



# Expertisebildung ist wertebasierte nationale (digitale) Sicherheit, Souveränität & Resilienz

Prof. Dr. (habil.) Beatrix Palt

**Das „Bauspiel: Ein Schiff“, Brücke, Anker, Schlepper, Verband, nationale (digitale) Sicherheit, Souveränität & Resilienz oder nachhaltige Beschaffung sein kann, nein, muss, um zu gewinnen – die Funktion bestimmt die Form.**

Seit dem Jahr 2022 erarbeitet ein inspiriertes zivil-militärisches Grüppchen, wie Ressourcen (Personal, Zeit & Geld) so eingesetzt werden können, dass unsere Wertegemeinschaft nachhaltig geschützt werden kann. Daher liegt ein lange gereiftes, einfaches, schnelles, sofort für neue und zur Sanierung bereits laufender Projekte anwendbares, cpm-konformes, generisches System „Nachhaltige Rüstung“, das sämtliche Freiheiten nutzt, die eine Berufung auf nationale Sicherheitsinteressen i.S.d. Art. 346 AEUV bietet, vor. Und immer mehr Menschen und Organisationen zeigen nun ihre Lösungsansätze und Erfahrungen in der zweiten Sonderbeilage zum InfoBrief Heer.

## Expertise gewinnt!

Weil Expertise mehr ist als eine neue Teilstreitkraft, ein Beschleunigungsgesetz, Systemhaus oder weiße Turnschuhe als Label für Agilität. Expertise ist Können, was jeder wirklich kann. Wozu gehört in den Spiegel zu schauen und die Frage beantworten zu können: Habe ich alles getan, wozu ich – alleine und zusammen mit anderen – in der Lage wäre, es zu tun, um die zur Verfügung stehenden Mittel produktiv so einzusetzen, das Leib und Leben in Frieden und Wohlstand, meins und das der anderen, gemäß unseres Men-

schensbildes- und -rechtsverständnisses, geschützt werden?

Expertise(bildung) ist wertebasiert. Vom Individuum ausgehend, entwickelt sie sich im Miteinander. Grundlage sind Verantwortung (für sich und andere), Vertrauen (ineinander und aufeinander), Verlässlichkeit und Verbindlichkeit. Weder angeordnet noch geschult entwickelt sie sich on-the-job durch Auseinandersetzung und Verarbeitung von Erfahrung, ist keine Frage von (Shift in) Mindset, sondern von persönlichen Dispositionen, z.B. Mut, Reife, Rückgrat. Expertinnen und Experten ist egal, was sie dürfen: Sie machen einfach (souverän).

Gewinnt der beste Kompromiss oder die beste, innovativste, raffinierteste, überraschendste Lösung (vgl. Pager & Funkgeräte)? Expertise zieht Leistungsträger an, Überzeugungstäter, die jedes Muster brechen um zu tun, was gemacht werden muss – kleine, wendige, leistungsstarke, wirkungsvolle Schlepper und Lotsen, die kompromisslos gegen jegliches Gequengel auf der Brücke oder im Maschinenraum, die größten Containerschiffe der Welt auf der Stelle umdrehen. So funktioniert jeder Turnaround: Nicht notwendige Ressourcen werden aus dem System herausgenommen und die Organisation und jedes systemrelevante Projekt ohne Wenn und Aber grundsanitiert. Der Fokus muss auf den richtigen Dingen liegen. Es geht um's Überleben!

Expertisebildung gewinnt immer – laut meinen Forschungen – als erstes die Leistungsträger. Sie braucht – so die internationale Expertiseforschung – zehn Jahre in einer Domäne (z.B. Schiffbau, Führung, Beschaffung). So weit zu Restrukturierung,



Foto: Beatrix Palt - Vortrag auf dem Marineworkshop der DWT e.V.

gen, Personalentwicklungs-, Laufbahn-, Beurteilungs- und Beförderungssystemen, nicht nur im Verteidigungssektor. Die zweite Sonderbeilage des InfoBrief Heer ist wieder ein Manifest derer, die begriffen haben, dass Zeitenwende mehr ist, als Ressourcen auf ein System zu kippen. Sie ist Exzellenz in Expertise, forschungs- und wertebasierte Zeitenwende, neue Geschäftsmodelle zum effizienten und effektiven Einsatz von Ressourcen, damit Frieden und Freiheit finanziert und realisiert werden können. Die Sonderbeilage ist alphabetisch angelegt, ohne Titel etc., weil es auf die Expertise ankommt. Ich danke allen Autorinnen und Autoren, dem Förderkreis Heer e.V. und Peter Tamm mit seiner Redaktion. Danke Markus Lehmann für die Idee und Umsetzung, die KI mit dem Bauspiel spielen zu lassen. Wir werden sehen, ob es besser ist sich selbst den Kopf für die Entwicklung persönlicher Dispositionen zu zerbrechen oder der KI zu überlassen, was produktiver ist. Dazu könnten die zwei Herren etwas sagen, die nach meinem Vortrag auf dem Marineworkshop die verstreuten Steine zu den im Heft abgebildeten Verband zusammenbauten. Am Ende zählt nur: gewinnen.

**Bauspiel: Ein Schiff – Expertise gewinnt.**



Foto: Autor

# Expertisebildung und Forschung:

## Wargaming als realitätsidentisches Scenario Learning

Prof. Dr. Klaus Beckmann

Heuer fand die Wargaming Initiative Conference (WIN24) der NATO unter inhaltlicher Verantwortung der Führungsakademie der Bundeswehr an der Helmut-Schmidt-Universität statt. Sie wurde mit dem Ausbildungskongress der Bundeswehr unter inhaltlicher Federführung der Universität verbunden, der sich seinerseits dem Thema Wargaming verschrieben hatte – und die dieses Feld auch weiter betreuen soll. In der Auswertung beider Vorhaben konnte ich zufrieden feststellen, dass sich etwas in Deutschland bewegt im Wargaming, und dass der erwartete Trend klar aufwärts gerichtet ist. Im vorliegenden Beitrag möchte ich den aufwachsenden Bereich des „Wargaming“ für den militärischen Leser gleichsam kartographieren und einige seiner Felder bewerten.

### Wargaming 101

Ich definiere ein Wargame als eine *Simulation mit menschlichem Input*. Wir haben also erstens einen Mechanismus, der realweltliche Zusammenhänge modellhaft abbildet, und zweitens die Möglichkeit für menschliche Spieler, in diesen Mechanismus auf definierte Weise einzugreifen. Damit stellt ein SIRA<sup>1</sup>-Durchgang ein Wargame dar. Ein Übungsdurchgang am Gefechtsübungszentrum des Heers

(GÜZ) dagegen nicht, weil die Teilnehmenden unmittelbar miteinander interagieren und nicht über eine „zwischen geschaltete“ Simulation.

Der Mechanismus der Simulation kann unterschiedlichste Formen annehmen. Welches Design angemessen ist, ergibt sich aus dem *Zweck des Wargames*. Diese Frage wiederum zerfällt in zwei Teile, erstens nach der Ebene der Analyse, und zweitens nach der intendierten Anwendung. Die nachfolgende Tabelle zeigt eine Matrix, die durch die beiden Dimensionen aufgespannt wird, und die entsprechenden Anwendungsgebiete.

### Anwendungsfelder von Wargames

Bei der Analyse steht meist die Ebene der Handlungen, also der Courses of Action (COA) im Mittelpunkt. Davon strikt zu unterscheiden ist die Ebene der Regeln, also die Beschreibung des vorliegenden Wargame und des Simulationsmechanismus einschließlich der für die Spieler zulässigen Optionen. In der Ökonomik gehört diese Unterscheidung von Handlungen- und Regelebene seit Hobbess' Leviathan zum Inventar. Nun können auch Regeln Gegenstand strategischer oder operativer Entscheidungen sein. Das Diktum des chinesischen Strategen und Philosophs Sun Tzu, es gelte „die Schlacht

zu beginnen, bevor sie beginnt“ und die Vorstellung von Preemption in der militärischen Führungslehre beruhen darauf. Will man dies in einem Wargame endogenisieren, dann gilt es verschiedene Ebenen von Spielregeln zu unterscheiden, solche, die man dem Einfluss der Spieler unterwirft, und Meta-Regeln, welche das Ringen um die Regelsetzung ordnen. Ganz oben auf dieser Leiter findet sich die semantische Ebene. Wie wird betrachtet, welche Begriffe, aussagenlogischen Systeme und Modelle für die Formulierung des Wargames genutzt werden.

Mit Blick auf die Anwendungsmöglichkeiten sind drei Gruppen zu unterscheiden: eine Nutzung in der Ausbildung, zur Unterstützung von Entscheidungsfindungsprozessen oder als Vehikel für wissenschaftliche Forschung.

### Wargaming in der Ausbildung

Historisch betrachtet ist die Ausbildung in Truppenführung auf der taktischen und höheren taktischen Ebene der erste Anwendungsfall von Wargames, der weite Verwendung fand und in militärisch-professionellen Kreisen genutzt wurde. Die zentrale Rolle kam dabei dem Preußischen Kriegsspiel zu, welches der Kollege Jorit Wintjes von der Universität Würzburg wiederbelebt hat. Die Regeln wurden im Laufe des 19. Jahrhunderts, während dessen sich das Kriegsspiel weiter verbreitete und auch internationale Beachtung fand, immer wieder überarbeitet, so dass auch die technische Entwicklung, insbesondere der Reichweitzuwachs bei den Hauptwaffen der Infanterie und der Artillerie, abgebildet werden konnte.

Semantik		Doktrinenentwicklung	Weiterentwicklung des Wargaming
Regeln		Sensitivitätsanalysen, Konzeptentwicklung	Historische und politische Untersuchungen
Handlungen	Handlungstraining und Drill	Teil der Beurteilung der Lage	Laborexperimente
	Ausbildung	Analyse	Forschung

Einen vollständigen Überblick über Wargaming in der (militärischen) Ausbildung brauche ich noch nicht einmal zu versuchen. Auf zwei aktuelle Entwicklungen sei indessen hingewiesen: Zum einen beobachtet man einen Boom von „kleinen“, oft ressourcenschonend analog umgesetzten Wargames, die hybride Szenarien zum Gegenstand haben und damit die Zusammenarbeit in ressortübergreifenden Krisenlagen schulen. Beispiele dafür sind die Wargames „HYDRA“ und „Neustart“, die an der Führungsakademie der Bundeswehr und an der Helmut-Schmidt-Universität intensiv genutzt werden. Und auf der anderen Seite prägt der technische Fortschritt in virtueller und künstlicher Realität (VR und AR) die Möglichkeiten für Wargames in der Ausbildung. Diese Entwicklung verdankt vieles den Fortschritten in der Spielindustrie bei den First Person Shootern und taktischen 3D-Games, deren virtuelle Welten auf „Engines“ wie eben Unreal oder Virtual Battlespace (VBS) laufen. Zu der Abbildung der Umgebung gehören neben einer realistischen Modellierung der physischen Umgebung und der Simulation auch die Bedienelemente, welche den Spielern zur Verfügung gestellt werden.

### Wargaming zur Entscheidungsunterstützung und zur Konzeptentwicklung

Diesen Abschnitt zum zweiten großen Anwendungsbereich von Wargames leite wie folgt ein: Ein so genannter Rehearsal of Concept (ROC) oder Rocdrill ist glorifizierte Auftragswiederholung. Zwar wird Wargaming als Teil militärischer Entscheidungsverfahren mittlerweile anerkannt und findet sich bekanntlich als ein Schritt im Comprehensive Operations Planning Directive (COPD) der NATO, um nur ein Beispiel zu nennen. Namentlich auf taktischer Ebene wird es aber kaum genutzt. Das hat einen Grund: „Der Krieg ist ein wahres Chamäleon“ (Carl von Clausewitz), und seine Modellierung dauert Zeit. Weil jedes Gefecht in concreto verschieden ist, wird man möglicherweise nicht auf eine vorgefertigte Simulation zurückgreifen können, und die Anfertigung einer neuen, maßgeschneiderten, wird man sich unter dem erheblichen Zeitdruck auf der taktischen Ebene nicht leisten können.

Deswegen wird es hier beim klassischen Sandkasten — oder einer digitalen Version davon — und einer Art des „Red Teaming“ bleiben müssen, bei der die eigenen COAs und die möglichen Ge-

genmaßnahmen dargestellt und durchgesprochen werden. Auch hier muss es aber Schleifen und eine unabhängige Beobachtungsinstanz geben, gerade wie dies die COPD vorsieht.

Grundsätzlich jedoch wird man in diesem Bereich drei Dinge anstreben:

1. Auf der Ebene der Handlungen (COAs) kann man mit einem Wargame verschiedene Optionen ausprobieren — „What if?“ — und im Vergleich mit der Wahl der Gegenseite beste Antworten finden.
- 2.. Auf der Regelebene geht es zunächst um eine Sensitivitätsanalyse. Wie robust bleibt meine Möglichkeit des Handelns, wenn sich die Spielregeln (z.B. die technischen Daten, die Truppeneinteilung der Gegenseite, die Witterungsbedingungen, die Rules of Engagement, oder vieles mehr) ändern?
- 3.. Ganz oben erkenne ich, dass die gewählten Spielregeln und vor allem das zugrunde liegende Simulationsmodell mein erwartetes Kriegsbild und meine Vorstellung widerspiegeln, wie sich (militärische) Führungsaufgaben vernünftig lösen lassen. Reflektiere ich diese systematisch, so gewinne ich Erkenntnisse auf der fundamentalen Ebene der *Principles of War* und daraus Ableitungen treffend für die Formulierung von Doktrin.

Das alles dauert Zeit und kostet Mühe. Je niedriger die Entscheidungsebene, desto weniger wird man davon in laufenden Entscheidungsprozessen unter sonst gleichen Umständen Gebrauch machen können. In der Ausbildung haben wir viel Zeit, so dass man diesen Ansatz ebenfalls verfolgen kann.

### Wargaming in der wissenschaftlichen Forschung

Wir haben in den vergangenen Abschnitten gesehen, dass die derzeitige Nutzung von Wargames im Militär sich in erster Linie auf Trainingsfragen konzentriert. Die Analyse von Handlungsalternativen durch Variationen der Parameter und Regeln des Spiels spielt ebenfalls eine Rolle, allerdings nur die zweite Geige.

Völlig übersehen wird das Potenzial von Wargames im „Labor“, d.h. als Mittel zur Datenerhebung und Analyse tatsächlicher Entscheidungsprozesse durch Militärfachleute. Und ebenfalls unterbelichtet ist die Möglichkeit, durch eine Variation von Spielregeln mehr über die historischen Bedingungen von Entscheidungen zu lernen, also Wargames als Methode der Militärgeschichte einzusetzen.

Der Verfasser ist auf zwei Ebenen unterwegs, diese Lücke zu schließen. Erstens als Fachprofessor, und zweitens als Präsident einer Bundeswehruniversität. In der ersten Rolle habe ich im Rahmen der *NATO Wargaming Initiative* ein einfaches Wargame vorgeschlagen, das für Laborzwecke verwendet werden kann. Damit ein Wargame im Labor nützlich ist, muss es schnell und einfach spielbar sein, ohne hohe Kosten für Vorbereitung und Schiedsführung zu verursachen, sowie eine einfache Variation seiner Parameter ermöglichen. Auf der anderen Seite muss das Spiel sinnvoll sein, was bedeutet, dass es relevante Szenarien auf einer soliden theoretischen Grundlage modellieren muss.

### Ausblick

Die zweite Ebene meines Interesses gilt der Weiterentwicklung der Fähigkeit zum Wargaming im besonderen und zu Analyse und Simulation in der Bundeswehr im allgemeinen. Zunächst gilt es, die vielen Expertise-träger im Bereich von Modellierung, Spieltheorie, Simulation, Datenanalyse und Wargaming an den Universitäten der Bundeswehr besser zu vernetzen und für die gestiegene Bedeutung von „Dual use“ zu motivieren. Wo es noch Lücken gibt, müssen diese geschlossen werden.

Das Fundament an den Universitäten der Bundeswehr zu legen ist zwingend erforderlich, weil den anderen Ausbildungseinrichtungen und wissenschaftlichen Instituten die Grundlagenforschung, das ständige Messen an der internationalen wissenschaftlichen Community („Peer review“) und die universitäre Unabhängigkeit fehlen.

Gemeinsam mit den anderen Ausbildungseinrichtungen können auf dieser Basis dann sowohl die Fähigkeiten zu Simulation und Wargaming als auch deren Verwendung in Ausbildung und Einsatz noch weiter entwickelt werden. Als Marktplatz und Showcase für diese Ideen und Entwicklungen bietet sich der Ausbildungskongress der Bundeswehr an. ■

### Autor:

**Prof. Dr. Klaus Beckmann** ist seit 2018 Präsident der Helmut-Schmidt-Universität/Universität der Bundeswehr Hamburg



Foto: Tobias Koch

## Sicherheit durch Technik – Das Beschaffungswesen der Bundeswehr zum Innovationsmotor für unsere Streitkräfte ausbauen

Dr. Reinhard Brandl MdB

Das Beschaffungswesen der Bundeswehr muss darauf ausgerichtet werden, mit den immer schneller werdenden Technologiesprüngen mitzuhalten und die daraus entstehenden Möglichkeiten für unsere Streitkräfte zu nutzen. In den Konflikten der Zukunft muss sich die Truppe gegen hochmoderne und äußerst flexible Waffen, Technologien und operative Methoden durchsetzen können. Die Digitalisierung der Bundeswehr bedingt die synchrone Nutzung der Dimensionen Cyber- und Informationsraum CIR und Weltraum in der Fähigkeitsentwicklung und der Operation. Das zeigt der russische Angriffskrieg gegen die Ukraine deutlich. Dieser ist massiven Änderungen in der Gefechtsführung unterworfen. Originär zivile, aber auch Dual-Use-Technologien kommen immer stärker zum Einsatz. Die ukrainische Armee hat eindrucksvoll gezeigt, dass der systematische Einsatz von (Mini)-Drohnen, der Rückgriff auf Künstliche Intelligenz (KI) und moderne Software sowie die Nutzung des von dem US-Raumfahrtunternehmen SpaceX betriebenen Satellitennetzwerks STARLINK auch für eine zahlenmäßig vermeintlich unterlegene Armee erhebliche strategische Vorteile im Feld mit sich bringen. Zudem steigen durch wachsende Datenmengen, Rechenkapazitäten und immer kürzere Softwarezyklen die Anforderungen an bestehende und in Entwicklung befindliche Waffensysteme und Plattformen, sich fortlaufend an schnell verändernde Gefechtsfelder anzupassen und ihre Leistungsfähigkeit zu steigern. Dies ist zukünftig fast ausschließlich nur noch über Software zu erreichen.

### Die Bundeswehr rüstet sich noch für die Kriege der Vergangenheit

An all diesen Fronten ist die Bundeswehr blank. Das liegt daran, dass wir derzeit aus den skizzierten Eindrücken noch keine Schlussfolgerungen für die Bundeswehr und ihre Fähigkeiten ableiten, die letztlich die Beschaffung beeinflussen. Vielmehr rüsten wir uns immer noch für vergangene Konflikte. Mit dem Sondervermögen „Bundeswehr“ zum Beispiel werden vor allem Lücken geschlossen, die seit Jahren beschrieben worden sind. Um einmal beim Leitbild der vorliegenden Sonderausgabe des „InfoBrief Heer“ zu bleiben: Die Bundeswehr spielt noch nicht mit dem dynamischen Holzklotzspiel „Bauspiel – Ein Schiff“. Sie fokussiert nach wie vor lieber Revell-Baukästen, deren Modelle auf ewig zusammengeklebt werden. Damit sich neue Technologieentwicklungen im Lichte immer kürzerer Innovationszyklen in der Bundeswehr künftig materialisieren, müssen wir das Beschaffungswesen der Bundeswehr nach vorne ausrichten. Dazu schlage ich im Folgenden zehn Maßnahmen vor.

### 10 Punkte für ein zukunftsorientiertes Beschaffungswesen

1. Wir müssen eine Strategie zum Umgang mit neuen Technologien in der Bundeswehr entwickeln. Diese Strategie hat das Leitbild Multi-Domain-Operations (MDO) als der durchgehenden Digitalisierung militärischer Wertschöpfungsketten mit dem Ziel einer möglichst weitreichenden Autonomisierung im Einklang mit völkerrechtlichen und ethischen Handlungsprinzipien zu fördern. Es muss nachvollziehbar sein, wie wir in

Deutschland mit diesen Technologien im Sinne einer neuen Bedrohung für unsere Sicherheit und unsere Streitkräfte sowie andererseits für die eigene Integration und Nutzung in der Truppe umgehen möchten.

2. Der Sonderstab Ukraine im BMVg leistet bereits einen wertvollen Beitrag zur Einsatzbewertung des Ukraine-Kriegs, mit den Ableitungen aus Erfahrungen und Informationen aus der Ukraine insbesondere mit Blick auf technologische Entwicklungen in der Gefechtsführung für die eigenen Streitkräfte erhoben, analysiert und evaluiert werden. Der Ansatz sollte – gegebenenfalls auch fest institutionalisiert – weitergeführt und verstärkt werden, damit die gewonnenen Erkenntnisse noch rascher in die Weiterentwicklung der eigenen Operationsführung, des Materials und der Ausrüstung sowie der Ausbildung einbezogen werden können.

3. Wir brauchen mehr Cyber- und IT-Experten im Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAAINBw). Das gilt für alle Ebenen der Behörde, um der exponentiell steigenden Bedeutung von Cyber und IT in der Verteidigung bei strategischen Beschaffungsüberlegungen gerecht zu werden. Dazu müssen wir auch Quereinsteigern aus der Industrie den Zugang zum BAAINBw erleichtern.

4. Alle Rüstungsprojekte müssen ab sofort auf die Prinzipien und Technologien von MDO einschließlich der privaten Cloud der Bundeswehr (pCloudB) und

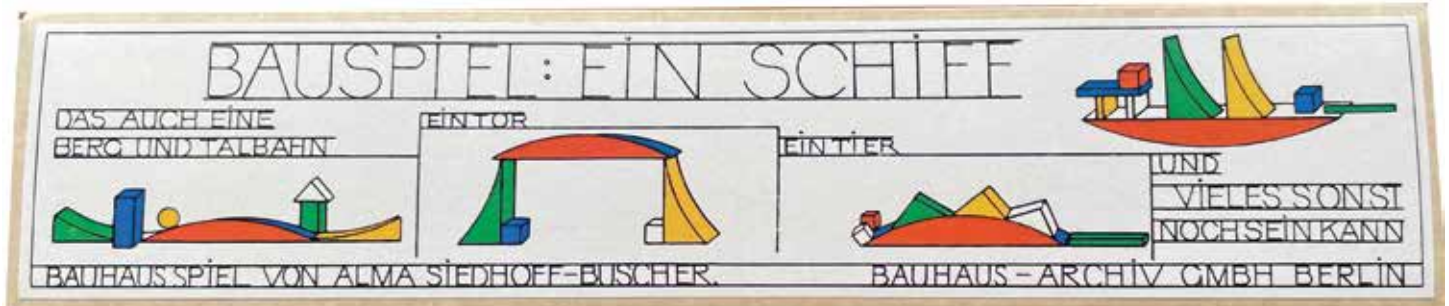


Foto: Beatrix Palt

den Ende-zu-Ende-Verbindungen sowie unter Berücksichtigung von Software-Defined-Defence (SDD) ausgerichtet werden, um den Anforderungen an eine hochagile Adaption von Waffensystemen auf neue Herausforderungen auf dem Gefechtsfeld gerecht zu werden. Vergabeverfahren und Verträge müssen die informationstechnischen Voraussetzungen von MDO von Beginn an berücksichtigen. Jedes Rüstungsgut ist plug-and-play-fähig an das zentrale MDO-Nervensystem der Bundeswehr zu gestalten. Standardisierte und wiederverwendbare Softwaremodule auf Basis einer normierten Middleware sowie offenen Schnittstellen und Datenformaten müssen unter Berücksichtigung multinationaler Interoperabilität entlang des Federated Mission Networking grundsätzlich ermöglicht werden.

5. Cyber und IT als Beschaffungsfeld und Bereiche mit hochdynamischen Innovationszyklen sind vom sogenannten „design freeze“ auszunehmen. Dieser wäre gerade dort, wo iterative und agile Entwicklungen dominieren, kontraproduktiv. Das Vergaberecht im Bereich von IT-Vergaben ist generell für das Modell des sogenannten „spiral development“ zu öffnen.

6. Die Bundeswehr muss als Auftraggeber für innovative Start-ups und kleine und mittlere Unternehmen (KMU) attraktiver werden. Diese verfügen oft nicht über die notwendigen Ressourcen zur Teilnahme an den langwierigen Beschaffungsprozessen. Wenn sie im Cyber Innovation Hub der Bundeswehr (CIHBW) eine Lösung entwickelt haben, sollten sie

Folgeaufträge erhalten können, ohne erneut eine weitere ressourcenzehrende Ausschreibung durchlaufen zu müssen.

7. Der CIHBW soll KMU und Start-ups im Bereich Defence und Dual-Use direkt nach dem Vorbild des High-Tech-Gründerfonds fördern können. Von allen operativen Akteuren im Geschäftsbereich des BMVg hat er in diesem Bereich die größte Expertise.

8. Die Vernetzung und Verflechtung von Defence-Start-ups und KMU mit großen Unternehmen sowie der Bundeswehr, die als Hubs und Experimentierumfeld für gemeinsame, agile und innovative IT-Lösungen agieren können, ist zu fördern. Die etablierten Industriepartner und die Bundeswehr können die Technologien der Start-ups mit ihrem Know-how häufig besser bewerten, direkt in die Waffensysteme integrieren und über den gesamten Lebenszyklus betreiben. Das ermöglicht es den kleinen Unternehmen ihre Produkte trotz des komplexen und langwierigen Beschaffungswesens in die Truppe einzubringen.

9. Zivilklauseln müssen auf den Prüfstand gestellt und gegebenenfalls aufgehoben werden. Dadurch setzen wir insbesondere bei Dual-Use-Forschung Spillover-Effekte in beide Richtungen frei und erzielen Effizienzgewinne hinsichtlich Zeit, Personal und Kosten.

10. Es muss deutlich mehr Geld für die wehrtechnische Forschung und Technologie veranschlagt werden. Der Entwurf für den Verteidigungshaushalt 2025 sieht

der Summe von Einzelplan 14 und Sondervermögen „Bundeswehr“ eine Absenkung des Ansatzes um rund 97 Mio. Euro auf etwa 517 Mio. Euro vor. Um aber Schlüsseltechnologien zu sichern und industrielle Fähigkeiten, Fachwissen bei Zukunftstechnologien sowie hochspezialisierte Arbeitskräfte in Deutschland zu erhalten, muss die Finanzierung der Wehrforschung auf bis zu einer Milliarde Euro erhöht werden.

### Fazit

Laut Experten wird Russland in fünf bis acht Jahren dazu in der Lage sein, die NATO herauszufordern können. Daher müssen wir unsere Streitkräfte dringend auf zukünftige Technologien vorbereiten und sie damit ausrüsten. Denn die westliche Philosophie sah bereits im Kalten Krieg nicht die zahlenmäßige Überlegenheit auf dem Gefechtsfeld vor, sondern demonstrierte durch eine technologische Überlegenheit ihre Dominanz und Abschreckung. ■

### Autor:

**Dr. Reinhard Brandl MdB** wurde am 01. August 1977 in Ingolstadt geboren. Seit 2009 ist er direkt gewählter Abgeordneter (CSU) für den Deutschen Bundestag im Wahlkreis Ingolstadt. In der 20. Legislaturperiode ist er im Bundestag Mitglied im Verteidigungsausschuss und im Gremium Sondervermögen „Bundeswehr“. Zudem ist er der digitalpolitische Sprecher der CDU/CSU-Bundestagsfraktion und Mitglied im Ausschuss für Digitales.



Foto: Bundeswehr

## Neue militär-strategische Kultur braucht einen Musterbruch

Flottenadmiral Christian Bock

**Wer mittlerweile schon das „End of Zeitenwende“ prognostiziert, unterschätzt das Leistungspotenzial derjenigen, die wollen und können! Aber dafür braucht es Grundlagen: Die strategischen Zusammenhänge von Nationaler Sicherheit, Verteidigungsbereitschaft, eigener Souveränität auch in Bündnissen und gesellschaftlicher Resilienz sind kaum breit bekannt. Die Zusammenhänge werden nicht zugänglich erklärt, nicht erlebbar gemacht und Entscheidungen folglich nicht danach ausgerichtet. Wie also schafft man eine solche Expertise(bildung) sowohl in allen Bereichen der Gesellschaft als auch innerhalb der Bundeswehr? Der Beitrag macht Vorschläge zum Weiterentwickeln der strategischen – vor allem militärstrategischen – Kultur in Deutschland.**

Noch einmal zur Einordnung: Die „Zeitenwende“ drückt sich im politischen Kern aktuell in zwei Dokumenten aus. Die Nationale Sicherheitsstrategie (NSS) der Bundesregierung und die Verteidigungspolitischen Richtlinien (VPR) sind Zeichen eines strategischen Umdenkens und von Veränderungen des strategischen Handelns in Deutschland. Mit dem Krieg in Europa, den Konflikten im Nahen Osten bis hin zum Indopazifik bedurfte es für Deutschland einer neuen strategischen Positionierung, gemeinsam mit den Veränderungen in NATO und der EU, um heute wie zukünftig gemeinsam mit Verbündeten und Partnern in dem sich kontinuierlich gefährlichen und komplexen strategischen Bedrohungsumfeld bestehen zu

können. Aber: Es sind halt nur Dokumente! Wie übersetzen sich die Inhalte in Expertise?

Dabei sind die NSS und die VPR bereits der Beginn eines Musterbruches – ein Ausbrechen aus bisherigen Pfaden. Eindeutig legen sie fest, dass wir uns mit feindlich gesinnten Staaten und Systemen und deren Aktivitäten auseinandersetzen und mit Gegenhandeln unsere Interessen schützen müssen. Dafür gilt es, die politischen Vorgaben mittels konkreter Maßnahmen umzusetzen. Die Militärstrategie der Bundeswehr, die gerade erstellt wird, enthält deshalb nicht nur militärstrategische Ziele und abgestimmte Effekte für unterschiedliche geostrategische Regionen. Sie muss auch von Maßnahmen flankiert werden, welche eine (militär-)strategische Kultur – das inhärente Verständnis der Zusammenhänge strategischer Abhängigkeiten in weiten Teilen der Gesamtbevölkerung – in Deutschland stärken. Warum? Weil einerseits jeder Bürger das Recht hat, die Sinnlogik unterschiedlicher Optionen des Einsatzes als auch Entscheidungen über das Militär zu verstehen. Andererseits ist es viel zu leicht, militärstrategisches Handeln bis hin zu diesbezüglichen politischen Entscheidungen als „Willkür“ abzutun und (bewusst) zu delegitimieren. Wie also bohrt man das dicke Brett, um der deutschen Gesellschaft als auch dem System Bundeswehr „Strategiedenke“ einzuhauchen?

Die Militärstrategie bekommt deshalb einen öffentlichen Dokumententeil. Im Grunde bedarf es neben diesem weiteren Dokument der Militärstrategie zusätz-

lich einer auf Dauer angelegten Kampagne, zusammengesetzt aus diversen Optionen und Maßnahmen für und mit unterschiedlichsten Ebenen und Multiplikatoren, von den Bundeswehrinstitutionen, den mündigen Bürgern, Fachleuten, politische Entscheidern, Medien, Bildung und Forschung bis zu den einschlägigen Think Tanks und über die Stammtische der Nation.

Militär-strategische Kommunikation und Öffentlichkeitsarbeit muss man für eine Kampagne wollen und können! Insofern ist allein schon diese Beilage ein Teil dieser Expertisebildung, welche u.a. die fachkundigen Netzwerke des Förderkreis Deutsches Heer und des Deutschen Maritimen Instituts über deren Medien erschließt. Was kann man sonst noch nutzen?

Den Generalinspekteur muss als militärischer Berater der Bundesregierung ein System umgeben, dass das immer komplexer werdende Handlungs- und Bedrohungsumfeld und dessen Auswirkungen auf Deutschland und unsere Partner durchdringt, um militärstrategische Handlungsoptionen als Beitrag zur Gesamtverteidigung entwickeln zu können. In dem interdependenten System zivil-polizeilich-militärisch integrierter Sicherheit springt es zu kurz, militärische Optionen losgelöst von gesamtgesellschaftlichen Aspekten wie z.B. der staatlichen Daseinsvorsorge und der Inneren Sicherheit zu betrachten. Die besondere Expertise des Militärischen Führungsrats könnte beispielsweise durch ein Forum oder Netzwerk interdisziplinärer Expertise ergänzt



Foto: Beatrix Palt

werden, welches anlassbezogen übergeordnete Antworten auf zukunftsgerichtete militärstrategische Fragestellungen unter Einbeziehungen von Experten aus der Wissenschaft, der Wirtschaft, der Gesellschaft, des Militärs und anderen Bereichen erarbeitet. Mit dem offenen Austausch verschiedener Einschätzungen und Perspektiven – außerhalb etablierter und fester Strukturen – könnten im Idealfall neue, überraschende Ideen und innovative Konzepte zur Lösung vorrangig militärstrategischer Problemstellungen entstehen. Militärstrategische Beratungs- und Entscheidungskompetenz ebenso wie der Diskurs darüber für und in der Bundeswehr würde gestärkt. Bw-interne Expertise könnte über die Teilnehmer des Forums als Multiplikator nach außen wirken, indem sie militärstrategische Fragestellungen und bundeswehreigene Expertise bewusst in den öffentlichen Diskurs einbringt.

Wir könnten auch von Partnern lernen! Eine klare (militär-)strategische Positionierung in der Welt und in den Bündnissen erfordert, sich eigene Stärken und Schwächen im Vergleich zu Gegnern bewusst zu machen. Große Nationen nutzen „Net Assessments“ als ein Tool, um dieses Bewusstsein zu schärfen. Damit analysieren und beurteilen Experten systematisch relative Stärken und Schwächen von Kontrahenten. Militärische, technologische, politische, wirtschaftliche und andere Faktoren werden vergleichend untersucht und daraus das Verhältnis zwischen den jeweiligen militärischen Fähigkeiten von Staaten aus verschiedenen Perspektiven bestimmt. Ausschlaggebend sind

nicht die absoluten Fähigkeiten der Kontrahenten, sondern das Kräfteverhältnis und die voraussichtliche Entwicklung dieses Verhältnisses. Die Ergebnisse dieser militärstrategischen Analyse haben die Charakteristik in die Zukunft gerichteter Diagnosen, um die Entwicklung militärischer Kräfteverhältnisse zu verstehen. Die Diagnosen zeigen naturgemäß immer Problemstellungen und -felder auf, die die priorisierte Aufmerksamkeit der politischen Leitung und auch des Souveräns erfordern, weil sie eine Gefahr für die (existenziellen) Interessen des Staates, und somit für die Nationale Sicherheit bedeuten. Solche (ungeschönten) Diagnosen wären ein Mehrwert für jeden Entscheider auch außerhalb der Bundeswehr, bedeuten aber ebenfalls einen Musterbruch zur Stärkung der strategischen Kultur.

Ein Musterbruch wird schon jetzt vollzogen in der Strategieausbildung in den Streitkräften und an Universitäten. Während an den Universitäten der Bundeswehr die Einführung von Studiengängen wie „Strategic Studies“ vorangetrieben wird, steigt auch in der zivilen akademischen Welt die Nachfrage nach (militär-)strategischen Inhalten. Für eine verstärkte Zusammenarbeit der Bundeswehr mit zivilen Bildungseinrichtungen für militärstrategische Inhalte sind natürlich noch umfassende Abstimmungen mit den zuständigen Ministerien von Bund und Ländern durchzuführen. Diesen steinigen Weg gilt es aber zu gehen, um die militärstrategische Kultur zu stärken. Die Anpassung der militärstrategischen Ausbildung in den Streitkräften ist da bereits

deutlich weiter. Ab 2025 werden Inhalte zu Kriegstheorie und Strategie in der Offizierausbildung erhöht. Angefangen vom jungen Leutnant bis zum lebens- und dienst erfahrenen Stabsoffizier werden die Kompetenzen zum ganzheitlichen Verständnis der Rolle des Militärs im Rahmen der gesamtgesellschaftlichen Verteidigung zur Abwehr von Bedrohungen schrittweise gestärkt.

Der Weg zu einer wehrhaften Gesellschaft – wie er in der Nationalen Sicherheitsstrategie vorgegeben ist – wird von der Bundeswehr konsequent beschriftet. Die erforderlichen Musterbrüche werden Konflikte erzeugen und Kraft kosten. Das erfordert Persönlichkeiten, die nach dem Zitat eines bekannten preußischen Generals handeln: „... an der Glut in seiner Brust, an dem Lichte seines Geistes soll sich die Glut des Vorsatzes, das Licht der Hoffnung aller anderen von neuem entzünden.“<sup>1</sup> Zum Glück gibt es viele, die wollen und können! ■

<sup>1</sup> Carl von Clausewitz, Vom Kriege, Buch 1

#### Autor:

**Flottenadmiral Christian Bock** ist als 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: Autorin

## Expertisebildung ist (jetzt) digital – aber der Mensch ein soziales Wesen

Andrea Bruckner

**Früher geschah Expertisebildung persönlich und vor Ort. Digitalisierung hat viel verändert – und das Lernen autonomer gemacht.**

Wirtschaftsprüfer müssen – wie andere Experten auch – schon immer eine anspruchsvolle Ausbildung absolvieren: ein Hochschulstudium bestehen und eine mehrjährige Praxisphase in einer Wirtschaftsprüfungsgesellschaft leisten, wo die Durchführung von Abschlussprüfungen als Mitglied des Prüfungsteams – angeleitet und überwacht durch erfahrene Kolleginnen und Kollegen – gelernt wird.

In der Vergangenheit war es bildlich so: Die Jungen saßen neben dem Älteren und Erfahreneren im Prüferzimmer und erhielten Vorgaben und Hinweise, was zu tun war. Durch zeitnahe persönliche Rückmeldung zu der erledigten Arbeit und im Rahmen von Feedback-Gesprächen im Prüferzimmer wurde so Schritt für Schritt gelernt, auf was es bei der Durchführung der Abschlussprüfung ankam. Nach und nach wurden neue Aufgaben und Themengebiete zur Prüfung übertragen, so dass sich Verständnis und Wissen praxisnah weiterentwickelten. Überall zuschauen und zuhören, Umsetzung der fachlichen und regulatorischen Vorgaben durch unmittelbare Anleitung in praxistaugliches Wissen – so haben durch „Training on the Job“ Generationen von Wirtschaftsprüfern ihren Beruf erlernt.

### Grundlegende Veränderung des Berufsbildes

Für die Umsetzung der gesetzlichen, regulatorischen und fachlichen Anforderungen in einer weniger digitalisierten Welt funktionierte das. Auch war die Abschlussprüfung weniger detailliert geregelt – so gab es bis zu Beginn des Jahres 2000 nur drei Fachgutachten, die prinzipienorientierte Vorgaben zur Durchführung der Abschlussprüfung und Erteilung des Prüfungsurteils enthielten.

Ab 1998 wurden die internationalen Prüfungsstandards sukzessive in deutsche Prüfungsstandards transformiert. Die Unternehmen wurden immer digitaler, die IT-kontrollbasierte Abschlussprüfung wurde relevant. Die ersten großen Skandale Anfang des Jahrtausends brachten als Reaktion eine stärkere Berufsaufsicht. Die Anforderungen an den Ablauf, Durchführung und Dokumentation der Abschlussprüfung stiegen und wurden extern kontrolliert. Damit wurde die Berufsausübung des Wirtschaftsprüfers in seiner Funktion als Abschlussprüfer grundlegend verändert.

Digitalisierung und immer neue Regulatorik verändern auch heute kontinuierlich die Anforderungen an die Berufsausübung, aber auch an das Lernen, die Expertisebildung. Heute erfol-

gen Durchführung und Dokumentation der Abschlussprüfung ausschließlich digital, es werden Kenntnisse der Anwendung und des Umgangs mit entsprechenden IT-Applikationen benötigt.

Auch der Prüfungsgegenstand, der vom geprüften Unternehmen erstellte Abschluss und die relevanten zu prüfenden Geschäftsprozesse sind i.d.R. digital und verlangen ein entsprechend angepasstes prüferisches Vorgehen. Deshalb besteht heute ein Prüfungsteam nicht nur aus unterschiedlich erfahrenen Prüfern, sondern auch aus verschiedensten Experten – etwa IT-Auditoren. Effizienz und Qualität einer Abschlussprüfung hängen von der Steuerung multidisziplinärer Teams bei Einhaltung umfangreicher beruflicher und fachlicher Vorgaben ab. Lernen durch Anleitung, Beobachtung, Überwachung und Feedback muss auch diese Elemente enthalten. Damit ist das (Projekt-)Management der Durchführung der Abschlussprüfung eine anspruchsvolle und relevante Aufgabenstellung des verantwortlichen Wirtschaftsprüfers.

Berufliche und fachliche Vorgaben und Wissen für den sukzessiven Aufbau bis zum Berufsexamen werden als kontinuierliche Schulungsangebote für die examinierten Wirtschaftsprüfer





Foto: J. Elstermeier

bereitgestellt. Basis für das zusätzlich benötigte Expertenwissen bleibt aber das Erfahrungswissen der routinierten Wirtschaftsprüfer. Art, Inhalt und Umfang der Abschlussprüfung verändern sich kontinuierlich, aber Lernen ‚on the job‘ bleibt zentral, weil (Berufs-) Erfahrungen und das Reifen der Persönlichkeit im Miteinander, im Austausch, in der persönlichen konstruktiven Auseinandersetzung entstehen.

### Die Corona-Pandemie als Einstieg in ein digitales ‚on-the-job-training‘

Durch die Corona-Pandemie entfielen ad-hoc „Prüfungen vor Ort“ und Präsenzs Schulungen. Alles wurde virtuell: virtuelle Trainings auf ‚Teams‘, Webseminare und Videoaufzeichnungen. Der Schwerpunkt lag auf der Wissensvermittlung: flexibel, „konservierbar“ und jederzeit abrufbar. Didaktische oder soziale Komponenten waren erst weniger ausgeprägt, wurden aber sukzessive implementiert. Das ist wichtig, weil durch Übungsfragen eine gewisse Überprüfung stattfindet, ob das vermittelte Wissen auch verstanden wurde. Da das aber nur einen geringen Aussagewert hat, muss die Überprüfung der Umsetzung in der Tagesarbeit in Form von Überprüfungen der Auftragsabwicklungen stattfinden. Trotzdem gilt: Diese Form der virtuellen Zusammenarbeit ist eine erhebliche Herausforderung für die Expertisebildung.

Denn das Lernen in „Tandems aus erfahrenen und weniger erfahrenen Prüfern“ funktioniert nur noch, wenn die erfahrenen Prüfer sich auch in Zeiten der virtuellen Zusammenarbeit aktiv um die Berufseinsteiger und weniger erfahrenen Kollegen kümmern. Die Expertisebildung wird damit zur echten und wichtigen Führungsaufgabe.

### Was lernen wir daraus?

Die Praxiserfahrung in der Zusammenarbeit in Prüfungsteams mit unterschiedlichem Erfahrungswissen ist also weiterhin notwendig für die Expertisebildung - Lernen ohne die unmittelbare Anleitung durch Erfahrene ist nicht ausreichend, die komplexen Anforderungen an die Durchführung einer effizienten und qualitativ hochwertigen Abschlussprüfung sicherzustellen. Wichtig wird sein, Expertisetandems dabei zu begleiten, Nähe, Austausch und konstruktive Auseinandersetzung virtuell genauso fachlich versiert, vertrauens- und verantwortungsvoll ernst zu nehmen und zu leben, wie es im persönlichen Miteinander funktioniert. Das setzt Wollen und Können voraus.

Dennoch ist Digitalisierung des Lernens ein großer Gewinn. Sie gibt uns neue Formen der Wissensvermittlung – und rundet unser Angebot in dieser Hinsicht ab. Aber wir müssen uns dazu insbesondere der Führungsaufgabe, also

der ergänzenden Anleitung und des Austausches von erfahrenen Kollegen mit Berufseinsteigern, explizit widmen. Diese Führungsaufgabe benötigt Kapazitäten und muss durch das Unternehmen aktiv geschult und gefordert werden. Nachhaltige Entwicklung von Wirtschaftsprüfern ist mehr geworden als die Vermittlung von beruflichen und fachlichen Standards. ■



### Autorin:

**Andrea Bruckner** ist eine erfahrene Wirtschaftsprüferin und Steuerberaterin und seit dem 1. Juli 2023 zusammen mit Parwáz Rafiqpoor Co-Vorstandsvorsitzende der BDO AG Wirtschaftsprüfungsgesellschaft. Gemeinsam verfolgen sie den integrativen Ansatz von Wirtschaftsprüfung und Beratung und leben dabei gleichzeitig eine klare Aufgabenverteilung. Dabei ist Andrea Bruckner für sämtliche internen Bereiche der Gesellschaft sowie das Qualitäts-/Compliance- und Risikomanagement, die digitale Transformation und die Nachhaltigkeit zuständig.



Foto: Autor

## Vergaberecht: Gestalten statt bekämpfen!

Rechtsanwalt Norbert Dippel

Gemäß den Verteidigungspolitischen Richtlinien sind „Abschreckungsfähigkeit, Kriegstüchtigkeit sowie Wirksamkeit im Einsatz (...) der Anspruch an eine zukunftsfähige, voll ausgestattete sowie dauerhaft und jederzeit einsatz- und kampfbereite Bundeswehr“. Damit ist klar: Zur Erlangung der Kriegstüchtigkeit kommen dem Beschaffungswesen und der Anwendung des Vergaberechts eine zentrale Bedeutung zu.

Die gern auch in Talkshows vorgebrachten Forderungen nach exzessiver Anwendung vergaberechtlicher Ausnahmen und radikalen Vereinfachungen verdecken dabei die eigentliche Problemstellung: Selbst wenn es kein Vergaberecht gäbe, müsste ein fachlich kompetenter Vertragspartner ausgewählt (vergaberechtlich: Eignungsprüfung), der Vertragsgegenstand definiert (vergaberechtlich: Leistungsbeschreibung) und bei mehreren möglichen Produkten oder Dienstleistern eine Auswahlentscheidung getroffen werden (vergaberechtlich: Wertungsentscheidung). Somit bestünde auch ohne Vergaberecht eine sachliche Notwendigkeit, die entsprechenden Schritte abzuarbeiten. Mit Blick auf etwaige Verbesserungen ist folglich der Ausgangspunkt sachlich geboten, sich in einem bekannten und bewährten vergaberechtlichen Rechtssystem zu bewegen. Unabhängig hiervon sind Möglichkeiten zur Verbesserung und insbesondere Beschleunigung des Beschaffungsprozesses auszuschöpfen.

### Gesetzesänderungen

Mit dem Bundeswehrbeschaffungsbeschleunigungsgesetz (BwBBG, 2022) wurde der Rechtsrahmen angepasst. Der Hauptanwendungsfall des BwBBG in der Praxis betrifft eine Aufweichung des Grundsatzes der losweisen Vergabe zugunsten der Generalunternehmervergabe. Von den im 19. Rüstungsbericht genannten 229 Anwendungsfällen des neuen Gesetzes betrifft dies 218 Fälle. Weitere 10 Anwendungsfälle betreffen vergaberechtliche Ausnahmen für Beschaffungen durch internationale Organisationen sowie Beschaffungen für Zwecke des militärischen Nachrichtenwesens unter Nutzung der neuen gesetzgeberischen Klarstellungen. In einem weiteren Fall kam eine neue Auslegungshilfe zur Vorabgestattung des Zuschlags aus Gründen eines überwiegenden Interesses der Allgemeinheit an einem raschen Abschluss des Vergabeverfahrens zum Tragen. Mit der neuen gesetzlichen Regelung wurde klargestellt, dass die unmittelbare Stärkung der Einsatzbereitschaft der Streitkräfte bei dem Abwägungsprozess zu berücksichtigen ist.

Um diese Rechtsänderungen und Anwendungsfälle richtig einordnen zu können, ist das Verständnis des Zusammenspiels von Europarecht und nationalem Vergaberecht wesentlich: Das Europarecht gibt insbesondere mit der Richtlinie 2009/81 über Vergaben im Verteidigungs- und Sicherheitsbereich den Rahmen vor, den das jeweilige nationale Recht umzuset-

zen hat. Dementsprechend können sich etwaige nationale Gesetzgebungsvorhaben nur in dem Rahmen bewegen, den das Europarecht eröffnet.

Betrachtet man sich die Aufweichung des Grundsatzes der losweisen Vergabe, fällt zunächst auf, dass das EU-Verteidigungsvergaberecht keine entsprechende Vorgabe enthält. Damit hat das BwBBG Freiheitsräume geschaffen, die das EU-Vergaberecht schon immer und noch im weiteren Maße vorgesehen hat. Es wurde lediglich eine deutsche Sonderlocke teilweise abgeschafft. Ein großer Teil dieser Gesamtvergaben wäre zudem auch bei der älteren Rechtslage möglich gewesen, wenn auch mit höherem Begründungsaufwand. Ähnliches gilt für die übrigen Anwendungsfälle, bei denen nunmehr die Berufung auf Ausnahmetatbestände leichter fällt. Rechtlich möglich war dies aber auch schon vor der Rechtsänderung, wenngleich mit höherem Begründungsaufwand. Die Klarstellungen und Erleichterungen des BwBBG leisten somit einen Beitrag zur schnelleren Beschaffung, indem sie vornehmlich den internen Begründungs- und Dokumentationsaufwand verringern. Zu hohe Erwartungen sollten damit aber nicht verbunden werden.

### Amtsinterne Maßnahmen

Bei der Betrachtung der Zahlen scheint der Erfolgsfaktor für eine funktionierende Beschaffung nicht in einer Veränderung des rechtlichen Rahmens zu liegen, sondern in der Art, wie das

Vergaberecht angewandt wird. Im Jahr 2023 wurden insgesamt 942 Vergabeverfahren im Oberschwellenbereich vom BAAINBw durchgeführt. Davon wurden lediglich 4 Verfahren im Wege eines Nachprüfungsverfahrens angegriffen. Im Ergebnis wurden sämtliche Nachprüfungsanträge zurückgenommen bzw. das BAAINBw hat die Verfahren gewonnen. In diesem Zeitraum wurden insgesamt 69 Rügen von Bieterinnen eingelegt, wovon in 20 Fällen teilweise oder ganz abgeholfen wurde. Hinzu kommt, dass in 2024 – soweit bekannt – bislang kein einziger Nachprüfungsantrag gestellt wurde.

Diese Zahlen weisen den Weg eindeutig in Richtung der engagierten und fachlich kompetenten Arbeit des BAAINBw. Die qualitätssichernden Maßnahmen bei der Begleitung der Vergabeverfahren tragen erheblich zur Rechtssicherheit und damit zur Beschleunigung bei. Hierzu gehört insbesondere auch die fachlich fundierte Auseinandersetzung mit Rügen durch das Justizariat des BAAINBw in Zusammenarbeit mit den Fachreferaten. Offensichtlich kommt der rechtlich tiefen und sachkundigen Behandlungen eine befriedende Wirkung zu. Wird mit der Rüge sachgerecht umgegangen, erübrigt sich meistens der Gang vor die Vergabekammer.

Hinzu kommen Maßnahmen der Qualitätssicherung im Vorfeld der Ausschreibung und vor allem vertiefte Prüfungen bei der Begründung von Ausnahmetatbeständen. Das alles erfordert personelle Ressourcen. Wie die Zahlen zeigen, sind diese offensichtlich gut investiert und führen insgesamt zu Beschleunigung und Rechtssicherheit. Die Zahlen belegen: Richtig angewandt ist das Vergaberecht durchaus praxistauglich.

### **Systembedingte Verwerfungen**

Die vorstehenden Ausführungen dürfen den Blick auf systembedingte Verwerfungen nicht verstellen, die insbesondere bei der Durchführung größerer Beschaffungsvorhaben auftreten können. Der linear organisierte Beschaffungsprozess gliedert sich in unterschiedliche

aufeinander aufbauende Teilschritte. Selbst bei Verkürzung der einzelnen Prozessschritte, bleibt es bei der linearen Abfolge. Gerade bei Großprojekten und bei sehr innovativen Beschaffungsgegenständen entwickeln die Verhandlungen mit den unterschiedlichen Bieterunternehmen ihre eigene Dynamik. Insbesondere in dieser Phase können die Bieterunternehmen ihr spezifisches Know-how im Hinblick auf die technische Lösung, der Finanzierung usw. in die Verhandlungen einbringen. Werden dadurch neue Aspekte aufgeworfen, die frühere Genehmigungsschritte betreffen, können die dann erforderlichen neuen Abstimmungen schnell zu zeitlichen Verzögerungen führen. Vor diesem Hintergrund besteht die Gefahr, dass die industrieseitig technisch oder wirtschaftlich bessere Lösung aufgrund der systemimmanenten Restriktionen keine Beachtung findet.

Ähnlich kann sich das Streben nach Rechtssicherheit auswirken. Verhandlungsbedingte Abweichungen von früheren Festlegungen bergen immer auch die Gefahr der rechtlichen Angreifbarkeit. Wird die Rechtssicherheit mit starren Festlegungen erkaufte, können Wirtschaftlichkeit und Innovation das Nachsehen haben.

Zudem weist die veränderte Sicherheitslage eine erhebliche technische Dynamik auf. Wie sich am Beispiel des Ukraine-Krieges zeigt, folgt auf die jeweilige technische Neuerung der einen Seite sehr zeitnah die entsprechende Reaktion der Gegenseite. Angesichts dieses sehr dynamischen Prozesses bleibt kein Raum für langwierige und starr aufeinander folgende Abstimmungs- und Genehmigungsprozesse auf der Auftraggeberseite, die wiederum in Verhandlungsrunden mit den Bieterinnen gespiegelt werden müssen.

Damit führen die systembedingten Verwerfungen aufgrund der derzeitigen Strukturen des Beschaffungswesens und der gelebten Beschaffungspraxis insbesondere bei Großprojekten zu einer inhärenten systembedingten Gefährdung der Kriegstüchtigkeit.

Die Lösung des Systemfehlers liegt nicht in einer weiteren Veränderung der Regulatorik, sondern in der ausdrücklich offensiven Anwendung der politischen Richtlinienkompetenz im Sinne der Kriegstüchtigkeit. Der Schutz seiner Bürger und der Funktionsfähigkeit seiner Institutionen bei Katastrophe, Krise und Krieg muss prioritäres politisches Ziel werden. In der angespannten Sicherheitslage müssen sich diesem Ziel andere Belange unterordnen und Entscheidungen im Sinne der Kriegstüchtigkeit engagiert und stringent umgesetzt werden.

Eine praktischer Ansatz könnte in einer stärkeren Einbindung des industriellen Know-hows in den Beschaffungsprozess liegen. Um das Bieter-Know-how einzubinden, bietet das Vergaberecht mit dem Verhandlungsverfahren und dem bisher nur stiefmütterlich genutzten wettbewerblichen Dialog eine taugliche Grundlage. Voraussetzung ist jedoch, dass tatsächlich umfassende und ergebnisoffene Verhandlungen geführt werden.

Um diese effizient gestalten zu können, müssen auftraggeberseitig neue Festlegungen auch mit Blick auf den bisherigen internen Abstimmungsprozess „durchgedrückt“ werden können. Der bislang weitgehend lineare Prozess würde damit durchbrochen. Vergewärtigt man sich die politischen Dimensionen richtungsweisender Beschaffungsvorhaben, muss dieser Weg auch die politische Rückendeckung haben. Sollte die Bedrohungslage tatsächlich so sein, dass in wenigen Jahren eine kriegerische Auseinandersetzung droht, muss Beschaffung deutlich aufgewertet und zur politischen Chefsache gemacht werden. ■

#### **Autor:**

**Norbert Dippel** ist Rechtsanwalt und Fachanwalt für Vergaberecht in Bonn.



Foto: Lutz Kampmann



Foto: Michael Dost

## Bewältigung geopolitischer Spannungen

### Innovationsdruck und Cyberrisiken aus Sicht eines mittelständischen Unternehmens: Expertise(bildung) als strategischer Ansatz für Innovation und Sicherheit

Lutz Kampmann und Michael Dost, Northrop Grumman LITEF

Mit einem multifunktionalen strategisch Ansatz begegnet LITEF als deutsches mittelständisches Unternehmen in der Entwicklung und Herstellung von Navigations- und Sensorsystemen den Herausforderungen durch geopolitische Spannungen, Innovationsdruck und Cyberrisiken. Vor dem Hintergrund globaler Konflikte, wie in der Ukraine, Israel und der Taiwanstraße, steigt die zentrale Rolle inertialer Systeme in militärischen Anwendungen und verschärft die Notwendigkeit, Informationssicherheit und fortschrittliche Fähigkeiten im Bereich der künstlichen Intelligenz (KI) auszubauen. LITEF steht als Entwickler inertialer Navigationssysteme vor der doppelten Herausforderung der externen Bedrohungslage bei gleichzeitigen internen Umstrukturierungen, beispielsweise hin zu SAP S/4 HANA, zu begegnen. Das Unternehmen meistert die Risiken und komplexen Herausforderungen wie Eskalation, Cyberangriffe, Sabotage und weitere sicherheitsrelevante Bedrohungen im Spannungsfeld von Transformationsdruck, Cybergefahren und einem volatilen Umfeld durch gezielte strategische Maßnahmen in den Berei-

chen Expertise, Organisation, Technologie und Informationssicherheit. Dieses Vorgehen kann als Blaupause für mittelständische Unternehmen dienen, die vor ähnlichen Herausforderungen stehen und nach effektiven Lösungen suchen.

#### Resilienz als Exogene und Endogene Herausforderung

Der Ukraine-Krieg hat nicht nur militärische, sondern auch technologische Dimensionen. Inertiale Navigationssysteme (INS) spielen eine zunehmend wichtige Rolle, da sie unabhängig von GPS arbeiten und so bei GPS-Störungen, z. B. durch Jamming, eine verlässliche Alternative bieten. Die Kompetenz basiert auf deutscher Technologie für mechanische, faseroptische und mikromechanische Inertialsensoren. Dies ermöglicht einen ITAR-freien Vertrieb der LITEF Produkte rund um den Globus. Doch mit der verstärkten Nutzung digitaler Systeme wächst auch das Risiko von Cyberangriffen und Desinformationskampagnen, die weit über das unmittelbare Konfliktgebiet hinausreichen. Gleichzeitig betreffen Geopolitische Spannungen im Nahen Osten und in der Taiwanstraße nicht nur die

Sicherheitslage vor Ort, sondern haben auch globale wirtschaftliche Auswirkungen. In Taiwan, einem zentralen Halbleiterproduzenten, könnten Eskalationen die weltweiten Lieferketten stören. Unternehmen weltweit versuchen, Abhängigkeiten von China zu verringern, um Lieferausfälle zu vermeiden.

Gleichzeitig durchlebt LITEF gerade die interne Umstrukturierung durch das Upgrade von SAP ECC 6 auf S/4 HANA. Diese Umstellung betrifft technologische und betriebliche Prozesse. Technologisch ermöglicht das Upgrade auf S/4 HANA Echtzeitdatenverarbeitung und schnellere Analysen, erfordert jedoch umfassende Anpassungen der IT-Infrastruktur. Schulungen und eine schrittweise Implementierung stellen sicher, dass alle Abteilungen optimal vorbereitet sind. Geschäftsprozesse werden durch grundlegend effizientere Abläufe ersetzt, auch unter Entwicklung und Einsatz von KI-basierten Lösungen. Die Echtzeitverarbeitung wird für schnellere Entscheidungen, eine höhere Transparenz aber auch Informationssicherheit genutzt.

Die exogenen und endogenen Herausforderungen sind identisch mit Blick auf eine resiliente Organisation, in der die Menschen die Organisation, Technologie, Informationssicherheit, Produkt- und Personalentwicklung und Fertigung meistern. Das erfordert sorgfältige Planung und Koordination, Organisations- und Personalentwicklung, vor allem aber die Expertise(bildung) aller, um die Transformation und das technologische Upgrade als gemeinsamen Entwicklungsprozess zu verstehen und aktiv zu gestalten.

### **Resilienz, Transformation und Expertise(bildung) – Balance zwischen Innovation und operativer Stabilität**

Innovation darf nicht auf Kosten der operativen Stabilität gehen. Daher verfolgt LITEF einen multifunktionalen Ansatz, um sicherzustellen, dass das Transformationsprojekt weder die Fähigkeit beeinträchtigt, auf externe Bedrohungen zu reagieren, noch neue Chancen zu nutzen.

### **Sicherheitsanforderungen und Transformation**

Um den Sicherheitsherausforderungen zu begegnen, bündelt LITEF seine Sicherheitsfunktionen in einem zentralen Team, das für eine konsistente Umsetzung der Sicherheitsmaßnahmen im gesamten Unternehmen sorgt. Die Zentralisierung stärkt das Risikomanagement, beschleunigt Entscheidungsprozesse und erlaubt eine gezieltere Nutzung von Ressourcen. Die zentrale Informationssicherheits-Roadmap umfasst klare Ziele und Verantwortlichkeiten, Risikobewertungen, KI-basierte Bedrohungserkennung, regelmäßige Mitarbeiterschulungen und Protokolle für schnelle Reaktionen auf Sicherheitsverletzungen.

### **Expertise(bildung)**

LITEF hat erkannt, dass der Erfolg seiner Projekte – darunter auch das komplexe SAP-Upgrade – maßgeblich von der Expertise seiner Belegschaft abhängt. Daher investiert das Unternehmen umfassend in die Entwicklung seiner Mitarbeiter. Ziel ist eine Kultur der kontinuierlichen Entwicklung der Expertise jedes Einzelnen und der Teams. Daher setzen wir auf Expertisetandems und Führung in selbstregulierten Teams.

Die Tandems bestehen aus Mitarbeitern unterschiedlicher Erfahrungsstufen, teilweise sogar aus unterschiedlichen Bereichen oder Abteilungen, arbeiten aber in

Projekten zusammen. Dadurch erleben sie sich gegenseitig im gemeinsamen Erfahrungs-, Vertrauens- und Entwicklungsraum. Sie beobachten sich und einander, geben sich konstruktives Feedback, „challengen“ sich. Regelmäßiges Feedback hilft allen individuelle Stärken auszubauen und Entwicklungsfelder frühzeitig zu erkennen. Sie arbeiten informell oder formell mit schriftlich fixierten Entwicklungszielvereinbarungen zusammen, um ihre Fortschritte messbar zu machen. Teilweise werden Erfahrungen in Entwicklungstagebüchern aufgearbeitet, teilweise öffentlich im Blog geteilt, kommentiert und weiterentwickelt: Erfahrungen, Tipps, Erfolge. Es geht um eine Feedback-Kultur, die auf Offenheit und konstruktivem Austausch basiert.

Wir sehen positive Effekte: die Tandems arbeiten bewusster und dadurch effizienter an ihrer eigenen Entwicklung: Probleme werden nicht nur angesprochen, sondern Ursachen hinterfragt und in Lösungen überführt. Teams agieren mutiger und führen sich selbst sowohl als Individuum als auch gemeinsam, führen auch externe Partner gezielter, entschlossener und selbstbewusster. Führung verteilt sich auf alle, die aktiv mitwirken. Das fördert eigenverantwortliche, selbstregulierte Teams. Mit zunehmender Expertise wandelt sich die Zusammenarbeit, das Arbeitstempo erhöht sich. Gleichzeitig steigt die Qualität – in kleinen, aber messbaren Schritten.

Zusätzlich hat LITEF kollaborative Lernplattformen geschaffen, die eine zentrale Anlaufstelle für Wissensaustausch und Zusammenarbeit bieten. Hier können Schulungen absolviert, Lerninhalte geteilt und gemeinsam an Projekten gearbeitet werden. Alles zusammen fördert die gemeinsame Entwicklungskultur, die die Innovationskraft des Unternehmens ausmacht.

### **Sicherstellung technologischer Widerstandsfähigkeit**

Gleichzeitig wird die technologische Widerstandsfähigkeit des Unternehmens in einer zunehmend digitalisierten Welt sichergestellt: flexibel, robust und zukunftssicher. Dies betrifft nicht nur das laufende SAP-Upgrade, sondern auch die Weiterentwicklung anderer kritischer Systeme. Durch kontinuierliche Investitionen in Technologie und die Expertise der Belegschaft stellt LITEF sicher, dass es operativ und technologisch für die Zukunft gerüstet ist.

Die Förderung einer Innovationskultur spielt eine zentrale Rolle, indem ein innovationenförderndes Arbeitsumfeld Veränderungen begrüßt und kreatives Problemlösen unterstützt. LITEF fördert ein Klima, in dem Mitarbeiter ermutigt werden, neue Wege zu gehen und in dem frische Ideen wertgeschätzt und aktiv umgesetzt werden.

Zusätzlich setzt LITEF auf strategische Allianzen mit Branchenakteuren, akademischen Einrichtungen und Regierungsbehörden. Diese Partnerschaften ermöglichen den Zugang zu modernster Forschung, fördern den Wissensaustausch und stärken die kollektiven Sicherheitsmaßnahmen des Unternehmens.

### **Fazit**

In einer zunehmend komplexen und volatilen globalen Landschaft müssen mittelständische Unternehmen wie LITEF eine Vielzahl von Herausforderungen meistern. Durch die Umstrukturierung seiner Sicherheitsfunktionen, die Etablierung einer robusten Informationssicherheits-Roadmap und die Investition in den Expertise Aufbau ist LITEF gut positioniert, sowohl den geopolitischen Druck als auch interne technologische Transformationen zu bewältigen. Durch diese strategischen Initiativen sichert LITEF nicht nur seine Widerstandsfähigkeit, sondern ebnet auch den Weg für nachhaltige Innovation und Erfolg im Verteidigungssektor.

Diese Strategie, die es ermöglicht, Herausforderungen zu meistern, während gleichzeitig die Umsetzungsgeschwindigkeit und Agilität bei moderatem Mitteleinsatz erhöht werden, kann als Blaupause für mittelständische Unternehmen dienen. ■

# LITEF

### **Autoren:**

**Lutz Kampmann** ist Geschäftsführer der Northrop Grumman LITEF GmbH

**Michael Dost** ist Leiter Informationssysteme der Northrop Grumman LITEF GmbH

LITEF ist eines der führenden Unternehmen in der Entwicklung und Herstellung von Navigations- und Sensorsystemen.



Foto: Autor

## Bauspiel: Ein Schiff – Parallele Bauhaus

Jens Elstermeier

Der Baukasten „Bauspiel: Ein Schiff“, der das Leitmotiv der Sonderausgabe zum InfoBrief Heer 03/2024 stellte, bietet die Möglichkeit, aus vorgegebenen Bausteinen – oder abgeleitet aus vorgefertigten, standardisierten Komponenten – vielfältige Modelle oder Lösungen zu erstellen. Dies führt mich zu folgenden vier Betrachtungswinkeln des *Bauspiels* in Hinblick auf die Erreichung von Kriegstüchtigkeit und Resilienz:

- Form,
- Qualität,
- Geschwindigkeit und
- Verfügbarkeit.

**Form:** Im Bauspiel sind die Formen vorgegeben. Zur Erreichung bestimmter Fähigkeiten in Bezug auf Kriegstüchtigkeit und gesamtstaatliche Resilienz müssen diese zunächst identifiziert oder definiert werden, seien es Systeme zur übergreifenden Führungsfähigkeit oder neue Kommunikations- oder Waffensysteme. Aufgrund steigender Komplexität und geforderter Agilität (Software Defined Defence, SDD) sollte dies im Sinne des Bauhauses, Architektur als Gesamtkunstwerk zu betrachten, interdisziplinär mit den jeweiligen Spezialisten im vertrauensvollen Miteinander passieren. Dabei sind für die Definition der Bausteine (= Lösung) alle notwendigen Anforderungen und Beteiligten bei der Festlegung der Form zu berücksichtigen, dem Ausspruch „form follows function“ („die Funktion bestimmt die Form“) von Louis Sullivan des Funktionalismus folgend.

Die zeitgerechte Bereitstellung passender Bausteine oder Lösungen hängt neben den Ressourcen stark von der Innovationsgeschwindigkeit ab. Dazu braucht es neben der fachlichen Expertise eine enge Zusammenarbeit von Bedarfsträgern und Industrie, um zielgerichtet zu investieren. Dabei ist aber nicht nur die inhaltliche Abstimmung des „was“ wichtig, von mindestens gleicher Bedeutung ist das „ob“. Wenn es um industrielle Innovationen geht, muss auch eine Verlässlichkeit und Wertschätzung vorhanden sein, um dauerhaft zu investieren. Hat die Industrie eine Lösung entwickelt, muss auch sichergestellt werden, dass diese nicht intern nachgebaut wird und so doch wieder ein internes „create“-Projekt entsteht (siehe unten, NATO ABC Paradigm). Am Ende müssen auch verlässliche Beauftragungen stehen.

**Qualität:** Das Bauhaus forderte die Zusammenführung von Kunst und Handwerk, um hohe Qualität auf entsprechender Expertise zu gründen. Disziplinen übergreifende Ausbildung gehörte zum Lehrkonzept. Forderungen wie Agilität, Software Defined Defence, Multi Domain Operations etc. erhöhen zunächst den Komplexitätsgrad. Sie stellen hohe Anforderungen an die Qualität, um diese Systeme und Fähigkeiten durchhaltetfähig zu designen und dann auch zu betreiben. Zusammenarbeit in integrierten Teams, mit Nutzervertretern, Industrie und Be-

schaffern. Dazu müssen nicht nur Nutzervertreter dauerhaft für diese Mitwirkung abgestellt werden, dies ist im Personalbedarf gerade bei knapper werdender Fachleute-Decke zu planen. Erfolgreiches Teamwork braucht Vertrauen – am Anfang vielleicht einen Vertrauensvorschuss basierend auf gemeinsamer Wertebasis, dann aber im Team wachsen muss es aber aufgrund gelebter Werte, Verlässlichkeit und Expertise.

**Geschwindigkeit:** Der Vorteil eines Baukastens oder verfügbarer Lösungen ist die Geschwindigkeit, mit der dann Fähigkeiten bereitgestellt werden können. Marktverfügbar ist hier sicher das aktuelle Schlagwort, unter dem „ABC Paradigma“ (Adopt, Buy, Create) hat die NATO aber bereits 2014 die Nutzung von verfügbaren (innerhalb der NATO und der NATO Mitgliedsländer) und marktverfügbaren Lösungen gefordert<sup>1</sup>. Dies wurde beim NATO Summit 2023 in Vilnius von den Staats- und Regierungsoberhäuptern bestätigt.<sup>2</sup> In diesem Jahr wurde die Policy aktualisiert und um den Servicegedanken ergänzt: „...the Council agreed that “[t]he default approach to technology intensive capabilities is to diminish complexity by delivering individual components iteratively, as services, within months. If the acquisition of services is not practical, the “Adopt, Buy, Create” approach will lead to more cost-effective solutions.“<sup>3</sup>



Foto: Autor

Marktverfügbarkeit benötigt aber auf Seiten der Industrie auch verlässliche Nachfrage und Beauftragung, um Investitionen in Entwicklung und Produktion zu rechtfertigen. Planbarkeit ist notwendig, nicht nur aus kommerziellen Gründen, auch um Personal vorzuhalten oder aufzubauen und auszubilden oder Material und Fertigungsstätten vorzuhalten.

Einen potenziellen Nachteil hat die Baukasten- oder marktverfügbare Lösung: Sie hat einen vorher definierten Funktionsumfang und ist damit keine Lösung, die zwingend 100 % aller Anforderungen erfüllt. Die Geschwindigkeit – und in vielen Fällen sicher auch die geringeren Kosten – einer 70- oder 80 % Lösung wiegen diesen Nachteil auf, erfordern aber eine andere Kultur. Marktsichtungen, sog. Market Surveys, gehören im Beschaffungsprozess der NATO mittlerweile zum bevorzugten Instrument. Beschränkte oder freihändige Vergaben nach erfolgter Marktsichtung, Analyse und Bewertung im reduzierten Anbieterkreis beschleunigen die Vergaben erheblich.

**Verfügbarkeit:** Jedem, der mit Bauklötzen, Lego, Fischer-Technik oder anderen Systemen neue Modelle kreieren wollte, ist es sicher schon passiert, dass es ein benötigtes Teil nicht gibt oder am Ende nicht genug Teile vorhanden sind.

Dementsprechend gilt es bei den Anforderungen oder Projekten zu priorisieren. Auch das Military Committee der NATO (MC) hat in seiner Weisung an die Strategic Commanders die Erwartung klargestellt, dass Fähigkeitsforderungen anhand des relativen und zeitnahen Beitrags einer spezifischen Forderung am militärischen Erfolg zu priorisieren sind.<sup>4</sup> Die ABC-Policy der NATO leitet sich aus diesem Ansatz ab, der in der Software-Entwicklung oder Fertigung unter „Build-versus-Buy-Analyse“ bekannt ist, und erweitert ihn um „Adopt“ und mit erster Priorität um den Einkauf von Services. Damit erweitert sich die Leistungserbringung bewusst auf die Industrie, in Bezug auf die Resilienz im Krisen- und Verteidigungsfall eine gute Maßnahme, nicht nur vor dem Hintergrund knapper werdender Arbeitskräfte.

Ziel muss es damit sein, ein erprobtes und eingeübtes Zusammenspiel von öffentlichem Auftraggeber, Nutzer und Industrie zu erhalten / zu entwickeln, um Resilienz in der Gesamtverteidigung zu erreichen und im Krisen- oder Verteidigungsfall Kontinuität in Betrieb aber auch schneller und innovativer Weiterentwicklung sicherzustellen. Nicht nur bei der Massenfertigung von Verbrauchsmaterial gilt es, Expertise und Kapazitäten zielgerichtet in Deutschland aufzubauen, das Zusammenspiel ein-

zuüben und damit Vertrauen zwischen den handelnden Personen zu erzeugen. Neben der Priorisierung von Budgets in den Haushalten für gesamtstaatliche Verteidigungsaufgaben – sicher das dickste der zu bohrenden Bretter – oder der Anpassung des Vergabeverhaltens gibt es auch viele kleinere Dinge, die geklärt werden müssen, z.B. Umgang mit Reservisten (Unabkömmlichstellung) sowie Definition und Erfassung kriegswichtiger Tätigkeiten und Berufe (Bergleute haben wir keine mehr, Cyberspezialisten und KI-Entwickler hatten wir 1990 noch nicht).

**Frei nach Walter Gropius Aussage in seinem Bauhaus Manifest von 1919: „Das Endziel aller (bildnerischen) Tätigkeit ist der Bau!...“: fangen wir doch gemeinsam an zu bauen!**

**Autor:**

**Jens Elstermeier** ist Senior Vice President Consulting Services, Head of Defence & Intelligence CGI Deutschland B.V. & Co.K

3 PO(2018)0259 (CFCDGM)

4 IMSM-0192-2021, MC Guidance to Strategic Commanders on Tolerance Implementation Framework



Foto: Bundeswehr

# Zukunft gestalten – Kriegstüchtigkeit und Innovation

Generalmajor Wolfgang Gäbelein

Diskussionen zur Einsatzfähigkeit und zur Einsatzbereitschaft der Bundeswehr finden auf den unterschiedlichsten Ebenen und in den unterschiedlichsten Foren statt. Das ist gut, denn nach langen Jahren der Unterfinanzierung und den bekannten Änderungen im sicherheitspolitischen Umfeld mit dem völkerwidrigen Angriff Russlands auf die Ukraine bedarf eine positive Entwicklung der Bundeswehr eines breiten Konsenses. Zu groß sind der Finanzbedarf und auch die notwendigen Änderungen, um dies allein einem kleinen Zirkel zu überlassen. Gleichzeitig dürfen sich die Maßnahmen nicht nur auf das Offensichtliche, das Naheliegende beschränken. Insbesondere die dynamische Entwicklung bei Zukunftstechnologien fordert, sich umfassend mit deren Auswirkungen zu befassen, einschließlich langfristig zu erwartender Konsequenzen. Es ist wichtig, die entscheidenden Technologien zu identifizieren, deren Potenzial zu analysieren und vor allem auch zu erkennen, in welchen Bereichen sie sich disruptiv auswirken können. Wir müssen uns in diesem Zusammenhang intensiv auch damit auseinandersetzen, welche Veränderungen wir perspektivisch vornehmen müssen, um das volle Potenzial der Zukunftstechnologien zu erschließen, u.a. im Bereich der Organisation, also der Zusammensetzung der kämpfenden Truppenteile, der Taktiken und Verfahren oder auch der Ausbildung. Gefordert ist eine ganzheitliche Betrachtung unter Berücksichtigung aller Planungskategorien. Die Analysen zum Gefechtsfeld der Zukunft weisen auf folgende wesentliche Charakteristika:

- eine Vielzahl vernetzter Sensoren schaffen nicht zuletzt auf Basis Datenfusion Voraussetzungen für ein nahezu „gläsernes Gefechtsfeld“; sie bieten ein hohes Maß an Transparenz; überraschende Aktionen sind nur schwer zu erreichen;
- gleichzeitig auftretende Effekte aus allen Dimensionen in alle Dimensionen führen zu einem komplexen Gesamtbild;
- skalierbare Effekte werden mit hoher Geschwindigkeit, großer Präzision über große Reichweiten projiziert, es gibt keine Sanktuarien mehr; betroffen ist die gesamte Gesellschaft;
- Systeme hoher Autonomie bringen Risiken, ermöglichen aber auch neue Wege und Verfahren; kritisch ist, inwieweit die Rivalen bereit sind, ethische und moralische Grenzen zu ziehen und auch einzuhalten.

Digitalisierung mit Software als verbindendem Element und Anwendungen künstlicher Intelligenz, Quanten- und Nanotechnologien, unbemannte Systeme, Hyperschallsysteme, Energiewaffen (Laser oder Mikrowellen) und Weltraumanwendungen bieten in diesem erhebliche Potenziale und ziehen so die größten Auswirkungen nach sich. Gefordert ist nun einerseits die bekannten Lücken zu schließen, um in einem vertretbaren Zeitraum den notwendigen Umfang an einsatzbereiten Kräften zur Landes- und Bündnisverteidigung bereitstellen zu können. Andererseits müssen die Weichen gestellt werden, die Streitkräfte auf die Zukunft vorzubereiten. Oder anders ausgedrückt: es gilt Einsatzfähigkeit zu schaffen und Einsatzfähigkeit in der Zukunft zu erhalten. Inwieweit besteht hier die notwendige Balance?

Die Bilanz stellt sich differenziert dar. Unsicherheiten und Grenzen im Finanzplan, die u.a. auch aus dem Haushaltsentwurf für 2025 resultieren, schränken die Möglichkeiten deutlich ein, in die Zukunft zu investieren. Beispielhaft dafür steht die Reduzierung der Mittel für Forschung und Technologiearbeit (kurz F&T). Feh-

lende Freiräume im Finanzplan zwingen zur Priorisierung auf Fähigkeitserhalt und quantitativen Aufwuchs. Auch die notwendige Konzentration auf marktverfügbare Systeme trägt nur bedingt zur Anwendung der genannten Technologien bei.

Dem gegenüber sind allerdings auch wichtige Weichen für die Zukunft gestellt. Das Sondervermögen gestattete die Realisierung von Maßnahmen zu Digitalisierung der Streitkräfte in signifikantem Umfang auf den Weg zu bringen. Auch die Beschaffung der F-35 wird eine Reihe neuer Möglichkeiten erschließen. Gleiches gilt für die Entwicklungsvorhaben Future Combat Air System/Next Generation Fighter (FCAS/NGF) und Main Ground Combat System (MGCS). Darüber hinaus ist die Truppe durchaus bereit und in der Lage neue Ideen zu kreieren und diese in ihrer Zuständigkeit wirkungsvoll zur Anwendung zu bringen.

In jeder Diskussion folgt über kurz oder lang der Vorwurf, dass alles zu lange dauert und es werden dafür Prozesse und Verfahren im Bereich der Planung und der Beschaffung verantwortlich gemacht und deren Änderung gefordert.

Zweifelsohne stellt sich die Frage, inwieweit alles schnell gehen muss. Die Antwort ist nicht einfach, oder etwas „flapsig formuliert“, es kommt darauf an. Die Entwicklung komplexer Waffensysteme darf durchaus eine angemessene Zeit dauern. Das gilt gerade dann, wenn F&T erforderlich ist um neue Technologien zu erschließen. Was aber schnell gehen muss, ist die Anpassung von Systemen in Nutzung (das gilt gleichermaßen für Waffensysteme, wie auch Systemverbände in Form von Kampfverbänden) auf der Basis von Erkenntnissen aus der Beobachtung aktueller Kriege und Konflikte. Beispielhaft hierfür steht die Integration von kleinen unbemannten Systemen in Kampfverbände um diesen neue Möglichkeiten zur Aufklärung oder zur Wirkung zu verschaffen. Hier besteht Handlungsbedarf.

Chancen bieten sich, wenn es gelingt, die bisher eher getrennt voneinander



agierenden Bereiche F&T, Innovationsmanagement und Fähigkeitsmanagement näher zusammenzubringen. Die Einrichtung des Forschungs- und Innovationshubs in der Abteilung Planung im Zuge der Neuorganisation des BMVg schafft hierfür eine günstige Ausgangslage. Es geht darum, neue Formate des Informationsaustausches zu etablieren und alle Mitwirkenden zu ermutigen, Möglichkeiten, die die Prozesse und Verfahren bieten, auszutesten und in der Folge auch entsprechende Anpassungen vorzunehmen. Das Problem sind weniger die Prozesse- sondern mehr deren Anwendung.

Übergreifend betrachtet bedarf es eines weiterentwickelten systemischen Ansatzes. Einerseits muss top-down Transparenz geschaffen werden, verbunden mit einem klaren langfristigen Ziel, andererseits sind bottom-up die Vielzahl an Ideen und Aktivitäten an der Basis zu erfassen und übergreifend zu nutzen. Oder anders ausgedrückt - gute Lösungsansätze müssen als Best Practices „in die Fläche gebracht werden“. Instrumente dafür sind bekannt und durchaus auch verfügbar. Wir müssen sie nur zielgerichtet nutzen. Zunächst geht es darum dem Systemgedanken eine stärkere Bedeutung einzuräumen. Systemverbünde oder Systeme von Systemen sind wichtiger als einzelne Waffensysteme. Es ist besser das Gesamtsystem zu optimieren als zu versuchen, mit einem neuen Waffensystem „einen großen Wurf zu landen“.

Architekturen, also modellhafte Beschreibungen komplexer Zusammenhänge, schaffen die notwendige Transparenz und bildet die inhärenten Wechselwirkungen in Systemen ab. Dies ist unerlässlich um Auswirkungen einzelner Änderungen auf das Gesamtsystem hinreichend präzise abschätzen zu können. Es geht es darum, Technologien zu identifizieren, in die mit dem Ziel langfristiger Entwicklungen investiert werden muss. Gleichzeitig stellt sich die Herausforderung Exzellenzbereiche zu definieren. Nur die entsprechende Konzentration auf einige herausgehobene Schlüsselbereiche wird letztendlich erfolgreich sein können. Denn Forschung im kompletten Spektrum ist weder finanzierbar noch von den absehbar verfügbaren Arbeitskapazitäten machbar. Eine entsprechende Konzentration bietet Perspektiven für die deutsche Rüstungsindustrie und sie schafft Ansatzpunkte für Kooperation

mit Partnernationen. Ein solcher Exzellenzbereich ist der U-Bootbau, ein neues Feld könnte z.B. die bodengebundene Luftverteidigung sein.

Neben Entwicklungsprogrammen im großen Stil bieten Ideen aus der Truppe Potenzial für kleine oder aufeinander aufbauende Verbesserungen und Innovationen. Auch diese erschließen neue Wege. Die Ideen gilt es in den Architekturen zu verorten. Damit unterstützen Architekturen auch ein schrittweises Vorgehen, das innerhalb der Fähigkeiten qualitative Verbesserungen ermöglicht oder dazu dient neue Spezifika auszuprägen. Dies gilt es zielgerichtet zu nutzen. Das Spektrum möglicher Schritte reicht dabei von der Vernetzung von Systemen bis zur Integration neuer Komponenten. Hier kommt Software eine entscheidende Bedeutung zu. Denn Software gestattet den Output analoger Systeme zu digitalisieren und diese mit anderen Systemen zu verbinden. Das gestattet u.a. eine bruchfreie Kette von Aufklärung über Führung hin bis zur Wirkung („Kill Chain“), ermöglicht hohe Aktions- und Reaktionsgeschwindigkeiten und ist Grundlage für die angestrebte Informations-, Führungs- und Wirkungsüberlegenheit. In Verbindung mit Software kann es gelingen obsoleten Systemen im Verbund eine neue Relevanz zu geben. Umfassend angewendet entsteht „Software Defined Defence“. Schrittweises Vorgehen in Verbindung mit neuen Technologien erschließt einen weiteren Vorteil. Es ist in vielen Anwendungen wichtiger, kleine Verbesserungen in überschaubaren Zeiträumen zur Anwendung zu bringen, als einen großen Qualitätssprung anzustreben, auf den die Nutzer, die Truppe sehr lange warten müssen. Errungenschaften können frühzeitig in neue Organisationsformen münden. Neue Taktiken lassen sich zunächst erproben und daraus resultierende Erkenntnisse entsprechend umsetzen. Wichtig ist den späteren Nutzer einzubinden um frühzeitig Erkenntnisse aus der Anwendung zu gewinnen und diese in die schrittweise Weiterentwicklung einfließen zu lassen. Dies kann u.a. in Form von institutionalisierten Dialogen, Experimentalserien oder Übungen erfolgen.

Bei der Integration neuer Technologien und schrittweisem Vorgehen ist eines wichtig: Scheitern muss erlaubt sein. Das gestattet einen breiten Ansatz und gleichzeitig weniger erfolgversprechen-

de Ansätze frühzeitig auszusortieren. Auch nicht erfolgreichen Versuche bringen Erkenntnisse. In diesem Kontext kann es auch gelingen, Start-ups gewinnbringend einzubinden. Denn gerade Start-ups bieten ggf. interessante Lösungen für spezifische Fragestellungen in einzelnen Schritten. Und jeder Schritt bringt Expertise und Kompetenzgewinn. Eine nicht triviale Herausforderung bleibt die Finanzierung. Das notwendige Maß an Flexibilität besteht nur dann, wenn entsprechende Vorhalte im Haushalt und Finanzplan bestehen. Dann sind auch „Seiteneinstiege“ in die Prozesse möglich. Die derzeitige Gesamtlage lässt dies allerdings nicht zu. Perspektivisch müssen Finanzmittel bereitstehen, die innovative Lösungen auch kurzfristig ermöglichen. In der Übergangsphase erfordert es Mut, zumindest für kleine Projekte Haushaltsmittel vorzuhalten, ohne Ergebnisse von F&T oder Experimenten hinreichend präzise vorhersagen zu können. Dies geht nur im Dialog.

Als Erfolgsrezept haben sich folgende Schritte erwiesen:

- die richtigen Partner zusammen zu bringen;
- schnell einen geeigneten Projektaufsatz definieren;
- einen Meilensteinplan für schrittweises Vorgehen definieren;
- frühzeitig einen Vorhalt für die Finanzierung erwirken.

Es geht nur gemeinsam, Nutzer, Bedarfsträger, Bedarfsdecker sowie Forschung und Industrie sitzen in einem Boot und sie sollten idealtypisch im „Gleichklang“ rudern. Wir brauchen die zielgerichtete Erschließung neuer Technologien durch Forschung und die Definition von Exzellenzbereichen, aber auch das schrittweise Verbessern mit innovativen Ideen. Wir brauchen das Ausfächern von Best-Practices, die Anwendung von Zukunftstechnologien im Kleinen und im Großen. Vertrauen entwickelt sich durch den umfassenden Dialog und durch „das gemeinsame Machen“. Scheitern muss erlaubt sein. Denn sicher ist: Zukunftstechnologien zu erschließen, sie zu beherrschen und nutzen zu können trägt wesentlich zur nationalen Sicherheit und vor allem zur nationalen Souveränität bei. ■

**Autor:**

**Generalmajor Wolfgang Gäbelein**  
ist Amtschef des Planungsamtes der Bundeswehr in Berlin



Foto: v. Saldern

## Mit DIANA auf der Jagd nach technologischem Vorsprung

Wolfgang Hellmich MdB

### Es ist ein noch recht junges Programm der NATO, DIANA, Defense Innovation Accelerator for the North Atlantic.

Intensive Studien einer mit großer Expertise versehenen Gruppe von Wissenschaftlerinnen und Wissenschaftlern (leider ohne deutsche Beteiligung) gingen der Entscheidung des Brüsseler NATO-Gipfels 2021 voraus, ein Programm zur Technologieförderung aufzulegen. Es war der Erkenntnis geschuldet, dass die NATO-Staaten in der internationalen Konkurrenz, vor allem aus Russland und China, um technologische Vorsprünge gerade auch im militärischen Bereich ins Hintertreffen geraten könnten. Mehr Innovation, Kooperation und Koordination waren von Nöten. Beim NATO-Gipfel 2022 in Madrid, der entscheidende strategische Weichenstellungen vornahm, wurde DIANA, Defence Innovation Accelerator for the North Atlantic, aus der Taufe gehoben. Ein zentraler Beschluss dieses Gipfels war die Verstärkung der Forschungs- und Technologieanstrengungen innerhalb der Allianz, die im Kontext von Sicherheitsherausforderungen wie Cyberangriffen und hybriden Bedrohungen gerade angesichts des völkerrechtswidrigen Angriffs Russlands auf die Ukraine aber auch die sprunghaften technologischen Entwicklungen immer dringlicher wurden. DIANA aber auch die Einrichtung eines Innovationsfonds mit 1 Mrd. Euro waren die Reaktion der NATO, um die NATO-Kooperation mit einem innovativen Ansatz zu versehen.

### Zielsetzung

Die Entwicklung von Technologien, die den Bündnisstaaten zugutekommen und ihre militärische Effizienz steigern, stehen im Mittelpunkt. DIANA zielt darauf ab, aktuelle Forschungsergebnisse und technologische Innovationen wirksam und effektiv zu nutzen, um die Streitkräfte der NATO-Staaten zu modernisieren und ihre Einsatzfähigkeit zu erhöhen. Aber nicht nur Technologien, sondern auch neuartige Ansätze, die für militärische Anwendungen von Bedeutung sein können, sollen schneller identifiziert, entwickelt und implementiert werden. Die Förderung innovativer Lösungen in den zukunftsweisenden Schlüsseltechnologiefeldern Künstliche Intelligenz, Datenanalyse und Cloud Computing, Cybersecurity, Quantencomputing, unbemannte Systeme, Biotechnologie, Logistik, Materialwissen- und Wirtschaft und etliche Felder mehr stehen im Fokus, um die Verteidigungsfähigkeit der NATO zu stärken. Der Technologievorsprung ist ein entscheidender Faktor, um seitens der NATO in einem an Komplexität und Kritikalität zunehmenden globalen Sicherheitsumfeld handlungsfähig zu bleiben und auch militärische proaktive Handlungsfähigkeit zu gewinnen. In der strategischen Fokussierung zielt DIANA auf militärische wie zivile Anwendungen ab. Synergien mit der zivilen Technologieentwicklung stehen ausdrücklich im Mittelpunkt dieses interdisziplinären Ansatzes. „Dual Use“ ist hier das entscheidende Stichwort.

### DIANA-Charta und weitere Dokumente

In der „Gründungsakte“ von DIANA wird mit besonderer Betonung auf den Wertekanon der NATO Bezug genommen. Zuletzt in der 2024 überarbeiteten KI-Strategie der NATO wird die Weiterentwicklung von Normen und Standards einer Integration und Anwendung verantwortungsvoller KI benannt. Dies ist Grundlage für die Kooperation mit NATO-Partnern, also in der globalen Reichweite auch DIANA, internationalen Organisationen, der alliierten Industrie und der Wissenschaft. Ausdrücklich wird auf die Resolution der UN-Vollversammlung zum Thema KI hingewiesen. Den Einrichtungen von DIANA wird aufgetragen, die Einhaltung von Zielen und Werten der NATO von Partnern zu prüfen, bevor Kooperationen oder Förderungen eingegangen werden. Das Programm „Wissenschaft für Frieden und Sicherheit“ (SPS) setzt hier die Maßstäbe. Die Bündnispartner, DIANA und der NATO-Innovationsfonds können so zum Beispiel innovative KI-Lösungen für die Verteidigungsbedürfnisse der NATO aus dem privaten Sektor beschaffen und die Rüstungsindustrie der Bündnispartner ermuntern, Systeme in Übereinstimmung den Anforderungen der Allianz und den Werten und Normen der NATO zu entwickeln, zu konstruieren und zu fertigen.

### Strategische Kooperationen

Basis von DIANA ist die Kooperation von Industrie und militärischen Forschungseinrichtungen, staatlichen wie

nicht-staatlichen Organisationen und der zivilen Wissenschaft. Deshalb ist die aktive Förderung von Partnerschaften von Start-Ups, kleinen und mittleren Unternehmen, Forschungseinrichtungen und der akademischen Welt ein wesentliches Element von DIANA. Hierdurch soll der Zugang zu innovativen Ideen und neuen Technologien nicht nur verbessert und beschleunigt werden, vielmehr soll auch die Verschleuderung von Ressourcen durch Nicht-Kooperation vermieden werden. Die Überwindung regulatorischer Hemmnisse für derartige Kooperationen hat sich die NATO zum Ziel gesetzt.

Der globale Austausch von Wissen und Technologien kann die Verfügbarmachung einer breiteren technologischen Basis erbringen. Eine Aufgabe liegt hier in der Sicherung der Ergebnisse, um einen Abfluss von Erkenntnissen in „falsche Kanäle“ zu verhindern. Gleichzeitig ist eine sorgsame Abstimmung mit den und Integration der Innovationsstrategien in die übergeordneten militärischen und sicherheitspolitischen Konzepte der Allianz zu gewährleisten.

### Instrumente von DIANA

DIANA verfügt über eine mehrstufige Organisationsstruktur. Ein strategisches Steuerungsgremium bestimmt die Ausrichtung. Thematische Arbeitsgruppen zu spezifischen Technologien werden mit Expertise aus den Mitgliedstaaten, Forschungseinrichtungen und der Industrie zusammengesetzt. Eine enge Zusammenarbeit mit bestehenden NATO-Einrichtungen, z.B. den Exzellenzcentern, maximieren die Ressourcennutzung. Mit speziellen Accelerator-Programmen wird darauf abgezielt, vielversprechende Technologien zu identifizieren und gezielt zu fördern. Die letzte Bewerbungsphase ist zu Beginn 2024 ausgelaufen. Hier wird die Entwicklung von Prototypen sowie ihre Integration in bestehende militärische Systeme effizienter gestaltet, so der Anspruch von DIANA. Darüber hinaus werden mit NATO-Test- und Technologiezentren und Unternehmensinkubatoren sowie Workshops und anderen Kooperationsformen das DIANA-Biotop ausgestaltet. Dass diese Ansätze in der NATO hohes

Interesse geweckt haben, zeigt das Beispiel Finnlands. Beginnend 2023 sind in 2024 ein Unternehmensinkubator sowie zwei Testzentren, die sich mit destruktiven Technologien befassen, an der Aalto-Universität und der Universität Oulu unter der Koordination eines Technologieforschungszentrums VTT gegründet worden. Diese Plattformen für die Entwicklung von Partnerschaften, dem Transfer von Wissen und der Implementierung gemeinsamer Forschung können die Dynamik und Agilität der Entwicklung von Know-How entscheidend erhöhen.

### Perzeption in Deutschland und was ist zu tun?

In der öffentlichen Wahrnehmung läuft DIANA unter dem Radar, fälschlicherweise. Immerhin hat DIANA mit der Summe von 5 Mio. Euro im Haushalt 2024 Eingang in den Einzelplan 14 gefunden. Mit Hinweis auf den rasanten Aufwuchs von DIANA ist dieses Programm auch in einem Sammeltitel ohne konkrete Summe im Haushaltsentwurf 2025, EP 14 zu finden. Die Evaluierungsberichte zu DIANA belegen diese rasante Dynamik. Auch im Organigramm des BMVg ist DIANA gesondert aufgeführt. Testzentren sind vor allem in Kooperation mit dem DLR, Fraunhofer-Instituten, TKMS/Atlas, Einrichtungen der Bundeswehr, der IABG und der Hochschule Wismar zu finden. Hier besteht erheblicher Nachholbedarf. Es mag sein, dass die vielfältig zu findenden Zivilklauseln an Universitäten und Fachhochschulen hier ein Hindernis sind. Im Positionspapier des Bundesministeriums für Bildung und Forschung (BMBF) zur Forschungssicherheit im Lichte der Zeitenwende wird deutlich gemacht: „Drittens gilt es die – teilweise – strikte Trennung zwischen ziviler und militärischer Forschung in Deutschland zu hinterfragen, um mögliche Synergien zu heben“. Zu einer ergebnisoffenen Neubewertung wird aufgerufen. Vor dem Hintergrund der Ziele und Absichten von DIANA, der Bedeutung von Dual-Use für den zivilen wie militärischen Bereich ist das dringend geboten. Ein Umdenken an dieser Stelle ist angesichts der Zeitenwende unumgänglich.

Die Ansiedlung von Testzentren muss zielgerichtet und koordiniert von Bund und Ländern angegangen werden. Das Potential von Start-Ups im Cyberbereich z.B. im Raum Dresden-Leipzig, Berlin-Brandenburg, Bayern oder auch Hamburg und Bremen kann solche Initialzündungen nicht nur gut gebrauchen, sondern kann auch Expertise zuliefern. In regionalen Kooperationsclustern können Schwerpunkte in bestimmten Kompetenzbereichen angesiedelt werden, Fragen der Maritimen Entwicklungen, der Luft- und Raumfahrt, Cyber und Informationsgesellschaft, Materialwissenschaft und auch Zivilschutz, Landsysteme und Sicherung der Infrastruktur – eine Liste von Möglichkeiten ist sehr lang. Die Zuständigkeit für DIANA sollte im BMVg zusammengefasst und gebündelt werden.

Zivile Akteure sollten in DIANA eingebunden werden. Veranstaltungen und Workshops können den zivilgesellschaftlichen Nutzen von DIANA stärken. And last but not least, ein Abgleich zwischen den Förderprogrammen der EU und der NATO könnte bei der Effizienz der Programme hilfreich sein. Aber das ist ein eigenes Kapitel.

### Kurzes Fazit

Das DIANA-Projekt stellt einen der innovativsten Schritte der NATO dar. Durch die Kombination von Forschung, Technologie, Expertise in Unternehmen wie ziviler Wissenschaft – und das im internationalen Maßstab – kann die Verteidigungsfähigkeit der NATO und die militärische Effizienz mit höherem Tempo gesteigert werden. DIANA kann zu einem wichtigen Baustein in der Sicherung technologischen Fortschritts in der NATO und seinen Bündnispartnern werden. Es kommt darauf an, diesen Weg weiter konsequent zu verfolgen und zu unterstützen. ■

### Autor:

**Wolfgang Hellmich MdB** ist seit Juni 2012 Mitglied der SPD-Fraktion des Deutschen Bundestages und Mitglied im Verteidigungsausschuss sowie im Gremium Sondervermögen „Bundeswehr“.



Foto: Autor

## IT-Forensik

### Was macht eigentlich diese Artefaktum?

Felix Juhl

Die Aufklärung von Cyberstraftaten ist eines der anspruchsvollsten Felder in der modernen Forensik. Die zunehmende Nutzung digitaler Technologien in allen gesellschaftlichen und wirtschaftlichen Bereichen sowie das Ansteigen cyberkrimineller Aktivitäten stellen forensische Ermittler vor Herausforderungen, die innovative Methoden und spezialisierte Fähigkeiten erfordern. IT-Forensiker nutzen dabei fortgeschrittene mathematische Modelle und Berechnungen, Künstliche Intelligenz (KI), Maschinelles Lernen (ML) und zunehmend auch Quantencomputing, um Täterprofile zu erstellen, Angriffe zu rekonstruieren und Beweise zu sichern. Insbesondere bei der Untersuchung von staatlich oder halbstaatlich gelenkten Straftätern und Spionageaktivitäten ist ein tiefergehendes Verständnis dieser Methoden unabdingbar, da Angreifer oft fortgeschrittene Taktiken anwenden, um ihre Identität und Herkunft zu verschleiern.

Ein wichtiger Baustein der IT-Forensik ist die probabilistische Analyse. Bei der Rekonstruktion eines Cyberangriffs oder der Bestimmung der Herkunft und Taktik von Tätern greifen Forensiker auf statistische Modellierung und Wahrscheinlichkeitsberechnungen zurück. Insbesondere bei der Analyse großer Datenmengen, etwa bei der Untersu-

chung von Netzwerkprotokollen, Benutzeraktivitäten oder Anomalien im Datenverkehr, kann die statistische Modellierung helfen, verdächtige Aktivitäten zu isolieren und Prioritäten für die weitere Untersuchung zu setzen.

Mittels Bayesscher Netzwerke beispielsweise lassen sich Abhängigkeiten zwischen verschiedenen Ereignissen analysieren. Durch die Anwendung dieser Methode kann ein IT-Forensiker die Wahrscheinlichkeit bestimmter Angriffsmuster berechnen und potenzielle Täterprofile erstellen, die auf häufigen Mustern und spezifischen Signaturen in der verwendeten Schadsoftware basieren. Diese statistische Analyse kann dabei helfen, Verbindungen zwischen verschiedenen Vorfällen herzustellen und Hinweise auf staatliche oder halbstaatliche Akteure zu erhalten, da solche Akteure oft charakteristische Angriffsmuster und komplexe Mehrstufenstrategien verwenden.

Künstliche Intelligenz und Maschinelles Lernen haben in der IT-Forensik der Artefaktum eine zentrale Rolle eingenommen. Besonders im Bereich der Anomalieerkennung und Musteranalyse bieten eigene, nicht öffentlich zugängliche ML-Algorithmen Möglichkeiten, die sich mit traditionellen Methoden nur schwer erreichen lassen.

Ein spezifischer Vorteil des Einsatzes von ML-Modellen ist die Fähigkeit, gezielte Angriffe durch Musteranalyse zu identifizieren und zu klassifizieren. Bei Advanced Persistent Threats (APTs), die oft von staatlich oder halbstaatlich gelenkten Akteuren durchgeführt werden, ist es schwierig, typische Anzeichen zu erkennen, da diese Attacken meist über längere Zeiträume unentdeckt bleiben und tief in die Netzwerkinfrastruktur eindringen. Durch die Anwendung unserer ML-Algorithmen zur Verhaltensanalyse können jedoch selbst geringfügige Anomalien identifiziert und verdächtige Aktionen frühzeitig erkannt werden. Unüberwachte Lernverfahren wie Clustering können darüber hinaus genutzt werden, um unbekannte Angriffsmuster und Zero-Day-Angriffe zu identifizieren, indem sie Verhaltensmuster gruppieren, die außerhalb der normalen Aktivitäten liegen.

Ein internes Forschungsfeld der Artefaktum, u.a. mit dem Massachusetts Institute of Technology (MIT) Boston, ist der Einsatz von Quantencomputing. Für IT-Forensiker bietet dies eine Chance, verschlüsselte Kommunikationskanäle, etwa die von kriminellen Organisationen oder von staatlichen Akteuren, zu entschlüsseln und wertvolle Erkenntnisse zu gewinnen. Darüber hinaus ermöglicht Quantencomputing die effizien-



Foto: Jamie Tchassanti mithilfe von Midjourney (KI)

### Auch ein Schiff...

te Analyse großer Datenmengen. Und komplexe Muster können in riesigen Datenströmen identifiziert und verdächtige Aktivitäten in Echtzeit analysiert werden.

Eine besondere Herausforderung in der Cyberforensik stellt die Erkennung und Verfolgung von Straftätern dar, die unter staatlicher oder halbstaatlicher Führung handeln. Diese Akteure verfügen häufig über Ressourcen und Zugang zu Technologien, die weit über das Niveau durchschnittlicher Krimineller hinausgehen. Sie nutzen nicht nur fortgeschrittene Malware und hochentwickelte Exploits, sondern auch psychologische und soziotechnische Methoden zur Verschleierung ihrer Identität und Herkunft. Aus jahrelanger Erfahrung wissen die Experten der Artefaktum, dass staatliche Angreifer oft charakteristische Taktiken und Techniken anwenden, die spezifischen geografischen oder kulturellen Hintergründen zugeordnet werden können.

Die Experten der Artefaktum besitzen ein umfassendes Wissen über bekannte Angriffsmethoden und -strukturen dieser Akteure. Sie analysieren oft nicht nur die technische Ausführung eines Angriffs, sondern auch die geopolitische Situation und das Motiv, um Rückschlüsse auf den Täter zu ziehen. Hierbei spielen auch Techniken zur Täuschungserkennung eine Rolle, da staatlich gelenkte Akteure gezielt falsche Spuren legen, um ihre Herkunft zu verschleiern. Die Fähigkeit, diese Täuschungen zu durchschauen und typische Signaturen oder „Fingerabdrücke“ bestimmter staatlicher Gruppen zu identifizieren, ist ein wesentlicher Teil des hochspezialisierten Cyberforensik Teams.

Absoluter Erfolg in der Cyberforensik setzt multidisziplinäre Fähigkeiten voraus. Die Kombination von Wahrscheinlichkeitsberechnungen, KI, ML und zukünftig auch Quantencomputing ist ein ein Alleinstellungsmerkma

und zeichnet die Experten der Artefaktum aus, die sich in der modernen Bedrohungslandschaft zurechtfinden. Neben technischen Fähigkeiten entwickeln unsere Forensiker auch taktische und strategische Denkmuster, da Angreifer zunehmend kreative und raffinierte Methoden anwenden, um ihre Spuren zu verwischen. Durch das Zusammenspiel dieser Technologien und tiefgehende Kenntnisse über die Cyberkriminalität, insbesondere über staatlich gelenkte Akteure, können wir nicht nur effizient auf Angriffe reagieren, sondern auch präventiv Maßnahmen ergreifen, um zukünftige Angriffe abzuwehren.

Die Experten der Artefaktum besitzen ein umfassendes Wissen in mehreren Disziplinen und können komplexe, wissenschaftliche Analysen durchführen. Dabei versteht wir es, aus den kleinsten Details und Spuren ein präzises Bild des Tatgeschehens zu entwickeln.

Unsere Expertise liegt auch in der Fähigkeit zur Hypothesenbildung und Tatort-Rekonstruktion. Wir formulieren Hypothesen, die auf den Beweisen basieren, und überprüfen sie durch die forensischen Daten, um den Tathergang nachzuvollziehen und arbeiten dabei mit akribischer Genauigkeit und Problemlösungsfähigkeit und dokumentieren jeden einzelnen Schritt der Untersuchung umfassend und gerichtsverwertbar.

Die zunehmende Vernetzung digitaler Systeme und die steigende Komplexität staatlicher und krimineller Angriffe machen unsere Form der Cyberforensik nicht nur zur Notwendigkeit, sondern zur unserer Kernkompetenz in der modernen forensischen Wissenschaft und Dienstleistung für unsere Kunden. ■

#### Autor:

**Felix Juhl** ist Mitglied der Geschäftsführung von ARTEFAKTUM LLC.  
<https://artefaktum.net>



## Über angewandte Technologieentwicklungen zur digitalen Souveränität

### Krisen und weltwirtschaftliche Transformationen als Entwicklungsmotor der inneren Sicherheit

Reimund Igel

Foto: Autor

Viele junge Bundesbürger/-innen empfinden der aktuellen SINUS-Jugendstudie 2024 zufolge die heutigen Krisen als allgegenwärtige Normalität. Eine sich rapide abzeichnende gesellschaftliche Spaltung innerhalb unserer bis zur Jahrtausendwende einigermaßen homogenen Werteordnung stellt unser aller Miteinander zeitnah vor besonders tiefgreifende Herausforderungen. Extremistische Positionen naiver Überlebensstrategien bilden ebenso wenig ein tragfähiges Fundament wie ein rückwärtsgerandter Zweckoptimismus im Umgang mit weltwirtschaftlicher Transformationen getreu dem Motto – ein weiter so wie immer – und bieten keinerlei belastbare und zufriedenstellende Antworten für die substanziellen und existenziellen Zukunftsängste der Breite unserer Gesellschaft. Deutschland braucht nicht nur ein ‚Gefühl‘ von Sicherheit, sondern für jeden erkennbar funktionierende resiliente Sicherheitsstrukturen, die glaubhaft einen unüberwindbaren Sicherheitsrahmen für alle Bereiche unseres freiheitlichen gesellschaftlichen Zusammenlebens fundamentalisiert.

In diesem Geiste versteht sich ein folgerichtiger Anspruch nach digitaler Souveränität jedoch gleichsam mit dem Dilemma verbunden, weder national noch europäisch vollumfänglich über

alle nötigen Ressourcen zu verfügen. In Teilbereichen exportiert Deutschland schon heute modernste Fertigungsanlagen und Produktionsmaschinen für den internationalen Markt. Ist es nicht längst an der Zeit, unsere erfolgreichen Exportschlager auch für unser aller Sicherheit viel intensiver auf unserem Binnenmarkt einzusetzen? Konzentrieren wir bestehende Stärken und Formen unter Staatsbeteiligung und Kooperation der Besten aus Wirtschaft, Wissenschaft, Forschung, Gesellschaft und Politik eine nationale ‚Chip-Agentur‘. Die Resilienz-Strategie des Landes Hessen vom Dezember 2023 sieht vor, Resilienz und Krisenfestigkeit der Gesellschaft nicht nur als Gemeinschaftsaufgabe zu begreifen, sondern den „Kommunen als Grundlage und Orientierungspunkt für eigene Maßnahmen sowie zur Sensibilisierung von Privatwirtschaft, Zivilgesellschaft, Wissenschaft und Medien“ zu dienen. Haben wir die Ernsthaftigkeit der Lage wirklich verstanden, dann müssen wir weit darüber hinaus gehen und unsere Fähigkeiten hierzu zeitnah deutlich ausbauen.

Seit Jahrzehnten kennen und leben wir vergleichbare Herausforderungen im Rahmen unserer Landes- und Bundesverteidigung, denn nur mit starken Verbündeten und dem Vertrauen, dass der Partner sich so verhält wie man es

abgesprochen hat, der Verlässlichkeit, dass der Partner auch in schwierigen Zeiten zu einem steht und der Verbindlichkeit, dass der Partner seine Zusagen immer bereit ist einzuhalten, definieren sich sicherheitspolitische Konstanten als unmissverständliche Botschaften.

Wir müssen unbeirrt und dauerhaft konsequent für den Erhalt und Ausbau unserer Schlüsseltechnologien kämpfen und dabei Forschung und Entwicklung als zentralen Bestandteil von Wachstum und Leistungsfähigkeit verstehen, um diese in partnerschaftlich modernste produktive Strukturen umzusetzen. Eine industriestrategische Ausrichtung einer gemeinschaftlichen industriepolitischen Agenda im Einklang kommunaler-, landes- und bundespolitischer Standortpolitik. Technologieentwicklungen dieser Güte beruhen weder auf einer Insellösung, noch können sie durch eine One-Man-Show generiert werden. Forscher, Entwickler und Experten aus unterschiedlichsten Bereichen arbeiten in weltweit verteilten Forschungseinrichtungen an gemeinsamen Lösungen. So besteht Chipentwicklung nicht nur aus einer Verbesserung von Lithographie, um kleinere Strukturen wie 1nm Chips zu fertigen. Grundlagenforschung für neue Materialien, neue Fertigungsmethoden, neue Strukturen im Design,



Foto: J. Eistermeier

neue Fertigungssysteme und –prozesse sind notwendig, um das Ziel des 1nm Chips zu erreichen. Das alles kann und wird niemals von einer kleinen lokalen Gruppe erreicht werden können.

In diesem Verständnis charakterisiert sich digitale Souveränität auch als eine gemeinschaftliche Bildung und Fusion von Expertise auf Grundlage gemeinsamer Werte. Partner sind dann nicht nur militärische Verbündete, wie in der NATO oder EU, sondern auch Wissenschaft, Behörden und Unternehmen. Verstehen wir Informationstechnologien als überlebenswichtigen und rationierten Rohstoff, ähnlich seltener Erden, erfordert es Vereinbarungen im Verständnis einer Notgemeinschaft zu einem abgestimmten Weg, dem sich alle nachgelagerten Aktivitäten, Prozesse und Methoden effizienter unterordnen lassen.

Cybersicherheit für unsere kritischen Infrastrukturen bedeutet am Beispiel unserer kommunalen Verwaltungen mit all ihren unterschiedlichen Netzwerktopologien, ggf. auch älteren Bestandsstrukturen, jetzt ein Mindestmaß an Modernisierungsbedarf von Altanwendungen und Ausstattungen unter der Vorgabe Nationaler Interoperabilität festzulegen. In Folge reihen sich Vorsorgemaßnahmen, Training und Entwicklung neuer

Expertisen für die unmittelbare Abwehr oder Wiederherstellung, auf Stunden- und nicht Wochenbasis, hinsichtlich systemrelevanter gesellschaftlicher Funktionen ein. NIS2 (Europäische Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit) konforme Implementierungen führen zu fiskalischen Herausforderungen und sind gemeinschaftlich zu schultern. Der Faktor Zeit wird in der Umsetzung zum existentiellen Prüfstein.

Welche Schwerpunkte setzen wir für die Bereiche der künstlichen Intelligenz, Chipfertigung, Quantentechnologie, Kryptographie und Cloudtechnologie in Deutschland?

Nutzen wir intensiver und proaktiver die sich bildenden Expertisen aus den Entscheidungen von Microsoft und Google für KI-Rechenzentren in Deutschland, die existierenden Fertigungstechnologien (z.B. Böblingen und Dresden) für Chips, erweitert um TSMC in Dresden, das neue Quanten-Valleys in Ehningen, mit dem Testcenter der NATO und die neuen Verschlüsselungstechnologien mit den neuen NIST Standards für Post-Quanten-Kryptographie, maßgeblich entwickelt in Europa.

Entscheidend ist die Vermeidung zukünftiger Vermögensschäden durch

Cyberangriffe durch eine Fokussierung auf eine zentrale und schnelle Überführung validierter Forschungs- und Entwicklungsergebnisse in technologische Industrielösungen. Wie am Beispiel Bau-schiff, ist es notwendig alle Bausteine an den richtigen Platz zu stellen und gemeinsam an einem Tisch die Expertisen für eine schnelle und effiziente Realisierung zu nutzen. Anstatt Jahre über eine Goldrandlösung zu philosophieren, könnten wir uns auf einen in Deutschland entwickelten Verschlüsselungs-Chip fokussieren, der es ermöglicht auf PCs und Servern, nur verschlüsselte Informationen zu verarbeiten, ähnlich dem Prinzip der bei Full Homomorphic Encryption verfolgt wird. National entwickelte Encryption Technologien würden das Risiko für bestehende Topologien mit nicht bis ins letzte Bit überprüfbarer Hardware minimieren und wäre die Basis für eine zukünftige Data Centric Security Strategie.

**Ganz im Sinne eines digitalen Regenschirms.** ■

**Autor:**

**Reimund Igel,**  
Senior Technology Sales Representative  
Geschäftsbereich Verteidigung



Foto: GDELS

## Brücken bauen in der Zeitenwende

Dr. Thomas Kauffmann

**Artikel 24 Absatz 2 des Grundgesetzes bestimmt: „Der Bund kann sich zur Wahrung des Friedens einem System gegenseitiger kollektiver Sicherheit einordnen; er wird hierbei in die Beschränkungen seiner Hoheitsrechte einwilligen, die eine friedliche und dauerhafte Ordnung in Europa und zwischen den Völkern der Welt herbeiführen und sichern.“**

### 75 Jahre NATO

Als das maßgebliche System kollektiver Sicherheit hat die NATO während der letzten 75 Jahre unseren Frieden und unsere Freiheit gesichert. Nach mehr als zwei Jahrzehnten der Entspannung haben die Ereignisse seit 2014 und 2022 unterstrichen, dass sich dieses System keinesfalls überholt hat. Dabei ist und war die NATO nicht nur ein Zweckbündnis, sie versteht sich ausdrücklich auch als westliches Wertebündnis. Als solches ist sie den Idealen der individuellen Freiheit, Demokratie, Menschenrechte und Rechtsstaatlichkeit verpflichtet. Artikel 2 des Nordatlantikvertrags sieht die Förderung der wirtschaftlichen Zusammenarbeit und des Wohlergehens aller Parteien vor. Daneben erstreckt sich die Partnerschaft auch auf allgemeine politische und kulturelle Fragen, Umwelt- und Klimaschutz, humanitäre und Katastrophenhilfe.

### Brücken bauen

Kern der NATO ist die enge transatlantische Kooperation zwischen den mittlerweile 30 europäischen Mitgliedern und den beiden nordamerikanischen Partnern. Diese Wertepartner, die ihren individuellen Beitrag zur kollektiven Sicherheits- und Verteidigungsfähigkeit leisten, sind Brückenbauer. Gemeinsam sorgen wir nicht nur sinnbildlich, sondern auch faktisch dafür, dass unsere Streitkräfte im Verteidigungsfall effektiv zusammen kämpfen und zusammen obsiegen können.

Die Erfahrungen der Geschichte zeigen, Brücken zu bauen erfordert eine andere Haltung und andere Fähigkeiten, als Brücken zu zerstören. Brücken zu bauen, dauert auch länger als Brücken zu zerstören. Brücken zu bauen ist anstrengender.

Brücken zu bauen verlangt:

1. Expertise – Können
2. Präzision – Planung – Verlässlichkeit
3. Schaffenskraft – Integrität
4. Teamwork

Was bedeutet das für die Rüstung in der Zeitenwende? Wie können wir schneller, effizienter, innovativer, digitaler und letztlich kriegstüchtiger werden?

### Die Transatlantische Brücke

Zunächst müssen wir die transatlantische Brücke stärken. Auf beiden Seiten dieser Brücke teilen wir dieselben Werte und sind schon deshalb bevorzugte Handelspartner füreinander. Auf beiden Seiten teilen wir auch das Ideal eines freien Marktes. Unsere Regierungen müssen für ein funktionierendes Marktumfeld sorgen, auf dem das beste Angebot auf die höchste Nachfrage trifft. Protektionismus treibt die Preise, er hemmt und verhindert Innovation. Regelbasierter, fairer, transparenter Wettbewerb fördert Innovation – das steht nicht im Gegensatz zu dem staatlichen Ziel, eigene Schlüsseltechnologien zu fördern. Anstelle einer europäischen Autonomie müssen wir eine «Grand Strategy» zwischen Europa und den Vereinigten Staaten entwickeln und vereint an dieser Brücke weiterbauen. Wir dürfen nicht zulassen, dass sie einzustürzen droht. Wir dürfen auch nicht zulassen, dass Europa im Zuge der «great power competition» zwischen den USA und China ins Hintertreffen gerät – dies muss im beiderseitigen, transatlantischen Interesse sein: Auch die USA werden in der zweiten Amtszeit von Präsident Trump angesichts der globalen Herausforderungen ein starkes, verlässliches Europa einfordern und eine gestärkte transatlantische Brücke zur Wahrung ihrer eigenen globalen Interessen brauchen.





Foto: J. Elstermeier

### **Kooperation ist die beste Brücke**

Nicht weniger wichtig sind die vielen Brücken, die wir alle mit unseren Geschäftspartnern bauen und bereits gebaut haben. Im Inland und über Grenzen hinweg, in ganz unterschiedlichen Größen, aber immer stabil und tragfähig. Kooperation ist die beste Brücke, die zwei eigenständige Unternehmen und Unternehmer verbinden kann. Gemeinsam mehr erreichen zu können als allein – das ist effizient und klug. Voraussetzung für diese Effizienz ist auch hier eine gemeinsame Wertebasis. Unsere Werte stehen nicht nur auf dem Papier, sind nicht allein Sache von Politikern und Diplomaten, sondern müssen von jedem Einzelnen von uns gelebt werden. Auf dieser Basis können Unternehmen und Individuen ganz unterschiedlicher Herkunft im beiderseitigen Interesse ihr Geschäft betreiben. Nicht nur auf seinen eigenen Vorteil bedacht zu sein, klug, aber gleichzeitig vertrauensvoll und mit

dem Gemeinwohl im Blick zu handeln, sollte unser Leitbild sein. Besonders verpflichtet sind große Unternehmen gegenüber ihren Partnern aus dem Mittelstand.

Schlagen wir die Brücke zwischen unseren nationalen – und damit bündnisweiten – Sicherheitsinteressen, freiem Markt und wertebasiertem unternehmerischem Handeln, dann ergibt sich für die Rüstungsindustrie die Leitlinie: Bei der Wahl unserer Schlüsselpartner darf es nicht um «billig» gehen, sondern um sicherheitsrelevante Kooperation im Bereich Hochtechnologie innerhalb einer Wertegemeinschaft, die sich durch Verlässlichkeit, Berechenbarkeit und vergleichbare Standards auszeichnet. Die eigene Expertise ist von entscheidender Bedeutung, aber reicht allein nicht mehr aus. Nur flexible, auf Zusammenarbeit und Partnerschaft angelegte Unternehmen treiben Innovation und Technologie. Sie lernen von anderen und voneinander, weil

sie mit offenen Augen durch die Welt gehen, erspüren Trends und zukünftige Bedürfnisse und sind in der Lage, diese effizient in leistungsfähige Produkte umzuwandeln und dem Nutzer zeitgerecht zur Verfügung zu stellen.

**Bauen wir Brücken, um bisher unverbundene Teile miteinander zu verbinden, um auf beiden Seiten des Atlantiks als Team zu arbeiten – und um Zeitenwende zu leben und aktiv mitzugestalten.** ■

**GENERAL DYNAMICS**  
European Land Systems

#### **Autor:**

**Dr. Thomas Kauffmann** ist Geschäftsführer von GDELS in Deutschland und als Mitglied des europäischen Konzernvorstands verantwortlich für den globalen Vertrieb der Unternehmensgruppe.



Foto: Autor

## Sicherheitsanker für Digitale Souveränität

### Geschützt und unabhängig „made in Germany“ und Europa

Markus Lehmann

Der gerade veröffentlichte Lagebericht des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zeigt eine deutlich gestiegene Bedrohungslage. Allein der deutschen Wirtschaft entsteht durch Cyberattacken jährlich ein Schaden von gut 179 Milliarden Euro. Zwei Drittel der Unternehmen (65 Prozent) sehen ihre Existenz durch einen erfolgreichen Cyberangriff bedroht. Russland und China haben sich zu den wichtigsten Ausgangsbasen von digitalen und auch analogen Angriffen auf die deutsche Wirtschaft entwickelt: 45 Prozent der betroffenen Unternehmen konnten mindestens einen Angriff nach China zurückverfolgen, 39 Prozent nach Russland. Angesichts der aktuellen sicherheits- und geopolitischen Lage stellt sich die Frage der Souveränität unseres Staates in Bereichen wie Digitalisierung, Produktion und Handel. Unsere wesentliche Wirtschaftsleistung erbringen wir in diesen Bereichen, zumal Deutschland arm an Rohstoffen ist und diese einführen muss. In den letzten Jahrzehnten profitierten wir als Handelsnation von der Auslagerung der Produktion in Schwellenländer mit günstigen Lohnkosten, von Handelsabkommen mit dem Osten wie dem Westen und einer starken deutschen Wirtschaft mit extrem erfolgreichen Außenhandelsbeziehungen. Begründet haben wir dies auf dem Siegel „made in Germany“ mit deutscher Ingenieurskunst, Innovationskraft und Erfindergeist. Mit der wachsenden Abhängigkeit von Digitalen Infrastrukturen stellt sich die Frage des nationalen Kontexts der digitalen Souveränität und deren Relevanz, insbesondere für Deutschland und die EU.

**Kann digitale Souveränität souverän sein, wenn sie nicht national ist? Die aktuellen Ereignisse zeigen, dass sie zumindest europäisch gedacht werden muss.**

Die großen Hyperscaler bestimmen unsere Tool-Landschaften und geben die Rahmenbedingungen für die Verarbeitung unserer Daten vor. Damit sind wir zwar weltweit interoperabel und können von den innovativen Weiterentwicklungen der großen Unternehmen partizipieren. Aber gleichzeitig erhöhen wir unsere technologische Abhängigkeit. Oft legen die Herkunftsländer dieser Hyperscaler den behördlichen Zugriff auf diese Daten fest und können Unternehmen verpflichten, diese Daten auch außerhalb Deutschlands herauszugeben. Durch die Wahl eines in Deutschland ansässigen Dienstleisters kann die Bundeswehr sicherstellen, dass ihre Daten nach den deutschen Datenschutzgesetzen geschützt sind. Allerdings beginnt damit das Dilemma. Denn im Rahmen der Bündnisverpflichtungen ist gerade die Interoperabilität in den gemeinsamen Stäben und Kontingenten unabdingbare Voraussetzung. Wir müssen also in gewissen Ausprägungen auf die Produkte von z.B. Microsoft, Google, Oracle etc. zurückgreifen oder mindestens deren Interoperabilität sicherstellen und benötigen zusätzliche Maßnahmen und Strategien zum Erhalt unserer Digitalen Souveränität. Im nachfolgenden sollen die rechtlichen, technologischen, materiellen und personellen Rahmenbedingungen betrachtet werden, die die Bedeutung des nationalen Einflusses auf die

Digitale Souveränität und damit den Sicherheitsanker für unser bekanntes Bauspiel herausstellen.

#### Partnerschaften geben Sicherheit

In erster Linie gehört dazu die Schaffung der politischen und rechtlichen Rahmenbedingungen durch Absprachen und Regelungen mit den Partnernationen. Dadurch sollen Schutz und Sicherheit der Daten gewährleistet werden, wenn diese nicht im Rahmen der gemeinsamen Aufgabenerfüllung bereitgestellt werden müssen. Kritiker argumentieren hier wiederum schnell, dass solche Abkommen keineswegs digitale Souveränität oder Datenhoheit garantieren und schnell obsolet sein können, sollte z.B. das aktuelle Datenaustauschabkommen zwischen der EU und den Vereinigten Staaten wie seine Vorgänger kippen. Besonders spannend ist dies mit Blick auf die Ergebnisse der Präsidentschaftswahlen in den USA.

#### Der nationale Datentreuhänder verspricht Datenschutz und Security

Der Datentreuhänder gewährleistet das vier-Augen-Prinzip und sichert die Nutzung der Daten innerhalb der vereinbarten Rahmenbedingungen ab, auch wenn wir auf potenziell unsicheren Infrastrukturen unterwegs sind. So werden Zugriff, Manipulation durch nicht-autorisierte Personen oder Abfluss der Daten vermieden.

#### Sichere Infrastruktur als Basis

Zu der nächsten Stufe der organisatorischen Absicherung der Datenzugriffe, die wir für die Umsetzung der Digitalen

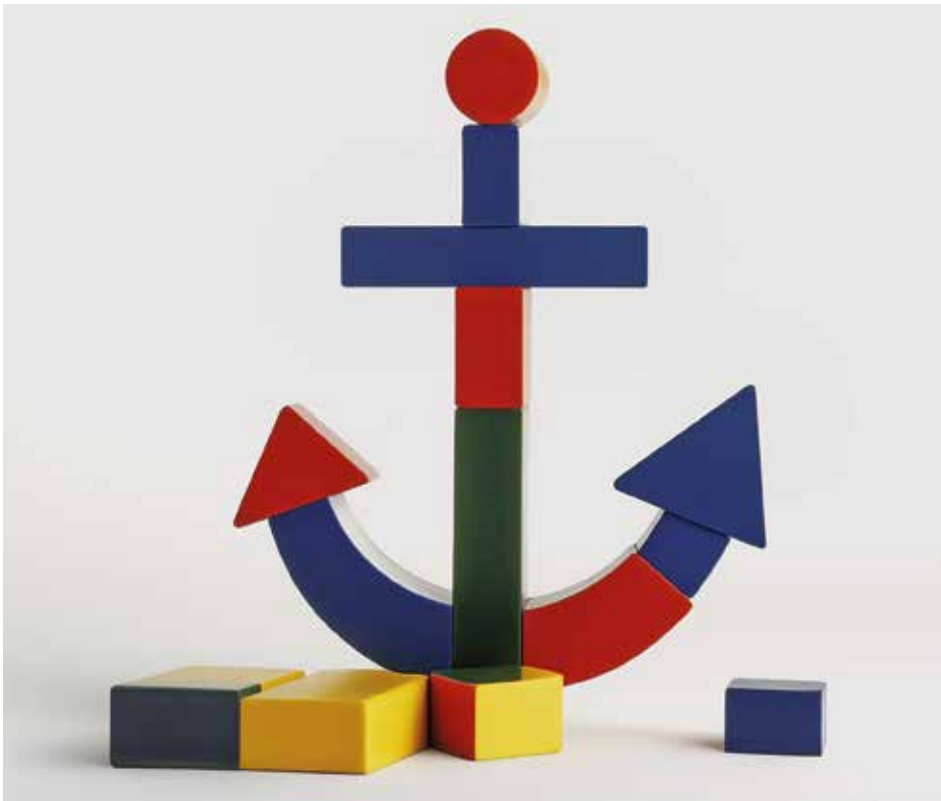


Foto: Jamie Tchassanti mithilfe von Midjourney (KI)

Mit KI können nicht nur Bilder entstehen, die der Schwerkraft widersprechen. Sondern zukünftig wird uns die KI Funktionalitäten liefern, die wir uns heute noch nicht vorstellen können.

Souveränität betrachten, gehört die Speicherung und Verarbeitung aller Daten in einer sicheren Rechenzentrums-Infrastruktur in Deutschland. Daten bleiben in Deutschland geschützt und können nicht ins Ausland verschoben werden. Kundenbetreuung und Datenverarbeitung erfolgen nach Regelungen zum Umgang mit Verschlusssachen mit dem Sperrvermerk „nur Deutschen zur Kenntnis“. Der Zugriff auf die Systeme durch Mitarbeiter aus dem Ausland wird unterbunden und alle administrativen Zugriffe auf Kundendaten werden protokolliert. Die Dokumente geben Nachweis über die durchgeführten Arbeiten und den Umfang des Zugriffs. Support- und Betriebszugriffe werden durch die zugrunde liegenden Datenzugriffskontrollen begrenzt und nur an akkreditiertes Personal weitergeleitet. Die Datenübertragung zwischen Rechenzentren und den Administratoren und Nutzern erfolgt über eine gesicherte Kommunikationsverbindung.

#### **Pseudonymisierung der Kundendaten**

Für vertrauliche und unbedingt schützenswerte Kundendaten setzen wir heute zusätzlich das Verfahren der Pseudonymisierung ein. Damit werden Kunden- und Auftragsdaten auch in den

internen Systemen des Serviceproviders nur anonymisiert dargestellt. Die Daten zur Kundenidentität sind intern und extern nur für das zum Zugang ermächtigte Personal in Klarlage einsehbar. So wird gewährleistet, dass sämtliche Kundendaten auch dann nicht verwertbar sind, wenn durch einen Cyberangriff oder einen Innentäter der unerlaubte Zugriff auf die Kundendaten gelungen ist. Kundenname, Adresse und genutzte Produkte und Plattformen können so vertraulich gehandhabt und alle Informationen geschützt werden.

#### **Verschlüsselung – stark erhöhter Schutz von Daten**

Nach der lokalen Einschränkung der Zugriffe auf Deutschland und der Pseudonymisierung ist die Verschlüsselung der Daten die nächste Sicherheitsstufe. Dabei werden die Schlüssel zur Verschlüsselung der Kundendaten außerhalb der Infrastruktur gespeichert und verwaltet. In der Regel besitzt nur der Kunde oder die vom Kunden beauftragten und autorisierten Mitarbeiter den Schlüssel für die sichere Verschlüsselung der Daten. Die Entschlüsselung von Kundendaten erfordert einen Aufruf von außerhalb der Infrastruktur, um den extern verwalteten Schlüssel des Kunden zu erhalten. Kunden dürfen darauf vertrauen, dass jede

Anfrage mit einer Begründung versehen ist und geprüft wird.

#### **Ausbildung und Qualifikation**

Organisatorische, materielle und technologische Sicherheitsmaßnahmen funktionieren nur, wenn Menschen ihnen vertrauen und sie einhalten. Zur Digitalen Souveränität gehört daher auch die digitale Bildung, Weiterbildung und stete Auseinandersetzung mit der IT-Sicherheit. Die Sensibilisierung und Bewusstseinsbildung der Mitarbeitenden für die Bedeutung der Digitalen Souveränität und den Schutz der eigenen Daten ist ein grundlegendes Wissen, das wir in der Schule, in den Firmen und der Gesellschaft täglich vermitteln müssen. Der Schutz der eigenen Daten muss eine Selbstverständlichkeit sein, die ohne „weiteres Nachdenken“ zur automatischen Handlung im Digitalen Raum gehört.

#### **Digitale Souveränität:**

##### **Basis staatlicher Souveränität**

Hackerangriffe, Desinformation sowie Spionage sind die Herausforderungen, denen wir uns im Cyberraum täglich stellen müssen. Cybersecurity ist für Unternehmen und Verwaltungen jeder Größe überlebenswichtig. Der Schutz von sensiblen Daten und Betriebsabläufen ist die Basis für unsere digitale Souveränität. Deutsche Firmen können hier den Unterschied ausmachen. Sie haben auch eine intrinsische Motivation, uns vor Angriffen zu schützen. Diese nationalen Ressourcen müssen wir besonders für die kritischen Bereiche unseres gesellschaftlichen Lebens stärken.

#### **Die gute Nachricht:**

##### **Wir müssen nicht danach suchen.**

Mit seinen Unternehmen und starken europäischen Partnern hat das Land einen grundsoliden Sicherheitsanker. Ein Sicherheitsanker für seine digitale Souveränität und damit auch für die demokratischen Werte auf dem Kontinent. ■



#### **Autor:**

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



Foto: Bundeswehr

# Abschreckungsfähige Landstreitkräfte

## Resilienz und die Industrie als Säulen der nationalen Sicherheit und Souveränität

Generalleutnant Andreas Marlow

Die Gewährleistung der Sicherheit, nach innen wie nach außen, ist Kernaufgabe eines souveränen Staates. Sicherheit ist Voraussetzung für Freiheit, Wohlstand, soziale Stabilität und politische Handlungsfreiheit. Für uns ist und bleibt die NATO unfraglich der Pfeiler der deutschen Außen- und Sicherheitspolitik. Wir vertrauen auf starke Partner in der NATO und unsere Partner vertrauen auf uns.

Als die wesentliche Kraft in Zentraleuropa will und muss Deutschland die Bundeswehr signifikant und schnell stärken. Deutsche Landstreitkräfte spielen dabei die Schlüsselrolle. Denn der Angriffskrieg Russlands gegen die Ukraine zeigt erneut, dass Kriege in Europa an Land entschieden werden. Nur mit starken und einsatzbereiten Landstreitkräften wird Russland abgeschreckt.

Die Ukraine zeigt uns auch, dass Krieg den Willen und die Fähigkeit zum Durchhalten erfordert. Diese Erkenntnis hatte auch schon Clausewitz, der die Stärke der Willenskraft als einen bestimmenden Faktor der Widerstandskraft einer Kriegspartei identifizierte. Die Frage ist daher, auf welchen Krieg (den wir dadurch verhindern wollen) bereiten wir uns vor? Müssen wir uns zur Abwehr eines Angriffs Russlands (als derzeit einzigem offen erklärten Gegner unserer europäischen Freiheitsordnung) auf einen Krieg mit einigen Wochen, Monaten oder gar Jahren Dauer vorbereiten? Jede dieser Optionen führt zu unterschiedlichen Schlussfolgerungen. Der worst case wäre, wie im Fall der Uk-

raine, ein jahrelanger Krieg. Gegen diesen Fall müssen wir gewappnet sein. Der Erhalt staatlicher Souveränität hängt damit von aufwuchs- und durchhaltefähigen Streitkräften, einer resilienten Gesellschaft und einer leistungsstarken Industrie ab.

### Landstreitkräfte als Rückgrat der Verteidigung

Deutschland stellt ab dem 1. Januar 2025 für die NATO drei Heeresdivisionen für die Verteidigung Europas bereit. Die erste („Division 2025“) muss ab diesem Zeitpunkt in hoher Einsatzbereitschaft schnell auf eine potenzielle Aggression Russlands reagieren können. Für die anderen beiden Divisionen gelten abgestufte Verfügbarkeiten. In den kommenden Jahren werden auch diese zur schnellen Einsatzbereitschaft an der NATO-Ostflanke befähigt.

Mit der Übernahme der Führung der Heimatschutzkräfte und der taktischen Führung in der Dimension Land (die mehr als das Heer umfasst) im Operationsplan Deutschland wird das Heer künftig noch mehr leisten müssen. Alle Aufgaben, sowohl das Bereitstellen der drei Heeresdivisionen für die Verteidigung der NATO-Ostflanke als auch die Führung des Heimatschutzes und anderer Kräfte im Operationsplan Deutschland können nicht alleine durch aktive Truppenteile sichergestellt werden. Sowohl das Feldheer und die Militärische Grundorganisation als auch die Heimatschutzkräfte müssen im Krisen- und Kriegsfall aufwuchsfähig sein. Dazu braucht das Heer zum einen die Fähigkeit, bruchfrei und

bei Bedarf beschleunigt große Mengen an Personal auszubilden und zum anderen eine einsatzbereite und voll ausgestattete Reserve, um unsere Fähigkeiten schnell zu verstärken und eine Brücke zu schaffen bis neues Personal bereitgestellt werden kann.

Ersteres untersucht das Ausbildungskommando derzeit und entwickelt Handlungsmöglichkeiten für die Ausbildung im Spannungs- und Verteidigungsfall. Wesentliches Element zum Decken eines höheren Ausbildungsbedarfes wird die Reduzierung von Ausbildungsabschnitten auf die Kernbefähigung zum Kampf oder der erforderlichen Spezialisierung sein.

Von der Einführung des Neuen Wehrdienstmodells, Basiswehrdienst, wird vor allem eine Stärkung der Personalgewinnung für die Reserve erwartet. Für die Ausstattung der Reserve darf funktionierendes Material nicht mehr entsorgt werden, sondern muss konsequent in Depots eingelagert werden.

Ziel ist es, reaktionsfähige und aufwuchsfähige Landstreitkräfte zu schaffen, die jeden Aggressor zur Überzeugung kommen lassen, dass ein bewaffneter Konflikt mit diesen ein unkalkulierbares Risiko für ihn ist.

### Resilienz: Die Stärkung der Gesellschaft

Die Bundeswehr wird aber in einem solchen Szenario nicht isoliert handeln können, sondern ist von einer resilienten Gesellschaft abhängig. Resilienz beschreibt die Fähigkeit, Krisen zu über-

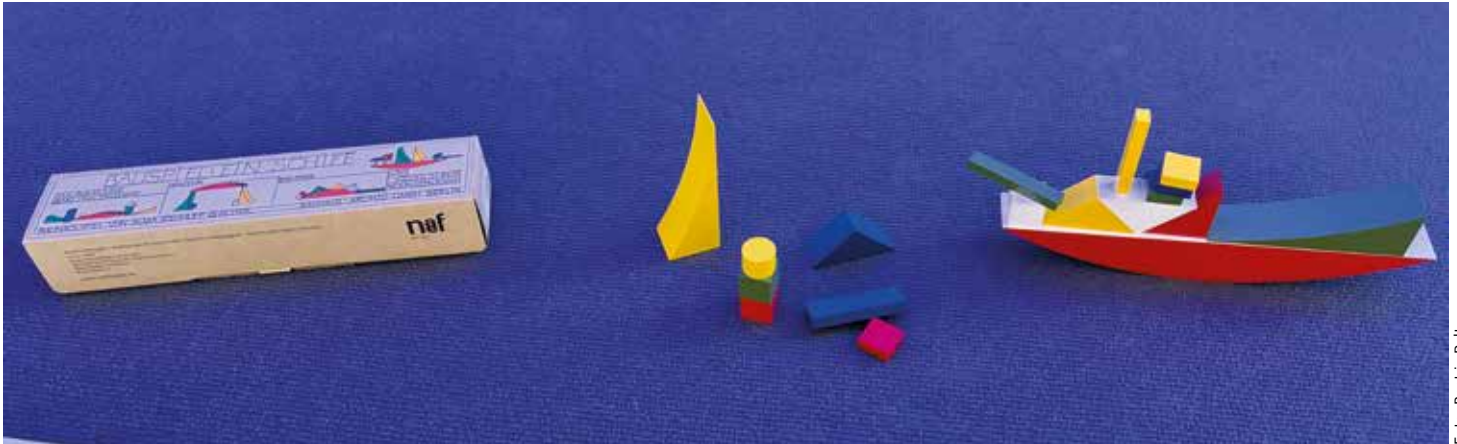


Foto: Beatrix Palt

stehen, sich schnell von Schocks zu erholen und handlungsfähig zu bleiben. Sie ist daher auch ein wichtiger Faktor der Abschreckung von Aggressoren. Eine resiliente Gesellschaft ist in der Lage, auch unter den extremen Bedingungen eines Krieges zu funktionieren. Dies schließt nicht nur die Versorgungssicherheit der Zivilbevölkerung und Streitkräfte, sondern auch die Aufrechterhaltung wichtiger Infrastruktur und der öffentlichen Ordnung ein.

Im Rahmen der Gesamtverteidigung gilt es, die Balance zwischen den Ressourcen für die Zivilgesellschaft und der Bundeswehr zu schaffen. Resilienz wird sich nicht ohne das Schaffen von Material- und Personalreserven sowohl in der Zivil- als auch in der Militärischen Verteidigung erreichen lassen. Beispielsweise werden die Heimatschutzkräfte primär verteidigungswichtige Infrastruktur schützen und die militärische Bewegungsfreiheit in Deutschland erhalten. Den Schutz ziviler Infrastruktur werden Polizei und zivile Sicherheitsdienste übernehmen müssen. Um die Koordinierung voran zu treiben, ist es angeraten, Elemente der Zivilen Verteidigung in militärische Manöver stärker einzubeziehen.

### **Die Rolle der Industrie: Garant für Sicherheit und Souveränität**

Die Verteidigung in der Ukraine hängt auch von Waffen- und Munitionslieferungen ab. Durch diese profitiert die Ukraine von der Leistungserbringung

der europäischen und amerikanischen Rüstungsindustrie. Doch die derzeitigen Produktionskapazitäten sind weder für die Unterstützung der Ukraine noch für die europäischen Streitkräfte ausreichend. Kapazitätssteigerungen sind notwendig. Insbesondere die Produktion von Munition muss ab Tag 1 eines Konfliktes die Durchhaltefähigkeit der Streitkräfte sicherstellen. Jede fehlende Artilleriegranate kostet letztlich Soldaten der Landstreitkräfte das Leben.

An den geringen Industriekapazitäten zeigt sich eine Konsequenz einer jahrelangen Unterfinanzierung der Streitkräfte, welche auch durch das Sondervermögen nicht gelöst werden kann. Nur wenn der Staat kontinuierlich Rüstungsgüter von der Industrie abnimmt, werden auch dauerhaft Kapazitäten vorgehalten, die die Ernsthaftigkeit der Verteidigungsbereitschaft signalisieren. Umso wichtiger erscheint es, in der Haushaltsplanung langfristig mindestens 2% des BIP für den Einzelplan 14 vorzusehen. Diese bilden indes nur das Fundament. Weitere Anstrengungen sind erforderlich.

### **Fazit: Synergien für nationale Sicherheit**

Die Bundeswehr und dabei vor allem die Landstreitkräfte, die resiliente Gesellschaft und die Industrie bilden gemeinsam die tragenden Säulen der nationalen Sicherheit und Souveränität. Alle drei Bereiche stehen in enger Wechselwirkung zueinander

und sind unverzichtbar für die Durchhaltefähigkeit eines Staates in einem Konflikt. Schon die Corona-Krise hat uns vor Augen geführt, wo dabei die Grenzen der weltweiten Vernetzung sind und wo eine Nation eigene Kapazitäten braucht. Wichtiger Baustein hierfür ist eine eigene Rüstungsindustrie mit den damit einhergehenden Fähigkeiten, zu denen ganz wesentlich die Fähigkeit Munition zu produzieren gehört.

In verschiedenen Verwendungen habe ich gelernt, dass unsere Partner große Erwartungen an uns haben und dass wir, vor allem anderen, als Landmacht verstanden werden. Deutschland wird als Drehscheibe fungieren und den Kern der Landstreitkräfte in der Zentralregion stellen müssen, sollte es zu einem Konflikt kommen. Nur Deutschland ist dazu in der Lage. Ich bin der Überzeugung, nur wenn wir dies so vorbereiten, dass es im Ernstfall auch mit Sicherheit funktionieren wird, erzeugen wir die glaubwürdige Abschreckung, um genau diesen Konflikt zu verhindern. Alle Akteure haben dabei Ihre Rolle und Verantwortung. ■

### **Autor:**

**Generalleutnant Andreas Marlow** ist seit September 2023 Stellvertreter des Inspektors des Heeres und Kommandeur Militärische Grundorganisation in Strausberg.



Foto: Autorin

## Expertise(bildung) gewinnt!

# Nachhaltige Rüstung – Bauspiel: Ein Schiff

Prof. Dr. (habil.) Beatrix Palt

„Ich möchte nicht auf meinem Grabstein stehen haben, dass ich nicht aus den Putschen gekommen bin“. Dieser Satz eines Generals war Antrieb zu meiner eigeninitiativen qualitativen empirischen Untersuchung (keine Auftragsforschung!) zur Kriegstüchtigkeit bzw. die Frage, wie und wodurch wir gewinnen, zu analysieren.<sup>1</sup>

Die Studie kommt zu dem Schluss, dass Beschaffungswesen und -praxis zum angenommenen inhärent systembedingten Vermögensschaden und zu einer inhärent systembedingten Gefährdung der Kriegstüchtigkeit führen. Die Lösung des Systemfehlers liegt nicht in einer weiteren Veränderung der Regulatorik, sondern in der (ausdrücklich offensiven) Anwendung von Staatsräson, verstanden als Ausübung der politischen Richtlinienkompetenz im Sinne der Kriegstüchtigkeit. Der Begriff der Staatsräson wurde gewählt, da die Erlangung der Kriegstüchtigkeit einem grundlegenden Zweck des Staates dient, nämlich dem Schutz seiner Bürger und der Funktionsfähigkeit seiner Institutionen bei Katastrophe, Krise und Krieg. In der angespannten Sicherheitslage müssen sich der Staatsräson andere Belange unterordnen und Entscheidungen im Sinne der Kriegstüchtigkeit engagiert und stringent umgesetzt werden.

Ausdrücklich sei darauf hingewiesen, dass die Erlangung der Kriegstüchtigkeit durch die im Beschaffungswesen tätigen Akteure nicht erreicht werden kann, da auch sie durch die inhärent systembedingten Verwerfungen eingeschränkt werden. Die Zustandsbeschreibung enthält somit keinen Vorwurf an die damit befassten Mitarbeitenden sämtlicher Institutionen und Ebenen.

### Das Problem:

#### Ein inhärenter Systemfehler führt zu angenommenen Vermögensschäden

Der angenommene Vermögensschaden durch inhärente Systemfehler in Beschaffungswesen- und Praxis zeigt sich bei nicht marktverfügbaren, mit Entwicklungsbedarf versehenen und daher mit Risiko behafteten Projekten selbst dann, wenn interoperable, marktverfügbare Wirksysteme vorgesehen sind. Er lässt sich nicht in absoluten Zahlen quantifizieren, sondern argumentativ-qualitativ über den Faktor Zeit: Durch Verzögerungen in Kombination mit den in den gewählten Preismodellen zu berücksichtigenden Preissteigerungen und der Bearbeitungspraxis in Verbindung mit (vor oder nach Vertragsabschluss spielt keine Rolle) sehr eng gestrickten Vorgaben kommt es immer wieder zu Nachsteuerungen (Ursache), die wiederum mit Aufwand verbunden sind (Wirkung). Das gilt selbst für Versuche mit Vertragsmodellen, bei denen die Spezifikation erst nach Vertragsabschluss erstellt wird (z.B. Flottendienstboot) oder die Entwicklung der Fregatte Klasse F127, die Millionenbeträge, Personal und Jahre verschlungen hat (Wirkung).

Weder Regeländerungen noch andere Verfahren – wenn sie nur an einzelnen Punkten ansetzen – (z.B. Vertragsabschluss vor Spezifikation) lösen das inhärent systemische Problem, solange die an Rüstung Beteiligten in interdependenter Abhängigkeit im Ist-Zustand festhängen (Ursache), während sie (nachvollziehbarerweise!) ihre Lobby- und / oder Wirtschaftsinteressen vertreten (Wirkung).

### Die Lösung:

#### Staatsräson, Expertise & nationale (digitale) Souveränität

Die Wirkung bisheriger Maßnahmen liegt bislang nur auf der Ebene von Kanzler- (Beschaffung F-35A, Entscheidung zur Stationierung amerikanischer Mittelstreckenraketen) und Ministerhandeln (Beschaffungen von Munition und marktverfügbaren Wirkplattformen) und kann sie auch nur liegen, solange niemand den inhärenten Systemfehler behebt. Ein inhärenter Systemfehler kann nur durch einen kompletten Systemwandel OBERHALB der Vertragsebene per Richtlinienkompetenz angewiesen werden und NICHT durch Vertragsgestaltungen UNTERHALB der Systemebene. Staatsräson ist der Hebel, der aber nur dann zur Kriegstüchtigkeit führt, wenn gleichzeitig auf politische Entscheidungsmacht, Exzellenz in Expertise und nationale digitale Souveränität gesetzt wird, um Wirksamkeit (Kriegstüchtigkeit) zu erzielen.

Staatsräson wirkt, wenn der Staat

1. seine politische Entscheidungsmacht zum Wohle des deutschen Volkes einsetzt, z.B. über die strategische Steuerung von Rüstungsunternehmen mit Staatsbeteiligung mit Sperrminorität und die strategische Steuerung von strategischen Entwicklungsprojekten,
2. durch gezielte Beauftragung qualitativ und quantitativ forschungs- und wertebasierter Exzellenz in Expertise(bildung) das Wer, Wie, Was und Wozu absichert,
3. nationale (digitale) Sicherheit, Souveränität & Resilienz durch Staatsbeteiligungen bei den nationalen Champions und Fähigkeitsträgern durchsetzt und durch Direktbeauftragungen zur

nachhaltigen und langfristigen Entwicklung, Erhalt und Ausbau von Technologieführerschaft beiträgt.

Somit gilt es, Rüstungsprojekte anders anzugehen, und zwar

- Als modulare verteilte Wirksysteme (wie z.B. European Sky Shield) und modular einsetzbare, schwimmende, fahrende, etc. „Rechenzentren mit Funktionsbausteinen“. Von der Idee bis inklusive Nutzung im kurzen, durchgehenden Prozess, die Forschung der nächsten 10 Jahre antizipierend, mit offenen Schnittstellen interoperabel designt, entwickelt und umgesetzt.
- Von einem zivil-militärischen Dimensionen-übergreifenden High-Performance-Team entwickelt und umgesetzt, mit freiwilliger Selbstverpflichtung zu einer wertebasierten Zusammenarbeitsethik, bei der sich die Organisationen UND handelnden Personen den Grundsätzen von Nachhaltigkeit gemäß dem Ehrbaren Kaufmann zu anständigem Verhalten verpflichten und an diesen Grundsätzen gemessen werden.
- Mit Festpreisen ohne Preisgleitklauseln, dafür aber hart gesetzten Meilensteinen mit gegenseitiger Erfüllungspflichtung, bei denen lediglich technische Unmöglichkeiten und höhere Gewalt, nicht aber organisatorische und persönliche Unzulänglichkeiten als Verzögerungsgrund akzeptiert werden.
- Mit allseitig nachhaltigen Geschäftsmodellen dazu (selbst)verpflichtet, aus den begrenzt zur Verfügung stehenden Ressourcen (Geld, Personal, Zeit) die maximal mögliche Exzellenz in Expertise herauszuholen.
- Durch eine offensive Industriepolitik begleitet, bei der der Staat seine Richtlinienkompetenz zum Einsatz bringt und seine nationalen Fähigkeits-Champions durch Minderheitenbeteiligungen mit

### So zeigt es sich im öffentlichen Diskurs

Zeit im Sinne von Tempo und Zeitpunkt von Entscheidung oder Zeit, die mangelnde Expertise, Haltung, jede fehlende oder (zu) langsame Aktion kostet, Zeit, die wir verlieren, kostet Geld, bindet (bezahltes) Personal, kostet Technologievorsprung – und damit Kriegstüchtigkeit. Absicherungsdenken mit Fokus auf einzelne Systeme und im Verantwortungspingpong der involvierten Institutionen. Detaillierte Spezifikationen mit linear aufeinander aufbauenden Prozessen und Staffeltabübergaben, jahrelange Planungszeiten, verzögerte Lieferungen von dann veralteten Technologien/Produkten, die aufgrund von Preisgleitklauseln zu weit von den ursprünglich geplanten Kosten entfernt sind. Rechte am geistigen Eigentum (Intellectual Property Rights, IPR), die nicht sofort, sondern erst zur Nutzung erworben werden, verschieben die Finanzierung, verteuern die Beschaffung. Im Vergleich zu anderen Nationen zu wenig Direktvergabe. Bei Vergaben ins Ausland zu wenig vertraglich geregelt, welche Zulieferungen in Deutschland produziert und wie kleine und mittlere Unternehmen (KMU) berücksichtigt werden müssen. Jeder Punkt an sich, das Zusammenspiel deutet sicher auf einen angenommenen inhärent systembedingten Vermögensschaden durch Beschaffungswesen und -praxis hin.

Sperrminorität schützt, steuert und im Sinne der nationalen Sicherheitsinteressen direkt beauftragt.

- Durch eine in diesem Sinne durch das Kanzleramt strategisch gesteuerte Agentur der Bundeswehr, in der die Exzellenz in Expertise zusammengezogen und zum Einsatz gebracht wird.
- Qualitätsgesichert durch wissenschaftliche Begleitforschung mit allseitigem Vetorecht zur Sicherstellung der quantitativen und qualitativen Gütekriterien deutschen Beschaffungswesens und -praxis, eingebettet in die Beschaffung der Wertegemeinschaft. Wobei Vetorecht nicht in Verträge eingreift, sondern sofort und unmittelbar Prozesse stoppt und nachsteuert, die nachhaltiger kriegstüchtiger Beschaffung zuwiderlaufen.
- Durch ein expertiseforschungs- und wertebasiertes Projektmanagementsystem und -Team, bei dem die Beteiligten von Werten geleitet sind: Verantwortung, Vertrauen, Verbindlichkeit- und Verlässlichkeit.

Staatsräson ist der Hebel, mit dem der inhärente Systemfehler behoben werden kann, der aber auch nur dann zur Kriegstüchtigkeit führt, wenn gleichzeitig auf Exzellenz in Expertise und auf nationale digitale Souveränität gesetzt wird - zusammen mit den oben beschriebenen Maßnahmen gleichzeitig eingesetzt, um die gewünschte Wirksamkeit zu erzielen. Teilstreitkraft-übergreifende Interoperabilität bemannt/unbemannt im Verband und ein forschungs- und wertebasierter Projektmanagementansatz ZUSAMMEN bewirken dann die finanzierbare Entwicklung von Wirkplattformen, Rüstungsmanagement entlang der Prinzipien moderner IT-Entwicklung, Expertise und Werten. Nur wer sich so verhält, kann dabei sein.

Der Staat schafft mit seiner Richtlinienkompetenz, dem Zusammenwirken aller betroffenen Ressorts (z.B. Verteidigung, Wirtschaft, Finanzen), den Einstieg in für nationale Souveränität und Resilienz erforderliche nationale Champions sowie seine Rüstungsindustriepolitik, die Voraussetzung für Kriegstüchtigkeit.

Was, wie, wozu und mit wem? Die Behebung des inhärenten Systemfehlers und Sanierung mit den Menschen, die das können. Bauspiel: Ein Schiff – Expertise gewinnt. ■

#### Autorin:

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

### Nachhaltig kriegstüchtige Beschaffung

	ZEIT
WAS & WIE?	Staatsräson: Politisches Entscheidungshandeln zur Behebung des Systemfehlers, Expertise(bildung) und nationale (digitale) Sicherheit, Souveränität & Resilienz
WOZU?	Für „Nachhaltige Rüstung“ als produktives, effizientes und effektives Beschaffungswesen und -praxis, wirkungsvoll & finanzierbar zugleich
WER?	Die wertebasierte Bestenauslese: Fachlich, methodisch und persönliche Dispositionen (z.B. Mut, Reife, Leidenschaft, Raffinesse & Cleverness) im Einklang mit Verantwortung, Vertrauen, Verlässlichkeit und Verbindlichkeit im Miteinander

Der generische Ansatz „Nachhaltige Wirtschaft“: Was kann ich einbringen?



Foto: Autor

## Bauspiel – die Zweite!

Peter Tamm

Nach dem ersten Aufschlag im Juli diesen Jahres hat es die Initiatorin, Frau Professor Beatrix Palt, wiederum erfolgreich geschafft, eine bedeutende Gruppe von Fachleuten aus Politik, Militär, Forschung, Bildung und Wirtschaft zu motivieren ihre Beiträge, Lösungen und konkreten Erfahrungen zur Expertise(bildung) zu kommunizieren. Die zweite Sonderbeilage zum InfoBrief Heer ist wieder eine gezielte Zusammenstellung aus Forschung & Lehre über das Beschaffungswesen in der Zeitenwende bis hin zu gesamtgesellschaftlichen Aspekten des Sicherheitsbegriffs einer wehrhaften Gesellschaft, die siegfähig sein will: Es bedarf der Expertise, eines strategischen modularen Baukastensystems – „Bauspiel: EinSchiff“ – die (finanzierbar!) zu nationaler (digitaler) Sicherheit, Souveränität und Resilienz führt.

Daher stellen Experten aus dem militärischen Bereich hier ihre Positionen dar und auch die Überlegungen der NATO zur Förderung der Innovation in Schlüsseltechnologien findet ihren Platz. Künstliche Intelligenz, Cybersicherheit, Schutz kritischer Infrastrukturen und natürlich Software Defined Defence sind die zentralen Aspekte der Expertise, die zu Sicherheit führen, wie führende Persönlichkeiten mit ihren Entwicklungsschwerpunkten und Lösungen zur Expertisebildung darstellen. Auch geht es nicht ohne Brückenbauen, um die Allianz Europas mit den

USA mit Expertise, Schaffenskraft und Teamwork zu festigen. Die empirische Studie zu nachhaltiger Rüstung werden weder Politik, Militär, Industrie, noch Bundesrechnungshof oder Verteidigungsausschuss ignorieren können.

Fazit: Wir zeigen konkret, wie wir schnell, effizient, innovativ, digitaler und finanzierbar werden, um kriegstüchtig zu sein. Daher bleibt „Bauspiel: Ein Schiff“ unverändert das Leitmotiv dieser Initiative. Diese besondere Form des Spielens bietet die erforderlichen Freiheiten, mit Kreativität, Fantasie und Ideenreichtum, modular vielfältige Modelle und Lösungen zu erstellen – jetzt auch unter Einsatz von KI.

Ich danke allen Autorinnen und Autoren und den dazugehörigen Teams dafür, dass sie mit ihren Beiträgen erneut ihre Positionen und ihre Ansätze präsentieren. Und ich danke dem Förderkreis Deutsches Heer e.V. für sein besonderes Engagement, dieses Thema in die richtigen Kanäle zu steuern. Er leistet damit einen wertvollen Beitrag an der Seite der Streitkräfte, und im Schwerpunkt des Heeres, um kriegstüchtig und auch siegfähig zu sein. Dies möchte ich von meiner Seite unterstützen!

Ich wünsche viel Freude und vor allem wichtige Erkenntnisse bei der Lektüre!

Ihr  
Peter Tamm

Entworfen wurde das Bauspiel im Rahmen der Gestaltung eines Kinderzimmers im „Haus am Horn“ für die große Bauhausausstellung 1923. Zu diesem Zeitpunkt war Siedhoff-Buscher in der Holzbildhauerei Bauhaus Weimar tätig. Alma Siedhoff-Buscher hat über weitere Spielzeuge hinaus unter anderem eine Malfibel sowie Kindergartenmöbel geschaffen. Gerade die Möbel waren in ihrer Multifunktionalität ihrer Zeit weit voraus. Das ikonische Bauspiel ist schon seit 1977 als Re-edition verfügbar. Heute wird es unter dem Siegel des Bauhaus-Archivs Berlin von der Manufaktur NAEF in der Schweiz hergestellt.



Foto: J. Elstermeier



Foto: Beatrix Palt

### 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](mailto:fkhev@fkhev.de)  
Web: [www.fkhev.de](http://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](mailto: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.  
Copyright Mittler Report Verlag GmbH