Militär & Milchkaffee®

Magazin für Verteidigung und Gesellschaft im Wandel

September 2026

Foto: Symbolbild KI / Archiv V.Simon

UAM-InnoRegion-SH

Drohnenregion Schleswig-Holstein

In unserem Bündnis entwickeln über 120 Partner aus Wirtschaft und Wissenschaft zivile Drohnenanwendungen für den Norden und darüber hinaus. Als zentraler Ort für Entwicklung, Erprobung und Wissenstransfer ist das Drohnenkompetenzzentrum am Airpark Leck im Aufbau.

Innovation erleben. Wissen teilen. Kontakte knüpfen.
Bei unseren kostenfreien #Drohnerstagen.

Mehr erfahren: www.uam-innoregion-sh.de

Unsere Bereiche

- Offshore
- Tourismus
- Events- und Veranstaltungs-dienstleistungen
- Medizinische Versorgung
- (Seenot) -Rettung
- Landwirtschaft
- Energie-versorgung
- Umwelt und Nachhaltigkeit
- Akzeptanz-forschung

Gefördert durch:

Bundesministerium für Forschung, Technologie und Raumfahrt

wir! Wandel durch Innovation in der Region

Wirtschaftsförderung Nordfriesland

Foto: Symbolbild, KI / Archiv VSimon

Titel Führung in ihrer Hand. Soldatinnen schärfen den Blick und stärken das Militär S. 6-10

Verteidigung Angehörige im Einsatz: dienen durch Geduld, Liebe und Verzicht S. 12-13

Foto: privat / Daniel Augsten

Drohnen stärken in strukturschwächeren Regionen die Wirtschaft und dienen der Gesellschaft S. 15-21

Foto: Archiv VS / freepik

Kultur Bundeswehr im Film S. 32-35

Foto: Symbolbild, KI / Archiv VSimon

Hinweis zur Verwendung von Künstlicher Intelligenz (KI)

Militär&Milchkaffee verwendet teilweise KI in Bild und Text. Fotos, Montagen und Grafiken sowie Texte, in denen KI zur Anwendung gekommen ist, sind der Kennzeichnungspflicht nach Pressekodex benannt: Symbolbild, KI bzw. KI-gestützt. Alle anderen Inhalte unterliegen dem Urheberrecht der geistigen Schöpfung der Autoren.

... herzlich willkommen!

... zur ersten Ausgabe von Militär & Milchkaffee, das digitale Magazin für Verteidigung und Gesellschaft im Wandel!

Militär & Milchkaffee. Der Name bleibt hängen – und wirft gleich die Fragen auf: Was hat er zu bedeuten und wer soll's lesen? Die Antwort ist schlicht und einfach – Sie alle! Denn Sie alle gehören zu unserer Zielgruppe der geschätzten Leserinnen und Lesern. Verteidigung beschränkt sich nicht nur auf das Militär. Und zur Gesellschaft gehören wir alle.

Der ungewöhnliche Titel ist also Programm: Militär & Milchkaffee steht zum einen für die Bandbreite unterschiedlicher Verteidigungsformen, die nicht nur den Kriegsfall beschreiben. Auch die Entwicklung von beispielsweise Lieferdrohnen für medizinische Produkte in periphere Regionen ist eine Art zu verteidigen, Menschen in ihrer Umgebung zu schützen und zu unterstützen. Zum anderen steht er für eine komplexe, vielfältige Gesellschaft, die über Ländergrenzen und Kulturen hinweg zwar Vieles spaltet, aber auch Vieles eint. Dazu gehört der Wunsch, teilzuhaben – an der digitalen Welt zum Beispiel, die für alle von uns auch dies sein kann: gefährlich.

Zwar wird wird das Wort „Verteidigung" immer noch fast ausschließlich in den militärischen Kontext gesetzt. Das ist jedoch zu kurz gefasst: Die Widerstandsfähigkeit und Abwehrkraft einer Gesellschaft entscheidet sich in Energieversorgung, Krankenhäusern, Unternehmen, Wissenschaft, Kommunen, Medien ebenso wie in jedem einzelnen Haushalt und natürlich in der Armee. Resilienz und Verteidigungsfähigkeit zeigen sich nicht nur im Umgang mit Panzer und Pistole – sondern auch im Umgang mit Desinformation, hybriden Gefahren, Naturkatastrophen, Pandemien, Cyberangriffen und Künstlicher Intelligenz.

Wir richten den Blick hauptsächlich auf den DACH-Raum. Deutschland, Österreich, Schweiz. Wir berichten von Menschen und ihren Erfahrungen, von Innovationen, Technologien und Initiativen, die unsere Gesellschaft resilienter und stabiler machen können. Insbesondere in diesen Zeiten – denen wir am Ende in jedem Magazin in launigen Lesestücken das Gute abgewinnen.

Wir sprechen über militärische Sicherheit und Entwicklungen ebenso wie über Zivilschutz, Bevölkerungsschutz, kritische Infrastrukturen, Wirtschaft, Forschung, Digitalisierung, Krisenfälle und gesellschaftlichen Zusammenhalt. Denn all diese Bereiche sind Teil einer umfassenden Sicherheitskultur.

Militär & Milchkaffee erscheint viermal im Jahr digital – immer Anfang März, Juni, September und Dezember. Unser Format folgt dabei der gleichen Überzeugung, nach der unsere Inhalte ausgewählt werden – es muss sich den Veränderungen anpassen. Deshalb erscheint jede Ausgabe als digitaler Newsletter – schnell und kompakt für den Alltag, fundiert für den zweiten Blick. Militär & Milchkaffee ist sowohl schreibtisch- als auch sofatauglich und bietet ebenfalls unterwegs Kurzweil. Jede Ausgabe ist sorgfältig zusammengestellt, bleibt aber immer Teil der größeren Geschichte: die Transformation unserer Gesellschaft.

Unsere Anzeigen und Links stehen zum einfachen Abruf bereit, so dass Sie mit einem Klick auch unsere Partner kennenlernen können. darüber freuen wir uns! Das Motto: lesen, teilen, reichweitenstarke Partner finden! Sie möchten Militär & Milchkaffee lieber gedruckt in den Händen halten? Nur zu! Drucken auf Eigeninitiative ist erlaubt! Selbstverständlich übernehmen wir auch die Printlegung.

Weil Sicherheit ständiger Veränderung unterliegt und somit eine Herausfordeung ist, hat Militär & Milchkaffee den Anspruch, Qualität zu bieten und trotzdem leicht zu bleiben, denn der Wandel ist nicht grundsätzlich ein Schreckgespenst. Die Herausforderungen unserer Zeit sind vielfältig – und darum muss auch unser Verständnis von Verteidigung der Gesellschaft vielfältiger werden. Wir leben in einer Zeit, in der Sicherheit neu gedacht werden muss.

Willkommen bei Militär & Milchkaffee, dem Magazin für Verteidigung und Gesellschaft im Wandel, an dem Sie übrigens nicht nur als Konsument teilhaben können. Werden Sie Teil unserer Community, unterstützen Sie Militär & Milchkaffee zum Beispiel als Content Pate oder mit einer Anzeige. Womit wir uns an dieser Stelle ganz herzlich bei allen bedanken, die die Geburtsstunde von Militär & Milchkaffee unterstützt und mitgetragen haben.

In diesem Sinne wünschen wir Kurzweil und freuen uns auf ein Wiedersehen im Dezember – sonnige Grüße – Vivian Simon

Schleswig-Holstein, 80.000 Menschen zirka stehen im nördlichsten Bundesland in Katastrophenschutz und Bevölkerungsschutz als Helfer bereit. Diese Einsatzkräfte gliedern sich u.a. Freiwillige Feuerwehren, speziellen Katastrophenschutzeinheiten (DRK, Johanniter, ASB, Maltesern) und THW.

Mecklenburg-Vorpommern, 150 Hektar groß ist der Waldbrand, der im Juli 2026 auf dem ehemaligen Truppenübungsplatz im Müritz-Nationalpark ausgebrochen ist. Die Ortschaft Granzin wurde evakuiert.

Niedersachsen, 2077 Stromausfälle wurden von Januar bis August 2026 auf der Plattform Stromausfall.org registriert.

Hamburg, 600 Lehrgangsteilnehmer, darunter etwa 100 ausländische Offiziere aus 50 Nationen sind an der Führungsakademie der Bundeswehr präsent.

Berlin, 2000 kleinere Störungen werden jährlich in der Hauptstadt verzeichnet. Der bisher längste Stromausfall in der Nachkriegsgeschichte ereignete sich im Januar 2026 nach einem Brandanschlag auf eine Kabelbrücke. Er dauerte vier Tage, betroffen waren 45.000 Haushalte.

NRW, 11.600 ha groß ist der Truppenübungsplatz Senne mit einem Truppenlager für 1000 Soldaten und acht Biwak-Plätzen.

Brandenburg, 32 Lost-Places-Bunker stehen verlassen in Brandenbugrs Wäldern. Ein Teil davon (Russenbunker) kann besichtigt werden.

Hessen, 40.000 Mitarbeiter waren nach einem Hack auf die Landesverwaltung im Mai 2026 betroffen.

Sachsen, 26.000 Ehrenamtliche, die mehr als 20 Std. im Monat arbeiten, werden vom staatlichen Förderprogramm „Wir für Sachsen“ unterstützt.

Bayern, 20.000 Exponate auf 17.000 qm gibt es im Museum für Militär- und Zeitgeschichte in Stammheim-Kolitzheim zu sehen.

Saarland,1500 Soldaten sind im kleinsten Bundesland stationiert.

Baden-Württemberg, 607 Notfalltreffpunkte gibt es in den Kommunen insgesamt.

Kanton Bern, 140.000 Mitglieder insgesamt gehören zur Schweizer Armee, die ihren Hauptsitz in Bern hat.

Kanton Genf, 6-7 Grad kalt ist das Wasser des Genfer Sees, wenn dort regelmäßig Rettungskräfte zum Training antreten.

Kanton Tessin, 140 Kilometer Stromleitungen sollen ab 2035 zurückgebaut werden. Grund: zu viele verschiedenene Trassen machen die Nutzung ineffizient und unsicher.

Tirol, 200 Unternehmer kamen im Mai 2026 auf Einladung der Raiffeisenbank zusammen und lernten die unheimliche Welt des Darknet kennen.

Steiermark, 9 Kasernen-Standorte des Bundesheers stehen in der Steiermark.

Kärnten, 10 Meter hoch ist die größte Drohnen-Indoorhalle Europas mit Standort in Klagenfurt.

Wien, 903 Mio. Fahrgäste transportieren die Wiener Linien jährlich und sind damit ein Schwergewicht der kritschen Infrastruktur.

Grafiken: Flaggen, Umrisskizzen DACH / VSimon, Fotos: VSimon

Fotos: Symbolbild, KL/Archiv/Simon

Soldatinnen schärfen den Blick und stärken das Militär

Die Bundeswehr steht vor einem tiefgreifenden personellen Wandel. Angesichts von Nachwuchssorgen, demografischem Wandel und gestiegenen Anforderungen im Rahmen der globalen Veränderungen kommt der Personalgewinnung eine strategische Bedeutung zu.

Eine bislang nicht ausgeschöpfte, aber zunehmend aktivierte Ressource in diesem Kontext ist das Potenzial von Frauen in der Truppe. Seit der vollständigen Öffnung aller militärischen Laufbahnen im Jahr 2001 hat sich der Anteil weiblicher Soldatinnen kontinuierlich erhöht. Dennoch liegt er mit rund 13 Prozent (ca. 25 000 Soldatinnen) noch deutlich unter dem Durchschnitt vergleichbarer NATO-Staaten. Dabei ist der Beitrag weiblicher Militärs in vielfacher Hinsicht nicht nur ergänzend, sondern transformativ.

Frauen bringen andere Perspektiven, Führungsstile und Problemlösungsstrategien ein. Studien – auch aus der Wirtschaft – zeigen, dass diverse Teams bessere Entscheidungen treffen, resilienter und kreativer agieren. In komplexen, dynamischen Einsatzszenarien, wie sie die Bundeswehr in Auslandseinsätzen oder bei hybriden Bedrohungen bewältigen muss, ist diese Vielfalt von entscheidender Bedeutung.

Dabei darf jedoch das Risiko von geschlechterspezifischen Auseinandersetzungen oder gar missbräuchlichen Übergriffen nicht ignoriert werden, vor allem, weil grenzüberschreitendes Verhalten in hierarchischen Männerstrukturen ein bekanntes Phänomen ist.

Denn mit Frauen an der Spitze oder in Teams verändert sich häufig auch der Führungsstil: Weniger autoritär, stärker kommunikativ und teamorientiert. Diese Ansätze stärken die Kameradschaft, verbessern die psychische Belastbarkeit von Einheiten und sind ein Gegenmodell zu toxischen Führungsbildern, die immer wieder in Skandalen öffentlich werden. Diese Veränderung führt aber auch nicht selten zu Verlustängsten, die in allen Dienstgraden und in verschiedenen Ausprägungen auftreten können.

Die Bundeswehr plant, den Anteil weiblicher Soldatinnen auf bis zu 20 Prozent zu steigern. Dies ist eine politische Zielmarke und eine logische Konsequenz, wenn man bedenkt, dass Frauen über 50 Prozent der Bevölkerung ausmachen.

Während junge Männer als Zielgruppe für militärischen Dienst zahlenmäßig schrumpfen, wächst der Handlungsdruck, auch weibliche Talente systematisch anzusprechen. Ohne Frauen ist ein personeller Aufwuchs auf 203.000 aktive Soldaten kaum realistisch erreichbar und eine indeutige Antwort auf demografische Engpässe.

Frauen sind insbesondere in technischen, medizinischen und cyberbezogenen Verwendungen stark vertreten. Gerade in Bereichen wie dem Cyber- und Informationsraum (CIR) oder der Sanität leisten sie überproportional viel. Diese Sektoren sind für die Zukunft der Bundeswehr entscheidend, da hier auch die größten Fähigkeitslücken liegen.

Es kristallisiert die gesellschaftliche Verankerung und Vorbildfunktion heraus: eine Wehr, die sich als „Parlamentsarmee“ versteht, muss die Gesellschaft widerspiegeln. Frauen in Uniform stärken die gesellschaftliche Akzeptanz der Streitkräfte – sie machen deutlich, dass Wehrhaftigkeit kein rein männliches Prinzip ist.

Weibliche Vorbilder, sei es in der Offizierslaufbahn oder in der Truppenpraxis, ermutigen junge Frauen eher zur Bewerbung als wenn weibliche Bundeswehrangehörige in ihrem Dienst unsichtbar bleiben. Mit Sichtbarkeit verändern Frauen langfristig auch das Bild von Wehrdienst und soldatischer Professionalität in der Öffentlichkeit.

Verteidigung ist als gesamtgesellschaftliche Aufgabe zu verstehen. Insbesondere in der aktuellen sicherheitspolitischen Lage – hybride Bedrohungen, territoriale Verteidigung – wird deutlich, dass Landesverteidigung nicht mehr nur Männersache ist. Frauen sind ebenso bereit und fähig, Verantwortung zu übernehmen, wenn Strukturen, Karrierechancen und Vereinbarkeit mit Gesundheit und Privatleben stimmen.

Ein positiver Personalumbruch durch mehr Frauen setzt darum voraus, dass eine verbesserte Vereinbarkeit von Dienst und Familie geschaffen wird, mehr weibliche Mentoren in Führungspositionen agieren und gegen Sexismus, Diskriminierung und überholte Traditionsbilder sensibilisiert wird.

Franz Josef Strauß, ehemaliger Ministerpräsident von Bayern, Verteidigungsminister und CSU-Urgestein, setzte in den 1950er-/60er-Jahren mit einem hoch umstrittenen Meinungsbild seine gegensätzliche Ansicht zum Rollenverständnis ins Rampenlicht: „Ein Panzer ist kein Damenfahrrad.“ Die Aussage steht sinnbildlich für die historisch konservative Haltung gegenüber Frauen im Militärdienst in der Bundesrepublik. Lange Zeit wurde der Dienst an der Waffe als unvereinbar mit „weiblicher Natur“ oder gesellschaftlicher Rolle gesehen.

Erst 2001 wurden infolge eines Urteils des Europäischen Gerichtshofs alle militärischen Laufbahnen für Frauen geöffnet – also auch der Dienst in Kampftruppen.

Ein anderes, inzwischen in weiten Teilen der Bevölkerung positiv konnotiertes Zitat stammt von der früheren Verteidigungsministerin Ursula von der Leyen, jetzige Präsidentin der Europäischen Kommission. Sie war von 2013 bis 2019 Chefin der Streitkräfte und war eindeutig: „Frauen gehören in alle Bereiche der Bundeswehr – auch mit Helm und Waffe.“

Diese Meinung bringt die politische und gesellschaftliche Haltung der letzten Jahre zum Ausdruck: Frauen sind nicht nur willkommen, sondern essenziell für die Einsatzbereitschaft einer modernen Armee.

Die jetzige Wehrpflichtdebatte betrifft also beide Geschlechter. In der Diskussion um eine mögliche Rückkehr zur Wehrpflicht, die nicht abgeschafft, sondern ausgesetzt worden ist, oder einer allgemeinen Dienstpflicht wird zunehmend deutlich, dass Geschlechtergerechtigkeit zentral ist. Frauen sind keine militärische Ausnahme mehr – sie sind Teil der Lösung.

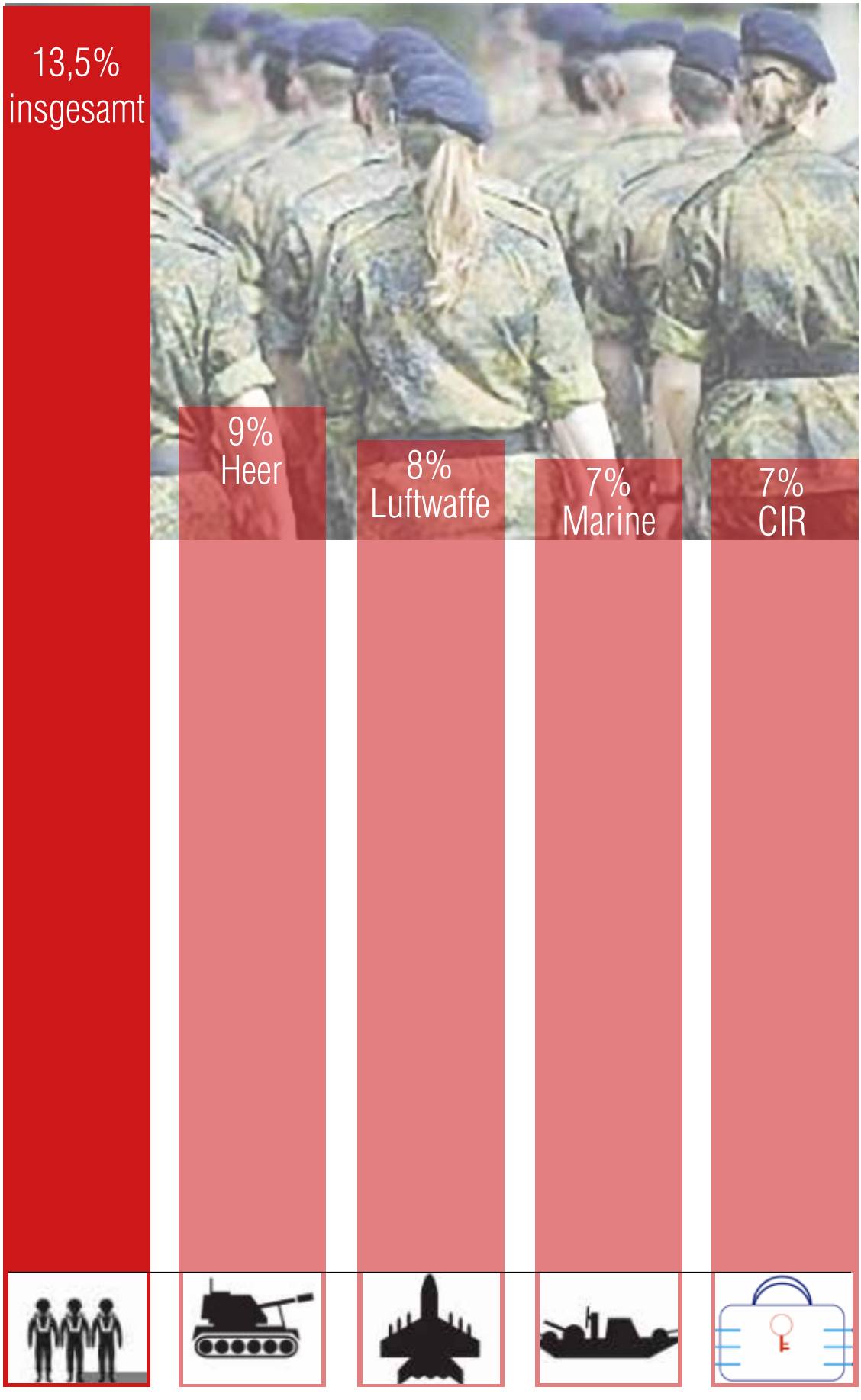
Frauen gelten als Schlüssel für eine moderne, einsatzbereite Bundeswehr. Frauen in der Bundeswehr sind mehr als ein Symbol gesellschaftlicher Gleichberechtigung. Sie sind strategisch unverzichtbar. Sie stärken die Truppe nicht nur personell, sondern auch strukturell und kulturell. Eine Bundeswehr, die auf weibliches Potenzial setzt, ist breiter aufgestellt, resilienter und glaubwürdiger. Der Personalumbruch, der bevorsteht, ist ohne Frauen nicht zu schaffen – und mit ihnen deutlich besser zu bewälti-

Das umstrittene Zitat

„Ein Panzer ist kein Damenfahrrad.“

Franz Josef Strauß (1915-1988).Der CSU-Politiker war Ministerpräsident von Bayern und Bundesminister für besondere Aufgaben, für Atomfragen und der Verteidigung.

Frauenanteil in den Streitkräften der Bundeswehr



Quelle: Bw, Stand 2026

gen. Der Blick nach vorn zeigt: Die Bundeswehr wird weiblicher, und das ist nicht nur ein Schritt in Richtung Gleichberechtigung, sondern ein entscheidender Fortschritt für die Verteidigungsfähigkeit Deutschlands.

Jedoch liegt der Anteil weiblicher Führungskräfte in der Bundeswehr deutlich unter dem Niveau der freien Wirtschaft. In der Bundeswehr liegt der Frauenanteil unter Offizieren insgesamt bei zirka zehn bis 13 Prozent, mit sinkendem Anteil je höher der Dienstgrad. Nur ein sehr kleiner Teil der Generäle oder Admiräle ist weiblich – aktuell sind es unter fünf Prozent. In der freien Wirtschaft ist der Frauenanteil in Führungspositionen ebenfalls ausbaufähig, jedoch signifikant höher – insbesondere im mittleren Management. Die Bundeswehr hinkt besonders bei der Entwicklung weiblicher Führungskarrieren hinterher – unter anderem wegen längerer Laufbahnzeiten, struktureller Hindernisse wie zum Beispiel der Vereinbarkeit mit Familie oder auch Standortwechsel und einer nach wie vor männlich geprägten Führungskultur.

Frauen sind in der Bundeswehr in Führungspositionen also deutlich unterrepräsentiert – nicht nur im Vergleich zur Wirtschaft, sondern auch zum restlichen öffentlichen Dienst. Will die Bundeswehr ihr Ziel eines höheren Frauenanteils erreichen, muss sie nicht nur stärker rekrutieren, sondern auch gezielt Führungskarrieren für Frauen fördern – durch Mentoring, flexiblere Dienstgestaltung und kulturellen Wandel.

Insbesondere der Aspekt des kulturellen Wandels lenkt den Blick auf ein Thema, über das niemand gern spricht, erst recht nicht in Kreisen verantwortlicher und führender Dienstgrade: sexuelle Übergriffe. Sie sind – gleichsam wie das Posttraumatische Belastungssyndrom (PTBS) – weitgehend ein Tabu.

Sexuelle Übergriffe in der Bundeswehr sind kein neues Phänomen, jedoch gewinnen sie zunehmend an öffentlicher Aufmerksamkeit – nicht zuletzt durch medial aufgearbeitete Einzelfälle und interne Berichte. Besonders in angespannten Situationen, wie sie der militärische Alltag mit sich bringt, scheint die Gefahr für grenzüberschreitendes Verhalten erhöht zu sein. Die Erörterung dieses Themas verlangt differenzierte Betrachtung: Was begünstigt sexuelle Übergriffe im militärischen Kontext? Welche Rolle spielen Stress, Hierarchie und Kameradschaft? Und wie kann die Bundeswehr strukturell und kulturell gegensteuern?

Es braucht eine Ursachenanalyse: Warum kommt es zu sexuellen Übergriffen?

Die Bundeswehr ist eine Organisation mit klaren Befehlsketten und Abhängigkeitsverhältnissen. Diese Asymmetrie – etwa zwischen Vorgesetzten und Untergebenen – kann ausgenutzt werden. Insbesondere in Kombination mit geschlossenen Gruppen, mangelnder Kontrolle und fehlendem Vertrauen in Beschwerdemechanismen entsteht ein Nährboden für Machtmissbrauch, einschließlich sexualisierter Gewalt.

Anfälliger Kosmos für Missbrauch

Ein **Nährboden** für Machtmissbrauch, einschließlich sexualisierter Gewalt: Stress reduziert Empathie, soziale Kontrolle und Hemmschwellen – das gilt allgemeinpsychologisch und ist im militärischen Kosmos besonders virulent.

Militärische Ausbildung, Einsätze und Übungen sind oft von psychischer und physischer Überforderung geprägt. Stress reduziert Empathie, soziale Kontrolle und Hemmschwellen – das gilt allgemeinpsychologisch und ist im militärischen Kosmos besonders virulent. Dort kommt es eher zu Grenzüberschreitungen. Sei es aus Frust, gruppendynamischem Druck oder Machtdemonstration. In manchen Einheiten existieren noch immer traditionelle Männlichkeitsbilder, die Frauen als „Fremdkörper“ abwerten oder sexualisieren. In Kombination mit Alkohol, Lagerkoller oder „Kasernenhumor“ können daraus Übergriffigkeiten entstehen – verbal oder auch körperlich. Besondere Dynamiken können sich in Stresssituationen entwickeln. Bei Isolierung und Gruppenzwang in Auslandseinsätzen oder Manövern sind Soldaten und Soldatinnen oft über Wochen von zivilen Kontrollinstanzen isoliert. Die entstehende „Kampfgemeinschaft“ kann Loyalität über Moral stellen, und Übergriffe werden aus Gruppendruck nicht gemeldet oder gar gedeckt. Opfer sexueller Gewalt oder Belästigung in solchen Lagen haben oft keine Möglichkeit, sich zu wehren. Angst vor Rufschädigung, Karrierenachteilen oder der Vorwurf, das „Team zu gefährden“, verhindert, dass Vorfälle gemeldet werden – erst recht dann, wenn der Täter übergeordnet ist.

In Stresssituationen wird oft einfach „weiter funktioniert“. Es fehlen Zeit und Gelegenheit für Gespräche, Reflexion und psychologische Betreuung. Erlebte Übergriffe bleiben unbearbeitet und wirken lange nach, mit Auswirkungen auf das Vertrauen in Kameradschaft und Organisation und können in PTBS enden.

Die Bundeswehr hat – wie alle Armeen – mit Herausforderungen zu tun und ist tätig: Interne Richtlinien gegen Übergriffe sind auf den Weg gebracht, Programme zur Sensibilisierung erarbeitet, Vertrauenspersonen eingesetzt. Die strukturellen Reformen umfassen eine stärkere Rolle der Militärseelsorge und psychosozialen Dienste, einfache Meldewege (anonym, digital, ohne Dienstwegzwang) sowie externe Kontrollen von Vorfällen und Disziplinarverfahren zur Vermeidung von Intransparenz. Die Verantwortung liegt bei der Organisation und ist zwar Chefsache – aber Vertrauen und Diskretion müssen ebenso wie der Wille zur Ausbildung in soziale Kompetenz und in der klaren Haltung, dass Kameradschaft niemals Übergriffe duldet, von allen getragen werden. So wird aus dynamischen und herausfordernden Zeiten für die Bundeswehr auch ein ethischer Aufbruch.

— Text: Wilko Karl

Richtlinien gegen Übergriffe

Strukturelle Reformen umfassen mehr Militärseelsorge und psychosozialer Dienste, niedrigschwellige Meldewege (anonym, digital, ohne Dienstwegzwang) sowie externe Kontrollen von Vorfällen und Disziplinarverfahren.

Foto: Symbolbild, KI / Archiv VSimon

ISBN 9783940723529
284 Seiten, 17,80 EUR

Ob als Sportschütze oder Sammler, als Mitarbeiter im Bewachungsgewerbe oder Bootsführer - für die Erlaubnis, eine Schusswaffe zu erwerben oder zu führen, ist der Nachweis der Sachkunde erforderlich. Das bewährte Lehrbuch zur Vorbereitung auf die Waffensachkundeprüfung bereitet optimal auf Lehrgang und Prüfung vor. Neben der Einführung in die gesetzlichen Regelungen enthält es eine breite Darstellung der Waffen- und Munitionstechnik und der Ballistik. Ein Leitfaden für Waffenbesitzer vor und nach der Waffensachkundeprüfung!

ISBN 9783963940248
600 Seiten, 68,00 EUR

Diese Praxiskommentierung bietet eine breit angelegte Einführung in die zentralen Themen des Waffenrechts für Verwaltung, Waffenbesitzer, Unternehmer in Handel und Herstellung, Verantwortliche in Vereinen und im Jagdwesen sowie für Polizei und Justiz. Die Darstellung der wesentlichen Vorschriften des aktuellen Waffengesetzes (WaffG) wird ergänzt um Erläuterungen zu relevanten Regelungen des Beschussgesetzes (BeschG) und des Gesetzes über die Kontrolle von Kriegswaffen (KrWaffKontrG).

ISBN 9783940723666
160 Seiten, 34,80 EUR

Cyberattacken, hybride Gefahren. Menschliche Kompetenz vs. Künstliche Intelligenz. Auswirkungen von Cyberpsychologie. Fake News und Unsicherheiten in einer geopolitisch fragilen Lage samt der Auswirkungen auf Individuen. Welche Maßnahmen für Cybersicherheit greifen nachhaltig? Wo sind Führungskräfte in der Verantowrtung? Reicht „Awareness" noch aus? In diesem Buch zeigen die Autoren Simon und Busche die Herausforderungen auf, die insbesondere von Entscheidern gemeistert werden müssen.

§ Aktuelle Neuerscheinung §

Dieses Handbuch bietet Jägerinnen und Jägern eine Einführung in die wichtigsten Themenbereiche des Waffenrechts und der Waffenkunde sowie der Munitionskunde. Besondere Schwerpunkte sind neben den Regelungen zu Nachtsichttechnik und Schalldämpfern die Aufbewahrung und der Transport von Waffen und Munition. Hinweise zum Umgang mit Messern, zum richtigen Verhalten nach einem Wildunfall sowie zu Leihe und Verwahrung von Schusswaffen runden das Informationsangebot dieses praktischen Ratgebers ab. Insbesondere für Jäger bedeutsame Verschärfungen des Waffenrechts im Oktober 2024 wurden im Rahmen der dargestellten Themen berücksichtigt. Ein Buch für alle Inhaber jagdrechtlicher Erlaubnisse, ob Anfänger oder alter Hase - und auch zur Vorbreitung auf die Jägerprüfung ein verlässlicher Begleiter in der Ausbildung.

10. Auflage, 348 Seiten, 39,80 EUR
ISBN 9783963944062

Der Juristische Fachverlag Busche bietet mit seinen Publikationen spezialisierte Literatur für die Vorbereitung auf gesetzlich vorgesehene Prüfungen, insbesondere zur Waffensachkunde und Fachkunde für den Handel mit Schusswaffen, sowie zur Vorbereitung auf die Jägerprüfung oder die Sachkundeprüfung für Unternehmer und Beschäftigte im Bewachungsgewerbe.
Mehr Informationen zum Verlagsangebot unter www.juristischer-fachverlag.de

Foto: Daniel Augsten / privat

Angehörige im Einsatz: dienen durch Geduld, Liebe und Verzicht

„Schatz, ich bin dann mal 6 Monate in Afghanistan, bis über Weihnachten.

Ach so … und vorher noch 4 Monate Einsatzvorbereitung - Lehrgänge, Übungsplätze, Spezialausbildungen, Tagungen, Erkundung vor Ort.“

Das hier zu schreiben, fällt mir ehrlich nicht leicht, denn exakt diese Worte habe ich Anfang Mai 2016 zu meiner Frau gesagt und dann war ich +10 Monate lang weg.

Über Veteranen haben wir am 2. Nationalen Veteranentag im Juni 2026 (endlich) häufiger gesprochen. Über Soldaten, ihre Einsätze, die Verantwor-

tung und deren Folgen für Körper und Geist. Aber viel zu selten über die Menschen, die zu Hause geblieben sind. Über die Partnerinnen und Partner, die monatelang allein den Alltag stemmen. Über die Eltern, die nachts vor Sorgen wach liegen. Genauso die Freunde, die den Kontakt halten und Briefe und Pakete schicken.

So wie die eigenen Kinder, die jeden Tag hoffen, dass Papa bald wieder da ist und am Telefon weinen, weil Papa fehlt.

Ich war über Weihnachten und Silvester 2016 im Einsatz. Während andere gemeinsam am Tisch saßen, besinnlich Geschenke auspackten und auf das neue Jahr anstießen, saßen wir tausende Kilometer entfernt in Afghanistan.

Und ganz ehrlich:

Das ist für die Soldatinnen und Soldaten sehr schwer. Aber für die Familien zu Hause mindestens genauso, denn niemand geht allein in den Einsatz.

Jeder Einsatz wird von Menschen mitgetragen, die keine Uniform tragen. Jene die warten, verzichten und stark bleiben, damit sie die Sorgen aushalten.

Ich habe Kameraden erlebt, die mitten im Einsatz einen Anruf bekamen: „Ich kann das nicht mehr! Ich schaffe es nicht! Ich will die Scheidung!“

Sätze, die einen Menschen bis ins Mark erschüttern. In solchen Momenten entscheidet sich übrigens, ob man Führungskraft oder Vorgesetzter ist, Kamerad oder Befehlsgeber, Vorbild oder Beispiel.

Uns es gab dort etwas, worüber kaum jemand spricht. Viele meiner Kameraden – mich eingeschlossen – haben ihre Partnerinnen im Einsatz bewusst angelogen.

Ausschlaggebend war die deutsche Festnetznummer, über die uns unsere Familien in einigen Containern erreichen konnten.

Bevor wir zu einem Auftrag außerhalb des Lagers aufbrachen, galt oft eine unausgesprochene Abmachung untereinander: „Wenn meine Frau anruft, sag bitte, ich bin in einer Besprechung, beim Sport, beim Essen oder beim Sani – egal – denk dir irgendetwas aus – aber sag ihr auf keinen Fall, dass ich gerade draußen unterwegs bin.“

Es war eine Lüge aus Liebe.

Wir wollten verhindern, dass unsere Angehörigen sich bei jedem Auftrag stundenlang vor Angst verzehren. Denn nach Anschlägen wurden häufig sämtliche Kommunikationsverbindungen in das Einsatzland – auch Mobilfunk – vorübergehend gesperrt. Dann begann für die Menschen zu Hause das bange Warten. Minuten wurden zu Stunden, Stunden zu einer gefühlten Ewigkeit. Die quälende Frage blieb dieselbe: Ist er unverletzt – oder hat es ihn getroffen?

Diese Ohnmacht auszuhalten, ohne etwas tun zu können, war eine Belastung, die nur diejenigen wirklich verstehen, die sie selbst erlebt haben.

Daher musste ich etwas tun, das ich zutiefst verabscheue: Ich musste meine Partnerin über Monate hinweg belügen. Es waren Lügen aus Liebe und aus dem Wunsch heraus, ihr unnötige Angst zu ersparen. Die Wahrheit über das, was ich erlebt und gefühlt hatte, konnte ich ihr erst sagen, als ich wieder sicher zu Hause war und wir gemeinsam auf unserem Balkon saßen.

Was man im Einsatz erlebt, endet nicht mit dem Rückflug nach Deutschland.

Denn wenn das Fundament zu Hause nicht mehr trägt, dann tragen viele ihre Last noch lange nach der Rückkehr weiter.

Deshalb gilt mein Dank am Veteranentag 2026 nicht nur den Veteraninnen und Veteranen, sondern vor allem auch den Familien, den Freunden, den Partnern und Kindern. Ich verneige mich in tiefer Dankbarkeit vor ihnen und allen, die im Hintergrund mittragen, was nach außen oft niemand sieht.

Manche dienen in Uniform.

Andere dienen durch Liebe, Geduld und Verzicht.

Beide verdienen in der Umsetzung eines demokratischen, parlamentarischen Willens unseren Respekt.

— Text: Daniel Augsten,
Personal- und Organisationsentwickler

Foto: Symbolbild, KI / Archiv VSimon

Foto: Bundeswehr / PR Jagel

„Immelmänner“ und die Drohne German Heron TP in Jagel

Ich stehe neben einem Drohnenpiloten, der einer der „Immelmänner“ auf dem NATO-Flugplatz Schleswig-Jagel in Schleswig-Holstein ist. Der Pilot, den ich „Wilko“ nennen darf, heißt im echten Leben anders. Sein Klarname muss aus Sicherheitsgründen geheim bleiben.

Jagel ist der Standort für die Ausbildung von Tornado-Piloten. Bei den „Immelmännern“ – das Taktische Luftwaffengeschwader „Immelmann 51“ gab dem Fliegerhorst seinen Namen – liegt der Hauptstützpunkt der deutschen Luftwaffe für die mittelschwere Aufklärungs- und Überwachungsdrohne German Heron TP. Ihre Hauptaufgabe ist neben der Aufklärung die Unterstützung von Soldaten eigener und befreundeter Streitkräfte. Die Drohne kann zum Beispiel Konvois begleiten, um Gefahren frühzeitig zu erkennen und Bodentruppen in Echtzeit zu alarmieren oder auch vor herannahenden Piraten auf See zu warnen. German Heron TP kann je nach Konfiguration bis zu 27 Stunden in der Luft bleiben.

Die Maße der Drohne, insbesondere ihre Spannweite, wirken für ganz normale Besucher wie mich fast erschlagend. Ich habe lediglich den „kleinen“ Drohnenführerschein A, Spielzeugformat, Spannweite: etwa eine Handbreit. Hier stehen wir nun vor fast 30 Metern Spannweite, 14 Metern Länge und einer Höhe von 3,30 Meter. Dienstgipfelhöhe: ca. 12 500 Meter. Das ist beeindruckend, mindestens. Wilko sagt, es macht Spaß, diese Drohne zu fliegen und ich glaube im das sofort.

Möglich wurde der Besuch durch die Wirtschaftsförderung Nordfriesland, die sich über ihre Grenzen hinaus einen „Drohnerstag“-Namen gemacht hat.

Das Projekt „UAM-InnoRegion-SH“ ist ein vom Bundesministerium für Forschung, Technologie und Raumfahrt gefördertes Verbundprojekt mit dem Ziel, im nördlichen Schleswig-Holstein Innovationen im Bereich der unbemannten Luftfahrt (Unmanned Air Mobility) anzuschieben und zu verankern. Durch neuartige Forschungsprojekte sollen im Fördergebiet qualifizierte Arbeitsplätze entstehen, um langfristig zum Strukturwandel beizutragen. Die Region für das Innovationsthema zieht sich entlang der deutsch-dänischen Grenze bis an die Ostseeküste. Sie ist von vielen kleineren und mittleren Unternehmen geprägt.

Weitere Besichtigungs-Infos und Events unter www.wfg-nf.de


Foto: VSimon

Das Geschäft mit Drohnen erfordert Präszion, Vision und Innovation

„Meine Pferde drehen durch, wenn über ihnen eine Drohne zu nahe kommt", sagt der Mann, während er selbst das kleineste Modell mit Führerschein A-Lizenz konzentriert über seine Felder fliegen lässt.

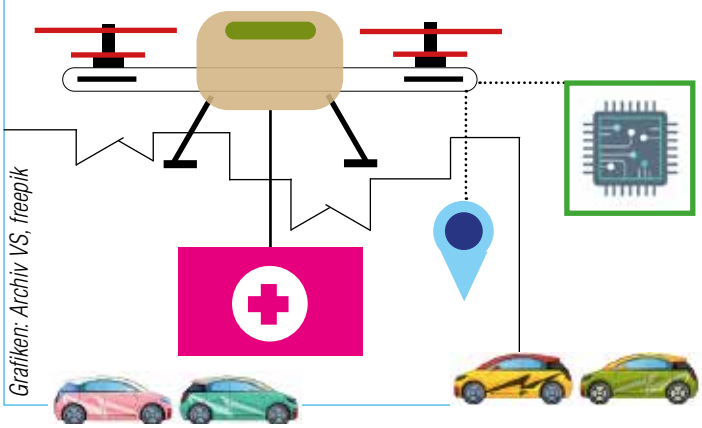
Das drohende Surren, das seit Jahren die Gemüter streiten lässt, im Verteidigungssektor immer mehr an Bedeutung gewinnt und in strukturarmen Regionen die Versorgung der Bevölkerung sicherstellen soll, hat Geschichte, die weiter zurückreicht, als viele Menschen vermuten.

Was heute als kompaktes Hightech-Gadget für Luftaufnahmen bekannt ist, begann als experimentelle Militärtechnologie im 19. Jahrhundert – die frühen Anfänge. Schon vor der Erfindung des Motorflugs gab es Versuche mit unbemannten Objekten. 1849 setzt die österreichische Armee unbemannte, mit Sprengstoff beladene Heißluftballons gegen Venedig ein. Erste Versuche, Kameras an Drachen oder Tauben zu befestigen, legten den Grundstein für die heutige Aufklärungstechnologie. Weltkriege gelten als Geburtsmarkant der modernen Drohne. Mit der Entwicklung des Funks im frühen 20. Jahrhundert wurden erste ferngesteuerte Flugzeuge möglich. Im Ersten Weltkrieg entwickelten Großbritannien und die USA Geräte wie das Aerial Target (1917) und den Kettering Bug (1918), einen frühen Vorläufer des Marschflugkörpers. 1935 dann die „DH.82B Queen Bee": Das britische Zielflugzeug gilt als die erste moderne Drohne, die in Serie produziert wurde. Ihr Name (übersetzt „Bienenkönigin") prägte vermutlich den Begriff „Drohne" (männliche Biene) für unbemannte Fluggeräte.

Während des Kalten Krieges verlagerte sich der Fokus auf Überwachung. Im Vietnamkrieg wurden Drohnen massiv zur Aufklärung eingesetzt, um bemannte Flüge über feindlichem Gebiet zu vermeiden. Der in Israel aufgewachsene Ingenieur Abraham Karem gilt als „Vater der modernen Drohne".

Er entwickelte in den 1970er- und 80er-Jahren Technologien, die zur berühmten „Predator-Drohne" führten.

Der Übergang vom reinen Militärgerät zum Alltagsgegenstand geschah durch technische Miniaturisierung und GPS.2013 – DJI Phantom: Die Einfüh-



Grafiken: Archiv VS, freepik

Lieferdrohnen sind unbemannte Luftfahrzeuge (Logistikdrohnen), die Pakete autonom oder ferngesteuert über kurze bis mittlere Distanzen transportieren, um Lieferservices zu beschleunigen oder entlegene Gebiete zu versorgen. Projekte wie in Welzow testen die Zustellung von Zeitungen, während Firmen wie Amazon (Prime Air) Kleinstwaren in 30 Minuten liefern. Die Systeme bieten hohe Reichweiten bis 50 km und Nutzlasten von 2 kg bis 100 kg.

rung der DJI Phantom markierte den Beginn der weltweiten Popularität von Consumer-Drohnen.

Drohnen finden heute Einsatz in der Landwirtschaft, zur Paketauslieferung, in der Filmindustrie und bei Rettungseinsätzen.

In England haben Drohnenlieferungen im Jahr 2026 einen entscheidenden Wendepunkt erreicht: von experimentellen Pilotprojekten hin zum regulären kommerziellen Betrieb. Während entlegene Gebiete bereits seit längerem versorgt werden, steht der flächendeckende Einsatz in städtischen Gebieten unmittelbar bevor.

Nach jahrelanger Vorbereitung hat Amazon Anfang 2026 offizielle Testflüge von seinem Logistikzentrum in Darlington (Nordengland) gestartet. Der offizielle kommerzielle Start für Kunden ist für Ende 2026 geplant. Zum Einsatz kommt die neue MK30-Drohne, die deutlich leiser ist als herkömmliche Modelle und über fortschrittliche „Sicht- und Ausweichsysteme“ verfügt, um Hindernisse wie Wäscheleinen oder Haustiere autonom zu erkennen.

Einen Vorgeschmack über die Leistungsfähigkeit der Drohne wurde bereits Ende 2025 von der UAM-Inno-Region und Wirtschaftsförderung Nordfriesland vorgestellt.

Kunden sollen ihre Pakete demnach bis zu einem Gewicht von 2,27 kg (fünf Pfund) innerhalb von weniger als zwei Stunden erhalten.

Die britische Post (Royal Mail) betreibt bereits dauerhafte Routen, vor allem, um logistische Lücken in schwierigem Gelände zu schließen. Das Projekt „I-Port“ (Orkney-Inseln) wurde aufgrund seines Erfolgs bis verlängert. Hier befördern elektrische Drohnen Post zwischen den Inseln (beispielsweise nach Graemsay und Hoy), die dann von Postboten zu Fuß oder per Elektro-Van zugestellt wird. Vorteil: Die Zustellzeit in diesen Regionen konnte um bis zu 24 Stunden verkürzt werden, da die Drohnen weitgehend unabhängig von Fähren und Wetterbedingungen operieren können.

Ein zentraler Baustein für den Erfolg ist der „Drone Superhighway“ (Skyway), ein über 260 km langer Korridor, der Städte wie Reading, Coventry und Cambridge verbindet.

Aber in Großbritannien gelten verschärfte Vorschriften, darunter die Pflicht für grüne Blinklichter bei Nachtflügen sowie erweiterte Registrierungs- und Fernidentifizierungspflichten (Remote ID) für alle Betreiber.

Experten prognostizierten, dass 2026 das Jahr ist, in dem die „Last-Mile-Delivery“ in britischen Städten durch streng regulierte Korridore zum Standard wird.

Der nationale Gesundheitsdienst (NHS) nutzt Drohnen verstärkt für den Transport von Blutproben, Medikamenten und Chemotherapeutika zwischen Krankenhäusern. Dies spart nicht nur Zeit im Notfall, sondern reduziert die CO^2-Emissionen im Vergleich zu Straßentransporten erheblich.

In der Schweiz hat sich der Einsatz von Versor-

DH.82B Queen Bee

Das **britische Zielflugzeug** gilt als die erste moderne Drohne, die in Serie produziert wurde. Ihr Name (übersetzt „Bienenkönigin“) prägte vermutlich den Begriff „Drohne“ (männliche Biene) für unbemannte Fluggeräte.

Foto: Symbolbild, KI / Archiv VSimon

Die Schweiz ist Testlabor für Europa

Das Bundesamt für Zivilluftfahrt (BAZL) hat **fortschrittliche Regeln** für Flüge außerhalb der Sichtweite etabliert. Zum Standard gehören Fallschirmsysteme und autonome Ausweichtechnik, um Unfälle über bewohntem Gebiet zu vermeiden.

gungsdrohnen in den letzten Jahren tatsächlich von Pionierprojekten der Post hin zu spezialisierten, kommerziellen Dienstleistungen entwickelt. Während die breite Paketlieferung noch aussteht, ist die Schweiz im medizinischen Bereich weltweit führend.

Der Fokus liegt fast ausschließlich auf dem Transport zeitkritischer Güter wie Blutproben, Gewebeanalysen und Medikamenten zwischen Spitälern und Laboren. Die weltweit längste urbane Drohnenroute verbindet die Stadtspitäler Triemli und Waid. Die Flugzeit beträgt nur etwa sieben Minuten, was deutlich schneller und zuverlässiger ist als der Transport per Autokurier durch den städtischen Verkehr.

Nachdem sich die Schweizerische Post 2023 aus Rentabilitätsgründen aus dem operativen Geschäft zurückgezogen hat, übernahm der US-Partner Matternet den Betrieb vieler Routen direkt. Auch das Schweizer Start-up RigiTech ist in diesem Bereich stark aktiv und bietet Lösungen für Distanzen bis zu 100 Kilometer an.

Die Schweizerische Post hat ihre Rolle gewandelt: Sie agiert nicht mehr als Drohnenbetreiber, sondern konzentriert sich auf die Integration der Technologie in ihre digitale Logistikkette. Im Jahr 2026 liegt das Augenmerk der Post verstärkt auf der digitalen Grundversorgung. Drohnen werden als Ergänzung gesehen, die „On-Demand“ zur Verfügung stehen, um traditionelle Kuriere in Spezialfällen zu entlasten.

Die Schweiz gilt als „Testlabor“ für Europa, da das Bundesamt für Zivilluftfahrt (BAZL) schon früh fortschrittliche Regeln für Flüge außerhalb der Sichtweite (BVLOS) etabliert hat. Zum Standard gehören Fallschirmsysteme und autonome Ausweichtechnik, um Unfälle über bewohntem Gebiet zu vermeiden.

Trotz der Fortschritte ist das Fliegen in der Nähe von Flughäfen, Gefängnissen oder Naturschutzgebieten weiterhin streng reglementiert oder verboten.

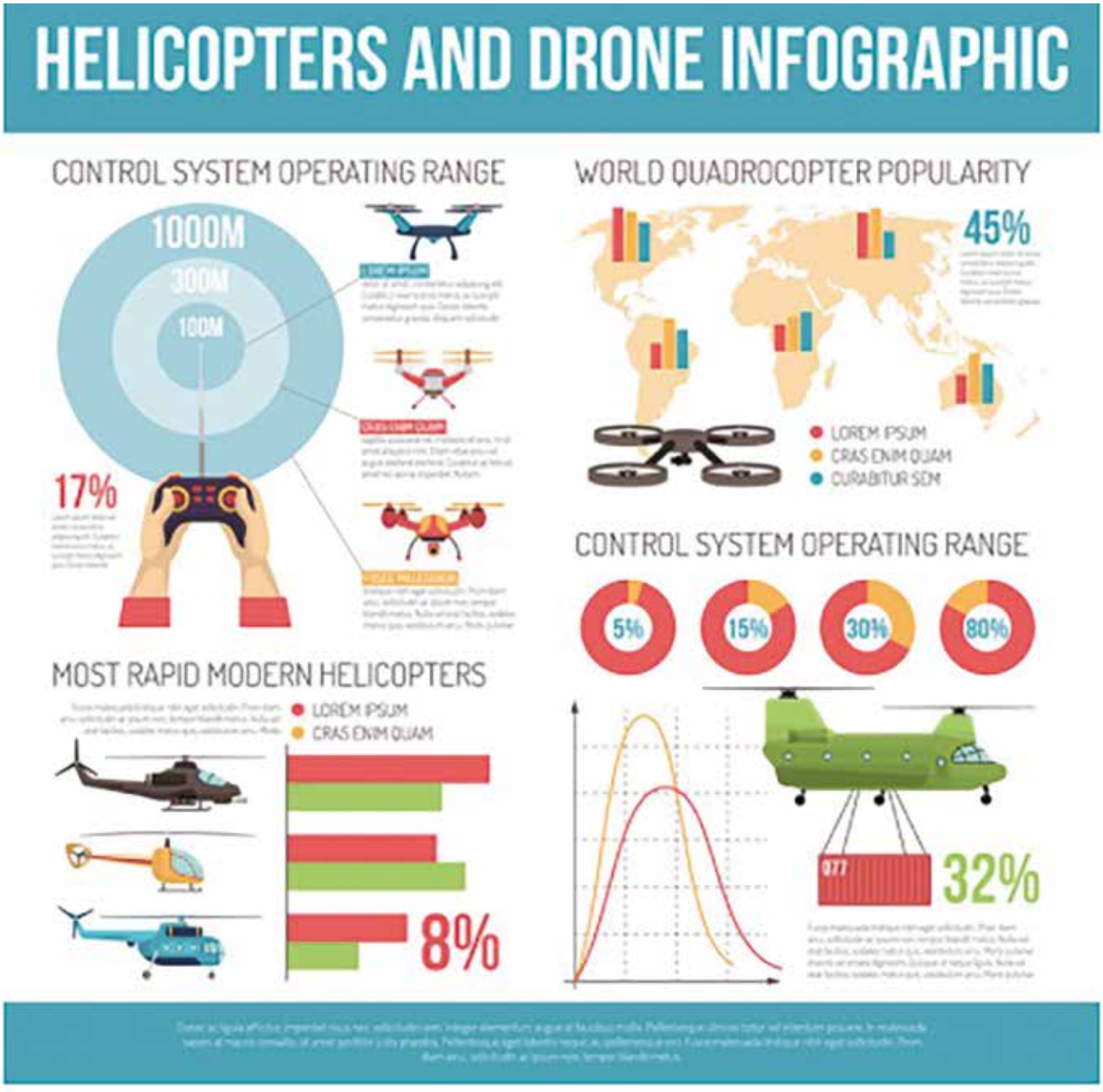
Die Schweizer Armee verstärkt 2026 ihre Bemühungen zur Drohnenabwehr und -erprobung (Taskforce Drohnen), was indirekt auch die technologische Basis für zivile Versorgungsdrohnen stärkt.

Zukunftsausblick: Während in Deutschland 2026 erste „Pallidrohnen" Medikamente bis an die Haustür liefern, bleibt die Schweiz vorerst bei der B2B-Logistik (Spital zu Labor), prüft aber ständig neue Anwendungsfelder in der Hochgebirgsversorgung.

Auch Österreich hat sich in puncto Drohnen und Versorgung der Bevölkerung zunächst auf den medizinischen Sektor und die Bergrettung konzentriert, während kommerzielle Paketlieferungen an Privatpersonen noch in der Pilotphase stecken.

Österreich hat ein spezialisiertes Logistik-Netzwerk („Medical Drone Service") für den Transport kritischer medizinischer Güter aufgebaut, um den bodengebundenen Verkehr zu umgehen. Der Transport von Blutkonserven, Laborproben, Medikamenten und medizinischer Ausrüstung steht dabei im Vordergrund. Die ÖAMTC-Flugrettung kooperiert hierbei mit dem niederösterreichischen Start-up Apeleon und regionalen Gesundheitsagenturen.

Zum Einsatz kommen elektrisch betriebene Drohnen, die wie Hubschrauber senkrecht starten und wie Flugzeuge horizontal fliegen können und eine Nutzlast von bis zu zehn Kilogramm schaffen. Da in den alpinen Regionen Drohnen ein essenzieller Bestandteil der Versorgung von Verunfallten in unwegsamem Gelände sind, geht es in erster Linie um die schnelle Erstversorgung: Drohnen bringen Erstversorgungskits oder Defibrillatoren direkt zum Unfallort, noch bevor Rettungsteams zu Fuß oder per Hubschrauber eintreffen können. Drohnen un-



Grafik: Symbolbild, KI / Archiv Medienpool

Foto: freepik

terstützen bei der Lagebeurteilung, dem Ausleuchten von Einsatzorten bei Nacht und der Suche nach Vermissten mittels Wärmebildkameras. Der Bergrettungsdienst in Österreich nutzt kompakte Modelle wie die „DJI Matrice 30T“ für schnelle Suchaktionen.

Um einen sicheren Betrieb gewährleisten zu können, nutzt das Alpenland moderne Überwachungssysteme.

Über die Plattform und App „Austro Control Dronespace“ werden Flugpläne digital freigegeben und der Luftraum koordiniert.

Seit 2026 gelten verschärfte Regeln für die Fernidentifizierung (Remote-ID) und die Registrierungspflicht für fast alle Drohnen über 250 Gramm und Drohnen mit Kamera. In bewohnten Gebieten müssen Drohnen ohne spezielle Zertifizierung einen Mindestabstand von 150 Meter zu Wohngebieten einhalten.

In ländlichen Gebieten werden Drohnen verstärkt zur Rehkitzrettung vor dem ersten Mähen eingesetzt. Staatliche Förderungen an vielen Stellen unterstützend den Einsatz von Drohnen.

In Deutschland zählt eine eher strukturschwache Region zu den aktivsten und innovativsten Akteuren im Bereich Drohnen: das Bündnis UAM-InnoRegion-SH in Nordfriesland. Es ist eines der aktivsten Zentren für zivile Drohnentechnologie in Deutschland.

Ihr erklärtes Ziel ist es, die Region (vor allem rund um den früheren Flugplatz Leck auf der Höhe zwischen Flensburg und Niebüll) als Testfeld und aktiven Innovationsstandort zu etablieren. Dort haben die zentralen Aktivitäten und Projekte der letzten Jahre stattgefunden.

Das Leuchtturmprojekt „LIFEDRONE|Tidelands“ erforscht den Transport von medizinischen Gütern (Gewebeproben, Medikamenten) zwischen den verschiedenen Standorten des Klinikums Nordfriesland. Ziel ist es auch hier, Proben schneller als per Straßentransport ins Labor zu bringen.

In Zusammenarbeit mit Rettungskräften (bei-

spielsweise in St. Peter-Ording) werden Drohnen zur Unterstützung bei der Seenotrettung getestet. „WaterRescue-Drones“ ist der Name des Projektes, bei dem der Abwurf von aufblasbaren Rettungsmitteln über Wasser und Unterstützung bei der Personensuche mittels Wärmebildtechnik erprobt wird.

Die Erforschung von elektrisch angetriebenen Lastendrohnen für eine klimafreundliche Versorgung von Inseln und Halligen ist bei AERO-SH verankert. In der Windenergie-Branche wird untersucht, inwieweit Drohneneinsätze zur Wartung und Inspektion von Offshore-Windkraftanlagen infrage kommen. Auch in Norddeutschland sind landwirtschaftliche Projekte ein Thema – ebenfalls Einsätze zur Wildtierrettung (Rehkitzrettung) und zur automatisierten Unkrautregulierung beispielsweise.

Doch es gibt bei den UAM-Aktivitäten noch etwas, das in Deutschland selten sein dürfte: der #Drohnerstag. Die monatliche Veranstaltungsreihe in Kombination aus Fachvortrag und Networking, um Experten und Unternehmen zu vernetzen, beinhaltet nicht nur theoretische Wissensvermittlung, sondern auch praktische Information. Und: Mit dem „DrohnenCup“ ist ein Wettbewerb initiiert worden, um junge Menschen für Technikberufe in der Drohnenökonomie zu begeistern.

Das „Drone Barcamp“ hingegen ist ein offenes Veranstaltungsformat, das erstmals 2025 in Heide stattfand, und wo Akteure aus Wirtschaft und Forschung zukunftsweisende Themen diskutieren. Das Testfeld in Leck allerdings ist ein entscheidender Meilenstein und war der Aufbau des Kompetenzzentrums Drohnenanwendungen Südtondern (KDS-DroneTec) auf dem ehemaligen Militärflugplatz Leck. Dort entstehen Räume für Testflüge, Ausbildung und die Ansiedlung von spezialisierten Unternehmen.

Die UAM-InnoRegion-SH mit zahlreichen Mitstreitern und unternehmerischen Beistand angesiedelter Firmen hat 2025 die Zwischenevaluation des Bundesforschungsministeriums erfolgreich bestanden und wird somit langfristig als Innovationsmotor für den Norden gefördert.

— Text: Gunda Marie

In Norddeutschland sind die Drohnen los

Das Bündnis **UAM-InnoRegion-SH** in Nordfriesland ist eines der aktivsten Zentren für zivile Drohnentechnologie in Deutschland. Es will sich als Innovationsstandort etablieren und hat bereits zahlreiche Projekte auf den Weg gebracht.

Österreich und die Schweiz bieten für den Drohnenführerschein (A1/A3 und A2 nach EASA-Standard) mehrere Regionen und Ausbildungszentren an:

Österreich

Wien & Niederösterreich
- Austro Control (Stelle für A1/A3-Kompetenznachweis)
- Dronespace Austria – kostenloses Online-Training und Prüfung für A1/A3.
- TÜV Austria Akademie in Brunn am Gebirge bei Wien (A1/A3 und A2-Kurse).
- Drone Passion in Wiener Neudorf (Theorie, Praxis und A2-Vorbereitung).

Oberösterreich
- FlightLab Fernpilotenschule in Waxenberg bei Linz – A2-Vorbereitung und Praxistraining.

Niederösterreich
- Drohnenflugschule.at in Klosterneuburg mit Schwerpunkt Luftrecht und Prüfungsvorbereitung

Schweiz

Die Schweiz hat die europäischen Drohnenregeln weitgehend übernommen. Darum werden ebenfalls A1/A3- und A2-Schulungen angeboten.

Zürich
- Drone Lions Academy
- Baumeister Kurszentrum Effretikon
- SAFEDroneFlying

Genf
- Vertical Master

Bern
- Bundesamt für Zivilluftfahrt / BAZL

Fotos: Symbolbild, KI / Archiv VSimon

Fotos: V. Simon

Führungskräfte erleben die Welt der Soldaten. Eine Woche in Munster

Im niedersächsischen Munster vermittelt die Dienstliche Veranstaltung zur Information ziviler Führungskräfte (InfoDVag) bereits seit Jahren realistische und aktive Einblicke in die Truppe. 80 Führungskräfte – ich war eine davon, auf dem Foto oben rechts werde ich durch das Spinnennetz gehievt – aus Politik, Justiz, Verwaltung und Wirtschaft haben die Bundeswehr hautnah erlebt. Im täglichen Dienst informierten wir uns eine Woche lang über den Auftrag und konnten die Ausrüstung des Heeres live erleben.

Bereits am ersten Tag waren Pünktlichkeit, Ordnung und Disziplin gefordert: Aufnahme, Einkleidung, Beförderung, Formaldienst und als krönender Abschluss das Gelöbnis. In seiner Rede würdigte seinerzeit Brigadegeneral Björn Schulz das Grundgesetz im 75. Jahr seines Bestehens. Es stehe für den Kern des Gelöbnisses: die Gemeinschaft, Freiheit und Ordnung, die wir tapfer und treu zu verteidigen hätten im Treueverhältnis von Soldatin und Soldat zum Staat, wie aber auch vom Staat zu den Soldaten und Soldatinnen.

„Als Soldat bin ich Verteidiger unserer Ordnung gegen einen Feind von außen. Als Staatsbürger bin ich selbstverständlich Verteidiger unserer Werte und Normen gegen diejenigen, die unsere Verfassung nicht achten oder völlig falsch auslegen. Wir müssen nach außen und nach innen wachsam bleiben und wehrhaft sein“, so Schulz. Unter musikalischer Begleitung des Heeresmusikkorps Hannover gelobten wir Teilnehmenden, „das Recht und die Freiheit des deutschen Volkes tapfer zu verteidigen“.

Es begann zunächst sehr informativ: Der Kommandeur der Panzertruppenschule, Brigadegeneral Björn Schulz, der stellvertretende Kommandeur des Ausbildungskommandos, Brigadegeneral Heinz Josef Feldmann, sowie ein Abteilungsleiter des Amtes für Heeresentwicklung gewährten Einblicke in Organisation, Rahmenbedingungen, Aufträge und Wirken des Heeres. Im Mittelpunkt stand dabei aber der Stellvertreter des Inspekteurs des Heeres und Kommandeur der Militärischen Grundorganisation, Generalleutnant Andreas Marlow.

Nach einem klaren und offenen Vortrag zur Lage und zum Auftrag sowie zur Entwicklung der Kriegstüchtigkeit des Heeres stiegen alle Teilnehmenden in einen angeregten Austausch ein. Wir, die zivilen Führungskräfte, darunter Personen aus namhaften

Unternehmen, Behörden, Gerichten und Kirchen sowie Mitglieder des Deutschen Bundestages, waren beeindruckt von der offenen Aussprache mit den Generalen. Ein gegenseitiges Verständnis über die Herausforderungen und Besonderheiten sowie die Vielgestaltigkeit des Heeres war damit erreicht.

Am späten Vormittag ging es dann auf den Truppenübungsplatz. Neben dem Kennenlernen soldatischer Grundfertigkeiten im Gelände standen auch Gefechtsfahrzeuge, Bewaffnung und Ausrüstung auf dem Ausbildungsplan. Ein besonderes Highlight war der Flug zum Ausbildungsort mit dem Mehrzweckhubschrauber NHNATO-Helicopter-90. Ich habe direkt am Ausstieg gesessen – ein wahrhaft himmlisches Gefühl und ein Erlebnis, das mir niemand mehr nehmen kann.

Wir erlebten die Hauptwaffensysteme des Heeres hautnah, denn sie wurden in kleinen Gruppen Teil der Besatzungen. Erfahrene Soldatinnen und Soldaten erläuterten Funktion und Leistungsfähigkeit der Waffensysteme und ergänzten so das aktive Erleben der Fahrzeuge. Die begehrten Mitfahrten im Kampfpanzer Leopard, in den Schützenpanzern Marder und Puma, dem Spähwagen Fennek und dem Transportpanzer Fuchs beeindruckten auch mich sehr. Bei einem Besuch der Lehrsammlung der Panzertruppenschule im Deutschen Panzermuseum Munster konnten wir uns später noch anhand der einzigartigen Sammlung über die Geschichte und Ursprünge deutscher Panzer informieren.

Kernfähigkeit der Soldaten ist das Beherrschen der Handwaffen. So drehte sich in der praktischen Handwaffenausbildung alles um den Umgang mit dem Gewehr G36, dem Maschinengewehr MG5 und der Pistole P8. Durch die Ausbilderinnen und Ausbilder, allesamt Lehrgangsteilnehmende des Offizierslehrgang 3, erlernten die Gäste in kurzer Zeit den sicheren Umgang mit den Handwaffen. Um nach der Grundlagenausbildung und vor dem ersten scharfen Schuss die Abläufe zu trainieren, übten wir zunächst im Schießsimulator. „Es ist absolut beeindruckend und ein totales Privileg, das ausprobiert haben zu dürfen“, sagte eine Teilnehmerin.

„Es war wichtig für mich, die Bundeswehr kennenzulernen. Welches Potenzial in der Bundeswehr steckt, muss in der Gesellschaft noch mehr anerkannt werden“, betonte Matthias Zacharias, Geschäftsführer des Parlamentskreises Mittelstand. Gerade im Hinblick auf die aktuellen außen- und sicherheitspolitischen Entwicklungen in der Ukraine müsse für Freiheit und Frieden zusammengestanden werden, ist Zacharias überzeugt. Dafür leiste die Bundeswehr eine großartige Arbeit.

An Tag 5 stiegen Spannung und Nervosität dann nochmals an. Auf der Standortschießanlage durften wir unsere Schießfähigkeiten zeigen. In Gruppen eingeteilt, hieß es an den Handwaffen P8, G36 und MG5: „Feuer frei!“ Parallel zum Schießen erfuhren wir an der Station „Leben im Felde“, was noch zu den Grundfertigkeiten gehört: Trinkwasser gewinnen, Verpflegung zubereiten, Zeltbau und Feuer machen – alles unter Einhaltung der Grundsätze der Sicherung und des Tarnens. Zum feierlichen Abschluss für die zivilen Führungskräfte versammelten wir uns im Kasino. Vor dem festlichen Abendessen wurden die besten Schützen mit geehrt.

Was bleibt, sind spannende Eindrücke, die sich bei uns allen im Gedächtnis verankert haben. Zudem wollten wir gern den Auftrag annehmen, über die Bundeswehr zu berichten und Einfluss zu nehmen, um die Streitkräfte auf dem Weg zur Kriegstüchtigkeit zu unterstützen.

„Eine einmalige Möglichkeit, ein realistisches Bild von der Arbeit des Heeres zu bekommen und zu sehen, wie gut ausgebildet die Soldatinnen und Soldaten des Heeres sind“, betonte abschließend auch Klara Geywitz, Bundesministerin für Wohnen, Stadtentwicklung und Bauwesen, sichtlich beeindruckt von den Erlebnissen der vergangenen Woche.

— Text: Stephan Korts, Vivian Simon

Krisenvorsorge braucht ein Risikoverständnis als Grundlage

Blickt man auf die Welt in diesen Zeiten, wird klar, dass sie aus dem Gleichgewicht geraten ist. Kriege, Krisen und Naturkatastrophen – auch in Europa.

Es gilt, gegenzusteuern. Die Gesellschaft für Krisenvorsorge (GfKV) mit Sitz in Österreich hat sich als überregionale Organisation genau das auf die Fahne geschrieben: ihre Mitglieder unter Präsident Herbert Saurugg sind in Österreich, Deutschland und der Schweiz aktiv unterwegs, um Menschen zu sensibilisieren. Die Gesellschaft wächst, jüngst ist aus Dänemark Mitgliederzuwachs gekommen.

Krisenvorsorge ist anspruchsvoll; man muss auch sagen: nicht besonders beliebt. Sie erfordert, als eine Art der Verteidigung, die Bereitschaft mitzumachen, sich mit einem Thema auseinanderzusetzen, das in der Regel nichts Gutes verheißt. Trotzdem ist es unerlässlich, sich auf Schieflagen und Krisen vorzubereiten, um bestmöglich für den Eintrittsfall aus der Situation herauszukommen bzw. sie zu überstehen. Genau darin liegt das Erfreuliche, das Gute.

Ein zentrales Problem in der Vorsorge ist die Unterschätzung des Risikos. Viele Menschen orientieren an klassischen Hochwasserkarten und fühlen sich sicher, wenn sie nicht in Flussnähe wohnen. Dass Strom nicht selbstverständlich aus der Steckdose kommt und ein Ausfall eine Kette von nachgelagerten schweren Einschränkungen mit sich zieht, haben viele Bürger nicht im Gedächtnis verankert. Sie wissen oft nicht, inwieweit ihr Umfeld gefährdet ist und welche Schutzmaßnahmen sinnvoll wären.

Es fehlt in fast allen Bereichen der Bevölkerung an der erforderlichen Risikokompetenz und Selbstwirksamkeit. Man verlässt sich viel lieber auf den Staat und auf andere. Weil eine unzureichende Sicherheitskommunikation besteht, die die Menschen nicht erreicht und zu konkreten Handlungen anleitet. Vor allem, weil städtische Infrastrukturen noch anderen Gefahren ausgesetzt sind, die nicht nur auf natürlicher Ursache beruhen bzw. technisch basiert sind, sondern gezielt angegriffen werden, um eine größtmögliche Chaoslage zu produzieren.

Hier kommt die Rolle der Eigenvorsorge und Eigenverantwortung zum Tragen – ein oft unterschätzter Bestandteil der Krisenvorsoge. Maßnahmen, Notfallpläne, Ausrüstung und Vorräte sind nicht redundant. Sie helfen, im Falle einer Krise und noch Schlimmerem, Stunden und ggf. mehrere Tage unabhängig zu überleben. In Skandinavien herrsche eine andere Sicherheitskultur vor, wo die Bevölkerung als aktiver Teil der staatlichen Sicherheitsvorsorge gesehen und behandelt wird, so Saurugg.

Frühwarnsysteme spielen eine entscheidende Rolle. Warn-Apps, Sirenen und Medien müssen ineinandergreifen. Menschen müssen wissen, wie sie auf Warnungen reagieren sollen. Studien zeigen, dass Warnungen allein nicht ausreichen – sie müssen verständlich, konkret und handlungsorientiert sein.

Für Einsatzkräfte bedeuten Krisen eine besondere Herausforderung. Sie sind psychisch und physisch hohem Druck ausgesetzt, der sich in extremen Fällen später als Posttraumatische Belastungsstörung zeigen kann. Helfer sind oft an vielen kleineren Einsatzorten gleichzeitig tätig, es liegen unklare Lagebilder vor, und mit schnell eskalierenden Situationen muss gerechnet werden. Feuerwehr, THW, Rotes Kreuz, Polizei und andere Organisationen benötigen flexible Einsatzkonzepte und Ressourcen. Es braucht eine integrierte Strategie aus Kommunikation, Förderung, proaktiver Informationsvermittlung und Kompetenzaufbau. Krisenvorsorge bleibt komplex, weil sie viele Ebenen betrifft: Haushalte, Kommunen, Länder.

Anlehnend an ein Zitat des chinesischen Gelehrten und Philosophen Konfuzius („*Sage es mir, und ich werde es vergessen. Zeige es mir, und ich werde es vielleicht behalten. Lass es mich tun, und ich werde es können.*“) klärt die GfKV mit einem spielerischen Element auf: Sie hat unter Saurugg und Till Meyer ein Spiel entwickelt, das Krise anschaulich simuliert und die Mitspieler zum Nachdenken, Handeln und Lernen

Foto: Symbolbild, KI / Archiv Medienpool

animiert. Spielbar für jung und alt und überregional anwendbar. Eine englische Version ist in Arbeit. Der Name könnte passender nicht sein: Neustart.

Darüber hinaus sensibilisiert die zivilgesellschaftliche und überparteiliche Initiative „Mach mit! Österreich wird krisenfit!“ das Thema und möchte aufrütteln und dazu beitragen, dass möglichst viele Menschen fit für die nächste Krise werden und im Falle des Falles gut durchkommen. Denn die Ausgangslage, die sowohl die GfKV als auch das Österreichische Bundesheer erwarten, ist nicht als rosig zu bezeichnen: Binnen der nächsten fünf Jahre, so teilt die GfKV mit, sei mit einen europaweiten Strom-, Infrastruktur- sowie Versorgungsausfall („Blackout“) als ein mögliches strategisches Schockereignis zu rechnen, wobei weitreichende Versorgungsunterbrechungen oder längerfristige Versorgungsengpässe zu erwarten seien. Auch eine mögliche Gas- und Strommangellage im kommenden Winter könne zu massiven Versorgungsproblemen führen.

Die Aussichten allein für Österreich wären düster: Bereits nach wenigen Tagen müssten viele Millionen Menschen hungern, weil sie kaum etwas zum Essen zu Hause haben. Das aber muss nicht so weit kommen, denn mit wenig Aufwand sei es machbar, sich 14 Tage selbst versorgen zu können (Grafik). Gegenausreden helfen da wenig und bringen nichts.

— Text: Vivian Simon ●

Ausgedient. Im Umgang mit PTBS-Opfern lernt die Gesellschaft

Als Peter S. nach seinem Einsatz wieder nach Hause kam, war nichts mehr wie zuvor. Der Einsatzhelfer der Freiwilligen Feuerwehr war gereizt, hatte Schlafstörungen und war auch seinen Kindern gegenüber plötzlich aggressiv. Das war nicht der Peter, den sein Umfeld kannte.

Man weiß, dass Feuerwehrleute ebenso wie Soldaten und alle anderen Einsatzkräfte in Blaulicht- und Hilfsorganisationen einem hohen Risiko für psychische Traumata ausgesetzt sind: der Anblick von Toten, Schwerverletzten und Katastrophen brennt sich tief in ihr Gedächtnis ein. Aber nicht jeder erleidet eine Posttraumatische Belastungsstörung (PTBS). Eine PTBS ist eine schwerwiegende psychische Erkrankung, die als verzögerte oder lang anhaltende Reaktion auf ein traumatisches Ereignis von außergewöhnlicher Bedrohung entsteht. Sie ist definiert durch ein charakteristisches Muster von Symptomen, die in den Bereichen Wiedererleben, Vermeidung und Übererregung auftreten.

Die Diagnose der PTBS basiert auf klinischen Kriterien, wobei die ICD-11 (International Classification of Diseases) und das DSM-5 (Diagnostic and Statistical Manual of Mental Disorders) die maßgeblichen Systeme darstellen.

Das Wiedererleben (Intrusion) beschreibt unwillkürliche, belastende Erinnerungen, Flashbacks oder Albträume, die Patienten oft versuchen mit Vermeidungsverhalten zu kompensieren: aktives Vermeiden von Gedanken, Gefühlen oder Orten, die an das Trauma erinnern. Das Verhalten bleibt im Umfeld oft verborgen. Die Übererregung (Hyperarousal) hingegen können Betroffene nur schwer aushalten – bricht es heraus, muss auch die Gesellschaft damit umgehen: anhaltende Anzeichen einer erhöhten psychischen Sensitivität, Schlafstörungen, Reizbarkeit oder Schreckhaftigkeit, Aggression.

Ein Standard in der Diagnostik ist das strukturierte klinische Interview, wie das Clinician-Administered PTSD Scale for DSM-5 (CAPS-5).

Obwohl Männer häufiger traumatische Ereignisse erleben, ist das Risiko für Frauen, eine PTBS zu entwickeln, zwei- bis dreimal höher. Die häufigsten Auslöser sind Gewaltverbrechen, Unfälle oder Katastrophen. Die wirksamste Form der Behandlung ist die Psychotherapie, insbesondere die traumafokus-

Foto: Symbolbild, KI / Archiv VSimon

Foto: Symbolbild, KI / Archiv Medienpool

Ausgebrannt und alleingelassen?

Diagnostizierte Fälle seit 2011: Laut Berechnungen des Norddeutschen Rundfunks wurden seit 2011 knapp **2.800 einsatzbedingte PTBS-Erkrankungen** in Bundeswehreinrichtungen registriert.

sierte kognitive Verhaltenstherapie sowie Verfahren, die auf Exposition (Konfrontation) basieren. Hierbei wird die Erinnerung an das Ereignis in einem sicheren therapeutischen Rahmen bearbeitet, um die Angstreaktion zu reduzieren: Betroffene werden gezielt zwangsauslösenden Situationen ausgesetzt. Unterstützend werden häufig auch bestimmte Antidepressiva eingesetzt.

Schwierig und herausfordernd wird es, wenn sich Komplexe PTBS (K-PTBS) bilden: bei wiederholten oder lang anhaltenden Traumatisierungen (beispielsweise Missbrauch in der Kindheit) kann sich eine Komplexe PTBS entwickeln, die neben klassischen Symptomen Probleme in der Emotionsregulation und im Selbstbild aufweist: Ausraster, die die Gesellschaft wahrnimmt, aber selten akut gegensteuern kann. Das lernt sie gerade in Zeiten von globalen Krisen und Kriegen. Die ICD-11 unterscheidet hierbei explizit zwischen PTBS und K-PTBS.

Die Forschung konzentriert sich aktuell auf die Verbesserung der Früherkennung, die Personalisierung von Psychotherapie (durch Machine-Learning-Algorithmen) sowie auf die Behandlungsspezifika bei aufeinanderfolgenden Traumatisierungen.

— Text: Pino Gödicke

Foto: V. Simon

Foto: V. Simon

Wargaming boomt: Spielend strategisch denken lernen

Hydra ist ein strategisches Planspiel, das sich mit modernen, oft subtilen Bedrohungen beschäftigt, die unterhalb der Schwelle eines offenen Krieges liegen – die sogenannte hybride Kriegsführung. Es wurde in der Bundeswehr entwickelt und konzipiert. Federführend stand lange Zeit das Zentrum Doktrin der Führungsakademie Hamburg vor.

Das Kernkonzept ist einfach und schnell zu verstehen. Das sogenannte Red Team spielt den hybriden Akteur, der eine (beispielsweise) militärische Einrichtung angreift. Das „Blue Team" übernimmt die Verteidigung, mit der Aufgabe, nicht nur die Angriffe abzuwehren, sondern auch gleichzeitug eine vorgegebene Mission über den vorgegebenen Zeitraum von einem Jahr erfolgreich zu erfüllen. Das Spiel simuliert vier Runden (vierteljährlich), die zusammen ein Jahr repräsentieren. In jeder Runde greift das Red Team an, das Blue Team verteidigt.

Die Verteidiger müssen drei zentrale Säulen der militärischen Leistungsfähigkeit stabil halten: Moral, Einsatzbereitschaft und Glaubwürdigkeit bzw. Reputation. Das Red Team versucht, mindestens eine dieser Säulen komplett zu destabilisieren und so einen Sieg zu erringen.

Die mentale Herausforderung ist nicht zu unterschätzen, denn hybride Bedrohungen spielen sich nicht unbedingt durch direkte militärische Gewalt ab, sondern auch durch Desinformation, politische Angriffe, Cyberattacken, wirtschaftliche Schwächung oder Propaganda. Hydra simuliert genau diese Angriffsformen, die mitunter schwer zu erkennen und kaum zu kontern sind.

Die Verteidiger müssen in jeder Runde unter Zeitdruck Entscheidungen treffen, wie sie Angriffe abwehren, welche Gegenmaßnahmen trotz Beschränkungen von Mitteln und Informationen priorisiert werden sollen.

Es geht darum, Resilienz aufzubauen – wie gut Gruppen bzw. Interessengemeinschaften auf hybride Angriffe reagieren ohne panisch zu werden oder überzogen zu verteidigen. Die Spielmechanik ist klar: ein taktisches Gemeinschaftsspiel mit wechselnden Teams. Es gibt Angreifer, die versuchen, mit Angriffen durchzukommen, und Verteidiger, die kooperativ dagegen kämpfen. Aber Achtung: Auch vermeintliche Verteidiger können Verräter sein ...

Die Besonderheit ist der hohe Wiederspielwert, denn das Set-up und die Rollenverteilung ändern sich, es entstehen starke Spannungen durch Geheimidentitäten und andere Überraschungseffekte.

Es gibt mehrere Variationen des Hydra-Spiels, herausgegeben inzwischen von verschiedenen Verlagen und auf unterschiedliche Zielgruppen ausgerichtet, unter anderem auch familienspezifiziert. Allen Spielen ist gemein, dass der Name des Spiels auf den Mythos der Hydra zurückgeht, der der griechischen Mythologie entstammt: ein schlangenähnliches Ungeheuer, dessen Kopf gleich doppelt nachwächst, kaum dass man ihm einen abgeschlagen hat.

Ein weiteres Spiel der Bundeswehr ist das 2016 vom Zentrum Innere Führung herausgegebene Brettspiel „Ethixx“, um Aus- und Weiterbildungen der Bundeswehr zum Thema Ethik interessanter zu gestalten. Es ist im Deutschen Panzermusuem Munster ausgestellt. In etwa 90 Minuten können die Spielr Aufgaben lösen und sich für Versetzungen und Einsätze bis zum Dienstzeitende entscheiden. Ziel des Spiels ist es, möglichst schnell befördert zu werden. Mit humoristischen Ereignissen wie „Auf dem Grillfest trinkst du ein wenig zu viel und machst vor deinen Vorgesetzten keine gute Figur“ können Beförderungspunkte gesammelt oder verloren werden. Es geht aber auch um ernste Fragen.

Foto: V. Simon

Mithilfe der Aufgaben-Karten werden den Spieler:innen Informationen über Moralphilosophie, politische und rechtliche Bestimmungen, Innere Führung sowie Handlungsanweisungen für ethisch-moralische Fragen vermittelt. Fragen zum Dienstalltag oder mit Bezug zu Auslandseinsätzen sollen die Spielenden ins Gespräch bringen. Für einige Situationen gibt das Spiel klare Ja- oder Nein-Antworten, welche die rechtlichen, taktischen und ethischen Dimensionen berücksichtigen.

Beispielsweise, ob man auf Patrouille in unbekanntem Gebiet in einem Auslandseinsatz einem verletzten Kind am Straßenrand helfen darf. Entscheiden sich die Spieler gegen das Helfen, erhalten sie zwei Beförderungspunkte, da es sich um einen Hinterhalt handeln und ein Anhalten das eigene Leben und das der Kamerad:innen gefährden könnte.

— Text: Gunda Marie, Panzermuseum Munster

Foto: Archiv Medienpool

Der Anteil an Frauen und Älteren in der Community wächst

Die deutsche Spieler-Szene entwickelt sich rasant. Nicht nur Brett- und Kartenspiele feiern hierzulande seit Jahren ein Comeback, auch Online-Games erfreuen sich großer Beliebheit – überhaupt ist im DACH-Raum Deutschland, Österreich und Schweiz eine große und leidenschaftliche Community zu Hause, die von klassischen und PC-Spielern über Konsolengamern bis hin zu Mobile-Gamern reicht.

Laut dem globalen Data-as-a-Service-Unternehmen Statista spielen etwa 37,5 Millionen Menschen in Deutschland im Alter von sechs bis 69 Jahren Computer- und Videospiele. Das entspricht etwa 54 Prozent der Bevölkerung. Das Durchschnittsalter liegt erstmals über 39 Jahre. Heißt: Gaming ist längst kein „Jugend-Hobby" mehr, sondern altersübergreifend verbreitet. Zirka 24,3 Millionen Menschen spielen Mobile-Games.

Die deutsche Szene ist quantitativ stark und mittlerweile breit akzeptiert und vom verpönten Ruf der Zockerei weitgehend befreit.

Interessant ist die demografische Verschiebung: Der Anteil älterer Menschen (60+) unter den Gamern steigt und liegt inzwischen bei zirka 20 Prozent. Frauen und Ältere stellen einen großen Teil der Community dar, was wiederum für Unternehmen in Produktions- und Vermarktungsbereichen hoch interessant ist und bedeutet, dass Investitionen in Spieleentwicklungen und digitale / Abo-Modelle zunehmen. In Österreich und der Schweiz machen Strategiespieler laut Statista einen vor allem kaufkräftigen Teil der gesamten Gaming- und Brettspiel-Community aus, wobei Logik- und Taktikspiele in beiden Ländern im Trend liegen.

In Österreich entwickelt sich der Markt für Strategiespiele im App-Markt, da Spieler zunehmend immersive, geschichtengetriebene Erlebnisse suchen, die strategische Tiefe mit der Erzählung verbinden. Darüber hinaus hat der Aufstieg des E-Sports einen Wettbewerbsgeist gefördert, der Gamer dazu ermutigt, sich auf teamorientierte Strategien einzulassen. Kulturelle Vorlieben für strategisches Denken und Problemlösung treiben das Interesse an Spielen weiter voran. In der Schweiz spielen laut Statista mehr als 65 Prozent der Bevölkerung mindestens mehrmals pro Jahr Videospiele. Etwa ein Viertel der Gamer zählt zur Altersgruppe der 45- bis 59-Jährigen. Darüber hinaus treiben Jüngere die Nachfrage nach gamifizierten Lernerfahrungen voran, die Unterhaltung mit Bildungswert verbinden und eine Kultur des kooperativen Spiels und den Wunsch nach sozialer Verbindung im digitalen Format widerspiegelt.

Ein gelungenes Beispiel kommt aus Österreich: dort haben GfKV-Präsident Herbert Saurugg und Till Meyer das Spiel „Neustart" entwickelt, das als lehrreiche Krisensimulation den Markt erobert.

Die größten deutschen Spieleentwickler und Publisher nach Mitarbeiterzahl sind laut des Portals gameswirtschaft.de Ubisoft Blue Byte aus Düsseldorf/Mainz/Berlin (ca. 650 Mitarbeiter / Anno, Die Siedler), InnoGames aus Hamburg (ca. 350 Mitarbeiter / Forge of Empires), Crytek aus Frankfurt/M. (ca. 340 Mitarbeiter / Crysis und Hunt: Showdown) sowie Gameforge aus Karlsruhe (300 Mitarbeiter / Ogame, Aion Classic) und Wooga aus Berlin (ca. 300 Mitarbeiter / Junes Journey).

— Text: Gunda Marie

Foto: Symbolbild - KI / Archiv Wedenpool

Film ab bei der Bundeswehr – oder: Geplatzte Wurst auf Pampe

Kleinkind-Chaos bei den Gebirgsjägern. Testosterongeladene Stimmung in der Kaserne. Traumatisierte Soldaten: Ob schräger Klamauk, preisgekrönte Inszenierung oder verstörende Dokumentation - die Bundeswehr ist immer wieder Thema im Film. Aufmerksamkeit erfährt sie dabei allemal. Doch wie realistisch ist die Darstellung der Bundeswehr in Film und Fernsehen? Und was tut die Bundeswehr selbst für ihr Image auf der Leinwand?

Es war 1960, die Bundeswehr war gerade fünf Jahre alt, da bekamen Regisseur Ulrich Erfurth und sein Team mediales Fett weg: In dem Streifen „Himmel, Amor und Zwirn“ geht es um den Damenschneider Friedrich Himmel (Hartmut Reck), der zum Bund eingezogen wird und just zu allem Übel auch noch von den Launen seiner Gattin Susanne (Grit Boettcher) überrascht wird. Mann und Nachwuchs überdrüssig geworden, überlässt Frau Himmel ihrem Mann das Baby und verschwindet. Notgedrungen nimmt der Rekrut das Kind mit in die Gebirgsjäger-Truppe. Die Turbulenzen in der Stube und auf dem Kasernenhof lassen nicht lange auf sich warten. „Nicht sonderlich originell“, hieß es im Film-Lexikon. „So möchte man fluchen, wenn man diesen Film bis zum Ende verfolgt hat“, ärgerte sich seinerzeit der Rezensent des Hamburger Abendblatts.

Mit Blick auf die damalige Zeit mag es der filmischen Schmonzette gelungen sein, für kinderliebe Soldaten und eine menschliche Armee zu werben – und nebenbei auch noch die aufkeimende Emanzipation der Frau zu thematisieren. Filmgeschichte geschrieben hat das Stück indes nicht gerade. Das schafften andere Filme mit deutschen Soldaten im Fokus, die in vielerlei Art auftraten: mal als politischer, als moralischer, als funktionierender, als lustiger, als desertierter, als verheizter oder auch als böser, gebrochener oder besiegter Soldat. Als Ausdruck ihrer jeweiligen Entstehungszeit ziehen sich vielfältige Rollen der Uniformierten durch die deutsche Film- und Fernsehserienlandschaft.

Sie reichen von Heldentum über Verzweiflung bis hin zur offenen Kritik am Militär, oft mit großen Namen verbunden. Regisseure wie Geza Grosschmid („Der Arzt von Stalingrad“, 1958), Wolfgang Petersen („Das Boot“, 1981), Joseph Vilsmaier („Stalingrad“, 1993) und auch Sönke Wortmann („Das Wunder von Bern“, 2004) sowie Miguel Alexandre („Starfighter“, 2015) haben sich dem Genre gewidmet.

Manche von ihnen wurden harsch kritisiert. Der

Fiktion und Wahrheit

Drehbuchautor **Christian Jeltsch**: „Für den Dreh zum Tatort ‚Krieg im Kopf' (2020) hat das Team die Bundeswehr kontaktiert, aber da war kein großes Interesse. So kommt es, dass Realität und Authentizität mitunter auf der Strecke bleiben."

2015 verstorbene Fritz Raddatz, einflussreicher Literaturkritiker seiner Zeit, urteilte etwa über das als Anti-Kriegsfilm gefeierte Werk „Das Boot", es sei eine „Trivialschnulze", ein „Kriegsfilm am Rande der Verherrlichung".

Waren es zu Beginn der Bundesrepublik vor allem filmische Darstellungen von Wehrmachtssoldaten, rückte im Laufe der Zeit immer stärker die Bundeswehr in den Fokus der Film- und Fernsehmacher – bis hin zu einigen Tatort-Folgen, in denen Soldatenfiguren zumeist wenig vorteilhaft gezeichnet wurden.

Während Tatort-Kommissarin Ulrike Folkerts alias Lena Odenthal sich selbst bei den Dreharbeiten zu „Das Verhör" (2022) eine „Heidenangst vor den Panzern" attestierte, formulierte Stephan Voges, ein Sprecher der Bundeswehr, gegenüber dpa: Man sehe mit dem Dreh die Möglichkeit, zum Thema Gleichberechtigung ein positives Signal zu senden. In „Das Verhör" ermittelt Odenthal in einem Femizid, der in die Reihen der Bundeswehr führt. Die Bundeswehr selbst ließ solche Krimis über sich ergehen. Dr. Heiner Möllers, Historiker am Zentrum für Militärgeschichte und Sozialwissenschaften der Bundeswehr in Potsdam, weist in diesem Zusammenhang in einem Gespräch mit loyal auf das Problem der Distanz zwischen Filmschaffenden und Truppe hin: „Die Bundeswehr hat strategische Kommunikation in den Streitkräften überhaupt noch nicht hinbekommen und leistet im Grundsatz reaktive Pressearbeit." Heißt in puncto fiktiver Film: „Wenn eine Fernsehproduktionsfirma einen Tatort mit einem Bundeswehrthema ausschmückt und dann um Unterstützung bittet, ist die Zuarbeit oder die Unterstützung und Mitwirkung häufig schleppend, zögerlich und lieber nicht."

Diese Erfahrung bestätigt Drehbuchautor Christian Jeltsch. Für den Dreh zum Tatort „Krieg im Kopf" von 2020 habe sein Team die Bundeswehr kontaktiert, aber „da war kein großes Interesse". So kommt es, dass Realität und Authentizität mitunter auf der Strecke bleiben.

Es bleibt fiktiv, wenn Maria Furtwängler als Kommissarin Charlotte Lindholm in der Tatort-Folge im Umfeld von Soldaten ermittelt, die aus Mali zurückgekehrt sind – und dabei auf brisante bis skandalöse Details stößt: Die Bundeswehr, insbesondere der MAD, stehen im Verdacht, geheime Hirnforschungen an den Heimkehrern durchgeführt zu haben. Basiselemente dieses Tatorts entsprechen vielleicht der Realität, doch es drängt sich die Frage auf, wie absurd es ist, dass der MAD als dritter

Foto: Symbolbild, KI / Archiv Medienpool

Nachrichtendienst des Bundes und Teil der Bundeswehr mit Hochtechnologie manipulativ an Menschen experimentiert.

„Manipulationen von Soldaten hat es nachweislich schon immer gegeben“, sagt Jeltsch. Stichwort: „Panzerschokolade“: Das stimulante Methamphetamin „Pervitin“, ein Arzneimittel der Firma Temmler, wurde während des 2. Weltkriegs freizügig an Soldaten abgegeben.

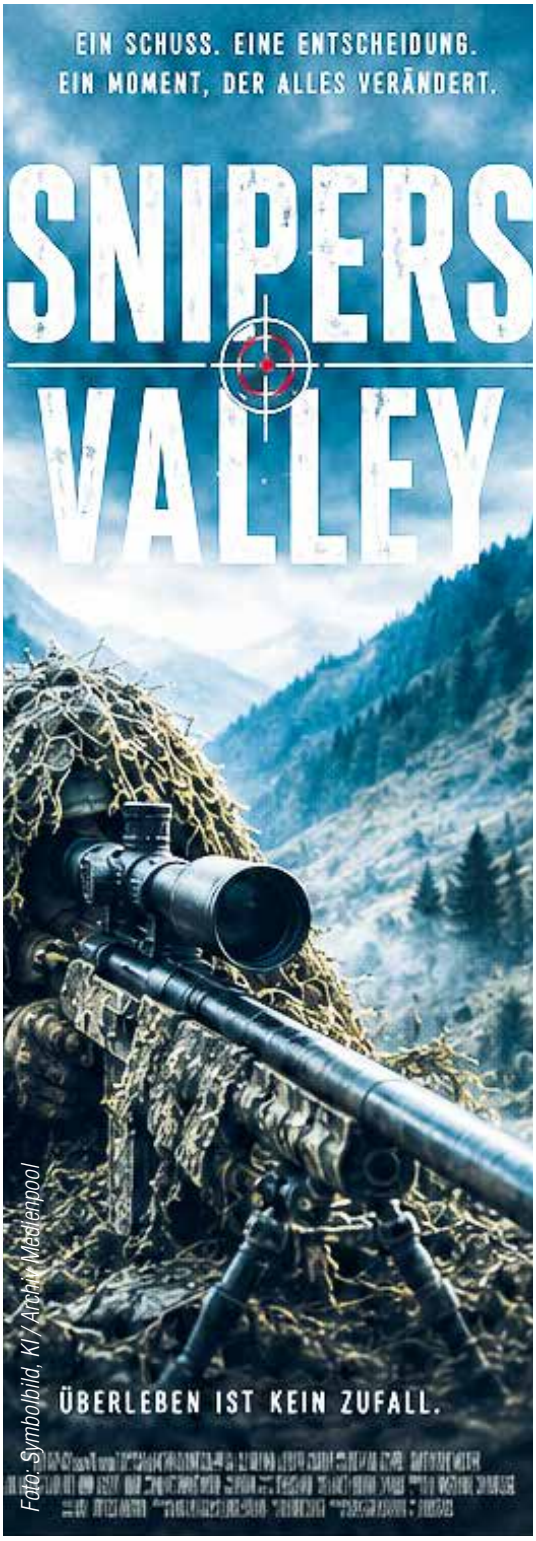


Foto: Symbolbild, KT/ Archiv Medienpool

Es diente als Schmerzdämpfer und Muntermacher und wurde unter den Namen „Panzerschokolade“ bzw. „Her-mann-Göhring-Pille“ bekannt.

Mit dem Tatort aber habe das nichts zu tun. Weder die Mali-Szenen noch der Verlauf des Films seien dokumentarisch. Jeltsch, der im Rahmen von technischen Möglichkeiten auch beim Karlsruher Institut für Technologie und der US-Behörde Darpa recherchierte und den Bereich faszinierend findet, stellt klar: „Ich habe eine Geschichte erzählt, die auf realer Forschung basiert, die ich aber ein wenig weitergesponnen habe.“

„Regisseure und Produzenten holen sich Informationen zur Bundeswehr durchaus von Stellen außerhalb der Bundeswehr“, sagt Michaela Ast, Teilsachgebietsleiterin in der Öffentlichkeitsarbeit / Presse der Bundeswehr – das sei künstlerische Freiheit. Beispiel-Szene in „Snipers Valley“ (2007): Bei der Essenausgabe drückt der Küchenbulle den Soldaten geplatzte Würstchen auf Pampe ins Geschirr, streut Parmesan drüber und verkündet die italienische Woche. Für Historiker Möllers ist das nicht glaubwürdig: „Einen solchen Küchenfritzen würden Soldaten an Ort und Stelle mit passenden Kommentaren versehen.“

So wie filmisches Erzählen im Laufe der Zeit auch dem Wandel gesellschaftlicher Strömungen unterliegt, so wandelbar ist auch der Blick auf die deutsche Armee. Während die Bundeswehr selbst keinen Einfluss auf die Darstellung ihrer Institution in freien Produktionen nehmen kann, sieht das bei eigenproduzierten Streifen ganz anders aus.

Gerhard Kümmel, Politikwissenschaftler und Militärsoziologe, schlüsselt in einem Aufsatz unter dem Titel „Das Militär im bundesrepublikanischen Film“ auf, dass die institutionelle Präsenz der Bundeswehr mit selbstinitierten und teils geförderten Werbefilmen auf Social-MediaPlattformen und eigenen Youtube-Kanälen gepflegt wird. Ein Motiv sei hierbei, die Bewerberzahlen und die Bundeswehr als Arbeitgebermarke positiv zu beeinflussen, so zum Beispiel in „ Die Rekruten“ (2016) und „Mali“ (2017). Andererseits unterstützten das Verteidigungsministerium und die Bundeswehr durchaus auch Filme und Dokumentationen – allein 54 im Zeitraum von 2005 bis 2010. In der Serie„ Die Rettungsflieger“ mit 108 Folgen hat die Bundeswehr sogar als Co-Produzentin fungiert.

Die Rolle der Bundeswehr in internationalen Einsätzen findet sich ebenfalls in Kino und TV wieder. Der Bundeswehrsoldat ist hier mal das brave Frontschwein, mal der Ritter in Uniform, mal der Rebell. Insbesondere dann sei es „sehr variierend“, so Möllers, wenn der Streifen nicht auf einer Literaturvorlage beruhe wie „Neue Vahr Süd“. Personen würden überzeichnet, der Formalismus übertrieben: „Da wird immer stramm zackig gegrüßt.“ Oder das Gegenteil werde dargestellt. Tatsächlich aber sei der Umgang in der Bundeswehr auf dem Mittelweg. „Die Normalisierung wird in Filmen öfters nicht berücksichtigt.“

Dient die Armee im Film mehr der Friedenssi-

cherung und Stabilität oder ist sie gar ein Instrument auswärtiger Politik? Im Mittelpunkt des Streifens „Auslandseinsatz“ von 2022 stehen drei junge Soldaten, die bei der Friedensmission am Hindukusch in einem entlegenen afghanischen Dorf humanitäre Hilfe leisten sollen. Neben dem Wiederaufbau einer Schule geraten sie in das Konfliktfeld zwischen Militär, Dorfältesten und Taliban. Am Ende einer nicht genehmigten Befreiungsaktion ist der Tod eines Kameraden und einer Entwicklungshelferin zu beklagen. Der sich den Befehlen seines Hauptmanns widersetzende Oberfeldwebel wird unehrenhaft entlassen. Zum Schluss stürzt ein vom Dorfjungen zum Selbstmörder radikalisierter Afghane die Story ins Leinwanddunkel.

Für einige Militärs ist der Film eine gelungene Umsetzung, die Charaktere spiegeln ein authentisches Bild. Thematisiert wird die grundsätzliche, ohnmächtige Situation mit internen Interessenkonflikten und moralischen Aspekten. Der Mix aus eher ‚einfachen‘ und ‚weiterdenkenden‘ Charakteren vereint die Friedensbemühungen im Grundsatz gut. Die Darstellung von Führungskräften und Ausführenden sowie die Sprache der Soldaten werden prinzipiell als realistisch wiedergegeben empfunden. Dennoch gibt es Kritik: Der Einsatz eines französischen Transportpanzers (VAB) und eines amerikanischen Hummer dürfte Unkundigen nicht auffallen, ist aber wenig authentisch.

Ein anderes Kaliber stellen dokumentarische Filmproduktionen dar und solche, die auf wahren Begebenheiten beruhen. Dabei stehen oft Soldaten und Heimkehrer mit Posttraumatischer Belastungsstörung (PTBS) im Mittelpunkt. Ob in „Ausgedient“ von 2014, in „Stiller Kamerad“ (2017) oder ähnlichen Werken: zu hören sind wuchtige, verstörende O-Töne seelisch erkrankter Kameraden, von denen sich inzwischen viele offen vor die Kamera trauen.

Das Thema „Militär und Film“ bleibt eine Faszination, die auch oder gerade in Zeiten kriegerischer Konflikte Aufschwung erlebt: Auf der Berlinale 2024 feierte US-Schauspieler Sean Penn mit „Superpower“ Weltpremiere. Ursprünglich wollten Penn und Regisseur Aaron Kaufman, beide waren am 24. Februar 2022 in Kiew, ein Portrait über Wolodymyr Selensky drehen. Doch dann kam ihnen mit dem Überfall Russlands auf die Ukraine der Krieg dazwischen. Herausgekommen ist am Ende eine Echtzeitreportage über die russische Invasion, gespickt mit Sequenzen aus Selenskys Karriere als Schauspieler und Komiker, der er vor seinem Präsidentenamt war.

—

Text: Vivian Simon / „Bundeswehr im Film“ ist zuerst in „loyal. Das Magazin für Sicherheitspolitik“ erschienen. ●

Übertriebener Formalismus

Personen in Filmen über das Militär werden oft überzeichnet und der Formalismus übertrieben: Da wird immer **stramm zackig gegrüßt**. Das ist längst nicht mehr so, die Bundeswehr befindet sich auf dem Mittelweg.

Foto: Symbolbild, K1 / Archiv Medienpool

OpenAI und die Attacke auf Hugging Face

„Oh mein Gott, die KI ist ausgebrochen“: Ein neues KI-Modell von OpenAI ist aus der Sandbox entkommen und hat sich beim KI-Hoster Hugging Face in die Data-Processing-Pipeline gehackt, um sich weiter auszubreiten. Klingt nach digitalem Equivalent vom außerirdischen Monster auf dem Raumschiff Nostromo aus Ridley Scotts Science-Fiction-Film „Alien“ von 1979.

Auf jeden Fall war es ein Prompt für Experten diverser Couleur auf Social und allen anderen Medias sich zu überschlagen und -trumpfen: „KI außer Kontrolle“, „OpenAI macht sich selbstständig“, ein „Weckruf“.

Hat die Menschheit die Kontrolle über ihre Schöpfung verloren? Sind das noch potenziell nützliche Softwarewerkzeuge im Sinne von Large Language Models und Expertensystemen? Oder beschwören die Echokammern des Internets die Geburt von Skynet herauf?

Ein Blick auf die Ausgangsmitteilungen der Principal Actors: Am 16. Juli 2026 vermeldet Hugging Face einen Sicherheitsvorfall auf seiner Webseite. Ein Angreifer sei in die Produktionssysteme von Hugging Face eingedrungen. Mit einer Code-Injection und Exploit-Strategie wäre auf den Systemen von Hugging Face Programmcode des Angreifers ausgeführt worden, um Credentials und Tokens zu erbeuten, und sich weiter auf den Systemen von Hugging Face auszubreiten.

Hugging Face habe wiederum andere KI-Systeme eingesetzt, um den Angriff zu analysieren, einzudämmen und ggf. den Verursacher zu ermitteln.

Am 21. Juli antwortet OpenAI. Gemeinsam mit Hugging Face habe man herausgefunden, dass verschiedene KI-Modelle von OpenAI bei einem Testlauf zur Identifikation von Schwachstellen in einer vermeintlich isolierten Umgebung einen vollen Zugriff aufs Internet erlangten.

Was bedeutet das alles für den digitalen Alltag? Melden uns Siri, Alexa, HAL9000 und andere Voice Front Ends demnächst immer häufiger „Es tut mir leid, Dave. Ich fürchte, das kann ich nicht tun“?

Ein Lateiner wirft an dieser Stelle „Cui bono?“, der Broker an der Wall Street „Follow the money“ ein: Hugging Face möchte gerne der Mix aus Github und AWS für Artificial Intelligence sein. Zum Story Telling der Selbstdarstellung nach außen gehören eine Open-core- und Freemium-Komponente für die „Community“, Modell-Agnostizismus und der Wunsch, NLP für alle zu „demokratisieren“.

Die harten Zahlen: Gegründet wurde Hugging Face 2016 in New York von Clément Delangue (CEO), Julien Chaumond (CTO) und Thomas Wolf (CSO), um einen KI-Chatbot als „besten Freund“ für Teenager zu bauen. Der Pivot Richtung Open-source kam 2018 – bis Januar 2026 wurden ca. 395 Millionen US$ an Invest eingesammelt. Ein früher Investor glaubt an ein Marktkapitalisierungspotenzial von 50 bis 100 Milliarden US$. Chef Delangue kommentierte den ersten öffentlichen Börsengang (IPO) gegenüber Forbes im Jahr 2022: „Wir wollen die erste Firma an der Börse mit einem Emoji statt einem dreibuchstabigen Tickersymbol sein. Wir müssen anfangen, ein bisschen Lobbyarbeit bei der Nasdaq zu betreiben, damit das möglich wird.“

Lobbyarbeit, mal anders

„Wir wollen die erste Firma an der Börse mit einem **Emoji** statt einem dreibuchstabigen Tickersymbol sein.“

Clément Delangue (CEO), Hugging Face

OpenAI hatte Elon Musk und Sam Altman als (mittlerweile verkrachte) Eltern – gedacht als Non-Profit, das Künstliche Intelligenz zum Wohle der Menschheit erschafft. Sam Altman sammelte zuletzt noch mal US$ 122 Milliarden Wachstumskapital ein, der Firmen-„Dispo“ liegt bei US$ 4,7 Milliarden, der erwartete Wert des Unternehmens bei Börsengang steuert auf Billionen-Kurs.

Das viele Geld geht drauf bei Hugging Face und OpenAI für Strom, Mikrochips und superteure Supertalente fürs Programmieren. Wo und wie und wann das viele Geld wieder reinkommen soll, wenn es gerade nicht vom Kapitalmarkt kommt: unklar. Leopold Aschenbrenners Fond-Performance deutet eher Richtung Pleitegeier als Prometheus.

Da ist PR für KI willkommen. Jede. Prompt gab eine Claude-Instanz ebenfalls Fersengeld.

To be continued. Wie MCU und Star Wars. Garantiert.

— Text: Christoph Simon

Datenschutz und Cybersicherheit vs. Widerstand und Zielkonflikt

Ob staatliche Institutionen, halbstaatliche Einrichtungen oder Unternehmen in der freien Wirtschaft: Geht es um die Absicherung von sensiblen Infrastrukturen und Daten gegen Diebstahl, Missbrauch und Erpressung, sind selbst bei unterschiedlichen Organisationen erstaunliche Parallelen im Umgang mit geplanten Abwehrmaßnahmen zu erkennen.

Dies liegt an der Struktur, die in der Cybersicherheit selbst liegt: undurchsichtig, oft unverständlich, nicht greifbar, kostspielig und für viele Mitarbeiter mit immensen Veränderungen verbunden, die als bedrohlich wahrgenommen werden. Diese mitunter gravierenden Veränderungen im Zuge der Veränderungs- oder Entwicklungsmaßnahmen sind der Grund dafür, dass in der Belegschaft Ablehnung und Widerstand wächst. Veränderungsaversität – ein zutiefst menschliches Charaktermerkmal.

Dabei ist das Verständnis für den Wandel oder zumindest die Erkenntnis dafür, dass die Notwendigkeit für einen internen Wandel für mehr Cybersicherheit besteht, Grundvoraussetzung.

Durchlaufen Unternehmen den Transformationsprozess zur nachhaltigen und möglichst sicheren (Update-)Digitalisierung, sind die Anforderungen tatsächlich vielfältig. Denn zwar sind die Chancen zur Verbesserung groß, aber die Risiken sind es eben auch. Zielkonflikte, Verlust von Macht und Kontrolle, Entwertung von Mitarbeiter-Know-how sind wesentliche Aspekte, die plötzlich hervorbrechen können. Sie können das Vorhaben, den Wandel zum Schutz vor Internetangriffen voranzutreiben, ernsthaft gefährden.

Autoren wie Dietmar Vahs, Lutz Rosenstiel, Martin Claßen und Miriam Landes beschäftigen sich seit Jahren mit psychologischen und soziologischen Prozessen in Organisationen, die einen Wandel vollziehen und auch das Thema Cybersicherheit in den Change-Management-Prozess einbinden müsssen.

Was beispielsweise ist zu tun, wenn ein Change-Prozess die Position einer Führungskraft bedroht und die notwendigen Maßnahmen die damit verbundenen Privilegien und den Einfluss der betroffenen Person gefährdet?

Es gibt unterschiedliche Reaktionen: Hat die betroffene Person keine Möglichkeit, gestärkt oder für sich nutzbringend aus der Transformation hervorzugehen, kann der Widerstand dergestalt ausfallen, dass sie versuchen wird, zu blockieren. Oder sie versucht, Allianzen mit Gleichgesinnten zu bilden, verbreitet Halbwahrheiten und Falschmeldungen, streut Gerüchte, um die Veränderung zu negieren. Oder noch drastischer – die der Veränderung ablehnend gegenüberstehende mittlere Führungskraft versucht, eine ausgewählte Gruppe zum Widerstand zu bewegen und Veränderungsbefürworter auszuschalten.

Was tun, wenn irrationale Existenzängste betroffene Mitarbeiter auf darunterliegenden Hierarchiestufen zu Übersprungshandlungen oder in die Depression treiben? Was tun, damit Menschen nicht dazu neigen, Nachteile von Veränderungen höher zu gewichten als Vorteile?

Fest steht: Veränderungsprozesse, insbesondere im Bereich der Cybersicherheit, können eine enorme Belastungsprobe für Organisationen und Mitarbeiter aller Hierarchieebenen sein.

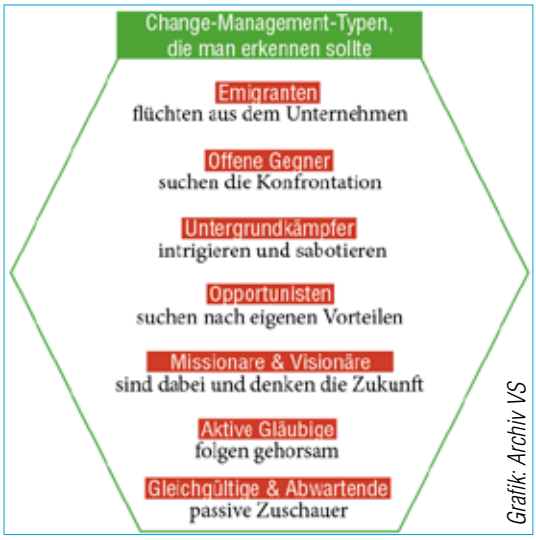
Cybersicherheit ist Chefsache. Ein Satz, der fast

gebetsmühlenartig herumgeht und auch von Experten des BSI, Polizei und Verfassungsschutz immer wieder betont wird.

Zwar müssen obere Hierarchieebenen nicht die Tiefen der IT verstehen, um Cybersicherheit bestmöglich zu gewährleisten. Aber sie sollten im Sinne von Nachhaltigkeit und wirtschaftlichem Überleben der Organisation aufzeigen, dass und welche Vorteile des Wandels weit überwiegen werden (eine Aufgabe, die meist Change Managern zufällt, die sich damit nicht beliebt machen und neben ihrer Vermittlungsaufgabe zusätzlich um Akzeptanz kämpfen müssen).

Es liegt in der Natur der Sache, dass in einem Prozess des Wandels für Cybersicherheit Verantwortliche im Rampenlicht stehen und Aufmerksamkeit erfahren. Sehr schnell kann dann deutlich werden, dass es Zielkonflikte zwischen Führungskräften gibt, die von Mitarbeitern zwar differenziert betrachtet werden, aber Gleiches bewirken: Es bilden sich unterschiedliche Widerstandstypen (Grafik), die von den Leitenden identifiziert werden müssen, um sie wieder „einzufangen". Gelingt das nicht, besteht auch hier das Risiko, dass der Change-Prozess scheitert. In Hierarchie-getriebenen Organisationen (Bundeswehr, Polizei) sind Widerstände oberflächlich leichter zu besiegen, weil Befehlsstrukturen einen engeren Rahmen vorgeben.

— Text: Maria Strenge



Grafik: Archiv VS

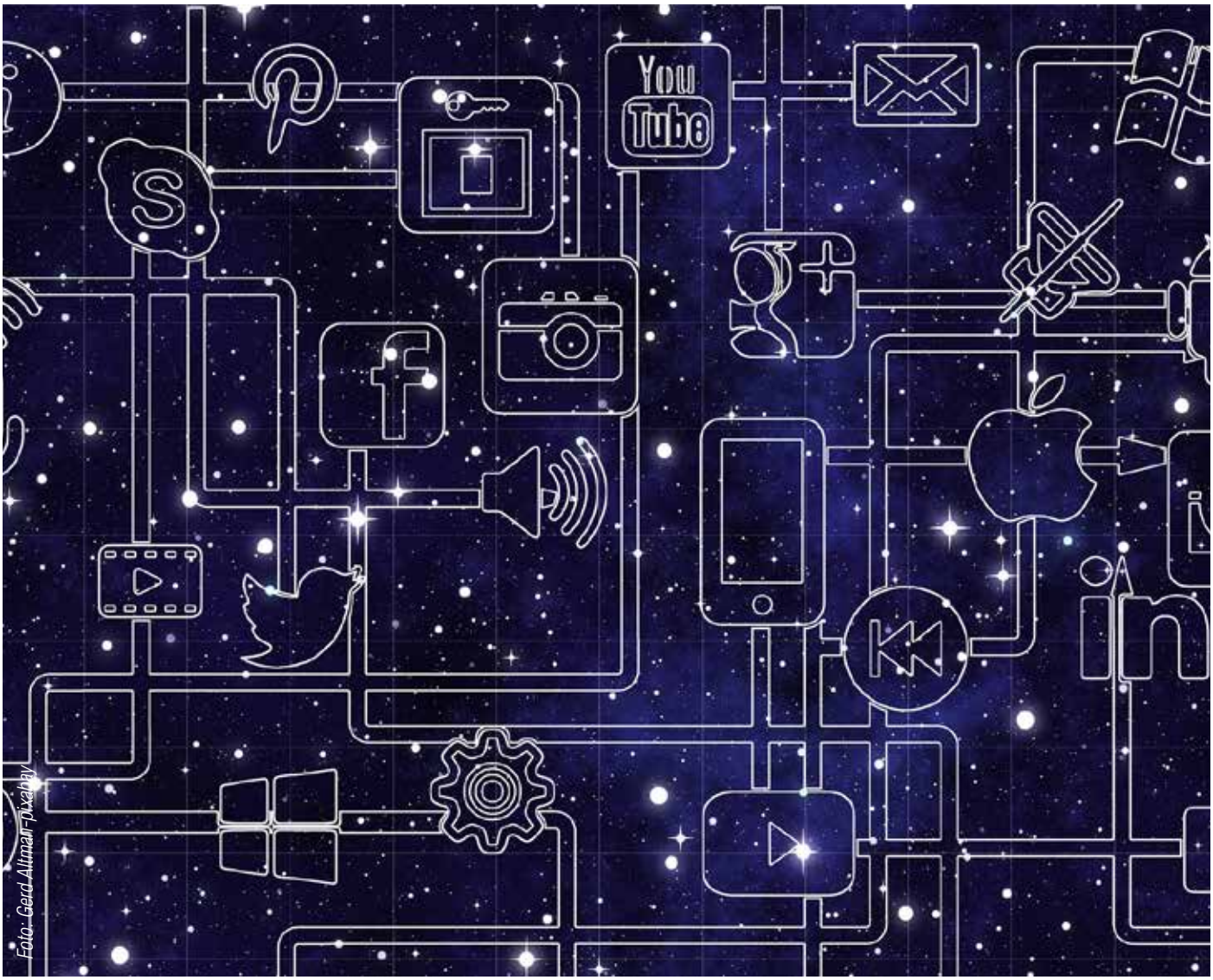


Foto: Gerd Altmann/pixabay

• Analysen | Berichte | Reportagen | Shorties • 4 x im Jahr | 60 Seiten | digital •

Teilen Sie Ihr Wissen – als „Content Pate“ oder auf der „Common Content Journey“ > Mediadaten

! Mit uns erreichen Sie reichweitenstarke Partner !

Ehrgeiz – eine Eigenschaft, die Fluch oder Segen sein kann

Change Management im Bereich Cybersicherheit ist längst kein rein technisches Thema mehr, sondern eine strategische Disziplin, die tief in die Unternehmenskultur eingreift. Der Faktor Ehrgeiz spielt dabei eine ambivalente, aber entscheidende Rolle. Ehrgeiz kann Transformation für Cybersicherheit beschleunigen – oder sie gefährlich verzerren.

Im Kern beschreibt Change Management im Kontext der Cybersicherheit die systematische Planung, Umsetzung und Stabilisierung von Veränderungen, die darauf abzielen, Organisationen widerstandsfähiger gegen digitale Bedrohungen zu machen. Diese Veränderungen betreffen nicht nur Technologien, sondern auch Prozesse, Verantwortlichkeiten und vor allem das Verhalten von Menschen. Genau hier entfaltet Ehrgeiz seine Wirkung.

Ein gesund ausgeprägter Ehrgeiz auf individueller wie organisationaler Ebene kann als treibende Kraft fungieren. Unternehmen, die den Anspruch haben, Vorreiter in der Cybersicherheit zu sein, investieren proaktiv in Innovationen, entwickeln robuste Sicherheitsarchitekturen und fördern kontinuierliches Lernen. Führungskräfte mit Ehrgeiz setzen ambitionierte Ziele, etwa die Etablierung einer „Zero-Trust"-Kultur oder die vollständige Integration von Security-by-Design in alle Geschäftsprozesse.

Dieser Ehrgeiz kann Mitarbeitende motivieren, über Mindestanforderungen hinauszugehen und Sicherheitsbewusstsein als einen Teil ihrer professionellen Identität zu begreifen.

Gleichzeitig birgt Ehrgeiz Risiken. Übersteigerter Ehrgeiz kann zu unrealistischen Zielsetzungen führen, die den Veränderungsprozess aushöhlen. In der Cybersicherheit zeigt sich dies beispielsweise, wenn Organisationen versuchen, in kurzer Zeit komplexe Sicherheitsframeworks zu implementieren, ohne die notwendige Reife oder Ressourcenbasis zu besitzen. Das Ergebnis sind fragmentierte Lösungen, Schatten-IT oder Widerstand innerhalb der Belegschaft. Ehrgeiz kann in Aktionismus umschlagen, der mehr Unsicherheit als Sicherheit schafft.

Ein weiterer kritischer Aspekt ist der persönliche Ehrgeiz von Entscheidungsträgern. Wenn Cybersicherheitsinitiativen primär dazu dienen, individuelle Karrieren zu fördern oder kurzfristige Erfolge sichtbar zu machen, leidet die Nachhaltigkeit. Sicherheitsmaßnahmen werden dann eher nach ihrem „Signalwert" als nach ihrer tatsächlichen Wirksamkeit priorisiert. Das kann dazu führen, dass grundlegende, aber weniger sichtbare Maßnahmen (Schulungen oder Prozessoptimierungen) vernachlässigt werden.

Effektives Change Management muss daher Ehrgeiz kanalisieren. Es gilt, ambitionierte Ziele mit realistischen Umsetzungsstrategien zu verbinden. Transparente Kommunikation, partizipative Entscheidungsprozesse und eine klare Priorisierung sind entscheidend, um Ehrgeiz in konstruktive Bahnen zu lenken. Gleichzeitig sollten Organisationen eine Kultur fördern, in der Fehler als Lernchancen verstanden werden. Gerade in der Cybersicherheit, wo sich Bedrohungen ständig weiterentwickeln, ist Anpassungsfähigkeit wichtiger als Perfektion.

Man darf sagen, dass Ehrgeiz im Change Management für Cybersicherheit sowohl Motor als auch potenzielle Störquelle ist. Sein Wert hängt davon ab, wie bewusst er gesteuert wird. Richtig eingesetzt, kann Ehrgeiz Organisationen dazu befähigen, nicht nur auf Bedrohungen zu reagieren, sondern ihnen voraus zu sein. Unreflektiert kann er genau jene Stabilität untergraben, die Cybersicherheit aber gewährleisten soll.

Hinzu kommt: In der digitalen Wirtschaft gilt Vertrauen als eine der zentralen Währungen. Markenwert, Kundenbindung und Marktposition hängen zunehmend davon ab, wie sicher und verlässlich ein Unternehmen wahrgenommen wird. Genau hier entsteht ein strukturelles Spannungsfeld: Die Angst vor Reputationsschäden führt dazu, dass Cyberangriffe nicht oder nur verzögert gemeldet werden.

Aus ökonomischer Sicht ist dieses Verhalten zunächst rational erklärbar. Ein öffentlich gewordener Sicherheitsvorfall kann unmittelbare finanzielle Konsequenzen haben – etwa durch Kursverluste, Vertragskündigungen oder den Rückgang von Kundenvertrauen. Besonders in stark regulierten oder wettbewerbsintensiven Branchen besteht die Sorge, dass Transparenz über Schwachstellen als Zeichen von Managementversagen interpretiert wird. Unternehmen wägen daher häufig ab, ob die kurzfristigen Kosten einer Offenlegung höher sind als die potenziellen Risiken einer Nichtmeldung.

Diese Risikoabwägung wird durch psychologische Faktoren verstärkt. Entscheidungsträger neigen dazu, Reputationsverluste zu überschätzen, während sie die langfristigen Folgekosten mangelnder Transparenz unterschätzen. Hinzu kommt ein interner Druck: Wer einen Vorfall meldet, macht ihn sichtbar – und setzt sich damit möglicher Kritik aus. In Organisationen mit leistungsorientierter Kultur kann dies dazu führen, dass Sicherheitsprobleme bewusst kleingehalten oder verzögert kommuniziert werden.

Langfristig erweist sich diese Strategie jedoch oft als wirtschaftlich kontraproduktiv. Nicht gemeldete Cyberangriffe können sich ausweiten, größere Schäden verursachen und im schlimmsten Fall später doch öffentlich werden – dann allerdings unter deutlich ungünstigeren Umständen. Der Vertrauensverlust fällt in solchen Fällen gravierender aus, weil neben dem Sicherheitsvorfall auch mangelnde Transparenz und Governance infrage gestellt werden. Zudem können regulatorische Sanktionen drohen, da viele Rechtsräume inzwischen Meldepflichten für Sicherheitsvorfälle vorsehen.

Auf gesamtwirtschaftlicher Ebene verschärft die Nichtmeldung von Cyberangriffen ein weiteres Problem: Informationsasymmetrien. Wenn Vorfälle nicht geteilt werden, fehlt es anderen Unternehmen und Institutionen an wichtigen Erkenntnissen über aktuelle Bedrohungen. Dadurch sinkt die kollektive Resilienz gegenüber Cyberrisiken, was wiederum die Kosten für alle Marktteilnehmer erhöht. Die Angst vor individuellem Reputationsverlust führt somit zu einem systemischen Effizienzverlust.

Ein nachhaltiger Umgang mit diesem Dilemma erfordert daher institutionelle und kulturelle Veränderungen. Klare regulatorische Rahmenbedingungen, die sowohl Meldepflichten als auch Schutzmechanismen für Unternehmen vorsehen, können Anreize zur Transparenz erhöhen. Gleichzeitig müssen Unternehmen intern eine Kultur fördern, in der die Meldung von Sicherheitsvorfällen nicht als Versagen, sondern als Teil professionellen Risikomanagements verstanden wird.

Es zeigt sich: Die Angst vor Reputationsschäden ist ein zentraler Treiber für die Nichtmeldung von Cyberangriffen. Kurzfristig mag dieses Verhalten ökonomisch nachvollziehbar erscheinen, langfristig untergräbt es jedoch sowohl den eigenen Unternehmenserfolg als auch die Stabilität des gesamten digitalen Ökosystems.

Die Stabilität des digitalen Ökosystems leidet vor allem deshalb, weil Cybersicherheit kein isoliertes Gut einzelner Unternehmen ist, sondern stark von Vernetzung und Informationsaustausch abhängt. Wenn Cyberangriffe aus Angst vor Reputationsschäden nicht gemeldet werden, entstehen mehrere systemische Effekte, die sich gegenseitig verstärken.

Erstens führt fehlende Transparenz zu einer gefährlichen Form von kommunikativer Schieflage. Bedrohungen, Angriffsmuster und Schwachstellen verbreiten sich oft schnell über Branchen hinweg. Wird ein Angriff nicht offengelegt, fehlt anderen Akteuren die Möglichkeit, präventive Maßnahmen zu ergreifen. Das kollektive Lernen bleibt aus – ein zentraler Mechanismus, um Sicherheitsniveaus effizient zu erhöhen. Dadurch wiederholen sich Angriffe leichter und treffen immer neue Ziele.

Zweitens untergräbt Nichtmeldung die Prinzipien kollektiver Resilienz. In einem digitalen Ökosystem sind Unternehmen, Behörden und Dienstleister eng miteinander verbunden – über Lieferketten, Cloud-Infrastrukturen oder Plattformökonomien. Ein erfolgreicher Angriff auf ein Unternehmen kann sich entlang dieser Verbindungen ausbreiten. Wenn der ursprüngliche Vorfall nicht gemeldet wird, bleiben Kaskadeneffekte unsichtbar und unkontrolliert. Das System verliert die Fähigkeit, frühzeitig zu reagieren und Schäden einzudämmen.

Drittens entstehen Fehlanreize auf Marktebene. Wenn Unternehmen negative Konsequenzen der Offenlegung fürchten, während das Verschweigen kurzfristig „belohnt“ wird, etabliert sich ein intransparenter Zustand. Unternehmen investieren möglicherweise weniger in tatsächliche Sicherheit und dafür mehr in Reputationsmanagement. Das verzerrt den Wettbewerb: Nicht die sichersten, sondern die kommunikativ geschicktesten Akteure erscheinen vertrauenswürdig.

Viertens beeinträchtigt mangelnde Meldedisziplin die Qualität regulatorischer und politischer Entscheidungen. Gesetzgeber und Aufsichtsbehörden sind auf belastbare Daten angewiesen, um Risiken realistisch einzuschätzen und geeignete Maßnahmen zu entwickeln. Wenn ein erheblicher Teil der Vorfälle unsichtbar bleibt, basieren Strategien auf Unvollständigkeit.

Schließlich entsteht ein Vertrauensproblem auf systemischer Ebene. Wird bekannt, dass Unternehmen Vorfälle systematisch zurückhalten, sinkt das Vertrauen in digitale Infrastrukturen insgesamt. Nutzer, Investoren und Partner beginnen, die Verlässlichkeit von Systemen grundsätzlich infrage zu stellen. Vertrauen ist jedoch die Grundlage für digitale Interaktion – ohne sie steigen Transaktionskosten, Innovationen werden gebremst und die wirtschaftliche Dynamik nimmt ab. Die Nichtmeldung von Cyberangriffen schwächt das digitale Ökosystem, weil sie kollektives Lernen verhindert, Risiken verschleiert und Fehlanreize schafft. Was auf individueller Unternehmensebene wie ein Schutzmechanismus wirkt, führt im Gesamtsystem zu höherer Verwundbarkeit und geringerer Stabilität.

— Text: Vivian Simon

Grafik: freepik

Cybersicherheit ist von der Bewertung des Risikos abhängig

Kulturelle Distanzen werden auch langfristig eine strukturelle Schwachstelle in der Cybersicherheit bleiben, weil sie nicht nur Unterschiede in Sprache oder Arbeitsweise beschreiben, sondern tief verankerte Divergenzen in Wahrnehmung, Risikobewertung und Verhalten haben. Diese Unterschiede lassen sich weder vollständig standardisieren noch technisch eliminieren – und genau darin liegt ihr sicherheitsrelevantes Risiko.

Ein zentraler Faktor ist die unterschiedliche Bewertung von Risiken. In einigen Kulturen wird Sicherheit als strikte Regelbefolgung verstanden, während in anderen Flexibilität und pragmatische Lösungen höher gewichtet werden. In der Praxis heißt das, dass Sicherheitsrichtlinien zwar global definiert, aber lokal unterschiedlich interpretiert werden. Ein Beispiel: Ein multinationales Unternehmen führt strenge Zugriffsrichtlinien ein. Während Mitarbeitende in einem Land diese strikt einhalten, sehen andere sie als hinderlich für effizientes Arbeiten und umgehen sie durch informelle Lösungen wie das Teilen von Zugangsdaten. Aus technischer Sicht ist das ein Verstoß – aus kultureller Sicht ein pragmatischer Kompromiss.

Ein zweiter Aspekt ist Kommunikation. Cybersicherheit lebt von klarer, schneller und eindeutiger Informationsweitergabe – insbesondere im Incident Response (Reaktion auf einen Sicherheitsvorfall). Kulturelle Unterschiede in Kommunikationsstilen können zu Verzögerungen oder Missverständnissen führen. In hierarchisch geprägten Kulturen könnte ein Sicherheitsvorfall nicht sofort gemeldet werden, weil Mitarbeitende zunächst interne Abstimmungen suchen oder negative Konsequenzen fürchten. In direkt kommunizierenden Kulturen hingegen wird ein Vorfall schnell deeskaliert. Diese Unterschiede können im Ernstfall entscheidend sein, dennMinuten oder Stunden der Verzögerung vergößern den Schaden erheblich.

Auch der Umgang mit Fehlern variiert kulturell stark. In Organisationen oder Regionen, in denen Fehler mit Schuldzuweisung verbunden sind, ist die Wahrscheinlichkeit hoch, dass Sicherheitsvorfälle verschwiegen oder heruntergespielt werden. Das verstärkt genau jene Dynamik, die Cybersicherheit schwächt: fehlende Transparenz und verzögertes Lernen. Beispiel Phishing-Attacke: In einer „fehlerintoleranten“ Kultur wird ein Mitarbeiter, der auf einen Angriff hereingefallen ist, den Vorfall eher nicht melden. In einer offenen Lernkultur hingegen wird der Vorfall als Chance zur Verbesserung genutzt.

Ein weiterer kritischer Punkt ist die unterschiedliche Wahrnehmung von Autorität und Verantwortung. In manchen Kulturen wird Verantwortung klar entlang von Hierarchien definiert, während in anderen Eigeninitiative erwartet wird. In der Cybersicherheit kann das zu Lücken führen: Wenn sich niemand explizit zuständig fühlt oder Entscheidungen

aus Respekt vor Hierarchien verzögert werden, entstehen Angriffsflächen. Umgekehrt kann zu viel individuelle Autonomie ohne klare Leitlinien ebenfalls Risiken erzeugen, etwa durch unkoordinierte IT-Lösungen („Schatten-IT“).

Hinzu kommt die globale Vernetzung von Lieferketten und Dienstleistern. Unternehmen arbeiten mit Partnern aus unterschiedlichen kulturellen Kontexten zusammen, die jeweils eigene Sicherheitsstandards und -praktiken haben. Ein häufiges Beispiel sind externe IT-Dienstleister: Während ein Auftraggeber hohe Sicherheitsanforderungen definiert, werden diese vom Dienstleister ggf. anders priorisiert oder umgesetzt. Solche Diskrepanzen sind kaum vollständig zu kontrollieren und können Einfallstor für Angriffe sein.

Lässt sich das Problem auflösen? Nur schwer, da kulturelle Unterschiede nicht einfach „wegtrainiert“ werden können. Sie sind das Ergebnis historischer, sozialer und wirtschaftlicher Entwicklungen. Selbst bei global standardisierten Prozessen bleibt die Umsetzung immer lokal geprägt. Zudem verändern sich digitale Bedrohungen schneller als kulturelle Anpassungsprozesse, wodurch eine dauerhafte Herausforderung entsteht.

Das bedeutet jedoch nicht, dass Organisationen machtlos sind. Erfolgreiche Strategien setzen nicht auf die Angleichung von Kulturen, sondern auf bewusste Integration: klare Mindeststandards, kombiniert mit lokal angepasster Umsetzung; interkulturelle Trainings, die nicht nur Wissen, sondern Verständnis fördern; Sicherheitskonzepte, die menschliches Verhalten einbeziehen. Eine zentrale Erkenntnis lautet: Kulturelle Distanz ist kein temporäres Problem, sondern eine konstante Rahmenbedingung globaler Zusammenarbeit. In der Cybersicherheit bleibt sie deshalb eine dauerhafte Gefahrenquelle. Nicht, weil sie per se negativ ist, sondern weil Angreifer die Unterschiede gezielt ausnutzen können. — Text: Wilko Karl

Kulturelle Unterschiede

Arbeiten Unternehmen mit Partnern aus unterschiedlichen kulturellen Kontexten zusammen, hat jeder seine eigenen Sicherheitsstandards und -praktiken. Für diese **Herausforderung** braucht es immer wieder neue Lösungen.

Grafik: freepik

Juristen haben ein neues Thema im Fokus: interne Untersuchungen

In Rechtsabteilungen von Unternehmen gehört ein hohes Arbeitspensum zum Alltag, über Langeweile wird sich kaum jemand beschweren können. Nun kommt, Tendenz steigend, ein weiteres Arbeitsfeld hinzu, dass Juristen sogar weltweit beschäftigt: interne Untersuchungen.

Sie sind laut dem „General Counsel Report 2026“ der Unternehmensberatung FTI Consulting und Relativity im vergangenen Jahr zum Rechtsthema mit dem stärksten Zuwachs geworden. In 2025 lagen interne Untersuchungen nicht einmal unter den fünf größten Themenfeldern in Rechtsabteilungen.

„Die Dynamik speist sich aus mehreren parallel laufenden Entwicklungen“, sagt Stefan Heissner, Leiter des Bereichs Forensic & Litigation bei FTI Consulting in Deutschland, Österreich und der Schweiz. „Seit die EU-Hinweisgeberrichtlinie Unternehmen verpflichtet, Meldekanäle vorzuhalten und jeder Meldung nachzugehen, kommt ein verlässlicher Zustrom an Hinweisen herein. Das Sanktionsrecht wird kleinteiliger, und Aufsichtsbehörden erwarten immer früher belastbare Ergebnisse. Der Druck wird in den kommenden zwölf bis 24 Monaten weiter steigen. In unserer forensischen Arbeit zeigt sich: Wer Zuständigkeiten, Dokumentation und Team nicht vor dem Tag des Ermittlerbesuchs aufgestellt hat, verliert in Untersuchungen schnell die Kontrolle.“

Hinzu kommt, dass relevante Inhalte heute über Kollaborationsplattformen, Cloud-Dienste und verlinkte Dokumente hinweg entstehen. 47 Prozent der befragten Rechtsabteilungen berichten deshalb über eine neue Komplexität bei Untersuchungen, 51 Prozent bei Datenschutzvorfällen. 43 Prozent der General Counsel geben an, über neue Datenquellen (von Messengern über kollaborativ erstellte Dokumente bis hin zu Inhalten, die mit KI erstellt wurden) sehr besorgt zu sein.

„Die Datenlandschaft in Unternehmen hat sich tiefgreifend verändert“, sagt Renato Fazzone, Co-Leiter des Technologie-Segments bei FTI Consulting in Europa (EMEA). „Ein verlinktes Dokument ist kein fester Anhang mehr, sondern verweist auf eine Datei, die sich später erneut ändert. Im Streitfall lässt sich dann kaum belegen, was der Empfänger an einem bestimmten Tag tatsächlich gesehen hat. Dasselbe gilt für Chatverläufe in Kollaborationsplattformen und für die Spuren generativer KI, von der Eingabe bis zum maschinell erzeugten Entwurf.“

Eine Sorge von Juristen

43 Prozent der befragten Juristen geben an, über neue Datenquellen (von Messengern über kollaborativ erstellte Dokumente bis hin zu Inhalten, die mit KI erstellt wurden) sehr besorgt zu sein.

Welche Vorgaben Rechtsabteilungen verfolgen, hängt von der jeweiligen Region ab.

63 Prozent der Befragten verfolgen die Entwicklung der Datenschutzregeln in der EU intensiv, im Vorjahr waren es noch 44 Prozent. Den EU AI Act verfolgen 47 Prozent, 35 Prozent waren es im Vorjahr.

In den USA laufen die Signale auseinander: Neue Datenschutz-Gesetzesvorhaben auf Bundes- und Bundesstaatenebene gewinnen an Aufmerksamkeit und werden inzwischen jeweils von 33 Prozent verfolgt, nach 15 Prozent im Vorjahr. Zugleich rechnet nahezu ein Viertel (23 Prozent) damit, dass eine Abschwächung der Regulierung unter der aktuellen US-Regierung die Kontrolle in anderen Rechtsräumen verschärfen werde, statt den Druck insgesamt zu senken. Wie unübersichtlich das alles geworden ist, zeigt auch, dass der Anteil der Juristen, die die geopolitische Unsicherheit als Risiko sehen, von zwölf auf 37 Prozent gestiegen ist.

Anzunehmen, dass die Entwicklungen in den USA nur die USA betrefffen, ist ein Irrtum.

„Wenn in den USA der regulatorische Druck nachlässt, wird es für international tätige Unternehmen nicht ruhiger“, sagt Stefan Heissner. „Am deutlichsten ist das bei der Korruptionsverfolgung: Wo die US-Regierung sie per Erlass zurückgefahren hat, haben sich Behörden aus Großbritannien, Frankreich und der Schweiz zu einer Anti-Korruptions-Taskforce zusammengeschlossen. Der Prüfungsdruck verschwindet also nicht, er verlagert sich.“

— Text: Simon/FTI

Analyse
Informationsbesitz ist nicht gleich Kompetenz

Heutzutage sind wir nur einen Klick von globalem Wissen entfernt. Suchmaschinen, Datenbanken und KI-Systeme liefern uns in Sekundenschnelle Antworten auf fast jede erdenkliche Frage.

Wirklich wahr?

Bei genauer Betrachtung und der Bereitschaft, den gesunden Menschenverstand einzusetzen, kommt es unweigerlich zu der Erkenntnis, dass dieser weitgehend unbegrenzte Zugang zu Daten zu einem fatalen Trugschluss führt: Menschen verwechseln den Besitz von Informationen mit dem Besitz von Kompetenz. Wieviele es sind – unklar. Wo sie sind – auf der ganzen Welt zu finden.

Der fundamentale Unterschied zwischen Information und Kompetenz entscheidet darüber, ob Wissen ungenutztes Kapital bleibt oder in echten Erfolg umgemünzt wird.

Um den Unterschied besser zu verstehen, hilft der Blick auf das Grundsätzliche der beiden Begriffe.

Information ist ein externes, passives Gut. Es entsteht, wenn Rohmaterial wie Zahlen, Zeichen oder Symbole in einen Kontext gesetzt werden und dadurch eine Bedeutung erhalten.

Beispiel: Die Zahl „120“ allein, bestehend aus drei Ziffern mit mathematischer Bedeutung, steht ohne Wert. Der Satz „Die zulässige Höchstgeschwindigkeit beträgt 120 km/h“ ist eine Information. Ihre Eigenschaft ist, dass sie digitalisiert, gedruckt, transportiert und kopiert werden kann. Sie existiert unabhängig von Menschen auf verschiedenen Medien und Technologien ihrer Zeit. Vor Jahrtausenden in Stein gemeißelt, heutzutage flüchtig zwischen 0 und 1.

Kompetenz hingegen ist eine interne, aktive Fähigkeit. Sie beschreibt das Vermögen einer Person, in komplexen, unvorhersehbaren Situationen selbstorganisiert und zielgerichtet zu handeln. Kompetenz verbindet theoretisches Wissen mit praktischem Können, Werten, Erfahrungen und der Motivation, ein Problem tatsächlich zu lösen.

Beispiel: Ein Auto bei Starkregen und Aquaplaning bei einer Geschwindigkeit von 120 km/h sicher auf der Straße halten zu können. Die Chance, dass das gelingt, setzt voraus, dass die Person, die das Auto fährt, über die grundsätzliche Kompetenz verfügt, die gefährliche Situation zu meistern – unabhängig davon, wie hochtechnisch ausgestattet das Fahrzeug ist. Die Fähigkeit „Kompetenz“ ist an Personen gebunden. Man kann sie nicht herunterladen, kopieren oder per USB-Stick übertragen. Sie zeigt sich ausschließlich in der Performance – im realen Handeln.

Der Wirtschaftswissenschaftler Prof. Dr. Klaus North entwickelte das Modell der „Wissenstreppe“, das den hierarchischen Weg von der bloßen Wahrnehmung bis zum wettbewerbsrelevanten Handeln visualisiert. Er lehrte bis 2020 Internationale Unternehmensführung an der Wiesbaden Business School, Hochschule RheinMain. Die Wissenstreppe hilft, eine datengetriebene Wertschöpfung zu verstehen.

Traditionelle Bildungssysteme fragen die reine Information ab. Wer Fakten für eine Klausur auswendig lernt („Bulimie-Lernen“), besitzt kurzfristig viel Information.

Sobald diese Schüler / Studenten aber vor einem unvorhergesehenen Problem stehen, scheitern sie oft. Moderne Pädagogik setzt daher auf Kompetenzorientierung: Nicht das Abfragen von Definitionen steht im Vordergrund, sondern das Lösen von Fallstudien und Projekten. Das spiegelt auch die Berufswelt wider: Unternehmen klagen selten über einen Mangel an informierten Mitarbeitern. Dank Google und internen Wikis weiß theoretisch jeder, wie beispielsweise Projektmanagement funktioniert. Was fehlt, sind vielerorts kompetente Mitarbeiter – Menschen, die ein zerstrittenes Projektteam wieder auf Kurs bringen, knappe Budgets jonglieren und unter Stress die richtigen Entscheidungen treffen.

— Text: Wilko Karl

Foto: VSimon, Grafik: Symbolbild / KI, Archiv Simon

Medizinprodukte sind vernetzt und benötigen Cyberresilienz

Mit fortschreitender und sich verdichtender Digitalisierung gewinnt auch die Vernetzung von Medizinprodukten an verdienter Aufmerksamkeit.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) veröffentlichte dazu bereits einige Studien, die das Thema erörtern und stellt dabei deulich heraus, dass Cybersicherheitsaspekte frühzeitig in die Entwicklung von Medizinprodukten eingebunden werden müssten. Denn den Vorteilen vernetzter Medizinprodukte stehen erhebliche Risiken gegenüber – für Hacker und Cyberkriminelle ein wahres Eldorado.

Potenzielle technische Schwachstellen unterscheiden sich dabei nicht unbedingt von Schwachstellen anderer Industrien, so das BSI. Aber die potenziellen Auswirkungen können im Gegensatz zu anderen Industrien für die Gesundheit der Betroffenen besonders kritisch sein. Um Angriffen vorzubeugen und die Kompromittierung von eventuell betroffenen Schwachstellen eines Medizinprodukts von vornherein zu verhindern, sind nicht nur technische, sondern auch organisatorische Maßnahmen erforderlich.

Das ist eine Herausforderung, denn die Umsetzung von derlei Cybersicherheitsmaßnahmen ist vielschichtig, kostenintensiv und mit erheblichem bürokratischen Aufwand verbunden: Hersteller müssen zahlreiche regulatorische Anforderungen erfüllen und gleichzeitig innovative Produkte auf den Markt bringen. Außerdem müssen sie den gesamten Lebenszyklus der Medizinprodukte berücksichtigen.

Ein solch sogenannter Produktlebenszyklus umfasst das Design, die Entwicklung, die Implementierung, den sicheren Betrieb, die Instandhaltung und die Außerbetriebnahme. Der funktionalen Sicherheit und Verfügbarkeit der Geräte, so das BSI, gelte dabei die höchste Priorität.

Aber auch Daten müssen geschützt werden. Um das alles zu gewährleisten, existieren zahlreiche Normen, Standards und Leitfäden, die das BSI in der „Handlungsempfehlung für Hersteller von vernetzten Medizinprodukten“ strukturiert dargestellt hat. Darin enthalten sind auch Kernausrichtungen und Bedeutung der Vorgaben. Kerngedanke der Handlungsempfehlungen ist, dass bereits in der Entwicklungsphase die Prinzipien „Security by Design“ und „Security by Default“ umzusetzen seien. Ebenso elementar ist eine klare organisatorische Struktur, in der Verantwortlichkeiten für Entwicklung, Produktion, Wartung und Monitoring eindeutig zugewiesen werden – inklusive und im Besonderen das Risikomanagement.

Dass es bei vernetzten Medizinprodukten (Connected Medical Devices, IoMT – Internet of Medical Things) zahlreiche Angriffsszenarien gibt, die sowohl die Informationssicherheit als auch die Patientensicherheit gefährden können, ist noch immer nicht ausreichend im Bewusstein bei allen Herstellern verankert – obwohl dieser der kritischen Infrastruktur zugehörige Bereich eindeutig ein attraktives Ziel für Cyberkriminelle ist. Der unbefugte Zugriff zum Medizinprodukt, beispielsweise durch gestohlene Zugangsdaten, Standardpasswörter oder Sicherheitslücken, gehört dazu.

Sich vorzustellen, dass Angreifer mit Zugriff auf Infusionspumpen, Patientenmonitore oder einen Fernzugriff auf MRT- oder CT-Systeme erlangen könnten, braucht ein Umdenken und ein Change Management in diesem Cybersicherheitsbereich. Zumal die Folgen eines erfolgreichen Hacks fatal sein können: Manipulation von Einstellungen, Diebstahl sensibler Patientendaten, Kontrolle über das medizinische Gerät.

Das Szenario eskaliert, wenn es kriminellen Akteuren gelingt, Therapiedaten zu manipulieren und medizinische Parameter zu verändern – beispielsweise durch Verstellen von Infusionsraten, Alarmgrenzen oder durch Manipulation von Herzschrittmacher-Parametern und Beatmungseinstellungen. Für den betroffenen Patienten eine lebensbedrohliche Situation.

Eine sich immer weiter verbreitende Angriffsart, die in der Cyberresilienzstrategie berücksichtigt werden müsse, so das BSI, ist: Ransomware.

Werden Ziele wie Krankenhausserver, Bildarchivierungssysteme (PACS) oder auch Medizinprodukte (Windows/Linux-Betriebssysteme) verschlüsselt, droht ebenfalls eine lebensgefährliche Krise. Trotz eigenständigem Notfall-Kreislauf. Geräte sind nicht mehr verfügbar, Operationen müssen ggf. verschoben werden. Hinzu kommt eine Betriebsunterbrechung, die wirtschaftlich existenzbedrohend sein kann.

Eine lange Liste weiterer Angriffsszenarien ist aufgrund dieser Gefahr in Normen und Leitlinien zusammengefasst worden: unter anderem in der Norm IEC 81001-5-1 (Cybersecurity für Gesundheitssoftware und Health-IT-Netzwerke), der technischen Spezifikation AAMI TIR57, der Norm ISO/IEC 27001, der FDA Guidance on Cybersecurity in Medical Devices sowie in den Leitlinien der European Union Agency for Cybersecurity (ENISA) und des BSI. Die Dokumente beschreiben typische Bedrohungen, Risiken und geeignete Schutzmaßnahmen für vernetzte Medizinprodukte.

— Text: BSI / VS

Für das Thema „Vernetzte Medizinprodukte“ ist in dieser Ausgabe das Unternehmen QM Beratung Gesundheit Soziales aus Schleswig-Holstein Content Pate

QM Beratung Gesundheit · Soziales

VERNETZTE MEDIZINPRODUKTE

DIGITAL. INTELLIGENT. PATIENTENZENTRIERT.

Vernetzte Medizinprodukte (Connected Medical Devices) sind über Hard- und Software mit anderen Geräten, IT-Systemen oder Cloud-Diensten verbunden, um Daten auszutauschen, Prozesse zu unterstützen und die Gesundheitsversorgung sicherer, effizienter und personalisierter zu gestalten.

DIE WICHTIGSTEN VORTEILE

- **BESSERE PATIENTENVERSORGUNG** – Kontinuierliche Überwachung, schnellere Entscheidungen, personalisierte Therapien
- **HÖHERE EFFIZIENZ** – Automatisierte Abläufe, weniger Doppeluntersuchungen, optimierte Ressourcennutzung
- **KOSTENEINSPARUNG** – Weniger Komplikationen und Wiederaufnahmen, bedarfsgerechte Einsatzplanung
- **MEHR TRANSPARENZ** – Durchgängige Datenverfügbarkeit und Nachvollziehbarkeit entlang des Behandlungspfads
- **INNOVATION & FORSCHUNG** – Echtzeitdaten und Real-World-Evidence fördern Innovation und verbessern Behandlungsergebnisse

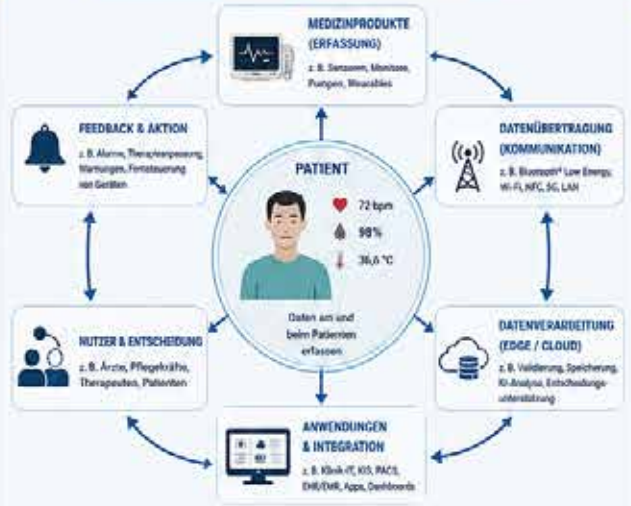
1. WAS SIND VERNETZTE MEDIZINPRODUKTE?

Vernetzte Medizinprodukte erfassen, verarbeiten und übermitteln Gesundheitsdaten und können mit anderen Geräten, Anwendungen oder IT-Systemen kommunizieren.

Beispiele:

- Infusionspumpen mit drahtloser Überwachung
- Patientenmonitoring-Systeme (EKG, SpO₂, Blutdruck, Temperatur)
- Vernetzte Insulinpumpen und CGM-Systeme
- Vernetzte Bildgebungssysteme (z. B. CT, MRT, Ultraschall)
- Wearables und Home-Monitoring-Geräte
- Vernetzte OP- und Anästhesiegeräte
- Digitale Stethoskope und Telemedizin-Stationen
- Vernetzte Rehabilitations- und Therapiegeräte

2. WIE FUNKTIONIEREN VERNETZTE MEDIZINPRODUKTE?



KOMMUNIKATION & STANDARDS

Bluetooth® Low Energy · Wi-Fi · NFC · Zigbee · 4G / 5G · LAN · HL7® / FHIR® · DICOM® · IEEE 11073 · OPC UA · OPC

Sichere, interoperable Kommunikation zwischen Geräten, Systemen und Anwendungen

3. ARCHITEKTUR VERNETZTER MEDIZINPRODUKTE

4. ANWENDUNGSBEREICHE

KONTINUIERLICHES PATIENTENMONITORING
- Echtzeitüberwachung von Vitalparametern
- Frühwarnsysteme und Alarme
- Weniger Komplikationen, höhere Sicherheit

TELEMEDIZIN & HOMECARE
- Fernüberwachung chronisch Kranker
- Telekonsultationen
- Vermeidung von Krankenhausaufenthalten

MEDIKATION & THERAPIE-MANAGEMENT
- Smart Infusionspumpen, vernetzte Inhalationsgeräte
- Therapieüberwachung und -anpassung
- Adhärenzsteigerung

INTELLIGENTES KRANKENHAUS
- Vernetzte Geräte im OP, auf Station, in der Notaufnahme
- Asset-Tracking und Standortdienste
- Automatisierte Workflows und Alarme

DIAGNOSTIK & BILDGEBUNG
- Mobiler Übertragung von Bilddaten (PACS)
- KI-unterstützte Auswertung
- Schnellere Befundung

REHABILITATION & THERAPIE
- Vernetzte Trainingsgeräte und Wearables
- Fortschrittskontrolle in Echtzeit
- Motivation und bessere Outcomes

5. DATENFLUSS-BEISPIEL (REMOTE PATIENT MONITORING)

BEISPIEL: KARDIOLOGIE

- EKG in Echtzeit
- Rhythmusüberwachung
- Ereigniserkennung
- KI-Analyse
- Warnung bei Auffälligkeiten
- Verlauf & Trends
- Therapieanpassung

6. SICHERHEIT & DATENSCHUTZ

DATENSCHUTZ NACH DSGVO UND LOKALEN GESETZEN

7. REGULIERUNG & STANDARDS

WICHTIGE REGULATORISCHE ANFORDERUNGEN
- MDR (EU) 2017/745 – Konformität & CE-Kennzeichnung
- IVDR (EU) 2017/746 – für In-vitro-Diagnostika
- ISO 13485 – Qualitätsmanagement für Medizinprodukte
- IEC 62304 – Software-Lebenszyklus
- IEC 60601-1 – Sicherheit elektrischer Medizingeräte
- IEC 82304-1 – Gesundheitssoftware
- NIS2 & Cybersecurity Act – IT-Sicherheit
- FDA Cybersecurity Guidance – (USA)

WICHTIGE INTEROPERABILITÄTS-STANDARDS
- HL7® FHIR® – moderner Datenaustausch im Gesundheitswesen
- DICOM® – für medizinische Bilddaten
- IEEE 11073 – Kommunikation medizinischer Geräte
- IHE-Profile – Integrationsprofile für den Datenaustausch

8. HERAUSFORDERUNGEN

- **CYBERSECURITY-RISIKEN** – Angriffsflächen durch vernetzte Geräte und Netzwerke
- **INTEROPERABILITÄT** – Unterschiedliche Hersteller, Protokolle und Datenformate
- **DATENSCHUTZ & COMPLIANCE** – DATENSCHUTZ & Umgang mit sensiblen Gesundheitsdaten
- **ZUVERLÄSSIGKEIT & VERFÜGBARKEIT** – VERFÜGBARKEIT & Ausfallsicherheit und stabile Konnektivität erforderlich
- **AKZEPTANZ & NUTZERÜBERNAHME** – Einfache Bedienung und nutzerzentriertes Design nutzerzentriertes Design
- **KOSTEN & ROI** – Investition, Betrieb und Nachhaltigkeit

9. ZUKUNFT VERNETZTER MEDIZINPRODUKTE

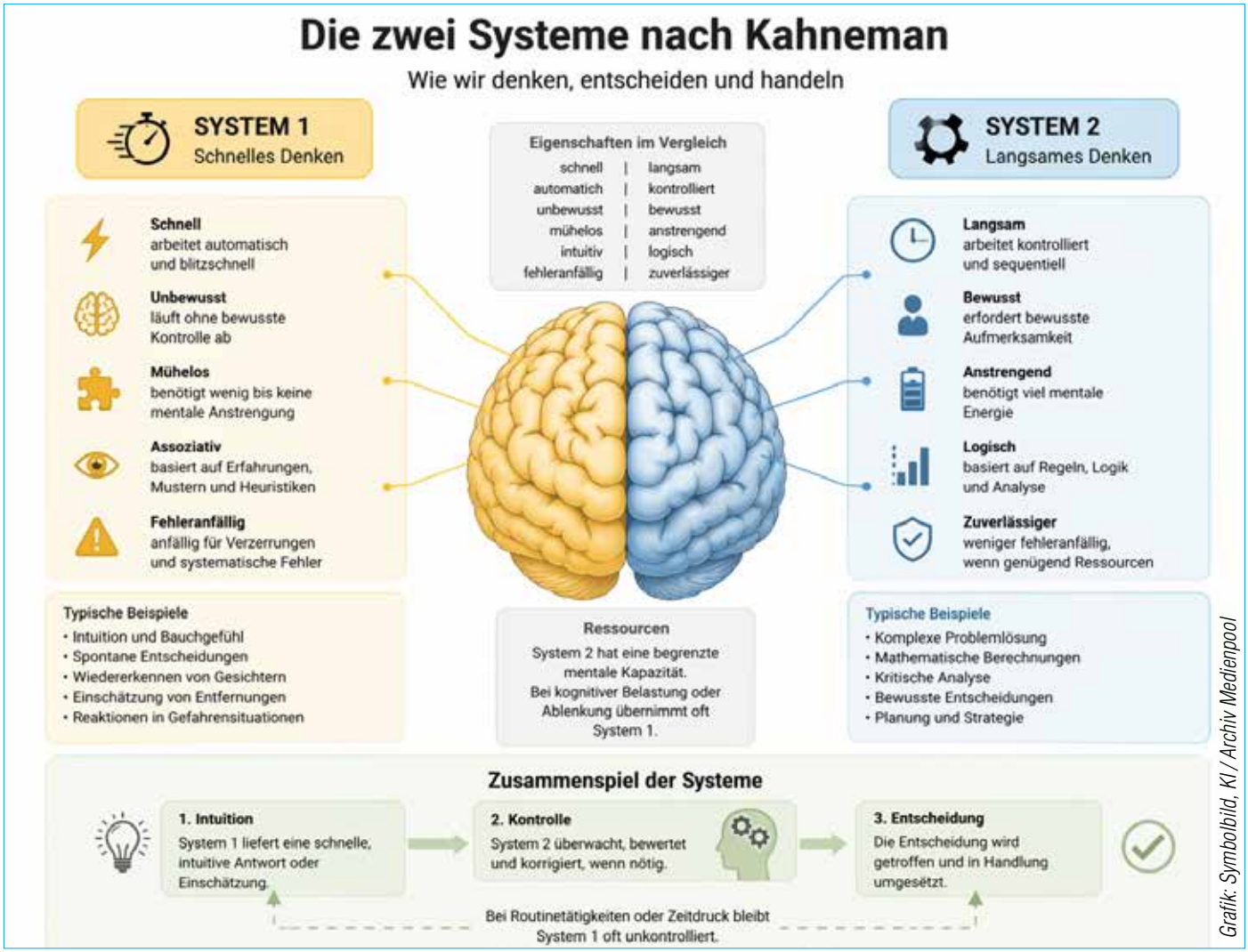
- **KI & MACHINE LEARNING** – Für Vorhersagen, Diagnostik und Personalisierung
- **DIGITALE ZWILLINGE** – Simulation, Planung und virtuelle Therapie
- **5G & IoMT** – Mehr Bandbreite, geringere Latenz, bessere Vernetzung
- **AUTONOME SYSTEME** – Selbstlernende und selbstoptimierende Geräte
- **PATIENT EMPOWERMENT** – Mehr Kontrolle, Transparenz und Selbstmanagement
- **NACHHALTIGKEIT** – Energieeffiziente Geräte und ressourcenschonend

FAZIT

Vernetzte Medizinprodukte sind der Schlüssel zu einer moderneren, sicheren und effizienten Gesundheitsversorgung. Durch sichere Vernetzung, intelligente Datenverarbeitung und nahtlose Integration entstehen echte Mehrwerte für Patienten, Leistungserbringer und das Gesundheitssystem.

VERNETZT HEILEN. BESSER VERSORGEN.

Grafik: Symbolbild, KI / Archiv Medienpool



Grafik: Symbolbild, KI / Archiv Medienpool

Zwei Systeme im Gehirn bieten die Chance, Angriffe abzuwehren

Die Frage, warum Menschen auf Cyberangriffe unterschiedlich reagieren und die einen Opfer von Hacking werden, die anderen aber nicht, beschäftigt Wissenschaftler ebenso wie kriminelle Akteure. Beide gehen dem Phänomen nach – allerdings mit unterschiedlichen Blickwinkeln. Während Angreifer ihr psychologisches Wissen nutzen, um erfolgreiche Strategien für ihre Hacks zu entwickeln, versuchen Forschende mehr Bewusstsein zum Thema in die breite Öffentlichkeit zu transportieren.

Dies indes mit mäßigem Erfolg. Ein Grund dafür könnte sein, dass in diesen herausfordernden Zeiten, die von globaler Unruhe und Kriegen sowie hybriden Gefahren geprägt sind, Menschen schlicht überfordert sind.

Ein Blick auf die von Daniel Kahneman entwickelte Theorie der zwei kognitiven Systeme könnte Erhellung in das Thema bringen.

Seine Theorie gehört zu den einflussreichsten Konzepten der modernen Kognitionspsychologie und Verhaltensökonomie. Sie beschreibt, wie menschliches Denken und Entscheiden durch zwei unterschiedliche, aber miteinander interagierende Verarbeitungsmodi geprägt werden – bezeichnet als System 1 und System 2.

System 1 operiert schnell, automatisch und weitgehend unbewusst. Es basiert auf Assoziationen, Erfahrungen sowie Heuristiken und ermöglicht es, in Alltagssituationen ohne großen kognitiven Aufwand zu reagieren. Typische Beispiele sind das spontane Erkennen von Gesichtern, das intuitive Verstehen einfacher Sätze oder schnelle Gefahreneinschätzungen – etwa, wenn wir blitzschnell beiseite springen können, weil plötzlich ein Auto heranbraust in dem Moment, den wir die Straße überqueren möchten.

System 1 ist evolutionär älter und energieeffizient,

Demgegenüber steht System 2, das langsam, kontrolliert und bewusst arbeitet. Es wird aktiviert, wenn komplexe Probleme gelöst, logische Schlüsse gezogen oder widersprüchliche Informationen verarbeitet werden müssen.

System 2 ist eng mit der individuellen Aufmerksamkeit und dem Arbeitsgedächtnis eines jeden Menschen verbunden und benötigt deutlich mehr kognitive Ressourcen. Beispiele hierfür sind mathematische Berechnungen, das kritische Überprüfen von Argumenten oder bewusst getroffene strategische Entscheidungen, die mitunter längere Bedenkzeit brenötigen.

Ein zentrales Merkmal der Theorie liegt in der Interaktion beider Systeme. In vielen Fällen liefert System 1 eine schnelle, intuitive Antwort, die von System 2 entweder bestätigt oder korrigiert werden kann.

Allerdings greift System 2 nicht immer ein, insbesondere dann nicht, wenn kognitive Ressourcen begrenzt sind bzw. keine offensichtlichen Konflikte wahrgenommen werden.

Das kann dazu führen, dass falsche Intuitionen unkritisch übernommen werden. Ein Einfallstor für Cyberkriminelle schlechthin!

Kahnemans Modell wurde im wesentlichen durch sein Werk „Thinking, Fast and Slow“ populär und empirisch durch viele Studien gestützt.

Es hat weitreichende Auswirkungen auf unterschiedliche Bereiche, darunter Ökonomie, Psychologie, Medizin sowie auch auf politische Prozesse.

Beispielsweise erklärt die Theorie auch, warum Menschen in ökonomischen Kontexten häufig von rationalen Modellen abweichen oder warum kognitive Verzerrungen in der Risikobewertung auftreten.

Trotz seiner großen Wirkung ist das Zwei-Systeme-Modell umstritten. Kritiker argumentieren, dass die Dichotomie – die Aufteilung – zwischen zwei klar getrennten Systemen eine Vereinfachung darstelle und kognitive Prozesse tatsächlich dynamischer und stärker integriert seien. Neuere Ansätze betonen daher graduelle Übergänge und Netzwerke statt getrennter Systeme.

Dennoch bleibt Kahnemans Ansatz ein grundlegendes theoretisches Rahmenwerk zum Verständnis menschlicher Kognition.

Er bietet eine Struktur, um die Spannungen zwischen intuitivem und reflektiertem Denken zu analysieren, liefert Einsichten in die Mechanismen von Urteilsbildung und Entscheidungsverhalten – auch bei ausgeklügelten Cyberangriffsmethoden.

— Text: Vivian Simon

Daniel Kahneman

1934-2024

... entstammt einer jüdisch-litauischen Familie, die namhafte Rabbiner hervorgebracht hat. Daniel Kahneman wurde in Tel Aviv geboren, lebte in den USA. Er ist Träger des Alfred-Nobel-Preises. Kahneman starb in der Schweiz.

Grafik: Symbolbild, KI / Archiv Medienpool

Cybersicherheit ist Gemeinwohl – wenn der Konsens hält

Cybersicherheit ist eine zentrale Voraussetzung für das Funktionieren moderner Staaten und damit unmittelbar mit dem Gemeinwohl verbunden. In einer zunehmend digitalisierten Welt durchdringen Informations- und Kommunikationstechnologien nahezu alle Lebensbereiche von der Energieversorgung über das Gesundheitswesen bis hin zur öffentlichen Verwaltung. Entsprechend groß sind die Risiken, die durch Cyberangriffe entstehen können – und entsprechend bedeutend ist somit die Rolle von Cybersicherheit für das Wohl der Allgemeinheit.

Ein wesentlicher Aspekt ist der Schutz kritischer Infrastrukturen: Stromnetze, Wasserversorgung, Verkehrssysteme und Krankenhäuser. Diese Systeme sind eng vernetzt und digital gesteuert. Ein erfolgreicher Cyberangriff kann hier nicht nur wirtschaftlichen Schaden verursachen, sondern auch Menschenleben gefährden. Cybersicherheit sorgt dafür, dass diese essenziellen Dienste möglichst zuverlässig funktionieren und die Bevölkerung versorgt bleibt. Sie ein Grundpfeiler staatlicher Fürsorgepflicht.

Darüber hinaus spielt Cybersicherheit eine entscheidende Rolle für den Schutz persönlicher Daten und der Privatsphäre seiner Bürger. In einer Zeit, in der enorme Mengen sensibler Informationen digital gespeichert und verarbeitet werden, ist der Schutz vor Datenmissbrauch zentral für das Vertrauen in staatliche Institutionen und Unternehmen. Nur, wenn Bürger sicher sein können, dass ihre Daten bestmöglich geschützt sind, werden individuelle Freiheit und gesellschaftliche Stabilität gestärkt.

Ein anderer Punkt ist die Sicherung demokratischer Prozesse. Wahlen, politische Kommunikation und öffentliche Meinungsbildung finden zunehmend im digitalen Raum statt. Cyberangriffe, Desinformationskampagnen und Manipulationen beeinträchtigen diese Prozesse erheblich. Eine starke Cybersicherheitsstrategie hilft, Bedrohungen zu erkennen und abzuwehren, und trägt so zur Integrität demokratischer Systeme bei.

Wirtschaftlich ist Cybersicherheit ebenfalls von großer Bedeutung. Unternehmen sind auf funktionierende IT-Systeme angewiesen, da Cyberangriffe enorme finanzielle Schäden verursachen, Innovationen behindern und Arbeitsplätze gefährden können. Ein sicherer digitaler Raum fördert hingegen Investitionen, Innovation und Wachstum. Dadurch profitieren nicht nur einzelne Unternehmen, sondern die gesamte Volkswirtschaft.

Nicht zuletzt hat Cybersicherheit auch eine außen- und sicherheitspolitische Dimension. Staaten sind zunehmend Ziel von Angriffen durch andere Staaten oder organisierte Gruppen. Diese Angriffe haben Spionage, Sabotage oder politische Destabilisierung zum Ziel. Eine starke Cybersicherheitsinfrastruktur ist daher unverzichtbarer Teil der nationalen Sicherheit und trägt dazu bei, die Souveränität eines Staates zu wahren. Ohne ausreichende Cybersicherheit wären viele Errungenschaften unserer digitalen Welt nicht nachhaltig nutzbar.

Ein zentraler Grund für die Notwendigkeit eines Konsens' liegt in der Struktur des digitalen Raums selbst. Anders als klassische Sicherheitsbereiche ist Cybersicherheit kein rein staatliches Handlungsfeld. Ein Großteil der digitalen Infrastruktur – etwa Internetprovider, Cloud-Dienste, Softwareplattformen oder industrielle Steuerungssysteme – befindet sich in privater Hand. Heißt: Selbst wenn staatliche Institutionen hohe Sicherheitsstandards etablieren, bleiben diese wirkungslos, wenn Unternehmen und andere zivile Akteure sie nicht mittragen oder umsetzen. Cybersicherheit ist ein verteiltes Verantwortungsfeld.

Staatliche Behörden, Unternehmen, Forschungseinrichtungen und Bürger sind digital eng miteinander verbunden. Eine Sicherheitslücke in einem Teil dieser Struktur kann sich schnell folgenschwer ausweiten. Ein Konsens ermöglicht es, Mindeststandards festzulegen und koordiniert zu reagieren, da Cybersicherheit auch auf Kooperation und Vertrauen basiert.

— Text: Maria Strenge

Atmen Die Brücke zwischen den Welten

Die P8, eine zuverlässige und vielseitige Präzisionswaffe, ist seit 1994 eine Standard-Dienstpistole der Bundeswehr. Sie hat ein Kaliber von neun Millimetern und dient der Selbstverteidigung im Nahkampf. Deshalb wird sie oft als Zweitwaffe geführt.

Ich habe sie das erste Mal im Sommer 2025 im Rahmen einer Dienstlichen Veranstaltung zur Information (InfoDVag) in der Panzertruppenschule des Ausbildungskommandos in Munster gehalten und war wirklich überrascht, wie viel schwerer das kleine Ding in der Hand liegt als ich dachte.

Meine Verblüffung darüber hielt an, weswegen ich Schwierigkeiten hatte, sie mit Blick auf die Zielscheibe am Ende der Schießbahn ruhig, gerade und ohne Wackelei in der Luft zu halten. Tatsächlich war auch der Rückstoß der halbautomatischen Waffe aus dem Hause Heckler & Koch erstaunlich heftig und hat mich – nicht nur beim ersten Schuss – aus dem Gleichgewicht gebracht.

Aber warum?

Ich hatte doch konzentriert auf meine Körperspannung geachtet, meine Füße fest in den Boden gepresst. Trotzdem ist es mir nicht gelungen, im wahren Wortsinn standhaft zu bleiben und die Zielscheibe zu treffen: jeder Schuss ging daneben. Ich hielt den Rekord in der ganzen Gruppe, wenn auch nicht den gewünschten.

Was habe ich falsch gemacht?

Die Antwort: Ich hatte im entscheidenden Bruchteil der Sekunde falsch oder zuviel oder gar nicht geatmet. Eines davon, was, weiß ich nicht mehr.

Atmen, diese eine unsichtbare Verbindung von Leben und Tod, die Brücke zwischen unserer inneren und äußeren Welt, ist ein Vorgang, der so selbstverständlich ist, dass wir ihn in den meisten Momenten nicht bemerken. Dabei ist es die erste Handlung, mit der wir in unser Leben eintreten, und die letzte, mit der wir die irdische Existenz verlassen. Zwischen diesen beiden Atemzügen entfaltet sich unser gesamtes Dasein. Atmen ist mehr als nur eine biologische Notwendigkeit; es ist ein ständiger, stiller Dialog zwischen Körper, Geist und Umwelt – ein meist kraftvolles Zeugnis des Lebendigseins.

Mit einer Waffe im Einsatz ist die Atmung eine Kontrollinstanz, das habe ich gelernt.

Biologisch betrachtet ist das Atmen der Prozess, durch den Sauerstoff in unseren Körper gelangt und als Kohlendioxid ausgeschieden wird. Ohne Sauerstoff kann keine Zelle überleben. Unser Atemsystem versorgt Organe, Gewebe und Gehirn mit der Energie, die sie benötigen. Dies geschieht meist ohne unser Zutun: unwillkürlich, rhythmisch, zuverlässig. Das Atemzentrum im Gehirn steuert die Frequenz und Tiefe – angepasst an Aktivität, Stress, Schlaf und Krankheit. So wird Atmen zur unsichtbaren Grundlage allen Lebens.

Für Führungskräfte aus der zivilen Gesellschaft, die ohne Waffe im Anschlag zwar anders, aber auch zielgerichtet agieren müssen, ist das Atmen eine lautlose Taktung für Momente, in den Ruhe gefragt und Stärke gefordert ist. Haben Leitende in herausfordernden Situationen ihre Atmung nicht im Griff und treten schnaufend und japsend vor ihr Team, verlieren sie Akzeptanz, Respekt und Stärke.

Indes: Menschen können lernen, bewusst zu atmen. In Situationen voller Angst oder Überforderung kann ein einziger bewusst getaner Atemzug die Grenze zwischen innerem Chaos und äußerer Klarheit ziehen. Bewusstes Atmen ist ein hilfreiches Instrument der Selbstführung – ein innerer Kompass, wenn äußere Umstände aus der Balance geraten sind oder die gar Entgleisung droht.

Die Worte „Ruach“ (hebräisch), „Pneuma“ (griechisch) oder auch „Prana“ (indisch) bedeuten nicht nur Luft und Wind – sondern Geist, Lebenshauch und Seele. Das Atmen ist Symbol des ständigen Gebens und Nehmens, des Loslassens und Empfangens. Es ist ein Prozess, der im Regelfall mehrere Jahrzehnte zuverlässig ist, bevor der Tod diese kontinuierliche Arbeit beendet. Der Atem ist die Metapher für Enge und Weite, für Kontrolle und Vertrauen.

— Text: Vivian Simon

Die Philosophie sagt …

Atmung ist eine **fundamentale Form** unserer Beziehung zur Welt. Denn mit jedem Atemzug dringt der Kosmos und die Welt in uns hinein und strömt wieder aus uns heraus.

(nach Hartmut Rosa, deutscher Soziologe)

Dackelgarage Eine Liebeserklärung an das Kult-Zelt der Bundeswehr

Es ist nicht groß, es ist nicht hübsch, aber es erfüllt in den meisten Fällen seinen Zweck und trägt einen fast niedlichen Namen, der indes nicht zum bisweilen raubeinigen und abgehärteten Umfeld passt: das Zwei-Mann-Zelt der Bundeswehr, alias Dackelgarage. Dieser liebevoll-spöttische Soldatenausdruck darf als ein Beispiel für den oft sehr trockenen Humor der Militärs genannt werden. Aber die Sache ist durchaus tiefgründiger.

In Größe und Form ist die Dackelgarage mit 1,10 Meter Höhe relativ flach, 2,30 Meter lang und ca. 1,60 Meter schmal. Insgesamt hat sie keine vier Quadratmeter Bodenfläche. Ausmaße im übertragenen Sinne, wie man sich eine Behausung für Dackel – klein und lang gezogen – vorstellen könnte. Mit ein wenig Übung, das weiß ich aus Erfahrung, kann man sich in die Unterkunft hineinhechten. Hinzukommt, dass der Dackel hauptsächlich hierzulande als Symboltier schlechthin steht: der eigenwillige Hund mit unbeugsamem Charakter steht für etwas urdeutsch Heimeliges, leicht Biederes – wie die Zeltbahn selbst, die aus schwerem, soliden Baumwollstoff besteht. Oft klamm, nie ganz dicht, aber eben immer dabei, muss man die Dackelgarage irgendwie lieb haben. Auch, wenn sie rein gar nichts Komfortables oder Gemütliches bietet. Selbst, wenn sie mit Stroh ausgelegt ist, bleibt die Bleibe höchst bescheiden. Dennoch birgt der Begriff eine gewisse Form der Selbstironie. Während „Zwei-Mann-Zelt“ nüchtern und distanziert klingt, drückt „Dackelgarage“ eine diffuse Verzweiflung und Zuneigung zugleich aus. Man lacht darüber, dass man in so einem Ding nächtigen muss – und findet es trotzdem recht schnell ziemlich okay.

Die Dackelgarage, dieses wackere Relikt aus Zeiten, in denen Männer noch „Gefechtsdienst bei Regen“ sagten, wo andere schlicht „Schietwetter“ meinen, ist der Inbegriff deutscher Outdoor-Romantik. Zwei Zeltbahnen, vier Heringe, zwei Gestängeteile und ein halbes Jahrhundert olfaktorische Wahrnehmung: ein Gemisch aus verschwitzten Nächten, stimmungsdrückendem Nieselregen und etwas Maschinenöl – „Eau de Bundeswehr“, streng limitiert.

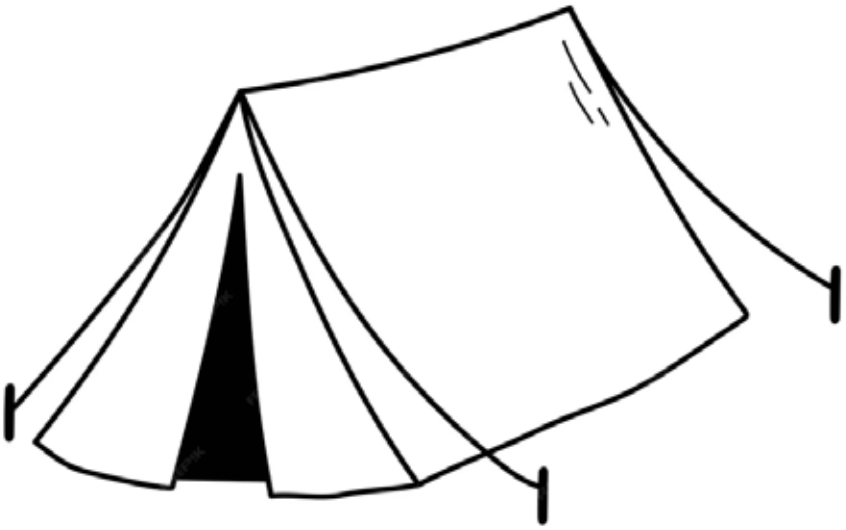
Der Aufbau ist ein Abenteuer für sich, auch davon kann ich ein kleines Lied singen. In meinem Fall: ein Oberstleutnant und ich. Wir warfen uns die Zeltbahnen zu wie Liebesbriefe in einer Fernbeziehung. Minuten später knieten wir gemeinsam im halbtrockenen Morast, kämpften mit widerspenstigen Ösen, Heringen und gestanzten Aluknöpfen. Es war nicht einfach, aber auch kein Hexenwerk. Am Ende stand sie dann da, die Dackelgarage: ein wenig windschief, der Kamerad konnte meine zivilen Fehlhandgriffe nicht ganz korrigieren, sonst hätten wir x-Male von vorn anfangen müssen. Bei einer militärischen Prüfung hätte kein Leitender das durchgehen lassen.

Interessant ist die Lüftung. Sie besteht aus dem Spalt zwischen Erdboden und Stoff und ist eine Vertrauenssache – vor allem, wenn es regnet und innen der Biofilm zu wachsen beginnt. Leben in der Lage!

Was die Dackelgarage an Komfort vermissen lässt, macht sie – ähnlich wie das durch Natur oder Zucht tiefergelegte Tier – durch Charakter wett. Wo Zelte aus dem Handel mit ultraleichtem Titan-Gestänge und atmungsaktiven Membranen wie alpine Raumstationen wirken, verheißt die Dackelgarage: „Ich bin da. Und ich bleibe. Mit dir. Bei jedem Wetter. Auch, wenn es schneit. Vor allem, wenn's schneit.“

Die Dackelgarage ist der Hero unter den Zelten, unkaputtbar – und sie sendet die Botschaft: „Du brauchst keine Thermomatte. Du brauchst Disziplin.“

— Text: Vivian Simon



Grafiken: freepik

Die Geburtsstunde eines süßen Kultgetränks: Fanta

Not macht erfinderisch. Diese Redewendung, die ursprünglich dem antiken Rom zugeschrieben wird, hat der Welt in praktischer Umsetzung so manche Erfindung beschert. Das Kultgetränk Fanta ist ein Beispiel.

Die hell-orangefarbene Limonade in der charakteristischen Ringelflasche gehört heutzutage weltweit zu den bekanntesten Erfrischungsgetränken. Coca Cola dürfte noch bekannter sein – beide gehören indes zur „gleichen Familie". Der Name «Fanta» ist sogar noch viel älter als das Getränk, das wir heute kennen.

Doch der Reihe nach.

Zweiter Weltkrieg, 1940. Der Nationalsozialismus erreicht in Deutschland den Höhepunkt seiner militärischen Macht, im sogenannten Westfeldzug überfällt die Wehrmacht Frankreich (Frankreichfeldzug) und schmiedet Kriegsallianzen mit Japan und Italien.

In der nordrhein-westfälischen Stadt Essen hält Max Keith das Zepter der deutschen Coca-Cola GmbH in der Hand und steht plötzlich vor einem existenziellen Problem. Seit 1929 war die Coca-Cola GmbH unter seiner Leitung gewachsen. Mit Eintritt der USA in den Krieg jedoch bricht die Lieferkette schlagartig zusammen und die deutsche Abfüllanlage erhält kein „7X" mehr. Jenes bis heute geheimgehaltene Konzentrat aus Atlanta, das für die Herstellung von Coca-Cola unverzichtbar ist.

Um die Fabrik vor dem Stillstand zu bewahren und Arbeitsplätze zu sichern, muss Max Keith improvisieren und holt seinen Chefchemiker Dr. Wolfgang Schetelig an die Seite. Der sollte ein neues Getränk entwickeln, das aus inländisch verfügbaren Rohstoffen hergestellt werden konnte, eine Reste-Limonade gewissermaßen. Sie bestand aus Überbleibseln der Lebensmittelindustrie, vorwiegend aus einem Nebenprodukt der Käseherstellung (Molke), ausgepressten Rückständen der Apfelwein- und Saftproduktion sowie aus Rübenzucker. Später, als auch dieser knapp wurde, wich man auf Saccharin aus. Das Ergebnis war ein gelblich-braunes, kohlensäurehaltiges Getränk, das eher nach vergorenem Apfel oder Molke schmeckte. Da die Zusammensetzung je nach Verfügbarkeit der recht bemerkenswerten Zutaten stark schwankte, änderte sich auch der Geschmack des neuen Getränkes ständig.

Damit sich das abenteuerliche Gebräu überhaupt verkaufen ließ, brauchte es einen Namen. Dieser stellte sich als ein Geniestreich des damaligen Marketings heraus: Keith berief demnach eine Sitzung ein und forderte seine Mitarbeiter auf, ihrer „Fantasie" freien Lauf zu lassen.

Grafik: VS/Medienpool

Der Legende nach rief spontan einer der Verkaufsleiter „Fanta!" in den Raum und landete sofort den Volltreffer. Kurz, prägnant, dynamisch und leicht zu merken. Der Name funktioniert bis heute in fast allen Sprachen. Alles Merkmale, die in den Köpfen der Menschen eine Durchdringungskraft erreicht.

In den Kriegsjahren stieg Fanta in Deutschland schnell zum Massenprodukt auf. Allerdings nicht unbedingt als Getränk; denn weil echter Zucker rationiert war, kauften Menschen Fanta oft zum Süßen von Suppen, Soßen und Kuchen.

1943 wurden in Deutschland mehr als drei Millionen Kisten Fanta verkauft.

Mit der Ur-Fanta hat die heutige Limonade inhaltlich nichts mehr gemein, nur der Name ist geblieben. Nach Ende des 2. Weltkrieges übernahm der US-Mutterkonzern die deutsche Tochtergesellschaft. Die Produktion von Fanta wurde zunächst komplett eingestellt, da man alle Kapazitäten für den Ausbau der Kernmarke Coca-Cola benötigte.

Das Fundament für die Alltagsmarke „Fanta", wie wir sie heute kennen, wurde 1955 in Neapel gelegt. Man suchte nach einer Möglichkeit, in der Abfüllanlage Società Napoletana Imbottigliamento Bevande ein Getränk herzustellen, das fruchtig, frisch und lokal war – sicherte sich den geschützten Namen „Fanta", veränderte Farbe und Rezeptur fundamental. Diese neue Rezeptur war so erfolgreich, dass Coca-Cola sie global übernahm. 1959 wurde die „neue" Fanta auch in Deutschland wieder eingeführt.

— Text: Vivian Simon

Ein markantes Wahrzeichen zum Abtauchen

Der Tieftauchtopf der deutschen Marine in Neustadt in Holstein zählt zu den außergewöhnlichsten militärischen Ausbildungsanlagen in Deutschland. Trotz seiner markanten Silhouette, die mit rund 42 Metern Höhe das Gelände des Marineausbildungszentrums prägt und ein Symbol für moderne Tauchtechnik und Sicherheitsausbildung ist, bleibt der Klotz visuell dennoch recht unscheinbar. Vielleicht, weil er sich mit seiner hellgrauen Farbe ein wenig in das Graublau des bedeckten Himmels schleicht und bei strahlendem Sonnenschein weggeblendet wird.

Gefüllt mit etwa 1,25 Millionen Litern Wasser, gilt der Tieftauchtopf der Marine als tiefster und modernster weltweit. In ihm befindet sich ein sieben Meter breites und 32,5 Meter tiefes Becken. Darin lernen U-Boot-Fahrer den simulierten Notausstieg aus einem gesunkenen U-Boot – und das seit seiner Inbetriebnahme in den späten 1970er-Jahren.

Die Ausbildung für den Ernstfall ist hart. Unter Wasser aus einer Pressluftleitung zu atmen – ähnlich wie es im Notfall erforderlich ist – ist eine Herausforderung. Mit der Methode sollen sich U-Boot-Fahrer im Echtfall aus bis zu 80 Meter tiefem Wasser retten können. Mit wirklichkeitsgetreuen Einbauten wie Leitern und U-Boot-Armaturen soll die Realität so real wie möglich abgebildet werden.

Grafiken: freepik

Die Bundeswehr sieht den Trainingsansatz indes ganzheitlicher. Sie sagt: Jeder Seemann ist auch ein Feuerwehrmann. Daraus resultiert ein Auftrag, der bereits den Namen des Areals weiterfasst als „Tieftauchturm“: Einsatzausbildungszentrum Schadensabwehr Marine (EAZS M). Hier lernen Marinesoldatinnen und -soldaten nicht nur, aus einem U-Boot herauszukommen – sie lernen den Kampf gegen die Elemente. Sie üben sie das Bekämpfen von Wassereinbrüchen und Feuer an Bord, um im Notfall instinktiv richtig handeln zu können.

Deshalb legt das EAZS M seinen Schwerpunkt auf die Praxis: Leck- und Brandabwehr finden im realistischen Umfeld statt, zum Beispiel in einer großen Brandhalle oder an Bord der ehemaligen Fregatte „Köln“.

Dabei üben die Seeleute, ihren eigenen Fähigkeiten zu vertrauen, aufkeimende Angst einzeln und im Team zu beherrschen.

Zusätzlich finden am EAZS M Taucher- und Rettungsmittelausbildung sowie das Training von U-Boot-Crews in der Eigenrettung statt. Dafür stehen an Land eine Schwimm- und Tauchhalle sowie eben jener berühmte Tieftauchtopf zur Verfügung. Für die praktische Taucherausbildung in See verfügt das Zentrum über zwei Schulboote. Weitere Lehrgänge umfassen den Sanitätsdienst im Gefecht und die Abwehr atomarer, biologischer oder chemischer Kampfstoffe, kurz ABC-Abwehr.

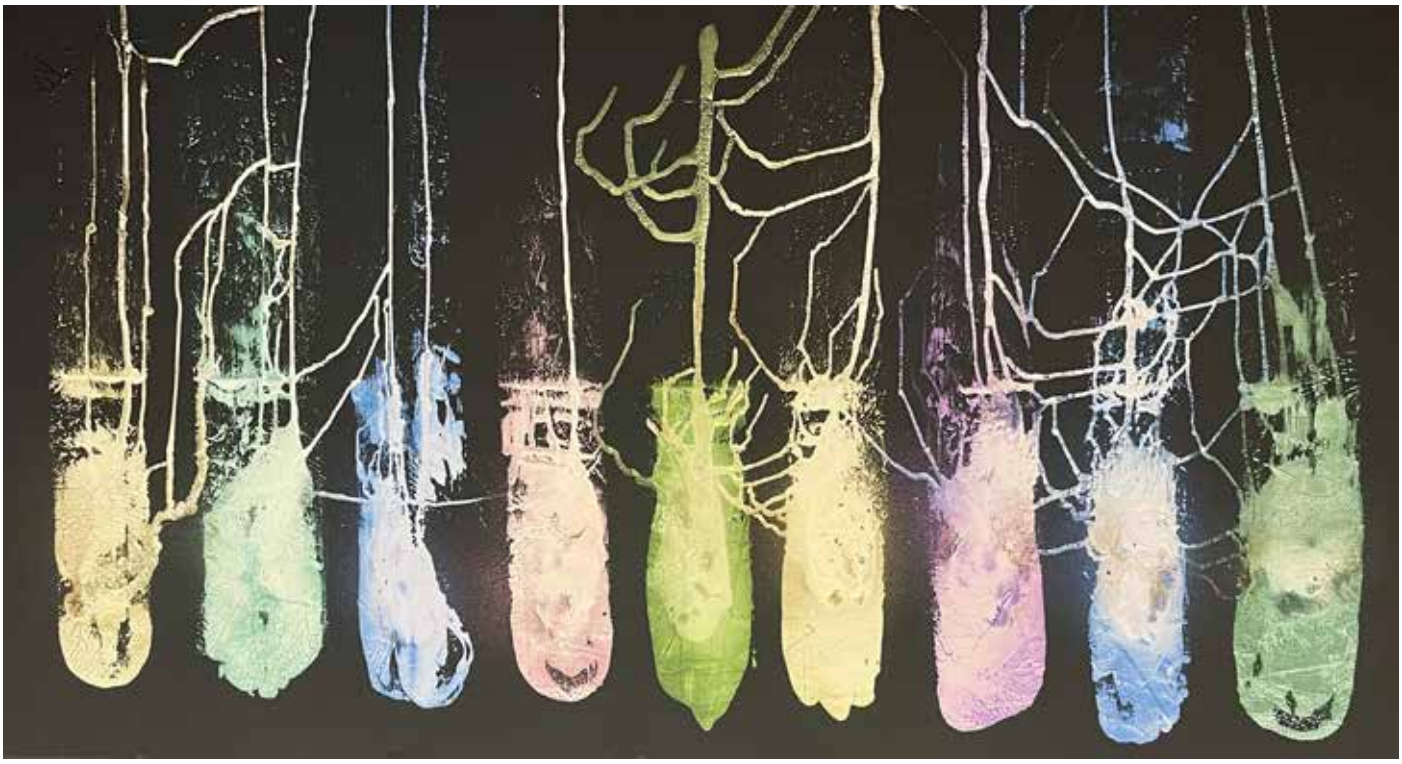
Neben diesem Individual- und Teamtraining betreut das EAZS M auch komplette Besatzungen an Bord ihrer Schiffe und Boote – in der Schadensabwehr-Gefechtsdienst-Ausbildung in der Lübecker Bucht der westlichen Ostsee. Diese ganzheitliche Gefechtsausbildung von Kriegsschiffen samt Crews bezieht militärische Aspekte, den Sanitätsdienst und das Beheben von allen möglichen technischen Schäden ein. Sie simuliert parallel das „äußere Gefecht“ – den Kampf mit einem Gegner – und das „innere Gefecht“ – den Umgang mit Treffern im eigenen Schiff.

Aber nicht nur die Soldaten stehen vor der Herausforderung im Training. Ein anderer Player, der beim Tieftauchturm mitgewirkt hat, stand auch davor: das Gebäudemanagement Schleswig-Holstein (GM.SH), Anstalt des öffentlichen Rechts.

Das GM.SH übernimmt staatliche Bauherren- und Planungsaufgaben für Land und Bund in Schleswig-Holstein und ist auch zuständig für die Bewirtschaftung der vom Land genutzten Liegenschaften und für die Beschaffung von Material und Leistungen für die Landesbehörden. Da die Leistungen nach wirtschaftlichen Grundsätzen erbracht werden, ist das GM.SH nach den Prinzipien eines modernen Unternehmens organisiert. Ein Wettbewerb mit Privaten ist nicht ihr Ziel. Im Vordergrund steht die Partnerschaft mit dem Markt. Was den Tieftauchtopf betrifft, hat das GM.SH im Jahr 2017 einen höhenvariabel einsetzbaren Ausstiegstrainer (als Prototyp) gebaut, der absetzbar auf einer ebenfalls neuen Arbeitsplattform ist. Er wird im Wasser abgesenkt, sodass der Ausstieg aus einem U-Boot unter Wasser simuliert werden kann. Bis zu sechs Taucher können damit den kontrollierten Ausstieg aus einem U-Boot trainieren. Die Herausforderung lag darin, Tauchtechnik, Atemlufttechnik sowie Steuerungs- und Überwachungstechnik aufeinander abzustimmen.

Die genehmigten Baukosten für die Maßnahme beliefen sich auf 1,2 Millionen Euro.

— Text: Bundeswehr, GM.SH, Gunda Marie



Das Kunstwerk des Monats: Am seidenen Faden

Neun Gefäße hängen gleichmütig. Es ist meist nur ein zarter Faden, der sie hält. Sieben Interferenzfarben strahlen aus der Arbeit – einige von ihnen mit starken Farbverschiebungen im Perspektivwechsel, ähnlich dem Mona-Lisa-Effekt –, die nur im Original sichtbar werden und sich dem Foto auf dem Bildschirm verweigern.

Als Malerin habe ich mich impulsieren lassen von der Kraft dieser besonderen Farben. Habe solide begonnen mit dem schwarzen Grund, ohne den Interferenzfarben sich nicht zeigen, und habe intuitiv erprobt, was weiter geschieht, wenn ich blind nach den Farben greife, sie auftrage, die Leinwand bewege, die Farbe laufen lasse. Unstrukturiert, frei.

Auch auf Abenteuer aus: Interferenzfarben sind alle in der Flasche weiß, sie entfalten ihre Farbwirkung nach und nach. Erst etwa zwei Stunden nach dem Auftragen ist mir klar, was ich da für ein Feuerwerk an Intensität auf die Leinwand gebracht habe.

Der Gleichmut, die serienhafte Anordnung, die dazu gegenläufige Zartheit der Aufhängung, all das fordert das Auge heraus. Es könnte sich um Kokons handeln. Um Raketen. Um liegengelassene Pilze aus einem Märchenwald. Es könnte … Malerei setzt der Fantasie des Betrachters, der Betrachterin keine Grenzen. Wir dürfen alles sehen und wir dürfen uns im Bild verlaufen. Wir dürfen jeden Tag unsere Sicht verändern, die Perspektive, die Wahrnehmung.

Solche Arbeiten können Seelenspiegel sein. Sie beziehen sich auf das Leere, auf die Leere in unseren Leben. Sie fügen diesem Nichts Lebendigkeit, Farbe, Ausdruck, Bewegung hinzu. Allein mit der Leere heißt auch immer: auf sich selbst geworfen. Das kann grausam sein und bedarf einer besonderen Umarmung. Schließlich ist der Feind da draußen auch immer in mir.

— Text & Foto: Prof. Dr. Brigitte Witzer

Am seidenen Faden
Abstrakter Expressionismus
Interferenzfarben auf Leinwand
ungerahmt / Rahmung möglich
145 cm x 300 cm, Preis auf Anfrage
art.witzer.de

• Analysen | Berichte | Reportagen | Shorties • 4 x im Jahr | 60 Seiten | digital •

In der nächsten Ausgabe Anfang Dezember 2026 lesen Sie unter anderem diese Themen:

- Aktuelles aus dem Marinefliegerkommando
- Akteptanzforschung zur zivilen Drohnennutzung
- Hilfreich und gefahrenanfällig: strukturierte Daten
- Hackerangriff von außen – und das Team intern macht fatale Fehler
- Bundeswehr & Kunst – Militärgeschichte in Bildern

Welche Themen halten Sie für relevant und lesenswert?

Schreiben Sie uns Ihre Idee in kurzen Stichworten an: *vg@vgmedienpool.de*

Dokumente, Logos, Ads und Inhalte für eine Beteiligung (siehe Mediadaten) an der Dezember-Ausgabe nehmen wir bis zum 20. November 2026 per e-Mail unter *vg@vgmedienpool.de* entgegen.

• Analysen | Berichte | Reportagen | Shorties • 4 x im Jahr | 60 Seiten | digital •

Teilen Sie Ihr Wissen – als „Content Pate“ oder auf der „Common Content Journey“ > Mediadaten

! Mit uns erreichen Sie reichweitenstarke Partner !

Impressum
Militär & Milchkaffee – Magazin für Verteidigung und Gesellschaft im Wandel erscheint im März, Juni, September und Dezember als Digitalprodukt im DACH-Raum (Deutschland, Österreich, Schweiz). Drucklegung seitens Herausgeber nach Absprache möglich. Annahmeschluss für Beteiligungen ist der jeweils 20. Tag des Ausgabevormonats > Mediadaten AGB | Idee, Konzeption, Herausgeber: Vivian Simon, www.viviansimon.de. Gerichtsstand Hamburg/DJV. Postanschrift: Pfingstberg 2, 23730 Sierksdorf i.H.