriegsgeschehens, sondern eine fundamentale Säule der ukrainischen Verteidigungsfähigkeit.¹ Und es ist ein Paradebeispiel für das, was man unter dem Oberbegriff des Battle Management System (BMS) zusammenfassen kann.

Dieser Text verfolgt drei Argumentationsstränge. Er erklärt erstens, was Battle Management Systeme als zentrale Infrastruktur vernetzter Gefechtsführung technisch leisten müssen, und warum ihre Wirksamkeit nicht nur eine technische, sondern ebenso eine rüstungspolitische und kulturelle Frage ist. Er zeigt zweitens, wie die Ukraine mit Delta auf allen drei Feldern gleichzeitig eine Antwort entwickelt hat, die unter Echtbedingungen funktioniert. Und er fragt drittens, wo die Bundeswehr auf jedem dieser Felder steht und was zu tun ist, um den notwendigen Sprung zu schaffen.

WAS IST EIN BMS?

Eines der größten Hindernisse bei der Auseinandersetzung mit Battle Management Systemen ist begrifflicher Natur. Eine allgemeingültige, verbindliche Definition

existiert nicht. Erschwerend kommt hinzu, dass die Terminologie im sicherheitspolitischen und militärischen Diskurs erheblich variiert: Command & Control (C2), C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance), Führungsinformationssysteme und Battle Management Systeme werden teils synonym, teils mit deutlich unterschiedlichen Bedeutungen verwendet.

Für die Zwecke dieses Textes gilt daher folgende Arbeitsdefinition: Ein Battle Management System ist eine skalierbare, modulare Plattform, die in Echtzeit Gefechtsfeld- und gefechtsfeldrelevante Daten aus heterogenen Quellen zusammenführt, aufbereitet und verschiedenen Nutzer:innengruppen in einer einheitlichen Lagedarstellung zugänglich macht, und die domänenübergreifend funktioniert und eingesetzt werden kann. Die Schnittstellenfunktion des Systems ist dabei nicht statisch, sondern durch die Nutzer:innen lage- und auftragsabhängig anpassbar. Informationen können in beide Richtungen übertragen werden. Eine verlässliche und unkomplizierte Bedienbarkeit unter Hochstressbedingungen ist keine nachgelagerte Optimierung, sondern konstitutives Merkmal eines funktionsfähigen BMS.²

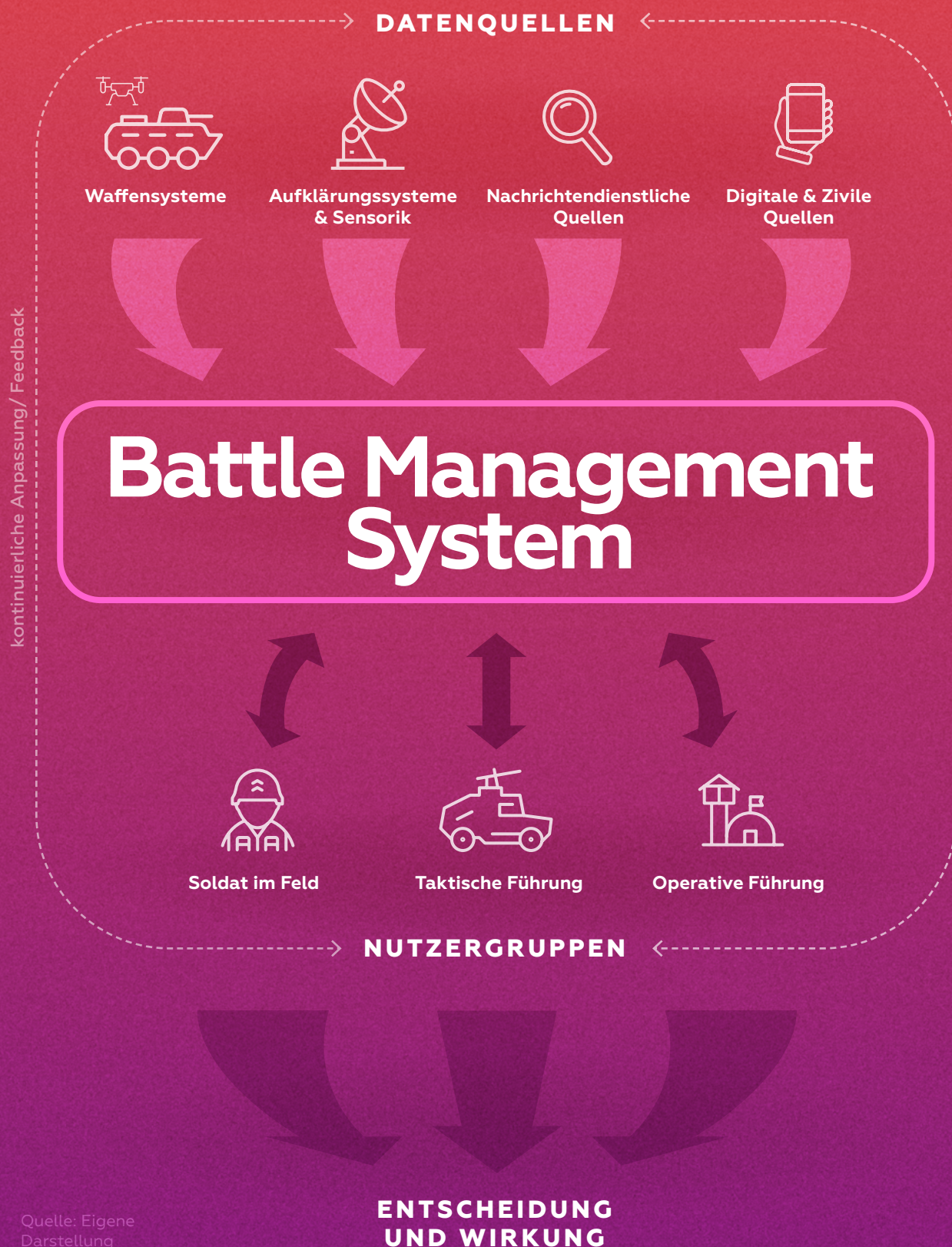
BMS ALS OPERATIVE NOTWENDIGKEIT MODERNER KRIEGSFÜHRUNG

Die sinnvolle, teils automatisierte Aggregation und Vernetzung von verschiedenen, heterogenen Datenquellen zu einem Gesamtlagebild, auf dessen Grundlagen militärische Entscheidungen getroffen werden, ist zu einer zentralen Fähigkeit im modernen Krieg geworden. Ein fähiges BMS ist dazu in der Lage, die sog. "Kill Chain"³, also die sequenzielle Abfolge von der Aufklärung des Ziels bis zu seiner Bekämpfung, zu beschleunigen und zu vereinfachen. Ein umfassendes Lagebild ist die Grundlage und nicht nur für die initiale Zielerfassung entscheidend, sondern für jede einzelne Phase: Es liefert die Lagekenntnis, auf deren Grundlage Entscheidungen getroffen werden; es ermöglicht die Koordination der einzusetzenden Mittel, und es stellt sicher, dass die erzielte Wirkung

1 Kateryna Bondar, "How Ukraine's War is Reshaping C4ISR for the Modern Battlefield", The Hague Centre for Strategic Studies (May 2025): <https://hcss.nl/wp-content/uploads/2025/05/02-Kate-Bondar-How-Ukraines-War-is-Reshaping-C4ISR-for-the-Modern-Battlefield-Final-v5.pdf> (Zugriff: 31.07. 2026).

2 Kai, Strell, "Künstliche Intelligenz und autonome Waffensystem in der modernen Kriegsführung – eine einführende Übersicht", Kieler Analysen zur Sicherheitspolitik Nr.55 (2026): https://www.ispk.uni-kiel.de/de/publikationen_neu/kieler-analysen-zur-sicherheitspolitik/2026/Strell_KI_und_autonome_Waffensysteme.pdf (Zugriff: 31.07. 2026).

3 Vitaliy Goncharuk, "Survival of the Smartest? Defense AI in Ukraine", in *The Very Long Game. 25 Case Studies on the Global State of Defense AI*, hrsg. von Heiko Borchert, Torben Schütz und Joseph Verbovsky (Springer, 2024), 375 – 395: https://link.springer.com/chapter/10.1007/978-3-031-58649-1_17 (Zugriff: 31.07. 2026).



Quelle: Eigene Darstellung

bewertet und die Ableitungen aus dieser Bewertung bei der nächsten Bekämpfung berücksichtigt werden können. Durch die Integration der verschiedenen Datenquellen in ein kohärentes, einheitliches Systemumfeld entsteht eine umfassendere Entscheidungsgrundlage: Informations- und Reibungsverluste an den Schnittstellen zwischen den Quellen werden reduziert, und blinde Flecken, also Bereiche, die bei isolierter Betrachtung einzelner Quellen und Datenpunkte unsichtbar blieben, werden sichtbar gemacht. Zum anderen geht es darum, Entscheidungen über die Bekämpfung eines Ziels und die dafür benötigten Mittel möglichst schnell treffen zu können. Denn: Im Grundsatz ist davon auszugehen, dass diese Fähigkeit auch bei Gegnern verfügbar ist, was zu einem algorithmisierten Sicherheitsdilemma führt.

Der allgegenwärtige Trend zur Automatisierung und zur Integration Künstlicher Intelligenz in militärische Prozesse verleiht der Fähigkeit, auf einer möglichst vollständigen und einheitlichen Datengrundlage schnell Entscheidungen zu treffen, zusätzliches Gewicht. Denn der menschliche Anteil an den beschriebenen Entscheidungsprozessen nimmt stetig ab. Damit droht jene korrigierende Instanz zu entfallen, die Fehler, Lücken oder Widersprüche in den Daten durch Erfahrung und Kontextwissen ausgleichen kann.⁴ Je stärker Entscheidungen also algorithmisch vorbereitet oder getroffen werden, desto unmittelbarer wirken sich Mängel in der Datenbasis und im technischen Grunddesign des Systems auf das Ergebnis aus, ohne dass ein Mensch diese Fehler im Entscheidungsprozess noch abfangen kann. Beispiele sind veraltete, unvollständige oder fehlerhafte Informationen oder sich widersprechende Entscheidungsvorschläge⁵. Eine verlässliche Datenbasis wird damit – neben gut ausgebildetem und auch in Hochstressumgebungen trainierten Soldat:innen – zur zentralen Bedingung dafür, dass Automatisierung und KI-gestützte Prozesse im militärischen Kontext überhaupt verantwortbar eingesetzt werden können.

DIE UKRAINE ALS BENCHMARK: DELTA UND DIE LEHREN DES ECHTBETRIEBS

Bei Delta handelt es sich um das 2023 offiziell in die ukrainischen Streitkräfte eingeführte, cloudbasierte BMS. Es kann als die derzeit fortschrittlichste, in einem hochintensiven Krieg bewährte Lösung im Bereich der BMS angesehen werden.

Dabei ist Delta ohne das ukrainische Innovations-ökosystem⁶, das seit 2014 stetig gewachsen ist und stets Schnittstellen zwischen dem ukrainischen Sicherheits- und Regierungsapparat⁷ sowie der Zivilgesellschaft unterhalten hat, nicht zu verstehen. Die Entwicklung von Delta verdeutlicht exemplarisch den ukrainischen Ansatz, Sicherheit dezentral nicht nur herzustellen, sondern auch fortlaufend weiterzuentwickeln.⁸ Hierbei ist der ständige Feedbackloop direkt vom Schlachtfeld die Stellschraube, um konsequente Innovation mit tatsächlichem Mehrwert für die Nutzer:innen zu verbinden.⁹ Ursprünglich 2015 maßgeblich von der NGO Aerozvidka mitentwickelt, die später als Unit A2724 in die ukrainischen Streitkräfte integriert wurde, liegt die Weiterentwicklung von Delta heute beim ukrainischen Verteidigungsministerium, konkret beim Center for Innovation and Development of Defense Technologies.¹⁰ Delta ist nicht als klassisches, monolithisches System zu verstehen, das zentral geplant und (weiter-)entwickelt wird. Soweit bekannt, deutet vieles darauf hin, dass Delta eher als modulare Entwicklungsinfrastruktur konzipiert ist: Bestimmte Kernfunktionen – Zugriffsverwaltung, Cybersicherheit, Cloudinfrastruktur – werden zentral administriert, während die Plattform gleichzeitig so angelegt ist, dass autorisierte Personen auf dieser Grundlage eigene Module und Funktionalitäten entwickeln und integrieren können. Delta ist damit kein Open-Source-Projekt im klassischen Sinne, aber auch kein geschlossenes System. Vielmehr ist Delta eine kontrollierte offene Plattform, die Modularität und

- 4 Candace, Rondeaux, "The Algorithmic Fog of War" Future Tense Fiction. Issues in Science and Technology (January 30, 2026) <https://issues.org/futuretensefiction/ai-combat-black-box-rondeaux/> (Zugriff: 31.07. 2026).
- 5 Kevin, Baker, "Kill chain. On the automate bureaucratic machinery that killed 175 children" <https://artificialbureaucracy.substack.com/> (21.03. 2026), <https://artificialbureaucracy.substack.com/p/kill-chain> (Zugriff: 31.07. 2026).
- 6 Jon-Wyatt Matlack, Sebastian Schwartz, Oliver Gill, "Ukraine's Drone Ecosystem and the Defence of Europe: Lessons Lost Can't be Learned", LSE Ideas, Research Report, April 2025: <https://www.lse.ac.uk/ideas/Assets/Documents/2025-04-05-DRONES-MatlackSchwartzGill-FINAL-WEB-03.pdf> (Zugriff: 31.07. 2026).
- 7 Matthew B Arnold, Viktoriia Roller, Khrystyna Zhyvogliad, "Apps at War: Army+, Reserve+ and the Rise of Digital Defence Governance in Ukraine", LSE Ideas, Research Report, Mai 2026: <https://www.lse.ac.uk/asset-library/2026-05-02-naw-appswar-02-web.pdf> (Zugriff: 31.07. 2026).
- 8 Goncharuk, "Survival of the Smartest? Defense AI in Ukraine", 375. https://link.springer.com/chapter/10.1007/978-3-031-58649-1_17 S. 375
- 9 Jack Matlack, Oliver Gill, "Teaching the humans in the loop: Supporting and integrating Ukraine's unmanned systems training into Europe's Security Architecture", LSE Ideas, Strategic Update, Juni 2026: <https://www.lse.ac.uk/asset-library/matlack-j-and-gill-o-teachinghumansintheloop-1.pdf> (Zugriff: 31.07. 2026).
- 10 Stefan Soesanto, "The Ukrainian Way of Digital Warfighting. Volunteers, Applications, and Intelligence Sharing Platforms", Center for Security Studies (CSS) (Juli 2024): https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSS_Cyberdefense_Report_Ukrainian_Way_of_Digital_Warfighting.pdf (Zugriff: 31.07. 2026).

Flexibilität für die Softwareentwickler:innen ermöglicht, ohne die sicherheitsrelevante Kerninfrastruktur preiszugeben.¹¹ Der Grundgedanke von Delta ist relativ simpel und aus der militärischen Notwendigkeit geboren: verschiedenste Daten- und Informationsquellen so niedrigschwellig wie möglich zu integrieren und zu teilen – unabhängig davon, ob die beteiligten Entwickler:innen aus staatlichen Stellen, NGOs oder der Zivilgesellschaft stammen.^{12 13}

Der Erfolg von Delta liegt genau hier begründet: Die einfache Zugänglichkeit, verbunden mit einer an moderne Alltagssoftware angelehnten Bedienbarkeit schafft eine hohe Nutzungsquote. Das System kann online und offline auf stationären Computern in Führungsstellen sowie in Fahrzeugen, aber auch auf Tablets oder Smartphones genutzt werden. Es wird wie eine handelsübliche App aufgespielt, benutzt und designt. Den Nutzer:innen stehen verschiedene Anwendungen und Funktionalitäten zur Verfügung, die ständig weiterentwickelt werden¹⁴. Im Zentrum des Systems steht Deltamonitor, eine interaktive Karte, die eigene und feindliche Positionen in Echtzeit anzeigt. Um dieses Kernmodul sind weitere Anwendungen gewachsen und in das System integriert worden.¹⁵ Dazu zählen unter anderem eine sichere Chat-Funktionalität oder Vezha, eine Videoanalyseplattform, die Drohnenfeeds in Echtzeit einspielt. Target Hub wiederum ermöglicht die Planung und den Einsatz kinetischer Wirkmittel; zugleich können darüber neue Ziele erstellt werden, die dann in Echtzeit ins System zurückgespielt werden. Ständig aktualisiert werden Informationen aus Satellitenbildern, Radar- und anderen Sensordaten, Geheimdienstinformationen aber auch Erkenntnisse, die aus der automatisierten Sichtung von Telegram-Kanälen gewonnen wurden.

DIE BUNDESWEHR: SYSTEMLANDSCHAFT, FÄHIGKEITEN, LÜCKEN

Die vernetzte Gefechtsführung, wie sie Delta jeden Tag in der Ukraine ermöglicht, setzt eine funktionsfähige digitale Infrastruktur voraus, die Daten aus verschiedenen Systemen und Teilstreitkräften in Echtzeit zusammenführen kann. Diese Voraussetzung fehlte der Bundeswehr lange: Sie hat historisch in jeder Teilstreitkraft eigene Führungsinformationssysteme entwickelt, die auf die spezifischen Anforderungen von Heer, Luftwaffe und Marine sowie des militärischen Nachrichtenwesens zugeschnitten waren. In einer Welt, in der die Teilstreitkräfte weitgehend nach eigenen operativen Logiken funktionierten, war diese Fragmentierung funktional. Sie ist es nicht mehr. Steigende Anforderungen an multinationale Einsatzführung, die rasante technologische Entwicklung und die zunehmende Vernetzung des Gefechtsfelds haben eine heterogene, nicht interoperable Systemlandschaft strukturell unhaltbar gemacht.

Deswegen startete die Bundeswehr 2012 das Programm Harmonisierte Führungsinformationssysteme der Streitkräfte (HaFIS). Ziel war eine einheitliche, teilstreitkräfteübergreifende Plattform für nationale und multinationale Einsätze, kompatibel mit NATO-Standards. HaFIS ist dabei ausdrücklich keine BMS-Applikation, sondern deren technische Voraussetzung: die Infrastrukturschicht, auf der die Daten der Teilstreitkraft-Systeme zusammengeführt und für eine übergreifende Führungsupplikation verfügbar gemacht werden.¹⁶

Auf Basis der HaFIS-Infrastruktur betreibt die Bundeswehr SitaWare als zentrales BMS – eine marktverfügbare Softwarelösung des dänischen Unternehmens Systematic, die von mehr als 30 Staaten und der NATO selbst genutzt wird. Die Einführung erfolgte schrittweise entlang der angebotenen Produktpalette von SitaWare: SitaWare Headquarters, entwickelt für größere Gefechtsstände, war das erste Produkt im Einsatz

- 11 Viktor Putrenko, Nataliia Pashynska, "Military situation awareness: Ukrainian experience," ACIG, vol. 3, no. 1, 2024: <https://www.acigjournal.com/pdf-190341-112702?filename=Military-Situation-Aware.pdf> (Zugriff: 31.07. 2026).
- 12 Stefan Soesanto, "The Ukrainian Way of Digital Warfighting. Volunteers, Applications, and Intelligence Sharing Platforms", Center for Security Studies (CSS) (Juli 2024): https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSS_Cyberdefense_Report_Ukrainian_Way_of_Digital_Warfighting.pdf (Zugriff: 31.07. 2026). S.49.
- 13 Kateryna Bondar, "How and Why Ukraine's Military Is Going Digital", Center for Strategic & International Studies (October 2025): https://csis-website-prod.s3.amazonaws.com/s3fs-public/2025-10/251006_Bondar_Military_Digital.pdf?VersionId=r49J5v0j6w9vC2XYafvbp6ve9GJEaBi (Zugriff 07.09.2026).
- 14 NATO Allied Command Transformation, "Battlefield Innovation: Ukraine's DELTA System Paves the Way for Allied Interoperability at CWIX24": <https://www.act.nato.int/article/delta-system-cwix/> (Zugriff: 31.07. 2026)
- 15 Kateryna Bondar, "Does Ukraine Already Have Functional CJADC2 Technology?", Center for Strategic & International Studies (Dezember 2024): https://csis-website-prod.s3.amazonaws.com/s3fs-public/2024-12/241211_Bondar_Ukraine%20CJADC2.pdf?VersionId=bxzcRKK_lmDJVz6xMtzeWwsmE2jkhcH5 (Zugriff: 31.07. 2026).
- 16 Bundesministerium der Verteidigung, "Zweiter Bericht zur Digitalen Transformation des Geschäftsbereichs des Bundesministeriums der Verteidigung, Teil 1, Berlin, März 2020": <https://www.bmvg.de/resource/blob/258260/cc60ba7e2570976df105baf97080fe45/20200312-download-zweiter-bericht-digitale-transformation-data.pdf> (Zugriff: 31.07. 2026).

und bereits vor 2019 in Betrieb, unter anderem im Einsatzführungskommando der Bundeswehr in Potsdam. 2019 fiel im Rahmen des Programms Digitalisierung landbasierter Operationen (D-LBO) die Beschaffungsentscheidung für SitaWare Frontline als BMS-Komponente für Gefechtsfahrzeuge des Heeres. Als erster Großverband erhielt die Panzergrenadierbrigade 37 das System, die 2023 die NATO-Speerspitze VJTF führte.¹⁷ Im September 2025 beschaffte die Bundeswehr eine Generallizenz für SitaWare Edge. Dabei handelt es sich um eine Android-Applikation für Soldat:innen auf handelsüblichen Mobilgeräten mit auf militärische Bedürfnisse zugeschnittener Nutzungsoberfläche. Parallel zur landbasierten Einführung wurde SitaWare auf die anderen Teilstreitkräfte ausgeweitet. Die Marine beschaffte 2023 maritime Erweiterungsmodule, die es ihren Führungsstellen ermöglichen, ein einheitliches maritimes Lagebild zu erstellen und mit land- und luftseitigen Kräften zu teilen.¹⁸ Die Luftwaffe entschied sich im Februar 2026 für die Einführung von SitaWare Headquarters, ohne dabei einen neuen Vertrag abschließen zu müssen, da auf die bestehende Generallizenz der Bundeswehr zurückgegriffen werden konnte.¹⁹ Seit Ende 2025 nutzt zudem der Sanitätsdienst mit SitaWare Battlefield Health eine eigens auf seine Anforderungen zugeschnittene Variante.

KONZEPT UND WIRKLICHKEIT: WARUM SITAWARE ALLEIN NICHT AUSREICHT

Betrachtet man die Systemlandschaft der Bundeswehr in ihrer Gesamtheit, ergibt sich auf dem Papier ein kohärentes Bild: SitaWare deckt konzeptionell alle Führungsebenen ab, vom Gefechtsstand bis zum einzelnen Soldaten, und ist, ähnlich wie das ukrainische Delta-System, als integrierender Layer über eine heterogene Systemlandschaft angelegt. Der entscheidende Unterschied liegt jedoch nicht in der Softwarearchitektur, sondern in deren Voraussetzungen und der Kultur, in der sie betrieben wird.

Technologie: Der Digitalisierungsgrad als Engpass

Die erste Lücke ist infrastruktureller Natur. Ein BMS kann nur aggregieren, was bereits digitalisiert und mit funktionierenden Schnittstellen versehen ist. Die

Einführung von SitaWare setzt einen bestimmten Digitalisierungsgrad aller im Verbund agierenden Einheiten und Systeme voraus, vom Radar über Drohnenfeeds bis hin zu Großwaffensystemen. Dieser Grad an Digitalisierung ist bisher bei der Bundeswehr nicht gegeben. Altgeräte ohne vernetzte Digitalisierungsfähigkeit bleiben strukturell außerhalb des Informationsverbunds, unabhängig davon, wie leistungsfähig das BMS selbst ist. Das „Shit in, shit out“-Prinzip gilt hier in seiner reinsten Form: Ein BMS ist nur so gut wie die Datenbasis, die es aggregiert. Solange die Einrüstung neuer und alter Hardware und die Digitalisierung bestehender Plattformen nicht abgeschlossen sind, bleibt das Lagebild, das SitaWare erzeugen kann, zwangsläufig lückenhaft.

Diese Erkenntnis, also stringente Standardisierung und offene, klar definierte Schnittstellen als zentrale Lehre aus der Ukraine, soll nun institutionell verankert werden. Das zeigt etwa die Etablierung der Zentralstelle MOSABw (Modular Open System Approach) im Beschaffungsamt BAAINBw, die eine größere Flexibilität und schnellere Integration verschiedener Waffensysteme sicherstellen soll. Das Ziel ist die Etablierung klar definierter Standards, um auch heterogene Systeme und Systemlandschaften erfolgreich zu integrieren und somit die Abhängigkeiten von einzelnen Herstellern mit proprietären Softwarelösungen zu reduzieren.²⁰

Rüstungspolitik: D-LBO Verzögerungen sind operationelles Risiko

Die zweite Lücke ist programmatischer Natur. SitaWare ist eingebettet in das Gesamtprogramm Digitalisierung landbasierter Operationen (D-LBO) – ein Rüstungsvorhaben der Bundeswehr mit einem Finanzvolumen von über 20 Milliarden Euro, bei dem es bereits zu massiven Verzögerungen gekommen ist. Hierbei handelt es sich nicht um ein reines Softwareprojekt, sondern um die Kombination zweier untrennbarer Komponenten: den Übertragungsmitteln (Funkgeräten, Satellitenverbindungen und Netzwerken) und den darauf aufsetzenden IT-Diensten, zu denen SitaWare als BMS-Anwendungsschicht gehört. Diese Architektur hat eine unmittelbare operative Konsequenz: Ein BMS ist nur so wirksam wie die Übertragungsinfrastruktur, auf der es läuft. Verzögerungen bei der physischen Einrüstung der Funkgeräte in Bestandsfahrzeuge sind daher keine

17 Dorothee Frank, „SitaWare Frontline – Das neue Battle Management System der Bundeswehr“ Europäische Sicherheit & Technik, 05.12.2019: <https://esut.de/2019/12/meldungen/ruestung2/16628/sitaware-frontline-das-neue-battle-management-system-der-bundeswehr/> (Zugriff: 31.07. 2026).

18 Europäische Sicherheit & Technik, „Marine wird mit Sitaware ausgestattet“: Europäische Sicherheit & Technik, 03.08.2023: esut.de/2023/08/meldungen/43745/marine-wird-mit-sitaware-ausgestattet/ (Zugriff: 31.07. 2026).

19 Hartpunkt, „Deutsche Luftwaffe führt Führungssoftware SitaWare ein“, hartpunkt, 04.02.2026: hartpunkt.de/deutsche-luftwaffe-fuehrt-fuehrungssoftware-sitaware-ein/ (Zugriff: 31.07. 2026).

20 Tobias Gürtler, „Bundeswehr richtet neue Drohnen-Zentralstelle ein“, Wirtschaftswoche, 10.07. 2026: <https://www.wiwo.de/unternehmen/industrie/usa-und-ukraine-als-vorbild-bundeswehr-richtet-neue-drohnen-zentralstelle-ein/100238891.html> (Zugriff: 31.07. 2026).

isolierten Beschaffungsprobleme, sondern direkt an die operative Nutzbarkeit des BMS gekoppelt. Die Verzögerung bei D-LBO bewirkt nicht nur einen Mangel an modernen Funkgeräten, sondern macht der Bundeswehr die zeitgemäße, verbundene Kriegführung aktuell unmöglich.

Kultur: Das digitale Mindset lässt sich nicht beschaffen

Die dritte und tiefste Lücke ist eine kulturelle. Moderne Softwareentwicklung ist kein einmaliger Beschaffungsvorgang, sondern ein zwingend kollaborativer, kontinuierlicher Prozess, der von Feedbackschleifen zwischen Entwickler:innen und Endnutzer:innen lebt²¹. Innovationen entstehen dabei nicht top-down aus Anforderungslisten, sondern bottom-up aus dem Realbetrieb. Wie die Ukraine zeigt, hängt die Wirksamkeit von Softwarelösungen im militärischen Kontext nicht primär von der Hardware ab, sondern von kontinuierlicher Systementwicklung unter Echtbedingungen, gelebter Mensch-Maschine-Kollaboration und der institutionellen Bereitschaft, schnell aus Fehlern zu lernen. Herkömmliche Beschaffungs- und Organisationsmodelle – ausgelegt auf statische, planbare Fähigkeiten – sind auf diese Realität strukturell nicht vorbereitet. In den meisten Streitkräften, auch der Bundeswehr, fehlen interdisziplinäre Strukturen, die Entwicklung, Adaption, Nutzer:innenfeedback und Anpassung in kurzen Zyklen verbinden.

DER WEG NACH VORNE

Erstens muss die Bundeswehr systematisch erheben, welche Systeme und Plattformen derzeit außerhalb des digitalen Informationsverbunds stehen, und einen verbindlichen Zeitplan zur Schließung dieser Lücken festlegen. Denn: Ein BMS aggregiert nur, was bereits digitalisiert ist bzw. über die Fähigkeit verfügt, überhaupt vernetzt zu sein. Die Zentralstelle MOSABw ist ein richtiger erster Schritt, muss jedoch mit den nötigen Befugnissen im Sinne einer konsequenten Durchsetzungsfähigkeit und politischer Rückendeckung gegenüber allen Zulieferern und Systemlieferanten der Bundeswehr ausgestattet werden, um offene Standards gegenüber Herstellern auch durchsetzen zu können und die Abhängigkeit von proprietären Systemlösungen konsequent zu verringern.

Zweitens muss D-LBO organisatorisch und institutionell auch aus der Truppe heraus als strategische Priorität behandelt werden: Die Verzögerungen bei der Funkgeräte-Einrüstung sind keine isolierten Beschaffungsprobleme, sondern blockieren direkt die operative Nutzbarkeit von SitaWare. Mit klaren Verantwortlichkeiten und einer konsequenten Priorisierung einsatzrelevanter Verbände muss hier Abhilfe geschaffen werden.

Drittens muss BMS-Kompetenz als nicht-auslagerbare Kernfähigkeit der Streitkräfte institutionell verankert werden: Wer das Betriebssystem seiner Streitkräfte nicht selbst versteht, und im Einsatz anpassen kann, verliert im Krisenfall die Kontrolle über seine eigene Operationsführung.

Viertens muss die Kooperation mit der Ukraine über diplomatische Absichtserklärungen hinausgehen und zu einem strukturierten institutionellen Austausch über agile Entwicklungsprozesse und Echtzeit-Nutzer:innenfeedback werden. Dies schließt die verstärkte Integration und Zusammenarbeit mit Akteur:innen der Zivilgesellschaft ein. Erfolgreiche Softwareentwicklung ist durch inkrementelle Fortschritte und ständige Feedbackloops geprägt und damit vor allem eine kulturelle Frage. Diese Lösung kann man nicht per Befehl verordnen, sie kann nur durch eine gelebte Innovationskultur auf allen Ebenen und Teilstreitkräften etabliert werden. Wo „Train as you fight“ nicht zum verbindlichen Entwicklungsparadigma wird, egal in welcher Domäne und auf welcher Ebene, wird „Computer sagt Nein“ die Standarderfahrung für die Bundeswehr im Ernstfall sein.

21. Guy Ward-Jackson, Keegan McBride, Elizabeth Segner, Laura Gilbert, Ott Velsberg, Jakob Mökander, "Open Source: How Middle Powers Can Build Influence in the Age of AI" Tony Blair Institute for Global Change, Februar 2026: <https://assets.ctfassets.net/75ila1cnaeah/1lktlktJiJxP6Wdl3adMom/8fee3bda39b670bb07a1c7209b74817e/6l2BX3wtN91ur2Sf5QcsP--140606022026> (Zugriff: 31.07.2026).



Advancing foreign policy. Since 1955.

Rauchstraße 17/18
10787 Berlin
Tel. +49 30 254231-0
info@dgap.org
www.dgap.org
[in @dgapev](#)

Die Deutsche Gesellschaft für Auswärtige Politik e.V. (DGAP) forscht und berät zu aktuellen Themen der deutschen und europäischen Außenpolitik. Dieser Text spiegelt die Meinung der Autorinnen und Autoren wider, nicht die der DGAP.

Die DGAP ist gefördert vom Auswärtigen Amt aufgrund eines Beschlusses des Deutschen Bundestages.

Herausgeber

Deutsche Gesellschaft für
Auswärtige Politik e.V.

ISSN 2198-5936

Redaktion DGAP

Layout Luise Rombach

Design Konzept WeDo

Fotos Autorinnen und Autoren © DGAP



Dieses Werk ist lizenziert unter einer Creative Commons Namensnennung – Nicht kommerziell – Keine Bearbeitungen 4.0 International Lizenz.