SONDERAUSGABE
zum InfoBrief HEER 03/2024

Expertisebildung ist Zukunftsfähigkeit

Prof. Dr. (habil.) Beatrix Palt

Foto: Autorin

„Es gibt nichts Gutes, außer man tut es!" Dieses Zitat Erich Kästners schrieb mein Vater auf Seite eins meines Poesie-Albums als Leitbild und liebevollen Appell, immer das Beste zu geben.

Wir können nicht wählen, wann wir wo geboren sind: Genetik, Familie, Peer Group, Sozialisation, politische und sozio-ökonomische Umweltbedingungen. Erfahrungen und Umfeld prägen Glaubenssätze, Leitbild, Mindset, persönliche Dispositionen und Motivation: Was wird wie positiv oder negativ sanktioniert. Welche Schlüsse und Konsequenzen wir (persönlich) ziehen und welche Entwicklung, Haltung, Kraft und Mut wir wollen, haben wir indes selbst in der Hand. Kann, darf und will Expertise sich (aus)bilden. Wie und wofür brennt das Herz. Wann und wofür wird welche Expertise eingesetzt.

Als Resonanz auf meinen Artikel „Bauspiel – das Schiff" in zwei Wochen eine Sonderbeilage zusammenzustellen, die dafür steht, wie Mitspielende ihre Bausteine neu- und so zusammenzulegen, dass dieses Land ressourcensparend kaltstartfähig ist, passt zu Kästners verbrieftem Lebensmoto, dass Satiriker Schulmeister sind „und im verstecktesten Winkel ihres Herzens blüht schüchtern und trotz allem Unfug der Welt die törichte, unsinnige Hoffnung, daß die Menschen vielleicht doch ein wenig, ein ganz klein wenig besser werden könnten …"

Zeitenwende – dafür stehen alle Artikel in dieser Sonderbeilage – ist technologischer, politischer, personeller und persönlicher Musterbruch zugleich und in Gleichzeitigkeit. Menschen entwickeln Menschen. Menschen entwickeln Werte, Menschenbilder, Innovationen, Technologien, Projekte, Organisationen, politische und sozio-ökonomische Systeme und Lösungen die uns – nach neuestem Erkenntnisstand digital – siegfähig machen. Was wir können, wollen, dürfen und tun(!) ist von Menschenhand gemacht, muss jede und jeder für sich selbst und andere verantworten.

Diese Sonderbeilage zeichnet sich dadurch aus, dass Menschen können, wollen und tun, was Gebot der Stunde ist: vorwärtsstrategische Lösungen präsentieren. Die Beiträge zeigen, dass siegfähig ist, wer in Gleichzeitigkeit und Geschlossenheit Expertise(bildung) vom Design über Planung bis zum Betrieb beherrscht und vorausschauend einbezieht, was in der Forschung am Horizont erscheint. Das können wir – das zeigt dies Heft – zu einem plan, -realisier- und wartbaren disruptiv-modularen Baukastensystem zusammenbauen.

Die Funktion bestimmt die Form, das Wirkprinzip für Digitalisierung 4.0, verantwortlich unser gemeinsames Ziel zu erreichen: die Verteidigung unseres Menschenbildes und Menschenrechtsverständnisses. Ohne Vorgaben gemacht zu haben, zieht sich Geschlossenheit als roter Faden durch alle Artikel als Kompass, als neuer Vector, als kleine Schlepper, der das große Schiff, den ganzen Verband, zur Handlungsfähigkeit zieht.

Commitment ist die Klammer, die die Artikel, die Bausteine zusammen hält, aus einem Dialog- den Handlungsraum macht. Commitment ist Geschlossenheit, ist Zeitenwende, ist Verantwortung, ist Verbindlich- und Verlässlichkeit. Beherzt wird ab-, um- und neu gedacht und aufgebaut, was gewinnträchtig ist: Expertise(bildung) ist jetzt gelebte Zukunftsfähigkeit.

Ich danke allen „Schreiberlingen" dieser Sonderbeilage, die ich – jenseits von Dienstgraden, Titeln und Funktionen – als solche bezeichnen durfte, und ihren Teams. Danke dem FKH und Peter Tamm für Dein „Leinen los" uns diesen Handlungsspielraum zu geben. Danke an die Parlamentarische Staatssekretärin Siemtje Möller, sich dieses inspirierten Grüppchens anzunehmen und wohlwollend mit Ihrem engagierten Grußwort zu begleiten. Danke an Jens Elstermeier für diese herrlichen Fotos. Ich wette, noch nie hat jemand einen Verband gelegt.

Diese Sonderbeilage ist nicht nach Bereichen oder Schwerpunkten, sondern alphabetisch sortiert. Das führt dazu, dass mit „V" am Ende steht, wer Treiber für Software Defined Defence bei der Bundeswehr ist – wer da ankommen will, muss das gesamte Heft bis hinten lesen.

Beatrix Palt, Siemtje Möller, Peter Tamm, Christian Bock, Jens Elstermeier, Wolfgang Gäbelein, Guido Gerdemann, Michael Giss, Timo Haas, Reimund Igel, Felix Juhl, Markus Lehmann, Jörg Lorentzen, Harald Mannheim, Andreas Marlow, Beatrix Palt, Daniel Prenzel, Michael Vetter, Michael Volkmer

Foto: Ulf Duda

Liebe Leserinnen und Leser,

wir befinden uns am Beginn eines spannenden Wandels in der Verteidigungstechnologie: Die Digitalisierung hat in alle Gesellschaftsbereiche Einzug gehalten und führt zu großen Veränderungen und Fortschritten – auch bei der Bundeswehr. Von der Drohne über den Schützenpanzer bis zur Fregatte für quasi alle Plattformen nimmt die Bedeutung der Digitalisierung zu.

Die schnelle Entwicklung von Software sowie exponentiell zunehmende Rechenkapazitäten und Datenmengen beschleunigen das Voranschreiten und fördern eine zunehmende Disruptivität dieses Prozesses. Um auf einem Future Operating Environment bestehen zu können, ist die digitale Ertüchtigung sowie Vernetzung von Waffensystemen und Plattformen essenziell. Folglich steht für die Bundeswehr „Software Defined Defence" im Zentrum der Streitkräfteentwicklung.

Dabei verdeutlicht die Zeitenwende die Defizite und Herausforderungen der Bundeswehr bei der Digitalisierung – wir haben noch viel Arbeit vor uns. Vor diesem Hintergrund ist das Thema dieser Sonderausgabe, Sofware Defined Defence und der Aufbau einer entsprechenden Expertise besonders interessant.

Das Leitmotiv dieser Sonderausgabe, das „Bauspiel Schiff" der Bauhaus-Designerin Alma Siedhoff-Buscher ist ein kluger Denkanstoß. Der Baukasten kann zu verschiedensten Schiffen, aber auch einem Tor oder Tieren zusammengestellt werden und stellt somit die Kreativität und Innovationsfähigkeit des Menschen in den Mittelpunkt. Genau das braucht es, um die Fähigkeiten für ein Future Operating Systems auszubauen und gleichzeitig die Plattformen, Fähigkeitsträger und Waffensysteme zu entwickeln und an die Digitalisierung anzupassen. Eine immense Innovationsaufgabe, der wir unter Zeit-, Personal- und Ressourcenknappheit begegnen. Ausschließlich mit unseren konventionellen Rüstungs- und Planungsprozessen kommen wir hierbei an unsere Grenzen. Unkonventionelle Wege und Prozesse müssen entwickelt werden, die Expertise und Kreativität in den Mittelpunkt stellen.

Auch schafft das „Bauspiel Schiff" eine gedankliche maritime Brücke zu einem beeindruckenden Beispiel von disruptiver Innovationskraft: die ukrainischen Streitkräfte im Schwarzen Meer. Mit unkonventionellen, innovativen und oftmals in Garagen gebauten Lösungen schafft es die Ukraine die scheinbar übermächtige russische Schwarzmeerflotte in Schach zu halten, Einheiten zu versenken und in einen geografischen Bereich zurückzudrängen; etwas, das konventionell nur mit größeren Flottenverbänden geleistet werden kann. Die Lösungen und der Pragmatismus der Ukraine können natürlich nicht eins zu eins auf die Herausforderungen Deutschlands und der NATO übertragen werden. Das Beispiel zeigt jedoch die Kraft unkonventioneller Wege und sollte uns zu einem Musterbruch in Teilen der Innovations- und Beschaffungsprozesse inspirieren.

Ich freue mich über die verschiedenen Einblicke, Perspektiven und Denkanstöße der Autorinnen und Autoren. Mögen die Impulse und Ideen die Digitalisierung der Bundeswehr weiter vorantreiben!

Es grüßt Sie herzlich,
Siemtje Möller
Parlamentarische Staatssekretärin beim Bundesminister der Verteidigung

Foto: Autor

Resilienz setzt Werte und Handeln voraus

Peter Tamm

„Bauspiel – Ein Schiff" schlägt die maritime Brücke zur Innovationskraft und führt ins konkrete Handeln. Startpunkt war der Beitrag von Frau Professor Palt im InfoBrief Heer 2/24, der – überraschend für das Heer – seeseitig an Land kam.

Zukunftsfähigkeit jetzt funktioniert nur, wenn wir unsere Bauklötze, unsere Expertise(bildung) und uns als Handelnde ohne Wenn und Aber in immer wieder neuen Konstellationen zusammentun und Lösungen entwickeln, die sofort realisierbar und dennoch zukunftsfähig sind. Handeln im doppelten Wortsinn bedeutet zu tun, was notwendig ist, um siegfähig zu sein und dabei so zu handeln, dass unser Tun nachhaltig ist. Als Hamburger Kaufmann, Hamburg als maritimer Metropolregion, Tor zur Welt, Drehscheibe Logistik als größter Seehafen Deutschlands, der auf die Tugenden des Ehrbaren Kaufmanns und den Handschlag als Selbstverständnis und Leitbild setzt, gilt, dass „Anstand…die Grundlage für nachhaltigen Erfolg" bildet[1]. Nachhaltigkeit hat drei Dimensionen, so definierte die Brundtland-Kommission, drei Säulen, auf denen sie steht: Ökologie, Ökonomie und Gesellschaft sollen im Einklang verbunden sein[2]. Zeitenwende ist nicht auf Bundeswehr und Rüstungsindustrie beschränkt, sondern eine gesamtgesellschaftliche Aufgabe. Sie ist technologischer, politischer, sozioökonomischer und persönlicher Musterbruch, bei dem sich jede und jeder einzelne fragen muss: Wofür stehen wir als Wertegemeinschaft und welche Gesellschafts- und Geschäftsmodelle passen dazu. Der ehrbare Kaufmann, der als in Europa gewachsenes Leitbild für verantwortungsvolles Handeln steht, basiert auf einem humanistischen Menschenbild.

Diese Sonderbeilage ist als dimensionenübergreifendes zivil-militärisches Commitment als Reaktion auf „Bauspiel – Ein Schiff" quasi von alleine entstanden, weil Menschen in, für und aus Organisationen das Heft des Handelns in die Hand nehmen und Lösungen präsentieren, wie Zeitenwende aus dem Stand funktioniert. Niemand hat das erwartet. Es ist einfach passiert, weil ein inspiriertes Grüppchen sich auf den Weg gemacht, die Sonderbeilage sich verselbständigt hat: vom Dialogforum zum Handlungs(spiel)raum.

Diese Sonderausgabe ist aufgrund ihrer Stärke ein Musterbruch, die nicht nur in der Anzahl der Artikel und Seiten begründet liegt, sondern im Handeln an sich: Es handelt sich – alle Artikel zusammen genommen in der Draufschau – um einen übergreifenden, breit verwendbaren dimensionenübergreifenden Lösungsansatz, ein Manifest, ein „how-to", das aus einzelnen Bausteinen – den Artikeln – besteht, die auch einzeln in allen Dimensionen nutzbar sind: Forschungs- und wertebasiert legen die Autoren, die Menschen, die Kreativität und Innovationsfähigkeit des Menschen an den Tag: Der Mensch im Mittelpunkt der Lösung, der Mensch, der will und kann, als Lösung der Defizite in der Digitalisierung. Aufgezeigt wird, dass nur der Mensch in der Lage ist mit Pragmatismus Digitalisierung als Führungsaufgabe anzugehen und Kritische Infrastrukturen – auch Seewege – zu schützen: Expertise-basierte Resilienz als Gesamtstaatlicher Sicherheitsbegriff setzt Werte voraus.

Ich danke allen Autorinnen und Autoren und den dazugehörigen Teams dafür, dass sie mit ihren Beiträgen gezeigt haben, was geht: innerhalb von zwei Wochen diese Sonderbeilage hinzubekommen, ist eine ausgewiesene Demonstration unserer Stärke. Die Expertise ist da bei denen, die wollen und können, das Commitment zur Geschlossenheit bei Gleichzeitigkeit auch. Leinen los! Danke an den FKH, der diese Sonderbeilage fördert.

Fortsetzung folgt!

Gute Erkenntnisse und
viel Freude beim Lesen.

Ihr
Peter Tamm
Geschäftsführer
Mittler Report Verlag GmbH

1 Versammlung Ehrbarer Kaufleute zu Hamburg e.V., https://veek-hamburg.de/vision-und-mission/, Abruf am 25.05.2024.
2 Volker Hauff (Hrsg.) (1987). Unsere gemeinsame Zukunft : der Brundtland-Bericht der Weltkommission für Umwelt und Entwicklung. 1. Aufl. Eggenkamp: Greven, S. 46.

Foto: Bundeswehr

Mit Bauhaus zur Kriegstüchtigkeit? – Eine strategische Perspektive!

Flottillenadmiral Christian Bock

„Kriegstüchtigkeit" – die Bereitschaft sich verteidigen zu wollen und gewinnen zu können – ist eine Geisteshaltung, der Spirit, nicht nur von Streitkräften, sondern ganzer Gesellschaften. Sie findet im Kopf statt und übersetzt sich dann systemisch in entsprechendes Agieren von Organisationen.

Zur Gesamtverteidigung Deutschlands etabliert sich gerade eine nationale Strategielandschaft: Die Nationale Sicherheitsstrategie definiert die integrierte Verteidigung. Die Verteidigungspolitischen Richtlinien geben dem militärischen Teil der Gesamtverteidigung den Weg vor. Die fast wieder veraltete Konzeption Zivile Verteidigung von 2016 erklärt den nichtmilitärischen Part der Gesamtverteidigung, deren Defizite mit dem OPLAN DEU aktuell aufgezeigt werden. Eine „Militärstrategie der Bundeswehr" ist beauftragt. Sie soll dem „Geist der Kriegstüchtigkeit" in der Bundeswehr einen Rahmen geben. Genügt dies mit Blick auf „Integrierte Verteidigung"? Muss nur die Bundeswehr „kriegstüchtig" sein? Haben wir in Deutschland die strategische Expertise für ein agiles System, das Ziele bildet und adaptieren kann sowie zur Disruption fähig ist?

Erfahrungen aus Kriegen Dritter zeigen: höchste Not zwingt zum Aufgeben nicht kriegstüchtiger Prozesse und zum Eingehen von Risiken. Aus der Not wird Tugend, indem man zwingend besser, flexibler, adaptiver und innovativer ist als jeder Gegner. Der strategische Erfolg hängt davon ab, inwieweit die eigenen Handlungen nicht den Erwartungen des Gegners entsprechen und Dilemmata erzeugen. Das ist das Grundprinzip von Überraschung. Diese lebt vom Ausbrechen aus bewährten Mustern, gerade in Zeiten von KI, ohne die strategische Verlässlichkeit und Berechenbarkeit gegenüber Partnern zu vernachlässigen.

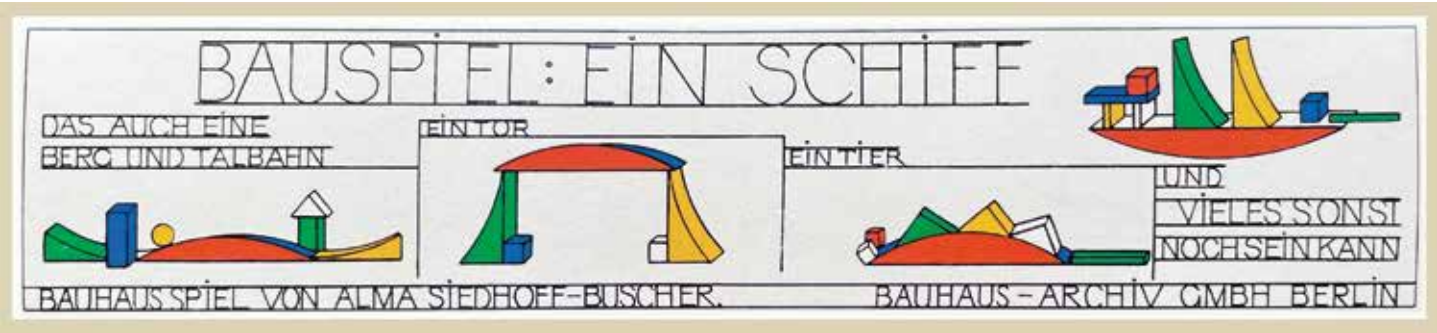
Kehren wir zuerst vor der eigenen Tür: Jahrzehntelang sozialisiert auf Kräfteabbau und durch Ressourcendefizite muss die Bundeswehr heute und künftig „gewinnen und agil agieren können" bei wechselnden Bedrohungslagen. Dies aber weiterhin mit begrenzten Mitteln und Personal. Wir wissen: bisherige Verfahren und Denkmuster der Vergangenheit sind unzureichend, um bei aktuellen Herausforderungen und höchsten Innovationsgeschwindigkeiten zu bestehen. Bewahren und Fatalismus sind dabei kein guter Ratgeber.

Als systemische Grundlage muss der Dreiklang „Expertise", „Spirit", „Gewinnen wollen" den Kern von Gesellschaften, Teams oder Kampfgemeinschaften bilden. Dies funktioniert nur, wenn das Ziel regelmäßig abgestimmt und im Bewusstsein verankert ist. Im idealen Zustand gibt das Ziel die Richtung und der Zweck die jeweilige Organisationsform vor. Entscheider bringen dann alle ihre maximal diverse sich gegenseitig ergänzende Expertise frei ein, finden neue Wege und entfalten Innovationsgeist. Basis sind Vertrauen, Kommunikations- und besondere Risikobereitschaft, sowie die Resilienz, mit Rückschlägen und Fehlern umgehen zu können, alles Prinzipien der Inneren Führung. Muss jeder so wirken können? Natürlich nicht! Muss jeder alles können und wissen? Natürlich auch das nicht! Es muss aber Expertiseträger auf jeder Ebene geben, die aus dem Zusammenwirken diverser Einzelteile, verschiedener Horizonte und Erfahrungen sowie unterschiedlicher Expertisen systemische Stärke erwachsen lassen. Solche Innovationscluster müssen traditionelle Muster brechen können.

Sinnbildlich für die Möglichkeit eines solchen adaptiven Vorgehens ist der Bauhausstil von 1919. Hier stehen der Nutzen des Produktes sowie der funktionale Einsatz der Materialien für das Produkt im Mittelpunkt. Einzelteile sind für spezifische Aufträge zielgerichtet zusammenzustellen und eingetretene Pfade zu verlassen, um sich an neue Lagen anzupassen oder gar neu zu gestalten – also das „Multi Domain Operations (MDO) – Konzept" der Architektur.

Auf den ersten Blick erscheint der Bauhausstil damit wie eine Patentlösung für das militärstrategische Problem, die Bundeswehr und Deutschland kriegstüchtig zu machen.

Bauhaus schafft Objekte für Kunst und Architektur, die nur für sich stehen. Militär aber handelt prinzipiell im-



Quelle: B. Palt

Bauspiel: Ein Schiff

mer im Zusammenhang mit anderen Akteuren, sei es im Gleichklang mit zivilen Ressorts und Bündnispartnern oder gegen militärische Gegner. Das strategische Problem ist somit weitaus komplexer als das Schaffen von Kunst oder Architektur.

Die gesamte Bundeswehr ist einer von vielen Teilbaukästen im Gesamtsystem der Integrierten Sicherheit Deutschlands. Die Einheiten der Bundeswehr sind die Einzelteile in diesem Kasten. Sie haben charakteristische Fähigkeiten und können zusammengestellt und kombiniert werden, um konkrete Funktionen bzw. konkrete Aufträge zu erfüllen.

Um alle zivilen und militärischen Teile der Bundeswehr zu einem „kriegstüchtigen" adaptiven Gesamtsystem flexibel entlang aller Aufgaben auszurichten, bedarf es nicht allein der „Militärstrategie der Bundeswehr", sondern auch der strategischen Expertise, also einer Kultur der „Strategen der Bundeswehr", die zum Musterbruch befähigt sind und dies auch dürfen!

In dem gleichzeitigem Verständnis, dass der Einsatz und Nutzen von Streitkräften nur komplementär und synchronisiert mit allen anderen Bereichen der Sicherheitspolitik funktioniert, bedarf es zwingend zusätzlich des interdisziplinären Expertiseaustauschs, eines tiefgreifenden Verständnisses der eigenen Fähigkeiten und Ziele sowie derer der Partner und der Gegner. Nur dann können Abschreckung und Verteidigung im ressortübergreifenden und gesamtgesellschaftlichen Handeln gelingen. Wie welche unterschiedlichen Ziele und Wirkungen in verschiedenen geostrategischen Räumen, sei es im Sahel, im Indopazifik oder gegenüber Russland flexibel und abgestuft eskalatorisch erzielt werden sollen oder können, muss auf Basis umfassender Expertise über gemeinsame Strategien erreicht werden. Hierbei sind kreatives Denken und auch unkonventionelles Handeln gefragt.

Auf „Integrierte Verteidigung" muss nicht nur die Bundeswehr, sondern die gesamte Gesellschaft ausgerichtet sein. Die strategische Kultur und Expertise für ein agiles System sind heute zu schaffen. Um den „Spirit der Kriegstüchtigkeit" zu entwickeln, muss die Bundeswehr als auch das politische System den „Musterbruch" systemisch fördern und solche Expertise ausprägen. Es gilt, strategische High Performance Teams zu bilden sowie Kreativräume und Experimentallabore zu schaffen, den Spirit auszutesten und zu -leben – sei es bundeswehrintern und mit anderen Playern. Dabei sind die Organisationsform und die Entscheidungsebene letztendlich unerheblich. Denn auch Funktionen wie ein „Nationaler Sicherheitsrat" oder ein „Generalstab" können nur solche Mehrwerte schaffen, die mit der vorhandenen Expertise, Diversität der Fachlichkeit und der Fähigkeit zum „Blick über den eigenen Tellerrand" und dem innovativen Freiheitsgrad der Mitglieder einhergehen.

Seit Jahrzehnten geben beispielsweise die Führungsakademie der Bundeswehr als auch die Bundesakademie für Sicherheit künftigen Entscheidern und Strategen der Zukunft Instrumente und Methoden zum Mitwirken, -denken und -innovieren an die Hand. Dort wird strategische Expertise in diversen zivil und militärischen High Performance Teams vermittelt. Deren Expertise kam immer nur so weit zur Geltung, wie dies die jeweils sozialisierten Strukturen, Prozesse und Vorgesetzten zuließen.

Jetzt gilt es darüber hinaus eine sicherheitspolitische „Strategische Kultur" in Deutschland zu entwickeln, welche „das Gewinnen können" in den Fokus nimmt und die bisherige Lehre in die Realität übersetzt! Den Expertise-„Laboren" müssen heute entscheidungs- und innovationsbefugte Expertiseorganisationen und -gremien folgen, die im Sinne der „Kriegstüchtigkeit" und der Gesamtverteidigung Deutschlands entscheiden können und dürfen. ■

Autor:

Flottillenadmiral Christian Bock ist Unterabteilungsleiter bei BMVg „MEO" zuständig für Militärstrategie und Einsätze Ausland. Er besitzt Expertise für Bundeswehrplanung, operativen Einsatz von Streitkräften, Militärpolitik sowie Ausbildung von Spitzenführungskräften aus diversen Verwendungen.

Foto: Autor

Software Defined Defence als Voraussetzung für dimensionsübergreifende Führungsfähigkeit

Jens Elstermeier

Paradigma: Software Defined Defence (SDD) ist die Voraussetzung dafür, zukünftig schnell genug auf veränderte Umgebungsbedingungen reagieren zu können, um so siegfähig zu bleiben.

These: Um SDD auf allen Ebenen innerhalb eines Waffensystems erreichen zu können, sind eine Schichtentrennung zwischen Plattform (z. B. Fahrzeug), Waffensystem, Führungssystem und Kommunikationssystemen sowie eine einheitliche, agile Methodik notwendig. Dabei sind für alle Schichten zum Beispiel Informationssicherheit, Life Cycle Management, Haftung, Akkreditierung, Vertragsmanagement, Schnittstellenmanagement schichtenspezifisch zu beachten.

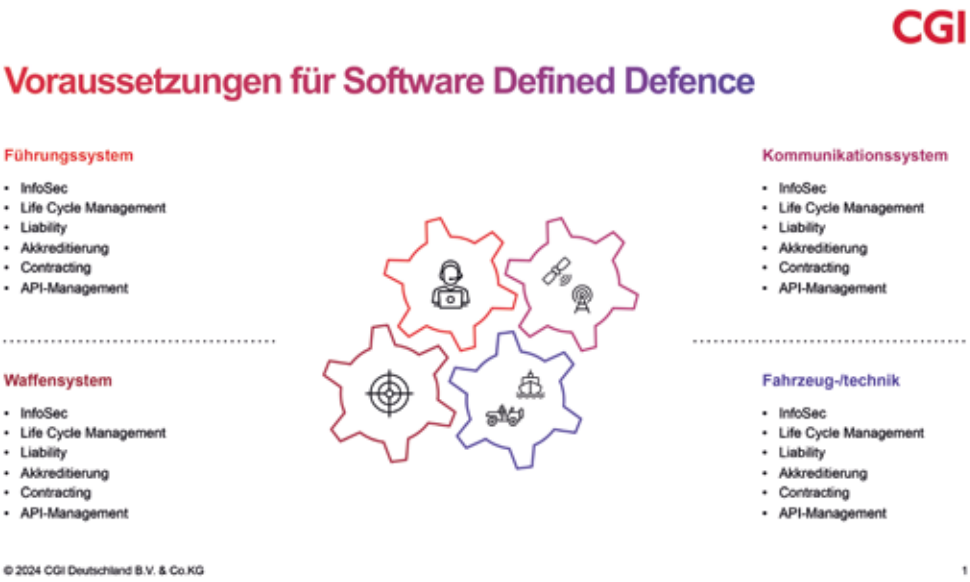
Fahrzeugtechnik, Waffensystem, Führungstechnik und Kommunikationstechnik müssen als einzelne, in sich geschlossene Subsysteme bereitgestellt werden.

Alle Zahnräder drehen sich dabei absehbar mit ihrer eigenen Geschwindigkeit, folgen ihrem eigenen Lebenszyklus. Die Besonderheit bei SDD ist aber die Anforderung an die Reaktionsgeschwindigkeit. Sie erfordert eine agile Herangehensweise auf allen Ebenen über den gesamten Lebenszyklus:

- Beschaffung
- Entwicklung
- Akkreditierung
- Betrieb

Dem einen oder anderen mag aufgefallen sein, dass sich die Zahnräder so aber noch nicht drehen können. Eine im wahrsten Sinne des Wortes zentrale Rolle spielt hier eine funktionierende Governance.

Diese regelt das Zusammenspiel in allen Bereichen, sowohl organisatorisch als auch technisch. Sie muss sowohl Aufbau- wie Ablauf-organisatorische Rahmenbedingungen schaffen, vertragliche Grundlagen z. B. für Haftung und Verwertungsrechte aufbauen als auch technische Regelungen wie Architekturvorgaben, Schnittstellenmanagement und Entwicklungsvorgaben aufzeigen.

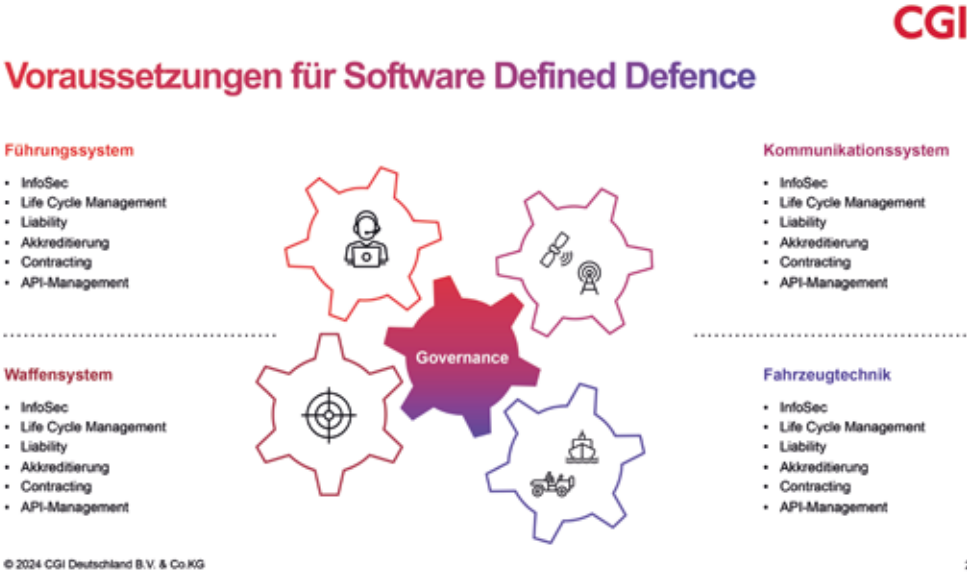


1

Um auf dieser Basis eine dimensionsübergreifende Führungsfähigkeit zu erzielen, braucht es ein Umdenken in der Technik – die z. B. von Generalleutnant Vetter, CIO im BMVg, zitierte „technologische Zeitenwende" –, aber genauso eine Zeitenwende in der Organisation und im Handeln aller beteiligten Organisationen: Bundeswehr, Beschaffung und Industrie.

Bleiben wir zunächst bei der Technik oder der technischen Zeitenwende. Um die Führungsfähigkeit der Zukunft zu erreichen, ist eine übergreifende Architektur über alle Systembestandteile hinweg zwingend erforderlich. Alle bisherigen Ansätze, ob Network Centric Warfare, NATO Network Enabled Capability (NNEC), Vernetzter Operationsführung (NetOpFü) oder Common Operational Picture (COP) sind an zum Zeitpunkt nicht verfügbarer Technologie oder mangelndem Willen gescheitert. Nun bieten marktverfügbare Technologien die technischen Grundlagen, über alle Dimensionen und alle Ausprägungen hinweg, und damit die Möglichkeit, durch zentrale Architekturvorgaben und die Bereitstellung eines Führungssystems für alle Dimensionen das Interoperabilitätsproblem zu lösen. Um die geforderte Anpassungsgeschwindigkeit zu erreichen und die betriebliche Komplexität zu minimieren, muss dieser Architekturansatz eine Lösung über alle Ausprägungen vom stationären Rechenzentrum über verlegefähige Hauptquartiere, Landfahrzeuge oder seegehende Einheiten bis zum mobilen Endgerät definieren. Da Deutschland nur im internationalen Verbund agieren wird, sind hier auch internationale Vorgaben, Standards und die Vereinbarungen zum Future Missi-

on Networking (FMN) zu berücksichtigen. Dabei kommt dem BMVg CIT und seinem nachgeordneten OrgBereich die Rolle zu, die Schichten Führungssystem und Kommunikationssystem zu spezifizieren und zentral für alle Projekte und alle Plattformen und Ausprägungen bereitzustellen. In der Praxis Bedarf es dazu auch der Durchsetzungsgewalt, individuelle Lösungen zu vermeiden, also einer Governance auf der Architekturebene, z. B. analog zur Design Authority im Office of the CTO der NATO Communications and Information Agency (NCIA) für die IT der NATO.



Eine zentrale Bereitstellung von Führungssystem und Kommunikationssystem ermöglicht auch von vornherein eine adäquate Berücksichtigung der daraus resultierenden Anforderungen an die Plattform, also z. B. ein Boot oder Schiff. Platzbedarf für die IT-Systeme, Kühlung und Stromversorgung müssen von Beginn an formbestimmende Kriterien sein, um auch zukünftigen Entwicklungen in der Software dauerhafte Integrationssicherheit zu garantieren.

Eine schnelle Anpassbarkeit an neue Umgebungsbedingungen erfordert eine agile Entwicklung und Weiterentwicklung in einem kontinuierlichen Prozess mit inhärenter Sicherheit: Development, security and operations (DevSecOps) – In kompetenten agilen Teams unter permanenter Beteiligung der Nutzer mit entsprechender Kenntnis und Entscheidungsbefugnis, um operative Anforderungen immer mitzudenken. Eine agile Entwicklung braucht eine moderne, cloudbasierte Entwicklungsumgebung, die diesen kontinuierlichen Prozess unterstützt, z. B. nach dem Vorbild der NATO Software Factory. Der generierte Code wird automatisiert getestet und integrierte Sicherheitsmechanismen ermöglichen einen kontinuierlichen, qualitätsgesicherten Prozess, der die Funktionalität Microservice-basiert in Containern bereitstellt. Diese können dann wiederum automatisiert durch Orchestration in verschiedene Sicherheitsdomänen auf verschiedenen Plattformen ausgerollt werden. Digitale Zwillinge bieten hier die Möglichkeit des Funktionsnachweises im Gesamtsystem im Zusammenspiel von Plattform, Waffensystem, Führungssystem und Kommunikationssystemen. Um dem Operateur vor Ort auch im Einsatz geforderte funktionale Erweiterungen bereitstellen zu können, ist sicherzustellen, dass die lokale Konfiguration zu jedem Zeitpunkt zu 100% bekannt ist. Damit ist eine lokale manuelle Konfiguration ein No-Go. Positiver Nebeneffekt: kein IT-Personal mehr vor Ort, außer für ggf. notwendigen Hardware-Tausch, Re-Start oder Auf- und Abbau.

Da es in einem solchen Entwicklungsprozess aber nun unmöglich ist, bei permanent erscheinenden Neuerungen in mindestens vier Schichten ein Gesamtsystem zu akkreditieren, bedarf es einer Akkreditierung des Prozesses, vergleichbar der Automobilindustrie. Schon in der Entwicklung werden durch akkreditierte Prozessschritte Services erstellt oder aktualisiert und getestet. Fertige Services werden als Template in einer „accredited container library" bereitgestellt und von dort durch geprüfte Orchestration-Mechanismen installiert. Die so entstehenden Gesamtsysteme erhalten dadurch automatisch die Zulassung, da der Prozess zugelassen ist. Auch das einzelne Auto durchläuft nicht jedes Mal eine individuelle Einzelzulassung, sondern das Baumuster und der Fertigungsprozess sind geprüft. Stichproben- oder Checksum-Tests des ausgerollten Systems sind natürlich möglich.

Allein mit der technischen Umsetzung ist es aber nicht getan, eine besondere Bedeutung kommt der Organisation – aber auch dem einzelnen Individuum – zu. Sowohl die Organisation muss sich agil ausrichten, um der zentralen Forderung der schnellen, iterativen „In Nutzung Bringung" gerecht zu werden, parallel dazu muss sich aber auch ein neues Vertrauensbewusstsein entwickeln, das auf gemeinsamer Erfahrung, persönlicher (intrinsischer) Motivation und einem klaren Fokus auf gemeinsame Zielerreichung beruht.

Schon im Beschaffungsprozess muss sich die geforderte Agilität in der Vertragsform niederschlagen. Nicht das Gewerk, vollständig und langwierig beschrieben, sondern es muss eine erste „Richtungsdefinition" definiert werden mit kurzfristig erreichbaren Zielen und der Möglichkeit, auch in Sackgassen abzubiegen und so zu lernen und Lösungsmöglichkeiten auszuschließen, um dann in möglichst kurzen Iterationen weitere Funktionalitäten zu liefern. Dauerhafte Service-Verträge mit Umfang oder „Story-Points" ohne Gewerkcharakter ermöglichen schnelles Reagieren auf neue Anforderungen im Betrieb. Eine zentrale Beistellung TSK-übergreifender Führungs- und Kommunikationssysteme erfordert auch die organisatorische Abbildung und Durchsetzungsfähigkeit sowie die zentrale Architekturverantwortung auf allen Ebenen, von CIT, über CIR, BAAINBw bis BWI.

Aber alle Teilstreitkräfte müssen auch personell/aufbauorganisatorisch einplanen, kompetentes und entscheidungsbefugtes Personal den Projekten auf allen Schichtebenen permanent beizustellen. Der permanente Austausch ist Grundgedanke agilen Vorgehens.

Auch die Betriebsorganisationen müssen sich am agilen Vorgehensmodell ausrichten, nicht nur technologisch, sondern in ihren organisatorischen Prozessen. Wie alle anderen Beteiligten aber auch im individuellen Miteinander von Nutzern, Beschaffern, Akkreditierern, Betreibern und Industrie – vertrauensvoll, zielorientiert, kompetent – spielerisch, bauspielerisch! ■

Autor:

Jens Elstermeier ist Leiter Geschäftsfeldentwicklung & Strategie, CGI Deutschland B.V. & Co.K

Foto: Bundeswehr

Software Defined Defence im Kontext von Multi Domain Operations

Unsere Herausforderungen erfordern neue Wege

Generalmajor Wolfgang Gäbelein

Zukunftsanalyse und Streitkräfteentwicklung setzen sich umfassend damit auseinander, wie künftige Kriege aussehen könnten und wie diese erfolgreich zu bestreiten wären. Es ist zwar nicht möglich die Zukunft vorherzusagen, Trendanalysen liefern jedoch Aussagen, welche Phänomene zu berücksichtigen sind. Daraus lassen sich Ableitungen treffen, wie mit den daraus resultierenden Folgen umzugehen wäre. Das gesamte Spektrum von technologischen – insbesondere Entwicklungen im Bereich von Künstlicher Intelligenz, bei unbemannten Systemen, in Verbindung mit Hyperschall oder auch Energiewaffen, wirtschaftlichen, sozialen, gesellschaftlichen oder politischen Entwicklungen ist dabei zu berücksichtigen.

Im Gefechtsfeld der Zukunft geht es u.a. um Geschwindigkeit, globale Reichweite, Vernetzung, Autonomie und beschleunigte Entscheidungsfindung. Es ist hyper, hybrid und total. Es besteht einen ungeheure Dynamik. Nebeneinander finden Aktionen in allen Bereichen statt und die gesamte Gesellschaft ist betroffen.

Der Blick auf den Krieg in der Ukraine, die Situation in Gaza sowie weltweit festzustellende hybride Aktionen zeigt, dass Teile dieser Charakteristika bereits heute auftreten. Die Vorbereitung auf das künftige Gefechtsfeld kann nicht auf die lange Bank geschoben werden. Gefordert ist die Befähigung für „Multi Domain Operations“ (MDO), als Operationen aus allen Dimensionen in alle Dimensionen unter Einbeziehung nichtmilitärischer Effekte.

Es ist nicht verwunderlich, dass sich zahlreiche Akteure in der Wissenschaft, der Industrie, den Streitkräften, ihren zivilen Äquivalenten und anderen Bereichen der Gesellschaft mit diesem Thema befassen – in den Partnerländern, aber auch bei den Konkurrenten.

Für die Bundeswehr ergeben sich bei der Herstellung der Befähigung für MDO zwei Herausforderungen. Einerseits müssen Lücken geschlossen werden, die aus Weichenstellungen der Vergangenheit und begrenzter Verfügbarkeit von Mitteln resultieren. Andererseits sind neue Fähigkeiten und neue Qualitäten zu schaffen. Dabei gibt es kein entweder oder. Es gilt insbesondere dem Faktor Zeit besonderen Stellenwert einzuräumen.

Das Potenzial von MDO zu erschließen fordert, in Effekten und weniger in Erbringungsdimensionen zu denken sowie eine Vielzahl von Effektoren, Führungsmitteln und Wirkmittel in einem Netzwerk miteinander zu verknüpfen. Die umfassende Digitalisierung liefert die Grundlage.

Alle künftigen Systeme müssen so gestaltet sein, dass sie netzwerkfähig sind. Sie müssen offene Architekturen besitzen und gemeinsamen Standards genügen. Doch auch vorhandene Systeme (legacy systems) lassen sich integrieren. Die IT-Technologien bieten weitreichende Möglichkeiten. KI-unterstützte Interfaces bieten das Potenzial, analog bereitstehende Daten zu digitalisieren, zu relevanten Informationen zu verarbeiten, in das Netzwerk einzuspeisen und so ein umfassendes Lagebild zu erzeugen. Gleichermaßen lassen sich unterschiedliche Effektoren anbinden. Software bekommt eine völlig neue Qualität. Der Begriff „software defined defence“ gewinnt damit die Qualität eines übergreifenden Ziels.

Die Dynamik im Bereich der Softwareentwicklung zwingt dazu deren bewährte Prinzipien zumindest in Teilen auch auf die Entwicklung von Waffensystemen zu übertragen. Dem Faktor Zeit trägt agiles Vorgehen Rechnung, bei dem ein klares, hinreichend abstraktes Ziel vorgegeben ist und die Detaillierung in definierten Entwicklungsschritten mit Zwischenzielen erfolgt. Der Rahmen durch das Dreieck Leistung – Zeit

– Kosten bleibt selbstverständlich weiter bestimmend. Das erfordert weiterentwickelte Managementverfahren, eine frühzeitige Entwicklungspartnerschaft zwischen Amtsseite und Industrie und vor allem die Bereitschaft, dem Entwicklungsteam ein hohes Maß an Freiheit einzuräumen und diesem Vertrauen entgegenzubringen. Oder anders ausgedrückt – auch bei dieser Form von Projektarbeit trägt das Prinzip „Führen mit Auftrag“. Es trägt nicht nur, es ist gefordert.

Mit schrittweisen Vorgehen erschließt sich eine weitere Möglichkeit. Es geht es darum, Fortschritte schnellstmöglich zur Wirkung zu bringen. Das bedeutet, ein neues System nicht erst dann für den Einsatz vorzusehen, wenn es die volle Leistungsfähigkeit erreicht hat, sondern bereits dann, wenn erste neue Fähigkeiten oder eine höhere Qualität bereitstehen. Das kann in einem ersten Ausrüstungsschritt mit einer zunächst begrenzten Stückzahl erfolgen. Weitere Ausrüstungsschritte liefern dann die beabsichtigten Leistungssteigerungen und die geforderte Quantität. Die Vorgehensweise trägt insbesondere dann, wenn neue Fähigkeiten des Systems über neue Softwarepakete, entsprechend einem „spiral development“, erzielt werden können. Die Konsequenz temporär mit unterschiedlichen Systemständen arbeiten zu müssen ist im Gesamtzusammenhang zu bewerten.

Wertvolle Beiträge liefern Experimente, insbesondere dann, wenn bestehende Systeme mit marktverfügbaren Systemen oder Komponenten ergänzt werden können. Es wird schnell deutlich, inwieweit in einem begrenzten Bereich die gewünschten Ziele erreicht werden. Deren Umsetzung muss konsequenterweise auch entsprechend zügig erfolgen. Dem trägt eine parallele Vorgehensweise Rechnung. Das bedeutet, zu einem frühen Zeitpunkt den Bedarf an Haushaltsmitteln in Form, einer Prognose einzusteuern, im Zuge des Experiments die bedarfs- und haushaltsbegründenden Dokumente zu erzeugen sowie früh zu entscheiden. Dass in dem einen oder anderen Fall die erwarteten Ergebnisse nicht erreicht werden, lässt sich nicht vermeiden. Scheitern muss erlaubt sein. Wichtig ist auf die Ursachen und weniger die Schuldigen zu blicken.

Bei der Vielzahl an Aktivitäten darf die Transparenz nicht auf der Strecke bleiben, insbesondere dann nicht, wenn es schnell gehen soll. Hierzu dienen Architekturen. Sie gestatten gleichsam wie in einem Bauplan allen Aktivitäten einen Platz zuzuweisen und deren Abhängigkeiten und Wechselwirkungen abzubilden. Architekturen sind auch für die zielgerichtete Steuerung unverzichtbar. Sie werden in dem Umfang detailliert, wie dies notwendig ist. Die Top-down-Betrachtung und die Bottom-up-Initiative stehen gleichberechtigt nebeneinander.

Digitalisierung und „software defined defence“ liefern nicht nur die Möglichkeit, neue Waffensysteme schneller zur Verfügung zu stellen, sondern insbesondere auch verfügbare Waffensysteme umfassender in Netzwerke zu integrieren. Jeder Schritt trägt zur Resilienz des Netzwerks bei und steigert die Qualität. Die Voraussetzungen zur Erschließung der Potenziale sind gegeben. Es erfordert allerdings Mut, die notwendigen Schritte zu gehen und die zweifelsohne vorhandenen Risiken in Kauf zu nehmen. Ebenso wichtig ist Vertrauen zu gewähren und auf Mikromanagement und Absicherungsdenken zu verzichten. Doch in letzter Konsequenz führt mit Blick auf die erfolgreiche Gestaltung der Zukunft an frühzeitigen Entscheidungen, die Spielräume zulassen, schrittweisem Vorgehen und parallelisiertem Handeln kein Weg vorbei. ■

Autor:

Generalmajor Wolfgang Gäbelein ist Amtschef des Planungsamtes der Bundeswehr in Berlin

Foto: Autor

Der Schutz kritischer Infrastrukturen als Design- und Planungsanforderung

Guido Gerdemann

Wir leben momentan in einer Zeit, die geprägt ist von einer veränderten Sicherheitslage, neuen geopolitischen Herausforderungen und Bedrohungen. Das ist eine Binse. Aber welche Konsequenzen hat dies Binse eigentlich konkret für uns als Bundesrepublik Deutschland, als Mitglied von Verteidigungs- und Wertebündnissen? Wie gehen wir in (naher) Zukunft mit diesen Herausforderungen um? Wieviel Zeit („Zeit ist ein Wert an sich geworden", Vizeadmiral Stawitzki, Abteilungsleiter Rüstung im Bundesministerium der Verteidigung, auf dem 25. DWT Marineworkshop) bleibt uns noch und was können wir finanzieren? Wie schaffen wir es die Landes- und Bündnisverteidigung, die Abwehr hybrider Bedrohungen und den Schutz der (maritimen) kritischen Infrastruktur koordiniert zu organisieren? Wie trennscharf können äußere und innere Sicherheit in Verbindung mit dem zuvor genannten noch betrachtet werden?

An dieser Stelle bedarf es neuer ganzheitlicher Ansätze und Herangehensweisen, bisherige Denk- und Vorgehensmuster müssen ggf. aufgebrochen werden, ergänzt oder gänzlich ersetzt werden. Dann kann es gelingen im Rahmen der knappen Ressourcen Zeit, Geld und Personal auch in Zukunft erfolgreich den neuen Herausforderungen zu begegnen.

Der Schutz (maritimer) kritischer Infrastrukturen beinhaltet die Absicherung von Wirkplattformen und die Absicherung dimensionenübergreifender Verbände bemannt / unbemannt in einer resilienten Military Combat Cloud (MCC). Dazu bedarf es veränderter, software-designed Herangehensweisen: die Funktion bestimmt die Form, und zwar nicht nur für einzelne Wirkplattformen, sondern für die gesamte MCC, die vom Ende her gedacht, bei Design und Planung beginnt. „Bauspiel – das Schiff" ist mehr als das Design einer Wirkplattform nach dem Wirkprinzip. Es ist ein disruptives modulares Baukastensystem, das vom Design über Planung und Betrieb bis hin zur Regeneration von beiden Enden aus zu betrachten ist: Von der MCC auf „das Schiff" (als Synonym für einen maritimen Fähigkeitsträger) und umgekehrt vom Schiff auf die MCC.

Die Aussagen des Inspekteurs der Marine Admiral Kaack kürzlich im Interview mit der DPA ernst zu nehmen heißt mit dem Rüstzeug, d.h. unter Einsatz der verfügbaren Mittel (Zeit, Geld, vor allem aber Personal) aufwarten zu können, um schneller und gleichzeitig besser zu sein. Das erfordert Expertise(-bildung), weil Menschen für (ihre) Entwicklung und den Einsatz ihrer Ressourcen verantwortlich sind. Expertise ist Können. Können setzt (persönliches) Wollen und (systembedingtes) Dürfen voraus. Dieser Artikel diskutiert drei Paradigmenwechsel als Konsequenzen aus „Bauspiel – das Schiff" als Design- und Planungsanforderung aus marinespezifischer Sicht. Ziel ist die sichere, resiliente MCC, die multifunktional der Sicherung von Verbänden und kritischen Infrastrukturen dient und daher den zivilen maritimen Bereich konsequenterweise einbezieht. Denn am Ende geht es (auch) um die Bündelung zivil-militärischer Kräfte und gemeinsame Expertise(bildung).

Paradigmenwechsel – Absicherung von Marineschiffen als Teil TSK-übergreifender Verbände und umgekehrt

Anschläge und Ausspähungen kritischer Infrastruktur im NATO-Gebiet erhöhen die Notwendigkeit des Schutzes der Unterwasser-Infrastruktur (Pipelines, Strom- und Datenkabel). Nicht zuletzt die Auswertung des Einsatzes der Fregatte Hessen verdeutlicht, dass Fähigkeitsträger der Marine schwimmende Rechenzentren sind, digitale Wirkplattformen mit TSK-übergreifenden Fähigkeiten der Verbandsflugabwehr und des Gebietsschutzes bemannt / unbemannt, überwasser / unterwasser inklusive Resilienz gegenüber physikalischen, hybriden und Cyberangriffen.

Maritime Fähigkeitsträger wurden in der Regel aus der Sicht der Formvorgabe (Seegebiet, Stehzeit, Klasse, Bewaffnung, Reichweite etc.) – nicht aber aus der Sicht der dimensionenübergreifenden Einsatz- und Führungsfähigkeit entworfen, geprägt durch die allseitige Fokussierung auf TSK und Abteilungen, sowohl amtsseitig als auch bei der Industrie. Der gemeinsame Einsatz ändert die Anforderungen an die Wirkplattformen. Verteilung von Risiko, Wirkung, Gewicht, Schnelligkeit, Kosten und Komplexität werden angepeilt. Dezentralisierung ist angesagt, um schneller, flexibler und kostengünstiger zu sein. Entscheidend sind Wirkung, Resilienz und Sicherung des Verbands zur Absicherung der Wirkplattform selbst und von Verbänden als quasi Teil kritischer Infrastruktur nach außen und innen – damit nicht die (manipulierte) Kaffeemaschine auf der Fregatte ein Desaster auslösen kann. Dies bedarf Änderungen in Design und Planung, weil berücksichtigt werden muss, welche Technologie verbaut und wie offen und (un-) berechenbar Schnittstellen bzw. Black Boxes sind. Um also domänenübergreifende Führungsfähigkeiten in Wirkketten – und -Netze zu bringen, ist IT Design-Autorität zwingend erforderlich. Marinespezifische Untersuchungen / Analysen bestehender und zukünftiger Fähigkeitsträger Überwasser und Unterwasser (bemannt und / oder autonom) in Bezug auf Verwundbarkeit der Systeme durch Cyberangriffe aufgrund der verbauten Komponenten müssen durch die interne Analyse der einzelnen Systeme in Hinblick auf die Verwundbarkeit ergänzt werden. Auch die Verwundbarkeit der Kommunikationslinien innerhalb eines Verbands (Lagebildaufbau) sollte detailliert analysiert werden, insbesondere vor dem Hintergrund der im Zielbild Marine 2035+ skizzierten autonomen Wirkmittel (FCSS). Man stelle sich vor, es gelingt einem Angreifer, einen solchen Fähigkeitsträger zu übernehmen und gegen die eigenen Einheiten einzusetzen / wirken zu lassen.

Paradigmenwechsel – Vom zivilen maritimen Bereich zur zivil-militärischen Zusammenarbeit

Der Koordinierungsverbund Küstenwache: Vier Bundesministerien (BMI, BMDV, BMF, BMEL) mit jeweils einer eigenen Behörde (Bundespolizei See, Generaldirektion Wasserstraßen und Schifffahrt, Zoll See, Bundesanstalt für Landwirtschaft und Ernährung) nehmen mit Einsatzkräften und Fähigkeitsträgern an der Gemeinschaftsaufgabe Küstenwache teil. Besonders die Bundespolizei See ist in diesem Zusammenhang mit ihren grenz- und allgemeinpolizeilichen Aufgaben als Anknüpfpunkt herauszuheben. Das Netzwerk des Maritimen Sicherheitszentrums (MSZ) und des Gemeinsamen Lagezentrums See (GLZS) in Cuxhaven gewährt Zugang zu allen maritimen Kompetenzträgern auf Bundesebene (Küstenwache, Marine, Havariekommando) sowie den Wasserschutzpolizeien der Küstenbundesländer. Diese Zusammenarbeit muss zukünftig intensiviert und vertieft werden, Informationen bruchfreier geteilt und verfügbar gemacht werden.

Daraus ergeben sich Anknüpfpunkte im Bereich der maritimen kritischen Infrastruktur (Pipelines, Seekabel, Off-Shore-Windparks), deren Sicherheit vorrangig in Verantwortlichkeit der jeweiligen Eigentümer / Betreiber liegt sowie die Potenziale im Deutschen Katastrophenschutz wie beispielsweise Risikoanalysen des BBK. Vor diesem Hintergrund wird auch das neue KRITIS-Dachgesetz Forderungen an turnusmäßige Risikoanalysen und -bewertungen von Betreibern Kritischer Infrastruktur, dem BBK sowie KRITIS-verantwortlichen Ministerien verlangen. Ressourcensimulationen, Übungen und Planspiele mit (vor Design und Planung simulierten) digitalen Zwillingen könnten vor allem im Kontext der Überwachung / Absicherung der maritimen kritischen Infrastruktur Zeit und Kosten sparen. Erfahrungen aus der Teilnahme an (NATO-)Übungen (z. B. REPMUS) können für die Erstellung von Konzepten zur Überwachung / Absicherung maritimer kritischer Infrastruktur genutzt werden. Ein durchgängiges und möglichst aktuelles Lagebild vom Weltraum bis auf den Meeresboden ist hier zwingend Voraussetzung. Insbesondere der Bereich Unterwasser(-Akustik) mit seinen speziellen Bedingungen bietet unter Nutzung von AI-unterstützter Auswertung von Massendaten viel Potential für Innovationen. Dies umfasst auch die Unterwasser-Überwachung von Häfen und Hafenanlagen mit ihren in Bezug auf die Unterwasser-Akustik besonders herausfordernden Bedingungen.

Paradigmenwechsel – Partnerschaften zur Absicherung (regionaler) kritischer Infrastruktur

Böswillige Aktionen anderer Staaten z.B. durch Cyberangriffe oder auch nur die Einschränkung der Kommunikation gefährden lokal, regional oder gar national die (Digitale) Nationale Souveränität. Nicht mehr nur einzelne Firmen oder Branchen sind das Ziel von dedizierten Cyberangriffen, Desinformationskampagnen oder hybrider Kriegsführung, sondern Bundesländer und Deutschland als logistische Drehscheibe im Fall der Landes- und Bündnisverteidigung. Besonders Metropolregionen wie z. B. Hamburg mit seinem Hafen (mit zivil-militärischem Schiffbau), dem Flughafen, dem Airbus Werk, dem „Nadelöhr“ Elbquerung und einem Bundeswehrkrankenhaus stellen ein lohnendes Angriffsziel und somit besonderes Sicherheitsrisiko dar. Für das Vorsorge- und Notfallmanagement kritischer Infrastrukturen bedarf es Partnerschaften. So ist die z. B. Zusammenarbeit mit dem nationalen Netzbetreiber erforderlich, da nur der Inhaber der technischen Infrastruktur durch einen gesondert gehärteten Internet-Verkehr zu einer belastbaren und wirkungsvollen strategischen Resilienz im Cyberspace verhelfen kann.

Aber nicht nur das. Partnerschaften, verlässliche und vertrauensvolle Partnerschaften sind in Zukunft unverzichtbar, wenn wir den neuen Herausforderungen und Bedrohungen erfolgreich begegnen wollen. Diese Partnerschaften umfassen dabei das gesamte Spektrum der beteiligten Akteure, angefangen von staatlichen Institutionen über die Industrie bis hinein in die Forschung und Wissenschaft.

Autor:

Guido Gerdemann ist Geschäftsführer bei MTG Marinetechnik GmbH

Foto: Autor

Kritische Infrastrukturen (KRITIS) und Software Defined Defence

Kapitän zur See Michael Giss

Die Zeitenwende kommt langsam an. Dennoch gibt es noch sehr viel zu tun. Insbesondere wenn es um die harte Umsetzung vor Ort geht, müssen wir uns ehrlich machen. Denn vieles, was in der Theorie gut aussieht, wird bei näherem Hinsehen komplizierter als gedacht. Software Defined Defense kann uns Prinzipien an die Hand geben, um auch im Bereich der territorialen Strukturen neu zu denken und voranzukommen.

Mit dem vollständigen Angriff Russlands im Jahr 2022 haben sich die Grundlagen für die Bundeswehr geändert. Die notwendigen Veränderungsprozesse sind eingeleitet und wirken sich nunmehr auch in der Fläche aus. Der Spannungs oder Verteidigungsfall wird sich zugegebenermaßen drastisch auswirken, sollte er jemals eintreten. Aus meiner Sicht als Kommandeur Landeskommando Hamburg ist ein solches Szenario gefühlt noch weit weg, realistisch gesehen allerdings auf der Zeitachse durchaus eher möglich, als wir alle es uns vorstellen. Ich bin davon überzeugt, dass wir innerhalb der nächsten 10 Jahre vor einer Herausforderung stehen, die einen solchen Fall nach sich ziehen wird.

Die einfache Frage, die sich mir jeden Tag stellt, ist: „Sind wir auf diese Herausforderungen vorbereitet?"

Und derzeit muss ich aus meiner Sichtweise sagen: "Das sind wir nicht!"

Eine Herausforderung ist bereits jetzt deutlich spürbar: die allgegenwärtige hybride Bedrohung. Insbesondere in Hamburg sehen wir Auswirkungen dieser Bedrohung nahezu täglich. Cyberangriffe und Störungen reihen sich in immer kürzeren Abständen aneinander. Erst sind es Angriffe auf die Dateninfrastruktur des Hafens, dann brennen z.B. Kabelschächte der Hafenbahn – nicht immer sind die Hintergründe deutlich beweisbar. Dennoch sind in einigen Fällen die Akteure zumindest erkennbar: Iran, Russland und andere. Eine umfassende Digitalisierung der Gesellschaft macht es den Akteuren einfacher, die notwendigen Einfallstore zu finden.

Der Hafen als kritische Infrastruktur im Rahmen Drehscheibe Deutschland

Wir stehen vor der Herausforderung, bei einem Spannungs- oder Bündnisfall mit dem Hafen Hamburg und dem Flughafen eine sehr fähige, aber auch kritische Infrastruktur (KRITIS) in Hamburg betreiben und sichern zu müssen. Es geht darum, mehrere hundert Tonnen Nachschub täglich umschlagen zu können und so den riesigen Hunger eines NATO-Feldheeres an einer Ostflanke zu decken. Das ist nicht ganz trivial, denn bereits jetzt sind die möglichen digitalen und analogen Angriffsflächen europaweit bekannt. Ein Containerschiff quer im Elbfahrwasser, eine Zerstörung von Weichenanlagen der Hafenbahn oder eine Beschädigung der Köhlbrandbrücke – alles Fälle, in denen sich innerhalb weniger Stunden ein Problem für die Lieferketten auftut. Bereits jetzt ist das eine große Herausforderung für die europäische Wirtschaft, der sich z.B. die Hamburg Port
Authority oder die Polizei umfassend stellt. Im Spannungs- und Verteidigungsfall würde diese Aufgabe darüber hinaus dem Heimatschutz zukommen, der noch meinem Kommando untersteht.

Im Fall einer Eskalation der hybriden Bedrohungen, zum Beispiel durch umfassende Sabotage an kritischer Infrastruktur oder zum Beispiel durch Aufwiegelung von Minderheiten, würde es dazu kommen, dass wir militärische Kräfte zur Absicherung kritischer Infrastruktur einsetzen müssen – und das umfangreich und kurzfristig. Schließlich kündigen sich hybride Eskalationen nicht unbedingt an – sie passieren einfach und wir müssen reagieren. Die Drehscheibe Deutschland wird also bereits vor Eintritt des schlimmsten Falles zu sichern sein. Dabei stehen wir vor der Herausforderung, dass wir voraussichtlich 40 Brigaden oder mehr durch Deutschland schleusen müssen – darunter ein großer Anteil auch durch Hamburg. Hier wirkt sich der OPLAN Deutschland, den wir derzeit mit den Behörden im Bundesland umsetzen, deutlich aus.

Wenn ich KRITIS in Hamburg anschaue, deren Übersicht, Pflege, Absicherung und nicht zuletzt Überwachung seit der Wende 1990 immer weiter dezentralisiert und abgegeben wurde, dann zeigen sich noch größere Probleme. Um hier die schieren Datenmengen überhaupt verarbeiten zu können, braucht

es künstliche Intelligenz. Das gleiche gilt für das militärische Lagebild im Bundesland, welches ich mit meinem Stab erstellen soll. Hierfür brauchen wir eine eigene Sentiment-Analyse durch künstliche Intelligenz, welche die unfassbaren Datenmengen analysiert und vorauswertet zur Verfügung stellt, um mir ein realistisches, eigenes, militärisches Bild zu ermöglichen.

Zu allerletzt fehlen mir bereits jetzt ausreichend Kräfte, um eine Sicherung der kritischen Infrastruktur überhaupt gewährleisten zu können. Diese Kräfte werden ab dem 01.04.2025 dem Heer unterstellt. Das bedeutet, dass wir als Landeskommando Hamburg den Schutz von kritischer Infrastruktur nicht mit eigenen Kräften, den Heimatschützern aus der Region, sicherstellen können, sondern auf die Zuweisung von Kräften aus dem Heer angewiesen sind.

Chancen für die Gesamtverteidigung

Eine umfassende Digitalisierung kann aus meiner Sicht auch Chancen mit sich bringen. Wenn man diese Digitalisierung unter den Prämissen der Software Defined Defense betrachtet, so kristallisieren sich aus meiner Sicht insbesondere diese Handlungsbereiche heraus:

1. Tiefgehende, interoperable Vernetzung: Daten stehen in allen Bereichen und Behörden zur Verfügung, ob nun in Bezug auf KRITIS oder die Gemengelage im Informationsraum. Alle beteiligten Akteure müssten auf einen gemeinsamen Informationsraum zugreifen können. Jede Behörde arbeitet auf den eigenen Systemen – aber eben per API auf einer gemeinsamen Datenbasis. Dies ist eine Erkenntnis aus dem Einsatz zum G20-Gipfel im Jahr 2017, wo Verbindungsoffiziere im Sekundentakt Informationen von einem System ins andere getippt haben (SIC!)
2. Autonomie in der militärischen Digitalisierung: Wir brauchen eigene Künstliche Intelligenz, die in Europa gehostet und entwickelt wird, um eine Abhängigkeit von den USA und China verhindern zu können. Dafür braucht es klare Investitionen und Entwicklungen.
3. Beibehalten des Regionalitätsprinzips: Bei aller Digitalisierung braucht es am Ende "Boots on the Ground". In Hamburg können wir derzeit pro Jahr eine Heimatschutzkompanie aufstellen. Dieses in der Bevölkerung vorhandene Momentum muss aus meiner Sicht in einer konsequenten Erhöhung der personellen und infrastrukturellen Ressourcen im Bundesland münden. Und wir dürfen nicht vergessen: Wir brauchen diese Reservistinnen und Reservisten, die regional verankert sind.

Das alles ist nur erreichbar, wenn wir moderne Methoden einsetzen, konsequent und plattformübergreifend vernetzen und einbinden (einen gemeinsamen BOS-Informationsraum zum Beispiel, in den alle BOS ihre Daten einspielen). Wir müssen die Agilität und die Fähigkeit zur Skalierung nutzen und vorhandenes Momentum aufgreifen. Nur so lassen sich aus meiner Sicht kurzfristig die Herausforderungen stemmen, die uns jetzt bevorstehen.

Autor:

Kapitän zur See Michael Giss ist seit 2018 Kommandeur des Landeskommando Hamburg, zuvor war er unter anderem im BMVg und im Einsatzführungskommando eingesetzt und Kommandant der Fregatte Emden.

Die Bauteile des Bauspiels

Quelle: J. Elstermeier

Foto: Autor

Software Defined Defence als ganzheitlicher Ansatz für Streitkräfte und Industrie

Dr. Timo Haas

Moderne Waffensysteme sind ohne Software undenkbar geworden

Eine militärische Auseinandersetzung und der Einsatz moderner Waffensysteme ohne Software ist heute undenkbar geworden. Noch vor wenigen Jahren wurde Überlegenheit durch Kaliber und Reichweite gekennzeichnet. Heutzutage geht es vielmehr um Vernetzung, Geschwindigkeit, Präzision und Wissen. Um im Gefecht der Zukunft zu bestehen, sind nicht allein Waffen- und Truppenstärke gefragt. Angesichts neuartiger Effektoren wie Hyperschall-Flugkörper oder erweiterte Fähigkeiten von Unbemannten Flugsystemen im Hinblick auf Bewaffnung und Vernetzung zu Schwärmen kommt es darauf an, Bedrohungen frühzeitig zu erkennen und eine schnelle Entscheidungsgrundlage zur Reaktion zur Verfügung zu stellen. Auf dem digitalen Schlachtfeld stellt Software nichtmehr nur eine Unterstützungsleistung für Waffen- und Kommunikationssysteme dar, sondern hat sich zu einem elementaren Bestandteil der modernen Kriegsführung entwickelt. Mittels Künstlicher Intelligenz (KI) und Maschinellem Lernen (ML) überwachen, steuern und optimieren softwarebasierte Systeme fortlaufend militärische Prozesse. Das Grundkonzept dieser Systeme ist die „Software Defined Defence" (SSD). SSD befähigt Streitkräfte schnell zu agieren, flexibel zu reagieren, und sich effektiv an den immer schnelleren Wandel auf und abseits des Schlachtfeldes anzupassen.

Datenverfügbarkeit und –austausch entscheiden heute über den militärischen Erfolg

Aufgrund der wachsenden Bedeutung von Software, hängt die Schlagkraft moderner Streitkräfte zunehmend von der Verfügbarkeit digitaler Dienstleistungen und dem reibungslosen Zusammenspiel unterschiedlicher operativer Systeme ab. Eine Schlüsselrolle spielt dabei die digitale Vernetzung aller Truppenteile, um den Zugriff auf Informationen in Echtzeit zu ermöglichen. Künstliche Intelligenz und Maschinelles Lernen werden dabei die Funktion haben, den Nutzer zu entlasten, Entscheidungszyklen zu verkürzen, Personal zu reduzieren und die Effektivität zu erhöhen. Das Lagebild des militärischen Führers wird so verdichtet, dass der Führungsprozess beschleunigt und Gefechtsstände mobiler und kleiner werden. Durch effektive Nutzung und effizientem Informationsaustausch verfügbarer Sensoren, Radaranlagen, Drohnen und Panzern sowie Kräften der Luftunterstützung und Luftverteidigung, ergänzt durch Aufklärungssatelliten und Informationen der elektronischen Kampfführung, kann die Kampfkraft eines Verbandes erheblich gesteigert werden. In der Zukunft entscheidet die Datenverfügbarkeit über den Erfolg oder Misserfolg auf dem Schlachtfeld.

Ein digitales Ökosystem zur Verbindung bestehender Systeme mit neuesten Technologien

Als führendes Systemhaus können wir die gesamte Wirkungskette „from sensor to shooter", sowohl plattformzentrisch als auch plattformübergreifend im vernetzten Systemverbund abdecken. Als Systemintegrator für Vernetzung verbinden wir dabei alle Akteure auf dem Gefechtsfeld miteinander im Sinne der Architekturvorgaben des Informations- und Kommunikationsverbundes D-LBO. Mit dem Tactical Core der Blackned GmbH stellen wir das Herzstück zur Digitalisierung moderner Streitkräfte zur Verfügung. Durch die Nutzung neuester Technologien zur Steigerung der Agilität bei gleichzeitiger Reduktion der Kosten stellt der Tactical Core die taktischen Elemente des geteilten Informationsraumes zur Entscheidungsunterstützung und Informationsüberlegenheit der Kommandeure auf dem Schlachtfeld bereit. Hierbei agiert der Tactical Core als Ökosystem aus Informationsanwendungen, Übertragungsmedien, und Plattform für Operationen unter schwierigsten Bedingungen.

In der Vergangenheit war es nicht unüblich, Informationssysteme und Systeme der taktischen Kommunikation analog zu Plattformen wie Schiffen, Luftfahrzeugen oder Fahrzeugen als unabhängiges, geschlossenes System eines ein-

zelnen Zulieferers zu beschaffen. Dieses Vorgehen führte oft zu Abhängigkeiten („Lock-In“) und erschwerte während der oft langen Nutzungsdauer eine nachträgliche Erweiterung oder Kampfwertsteigerung der Systeme, insbesondere, im Falle der Erweiterung durch Fremdsysteme („best of breed“). Zusätzlich erzeugen derartige abgeschlossene, anbieterspezifische Systeme isolierte Datensysteme („Silos“) und erschweren die Zusammenarbeit mit anderen Systemen und Organisationen.

Der Tactical Core überbrückt diese Digitalisierungsherausforderungen durch seine Unabhängigkeit von Anwendungen, Übertragungsmedien und Rechnersystemen und ermöglicht den Zugriff auf geteilte Informationen. Diese Unabhängigkeit erlaubt den Weiterbetrieb bestehender Systeme und Investitionen bei gleichzeitiger Nutzung neuester Technologien und Dienstleistungen in einem ganzheitlichen, offenen Ökosystem unterschiedlichster Fähigkeiten in einer integrierten Anwendung.

Digitalisierung ist mehr als moderne Waffensysteme

Im Zuge der vorher beschriebenen Digitalisierung fokussieren sich Streitkräfte und Industrie aktuell auf die Produktdigitalisierung; also auf die Digitalisierung und Vernetzung von Waffensystemen. Und wir sind mit dem Tactical Core hier sehr gut aufgestellt. Jedoch betrifft die Digitalisierung alle Lebensbereiche und hat in den letzten Jahren an Relevanz gewonnen. In diesem Zusammenhang ist für Unternehmen wie auch Streitkräfte die Frage nach einer geeigneten Digitalstrategie in den Vordergrund gerückt. Aufbauend auf der Analyse der Unternehmensumwelt im digitalen Kontext, ist es möglich, eine zukunftsfähige Digitalstrategie zu entwickeln. Eine Digitalstrategie ist die ganzheitliche Ausrichtung von Digitalisierungsvorhaben, um den digitalen Wandel zu antizipieren und mitzugestalten. Aufbauend darauf erfolgt die Digitale Transformation der gesamten Organisation. Dieser Schritt ist notwendige Voraussetzung für eine erfolgreiche Produktdigitalisierung und Erreichung einer digitalen Überlegenheit. Software Defined Defence bedeutet demnach auch, dass sich Organisationen selbst digitalisieren müssen. Eine erfolgreiche Digitale Transformation beinhaltet daher nicht nur Produkte bzw. einzelne Elemente des Geschäftsmodells, sondern erstreckt sich entlang der gesamten Wertschöpfungskette.

Digitaler Wandel erfordert neue, ganzheitliche Denkmuster

Digitaler Wandel im Sinne eines ganzheitlichen Ansatzes ist ein Mix aus Produktdigitalisierung, Prozessdigitalisierung und digitalen Denken – dem Mindset bzw. der Kultur. Jahrzehnte klassischer, analoger Geschäftsmodelle in der Rüstungsindustrie, wie auch den Streitkräften, haben zu entsprechenden Denkmustern geführt und diese verfestigt. Teils starre Organisationsstrukturen, hierarchisch strukturiert und mit einer gewissen konservativen Haltung müssen aufgebrochen werden, wenn wir SDD tatsächlich Wirklichkeit werden lassen wollen. In den 20er-Jahren dieses Jahrhunderts haben die digitalen Vordenker und Verantwortlichen unserer Industrie die große Aufgabe, darauf die geeigneten Antworten und Lösungen zu finden und diese zu implementieren. Inwiefern müssen Geschäftsmodelle digitalisiert werden? Wer ist überhaupt bereit dazu und von der Notwendigkeit überzeugt? Was können die Unternehmen für sich und wir gemeinsam in Deutschland tun, um unsere Marktpositionen zu sichern? Welche Teile der Wertschöpfungskette verdienen besonderes Augenmerk? Wie bringen wir aktuelle Geschäftsmodelle (oftmals die Cash Cow im Unternehmen) und das neuartige digitale Geschäftes in ein gesundes Spannungsfeld? Wie werden wir effizienter? Wo müssen wir stärker automatisieren? Und zu guter Letzt, wie binden und entwickeln wir unsere Belegschaft und gewinnen junge Talente dazu?

Der Wettbewerb um digitale Talente geht in die heiße Phase

Digitalisierung bedeutet auch immer eine Verschmelzung von bisher getrennten Systemen. Talente, die bisher in den hippen „New Tech-Unternehmen“ (Silicon Valley lässt grüßen) angeheuert wurden, werden zukünftig auch in der Rüstungsindustrie gebraucht. Wie wollen wir diese Menschen für uns gewinnen und somit in den direkten Wettbewerb zu großen hochmodernen IT-Konzernen treten? Der „War of Talent“ ist bereits in eine hochintensive Phase übergegangen. Wir werden uns warm anziehen müssen. Die Generationen haben alle ihre besonderen Merkmale. War für Generation Y der Sinn („Purpose“) von besonderer Bedeutung, kommt für Gen Z bekanntlich die Lebensqualität in Form von Freizeit („Work-Life-Balance“) und der Selbstverwirklichung hinzu. Die Maslow-Pyramide hat ihre Spitze erreicht. Gefühlt bleibt keine Zeit mehr, um über diese Fragen nur unverbindlich zu grübeln – egal ob das auf einer der bekannten Veranstaltungen unserer Community geschieht oder bei einer agilen Design Thinking Session passiert. Am besten steht das Zielbild der Transformation bereits, eine Strategie ist verabschiedet und befindet sich bereits in der Implementierung.

Eile ist auch deshalb geboten, weil wir spätestens mit der Zeitenwende erkannt haben, dass wir nicht nur von Freunden umgeben sind und ein Krieg in Europa wieder möglich erscheint. Die Corona-Pandemie hat auch unserer Branche, die lange als verkrustet und chronisch analog galt, gezeigt, wie schnell wir digital werden können, wenn wir nur wollen und vor allem müssen.

Als Chief Digital Officer treibe ich die digitale Transformation konsequent voran

Software Defined Defence wird sich nur realisieren lassen, wenn wir, die europäische Rüstungsindustrie, akzeptieren, dass die Digitalisierung unserer Produkte nur auf digitalen Unternehmen basieren kann. Als führendes Systemhaus entwickeln wir uns hier stetig weiter und richten unsere Organisation und Prozesse konsequent an den Anforderungen der Digitalen Transformation aus. In der neu geschaffenen Position als Chief Digital Officer (CDO) der Rheinmetall AG treibe ich diesen Wandel konsequent voran. Die kommenden Jahre werden zeigen, ob wir dieses Jahrzehnt wirklich als eine digitale Dekade bezeichnen dürfen.

Autor:

Dr. Timo Haas ist seit Januar 2024 Chief Digital Officer bei der Rheinmetall AG.

Foto: Autor

IT-Technologie im Kontext von Software Defined Defence – Entwicklungsgeschwindigkeit erfordert eine neue Art der Zusammenarbeit.

Reimund Igel

Alle Bereiche unserer nationalen wie internationalen Wertschöpfungsketten gesellschaftlicher Daseinsvorsorge und deren integrierte systemrelevanten Sicherungssysteme sind mit digitalen Lebensadern durchzogen, vernetzt und in Teilen funktional unmittelbar voneinander abhängig.

Charakteristisch hierbei sind hybride Netzwerktopologien äußerst unterschiedlicher Güte und Sicherheitsarchitektur. Unterschiedliche Zuständigkeiten zwischen Bund und Ländern in der Strafverfolgung und Incident Response sind für unsere nationale digitale Verteidigungsfähigkeit nicht immer förderlich.

Die kontinuierlich steigende Bedrohungslage im Cyberbereich ist auch eine Folge der systemischen Auseinandersetzungen zwischen westlichen Demokratien und autokratischen repressiven Staatsformen. Das Rennen um technologische Vorherrschaften und/oder diesbezügliche Abhängigkeiten hat längst begonnen und wirkt sich direkt auf unsere innere wie äußere Sicherheitslage aus. Hard- und Software wirken zusammen. Die ersten Bedenken hinsichtlich der eingesetzten Technologien auf Netzbetreiber Ebene erfahren internationale Aufmerksamkeit und unterstreichen die besondere Sensibilität in der Frage, welcher Hardware wir zukünftig noch vertrauen können. Üben wir die alleinige Kontrolle darüber aus oder müssen wir für den Fall extern ausgelöster Kill Switches mit unvorhersehbaren Systemzusammenbrüchen rechnen.

Insellösungen wie auch der Anspruch auf eine rein ordnungspolitische staatliche Sicherheitsvorsorge werden der Bedrohungslage nicht vollumfänglich gerecht. Eine gesamtgesellschaftliche Herausforderung bedarf auch einer koordinierten Zusammenarbeit aller Akteure, ob staatlich oder nicht-stattlich, zivil oder militärisch.

Richten wir unser Augenmerk auf das im transatlantischen Bündnis interkontinental etablierte Federated Mission Networking (FMN), ist klar: Hier arbeiten die beteiligten Nationen an einer Interoperabilität der IT-Infrastruktur von der Cloud bis zur Cybersicherheit zusammen, um im Krisenfall übergreifend die im Einsatz benötigten IT-Services zur Verfügung stellen zu können. Neueste Technologien und Interoperabilität werden gemeinsam vertestet, verprobt und anschließend national umgesetzt.

Adaptieren wir diese Verfahren, Methoden und Vorgehen für einen Cybersicherheits-Schutzschirm, ist das ein schnell gangbarer Weg; eine skalierbare Defense-Cloud unserer kritischen Infrastruktur. Ein bereits erprobtes, schnelles und bewährtes multimodulares wie auch -laterales Sicherheitsmanagement; profitieren wir doch unmittelbar von diesen Erfahrungen, sparen Kosten und vermeiden durch diese Art der Bündelung strukturelle Risiken infolge disruptiver Einflüsse allzu dominanter Partner.

Gewinnen wir wertvolle Zeit durch Nutzung bereits erfolgter Entwicklungsarbeit und konzentrieren wir alle Kräfte mit Fokus auf eine zügige Implementierung, ohne gleich in neue und kostspielige Basis-Topologien investieren zu müssen. Reihen wir doch Baustein für Baustein an Exzellenzen aneinander, binden wir diese dort ein, wo sie benötigt werden und nutzen wir nicht nur die Schnittstellen-Standards des FMN, sondern entwickeln dazu auch neue, sofern erforderlich.

Diese Bausteine einer krisenresistenten IT-Infrastruktur und die dazu benötigten Technologien unterliegen einem ständigen Weiterentwicklungsprozess zur Anpassung an die neuesten marktverfügbaren Lösungen. Durch die rasante Entwicklung im Bereich der Software- und Hardwarefähigkeiten entsteht bereits bei der Planung

von zivil-militärischen Wirkplattformen und Einsatzsystemen der Bedarf nach einer zukunftsorientierten Wirkanalyse. Stellen wir doch unsere integrierten Cybersicherheits-Assets auf die Probe. Gerne per War-Gaming Demonstrator, denn wir suchen doch genau den 'Game-Changer' der unsere Handlungsfreiheit sicherstellt.

Das neue Fachkräfteeinwanderungsgesetz hilft zwar auch einige Lücken des IT-Fachkräftemangels in der Breite zu schließen, aber uns ist buchstäblich die Zeit davongelaufen. Linderung versprechen hier nur modernste hocheffiziente Expertise-Bildungsmaßnahmen, idealerweise On-the-Job, denn schon sehr bald erreichen wir den Zeitpunkt der technischen Singularität. Diese sehr wenigen noch verbleibenden Jahre müssen zwingend pro-aktiv gestaltet werden. Wissenschaftlicher IT- und KI-Technologievorsprung als Motor und Impulsgeber mit Garantiesiegel stärkster Verteidigungslinien und bester Wettbewerbsbedingungen.

Ein Plädoyer für ein geeintes Zusammenspiel zwischen Staat, Wissenschaft, Wirtschaft und Gesellschaft. Mit vertrauenswürdigen Service-Providern, die diese Erkenntnisse und Fähigkeiten im Gleichklang umsetzen, einer wehrtechnischen Industrie, die sich bei der Fertigung von militärischen Systemen an diesem Rahmen orientiert und einer Bundeswehr, die in der Zusammenarbeit neue Wege geht.
Neben dem EU AI Act stellen auch KI-Enabling-Strukturen sicher, dass die eingesetzte KI manipulationssicher, nachvollziehbar und nachweisbar bleibt. Prioritär sind in diesem Zusammenhang Fragestellungen zu Trainingsdaten, Bias und Korrekturfähigkeiten an den erlernten Algorithmen. KI-Enabling integriert eine kritische Vorfeld-Analyse der bereits genutzten und zukünftigen KI-Lösungen auf mögliche KI Blackbox Anteile/Inhalte oder ungeprüfte KI Open Sources. Etablierten Partnerschaften, wie das Jülichs JUNIQ und bei der Universität der Bundeswehr FI CODE sind schon heute Bausteine eines vitalen nationalem/internationalem Öko-Systems zum Aufbau einer führenden Rolle in der Softwareentwicklung für Quantencomputer. Durch die deutsche wie auch europäische Mitwirkung an der Post Quantum Cryptography wird eine Internationale Standardisierung von quantensicheren Verschlüsselungsverfahren bei der US NIST vorangetrieben, um Industrie-Standards zügig einzuführen. Hybride Cloud Technologien bieten mit dem containerbasierten Modell und der Fähigkeit zum Verschieben von Anwendungen Standort- bzw. geoübergreifend eine viel größere Flexibilität, als mit heutigen Virtualisierungslösungen. Gleiches gilt für Hybrid Cloud Technologien mit High Performance Computing, hybride Quantum-/klassische Computer, Quantensafetechnologien für Altanwendungen und vendoragnostische Nutzungen von Hyperscalern.

In Deutschland und Europa existiert bereits ein großes Know-how an Zulieferexpertise für modernste Chip Fertigungsanlagen und mit den Forschungseinrichtungen wie das renommierte Forschungslabor in Rüschlikon bei Zürich, stellt Europa auch die Fachexpertise für die Forschung und Entwicklung der Chips (CPU, KI, QBits) der nächsten Generation. Dazu wurde mit dem ETH Zürich ein einzigartiges Nanotechnologie Labor zur Entwicklung von Prototypen entwickelt und gebaut. Wesentliche Bausteine auf dem Weg einer nationalen und europäischen Chip-Entwicklung zukunftsorientierter Chipfertigung deren wir dann auch guten Gewissens zukünftig vertrauen können. Made by EU/GER !

Autor:

Reimund Igel,
Senior Technology Sales Representative
Geschäftsbereich Verteidigung

Foto: Autor

Erkennung und Abwehr von Anomalien in hybriden Netztopologien

Felix Juhl

In der sich ständig weiterentwickelnden Cybersicherheitslandschaft war 2023 ein dramatischer Anstieg der Komplexität von Cyberbedrohungen. Der Einfallsreichtum bei der Durchführung der Angriffe wird durch den Einsatz von KI immer ausgeklügelter. VOLT Typhoon blieb fünf Jahre unentdeckt in der kritischen Infrastruktur der USA Es gab keine auffälligen Kompromittierungsindikatoren, Anzeichen für laterale Bewegungen, Rechteausweitung oder Datenexfiltration, zumal legitime Nutzerkonten verwendet oder erstellt und keine zusätzliche Malware in die betroffenen Systeme eingeschleust wurden. VOLT Typhoon war, im Gegensatz zu APT31 keine Cyberspionage um (militärische) Geheimnisse zu erlangen. Die Operation war ein strategisches Pre-Positioning für zukünftige disruptive oder zerstörerische Cyberangriffe auf kritische Infrastrukturen im Falle einer größeren Krise oder eines Konflikts.

Im Gegensatz zu einem strategischem Pre-Positioning startete Moskau zu Kriegsbeginn den wohl größten militärischen Cyberangriff gegen Dutzende ukrainischer Netzwerke, Systeme und kritische Infrastrukturen, wie das das Viasat-Satellitenkommunikationsnetz. Allerdings bewies die Ukraine eine beeindruckende Verteidigungsstärke, was an jahrelanger Erfahrung von Cyberangriffen aus Russland liegt. Seit Kriegsbeginn arbeitet eine Allianz von Experten aus konkurrierenden Unternehmen zusammen, um russische Cyberangriffe zu vereiteln oder abzuwehren. Der Ukrainekrieg kann als ernstzunehmendes Versuchsfeld für Annahmen über Informationswaffen betrachtet werden.

Wir wissen um die Angriffstechniken, von staatlichen und staatlich- gesponserten Akteuren, die sich einen vollständigen Systemzugang zu Kontrollsystemen (ICS), Überwachungs-, Steuerungs- und Datenerfassungsgeräten (SCADA) Kommunikationsnetzen und anderen Systeme zu Land, See und Weltraum verschaffen können. Spätestens seit PEGASUS, das inzwischen mit Forensik auf Zielgeräten festgestellt werden kann, oder ähnliche Spionagesoftware, die als Leak im Internet abrufbar sind, ist das Spektrum der Bedrohungen unüberblickbar erweitert und kritischen Infrastrukturen, die innere Sicherheit und Landesverteidigung oder ganzen Metropolregionen wie zum Beispiel Hamburg sind mehr denn je Ziele. In der Region Hamburg liegen beispielsweise unsere im Bau befindlichen Fregatten, Energieversorger, wichtige Militärische Einrichtungen, systemrelevante Rüstungsindustrien wie Airbus und der Hamburger Hafen als Lebensader unserer Logistikketten. Überlebenssichernde Wertschöpfungsketten zum Schutz und Erhalt unseres Staates.

Branchenspezifische Resilienz-Standards, oder Security Standardlösungen allein reichen bei weitem nicht mehr aus. Was nutzen Sicherheitszertifizierungen, wenn ignoriert wird, dass z.B. OTP (One-Time-Pad, Einmalverschlüsselung) basierte Zwei- Faktor-Authentisierung umgangen werden kann, VPN (Virtual Private Network) -Tunnel nicht wirklich sicher sind, Datenschutz nur den Tätern hilft und nur wenige Labore dieser Welt manipulierte Hardware erkennen können. Hersteller von Industrierobotern verwenden „Hardware Detektoren" um die Gewährleistung aufrecht zu halten. Was aber, wenn Hardware, Chips oder das Ersatzteil, wissentlich oder unwissentlich, weil extern beschafft, manipuliert ausgeliefert wird? Kein System der Welt kann zum heutigen Zeitpunkt automatisch derartiger Schwachstellen erkennen. An der TU München forscht ein Team an Möglichkeiten zur Auswertung und Erkennung von versteckten Blackspots in Embedded Systemen und Chip-Architekturen.

Es ist wichtig jetzt neue Wege zu gehen, neue Ideen voranzubringen und unbequeme Fragen zu stellen. Nicht nur aus forensischer Sicht ist die Souveränität eines Staates mehr denn je auch eine Frage der digitalen Kriegstüchtigkeit. Widerstand durch Qualität, Stärke

durch eine Fusion von Expertise. Wir wissen doch ganz genau, was wir heute schon können, kennen viele der Offensivmittel oder -verfahren und unsere Defensiv-Möglichkeiten. Reagieren wir jetzt darauf, indem wir unmittelbar alle systemrelevanten Bedarfsträger durch eine umspannende Defense Cloud mittels eines modularen Baukastensystems schützen. Nicht morgen sondern heute! Im Rüstungsbereich findet dieses Umdenken bereits statt, vor allem wegen der Erkenntnis; erfolgreich ist, wer die Informationsüberlegenheit hat, erhält und sicherstellt.

Das vorgeschlagene Air Gapping ist eine durchaus sinnvolle physikalische Abschottung, bei einer Defence Cloud aber nicht ohne Risiken; thermische Manipulationen, verdeckte Oberflächenvibrationen, LEDs, Ultraschallübertragungen, Funksignale und Magnetfelder gehören, wie nicht gepatchte Systeme, die unbemerkt bleiben, mangelnde Sichtbarkeit des Netzwerkverkehrs und Wechselmedien (Beispiel STUXNET), die physisch mit dem Netzwerk verbunden werden zu den Schwachstellen. Und der Faktor Mensch. Bereits 2018 verschafften sich russische Akteure erfolgreich Zugang zu sensiblen Air-Gapped-Systemen im Energiesektor und in anderen kritischen Infrastrukturen.

Grundsätzlich aber bieten Defence Clouds, Software und künstliche Intelligenz (KI) entscheidende Vorteile für moderne Militäroperationen, verbessern die Interoperabilität zwischen verbündeten Streitkräften und unterstützen das Erreichen von Entscheidungsvorteilen gegenüber dem Gegner. Da der Großteil der Funktionen vieler militärischer, auch schwimmender, Plattformen heute von Software gesteuert wird, wird immer deutlicher, dass sie nicht einfach auf die militärische Hardware aufgesetzt wird. Vernetzte Software ist inzwischen ein fester Bestandteil eines Waffensystems.

Die Erkennung von Anomalien ist von entscheidendster Bedeutung, um die Zuverlässigkeit und Sicherheit zu gewährleisten. Wenn man bei der Planung von und in Betrieb befindlichen hybriden Umgebungen und dimensionen-übergreifenden bemannten/ unbemannten Systemen und Verbänden in einer Combat Cloud oder kritischen Infrastrukturen über eine sichere, realisier- skalier und umsetzbare Anomalieerkennung, zeigt das Beispiel Ukraine die Lösung bereits auf.

Es gilt eine kollektive Cyber-Verteidigung aufzubauen, die es jedem angeschlossenen Teilnehmer und System in der Defence Cloud ermöglicht, automatisch und kontinuierlich anonymisiert aus Vorfällen und Vorgängen bei anderen Systemen und Teilnehmern zu lernen abzuwehren und durch smarte Backups im Schadensfall sofort wieder in der Normbetrieb zurückzukehren. Diese Zusammenarbeit in Echtzeit schützt nicht nur Ihr eigenes Ökosystem, sondern die gesamte unter dem Schutzschirm befindlichen Teilnehmer. Durch die Möglichkeit, punktuelle Erkennungen sofort miteinander zu verknüpfen, erhält man präzise Vorhersagefähigkeiten in Bezug auf eine erkannte Abfolge von Ereignissen im gesamten Umfeld. Nach demselben und heute schon verfügbaren Baukastenprinzip können auch Systeme und Netze der verteidigungsindustriellen Basis und des Verteidigungsministeriums, durch die bidirektionale Integrationen in SIEM (Security Information and Event Management) – und SOAR (Security Orchestration, Automation and Response) -Tools „abgeschirmt" werden und eine Erkennung und Klassifizierung „unknown unknowns" ermöglicht werden.

Autor:

Felix Juhl ist Mitglied der Geschäftsführung von ARTEFAKTUM LLC.

Foto: Autor

Expertisebildung braucht Geschlossenheit

Markus Lehmann

Im Rahmen der Landes- und Bündnisverteidigung kommt Deutschland als eine der technologisch und wirtschaftlich führenden Industrienationen eine zentrale Rolle zu. Unbestritten braucht es technologische Überlegenheit, um kritische Infrastrukturen zu sichern und zu verteidigen. Aber die Friedensdividende ist aufgebraucht. Die aktuellen Bedrohungen sind bekannt: Klima, Autokratien, Demographie, Migration und weitere. Dazu kommen Lieferketten, die nicht mehr belastbar sind. Es fehlt an allen Ecken und Enden: Expertise, Zeit, Geld, Personal. Deutschland stellt sich neu auf... Oder doch nicht?

Die Sicherheit Deutschlands ist eine gesamtstaatliche Aufgabe, so liest man. Beschränkt Gesamtstaatlichkeit sich allein auf die Gesamtheit der staatlichen Organisationen, ist das riskant. Arbeiten Politik, Sicherheitsorgane, Wirtschaft und Gesellschaft nicht zusammen, gefährden sie die politische, polizeiliche und militärische Führungs- und Handlungsfähigkeit und damit unsere stabile, resiliente Grundversorgung. Es bedarf daher Partnerschaften, die sich durch Geschlossenheit auszeichnen, die diese Resilienz und Redundanz, vor allem aber die materielle, personelle und IT-Sicherheit in ihren Strukturen verankern. Gesetzliche Hürden wie Kartell- und Vergaberecht lassen aus Marktbegleitern und Wettbewerbern aber nicht einfach so Partner werden. Neben den rechtmäßigen Grundlagen fehlen Vertrauen und Transparenz über das beidseitige Tun. Berateraffären, Studienergebnisse zu überzogenen Forderungen, Schlechtleistung, überhöhten Preisen und Terminuntreue tun das ihrige dazu. Sie führen (verständlicherweise) allseitig zu juristischem Absicherungshandeln, Rügen und Klagen, die in Folge mehr lähmen und trennen als zu dem zu führen, was sinnvoll ist: wertebasierte Geschlossenheit, die auf der Expertise (-bildung) beruht.

Geschlossenheit durch Partnerschaften

Längst wird in vielen Bereichen versucht, alle relevanten Stellen aus Forschung, Politik, Wirtschaft und Gesellschaft zusammenzubringen. Damit den Worten Taten folgen, müssen aus Gesprächskreisen, Industrie- und Marktdialogen (endlich) Handlungskreise werden, die sich durch Geschlossenheit auszeichnen. Es braucht verlässliche, vertrauensbasierte, strategische Partnerschaften, die auf einem wertebasierten Wettbewerb beruhen. Dabei stehen Respekt und Vertrauen sowie das schnelle Handeln Hand in Hand und Schulter an Schulter im Vordergrund. Geschlossenheit sorgt für gemeinsame Anstrengung, die kreativsten Köpfe, die besten Produkte und die wirkungsvollste Lösung zusammen zu bringen, zügig und miteinander die Expertise zusammen zu werfen und aus diesem Pool heraus die richtigen Weichen zu stellen. Fähigkeiten und Funktionen bestimmen das Maß des Handelns, die die Wirkungsüberlegenheit zum Zielbild hat. Denn Aggressoren, Klimawandel und demokratische Entwicklung warten nicht, bis Deutschland sich neu aufgestellt, auf- und ausgerüstet hat.

Schnelligkeit durch Geschlossenheit

Geschlossenheit und Partnerschaft können dabei langwierige Abstimmungen, Verhandlungen und Vergaben deutlich verkürzen und führen zu Handlungsschnelligkeit. Diese zeichnet sich nicht allein -wie derzeit oft thematisiert- durch eine beschleunigte Beschaffung aus. Neben der Beschaffungsschnelligkeit müssen wir auch bei der Innovation und Entwicklung neuer technologischer Lösungen schneller werden. Und im Rahmen des Ansatzes von „software defined defence“ reden wir dann insge-

samt von der Innovations-, Adaptions- und Entscheidungsschnelligkeit. Gerade die aktuellen Entwicklungen rund um künstliche Intelligenz und deren Mehrwert und Verwendungsmöglichkeiten zeigen die Notwendigkeit des Einsatzes agiler Methoden, um im partnerschaftlichen Miteinander eine ständige Weiterentwicklung der eigenen Fähigkeiten an die sich ständig wechselnden Rahmenbedingungen vorzunehmen.

Aus dem Dialog mit den Sicherheitsbehörden, deren IT- und Telekommunikations-Dienstleistern, mit der Bundeswehr und der BWI muss jetzt ein Geschlossenheitsraum werden, damit aus Dialogen ein modulares Baukastensystem wird, das überzeugend, überlegen und marktführend ist. Expertise – das lehren uns erste Erkenntnisse aus dem Krieg gegen die Ukraine und dem Krieg in Gaza – bedeutet dabei, bei gleicher Technologie schneller die richtigen Schlüsse zu ziehen und schneller und zielführender als der Gegner zu handeln. Die Entwicklungs- und Adaptionszeit von Softwarelösungen als Reaktion auf neue Fähigkeiten auf der Gegnerseite muss auf Monate, Tage, ja manchmal Stunden verkürzt werden. Eine sichere Kommunikations- und IT-Infrastruktur ist die Basis, auf der diese Multicloud-basierten Softwarelösungen dimensionsübergreifend und interoperabel mit den Bündnispartnern aufgesetzt werden. Eine ad-hoc gemeinsam in groben Zügen vertrauensvoll miteinander abgestimmte Sicherheitsstrategie ermöglicht die Schaffung gemeinsamer Datenräume der Sicherheitsinstitutionen. Die Absicherung dieser Datenräume, unserer digitalen Systeme und IT- und Kommunikationsinfrastruktur im Cyberraum und damit die Erhöhung unserer Cyber Resilienz kann nur gemeinsam gelingen. Amtsseite, Industrie und Wirtschaft stehen dabei geschlossen zusammen und vereinbaren gemeinsam Maßnahmen, Leitlinien, Standards und Kooperationen. Die dafür notwendige Expertisebildung auf allen Seiten der Beteiligten hat nicht nur technologische und projektorientierte, sondern auch soziale Ansätze. Die Expertisebildung und die Orchestrierung aller Akteure in einem Partner-Ökosystem erfordert einen kontinuierlichen Prozess, bei dem auf der Grundlage von „software defined defence“ die Erfahrungen, das Wissen und die Fachkenntnisse sofort in Geschlossenheit gebündelt, dann kontinuierlich überprüft, weiterentwickelt und zur Bewältigung neuer Herausforderungen zum Schließen von Fähigkeitslücken verbessert werden.

Die Begleitung, Steuerung und Umsetzung dieses Prozesses kann übernehmen, wem alle seitens der Politik, der Forschung, der Bedarfsträger und Nutzer genau wie auf Seiten der industriellen Partner vertrauen und der dafür anerkannt ist, die Rolle im Rahmen eines wertebasierten und nachhaltigen Projektmanagements zu steuern. Nur wenn wir jetzt geschlossen die wertebasierte Expertisebildung vorantreiben, können wir aus (militärischen) Ereignissen und Lagen per sofort anfangen, die richtigen Schlüsse ziehen, die richtigen Handlungsempfehlungen einleiten und wirkungsvolle Maßnahmen umsetzen, was schlussendlich bei knappen Ressourcen (Zeit, Geld, Personal) zum Erfolg führt. Dieser Plan geht nur mit wertebasierter Geschlossenheit auf.

Autor:

Markus Lehmann ist Account Director bei Deutsche Telekom Global Business Solutions GmbH

Fotos/Grafik: Bundeswehr

Digitalisierung der Dimension See

Seekrieg im Fokus

Kapitän zur See Jörg Lorentzen

Aktuelle Ideen, Konzepte und Entwicklungen in den Themenfeldern Software Defined Defence (SDD), Multi Domain Combat Cloud (MDCC) und Multi Domain Operations (MDO) werden auch in der Marine aufmerksam verfolgt, um die erkennbaren Potentiale für eine erfolgreiche Seekriegsführung möglichst bald verfügbar machen zu können. Die dafür erforderliche bessere Digitalisierung der Operationsführung über die Dimensionsgrenzen (Land, Luft, See und Cyber) hinweg ist mit einer Reihe von Projekten und Maßnahmen eingeleitet und wird Stück für Stück in Abstimmung mit den anderen Teilstreitkräften national und im Bündnis in den kommenden Jahren umgesetzt.

Warum dauert das so lange?

Die Seekriegsmittel der Marine sind im Kern die Schiffe und Boote der Flotte sowie die fliegenden Waffensysteme, die in diesem Artikel aber nicht betrachtet werden. Die Schiffe und Boote werden für eine Nutzungszeit von etwa 30 Jahren konzipiert: eine lange Zeitdauer, in der die technische Entwicklung nicht stehen bleibt. Manche Schiffe (im Unterstützungsbereich) sind heute sogar bereits seit fast 50 Jahren im Dienst. Zur Erinnerung: Vor einem halben Jahrhundert gab es in Deutschland noch analoge Telefone mit Wählscheibe, um welche sich in Ost und West der jeweilige Minister für Post- und Fernmeldewesen kümmerte, und vor drei Jahrzehnten gingen die ersten digitalen Mobilfunktelefone in den neuen D- und E-Netzen in Betrieb.

Die Digitalisierung der Operationsführung, auch für ältere Kriegsschiffe, erfordert eine ständige technische Erneuerung, insbesondere der IT-Infrastruktur sowie der Informationsverarbeitungs- und -Übertragungssysteme an Bord und natürlich auch an Land in den Führungseinrichtungen der Marine. Außerdem müssen in den Operationsgebieten der Seestreitkräfte die notwendigen, leistungsfähigen Datenübertragungsnetzwerke zur Verfügung stehen, um eine digitale und vernetzte Operationsführung auch zu ermöglichen.

Über die Digitalisierungsplattform des Geschäftsbereiches BMVg sollen modular aufgebaute, wiederverwendbare, skalierbare, leicht und schnell adaptierbare IT-Services zur Verfügung stehen, die nach Servicegruppen in Clustern zusammengefasst sind. Die IT-Infrastruktur fällt dabei z.B. in das Cluster der „CORE-Services“, die Informationsverarbeitungs- und -Übertragungssysteme sind den Clustern der „Community of interest-(COI)-Services“, sowie den „Communications-(COMMS)-Services“ zugeordnet. Damit entsteht zunehmend ein „IT-Baukasten“, der es dem Planer und Rüster ermöglicht, bestehende Waffensysteme nachzurüsten sowie für zukünftige Waffensystemprojekte interoperable IT-Bausteine abzurufen und zu einer Gesamtlösung zu integrieren.

Dabei sind die gerüsteten, miteinander vernetzten IT-Services als „Wirkverbund“ zu betrachten, um deren Abhängigkeiten besser koordinieren, in das IT-System der Bundeswehr (IT-SysBw) nahtlos einbinden und in die Waffensysteme Schiff und Boot integrieren zu können. Zur Verbesserung der Führungsfähigkeit und Wirkung gegen einen Gegner ist also die plattform-, projekt- und produktspezifische Herangehensweise zu Gunsten einer netzwerk-, system- und diensteorientierten Herangehensweise zu verändern. Nur bei konsequenter Umsetzung dieses Vorgehens wird es gelingen, die Marine umfänglich zur vernetzen Operationsführung sowie MDO zu befähigen.

Logo des National Maritime Command and Control Service der Bundeswehr (NMC2SBw)

Die Digitalisierungsplattform befindet sich derzeit noch im Entstehen und die daraus abgerufenen IT-Bausteine müssen anschließend mit Hilfe des Bundesamts für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAAINBw) und den industriellen Part-

Der Einsatzgruppenversorger Frankfurt am Main bricht zum Indo-Pacific-Deployment (IPD) 2024 im Beisein des Bundesministers Boris Pistorius und des Inspekteurs der Marine Vizeadmiral Jan Christian Kaack auf.

nern in die Schiffe und Boote eingerüstet, erprobt und getestet sowie zur Nutzung freigegeben werden. Das dauert trotz aller Bemühungen zur Straffung der Beschaffungs- und Rüstungsprozesse derzeit noch zu lange.

Was unternimmt die Marine?

Die Marine erhält in den nächsten Jahren mit den neuen Fregatten Klasse 126, den Flottendienstbooten Klasse 424 sowie den Betriebsstofftransportern Klasse 707 eine Reihe von hochmodernen Kriegsschiffen, welche auch im Bereich der IT-Services state-of-the-art sein werden.

Für die Bestandsflotte und Führungseinrichtungen stehen derzeit die Projekte German Mission Network (GMN) Block 2 und 4 im Fokus. GMN 2 soll noch in diesem Jahr unter Vertrag gehen und der Ausrüstung des neuen Führungszentrums im Marinekommando dienen. Parallel wird ein maritimes Battle Management System (mBMS) als sogenannter „National Maritime Command and Control Service Bundeswehr (NMC2SBw)" über die Projekte GMN 2 sowie F126 realisiert. Der NMC2SBw ist die marinespezifische Erweiterung des Mission Enabling Service der Bundeswehr (MESBw), welcher die wesentlichen Funktionalitäten eines C4I[1]-Services in der Bundeswehr auf Basis der Software SITAWARE der Firma Systematics bereitstellt. Mit dem Projekt GMN 4 wird in den nächsten Jahren die Bestandsflotte mit der aktuellen und notwendigen IT-Infrastruktur nachgerüstet, um eine digitale Operationsführung an Land und Bord unter anderem auch mit dem NMC2SBw zu ermöglichen.

Zur Vernetzung der Seekriegsmittel dienen der Terrestrische Kommunikationsverbund der Marine (TKM) mit seinen Funksende- und Empfangsstellen sowie die Nutzung von Kommunikation über geostationäre Satelliten. Die Datenübertragungsraten über diese Wege sind begrenzt und die benötigten Signallaufzeiten über die hochfliegenden Satelliten beeinträchtigen die Nutzung diverser operativer IT-Services.

Seit Mitte 2023 stehen u.a. mit „OneWeb" der Firma Eutelsat erstmals kommerzielle Low und Medium Earth Orbit Satcom Systeme (LEO/MEO) für die operative Nutzung in See zur Verfügung. Diese wurden sofort an Bord von Schiffen der Marine, mittlerweile auch unter Einsatzbedingungen, erfolgreich erprobt. Mit diesen Systemen als Ergänzung zu den bestehenden Informationsübertragungsanlagen eröffnen sich auf Grund der hohen zur Verfügung stehenden Datenübertragungsraten sowie der geringen Latenz ganz neue Möglichkeiten hinsichtlich operativer Nutzung. Derzeit erfolgt ein weltweiter Dauer- und Leistungstest an Bord des Einsatzgruppenversorgers Frankfurt am Main sowie der Fregatte Baden-Württemberg im Rahmen des Indo-Pacific-Deployment (IPD 24).

Ausblick

Bundeswehrgemeinsame Forderungen zur Befähigung zu MDO sowie technische Entwicklungen wie SDD- und MDCC-fähige Lösungen werden gemeinsam mit dem Planungsamt der Bundeswehr, dem BAAINBw, dem Kommando Cyber- und Informationsraum (KdoCIR) sowie dem Zentrum Digitalisierung der Bundeswehr aufgegriffen, im Sinne der „digitalen Transformation" für die Weiterentwicklung der IT der Bundeswehr operationalisiert und fließen dann in die Entwicklung neuer IT-Services und Systeme wieder ein; zum Beispiel in ein standardisiertes Integrationsmodul für *„uncrewed systems"*.

Um auch in Zukunft erfolgreich den Seekrieg führen und streitkräftegemeinsam und multinational im Gefecht wirken zu können, werden mit der Digitalisierung der Dimension See konsequent die Voraussetzungen für eine zeitgemäße Operationsführung geschaffen. Bestandsflotte sowie neue Waffensysteme der Marine einschließlich autonomer und teilautonomer Systeme werden somit besser technisch vernetzt und taktisch geführt werden können.

Damit die digitalisierten Waffensysteme und Führungseinrichtungen der Flotte auch dauerhaft genutzt, betrieben und erfolgreich eingesetzt werden können, erfolgt parallel eine Reorganisation der IT-Kräfte der Marine. Nach außen hin sichtbares erstes Zeichen war die Aufstellung des Systemzentrums Digitalisierung Dimension See am 01. Februar 2024 als Teil des Marineunterstützungskommandos in Wilhelmshaven.

Autor:

Kapitän zur See Jörg Dieter Lorentzen ist Diplom-Informatiker und M6 im Marinekommando in Rostock.

1 Command, Control, Computers, Communications and Intelligence

Foto: Autor

Flexibilität, Innovation und Umsetzung als Erfüllungsparameter fähigkeitsbasierender Industriebeiträge

Harald Mannheim

Die modernen Herausforderungen in der Kriegsführung und Verteidigung erfordern eine Anpassungsfähigkeit und Innovationskraft, die die bisherigen traditionellen Konzepte übersteigt. In einer schneller werdenden Welt (mit schnellen Veränderungen, Prozessen und Datenströmen), in der insbesondere disruptive Technologien und Anwendungen den Wandel vorantreiben, müssen militärische Strategien flexibler und anpassungsfähiger sein als je zuvor.

Dazu kommt die Re-Orientierung von internationalen Einsätzen auf die Landesverteidigung. Kam es in internationalen Einsätzen in erster Linie auf die Verknüpfung der jeweilig nationalen militärischen Beiträge untereinander an, so wird künftig zusätzlich die digitale Durchgängigkeit mit nationalen Zivilschutzeinrichtungen, Behörden und Liegenschaften, eine völlig neue Bedeutung erlangen. Darüber hinaus ist zunehmend mit neuen Gefährdungsszenarien wie Cyberattacken und psychologischen Angriffen auf die Verteidigungsbereitschaft unter anderem mittels Fake-Informationen oder provozierter Panik zu rechnen. Die Bedeutung von Information Warfare und der Cyber-Dimension hat bereits heute enorm zugenommen. Die effektive Begegnung hybrider Bedrohungen erfordert neue Ansätze, die nicht mehr nur auf die Duellfähigkeit einzelner Einheiten setzen, sondern die Bedeutung von vernetzten und kooperativen Operationen betont. Im Kern steht dabei der „Best Fit Approach", der die Notwendigkeit widerspiegelt, sich flexibel an die sich ständig ändernden Bedingungen anzupassen. Und nicht zuletzt ist eine Ertüchtigung der Streitkräfte in ihrer ganzen Breite und Tiefe zwingend. Der frühere Fokus von relativ starren militärischen Formationen verschiebt sich auf dynamische, flexible Kräftezusammenstellungen, die sich den dynamischen Einsatzumgebungen mit ihren taktischen und operativen Fähigkeiten ständig anpassen können müssen. Die militärische Führung muss sich dem stellen und ein neues Strategieverständnis entwickeln, das die Komplexität und Vielfalt der modernen Kriegsführung berücksichtigt.

Multi-Domain-Operations – auch über militärische Dimensionen hinaus

Der Multi-Domain-Operations Ansatz (MDO) verfolgt das Ziel des kooperativen Wirkens über alle Dimensionen hinweg. Dieses Konzept betrifft nicht nur die Streitkräfte selbst, sondern beinhaltet einen gesamtgesellschaftlichen Ansatz, um den Herausforderungen der modernen Kriegsführung erfolgreich zu begegnen. Zum Beispiel müssten in Deutschland, als logistische Drehscheibe, die Straßen- und Brückenzustands-Register in die Führungs- und Planungssysteme integriert werden.

Um flexibel auf Bedrohungen reagieren zu können, müssen in Europa Einsatzverbände neu überdacht werden. Statt starrer Strukturen sollten dynamische Einheiten gebildet werden, die sich schnell vernetzen, dabei aber auf nationale sowie europäische Souveränität Rücksicht nehmen können. Kurz: Es muss eine schnelle (Um-)Gliederungsfähigkeit entwickelt werden.

Bauspiel Schiff im militärischen Sinne

Die Bedeutung von Flexibilität, Anpassungsfähigkeit und Innovation kann am Beispiel „Bauspiel Schiff" (Bauhaus-Konzept) verdeutlicht werden. Ein Spiel, das kreatives Denken und flexibles Gestalten fördert. Übertragen auf den militärischen Kontext wird die Kreativität in der militärischen Führungsfähigkeit (Flexibilität und Schnelligkeit) unter Berücksichtigung andockfähiger und zur Verzahnung befähigter Strukturen auf dem Gefechtsfeld zum strategischen Vorteil. Dem Gegner relativ und strukturell überlegen zu sein, ihn zu überfordern, indem er sich nicht auf Lösungen einstellen kann, wird zum Erfolgsfaktor.

Eine mögliche Antwort auf den dynamischen Charakter digitaler Gefechtsfelder bietet der derzeit in der Verteidigungsindustrie viel diskutierte „Software-Defined-Defence-Ansatz" (SDD).

Analog zum „Bauspiel Schiff" ermöglicht dieser durch seine Modularität und den Verzicht auf proprietäre Schnittstellen unter Nutzung innovativer Technologien und agiler Ansätze eine schnellere, flexiblere und vor allem nachhaltige Handlungsfähigkeit auf die sich stetig ändernden Bedrohungen. Die offen gestaltete Architektur muss dabei bestimmt sein durch die sich schnell ändernden taktischen und funktionalen Anforderungen und nicht durch die technische Machbarkeit: Die Form folgt also der Funktion.

Die Verbindung von SDD mit dem MDO-Ansatz kann zu einer Potenzierung der Entfaltung der militärischen Führungsfähigkeit führen. Die Entwicklung in

diese Richtung und damit die Förderung gemeinschaftlicher Ansätze und die Überwindung von Silo-Denken erfordert allerdings ein Umdenken sowohl des öffentlichen Auftraggebers als auch in der Industrie: Dazu gehören verzahnte und einheitlich formulierte Anforderungslagen seitens des öffentlichen Auftraggebers, das Neudenken der Beschaffungswege mit dem Fokus auf den Faktor Zeit sowie das Verfolgen von gemeinschaftlichen nationalen sowie europäischen Ansätzen durch die Industrie stets unter der Berücksichtigung offener Architekturen. Diese gehen dann über die jeweils projektspezifischen Forderungen und Umsetzungen hinaus.

Auch wenn durch die Umsetzung des SDD-Ansatzes bereits kurzfristig eine Effizienzsteigerung erwartet werden kann, ist jedoch zunächst mit einer Anschubfinanzierung zu rechnen, die vor allem durch den öffentlichen Auftraggeber getragen werden muss.

Basis zur Umsetzung des SDD-Ansatzes kann die stringente Einbindung und Ausweitung von Erprobungslaboren sein – das Labor nicht als räumliche Einrichtung, sondern im Sinne der Sand-Box/Real-Labor-Definition.

Im Real-Labor (Regulatory Sandbox) kann man zum Zwecke der Demonstration und dem Ziel Erkenntnisse agil und schnell zu adaptieren, mittels einer Experimentierklausel von einschränkenden Regularien freigestellt werden. Betriebseinschränkungen (z.B. Flugzulassungen), juristische Einschränkungen (z.B. Datengovernance) gehören dazu, aber auch Vergaberichtlinien können hier für zeitliche, räumliche und juristische Bereiche außer Kraft gesetzt oder eingeschränkt werden.

Zum Beispiel könnten so Veränderungsbestellungen oder angepasste Softwarebausteine während der operationellen Nutzung ermöglicht werden, Legacysysteme können integriert oder ersetzt werden. Auch die (ggf. zeitlich begrenzte) Zusammenschaltung mit Systemen und Funkdiensten der Behörden und Organisationen mit Sicherheitsaufgaben (BOS) könnte ermöglicht werden, ebenso wie die Integration von öffentlichen Daten (Newsfeeds, soziale Medien etc.).

Die Bedeutung des Faktors Mensch – Human Machine Interface als Schlüsselkompetenz

Bei all diesen Überlegungen und Ansätzen bleibt eines bestehen: Der Faktor Mensch. Es ist deutlich, dass die effektive Nutzung neuer Systeme und ihre Performanz vom Nutzer abhängt. Bei allen Planspielen und den daraus resultierenden neuen Ansätzen sollte das Human Machine Interface (HMI) im Zentrum stehen. Die kognitive Dimension gewinnt an Bedeutung.

Die Gestaltung von Systemen sollte stets den Fokus auf die Bedienoberfläche und Bedienerunterstützung legen, anhand derer Szenarien erprobt werden können, und deren Ergebnisse in neue Ansätze, wie zum Beispiel agile Beschaffungsprozesse münden können. Benötigt werden offene Systeme, die aus Lessons-Learned oder roten Zwillingen (Feindsimulationen) heraus permanent erweiterbar und aufaddierbar sind.

Ein regelmäßiger Austausch zwischen Anwendern, Forschung und Industrie ist notwendig und sollte auch vertraglich so gestaltet werden können, dass er für innovative Beiträge aus der Industrie offen und interessant ist. Damit könnten völlig neue Innovationsprozesse initiiert und genutzt werden, um zukünftige Anforderungen der Führungsfähigkeit wesentlich besser zu bedienen, als bisherige.

Die Zukunft der Kriegsführung liegt in der Befähigung zur kontinuierlichen Anpassung und Innovation. Die militärische Führung muss bereit sein, neue Wege zu gehen und sich kontinuierlich weiterzuentwickeln, um den sich ständig verändernden Bedingungen gerecht zu werden. Nur durch Flexibilität und Anpassungsfähigkeit können die Herausforderungen der modernen Kriegsführung unter Wahrung von Sicherheit und Stabilität erfolgreich bewältigt werden.

Autor:

Harald Mannheim ist Geschäftsführer Airbus Defence and Space GmbH, Head of Defence Digital & Cyber

Bauspielobjekte

Quelle: J. Elstermeier

Foto: Bundeswehr

Bedeutung von Software Defined Defence für die Dimension Land

Generalleutnant Andreas Marlow

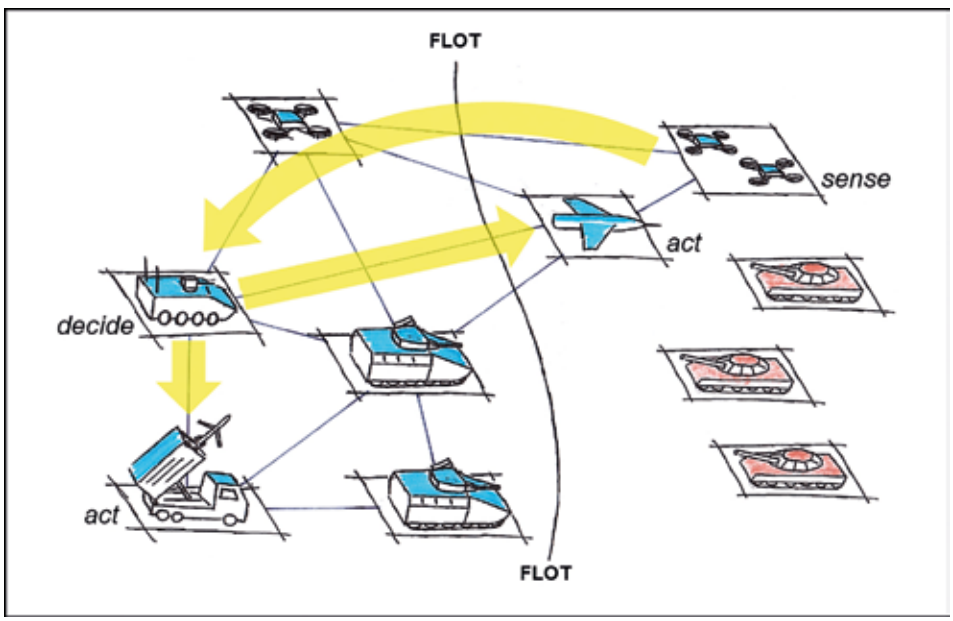
Hinter dem Begriff Software Defined Defence, kurz SDD, verbirgt sich der Ansatz, das Potential von Software für die stetige Verbesserung und Erweiterung der Fähigkeiten von Waffensystemen zu nutzen. Rüstungsprojekte können dadurch von den kurzen Innovationszyklen und der Skalierbarkeit von Software profitieren. Die Chancen daraus sind weitreichend, erfordern aber die enge Einbindung der Nutzer.

Im Krieg spielt die Fähigkeit, sich schnell an die sich ändernden Rahmenbedingungen des Konfliktes anzupassen, eine entscheidende Rolle. Die Adaptionsfähigkeit beeinflusst die Überlegenheit und Durchhaltefähigkeit von Streitkräften. Je schneller diese Anpassungen vonstattengehen, umso eher haben unsere Soldatinnen und Soldaten adäquate Antworten auf die Bedrohungen durch den Gegner und können siegreich sein. Die Anpassungsfähigkeit der ukrainischen Streitkräfte ist vermutlich der bestimmende Faktor dafür, dass es der russischen Föderation nicht gelungen ist, die gesamte Ukraine einzunehmen. Der Einfallsreichtum der Ukrainer schließt die Weiterentwicklung von Waffensystemen durch Softwareanpassungen ein. Sehr bekannt wurde die Entwicklung einer App, um die 155 mm Munition unterschiedlicher Nationen, mit den deutschen und niederländischen Panzerhaubitzen 2000 zu verschießen. Ganz im Sinne des „Bauspiels" haben die Ukrainer gelernt, das Schiff neu zusammenzusetzen.

Das ist nur eines von vielen Beispielen dafür, welchen operativen Nutzen SDD liefern könnte. Um sich dem Thema zweckmäßig zu nähern, bietet es sich an, den Bereich auf zwei Ebenen zu betrachten. Zum einen auf der Mikroebene, d.h. der Ebene des einzelnen Waffensystems, wie es im Beispiel zu sehen war, und zum anderen auf der Makroebene, welche die Auswirkungen von SDD-Systemen auf dem Gefechtsfeld der Zukunft, dem Future Operating Environment, beschreibt.

Auf der Mikroebene bietet die Digitalisierung von Systemen die Möglichkeit, schneller als bisher Erkenntnisse aus der Nutzung sowie neue Fähigkeiten in bestehende Systeme zu implementieren. Im Vergleich zu der in der Vergangenheit meist durch Hardwareänderung – und damit zeitaufwändigen – erfolgten Weiterentwicklung und Anpassung, werden SDD-Waffensysteme in ihrer Vernetzung und Funktion kontinuierlich „up to date" gehalten. Der Vorteil von Software, die schnelle Anpassbarkeit, Erprobung und anschließende Implementierung von neuen Versionen, kann so voll zur Geltung kommen.

Auf der Makroebene legt SDD den Grundstein für Multi Domain Operations. Durch eine offene Systemarchitektur können Synergien zwischen den Waffensystemen, Sensoren und Entscheidern geschaffen werden. Die Komplexität der heutigen multi-pur-



Grafik: Bundeswehr

pose-Waffensysteme könnte reduziert werden. So könnten klassische Plattformen beispielsweise in single-purpose-Systeme entlang der Wirkkette Sense (Aufklären), Decide (Entscheiden) und Act (Wirken) „aufgebrochen werden". Das Schließen der Kette zwischen Aufklärung und Wirkung kann damit dynamischer erfolgen. Wesentlich für das Funktionieren dieses Konzeptes ist die enge Vernetzung aller Systeme in einer combat cloud sowie entsprechende Fähigkeiten zur teilautomatisierten Auftragserfüllung. Die Synergien würden eine Landstreitkraft schaffen, welche heutigen Armeen in vielfacher Hinsicht überlegen wäre. Doch trotz dieses Potentials sollten wir keine überzogenen Erwartungen an SDD-Systeme stellen:

Auch wenn – wie im Bauspiel – disruptives Vorgehen der Weg wäre, um die ohnehin immer schneller werdenden Innovationszyklen zu unterlaufen, trifft der Wille und das Mindset, Änderungen schnell umzusetzen, oft auf begrenzte Ressourcen und existierende Rahmen. So wird das Heer über Jahrzehnte mit einigen der derzeit eingesetzten Waffensysteme weiterkämpfen müssen. Diese klassischen Systeme können nicht ohne weiteres in gleicher Weise weiterentwickelt werden, wie voll digitalisierte Systeme. Daher ist die flächendeckende, schnelle Einführung des Programms D-LBO von so entscheidender Bedeutung. Denn Bausteine von D-LBO können bereits, unabhängig von der Plattform in welcher sie integriert werden, nach den Grundsätzen von SDD weiterentwickelt werden.

Dennoch ist es erforderlich, auch „smarter" zu rüsten, möglichst dimensionsübergreifend. Um die Vorteile von SDD im Rüstungsprozess voll zur Geltung zu bringen, müssen wir unsere eigenen Verfahren überprüfen. Für deren Anpassung lassen sich bereits jetzt einige Grundsätze ableiten:
Wie dargestellt, ist die schnelle und kontinuierliche Weiterentwicklung von Systemen die Kernchance von SDD. Wir alle erleben heutzutage, wie die Nutzererfahrung von Smartphones durch Software-Updates in schnellen Zyklen verbessert wird. Eine abschließende Zielvorgabe, nach deren Erfüllung die Entwicklung eines Projekts beendet wird, gibt es dabei nicht. Aus dem Feedback der Nutzer werden ständig neue Ziele abgeleitet, für deren Umsetzung zunächst Prototypen entwickelt und getestet werden. Falls diese die Vorgaben erfüllen, wird die Software weiterentwickelt und als Update allen Nutzern, häufig auch für andere Hardware, zur Verfügung gestellt. Dieser spiral development cycle ist bereits heute im Rüstungsprozess als Produktänderung bzw. -verbesserung angelegt. Es kommt nun darauf an, ihn den Erfordernissen einer schnellen Entwicklung im Sinne von SDD anzupassen.

Wesentliche Anteile der Entwicklungsarbeit verschieben sich durch SDD in die Nutzungsphase, in welcher ständige Anpassungen an der Software durchgeführt werden. Für einige Systeme könnte es sogar ausreichend sein, nur ein Basisprodukt, mit rudimentären Funktionalitäten, zur Verfügung zu stellen, bei gleichzeitiger Definition eines auf in die Zukunft gerichteten, hinreichend unscharfem Entwicklungsziel. Die dabei entwickelten Lösungen müssen nicht auf ein Waffensystem alleine beschränkt bleiben, sondern können auf viele weitere Systeme übertragen werden.

Auch aus diesem Grund müssen wir unseren Blickwinkel ändern und die Systeme in der Dimension Land ganzheitlicher betrachten. Wir müssen dazu die gesamte Entscheidungshierarchie in der Beschaffung und Nutzung neu denken. Das Systemzentrum Digitalisierung Dimension Land, welches bereits heute die Nutzererfahrung bei digitalisierten Waffensystemen und dem Programm D-LBO einbringt sowie die taktisch/operative Testung dieser durchführt, sollte als Motor für Anpassungsprozesse eingebunden werden. Die dort eingesetzten Soldatinnen und Soldaten sind zum einen erfahrene Führer mit Expertise im Gefecht der verbundenen Waffen, zum anderen sind sie Systemexperten, welche die Realisierbarkeit von Zielvorgaben durch Softwareanpassungen abschätzen können. Mit den vielfältigen Werdegängen und der breiten Bildung unserer Offiziere haben wir bereits gute Voraussetzungen, Personal mit der Expertise für SDD gezielt aufzubauen und im Systemzentrum Digitalisierung Dimension Land einzusetzen.

Digitalisierte Systeme haben in Verbindung mit SDD das Potential, die Weiterentwicklung unserer Streitkräfte grundlegend zu beschleunigen und enger mit den Bedarfen der Truppe zu koppeln. Ein Erkenntnisproblem, dass SDD für die Fähigkeitsentwicklung des Heeres bestimmend sein sollte, liegt also nicht vor. Innovationszyklen in der Informationstechnik geben meines Erachtens heute die Geschwindigkeit vor, mit der wir rüsten müssen. Es gilt vor die Welle zu kommen. Dazu sind unsere bisherigen Prozesse und Verfahren zu hinterfragen. Aber selbst wenn dies geschieht, wird die Frage der verfügbaren (finanziellen) Ressourcen dazu führen, dass nicht das gesamte Heer zur gleichen Zeit den gleichen Stand hat. Also gilt es auch hier, das „Bauschiff" stetig neu zusammenzusetzen und eine neue, kreative Lösung zu finden. Hierzu setze ich auf einen inklusiven Prozess, der alle Dimensionen einbindet, weil wir das Potential von SDD sonst nicht umfänglich ausschöpfen werden.

Autor:

Generalleutnant Andreas Marlow
ist Stellvertreter des Inspekteurs des Heeres und Kommandeur Militärische Grundorganisation im Kommando Heer in Strausberg

Foto: Autorin

Expertise – wer kann, der kann.

Forschungs- und wertebasiert zu innerer und äußerer Souveränität

Prof. Dr. (habil.) Beatrix Palt

Alle reden über Mindset und Agilität, die es für Siegfähigkeit braucht. Scrum, Objectives and Key Results (OKR) etc. werden absolviert, als ob die Schulung von Regulatorik der Schlüssel wäre. Siegfähigkeit ist eine Frage von Kopf, Herz und Hand – der Leidenschaft und Frage, wofür das Herz brennt. Sie geht von der Entwicklung des Individuums aus und in eine Werte- und Interessensgemeinschaft ein, wenn sich zusammenfindet, was sich zusammengehörig fühlt. „Bauspiel – das Schiff" bietet eine Systematik für Expertisebildung als disruptiv-modulares Baukastensystem an, ein Prinzip für eine Military Combat Cloud, bei der Wirkung die Form bestimmt: „Bauspiel ein Schiff – das auch eine Berg und Talbahn,… und vieles sonst sein kann" schreibt die Erfinderin, Alma Siedhoff-Buscher, auf die Verpackung: „Die Form – einfach – unverwirrend klar und bestimmt – Vielfältigkeit und Reize schafft das Kind selbst durch Zusammenstellen, Bauen. Also – eine dauernde Entwicklung". 1924, Bauhaus in Weimar. Das Bauspiel ist doppelt disruptiv, weil die Reformpädagogik die ganzheitliche Entwicklung des Menschen in den Mittelpunkt stellend, auf Kopf, Herz und Hand als neues Wirkprinzip abzielt.

Mit wenigen (Personal, Zeit und Geld) aber einfachen Bauklötzen Wirkung zu erzielen heißt siegfähig zu sein: Die Entwicklung der Menschen sichert den finanzierbaren zeitlichen Vorsprung, weil nur Menschen, die schneller darin sind, ad hoc die richtigen Schlüsse aus Lagen zu ziehen, Technologien so wirksam zum Einsatz bringen, dass unsere Wertegemeinschaft sich verteidigen kann. „All in" leisten Menschen für sich, die Sache und die Gemeinschaft nur, wenn sie aus Überzeugung für das brennen, was sie tun. Dann gehen sie die Meile mehr, die Vorsprung erzeugt. Vorsprung durch Leidenschaft – Kopf, Herz und Hand. Das können Sie bei herausragenden Innovationen, Ballettaufführungen und generell jedem Sieg sehen: Das (Bau-) Spiel geht auf, wenn aus individueller Exzellenz Gruppenexpertise wird.

Was aber ist Expertise? Wie und wodurch bildet sie sich unter welchen Rahmenbedingungen aus? Wie (schnell) rentiert sie sich persönlich, generell und für Siegfähigkeit?

Expertie ist Können. Der Vergleich der Learnings des Ukrainekriegs mit denen aus dem Schlag und Gegenschlag Iran-Israel-Iran führt uns vor Augen, dass Technologievorsprung notwendig, aber nicht hinreichend ist, wenn bei gleicher technologischer Ausstattung Luftabwehrsysteme um so wirksamer sind, je schneller Learnings in (anderes) Handeln umgesetzt werden. Das korrespondiert mit meiner Forschung, dass die Entwicklung der persönlichen Dispositionen der entscheidende Trigger sind: Es ist die Fähigkeit zum Musterbruch, d.h. die Fähigkeit der Person mit ihren Glaubenssätzen, Verfahren und Erfahrungen, wie es immer funktioniert hat und wie nicht, zu brechen – auch mit sich selbst, den eigenen Verhaltensweisen und -mustern, der eigenen Sozialisation, Ängsten, Bequemlichkeiten, also der eigenen Biografie, um jenseits der (eigenen) Begrenztheit neu zu denken und zu handeln – nur so entsteht Innovation. Individuelle Selbstregulierung aus der eine selbstregulierte Gruppe hervorgeht. Nachhaltiger (persönlicher, technologischer, zeitlicher) Vorsprung setzt aber gegenseitigen Respekt, Anerkennung und Vertrauensvorschuss voraus: Demut vor Mensch und Menschheit, die in unserer Wertegemeinschaft schützenswert sind. Demut sich nicht (mit dem moralischen Zeigefinger) über andere zu erheben, sondern als Individuum Verantwortung für sich selbst und das Gemeinwohl zu übernehmen, das Beste zu geben. Das erfordert Geschlossenheit – in der Person als Persönlichkeit und mit den anderen zusammen, um mit dem Virulenten, Unperfekten, Unfertigen und dem Risikobehafteten im Reinen, handlungsfähig zu sein. Wer das kann, kann in jeder Lage handeln, entscheiden und für das gerade stehen, was die Konsequenz seines Handelns ist. Wer kann, der kann.

Expertise ist Können, ist exzellente Leistung in einer Domäne: vorwärtsstrategisch handeln und Komplexität – auch in hybriden, asymmetrischen und dysfunktionalen Lagen – zu beherrschen. Es ist die Fähigkeit, Informationen aus unterschiedlichen Bereichen zu verarbeiten, kombinieren, abstrahieren, ungewöhnliche Muster zu entdecken und aufgabenkompatibel organisiertes Wissen und erfahrungsbasiertes Können zu innovativen Lösungen zu entwickeln. Eine Domäne kann Chirurgie, Schachspiel, Projektmanagement oder auch Führung sein. Sie bildet sich über fünf, nach meinen Forschungen empirisch belegt, über sechs Stufen aus.

Die neue, sechste Stufe ist für jeden Turnaound, für Siegfähigkeit, entscheidend, weil nur zur dimensionenübergreifend-integrierenden Offensive in der Lage ist, wer die Expertise des anderen, aber auch anerkennen kann, dass Expertise sich zurückentwickelt, wenn neue Erfahrungen und die domänenübergreifende Expertisebildung einer Gruppe nicht zugelassen wird. Expertisebildung setzt bei persönlichen Schwächen an – Deliberate Practice, dem angeleiteten Üben, das der Perfektionierung dient, und Entwicklung durch Problemlösen on-the-job, zur Ausbildung vorwärtsstrategischen Handelns. Sie setzt bei der Offenlegung (persönlicher) Schwächen und im Miteinander an. Weil Entwicklung die Beobachtung erster Ordnung braucht und Schmerz, Glück und Feedback nur sofort und direkt wirken. Sich selbst und den anderen ungeschminkt zu erleben, setzt Vertrauen – auch als Vorschuss – voraus. Hören wir mit der Fehlerkultur auf! Die führt – das weiß die Pädagogik längst – nur zu Fehlervermeidung – mehr nicht. Coaching und Mentoring betrachten, was bereits durch das Gehirn des Erzählenden gefiltert als subjektive Wahrnehmung kommt. Die Einordnung der Persönlichkeiten nach Farben führt dazu, Menschen nach Farben in Schubladen und Teams zu stecken – nicht nach Vertrauen. Hirnscans zeigen bildhaft die tiefgreifenden Spuren von Erfahrung im Gehirn.

Zeit, zu schauen, was an Forschung marktverfügbar ist und Expertise als forschungs- und wertebasierte Wirkplattform zu nutzen. Expertisebildung mit Leidenschaft funktioniert in allen Wertesystemen. Verteidigen wir mit forschungs- und wertebasierter Expertisebildung unser Wertesystem, führen Vertrauen, Respekt, Demut, Transparenz zu innerer und äußerer Geschlossenheit mit Exzellenz als Wirkprinzip, sind wir unschlagbar, weil wir schneller sind.

Expertise ist Zeit, ist Geld, ist Technologievorsprung, ist Wettbewerbsvorteil, ist Sicherheit, ist gesamtheitliche systemische Resilienz. Ziehen wir Expertise in selbstregulierten Teams zusammen und entlasten diese – wo immer möglich – von Regulatorik und Mikro-Management – kommen wir mit ca. 10% des Personalkörpers on-the-job ins Ziel, weil Expertise-Tandems on-the-Job die Wirksamkeit eines Schnellkochtopfs entfalten, in denen erst Menschen, dann Teams, unter Hochdruck zu Rohdiamanten werden, die sich in der gegenseitigen Reibung zu Diamanten schleifen. So wird aus innerer äußere Souveränität. Wer kann, der kann…

Expertisebildung in 6 Stufen	
Stufe I: Neuling	• Verfügt über keine bzw. geringe Wissensbestände in einer Domäne • Das Handeln folgt externen Anweisungen oder Plänen • Ist ausschließlich in der Lage, einem Plan zu folgen. • Details werden zwar erkannt, können jedoch keinem Ganzen zugeordnet werden
Stufe II: Fortgeschrittene Anfänger	• Hat Vorwissen und kann eigene Leitlinien des Handelns ableiten und verfolgen • Mit der Verfolgung paralleler Leitlinien und Handlungsstränge ist die Person aber überfordert • In Problemfällen werden Details wahrgenommen. Diese können aber nicht zu typischen Merkmalen oder Mustern oder in sinnvolle Zusammenhänge gebracht werden
Stufe III: Kompetenz	• Aus der Erfahrung in der Anwendung von Wissensbeständen werden eigene Leitlinien für komplexe Situationen entwickelt • Problemsituation werden angemessen analysiert und in einen sinnhaften Zusammenhang eingebettet
Stufe IV Profizienz / Gewandheit	• Gewandte agieren routiniert und flexibel und bringen sehr gute Leistungen in einer Domäne • Sie sind in der Lage, auf ein langfristiges Ziel hin orientiert zu bleiben und gleichzeitig eine Vielzahl an Teilzielstellungen variabel anzupassen und zu verfolgen. • Situationen werden ganzheitlich und reichhaltige Erfahrungen zur Sinnerschließung genutzt
Stufe IV Expertise	• Expertentum zeichnet sich durch zuverlässig hohe Performance in Problemsituationen aus • Personen auf dieser Stufe sind nicht auf die Vergegenwärtigung von Regeln und Leitlinien angewiesen, sie handeln intuitiv und erfassen Situationen spontan
Stufe VI Musterbruch	• Lassen trotz höchster Expertisestufe neue Erfahrungen als Grundlage weiterer Entwicklung zu • Sind zum Musterbruch in der Lage, d.h. alles in Frage zu stellen, wie es immer schon gut war und wie nicht, Biographie, Sozialisation, Erfahrungen, Verhalten, Glaubenssätze – auch sich selbst • Sind in der Lage, die Expertise anderer – in derselben oder in anderen Domänen – zu respektieren zusammen zu führen und (sich) im Miteinander weiter zu entwickeln

Quelle: vgl. Hartheis, Billet & Gruber (2020), Palt (2020, unveröffentlicht), Palt 2024b und empirische Befunde aus Projekten (2014-2024)

Zum Weiterlesen:

Gruber, H. (2021). Reflexion. Der Königsweg zur Expertise-Entwicklung. Journal für LehrerInnenbildung 21(2021)1, 108-117.
Gruber, Jansen, Marienhagen & Altenmüller (2010). Adaptations During the Acquisition of Expertise. Talent Development & Excellence. 2 (2010) 1, 3-15.
Hartheis, Billett, Gruber (2020). Expertiseentwicklung: Umwandlung von Wissen in Können. In: Hermkes, Neuweg, Bonowski (Hg). Implizites Wissen.
Berufs- und Wirtschaftspädagogische Annäherung. Bielefeld: wbv Publikationen, 155-175.
Palt, B. (2024a). Expertisebildung: Feuer, Leidenschaft, Sexyness – Wie ein Rennstall gewinnt. Europäische Sicherheit & Technik. 3/2024, 43-44.
Palt, B. (2024b). Expertisebildung: Musterbruch führt zur Souveränität – „Bauspiel – ein Schiff". InfoBrief Heer 29 (April 2024) 2, 11-12.

Autorin:

Prof. Dr. (habil) Beatrix Palt kommt aus der Unternehmenssanierung und macht mit dem INP Institut für Nachhaltiges Projektmanagement wissenschaftliche Begleitforschung für Organisationen.

Fotos/Grafiken: BMVg

Software Defined Defence

Kapitän zur See Daniel Prenzel

„Software Defined Defence“ (SSD) als neues zentrales Paradigma für die Entwicklung der Streitkräfte der Zukunft hat das Ziel, die enormen Potenziale von Software für die flächendeckende Steigerung der Leistungsfähigkeit der Bundeswehr zu nutzen.
Eine Begrenzung auf zukünftige Plattformen und Waffen greift dabei zu kurz, da auch eingeführte Systeme von den neuen Möglichkeiten der digitalen Welt profitieren sollten.

Software Defined Defence

Digitalisierung verändert zunehmend und in immer größerer Geschwindigkeit sämtliche Lebensbereiche der Gesellschaft. Hierfür verantwortlich sind insbesondere die rasante Weiterentwicklung von Software in immer kürzeren Zyklen, zunehmende Datenmengen sowie exponentiell steigende Rechenkapazitäten. In der Privatwirtschaft wirkt sich Software disruptiv auf ganze Branchen aus, u.a. durch den Einsatz von „Künstlicher Intelligenz“ (KI). Keiner kann sich mehr dem Einfluss und einer „Abhängigkeit“ von Software entziehen, seien es Apps auf dem Smartphone, Entertainment-Systeme im Auto oder die Steuerung der Haustechnik.
Auch in den Streitkräften hat die Bedeutung stetig zugenommen. Nahezu alle Waffensysteme, beispielsweise Panzer, Schiffe oder Flugzeuge, könnten ohne entsprechende Software ihre Fähigkeiten nicht entfalten und wären damit für die Auftragserfüllung nicht geeignet. Aber in der Wahrnehmung und damit auch in Rüstung und Beschaffung steht immer noch die Plattform mit Ihren physikalischen Eigenschaften und weniger die Software im Fokus der Betrachtung.
SDD schafft die Voraussetzungen, um schnell auf sich ändernde Bedrohungen durch reine Anpassungen von Software, ganz ohne physische Hardware-Modifikationen reagieren zu können. Kern ist eine Verschiebung des Fokus hin zu mehr modularisierten und wiederverwendbaren softwarebasierten Komponenten. Verbesserungen der Fähigkeiten und der Leistungsfähigkeit erfolgen lageangepasst über rasche Änderungen an der Software. Auch Fähigkeitsgewinne durch neue Software und Vernetzung bisher nicht interagierender Systeme können schneller als in herkömmlichen Systementwicklungszyklen erreicht werden. Inkrementelle Vorgehensmodelle, hohe Agilität sowie Flexibilität der Softwareentwicklung können damit auch bei Waffensystemen zur Anwendung kommen. Eine digitale Ertüchtigung von Systemen ist hierfür von entscheidender Bedeutung.

Potentiale von SDD

Mit der Umsetzung von SDD als zentralem Leitprinzip für die zukünftige Streitkräfteentwicklung können eine Vielzahl von Potentialen und Mehrwerten erschlossen werden
Dank kurzer Entwicklungszyklen von Software kann die Leistungsfähigkeit insbesondere von Führungs-, Informations- und Waffensystemen der Bundeswehr deutlich schneller gesteigert werden, denn mit Software lassen sich viel zügiger, größere Sprünge in der Fähigkeitsentwicklung erreichen als dies bei physischen Systemkomponenten möglich wäre.
Die Möglichkeit und Notwendigkeit, immer größere Datenmengen zu erfassen, erfordert eine hochprofessionelle Datenverarbeitung. SDD schafft die Voraussetzungen, die Daten- und Informationsflut nicht nur beherrschbar zu machen, sondern zum Vorteil der Bundeswehr zu nutzen. Denn mit zeitgemäßer Software und Unterstützung durch KI lassen sich die Daten zahlreicher Sensoren in kürzester Zeit zu aussagekräftigen, hochqualitativen Informationen verdichten und eine Überlegenheit im militärischen Entscheidungsprozess generieren.
Deutliche Potentiale liegen in einem effizienteren Einsatz der begrenzten personellen Ressourcen. Die Möglichkeiten der Automatisierung durch Software sind immens, wobei menschliche Akteure nichtsdestotrotz alle Entscheidungen treffen („Human in the loop“ by design). Angesichts steigender Datenmengen und begrenzter personeller Ressourcen ist Automatisierung für die Leistungsfähigkeit der Bundeswehr nicht nur erfolgskritisch, sondern alternativlos.
Last-but-not least sind auch die finanziellen Ressourcen zu erwähnen. Steigende Kosten für neue und insbesondere für in Betrieb befindliche Waffensys-

teme sowie erhöhte Leistungsanforderungen an die Bundeswehr erfordern dringend die Ausschöpfung der nicht bzw. nicht umfänglich genutzten Potenziale der Legacy-Plattformen, um die Leistungsfähigkeit der Bundeswehr zu relativ geringen Kosten zu steigern.

Umsetzung von SDD

Schon die kleine Auswahl von offensichtlichen Potentialen zeigt, dass die Umsetzung von SDD für und in der Bundeswehr erfolgen muss.

Für die Bundeswehr hat die Abteilung Cyber- und Informationstechnik des BMVg den Lead übernommen. Ein erster wesentlicher Schritt ist die Schaffung eines gemeinsamen Verständnisses und Zielvorstellung für dieses umfassende Thema. Mit einem Team von fachlich zuständigen Stellen wird dies vorangetrieben. Hierzu werden und wurden verschiedene Workshops und Veranstaltungen zu übergreifenden aber auch detaillierten Aspekten durchgeführt. Das Erkenntnis, dass SDD der Weg ist, um viele aktuelle Herausforderungen anzugehen ist dabei breiter Konsens.

Dies ist jedoch nur ein erster Schritt. Viele weitere Themenfelder und Aspekte, die zum Teil bereits identifiziert wurden, müssen nun vorangebracht werden.

Ohne grundlegende technische Anpassungen wird SDD nicht umsetzbar sein. Wesentlich sind das Entwickeln, Abstimmen und Vorgeben von entsprechenden Architekturen und Standards. Denn zum einen müssen die Bestandssysteme digital ertüchtigt werden, da diese noch in der „alten Welt" entwickelt und beschafft wurden. Zum anderen müssen aber zukünftige Systeme bereits „SDD-ready by design" sein. Neben den Plattformen ist natürlich auch die IT-Landschaft anzupassen. Die Digitalisierungsplattform Geschäftsbereich BMVg ist hierfür die komplementär anzuwendende Methode, die die Bundeswehr in die Lage versetzt, dass SDD umzusetzen.

Ein weiteres Themenfeld ist die Softwareentwicklung selbst. Neben der Frage „Womit?" – eine oder mehrere Entwicklungsumgebungen – wird insbesondere die Frage „Wer?" zu beantworten sein. Aber auch prozessuale Fragestellungen sind in diesem Kontext zu beantworten, u.a. zu Zyklen, Medien, Ausrollen, Pflege. Dies alles wird voraussichtlich in einer Software Factory Bw münden, deren Ausgestaltung in allen Facetten einiges an Grundlagenarbeit, aber auch Erprobung bedarf. Allerdings existiert mit der „Plattform42" der BWI GmbH bereits ein solides Fundament, welches man als Basis hierfür verwenden und weiterentwickeln kann.

Sicherheitsaspekte sind für die Streitkräfte von besonderer Bedeutung. Zwar können durch die Umsetzung von SDD einige Sicherheitsherausforderungen gemindert werden, indem z.B. Sicherheitspatches schneller durchgeführt werden können. Gleichzeitig entstehen aber auch neue Angriffsvektoren, die abgesichert werden müssen. Kein unbefugter Dritter soll die Systeme „updaten". Sicherheit, insbesondere Informationssicherheit, ist sowohl in den Plattformen, der IT, der Software-Entwicklung als auch in den Prozessen immer mit zu denken.

Künstliche Intelligenz ist dabei ein Themenfeld, das in rasanter Geschwindigkeit neue Möglichkeiten eröffnet und somit den Anpassungsdruck weiter erhöht. Dabei ist KI sowohl Unterstützer als auch Treiber von und für SDD.

Zusammenarbeit mit Industrie

Neben den Arbeiten innerhalb der Bundeswehr findet im Rahmen des Gesprächskreises 4 (GK4) „Innovation Cyber/IT" des strategischen Industriedialogs mit dem Bundesverband der Deutschen Sicherheits- und Verteidigungsindustrie e.V., dem Bundesverband der Deutschen Luft- und Raumfahrtindustrie e.V. und dem Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. die gemeinsame Erschließung von SDD statt.

In einem ersten wesentlichen Schritt wurde eine gemeinsame Position erarbeitet und angelehnt an die Berliner Sicherheitskonferenz veröffentlicht[1].

Dies war jedoch nur der Auftakt für eine intensive Arbeit in verschiedenen Arbeitsgruppen unter breiter und ambitionierter Beteiligung vieler Firmen, Unternehmen und Angehörigen des GB BMVg. Die dabei behandelten Fragestellungen decken eine Vielzahl von Aspekten ab, die für die weitere Umsetzung und Etablierung von SDD elementar sind. Ausgewählte Beispiele sind:

- Wie können Bundeswehr, BWI und Industriepartner gemeinsam zertifizierte KI-Modelle sicher entwickeln und bereitstellen?
- Wie passen Containerisierung und Container-Orchestrierung konzeptionell in SDD?
- Wie sieht eine angepasste Systemarchitektur aus? Welche Verbesserungen sind erforderlich?
- Welche Methodiken für Softwareentwicklung gibt es und wie können diese zur Schaffung einer einheitlichen Methode für die Bundeswehr beitragen?
- Wie können Bundeswehr und Industrie bei der Softwareentwicklung zusammenarbeiten?
- Wie sichert man eine Software-Lieferkette ab?
- Was muss man bzgl. der Rechtesituation beachten?
- Passen die Verträge und Vertragsmuster zu den Anforderungen von SDD?

Aus den entstehenden Arbeitspapieren werden absehbar weitere Fragen resultieren, aber auch wertvolle Empfehlungen für die weitere Umsetzung von konkreten Projekten.

Ausblick

Die weitere Erschließung des Themas ist alternativlos. Dabei müssen bereits identifizierte, aber auch neue Fragestellungen ohne Denkverbote beantwortet werden, um als Grundlage für zielführenden Lösungen dienen zu können. Dazu zählen auch erforderliche Anpassungen an Vorschriften, Verfahren, Vorgaben, sofern sie den Zielen SDD hinderlich sind.

Aber nur Konzepte allein helfen nicht. Die vorhandenen Gedanken und Ideen müssen schnellstmöglich in die Praxis kommen. So kann man einerseits den Mehrwert nachweisen und anderseits die Entwicklung ergebnisorientiert vorantreiben. Hierfür sollen in naher Zukunft erste prototypische Nachweise von Teilaspekten umgesetzt werden, die dann als Nukleus für Ergänzungen und einen iterativen Aufwuchs dienen. Mögliche Schwerpunkte sind z.B. die Etablierung und Erprobung einer Software Factory Bw und die Anwendung auf bzw. Verbindung zu geeigneten Plattformen und Systemen.

Das alles kann aber nur gemeinsam – Bundeswehr mit Industrie – gelingen.

Autor:

Kapitän zur See Daniel Prenzel
ist Referent in der Abteilung Cyber/Informationstechnik I 3 im BMVg.

1 https://www.bmvg.de/resource/blob/5711942/6fb70a45412601fdf03f63aeebf72451/cyber-defined-defence-papier-data.pdf

Foto: BMVg/Eibe

In welcher Zeitenwende stecken wir gerade?

Generalleutnant Michael Vetter

Fundamentale Veränderungen der globalen Ordnung, Bedrohungen im und aus dem Cyberraum sowie die Entwicklung von disruptiven Technologien bestimmen die aktuellen Herausforderungen für die Streitkräfte. Der sicherheitspolitischen Zeitenwende folgt eine technologische Zeitenwende. Nur Streitkräfte, die technisch auf der Höhe der Zeit sind, werden erfolgreich sein – dies gilt insbesondere bei der Landes- und Bündnisverteidigung.

Software Defined Defence trägt dazu bei, diese technologische Zeitenwende zu realisieren. Dazu gehört auch, der Bundeswehr den Zugang zu Anwendungen der Künstlichen Intelligenz (KI) zu eröffnen. Neben den technologischen Aspekten stellt sich hier auch die Frage: Verfügt die die Bundeswehr über den notwendigen Mindset, um diese disruptiven Technologien zu beherrschen? Stehen wir am Anfang einer weiteren – digitalen – Zeitenwende?

"Geostrategic competition and rapidly advancing technology are driving fundamental changes to the character of war. […] Today, we are witnessing another seismic change in the character of war, largely driven again by technology."

Diese Beobachtung von General Mark A. Milley, dem ehemaligen Chairman der US Joint Chiefs of Staff, vor gut einem halben Jahr belegt eindrücklich: Die durch den russischen Angriffskrieg gegen die Ukraine manifestierte sicherheitspolitische Zeitenwende geht einher mit einer Zeitenwende im technologischen Bereich. Es sind vor allem digitale Technologien, die disruptiv in alle Bereiche von Staat, Wirtschaft und Gesellschaft wirken – und eben auch in die Bundeswehr. Technologie verändert zunehmend auch den Charakter des Krieges.

Die Streitkräfte stellen sich diesem Wandel. Der russische Angriffskrieg gegen die Ukraine gibt einen Eindruck, wie mit neuen Technologien auf dem Schlachtfeld effizient und schnell Wirkung erzeugt werden kann. Dazu zählen kostengünstige Drohnen, die selbständig aufklären, die Nutzung von Sensoren, welche gegnerische Fahrzeuge erkennen und deren Standort melden oder intelligente Munition, die sich ihre Ziele in einem bestimmten Gebiet selbst suchen und bekämpfen kann. Diese sehr dynamische Entwicklung wird mittelfristig viele bislang fest verankerte Grundsätze der Kriegsführung in die Geschichtsbücher verbannen.

Der bereits laufende Wandel erfordert nicht nur die Implementierung der erwähnten Technologien, sondern auch einen klugen und besonnenen Umgang damit. Die Soldatinnen und Soldaten benötigen hierzu entsprechende Expertise. Neben digitalen Skills und fundierten Kenntnissen der operativen Rahmenbedingungen im Cyber- und Informationsraum ist auch ein „ethischer Kompass" vonnöten, der sich u.a. aus der besonderen Verantwortung bei der Verwendung von KI-unterstützten Systemen ergibt.

Für die Bundeswehr ist konsequente Digitalisierung ein zentraler Schlüssel, um den „Dreiklang" aus Informations-, Führungs- und letztendlich Wirkungsüberlegenheit zu realisieren. Denn nur so werden moderne Streitkräfte zukünftig erfolgreich sein können – kurz gesagt: wer nicht digitalisiert – verliert!

Ein besonderer Treiber bei der Digitalisierung der Bundeswehr wird das neue Paradigma „Software Defined Defence", kurz SDD, werden. SDD hat das Potential, das Zusammenspiel von Hard- und Software disruptiv zu erneuern und die Leistungsfähigkeit der Bundeswehr wesentlich zu steigern. Fast alle bekannten Waffensysteme brauchen heute Hard- und Software, damit sie im Einsatz ihre Wirkung erzeugen können.

Durch SDD verlagert sich der Fokus von der „Plattform" zum „Netzwerk" und auf das Prinzip, Fähigkeitsverbesserungen durch kontinuierliche Software-Updates zu erreichen. Dieses Vorgehen ist vergleichbar mit modernen Smartphones, auf denen Fähigkeiten als Applikationen bereitgestellt werden. Ein Austausch der IT-Hardware oder eine

umfassende Anpassung der Plattformen und Waffensysteme ist nicht mehr notwendig. Produktverbesserungen, die einen Zuwachs an Fähigkeiten mitbringen, können über Softwareentwicklungen und -änderungen umgesetzt werden.

Aufwändige Modifikationen von Plattformen werden zugunsten von Software-Updates weniger werden. SDD kann durch flexible und adaptive IT-Architekturen in Verbindung mit künstlicher Intelligenz einen technologischen Wechsel erzwingen, der auf der einen Seite zur massiven Steigerung der Leistungsfähigkeit der Streitkräfte und auf der anderen Seite auch zur Senkung der Ausgaben beitragen kann.

Die Digitalisierungsplattform des Geschäftsbereichs BMVg (DigPlattf) bildet bereits eine umfangreiche Basis für die Implementierung von Software Defined Defence. Jedoch kann eine Implementierung von SDD auf dieser Basis nur gelingen, wenn im Vorfeld die notwendigen Rahmenbedingungen und Prozesse für Planung und Ausrüstung der Bundeswehr zusammen mit der Industrie neu gedacht oder zumindest neu ausgestaltet werden. Hier leistet die Arbeit zu SDD im Strategischen Industriedialog, bei der alle wichtigen Player aus Industrie, Wissenschaft und Bundeswehr mitarbeiten, eine wichtige Rolle. Damit manifestiert sich auch hier ein Paradigmenwechsel, der die aktuellen Bestrebungen der Beschleunigung bei der Beschaffung weiter vorantreiben wird.

Ein zentrales Element von SDD sind Methoden der Software-Entwicklung. Grundlage wird ein „Software Engineering Framework" sein, das Standards, Methoden und Best Practices vorhält, mit denen Anwendungen für die Bundeswehr zukünftig in einer Software Factory schneller entwickelt werden. Auch im Backend ergeben sich Anpassungsbedarfe. Test- und Experimentalstrukturen müssen etabliert werden, um Software pflegen und weiter zu entwickeln. Auch sicherheitskritische Updates sollen schnell skaliert und verteilt werden. Über Experimentalstrukturen müssen Software-Updates auf ihre Einsatztauglichkeit überprüft und bei positivem Ergebnis schnell in die Fläche gebracht werden können.

Stichworte wie offene Schnittstellen, Security by Design, standardisierte Rollouts sowie neue Konnektivitätstechnologien in Verbindung mit KI werden nicht nur für die Entwickler, sondern auch für den zukünftigen Nutzerkreis innerhalb der Bundeswehr eine große Rolle spielen.

Digitale Transformation ist eine Führungsaufgabe. Sie erfordert eine „Kultur des digitalen Denkens und Machens", die weit über das bisher gepflegte Führungsdenken hinausreicht. Die Einführung eines softwarezentrierten Konzepts wie SDD wird mittelfristig nicht nur Auswirkungen auf das Fachpersonal haben, sondern auch einen Wandel der Führungskultur auf allen Ebenen erzwingen, den wir gemeinsam gut vorbereiten müssen.

Der Anteil Führungsfähigkeit und Digitalisierung des Sondervermögens in Höhe von rund 20 Milliarden Euro ermöglicht für die Bundeswehr wesentliche Verbesserungen. Damit investieren wir in die gesamte Funktionskette von der IT-Infrastruktur in Deutschland bis zum abgesessenen Soldaten. Wir schaffen einen durchgängigen und interoperablen Informations- und Kommunikationsverbund. Dieser Verbund ist die Basis, um erfolgreich an Multi-Domain Operations (MDO) teilhaben zu können.

Die Bundeswehr stellt sich den Herausforderungen der Zeitenwende und geht diese konsequent an. Digitalisierung, Führungsfähigkeit und das Paradigma SDD werden wesentlich Kriegstauglichkeit und Zukunftsfähigkeit der Bundeswehr unterstützen. Neben „Tech" ist aber auch ein „digitaler Mindset" in der Bundeswehr vonnöten, um die technischen Möglichkeiten in glaubwürdige militärische Fähigkeiten zu überführen.

Im BMVg ist die Abteilung Cyber/Informationstechnik (CIT) für die Planung, Realisierung und den Betrieb von Informationstechnik-Services in der Bundeswehr verantwortlich und treibt damit die Digitalisierung des Geschäftsbereiches BMVg maßgeblich voran. Ein weiterer Schwerpunkt der Abteilung ist die nationale und internationale Zusammenarbeit in allen cyber- und digitalpolitischen Fragen einschließlich der gesamtstaatlichen Cybersicherheit. Außerdem ist die Abteilung CIT zuständig für die Cyber- und Informationssicherheit in der Bundeswehr, für Forschung und Entwicklung sowie für das Thema Innovation im Bereich der Cyber- und Informationstechnik.

Autor:

Generalleutnant Michael Vetter ist Leiter der Abteilung Cyber/Informationstechnik (CIT) und Chief Information Officer (CIO) im Bundesministerium der Verteidigung (BMVg).

Foto: Bundeswehr

Agile Einführung innovativer IT-Lösungen in die Bundeswehr

Kriegstüchtig durch Geschwindigkeit

Brigadegeneral Michael Volkmer

„Den Feuerkampf gewinnt, wer schneller schießt und besser trifft." Diese Erkenntnis ist auf der taktischen Ebene allseits anerkannt. Im Ukraine-Krieg zeichnet sich ab: Wer schneller und agiler digital rüstet, gewinnt den Krieg.

Insbesondere die Geschwindigkeit, mit der marktverfügbare Top-Technologien und Produkte für die Truppe auf dem Gefechtsfeld verfügbar gemacht werden, schafft entscheidende operative und taktische Vorteile. Neue Fähigkeiten im Bereich Drohnen, Artificial Intelligence (AI) sowie Command & Control machen den entscheidenden Unterschied.

Die Bundeswehr hat ihre Verfahren im gegebenen gesetzlichen Rahmen in den letzten beiden Jahren beschleunigt und im Bereich Cyber- und Informationstechnologie (CIT) neue Wege bei Planung und Rüstung eingeschlagen.

Die Frage, die Bundeswehr und Industrie in der Zeitenwende umtreibt ist: Reicht das?

Landes- und Bündnisverteidigung ist unser primärer Auftrag. Kriegstüchtig ist heute nur, wer das Führen von Multi Domain Operations (MDO) beherrscht, also das synchronisierte Erzielen von Effekten in und aus allen Dimensionen. Dazu benötigen Streitkräfte, so wie unser Körper, ein Nervensystem, dass die Wirkelemente vernetzt und steuert. Ein „digitaler backbone" ist die Grundlage, um den Prozess Aufklärung – Führung – Wirkung im Rahmen von MDO schneller zu durchlaufen als der Gegner es kann. Im Englischen wird dieser Prozess auch als „Kill Chain" bezeichnet.

Die IT-Innovationszyklen in der Industrie werden in Monaten gemessen. Die Frage ist: Wie können innovative, aber überschaubare IT-Lösungen mit hohem Mehrwert für den Kampf in den Streitkräften getestet und im Erfolgsfall schneller als bisher nachhaltig eingeführt werden?

Es geht in diesem Beitrag nicht um die Rüstung großer Waffensystem- oder IT-Programme. Es geht um marktverfügbare oder eigenentwickelte innovative Lösungen, mit Kosten, die im einstelligen Mio €-Bereich liegen und die bestenfalls unterjährig, zumindest aber in einem Korridor von ein bis maximal zwei Jahren umgesetzt werden müssten. Hürden im vorwettbewerblichen Dialog zwischen Industrie, Wissenschaft und Forschung müssten beseitigt werden, um angemessen „speed" in den Prozess zu bringen.

Innovationslandschaft Cyber/IT

Die Bundeswehr hat mit Aufstellung der Abteilung CIT im BMVg und dem zur Teilstreitkraft (TSK) aufgewerteten Cyber- und Informationsraum (CIR) organisatorisch auf die zentrale Bedeutung der IT für die gesamte Bundeswehr reagiert.

In diesem Kontext haben wir eine Innovationslandschaft CIT mit Elementen wie dem Cyber Innovation Hub in Berlin, der FI-CODE an der UniBw in München, weiteren Innovationselementen in der BWI sowie im ZDigBw aufgebaut, die Digitalisierungsbedarfe nutzernah aufgreifen, identifizieren und Lösungen testen.

Eine verzugslose Umsetzung mit in der Truppe erprobten Lösungen ist aber nur in wenigen Ausnahmefällen möglich, z.B. bei Gefahr für Leib und Leben oder besonderer gesetzlicher Auflagen.

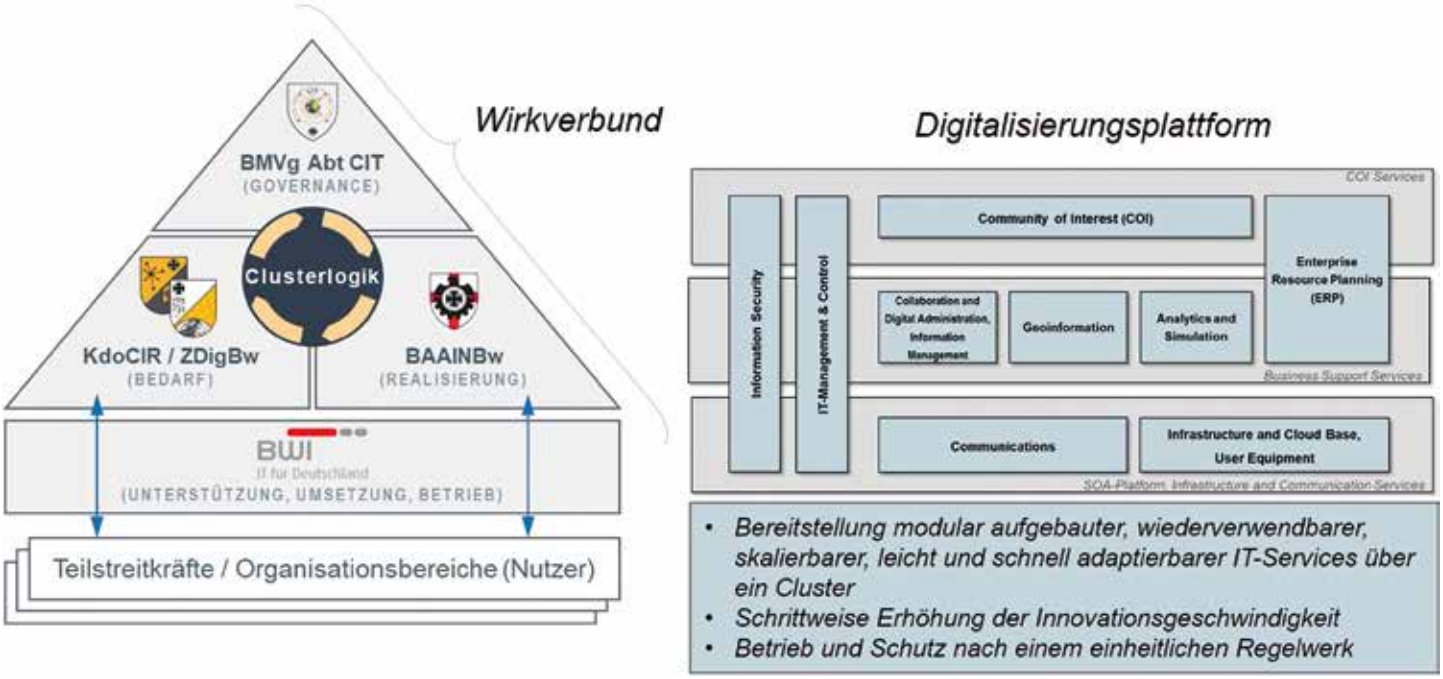
Bedarfs- und Haushaltsbegründungen müssen auch für kleine Lösungen erstellt werden, evtl. Konkurrentenklagen im Wettbewerb verzögern die Einführung zusätzlich.

Der Planungs- und Umsetzungsprozess (IPD) im GB BMVg orientiert sich an der jährlichen Haushalts- und Finanzplanung des Bundes. Im Regelverfahren erfolgt damit eine Umsetzung bestenfalls in zwei bis drei (!) Jahren.

Bw-interne Beschleunigungserlasse helfen, aber hebeln Gesetze nicht aus.

Digitalisierungsplattform

Mit der Digitalisierungsplattform (DigiPlf) wurde ein neues Regel- und Gestal-



Quelle: Bundeswehr

Der Wirkverbund und die Digitalisierungsplattform

tungsprinzip im Geschäftsbereich BMVg für das Teilportfolio CIT etabliert. Ziel ist es, standardisierte und wiederverwendbare IT-Services modular in neun Clustern beschleunigt zu planen und zu beschaffen; dies hat sich bei den Projekten im Sondervermögen außerordentlich bewährt.

Mit den Projekten im Sondervermögen wird eine einsatzbezogene IT-Basisinfrastruktur in den nächsten ein bis fünf Jahren geschaffen. Schnelle Erfolge sollen für die Brigade 45 in Litauen sichtbar werden.

Durch eine eng verzahnte gemeinsame Steuerung im Wirkverbund zwischen BMVg, dem ZDigBw als Bedarfsträger und dem BAAINBw als Bedarfsdecker wurden Arbeiten parallelisiert, im Gegensatz zur gewohnten Wasserfall-Planungs- und Realisierungspraxis. Dadurch wurde der Prozess bis zur Ausschreibung signifikant beschleunigt.

Dieser Erfolg mit Vorbildcharakter ist zunächst den (einmaligen) Rahmenbedingungen des Sondervermögens und dem hohen Einsatz der Menschen im Wirkverbund der DigiPlf und in den TSK zu verdanken und ist jetzt zu verstetigen.

Industriedialog und -einbindung

Der Faktor Zeit in der Beschaffung ist in der derzeitigen sicherheitspolitischen Lage entscheidend; ein pragmatischer und zielführender Industriedialog unter neuem rechtlichem Framework kann signifikante Fähigkeitsvorteile bringen.

Jetzt gilt es, die mit dem Sondervermögen angestoßenen IT-Projekte durch viele weitere, auch kleinere, innovative Digitalisierungslösungen schnell zu ergänzen. Damit könnte der „digitale backbone" für MDO weiter ausgebaut werden und Mehrwerte für Soldatinnen und Soldaten bringen. Themen wie Software Defined Defence (SDD), Cloudtechnologien und AI müssen wir gemeinsam mit den Unternehmen denken und analysieren, um pragmatische Lösungen zu finden.

Dafür ist ein frühzeitiger Dialog schon vor Einstieg in den Planungsprozess mit Industrie und Wissenschaft elementar.
In der Praxis stehen aber immer noch gesetzliche Regelungen einem vorwettbewerblichen „schadlosen" Dialog zwischen Industrie, Forschung und Amtsseite im Wege.

Marktteilnehmer laufen heute Gefahr, bei einer Ausschreibung benachteiligt zu werden oder gar nicht zum Zuge zu kommen, wenn sie sich ggf. zu früh und individuell in z.B. Experimente, Anwendungsszenare oder Tests einbringen.
Bilaterale Industriedialoge mit der Bundeswehr sind möglich, unterliegen aber einem strengen und aufwendigem Compliance-Regime auf beiden Seiten. Innovative Start-Ups ohne Compliance-Erfahrung geben oft vorzeitig auf, sie können auf einen Auftrag nicht mehrere Jahre warten.

Der Strategische Dialog zwischen dem BMVg und dem Industrieverband BDSV zum Thema SDD oder die Kooperationsvereinbarungen der TSK CIR mit der BITKOM gehen in die richtige Richtung, ebenso wie Messen, Veranstaltungen und Foren. Hier übernehmen Verbände oder Vereine eine koordinierende Rolle für einen transparenten und für den Markt offenen Dialog, der gerne genutzt wird, am Ende aber „generisch" bleibt.

Rechtliche Hürden

Für die Beschaffung von IT für die Bundeswehr gelten umfangreiche gesetzliche Vorgaben aus dem Haushalts-, Wettbewerbs-, Vergabe- und Preisrecht. Gesetze, die für einen fairen Wettbewerb und ohne Berücksichtigung einer existenziellen sicherheitspolitischen Gefährdung gemacht wurden. Die vielen, auf dem Rechtsweg einklagbaren Vorgaben erschweren die schnelle Einführung pragmatischer und oft auch wirtschaftlicher Lösungen. Ein schnelles Einführen auch kleinerer innovativer Lösungen ist derzeit nahezu nicht umsetzbar. Das frustriert viele innovative Akteure innerhalb und außerhalb der Bundeswehr. Angemessen finanziell hinterlegte Innovationskorridore würden helfen.

Hier gilt es anzusetzen, um in dieser für unser Land kritischen Situation z.B. gesetzlich klar geregelte Ausnahmetatbestände für IT zu verankern. Wenn Entwickler, Informationssicherheit und Operateur mit dem Markt nach einfacheren Spielregeln zusammengebracht, Vergaberechtsregeln für definierte Anwendungsfälle vereinfacht würden, könnten wir schneller sachgerechte IT-Lösungen in die Truppe bringen.

Bisherige Ausnahmetatbestände, wie z.B. das Feststellen von nationalen Sicherheitsinteressen oder Alleinstellungsmerkmale werden immer noch sehr zurückhaltend angewendet.

In Zeiten zunehmenden Fachkräftemangels sollten Ausnahmetatbestände klar festgelegt werden, damit die Prozessbeteiligten in der Bundeswehr sich langwierige Mitzeichnungsrunden für Ausnahmebegründungen sparen und sich auf die wesentlichen inhaltlichen Aufgaben und Beschreibungen konzentrieren können.

Die substanziellen Regelungs-Stellschrauben für beschleunigte Beschaffungen liegen im Haushalts-, Wettbewerbs-, Vergabe- und Preisrecht. Sie sind Grundlagen für die Compliance-Regeln auf Amts- sowie Industrieseite.

Diese Gesetze sollten ebenfalls die Zeitenwende reflektieren, schnelle Innovationszyklen der IT berücksichtigen und daraufhin angepasst werden.

Fazit

Die Geschwindigkeit, mit der wir innovative und augenscheinlich markverfügbare Lösungen in die Bundeswehr einführen können, ist immer noch zu gering. Die Kriege, die wir aktuell analysieren, zeigen sehr klar: Wir müssen digitale High-Tech Lösungen deutlich schneller in die Truppe bringen und auf technologische Innovationen und operative Erfordernisse schneller und agiler reagieren.

Dies wird uns deutlich besser gelingen, wenn wir gemeinsam mit Industrie und Wissenschaft hochinnovative Ideen und Lösungen testen, evaluieren und dann überschaubare und vergleichsweise kostengünstige Lösungen schnell in die Nutzung bringen.

Mit der DigiPlf haben wir eine neue Steuerungs- und Planungssystematik in der Bundeswehr etabliert. Diese hat sich in der Lage Sondervermögen bewährt. Sie ist grundsätzlich darauf ausgerichtet, IT effizient zu planen und schnell in die Bundeswehr einzuführen.

Zeitkonsumierende Einflussfaktoren liegen aber weiterhin in dem genannten Rechtsrahmen.

Das seit fast über 70 Jahren bestehende, „analoge" Regelwerk von Gesetzen und Verordnungen für Beschaffungen, gerade auch von IT, sollte auf die Zeitenwende hin angepasst werden.

Das Bundeswehrbeschaffungsbeschleunigungsgesetz könnte dafür weiterentwickelt werden.

Beschleunigung ist eine Aufgabe, die von allen staatlichen Akteuren gemeinsam im Dialog mit Industrie und Bundeswehr angegangen werden sollte. Nur so können Digitalisierung und Kriegstüchtigkeit innerhalb eines vernünftigen Zeitrahmens erreicht werden.

Autor:

Brigadegeneral Michael Volkmer
ist seit Oktober 2022 Kommandeur des Zentrums für Digitalisierung der Bundeswehr und Fähigkeitsentwicklung CIR (ZDigBw) und war zuvor Referatsleiter bei BMVg CIT. Er gibt in diesem Artikel seine persönliche Meinung wider.

IMPRESSUM

Herausgeber: Förderkreis Deutsches Heer e.V.
Büro Berlin: Behrenstraße 42, 10117 Berlin
Tel.: (030) 20165623
Büro Bonn: Adenauerallee 15, 53111 Bonn
Tel.: (0228) 261071, Fax: (0228) 261078
E-Mail: fkhev@fkhev.de
Web: www.fkhev.de

Mit der Herausgabe beauftragt:
Mittler Report Verlag GmbH, Bonn
Ein Unternehmen der Gruppe Tamm Media
Redaktion: Wolfgang Gelpke, Christian Kanig
Anschrift: Beethovenallee 21, 53173 Bonn
Tel.: (0228) 3500873, Fax: (0228) 3500871.
E-Mail: W.Gelpke@Mittler-Report.de
Der Info-Brief Heer erscheint fünfmal im Jahr.
Abonnementpreis für Nichtmitglieder beim Förderkreis Deutsches Heer e.V. 20,– € p.a.
Bestellungen bei: Mittler Report Verlag GmbH, Beethovenallee 21, 53173 Bonn.

AUS DEM FKH

Jahresprogramm 2024

17. – 21. Juni 2024	EUROSATORY, Paris
26. Juni 2024 *	**Mitgliederversammlung 2024, Berlin**
26. Juni 2024 *	**Berlin-Empfang, Berlin**
2. Sep. 2024	6. FKH-BDSV Thementag, Berlin
11. Sep. 2024	Parlamentarischer Abend, Berlin
25. – 26. Sep. 2024	Feldlager-Symposium bei Kärcher Futuretech, Schwaikheim
14. – 16. Okt. 2024	AUSA Annual Meeting 2024 mit Empfang FKH am 15. Oktober, Washington, D.C., USA
23. - 24. Okt. 2024 *	**Herbst-Symposium bei Hensoldt Optronics, Raum Oberkochen**
14. Nov. 2024	Info-Lunch, ggf. Präsidiumssitzung, Berlin
28. Nov. 2024	Parlamentarischer Abend, Berlin
9. Dez. 2024 *	**Kurz-Symposium 2024 mit Jahresabschlussempfang, Berlin**
19. Dez. 2024	Info-Lunch, Präsidiumssitzung, Berlin

* = Einladungen an alle Mitglieder