



Shape the future
with confidence

Software Defined Defense

Vom strategischen Paradigmenwechsel
zur Transformation
Februar 2025

■ ■ ■ ■
The better the question.
The better the answer.
The better the world works.



Defense in Zeiten
des rasanten techno-
logischen Wandels

SEITE 2

Was ist SDD?

SEITE 3

Was sind aktuelle
Herausforderungen
der Industrie?

SEITE 3

Wie kann SDD
umgesetzt werden?

SEITE 4

Was heißt das für Sie?

SEITE 6

Kontakte

SEITE 7

Defense in Zeiten des rasanten technologischen Wandels

Die sicherheitspolitische Lage hat sich seit Russlands völkerrechtswidrigem Angriff auf die Ukraine entscheidend verändert. NATO-Staaten wie Deutschland reagieren mit höheren Budgets, Modernisierungsprogrammen und neuen Konzepten, um die Verteidigungsfähigkeit zu stärken.

Die Landes- und Bündnisverteidigung (LV/BV) als Kernaufgabe der Bundeswehr ist somit wieder in den Fokus entsprechender Richtlinien gerückt.

Aktuelle und zukünftige Konfliktszenarien verlangen neben konventionellen Fähigkeiten den Einsatz neuer Technologien: künstliche Intelligenz (KI), Cybersecurity und unbemannte Systeme. Eine Schlüsselrolle spielt dabei, Software- und KI-basierte Fähigkeiten flexibel und schnell zu entwickeln und auszurollen. Das neue Paradigma Software Defined Defense (SDD) erfordert von Bundeswehr und Industrie eine grundlegende Transformation entlang der Lieferketten, um in Zeiten des rasanten technologischen Wandels nachhaltig erfolgreich zu sein.

Was ist SDD?

Das Geschehen in der Ukraine führt uns vor Augen, wie essenziell eine hohe Anpassungsfähigkeit ist. Digitale Verteidigungsstrategien sind innovations- und datengetrieben und es gilt, softwarebasierte Fähigkeiten innerhalb von Tagen, höchstens Wochen auszurollen. Dies ist der Kontext, in dem SDD erfolgskritisch ist.

In einer eng gefassten Definition beschreibt SDD die Beschleunigung militärischer Operationen und die schnellere Anpassung an neue Sicherheitsrisiken. Diese Agilität soll durch die Entwicklung neuer oder verbesserter Fähigkeiten mittels Software erreicht werden. Digitalisierung und Vernetzung sind dabei die zentralen Schlüsselwörter.

EY und IBM teilen die Auffassung, dass diese Definition von SDD zu kurz greift, da sie den zusätzlich zur Digitalisierung notwendigen Kulturwandel, die damit einhergehende Transformation, die Notwendigkeit einer Plattform und ein erweitertes Verständnis für unternehmensübergreifende Zusammenarbeit bei Bundeswehr und Industrie außer Acht lässt. Die Industrie ist gefordert, mit dem technologischen Wandel Schritt zu halten und sich angemessen für den Paradigmenwechsel aufzustellen. Es bedarf einer klaren Vision und einer weitreichenden Strategieanpassung, um die Vorteile des Wandels für sich zu nutzen.

Unsere Erfahrungen aus anderen Sektoren wie der Automobilindustrie zeigen, dass erfolgreiche Industrieakteure sogenannte Force Multipliers für sich nutzen. Ziel ist es dabei, durch einen gesteigerten Automatisierungsgrad Plattformen

schneller an veränderte Rahmenbedingungen anpassen zu können. Auch Edge- und IoT-Services sollen genutzt werden, um Technologie vernetzt und intelligent einzusetzen. Zusätzlich werden unternehmensübergreifende Partnerschaften geschlossen, um Innovationen zu stärken und in nicht differenzierenden Bereichen Skaleneffekte nutzen zu können.

Marktakteure mit ausgeprägten SDD-Kompetenzen werden wertvolle Partner für die Bundeswehr, vor allem bei der Entwicklung eines optimierten Fähigkeitsportfolios. Eine proaktive Herangehensweise an SDD ist der Schlüssel, um den Herausforderungen von heute und morgen erfolgreich zu begegnen.

Was sind aktuelle Herausforderungen der Industrie?

Nach einer langen Phase schrumpfender Verteidigungsausgaben und Innovationszyklen im Zeitlupentempo ist es nun eine der großen Herausforderungen des Sektors, neue Fähigkeiten zügig bereitzustellen und bedarfsgerecht weiterzuentwickeln. Das schließt den Auf- oder Ausbau leistungsfähiger Software und KI-gestützter Systeme nach den neuen Paradigmen von SDD ein. Diese wurden in Arbeitsgruppen der Verteidigungs- und Sicherheitsindustrie, des BDSV, des BDLI, des Bitkom und des BMVg erstellt und in einem entsprechenden Positionspapier festgehalten. Demnach betont SDD Anforderungen an System und Mensch wie zum Beispiel Interoperabilität, Vernetzung und Resilienz.

Neben der Optimierung vorhandener Güter sehen wir im Sektor u. a. folgende Herausforderungen:



Wie kann SDD umgesetzt werden?

Sowohl für die Bundeswehr als auch für die Industrie gilt es zunächst, das neue Paradigma SDD anzunehmen. Für Industrieakteure bedeutet dies, dass sie entlang der Wertschöpfungskette einen Transformationsweg beschreiten, auf dem Vernetzung, Digitalisierung, Interoperabilität und Agilität rapide gesteigert werden. Die rasante Entwicklung der Technologie steht im Kern der Transformation (*Technology@Speed*), während die Fokussierung der Wertschöpfung auf Kunden, Mitarbeitende und weitere Stakeholder zunimmt (*Humans@Center*). Es bedarf eines Ausbaus der Lieferketten, um Innovationen aus dem erweiterten Ökosystem zu integrieren, beispielsweise von IT-Systemhäusern und Start-ups (*Innovation@Scale*).

Dies umfasst eine Erweiterung und teilweise eine komplette Neuausrichtung des gegebenen Kompetenzspektrums, ganzheitlich betrachtet in den typischen Planungskategorien Produktion, Infrastruktur, Personal, Betrieb und Organisation, aber damit eben auch in Bereichen wie dimensionenübergreifender Strategie, Prozesse, Standards, Architekturen und Technologien.

Das Thema SDD ist nicht neu. Industrie und Bundeswehr sind bereits auf dem Weg. Wie jede Transformation ist jedoch auch dieser Veränderungsprozess nicht einfach. Starke Partner können auf diesem Weg maßgeblich unterstützen. Mit IBM als Vorreiter für die Nutzung exponentieller Technologien und EY mit seiner anerkannten Transformationsexpertise haben Unternehmen die Katalysatoren und Brückenbauer vom Ist zum erfolgreichen Soll an Ihrer Seite.

■ Exponentielle Force Multipliers nutzen

Exponentielle Force Multipliers sind Tools, Technologien und Strategien, mit denen Organisationen den Einsatz innovativer Technologien wie z. B. Cloud, KI, Automatisierung, Robotics, Internet of Things, Digital Twin, Edge Computing, Virtual Reality und Cybersecurity erheblich effektiver skalieren können. Sie wirken exponentiell, da sie umso stärkere Effekte generieren, je umfangreicher sie angewendet und eingesetzt werden. Netzwerkeffekte, Skalierung, Feedback-Schleifen und ineinandergreifende Innovationen tragen dazu bei. Die Nutzung von Kompetenzen innerhalb des erweiterten Ökosystems verstärkt die Transformation weiter. Die Wirkung richtet sich also nicht nur nach innen, sondern es wird auch ein exponentieller Mehrwert über das eigene Unternehmen hinaus erzielt.

Grundlage für eine Informations- und Wirkungsüberlegenheit sind qualitativ hochwertige Daten und deren KI-gestützte Analyse, Bewertung und softwarebasierte Nutzung. **Künstliche Intelligenz** ist einer der entscheidenden Faktoren für eine erfolgreiche Verteidigung geworden und spielt bei der Kompetenzerweiterung eine zentrale Rolle. Um diesen Force Multiplier nutzen zu können, ist eine effektive Governance über den gesamten Lebenszyklus von Daten und KI erforderlich. Zur erfolgreichen Umsetzung tragen außerdem Innovationsfähigkeit auf diesem sich rasant wandelnden Forschungsgebiet und die Weiterentwicklung von Kompetenzen in der Organisation bei.

Daneben wird die Befähigung zu SDD wesentlich durch die **Trennung von Hard- und Software**, die **Standardisierung von Hardware** und den schrittweisen **Umstieg auf eine modularisierte, containerbasierte Plattform** getrieben.

Standardisierte und skalierbare Softwarelösungen reduzieren die Komplexität, dienen der Wiederverwendung, erleichtern die Wartung und verbessern die Upgrade-Fähigkeit und Zusammenarbeit mit Bündnispartnern.

Die Sicherheitsanforderungen an die Cloud im Verteidigungssektor sind erhöht - Public-Cloud-Lösungen sind hier nicht in allen Fällen nutzbar. Eine geeignete **hybride Cloud-Strategie** ist erforderlich, um die Entwicklung in gesicherten Umgebungen nach den aktuellen Softwareentwicklungsparadigmen zu unterstützen. Dazu zählt insbesondere eine **Kubernetes-basierte Orchestrierung** der containerisierten Anwendungen.

Die Transformation hin zu cloudfähiger Software ist eine wichtige Grundlage für KI und SDD, um Agilität und Geschwindigkeit zu gewährleisten. Damit die Integration der Software in eine Verteidigungsplattform gelingt, ist eine industrialisierte Entwicklung auf der Basis von **Secure DevOps** erforderlich. Dazu sind Kulturveränderungen, die Einführung neuer Arbeitsweisen und die Etablierung einer durchgehenden technischen Softwareentwicklungsplattform notwendig. Wichtig ist dabei, die besonderen Anforderungen im Defense-Bereich zu beachten, z. B. im Bereich der Cybersecurity.

SDD kann nur dann erfolgreich sein, wenn die zugrunde liegenden Prozesse und Technologien auch in Zukunft sicher und funktionsfähig bleiben. **Cybersecurity** leistet einen wesentlichen Beitrag dazu. Damit dies ganzheitlich zum Tragen kommt, ist es erforderlich, dass dabei selbst KI genutzt wird, um sich gegen KI-gestützte Angriffe zu verteidigen zu können. Eine schnelle Updatefähigkeit zur Behebung von Cyberschwachstellen ist für SDD unabdingbar.

Das Beispiel Cybersecurity veranschaulicht die sich exponentiell verstärkenden Effekte von KI und Vernetzung, die es umfassend zu erschließen gilt. Entsprechend bedarf es eines ganzheitlichen Ausbaus von Kompetenzen, Technologien

und Arbeitsweisen der Organisation auf der Basis einer auf SDD ausgerichteten Kultur unter Berücksichtigung der spezifischen Gegebenheiten im Defense-Kontext und unter Erfüllung der gesetzlichen und operativen Anforderungen.

Force Multipliers spielen eine entscheidende Rolle bei der SDD-Transformation, da sie die operative Effizienz steigern, eine schnelle Entscheidungsfindung ermöglichen und die Auswirkungen des technologischen Fortschritts verstärken, um einen strategischen Vorteil zu erreichen.

■ **Managen der Transformation**

Die digitale Transformation entwickelt sich rasant. Unternehmen, die nicht auf aktuelle Herausforderungen reagieren, riskieren, hinter ihren Wettbewerbern zurückzubleiben. SDD ist nicht nur eine Lösung für diese aktuellen Herausforderungen, sondern auch ein zukunftsorientierter Ansatz. SDD unterstützt Unternehmen dabei, sich auf zukünftige Sicherheitsrisiken und Technologien vorzubereiten. Die frühzeitige Implementierung von SDD ist ein klarer **Wettbewerbsvorteil**.

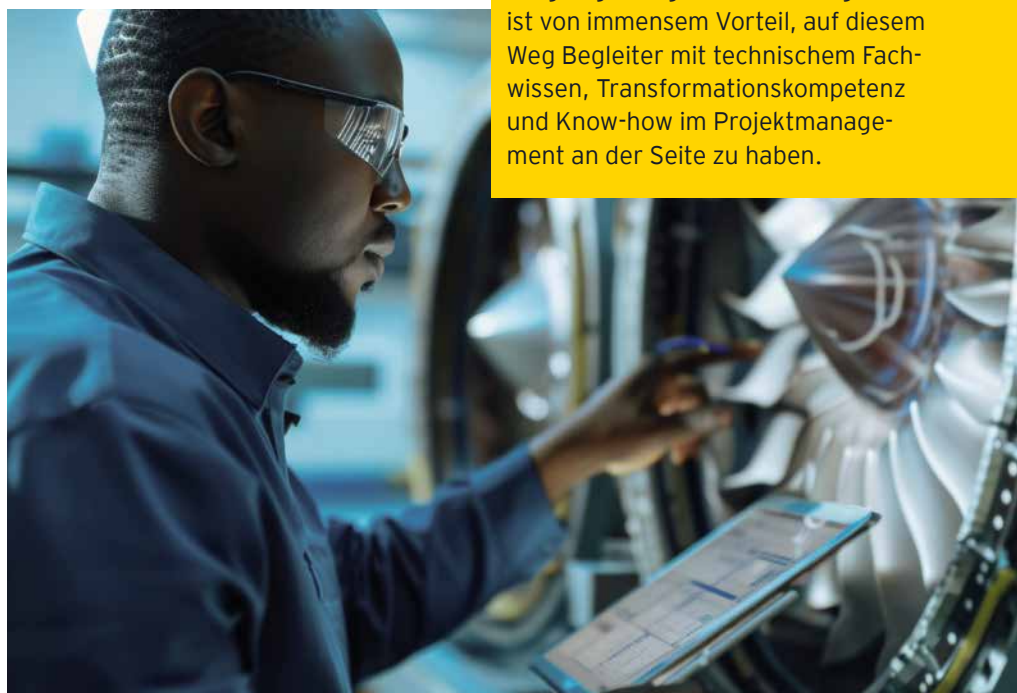
Als ersten Schritt zum Management der Transformation bedarf es einer Strategie und Vision. Daraus lassen sich klare Ziele ableiten, die wegweisend für die kommenden Veränderungen werden. SDD erfordert eine Neubetrachtung von Geschäfts- und Partnerschaftsmodellen, Prozessen und Handlungsoptionen für gezieltes Wachstum. Unternehmensstrategien innerhalb der Industrie variieren, doch mit SDD sind gewisse Anforderungen klar gesetzt. Beispielsweise ist eine grundlegende Digitalisierung und Automatisierung mit zwei Hauptzielen erforderlich:

A Optimierung der Produktentwicklung:
Für eine kundenzentrierte Verbesserung der Produktqualität und zur Effektivitätssteigerung sollten Produktportfolios angepasst und Automatisierungsmaßnahmen umgesetzt werden.

B Optimierung der Organisation:
Arbeitsprozesse sollten digitalisiert und automatisiert werden, einschließlich der gesamten Geschäfts- und Produktionsprozesse. Übergeordnetes Ziel ist hierbei die Effizienzsteigerung.

Die Arbeitsweisen der traditionellen Akteure im Verteidigungssektor unterscheiden sich in hohem Maße von jenen in der Softwareentwicklung. Für den Wandel zu SDD ist es jedoch erforderlich, dass sich sämtliche Akteure an die Entwicklungszyklen, Innovationsfreiräume und das agile Mindset der IT-Branche anpassen.

Innovationsfähigkeit ist für alle Beteiligten unerlässlich. Hieraus ergeben sich Herausforderungen in der Anpassung von Prozessen und im Management von Technologie und Personal.



SDD erfordert stetige Innovation
Innovationsmanagement ist ein zentraler Hebel aller Transformationsvorhaben. Für ein modernes Unternehmen im Verteidigungssektor gilt es, über die notwendigen technologischen Kompetenzen zu verfügen, diese weiter zu fördern und eine gezielte Steuerung von Projekten und Programmen sicherzustellen.

Gleichzeitig bedarf es eines Ausbrechens aus dem reinen Hardwaredenken hin zu Systemen entlang der gesamten Sensor-to-Effector Chain. Ziel ist eine kontinuierliche Entwicklung vernetzter und resilienter Systeme. Die Einführung agiler Prozesse fördert Effizienz und Innovationsgeist. Organisationen können zudem die Expertise des Defense-Ökosystems nutzen und gezielt Partnerschaften eingehen, um den Anforderungen nach mehr Vernetzung und Interoperabilität gerecht zu werden.

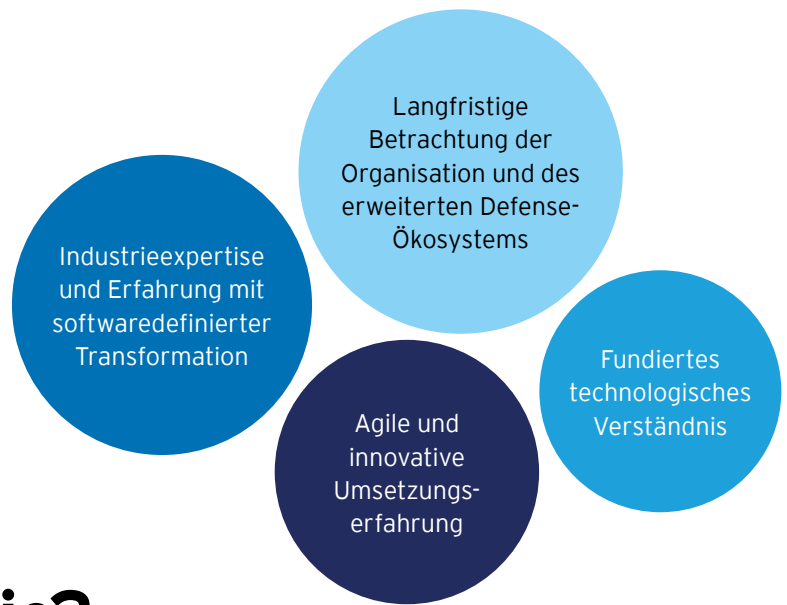
Die Zusammenarbeit in einem multi-sektoralen Ökosystem bringt jedoch Herausforderungen mit sich, z. B. in der Abstimmung verschiedener Interessen, bei Datenaustausch und Systeminteroperabilität, im Ressourcenmanagement und in der effektiven Kommunikation. Diese Herausforderungen gilt es gezielt zu managen. Es ist von immenssem Vorteil, auf diesem Weg Begleiter mit technischem Fachwissen, Transformationskompetenz und Know-how im Projektmanagement an der Seite zu haben.

“

Die Reise ist vorgezeichnet, aber es braucht einen Guide.

EY und IBM sind Vorreiter für die Nutzung exponentieller Technologien, anerkannte Transformationspartner und Cybersecurity-Profis.

Als Ihre Partner und Guides bringen wir Folgendes mit:



Was heißt das für Sie?

Um diese Reise mit einer klaren Richtung anzutreten und ganzheitliche Lösungen für aktuelle und künftige Herausforderungen zu finden, braucht es eine Standortbestimmung. Dabei helfen folgende Fragen:



Wo auch immer Sie auf dem Weg zur Transformation gerade stehen, wir bringen Sie den nächsten Schritt voran.

Sie haben Fragen dazu, was die SDD-Transformation für Sie bedeutet? Nehmen Sie Kontakt mit uns auf - wir beraten Sie gerne.

Kontakte



Holger Wilkens

Partner EY Technology Consulting,
Software Defined Defense Lead
holger.wilkens@de.ey.com



Andreas Frank

Partner EY Forensic,
Defense Lead Germany
andreas.h.frank@de.ey.com



Wolfgang Schneider

Senior Partner IBM Deutschland,
Leader Smart Multi Domain
Operations
wolfgang.schneider6@de.ibm.com



Dr. Stefan Mück

Distinguished Engineer
und Partner, CTO
stefan.mueck@de.ibm.com

EY | Building a better working world

Mit unserer Arbeit setzen wir uns für eine besser funktionierende Welt ein. Wir helfen unseren Kunden, Mitarbeitern und der Gesellschaft, langfristige Werte zu schaffen und das Vertrauen in die Kapitalmärkte zu stärken.

In mehr als 150 Ländern unterstützen wir unsere Kunden, verantwortungsvoll zu wachsen und den digitalen Wandel zu gestalten. Dabei setzen wir auf Diversität im Team sowie Daten und modernste Technologien in unseren Dienstleistungen.

Ob Assurance, Tax & Law, Strategy and Transactions oder Consulting: Unsere Teams stellen bessere Fragen, um neue und bessere Antworten auf die komplexen Herausforderungen unserer Zeit geben zu können.

„EY“ und „wir“ beziehen sich in dieser Publikation auf alle deutschen Mitgliedsunternehmen von Ernst & Young Global Limited (EYG). Jedes EYG-Mitgliedsunternehmen ist rechtlich selbstständig und unabhängig. Ernst & Young Global Limited ist eine Gesellschaft mit beschränkter Haftung nach englischem Recht und erbringt keine Leistungen für Mandanten. Informationen darüber, wie EY personenbezogene Daten sammelt und verwendet, sowie eine Beschreibung der Rechte, die Einzelpersonen gemäß der Datenschutzgesetzgebung haben, sind über ey.com/privacy verfügbar. Weitere Informationen zu unserer Organisation finden Sie unter ey.com.

In Deutschland finden Sie uns an 18 Standorten.

© 2025 EY Deutschland GmbH Wirtschaftsprüfungsgesellschaft
Steuerberatungsgesellschaft
All Rights Reserved.

Creative Design Germany | KKL 2502-1221
ED None

Diese Publikation ist lediglich als allgemeine, unverbindliche Information gedacht und kann daher nicht als Ersatz für eine detaillierte Recherche oder eine fachkundige Beratung oder Auskunft dienen. Es besteht kein Anspruch auf sachliche Richtigkeit, Vollständigkeit und/oder Aktualität. Jegliche Haftung seitens der Ernst & Young Consulting GmbH und/oder anderer Mitgliedsunternehmen der globalen EY-Organisation wird ausgeschlossen.

ey.com/de

IBM

is a trademark or registered trademark of IBM Corp.,
in the US or other countries or both.