Neue Dimensionen

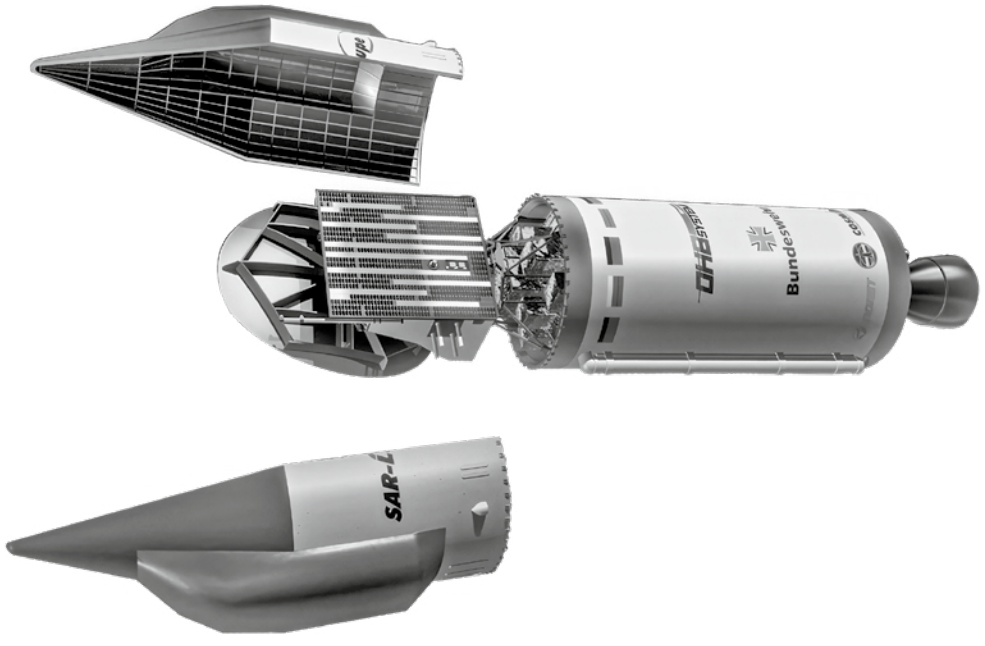
YNSIDE

YNSIDE.EXTRANET-BW.DE

INFOS AUS DER BUNDESWEHR AUCH UNTERWEGS

YNSIDE

Das Rückgrat moderner Streitkräfte
Der Weltraum, der Cyberraum und viele Fähigkeiten einer digitalen, vernetzten Armee – wie der Einsatz von künstlicher Intelligenz – sind eng miteinander verknüpft. Der Austausch von Daten erfolgt im Cyber- und Informationsraum und ist auf weltraumgestützte Systeme angewiesen. Dazu zählen spezielle Satelliten wie das Aufklärungssystem SAR-Lupe der Bundeswehr (Bild), aber auch zivile Systeme wie GPS oder Kommunikationssatelliten. Sie sind das Rückgrat moderner Streitkräfte und stellen die Führungsfähigkeit der Bundeswehr sicher.



Titel: Shutterstock/Smiltena (Wald), Shutterstock/Maximilian Cabinet
S. 3: Bundeswehr

Vom Boden bis ins Weltall

Die Bundeswehr schützt Deutschland und seine Verbündeten nicht nur an Land, in der Luft und auf dem Wasser. Der **Cyber- und Informationsraum sowie das Weltall** werden zunehmend Schauplatz militärischer Aktivitäten.

TEXT *Beate Schöne*

Aufklären

Den Feind anhand elektromagnetischer Signale zu orten und seine Funksprüche abzuhören – das ermöglicht der Tragbare Empfänger PR100. Mit dieser Fähigkeit unterstützen die hochmobilen LEKE-Kräfte des Kommandos Cyber- und Informationsraum andere Spezialisierte Kräfte. Ihre Informationen schärfen das Lagebild und ermöglichen wirkungsvolle Entscheidungen im Einsatz.

S. 4–5: Bundeswehr/Maximilian Bosse

Abwehren

Hier wird die digitale Infrastruktur Deutschlands geschützt: Die Mitarbeitenden des Nationalen IT-Lagezentrums beim Bundesamt für Sicherheit in der Informationstechnik (BSI) überwachen rund um die Uhr Entwicklungen im Cyberraum. Bundeswehrangehörige unterstützen hierbei in der Lagebeobachtung, um Bedrohungen frühzeitig zu erkennen.

S. 6–7: Bundeswehr/BSI/Bernd Lommel

Befähigen

Mit dem Start der ersten Ariane-6-Rakete vom Weltraumbahnhof Kourou in Französisch-Guayana im Jahr 2024 wurden Satelliten ins All gebracht, die die europäischen Kommunikationswege stärken und wichtige Daten für die Sicherheit liefern sollen. Denn die Sicherheit Deutschlands und seiner Verbündeten wird heute auch im Weltraum verteidigt: Ohne funktionierende Satellitentechnik sind viele militärische Operationen überhaupt nicht durchführbar.

S. 8–9: ArianeGroup

Hol dir die digitale Y!

Für alle Bundeswehrangehörigen mit einem Ynside-Zugang gibt es hier das Y-Magazin digital: browseroptimiert und an alle Bildschirme angepasst. Dazu gibt es viele Extras wie animierte Infografiken und zusätzliche Inhalte. Probiere die digitale Y jetzt aus!

Zusätzliche Dimensionen auf dem Gefechtsfeld
Editorial

Habt ihr das Cover sofort entschlüsselt? Auf der linken Seite ist ein gewöhnliches Luftbild eines Waldes zu sehen. Die vielen Bäume und ihr dichter Wuchs machen es unmöglich zu erkennen, ob sich auf dem Boden etwas befindet. Ganz anders die rechte Seite: eine Satellitenaufnahme, die mit künstlicher Intelligenz (KI) ausgewertet wird. Die KI identifiziert feindliche Drohnen und Infanterie. Auch die Vegetation und Bodenbeschaffenheit kann sie bestimmen. Die stilisierte Gegenüberstellung der beiden Waldstücke veranschaulicht einen tiefgreifenden Wandel in der Kriegsführung. Das Gefechtsfeld wird immer stärker von zwei neuen Dimensionen geprägt: dem Cyber- und Informationsraum und dem Weltraum. Wer sie nicht beherrscht, gerät im Ernstfall ins Hintertreffen.

Fast neun Jahre ist es her: Am 1. April 2017 wurde der Cyber- und Informationsraum (CIR) als eigenständiger militärischer Organisationsbereich der Bundeswehr in Dienst gestellt. Andere NATO-Staaten bauten zu der Zeit vergleichbare Strukturen auf. Am 1. Mai 2024 folgte der nächste Schritt: CIR ist seitdem neben Heer, Luftwaffe und Marine die vierte Teilstreitkraft. Die Bundeswehr definiert den Cyberraum als virtuellen Raum, in dem Menschen, Systeme und Daten weltweit miteinander verbunden sind. Im Zentrum steht das Internet, über das wir Informationen austauschen, miteinander kommunizieren und uns vernetzen. Gerade in sozialen Medien wird immer deutlicher, dass unser Informationsraum – die Gesamtheit aller Informationen, ihre Verbreitung und Verarbeitung – auch geschützt werden muss.

Rund 15.000 Menschen arbeiten bei CIR, verteilt auf 25 Dienststellen in ganz Deutschland. Sie sichern unsere IT-Systeme, wehren Cyberangriffe ab und klären auf – sowohl auf strategischer als auch taktischer Ebene. Der Cyber- und Informationsraum betrifft alle Truppenteile und treibt die Digitalisierung der gesamten Streitkräfte voran, vom Arbeitsplatz über Waffensysteme bis zum Gefechtsfeld. Ohne CIR wäre die Truppe nicht führungsfähig: Sie könnte weder sicher kommunizieren noch gemeinsam operieren.

Darum geht es in diesem Heft. Wir stellen die neuen Dimensionen der Bundeswehr vor. In Frankenberg (Eder) haben wir ein Basiscamp der LEKE-Kräfte besucht. Hier können Soldatinnen und Soldaten herausfinden, ob sie den hohen Anforderungen der Spezialisierten Kräfte von CIR gewachsen sind. In einem fiktiven Szenario schildern wir einen Cyberangriff auf Berlin und erklären, wer die Abwehr organisiert und welche Rolle CIR dabei spielt. Ausführlich beleuchten wir auch das Thema KI: Wie verändert die technologische Revolution das Militär – und wie stellt sich die Bundeswehr darauf ein? Wir stellen euch die wichtigsten KI-Projekte in der Truppe vor.

Aufklärung, Kommunikation und Navigation – für all dies brauchen wir den Weltraum. Ohne Satelliten und Trägersysteme würde das digitale Leben in Deutschland zum Erliegen kommen. Für einige Staaten ist der Weltraum deshalb längst ein militärisches Operationsgebiet – die fünfte Dimension. Wir haben die Ariane Group in Bremen besucht, wo die Oberstufe für Europas neue Trägerrakete Ariane 6 hergestellt wird. Außerdem sprechen wir mit CIR und Luftwaffe – den verantwortlichen Teilstreitkräften im Weltraum – über die erste deutsche Weltraumsicherheitsstrategie und die Pläne der Bundeswehr, im Weltraum unabhängig und verteidigungsbereit zu werden.

All das lest ihr in dieser Ausgabe. Und auch wir zeigen unsere digitale Seite: Als Extra haben wir ein Spiel für euch entwickelt. Wir nehmen euch mit auf eine LEKE-Mission. Könnt ihr die feindlichen Kräfte aufklären? Wir wünschen euch viel Erfolg dabei und viel Spaß beim Lesen des Heftes.

Die Y-Redaktion

Das ganze Heft in 15 Minuten

Das Digitale erobert unsere Welt und die Bundeswehr stellt sich verstärkt auf die neuen Dimensionen Cyber- und Informationsraum sowie Weltraum ein. Welche Fähigkeiten die Truppe hier hat, was die Herausforderungen der Zukunft sind und wie die Bundeswehr ihnen begegnet, liest du in dieser Ausgabe von Y.

Intro

Vom Boden bis ins Weltall
Der Cyber- und Informationsraum sowie der Weltraum rücken in den Fokus der Truppe.

- Die LEKE-Kräfte der Teilstreitkraft CIR sind spezialisiert für den Elektronischen Kampf bei besonderen Einsätzen.
- Im Nationalen IT-Lagezentrum beteiligen sich auch Bundeswehrangehörige an der Überwachung des Cyberraums.
- Das französisch-deutsche Raumfahrtunternehmen Ariane Group arbeitet eng mit der Bundeswehr zusammen, damit Europa im Weltraum unabhängig wird.

Seite 04–09

Kapitel 1 – Cyberkrieg ▸

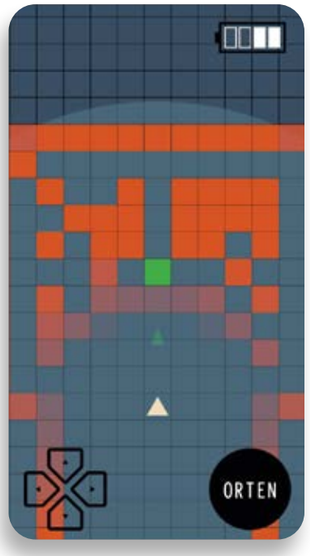
Dem Feind auf der Spur
Die LEKE-Kräfte der Bundeswehr orten Signale, stören Kommunikation und sichern Operationen durch elektronische Aufklärung.

- Im LEKE-Basiscamp lernen Interessierte die anspruchsvollen Aufgaben der Spezialisierten Kräfte von CIR kennen.
- Tarnung, Funkdisziplin und präzise Peilung sind entscheidend für den Erfolg im Einsatz.
- Durch ihre Luftbeweglichkeit und technische Expertise sind die LEKE-Kräfte unverzichtbar im modernen Gefecht.

Wie die Spezialisierten Kräfte im Verborgenen wirken, erfährst du hier.

Seite 18–27

S. 12: Bundeswehr/Maximilian Bosse (E.S.o.), Bundesfoto/BSI/Bernd Lommel (E.S.m.), ArianeGroup (E.S.u.), Bundeswehr/Jörg Hüttenhölscher (Z.S.1–4)
S. 13: Y/C3 Diana Rosenfeld, Illustration (E.S.1–2), Shutterstock/NewAfrica (E.S.u.), Bundeswehr/Lea Bacherle (Z.S.), Y/C3 Markus Spiller, Illustration (D.S.1–3)



Deine Mission – das Y-Game
Smartphone raus und los geht's. Zu unserer LEKE-Story gibt es auch ein Mini-Game:

- Per scannbarem QR-Code im Heft geht es mit dem Smartphone direkt zum Spiel.
- Dein Auftrag ist es, eine LEKE-Einheit zu führen und feindliche Kräfte zu orten.
- Die Story und mehrere Aufgaben machen dir die Lösung nicht leicht.

Die Anleitung und den QR-Code zum Y-Game findest du hier.

Seite 28–29

„KRIEGSTÜCHTIGKEIT BIS 2029 STEHT GANZ OBEN AUF UNSERER TO-DO-LISTE."

Auge, Ohr und zentrales Nervensystem
Vizeadmiral Dr. Thomas Daum erklärt im Interview, wie hybride Angriffe aussehen und warum der Cyber- und Informationsraum für die Bundeswehr unverzichtbar ist.

- Drohnen, GPS-Störungen und Cyberangriffe prägen das moderne Gefechtsfeld.
- CIR überwacht, schützt und unterstützt alle anderen Teilstreitkräfte mit digitalen und elektronischen Fähigkeiten.
- Die technologische Entwicklung im CIR ist rasant und entscheidend für die Kriegstüchtigkeit der Bundeswehr.

Wie die vierte Teilstreitkraft den Kampf der Zukunft gestaltet, liest du hier.

Seite 30–35

Blackout in Berlin
Ein Cyberangriff legt Teile der Hauptstadt lahm – Ampeln fallen aus, Krankenhäuser schalten auf Notstrom und die öffentliche Ordnung ist gefährdet.

- Das fiktive Szenario zeigt, wie Angriffe auf kritische Infrastrukturen ablaufen können.
- Staatliche Stellen und die Bundeswehr arbeiten im Ernstfall zusammen, um die Schäden schnell zu beheben.
- IT-Sicherheit wird zur Schlüsselaufgabe – für Staat, Wirtschaft und jeden Einzelnen.

Wie die Bundeswehr in solchen Krisen unterstützt, erfährst du hier.

Seite 36–42

Kapitel 2 – Künstliche Intelligenz ▸

Aufklären und wirken
Elektronische Kampfführung (EloKa) kann der Truppe auf dem modernen Gefechtsfeld den entscheidenden Vorteil bringen.

- Neue Flottendienstboote und Aufklärungsflugzeuge verbessern die Überwachung und Informationsgewinnung.
- Hochmobile EloKa-Systeme am Boden wirken effektiv gegen den Feind und verbessern die taktische Führung.

Wie die Bundeswehr ihre EloKa-Fähigkeiten weiterentwickelt, erfährst du hier.

Seite 44–47

Kampfwertsteigerung per Software
Mit Software Defined Defence (SDD) wird die Bundeswehr agiler und schneller.

- Offene Quellcodes ermöglichen schnelle Anpassungen bei vorhandenen Systemen.
- Die Vernetzung über flexible Schnittstellen fördert Multi-Domain Operations.
- Entwicklung, Sicherheit und Betrieb werden effizienter gestaltet.

Wie Software die Zukunft der Streitkräfte prägt, bekommst du hier erklärt.

Seite 48–49

Die neue Normalität
Künstliche Intelligenz revolutioniert auch das Militär – von autonomen Fahrzeugen bis zu KI-gestützten Drohnen.

- KI ermöglicht schnelle Datenverarbeitung, präzise Zielerkennung und autonome Entscheidungen.
- Zuverlässigkeit und Kontrolle von KI-Systemen gehören noch zu den Herausforderungen.
- Der effektive Einsatz von KI wird entscheidend für die Konflikte der Zukunft sein.

Wie die Bundeswehr KI nutzt und welche Fragen noch offen sind, liest du hier.

Seite 50–57

S. 14: Abell & Stone/David Melzer (E.S.1–4), Bundeswehr/Lea Bacherle (Z.S.o.), Bundeswehr/Marco Dorow (Z.S.m.), STARK Systems (Z.S.u.), UNITED24 (D.S.1), picture alliance/dpa/MAXPPP/VCG (D.S.2), IMAGO/SOPA Images/Mykhaylo Palinchak (D.S.3), Quantum Systems (D.S.4)
S. 15: Bundeswehr/Tom Twardy (E.S.o.), Bundeswehr/Susanne Krause-Weers (E.S.m.), Bundeswehr/Elian Hadj Hamdi (E.S.u.), ArianeGroup (Z.S.1–3), Y/C3 Visual Lab, Infografik (D.S.1–3)

Kapitel 3 – Weltraum ▸

Die Zukunft ist jetzt
Mit KI-Anwendungen beschäftigen sich viele Stellen innerhalb der Bundeswehr.

- KI kann die Einsatzfähigkeit durch schnelle Datenverarbeitung und präzise Lagebilder optimieren.
- Projekte wie „Uranos“ und „Minesweeper“ zeigen, wie KI militärische Operationen sicherer und effizienter macht.
- Von der Fake-News-Erkennung bis zur Wartung von Waffensystemen sollen KI-Anwendungen vielfältige Aufgaben übernehmen.

Einblicke in die Welt der KI und wie die Bundeswehr sich der Herausforderung stellt, findest du hier.

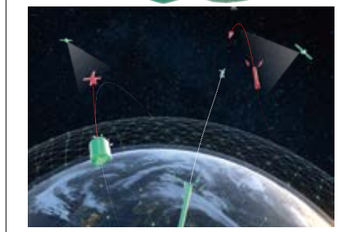
Seite 58–61

Das Tor zur fünften Dimension
Im Bremer Werk der Ariane Group entsteht Europas neue Schwerlastrakete Ariane 6. Y hat sich die Produktion angeschaut.

- In einer 6.000 Quadratmeter großen Werkshalle wird die Oberstufe gefertigt.
- Modernste Verfahren wie Laser-Isolierung und Fließfertigung sorgen für Effizienz und höchste Qualität.
- Mit einem Spezialschiff werden die Bauteile der Rakete zum Weltraumbahnhof Kourou in Südamerika transportiert.

Den ganzen Bericht mit beeindruckenden Bildern gibt es hier.

Seite 62–70

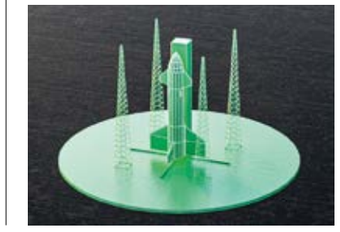


Stark im Orbit
Im Interview erklärt Generalleutnant Holger Neumann, wie die Luftwaffe im Weltraum agiert und welche Rolle die neue Weltraumsicherheitsstrategie spielt.

- Der Weltraum wird zunehmend zum Operationsraum – von Aufklärung bis zu Counter-Space-Fähigkeiten.
- Deutschland investiert in eine militärische Weltraumarchitektur, um seine Resilienz und Abschreckung zu stärken.

Wie die Luftwaffe den Weltraum schützt und nutzt, erfährst du hier.

Seite 72–77



Outro ▸

Blick in den Himmel
Weltraumkommando und Kommando CIR arbeiten gemeinsam daran, die Weltraum-infrastruktur der Bundeswehr zu schützen.

- Im Weltraumlagezentrum überwacht das Weltraumkommando den Orbit und erstellt ein militärisches Lagebild.
- Das Kommando CIR stellt unter anderem satellitengestützte Kommunikation, Aufklärung und Geoinformationen bereit.

Wie die beiden Kommandos arbeiten und den Weltraum nutzen, erfährst du hier.

Seite 78–85

Cyberwelten
Bilder von digitalen Räumen haben Autoren und Filmemacher bereits entworfen, lange bevor es das Internet gab.

- Der Roman „Neuromancer“ hat bereits 1984 den Begriff Cyberspace definiert.
- Das Manga „Ghost in the Shell“ hat sich früh mit der Frage nach dem Geist in künstlichen Körpern beschäftigt.
- Der Kinofilm „Tron“ von 1982 wurde stil-bildend für die Ästhetik digitaler Räume.

Noch mehr Bücher, Filme und Spiele, die unser Bild von Cyberwelten geprägt haben, gibt es hier.

Seite 86–92

Dranbleiben
Die Themen Cyber- und Informationsraum, künstliche Intelligenz und Weltraum sind mit einem Heft natürlich nicht erschöpfend behandelt.

- Auf bundeswehr.de und Ynside gibt es noch viele weitere Artikel.
- Tipps für spannende Bücher, Games und Ausstellungen dürfen natürlich auch nicht fehlen.

Seite 94–98

S. 16: Fraunhofer FHR/Uwe Beilhäuser (E.S.1), Bundeswehr/Jennifer Heyn (E.S.2.), OHB (E.S.3), picture alliance/dpa/Alexander Welscher (E.S.4.), Alamy Stock Photo/LANDMARK MEDIA (Z.S.o.), CD PROJEKT S.A. (Z.S.m.), Alamy Stock Photo/Photo12 (Z.S.u.), Bundeswehr/Francis Hildemann (D.S.o.), Carola Hartmann/ Miles-Verlag (D.S.m.Buch), Bundeswehr/Maximilian Bosse (D.S.m.), Technik Museum Speyer (D.S.u.)

1

Kapitel

Cyberkrieg

TEXT *Beate Schöne*
FOTO *Jörg Hüttenhölscher*

Dem Feind auf der Spur

LEKE-Kräfte orten Signale, hören den Gegner ab und stören dessen Technik. In Frankenberg (Eder) konnten interessierte Bundeswehrangehörige sich genau ansehen, welche Aufgaben diese Spezialisierten Kräfte übernehmen – und sich für eine Verwendung bei ihnen empfehlen.

S. 18–19: Bundeswehr/Jörg Hüttenhölscher

Kompetenzerweiterung beim Lufttransport LEKE-Kräfte sichern während des Trainings die Anlandung eines NH-90. Die Übung erweitert ihre Fähigkeiten jenseits des bisher genutzten Hubschraubers H145M LUH SOF.

„Als Truppenoffizier zu den LEKE-Kräften zu kommen ist schwierig, aber nicht unmöglich.“

Leutnant Lina Jäger,
Lehrgangsteilnehmerin

Es ist Anfang Dezember. Der Waldboden ist mit Laub bedeckt, der Wind pfeift durch die Bäume. Mehrere Soldaten haben sich am Waldrand verteilt, um die Umgebung zu beobachten und zu sichern. In der Ferne ertönen Rotorgeräusche. Einer der Soldaten hebt seinen Arm und gibt das Zeichen zum Loslaufen. Zwei Kameraden rennen aus der Deckung auf das freie Feld und weisen mit einer Signalflagge dem heranfliegenden NH-90 den Landeplatz. Die Türen schwingen auf, Trupps springen heraus und sichern die Umgebung. Die Soldaten aus dem Wald laufen zum Hubschrauber und steigen ein. Der Hubschrauber hebt wieder ab, während die abgesetzten Kräfte im Wald in Deckung gehen.

Die Soldaten führen ein Air Ground Integration Training (AGIT) durch. Mit dem Verfahren werden Anlandung, geordnetes Auf- und Absitzen sowie das Zusammenspiel von Bodentruppen mit Luftunterstützung für den Ernstfall geübt. Die Kräfte gehören zu LEKE: Luftlandefähige Komponente zur Nahunterstützung im Einsatz. Als Spezialisierte Kräfte des Cyber- und Informationsraums (CIR) sind sie im hessischen Frankenberg stationiert und Teil der 5. Kompanie des ElоKa-Bataillons 932. Sie führen den Elektronischen Kampf dort, wo es kein anderer kann. Die LEKE-Kräfte agieren lautlos und hochmobil. Sie orten, erfassen und analysieren feindliche elektromagnetische Signale, stören Kommunikation und ermöglichen so sichere Operationen. Ähnlich wie Fernspäher oft vor der eigentlichen Mission vor Ort, wirken sie im Verborgenen: Sind Fernspäher das Auge, ist LEKE das Ohr.

Antreten zum Basiscamp

Wenige Minuten später kündigt ein tiefes Dröhnen den nächsten Landeanflug des NH-90 an. Zehn Soldatinnen und Soldaten, die nicht zu LEKE gehören, beobachten das taktische Vorgehen am Rand der Landefläche. Noch ein Durchgang – dann sind sie selbst an der Reihe. Sie nehmen am einwöchigen LEKE-Basiscamp teil, das erstmals durchgeführt wird. Ziel ist es, einen realistischen Einblick in Auftrag, Fähigkeiten und Belastungen der Spezialisierten Kräfte zu bekommen. Unter den Teilnehmenden ist Leutnant Lina Jäger*. Sie und ihre neun Kameraden hatten Losglück, denn nur zehn der insgesamt 18 Teilnehmenden dürfen mitfliegen. „Ich bin ganz schön aufgeregt, denn es ist mein erster Flug mit einem Hubschrauber“, so die 24-Jährige. Für die LEKE-Kräfte ist die Übung mit dem NH-90 eine Kompetenzerweiterung, für Jäger und ihre Kameraden bedeutet der Flug vor allem eins: ein unvergessliches Erlebnis.

Das Basiscamp soll künftig halbjährlich in Frankenberg durchgeführt werden. Zwei Frauen und 16 Männer, aus verschiedensten Dienststellen und Berufen, nutzen das Camp, um herauszufinden, ob die Intensität der LEKE-Verwendung etwas für sie sein könnte. Das Feld, aus dem die Teilnehmenden kommen, ist groß: Vom zivilen Praktikanten bis zum erfahrenen Infanterie-Hauptfeldwebel ist alles dabei. Gesucht werden hauptsächlich Soldatinnen und Soldaten im Unteroffizierdienstgrad mit Portepee. „Als Truppenoffizier zu den LEKE-Kräften zu kommen ist schwierig, aber nicht unmöglich“, weiß Jäger. Sie ist derzeit für Personalwerbung zuständig und eher im Innendienst tätig. Aber sie ist gerne im Feld, springt in ihrer Freizeit Fallschirm und sucht bewusst nach fordernden Verwendungen. Von LEKE erfahren hat sie durch Kameraden und einen Artikel auf Ynside. Ihre Neugier war geweckt. „Ich mag sowohl körperliche als auch geistige Herausforderungen“, erklärt Jäger. „Deswegen bin ich Soldatin geworden.“ Sie will an ihre Grenzen kommen und auch darüber hinausgehen. ❱

*Mit Sternchen gekennzeichnete Namen sind zum Schutz der Personen geändert.

S. 20–21: Bundeswehr/Jörg Hüttenhölscher (2)

Teamwork unter Deckung
Lina Jäger und ihre Kameraden errichten ein Versteck aus Stangen und Plane. Ziel ist es, möglichst lautlos zu agieren, unentdeckt zu bleiben und die eigenen Spuren zu verwischen.

„Die Planungsphase ist eine der entscheidendsten.“

Oberbootsmann Raschek,
LEKE-Soldat und Ausbilder

Komfort für Durchhaltevermögen
Beim Versteckbau ist es wichtig, dass die Stelle gut getarnt wird. Das Versteck muss aber auch so komfortabel sein, dass es sich dort lange ausharren lässt. Das erhöht die Durchhaltefähigkeit.

Verstecken und unerkannt bleiben
Zurück auf dem Boden wartet auf Jäger und ihre Kameraden die nächste Aufgabe: Tarnung. Laub, Holz und Äste werden auf die Zeltplane geworfen, um das Versteck möglichst gut an die Umgebung anzupassen. „Tarnung ist wichtig, aber sie darf nicht zu schwer werden, sonst bricht der Zeltbau zusammen“, warnt Oberbootsmann Raschek*. Er ist seit fünf Jahren LEKE-Soldat und Ausbilder beim Camp. Normalerweise sind er und die anderen Ausbilder aktive LEKE-Trooper. Das heißt, sie sind mit den Spezialkräften unterwegs und bilden nicht primär aus. „Wir möchten eventuelle Hemmschwellen abbauen, Fragen beantworten und den hoffentlich potenziellen Bewerbern authentisch unsere Arbeit zeigen“, erklärt der 35-Jährige.

Mittlerweile ist das Versteck kaum noch zu sehen. Es hätte noch mehr im Waldinnern und auf ebenerem Grund sein können, aber die Teamarbeit war gut, resümiert Raschek. „Beim Versteckbau achten wir neben Tarnung auch auf Komfort, indem wir Unebenheiten wie Steine oder Wurzeln möglichst entfernen. Das wirkt sich positiv auf die Durchhaltefähigkeit aus“, sagt Raschek. Man wisse nie, wie lang man an der Stelle verharren muss. Gleichzeitig müsse der sogenannte Footprint möglichst minimal und die LEKE-Kräfte unentdeckt bleiben. ❱

S. 22–23: Bundeswehr/Jörg Hüttenhölscher (3)

Suchen, Erfassen und Peilen: Das Peilgerät deckt alles ab, was den Elektronischen Kampf ausmacht.

Elektronische Aufklärung
Mit dem PR100 scannen die Soldaten die Umgebung, um feindliche Funkquellen zu orten. Die portable Technik gilt als „Arbeitstier" der LEKE-Kräfte.

Lernen am System
Ein LEKE-Ausbilder erläutert Leutnant Jäger die Anzeige des PR100. So lernen Teilnehmende, Signale richtig zu deuten und einzuordnen.

Verbindung halten
Im Basiscamp üben die Soldaten den Einsatz des Satellitentelefons BGAN, das auch Kommunikation abseits regulärer Netze ermöglicht.

S. 24–25: Bundeswehr/Jörg Hüttenhölscher (3)

Kommunikation abhören

Ein Schwerpunkt des Camps ist der Umgang mit verschiedenen elektronischen Systemen – vom Satellitentelefon BGAN über das Handfunkgerät PRC6809 bis zum Peilgerät PR100. Die Teilnehmenden erhalten einen Überblick über die vielen Fähigkeiten luftbeweglicher Operationen: Spektrumüberwachung, Ortung, Peilung von Störsignalen bis hin zur Funkdisziplin. „Wer zu uns kommt, muss zwingend ein Interesse an Technologie haben. Denn das ist der Kern unserer Verwendung", sagt Major Maximilian Seeger*. Er ist seit 2024 Chef der 5. Kompanie und heute zur Dienstaufsicht auf dem Truppenübungsplatz. Bewusst hält er sich im Hintergrund – beobachtet, sammelt Eindrücke und führt kurze Gespräche am Rand. „Es geht nicht darum, Druck aufzubauen", sagt er. „Die Woche soll zeigen, ob jemand geeignet sein könnte oder nicht." Das Wichtigste sei, dass man motiviert ist.

Nach der Theorie folgt die Praxis. Aufgeteilt in drei Sechsergruppen gehen die Soldatinnen und Soldaten in den Wald. Ihr Auftrag: das elektromagnetische Spektrum erfassen, Signale erkennen und aufzeichnen sowie das abzuhörende Gebiet orten und mithilfe einer Kreuzpeilung eingrenzen. Leutnant Jäger trägt zum ersten Mal ein PR100, ein leistungsstarkes Gerät zur Spektrumüberwachung und Peilung – für LEKE-Kräfte das Arbeitstier. Es ist handlich, zuverlässig und deckt alles ab, was den Elektronischen Kampf ausmacht: Suchen, Erfassen und Peilen.

Erstaunlich intuitiv

Beim Suchen wird das Spektrum in verschiedenen Frequenzbereichen überprüft. Während hohe Frequenzen wie ein WLAN-Signal mit 2,4 Gigahertz geringe Reichweiten haben, können tiefe Frequenzen wie Funkgeräte mit 30 Megahertz große Distanzen überbrücken. Sobald die Teilnehmenden ein Signal empfangen, sollen sie es als Audiodatei aufnehmen, um es später auswerten zu können. Beim Peilen wird als Erstes geschaut und markiert, aus welcher Richtung das stärkste Signal kommt. Danach bewegen sich die Soldatinnen und Soldaten zu einem weiteren Punkt, der L-förmig zum ersten Punkt liegt und peilen das stärkste Signal erneut an. So entsteht eine Kreuzpeilung, die den vermuteten Standort feindlicher elektromagnetischer Quellen gezielt einschränkt. Noch genauer wird es, wenn man eine weitere Peilung an einem dritten Ort vornimmt. Wenn die drei Peillinien genau in einem Punkt zusammenlaufen, hat man den exakten Standort gefunden. Ansonsten entsteht ein kleines Dreieck, das den vermuteten Standort weiter einschränkt. ❯

Disziplin, Wille und Belastbarkeit
Leutnant Jäger und die anderen Teilnehmenden trainieren den Nahkampf, um in Zukunft mit Spezialkräften und Spezialisierten Kräften gemeinsam operieren zu können.

Bereit für die Nacht
Im Zelt rüstet sich Leutnant Jäger für die bevorstehende Abschlussübung aus. Neben der Schutzweste, dem Gewehr G36 und dem Gefechtshelm darf auch das Nachtsichtgerät nicht fehlen.

Leutnant Jäger ist begeistert: „Auch wenn das Gerät kompliziert aussieht, ist es erstaunlich intuitiv." Jäger dreht sich und hört plötzlich etwas. Zunächst nur Rauschen und lautes Knacken, kurz danach versteht sie klare Worte. „Es ist faszinierend zu merken, dass eine klitzekleine Drehung so einen Unterschied machen kann", sagt sie. Abends wird das tagsüber Gelernte in Gruppenübungen vertieft. „Hier kombinieren wir alles Gelernte und agieren als Team", so Jäger.

Den Gegner orten in der Nacht

Inzwischen ist es fast komplett dunkel. In wenigen Minuten treffen sich die Gruppen zur Vorbesprechung. „Die Planungsphase ist eine der entscheidendsten. Je mehr im Vorfeld geklärt ist, desto lautloser und unentdeckter kann operiert werden", erklärt Raschek. Leutnant Jäger bereitet sich vor, wechselt Batterien, legt Ausrüstung an – inklusive G36 und Nachtsichtgerät. Kurz darauf werden die Aufgaben verteilt: Gruppenführer und Stellvertreter, ein Funker – der sogenannte Master Signal – und ein Master Medical für die Sanität. Jäger übernimmt die Orientierung und Sensorik.

Nach dem Absetzen an unterschiedlichen Drop-off Points heißt es: rundum sichern, im Wald untertauchen und zum Treffpunkt, einer Lagerhalle, vorarbeiten. Leutnant Jäger darf sich und ihre Gruppe nicht durch das Licht des GPS-Geräts verraten. Deshalb verschwindet sie unter ihrer Jacke, die anderen gehen in eine 360-Grad-Sicherung. „Wichtig ist, dass man als Team fungiert", sagt Jäger. Sie hat einen unauffälligen Weg gefunden. Das Team arbeitet sich möglichst lautlos durch Gestrüpp und teils unebenes Gelände. Eins haben alle schnell verstanden: Jedes Mal, wenn das Funkgerät gedrückt wird, verrät man möglicherweise seinen Standort. An der Lagerhalle angekommen, heißt es: Versteck aufbauen, beobachten, elektromagnetische Signaturen erfassen und feindliche Bewegungen aufklären und dokumentieren.

„Interesse an Technologie und Motivation sind zwingend."

Major Maximilian Seeger,
Kompaniechef

Die letzte Mission

Stunden später hat das Team seinen Auftrag erfüllt. „Das Camp bildet nicht eins zu eins die Realität ab, das geht aufgrund operativer Sicherheit nicht, aber es gibt einen authentischen Einblick", so Raschek.

Disziplin, Wille und Belastbarkeit sind elementar, um mit den Spezialkräften gemeinsam operieren zu können. Auch Nahkampftraining gehört dazu – nicht als Spektakel, sondern zur Kontrolle des Körpers. „LEKE-Kräfte müssen schnell reagieren und dürfen nicht die Übersicht verlieren", sagt Raschek. Bei der Abschlussübung „Letzte Mission" zeigt sich, wer den hohen Anforderungen gewachsen ist. Ob Lina Jäger wieder Navigatorin ist, weiß sie noch nicht. Was sie aber ganz sicher weiß: dass sie sich für das zweiwöchige Trainingslager bewerben wird, welches als Vorbereitung für das Eignungsfeststellungsverfahren dient. „Was LEKE-Kräfte besonders macht, ist nicht eine einzelne Fähigkeit, sondern ihre Kombination: luftbeweglich, verlegefähig, technisch hochspezialisiert und taktisch präzise", bringt es Major Seeger auf den Punkt. Sie wirken dort, wo Sekunden entscheiden und Signale mehr zählen als Schüsse.

S. 26–27: Bundeswehr/Jörg Hüttenhölscher (3)

TEXT *Michael Schulz* **Illustration** *Diana Rosenfeld*

MISSION FEINDLICHE SIGNALE

Stiefel schnüren, Helmgurt festziehen, Smartphone zücken – deine geheime Mission beginnt. In unserem Y-Game „Feindliche Signale“ führst du einen Trupp spezialisiert auf Elektronischen Kampf. **Dein Ziel: die versteckte Basis des Feindes aufspüren.**

Scanne jetzt den QR-Code rechts.

AUFTRAG STARTEN

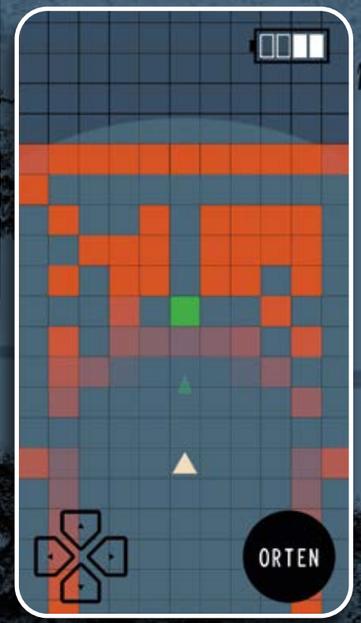
Im Grenzgebiet eines befreundeten Landes sind feindliche Kräfte aktiv und planen Sabotageakte. Du führst einen Trupp der spezialisierten LEKE-Kräfte und musst den Gegner anhand seiner elektromagnetischen Signale erfolgreich orten.

TRUPP FÜHREN

Steuere den Trupp durch das abgelegene Gebiet, sammle Informationen und finde eine gute Position, um Funksignale des Feindes zu empfangen und ihr Geheimversteck zu finden. Denn nur mit deiner Hilfe wissen die Kommandosoldaten, wo sie zuschlagen müssen.

FEIND ORTEN

Die feindlichen Signale zu orten, ist alles andere als einfach. Dein Können ist gefragt, um Signale zu empfangen und den Bereich, in dem sich der Gegner aufhält, Schritt für Schritt einzugrenzen.



JETZT SPIELEN!

S. 28–29: YC3 Diana Rosenfeld, Illustration (5); Shutterstock/NewAfrica (Foto)

AUGE, OHR UND ZENTRALES NERVENSYSTEM

Vizeadmiral Dr. Thomas Daum trat 1981 in die Bundeswehr ein. Der Marineoffizier und promovierte Informatiker führt seit September 2020 den Cyber- und Informationsraum, die vierte Teilstreitkraft (TSK) der Bundeswehr.

GPS-Signale fallen aus, Drohnen kreisen über Kasernen und die Netze der Bundeswehr stehen unter Dauerbeschuss. **Vizeadmiral Dr. Thomas Daum** erklärt, wie hybride Angriffe aussehen, welche Rolle Drohnen und Cyberoperationen spielen – und warum der Cyber- und Informationsraum (CIR) von zentraler Bedeutung für das moderne Gefechtsfeld ist.

Das Interview führte Torsten Stephan.

Y: In den Medien häufen sich Berichte über Drohnenüberflüge bei unseren NATO-Partnern und auch über Deutschlands kritischer Infrastruktur. Was wird damit bezweckt und wer steckt dahinter?
Vizeadmiral Dr. Thomas Daum: Diese Vorfälle muss man differenziert betrachten. Oft kann man nicht zuordnen, wer die Drohnen steuert. Wir haben Drohnen nahe einer Kaserne gesichtet, wo sich herausstellte, dass ein Landwirt damit seine angrenzenden Felder abflog. Gleichzeitig registrieren wir aber Drohnenüberflüge über unseren Ausbildungsstandorten für ukrainische Soldatinnen und Soldaten. Wir müssen dort davon ausgehen, dass gegnerische Kräfte das Gelände auskundschaften und es sich also um Spionage handelt. Bei zivilen Flughäfen dienen solche Aktionen der Destabilisierung: Wenn der Flughafen stillsteht, klagen die Menschen eher über die eigene Regierung als über den Verursacher. Diese Taktik – Verunsicherung, Diskreditierung und Fokusverschiebung – ist Teil einer hybriden Kriegführung. Für solche Aktionen werden oft sogenannte Wegwerfagenten angeworben, die bei einer Enttarnung offiziell keine Verbindungen zu einem ausländischen Nachrichtendienst hatten. Bei allen hybriden Aktivitäten ist die Attribuierung, also die Rückverfolgung und Zuschreibung, schwer. Wenn man sich aber fragt, wem die Aktivitäten nutzen, dann lautet die Antwort meistens: Russland.

Die Bundeswehr soll die zivilen Stellen im Inland künftig bei der Drohnenabwehr unterstützen. Sind wir darauf vorbereitet und welche Rolle spielt die Teilstreitkraft CIR dabei?
Wir dürfen unter bestimmten Voraussetzungen schon heute Klein- und Kleinstdrohnen über unseren Kasernen und Truppenübungsplätzen mit kinetischen Mitteln oder der Elektronischen Kampfführung abwehren. Die Teilstreitkraft CIR verfügt zum Beispiel schon über begrenzte Mittel, um Bereiche im elektromagnetischen Spektrum zu sperren. Damit lassen sich Frequenzen, auf denen handelsübliche Drohnen gesteuert werden, gezielt blockieren. Die darüber hinausgehende Abwehr im öffentlichen Raum ist eine polizeiliche Aufgabe. Die Bundeswehr kann also unterstützen, soweit es das Grundgesetz zulässt – Stichwort Amtshilfe. Unterstützt wird auch international, beispielsweise durch die Deutsche Luftwaffe zum Schutz des Flughafens im belgischen Brüssel.

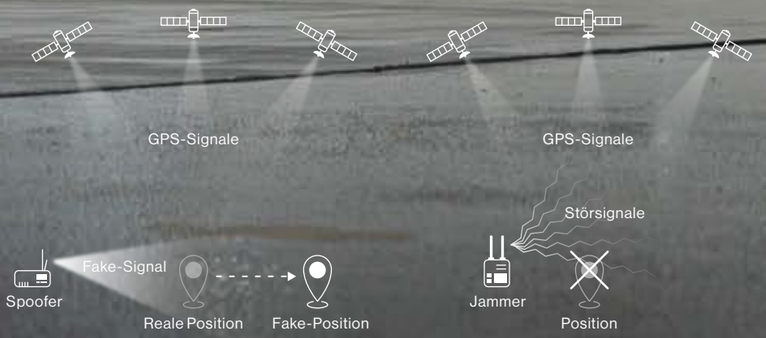
Ein weiteres, relativ neues Phänomen ist das GPS-Spoofing. Auf der Ostsee und im Luftraum allgemein werden gezielt Funkverbindungen und GPS-Signale gestört. Mit welchem Ziel?
Das GPS-Jamming, also das Stören des Signals mit der Folge Nichtverfügbarkeit, oder auch das aufwendigere GPS-Spoofing, worunter beispielsweise das räumliche Verschieben von GPS-Positionen zählt, sind typische Techniken beim Elektronischen Kampf. Sie gehören auch zu den hybriden Maßnahmen, die sehr wahrscheinlich von Russland ausgehen. An der NATO-Ostgrenze und insbesondere in den baltischen Staaten sind diese Störungen an der Tagesordnung. Sie führen teilweise zum Ausfall des zivilen Flugverkehrs und sogar zum Abdrehen auf einen Ausweichflughafen, wenn Piloten bei schlechtem Wetter oder schlechter Sicht auf den Instrumentenflug angewiesen sind. Auch der Schiffsverkehr ist durch GPS-Störungen betroffen. Wir müssen uns dieser Gefahren bewusst sein und uns darauf einstellen. Zum Beispiel durch Härtung unserer Systeme und das Nutzen alternativer beziehungsweise redundanter Lösungen. Notfalls gibt es auch immer noch die gute alte analoge Karte. Es gilt, Technik nie blind zu vertrauen, sondern stets auch kritisch zu hinterfragen.

Der Cyber- und Informationsraum gerät immer mehr in den Fokus. Wie schätzen Sie die Bedrohungslage ein? Sind wir bereits in einem hybriden Krieg mit Russland?
Bundeskanzler Friedrich Merz hat kürzlich treffend gesagt: „Wir sind nicht im Krieg, wir sind aber auch nicht mehr im Frieden.“ Das beschreibt die aktuelle Lage sehr gut. Deutschland wird nicht erst seit Beginn des russischen Angriffskriegs gegen die ›

S. 31: Bundeswehr/Stefan Uj

PEGASUS
Das Akronym steht für Persistent German Airborne Surveillance System. Das System bringt modernste Signal Intelligence (SIGINT)-Fähigkeiten und fliegende Aufklärungssensorik in die Bundeswehr. Es dient der Krisenfrüherkennung, Lagebeurteilung und Feststellung der Bedrohungslage.

Ukraine regelmäßig attackiert. Wir sind in der Teilstreitkraft CIR bereits vor einem Spannungs- oder Krisenfall gefordert. Zu den hybriden Aktivitäten gehören Cyberangriffe auf deutsche Institutionen und Firmen, die fast täglich stattfinden. Wir beobachten auch gezielte Maßnahmen im elektromagnetischen Spektrum, zum Beispiel das Stören des GPS-Systems auf der Ostsee oder das Stören des Truppenfunks an der NATO-Ostgrenze. Und wir sehen immer wieder Desinformationskampagnen. Die Aktionen sollen vor allem das Vertrauen der Bevölkerung in den Staat untergraben und werden bewusst gewählt, weil sie sich schwer zurückverfolgen lassen. Es ist daher sehr wichtig, Quellen und Botschaften im Internet und besonderen sozialen Medien kritisch zu hinterfragen – gerade als Angehörige der Streitkräfte und Staatsbürger in Uniform.



Spoofing
Satellitensignale können durch Störsender verändert werden, was die Positionsergebnisse verfälscht. Dabei werden echte durch falsche Vermessungsdaten überschrieben.

Jamming
Satellitensignale können aber auch gestört werden. Das Ergebnis ist dasselbe wie beim Spoofing. Solche Störversuche muss die Truppe erkennen und Gegenmaßnahmen ergreifen.

S. 32: C3/Visual Lab, Infografik
S. 32–33: Bundeswehr/Lea Bacherle

Auch die Bundeswehr und ihre Netzwerke werden regelmäßig angegriffen – von Phishing-Attacken bis zur gezielten Spionage. Wie gut sind wir bei der Cyberabwehr aufgestellt?
Das stimmt, im Cyberraum wird die Bundeswehr heute 24/7 angegriffen. Das fällt insbesondere bei wichtigen politischen Entscheidungen zur Ukraine auf, nach deren Veröffentlichung unsere Firewalls wegen DDoS-Attacken glühen. Unsere Frauen und Männer im Zentrum für Cyber-Sicherheit der Bundeswehr machen einen hervorragenden Job. Wir trainieren unsere Cyberabwehrfähigkeiten regelmäßig ressortübergreifend und international. Bei der NATO-Übung Locked Shields haben wir im Jahr 2025 zusammen mit dem Bundesministerium des Innern, dem Bundesamt für Sicherheit in der Informationstechnik, der zivilen Wirtschaft und unserem Übungspartner Singapur den ersten Platz belegt. Cybersicherheit kann man nur gemeinsam erreichen und es kommt auf jeden Einzelnen an. Die Technik für Firewalls und Antivirensoftware kann noch so raffiniert und ausgeklügelt sein, am Ende entscheidet oft das Nutzerverhalten am Rechner darüber, ob eine gegnerische Attacke Erfolg hat. Das gilt auch für unsere Partner in der Rüstungsindustrie und im Dienstleistungssektor: Wenn die IT unserer Partner kompromittiert wird, kann dies erhebliche Auswirkungen auf uns haben. Wir sind als Bundeswehr gut aufgestellt, aber wir sind nicht allein maßgeblich. ›

Drohnenabwehr Während der Übung National Guardian trainierte die Truppe den Umgang mit dem schultergestützten Störsender HP-47. Das System besteht aus zwei portablen Jammer-Kanonen und stationärer Sensorik.

Locked Shields
Bei der größten jährlichen Cyberabwehrübung der NATO trainieren IT-Fachleute aus aller Welt gemeinsam.

Joint Intelligence Center (JIC)
Hier werden alle verfügbaren Informationen gesammelt, verarbeitet und an die richtige Stelle passend weitergeleitet.

Ohne CIR geht im Krieg nichts mehr. Was leisten Ihre Soldatinnen und Soldaten im Gefecht der verbundenen Waffen?
Erstrangig führen unsere Einsatzkräfte den Kampf in der Dimension CIR: Offensive Cyberoperationen legen Verbindungen oder Systeme des Gegners lahm, aktives Stören im elektromagnetischen Spektrum behindert den gegnerischen Truppenfunk oder die Radaraufklärung, offensives Wirken im Informationsraum zielt auf die Überzeugung und die Moral gegnerischer Kräfte.

Dazu kommt unser Unterstützungsauftrag für die anderen Teilstreitkräfte. CIR wurde von Verteidigungsminister Boris Pistorius sehr treffend als „Auge, Ohr und zentrales Nervensystem der Streitkräfte“ beschrieben. Unsere EloKa-Kräfte überwachen permanent das elektromagnetische Spektrum auf gegnerische Aktivitäten: an Land wie bei der Mission Vigilant Owl, zu Wasser mit unseren Flottendienstbooten oder künftig in der Luft mit den Aufklärungsfliegern PEGASUS. Auch im Cyberraum liefern wir viele Erkenntnisse über gegnerische Aktivitäten. CIR verantwortet mit dem Joint Intelligence Center die zentrale Aufbereitung aller Informationen zu einem ganzheitlichen Lagebild für alle Truppenteile und unsere Verbündeten. Dazu kommen unsere Fähigkeiten bei der Einsatzunterstützung aus dem Weltraum: Unsere Aufklärungssatelliten und künftig noch weitere Systeme generieren fast ein Echtzeitlagebild, wie wir es nur aus dem Ukrainekrieg kennen. Gleichzeitig sind wir für die Cloudspeicher und Kommunikationsverbindungen und deren Sicherheit verantwortlich. Auch die Karten, die wir alle ganz selbstverständlich nutzen, stammen von unserem Zentrum für Geoinformationswesen der Bundeswehr. Unser Zentrum Digitalisierung der Bundeswehr treibt gemeinsam mit dem Bundesamt für Ausrüstung, Informationstechnik und Nutzung zahlreiche Projekte zur Digitalisierung der Truppe voran – sie reichen vom Einsatz von KI in Drohnen über die Quantenverschlüsselung unserer Kommunikation bis zum Aufbau einer eigenen Combat Cloud.

Der Ukrainekrieg zeigt sehr deutlich, wie wichtig der Elektronische Kampf ist. Woran liegt das und welche Schlüsse ziehen Sie daraus?
Spätestens seit der Reform zur Modernisierung der Streitkräfte 2008 hat Russland seine Fähigkeiten zur vernetzten Operationsführung in den Fokus gerückt. Eng damit verbunden ist der anhaltende Fähigkeitsaufwuchs im Funkelektronischen Kampf, dem russischen Begriff für EloKa. Russland hat auf jeder Ebene – taktisch, operativ und strategisch – Fähigkeiten für die Elektronische Kampfführung optimiert. Das gilt für alle Dimensionen: See, Land und Luft. Es ist extrem erfolgreich, auch gegen westliche Waffensysteme, weshalb die Führungsfähigkeit der ukrainischen Streitkräfte entlang der Frontlinien erheblich eingeschränkt ist. Russland demonstriert seine Dominanz auch mit hybriden Angriffen gegenüber NATO-Mitgliedern. Wir müssen nachziehen, um auf dem Gefechtsfeld konkurrenzfähig zu bleiben.

Mit der Mission Vigilant Owl, kurz VIGO, betreibt CIR seit diesem Jahr auch einen Einsatz in Litauen. Was ist ihr Auftrag an der NATO-Ostflanke?
VIGO ist seit Januar 2025 die erste anerkannte Mission, die von der TSK CIR geführt wird. Auftrag ist, durch Aufklärung im elektromagnetischen Spektrum die NATO-Ostgrenze zu schützen und unsere Panzerbrigade 45 in Litauen zu unterstützen. Als Auge und Ohr am Feind ist VIGO ein ganz wichtiges Frühwarnsystem, beispielsweise während der russischen Übung Zapad 2025 in Belarus und im Westen Russlands. Wir haben in der Ukraine 2013 und 2021 erlebt, dass Russland genau diese Übungstätigkeiten nutzte, um Truppen zusammenzuziehen, die dann anschließend überraschend angegriffen haben. Das darf sich nicht mehr wiederholen.

S. 34: Bundeswehr/Mario Bähr (o.), Bundeswehr/Martina Pump (m.), Bundeswehr/KSA (u.)
S. 35: Bundeswehr/Lea Bacherle

„KRIEGS-TÜCHTIGKEIT BIS 2029 STEHT GANZ OBEN AUF UNSERER TO-DO-LISTE.“

Vizeadmiral Dr. Thomas Daum

Bis 2029 soll die Bundeswehr kriegstüchtig sein. Wo steht die TSK CIR?
Kriegstüchtigkeit bis 2029 steht ganz oben auf unserer To-do-Liste. Es ist festgelegt, welche Aufgaben meine TSK im Ernstfall erfüllen muss. Wir sind für die digitale Kriegstüchtigkeit der gesamten Bundeswehr verantwortlich. Da gibt es noch viel zu tun. Das Schlachtfeld wandelt sich permanent: Der Kampf um und mit Informationen steht im Vordergrund und ergänzt das kinetische Gefecht. Jedes System ist auch ein Sensor, den es zu nutzen und zu schützen gilt. Die Bilder aus der Ukraine zeigen uns ein gläsernes Gefechtsfeld in nahezu Echtzeit, in dem aufgeklärte Systeme direkt durch Drohnen oder Artillerie bekämpft werden. Die Folgen für den Kampf und damit die technischen Anforderungen an die Streitkräfte sind enorm: Alle Daten müssen gesammelt, mithilfe von künstlicher Intelligenz ausgewertet und dem militärischen Führer verfügbar gemacht werden. Die Kill-Chain, also der Prozess vom Erkennen eines gegnerischen Ziels bis zu dessen Bekämpfung, wird immer kürzer. Nur wer schneller über die notwendigen Informationen verfügt, auf dieser Basis eher entscheiden kann, sodann schneller schießt und präziser trifft, wird in der Gefechtssituation überlegen sein. KI wird auch in diesem Gefecht entscheidend werden. Der Prozess der Bedrohungsbewertung bei anfliegenden gegnerischen Drohnen, Flugkörpern und Raketen, das Festlegen der Bekämpfungsreihenfolge und die Zuordnung der Abwehrwaffen wird nur durch Automatisierung das Überleben sichern, der Mensch wird dazu nicht mehr in der Lage sein. Das ist keine Zukunftsmusik, sondern passiert bereits.

Die technologische Entwicklung im CIR ist rasant. Worauf muss sich die Bundeswehr künftig einstellen?
Die technologische Entwicklung und die damit verbundenen Innovationszyklen werden immer schneller. Wir treiben Themen wie KI, Combat Cloud oder Aufklärungstechnik schnellstmöglich voran. In vielen Bereichen denken wir um und sind flexibler. Wir denken Technologien nicht mehr als Einzelprojekte, sondern vernetzt und rollierend. Auch jahrelange Planungsphasen können wir uns nicht mehr erlauben. Ein Beispiel: Die TSK CIR verantwortet die Satelliten der Bundeswehr, Kommunikations- und Aufklärungssatelliten. Die einstellige Zahl reicht heute nicht mehr. Es bestehen viel höhere Anforderungen an Datendurchsatz und -geschwindigkeit sowie viel breitere Aufklärungserfordernisse. Zugleich erkennen wir eine Aufrüstung im Weltraum. Während wir uns verpflichtet haben, gefährlichen Weltraummüll durch den Einsatz kinetischer Waffen zu vermeiden, stationieren unsere potenziellen Gegner Waffensysteme im Weltraum. Wir setzen deshalb nicht nur auf wenige große, sondern vor allem viele zusätzliche kleine Satelliten. Diese sind zwar etwas weniger leistungsfähig, jedoch lassen sie sich leichter ins All bringen, sind schneller verfügbar und auch leichter ersetzbar – so steigern wir unseren Schutz und unsere Resilienz im All.

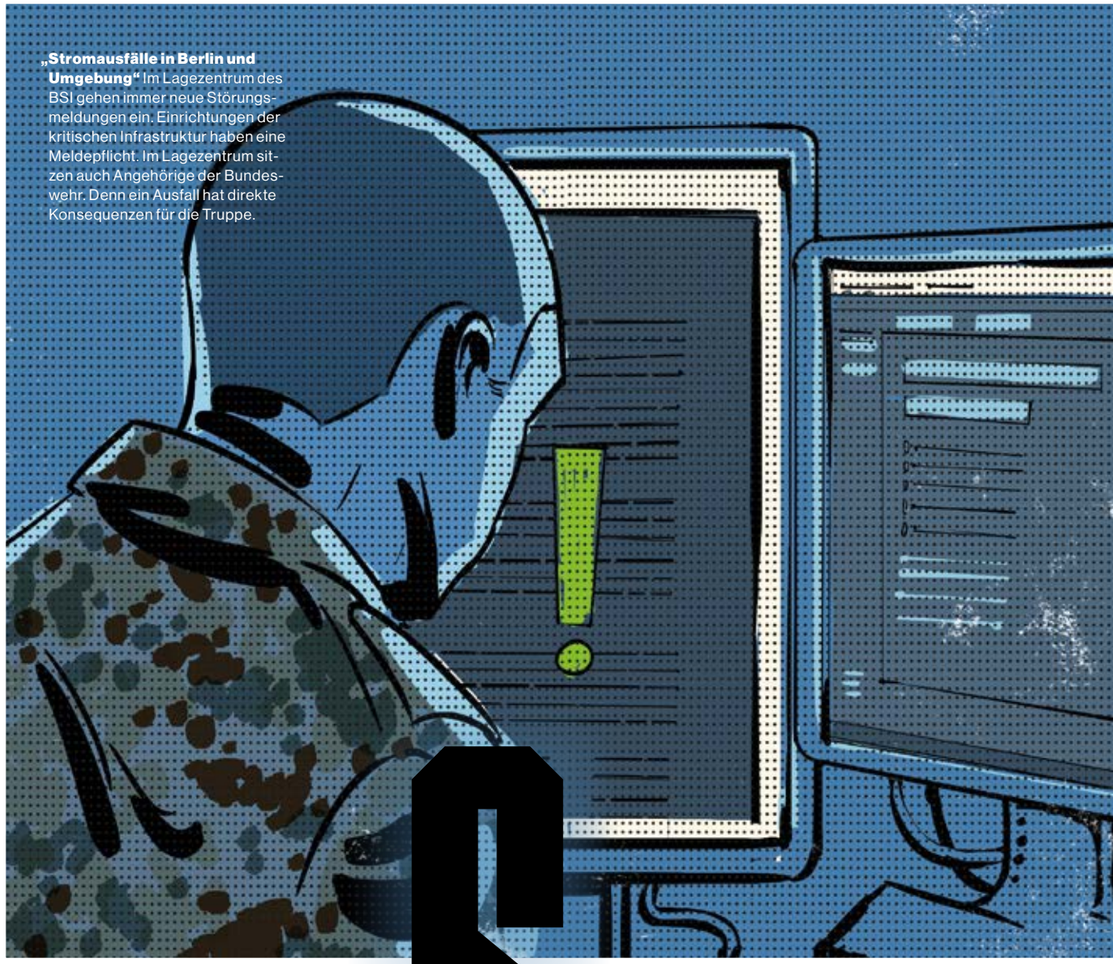
Aufklärungsmission VIGO
Um im elektromagnetischen Spektrum gegnerische Aktivitäten aufzuklären, nutzen die EloKa-Kräfte in Litauen verschiedene Systeme.

Blackout in Berlin

Welche Folgen kann ein Cyberangriff haben? Wie unterstützt die Bundeswehr dabei? Y zeigt es, in diesem fiktiven, aber realistischen Szenario.

TEXT *Florian Stohr*
ILLUSTRATION *Markus Spiller*

Vernetzter Alltag
Auf den Straßen von Deutschlands Hauptstadt sind tagtäglich unzählige Menschen unterwegs. Egal, was sie gerade tun, eins haben sie ziemlich sicher dabei: ihr Handy. In einer hochmodernen Gesellschaft sind mobile Geräte unverzichtbar. Alles ist vernetzt und digital – auch Straßenbahnen, Autos, Ampeln und Co.



„Stromausfälle in Berlin und Umgebung“ Im Lagezentrum des BSI gehen immer neue Störungsmeldungen ein. Einrichtungen der kritischen Infrastruktur haben eine Meldepflicht. Im Lagezentrum sitzen auch Angehörige der Bundeswehr. Denn ein Ausfall hat direkte Konsequenzen für die Truppe.

„Schwere Störung unserer Server“ – die Meldung eines Berliner Energieunternehmens lässt die Fachleute im Nationalen IT-Lagezentrum des Bundesamts für Sicherheit in der Informationstechnik (BSI) aufhorchen. Was bedeutet das für die Stromversorgung? Die Frauen und Männer blicken angespannt auf ihre Bildschirme. Kurz darauf geht über das Melde- und Informationsportal des BSI eine weitere Nachricht ein: „Stromausfälle in Berlin und Umgebung“. Welche Bezirke und wie viele Menschen sind davon betroffen? Wie schwer sind die Schäden und wie kam es dazu?

Innerhalb einer Stunde verzeichnet das BSI über 20 Meldungen. Für Einrichtungen und Unternehmen der kritischen Infrastrukturen (KRITIS) wie Energie, Wasser, Verkehr oder Telekommunikation besteht eine gesetzliche Meldepflicht bei IT-Störungen. Aber es melden sich auch Betreiber freiwillig. Die Informationen ❱

S. 36–37: Y/C3 Markus Spiller; Illustration (2)

verdichten sich: In drei Randbezirken Berlins gibt es keinen Strom mehr. Rund 100.000 Menschen sitzen im Dunkeln. Im Straßenverkehr bricht Hektik aus, auch das Internet ist zusammengebrochen. Kann das Zufall sein oder ein Anschlag auf wichtige Stromleitungen? Die Fachleute im BSI haben einen anderen Verdacht: Es könnte auch ein großangelegter Cyberangriff auf Deutschlands Hauptstadt und politisches Zentrum sein.

**Mit Sternchen gekennzeichnete Namen sind zum Schutz der Personen geändert.*

Nationale IT-Krise

Das Nationale IT-Lagezentrum ist hochmodern. Das Licht ist abgedunkelt, auf den Bildschirmen der Frauen und Männer sind unzählige Tabellen, Grafiken und Programmiercodes zu sehen. Gearbeitet wird im 24-Stunden-Dienst. Das BSI ist die zentrale Ansprechstelle für die Informationssicherheit Deutschlands. Es untersucht Angriffe und Sicherheitslücken in Staat, Wirtschaft und Gesellschaft, entwickelt Sicherheitsstandards und berät KRITIS-Organisationen. „Bei einem Angriff brauchen wir schnellstmöglich alle Informationen für unser Lagebild“, sagt Hauptmann Gerrit Ohlert*. Der IT-Offizier gehört dem Cyber- und Informationsraum (CIR) an und ist einer von zwei Vertretern der Bundeswehr beim Lagezentrum des BSI. „Wenn wir wissen, womit wir es zu tun haben, können wir die Schäden beseitigen“, erklärt er. Im fiktiven Szenario erhärtet sich der Verdacht eines Cyberangriffs: Das Berliner Energieunternehmen meldet unregelmäßige Zugriffsprotokolle bei einem IT-Zulieferer. Das BSI schlägt Alarm und aktiviert sein nationales Krisenreaktionszentrum.

Ein Ausfall der kritischen Infrastruktur in einem modernen, digitalisierten Land wie Deutschland hat dramatische Folgen: Ampeln fallen aus,

S. 38–39: Y/C3 Markus Spiller, Illustration (2)

Kann das Zufall sein oder ein Anschlag auf wichtige Stromleitungen?

Züge bleiben stehen, Krankenhäuser schalten auf Notstrom. Geschäfte sind geschlossen. Geldautomaten funktionieren nicht mehr. Kein Wasser, keine Heizung. Die Kommunikation kommt zum Erliegen. Niemand kann mehr telefonieren oder ins Internet. Die öffentliche Ordnung ist gefährdet. „Die IT-Systeme von KRITIS-Organisationen sind entsprechend gut geschützt“, erklärt Ohlert. „Die Ebene darunter, also Zulieferer und Subunternehmen, sind es oft nicht. Ihre IT anzugreifen ist einfacher.“ Ein Lieferkettenangriff, mit dem Ziel, indirekt und auf Umwegen in kritische Infrastrukturen einzudringen. „Dafür reicht eine Schwachstelle bei der IT-Sicherheit“, sagt der IT-Experte.

Im Szenario haben Polizeien, Feuerwehren, das Technische Hilfswerk (THW) und andere Behörden und zivile Organisationen Krisenstäbe gebildet. Wer regelt den Straßenverkehr? Wie kommen Flugzeuge sicher auf den Boden und wie fahren Rettungswagen ohne GPS? Das Bundesinnenministerium ist alarmiert und untersucht mögliche politische Hintergründe: Ist der Cyberangriff eine Bedrohung der staatlichen Ordnung, ein Verteidigungs- oder sogar NATO-Bündnisfall? Unwahrscheinlich, aber nicht unmöglich. Russlands Vollinvasion in die Ukraine im Februar 2022 begann mit einem lange vorbereiteten, massiven Cyberangriff. Dabei wurden unter anderem die Websites von ukrainischen Regierungsstellen und Banken gehackt, die Satellitenkommunikation unterbrochen und das öffentliche Mobilfunknetz zerstört. ❯

Die Stadt steht still
In mehreren Berliner Bezirken ist der Strom komplett ausgefallen. Der Autoverkehr kommt zum Erliegen, die Bahnen stehen still, keine Ampeln und kein Licht. Krankenhäuser und andere wichtige Einrichtungen schalten um auf Notstrom – aber der ist zeitlich begrenzt.

Von der Welt abgeschnitten
Erst ist der Strom weg, dann die Kommunikation. Systemausfälle breiten sich kaskadenartig aus. Im Szenario fallen alle gewohnten digitalen Systeme und Dienste aus. Die öffentliche Ordnung ist gefährdet.

Im Krisenmodus
Schnell werden Krisenstäbe gebildet. Im BSI-Lagezentrum sammeln die Fachleute alle verfügbaren Informationen für ein Lagebild. Der Verdacht bestätigt sich: Es ist ein breit angelegter Cyberangriff.

Für den behördenübergreifenden Austausch zur Cybersicherheit haben die staatlichen Behörden 2011 das Nationale Cyber-Abwehrzentrum gegründet. Alle sicherheitsrelevanten Akteure gehören ihm an – von der Bundespolizei und dem BKA über die Nachrichtendienste bis zum BSI und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe. Oberstleutnant Jan Peltzer* vertritt das Kommando CIR mit zwei weiteren Stabsoffizieren im Cyber-Abwehrzentrum: „Alle bringen ihre Erkenntnisse ein, die sie über ihre jeweiligen Kanäle ermitteln, auch die Bundeswehr." Das Kommando CIR betreibt und schützt die Führungs- und Kommunikationsstrukturen in der Bundeswehr. Ohne sichere Kommunikation könnte die Truppe kaum operieren. „Wir brauchen die Informationen, um unseren Auftrag zu erfüllen und verteidigungsfähig zu bleiben", erklärt Peltzer.

Angriffe auf die Bundeswehr

„Die IT der Bundeswehr wird täglich angegriffen – von einfachen Phishing-Mails zum Datenklau bis zu Angriffen auf die Websites. Unsere Systeme sind gut gesichert und wir können Fehlerquellen schnell beheben. Aber wir sind auch abhängig von zivilen Unternehmen – zum Beispiel bei der Versorgung von Dienststellen", sagt der Oberstleutnant. Die Auswirkungen von Cyberangriffen treten oft wellenförmig auf. Immer wieder werden neue Schäden sichtbar, an immer neuen Stellen. Weil alles miteinander zusammenhängt. „Im Szenario gibt es einen typischen Kaskadeneffekt. Häufig liegt der eigentliche Angriff schon zeitlich zurück", so Peltzer. Eine Kaserne des Heeres ist betroffen, sie liegt in einem der Berliner Bezirke. Es gibt weder Strom noch Wasser oder Internet. Aufgrund der unklaren Lage ordnet der Kommandeur Vorsichtsmaßnahmen an: Die Gefährdungsstufe wird auf Bravo erhöht, die Notfallpläne greifen. Unter anderem wird das Wachpersonal der Kaserne verstärkt. Soldatinnen und Soldaten patrouillieren am Kasernenzaun.

Im BSI werden derweil die Spuren des Cyberangriffs verfolgt. Wie weit reicht er zurück und wie lassen sich die beschädigten Systeme isolieren? Im Lagezentrum herrscht Hochbetrieb. Es muss schnell gehen, um den Kaskadeneffekt zu durchbrechen. Hauptmann Ohlert kennt sich mit solchen Szenarien gut aus: „Wir versuchen, Fehlerquellen zu finden, Muster und Zusammenhänge zu erfassen." Das Lagebild wird immer besser, bis der Hergang schließlich klar ist: Der Angriff ist eine Kombination aus Social Engineering und Ransomware. Über einen gehackten Account eines Administrators des IT-Subunternehmers wurde eine Schadsoftware installiert. Fachleute sprechen auch von einem „Low-and-Slow-Angriff". Der Angreifer bewegte sich schon länger unbemerkt im Netz des Dienstleisters und verschaffte sich so Zugang auf Server des Energieversorgers. „Ein Administrator, der die IT-Sicherheit vernachlässigt hat, reicht aus. Persönliche Accounts dienen Angreifern häufig als Einfallstor", so Ohlert.

Wer ist für den Cyberangriff verantwortlich? Im Lagezentrum weiß man noch nichts Genaues. „Wir haben in den meisten Fällen ein Attributionsproblem. Das bedeutet, die Verantwortlichen verschleiern ihre Aktivitäten sehr gezielt und bleiben verborgen", sagt Ohlert. Aber für die Suche nach den Angreifern bleibt auch diesmal keine Zeit. Die Verteidigung hat Vorrang. Im BSI prüfen die Expertinnen und Experten die Abwehrmaßnahmen, die die betroffenen Akteure zur Wiederherstellung ihrer Systeme ergreifen. „So ein Vorgang ist komplex. Es kann durchaus Wochen dauern, bis alles wieder voll funktioniert", so Ohlert. Nachdem die auffälligen Systeme ermittelt und isoliert wurden, geht es darum, die Grundfunktionen zu erhalten sowie die infizierten Systeme zu bereinigen und Back-ups wiederherzustellen. Die Unternehmen bewältigen ihre IT-Sicherheitsvorfälle selbst. Manche greifen dazu auch auf spezialisierte Firmen zurück. Die staatlichen Stellen werden von den Fachleuten des CERT-Bund unterstützt, den Notfallteams des BSI. Im Nachhinein lassen sich die Spuren oft noch genauer zurückverfolgen: Im Dezember 2025 machte die Bundesregierung beispielsweise öffentlich, dass Russland einen Cyberangriff auf die nationale Flugsicherung durchgeführt hatte und eine Desinformationskampagne im Bundestagswahlkampf betrieb. Der russische Botschafter wurde einbestellt. ❯

Schäden bei der Bundeswehr
Die IT-Systeme der Truppe sind gut geschützt, aber sie ist durch ihre Abhängigkeit von zivilen Unternehmen oft indirekt von Cyberangriffen betroffen. Die erste Aufgabe der Fachleute von CIR ist immer, die eigenen Systeme wiederherzustellen.

Vom Opfer zum Verteidiger
Vor Ort unterstützen mobile Teams von CIR bei der Behebung der Störungen und der Bereinigung infizierter Systeme. Die Soldatinnen und Soldaten sind schnell und flexibel einsetzbar – in Deutschland und weltweit.

S. 40–41: Y/C3 Markus Spiller, Illustration (3)

Schnelle Unterstützung
Die Bundeswehr kann zivile Stellen in Krisenlage per Amtshilfe unterstützen. Im Szenario sind auch Logistik- und Sanitätskräfte im Einsatz. Sie übernehmen den Transport wichtiger Medikamente und Organe.

Die Lage wieder im Griff
In einer Pressekonferenz werden wichtige Fortschritte vermeldet. Nach 18 Stunden funktioniert die kritische Infrastruktur Schritt für Schritt wieder, die öffentliche Ordnung kehrt zurück. Die vollständige Behebung aller Schäden des Cyberangriffs kann Wochen dauern.

Noch enger zusammenarbeiten

„Die Hauptaufgabe der Bundeswehr ist immer, die eigenen Systeme zu schützen. Wir müssen verteidigungsbereit bleiben, selbst wenn um uns herum die zivile Infrastruktur ausfällt“, sagt Oberstleutnant Peltzer. Der IT-Offizier weiß, dass die Bundeswehr stets mit Angriffen wie diesem rechnen muss: „Wir sind dabei oft nur indirekt betroffen, also gleichzeitig Opfer und Verteidiger.“ Verteidigen heißt im Szenario nicht nur die eigenen Systeme zu schützen, sondern in der Krisenlage auch per Amtshilfe zu unterstützen. Zwei Krankenhäuser, in denen der Notstrom ausgeht, brauchen dringend Hilfe bei der Verlegung gefährdeter Patientinnen und Patienten. Logistikkräfte und Sanitätspersonal werden alarmiert. Außerdem unterstützen sogenannte Response Teams vom Kommando CIR mit ihren IT-Fähigkeiten die Bezirksämter direkt vor Ort.

18 Stunden später, im BSI atmet man auf. Im Lagezentrum gehen erste Meldungen ein, dass betroffene KRITIS-Einrichtungen ihre Systeme wiederherstellen konnten. Strom- und Wasserversorgung laufen langsam wieder an. Auch die Zusammenarbeit der staatlichen Krisenstäbe zahlt sich aus: Schritt für Schritt kehrt die öffentliche Ordnung zurück. „Das Schlimmste wäre jetzt überstanden, aber es würde noch einige Zeit brauchen, bis alles wieder wie gewohnt funktioniert“, sagt Ohlert. „Vollständige Sicherheit gibt es nicht. Wir müssen uns an solche Lagen gewöhnen, aufpassen und vorbereitet sein.“ Der IT-Offizier verspricht sich viel vom neuen Cybersicherheitsstärkungsgesetz, das im Dezember 2025 in Kraft getreten ist. Künftig unterliegen auch kleinere Unternehmen Vorgaben und Meldepflichten beim BSI. „Am Ende kommt es aber auf uns alle an“, so Ohlert. „Jeder Einzelne trägt zur IT-Sicherheit des großen Ganzen bei.“

S. 42: Y/C3 Markus Spiller, Illustration (2)

Aufklären und wirken

Das PEGASUS-Aufklärungsflugzeug ist von außen nur durch die Ausbuchtungen am Rumpf – die Radome – sowie zusätzliche Antennen von der zivilen Variante zu unterscheiden.

TEXT *Ingmar Hötschel*

Welche Bedeutung die **Elektronische Kampfführung** heute einnimmt, zeigt sich tagtäglich im Kriegsgeschehen in der Ukraine. Wie stellt sich die Bundeswehr auf diese neuen Herausforderungen ein?

In geschützten Fahrzeugen bereiten die EloKa-Kräfte das Lagebild auf und leiten bei Bedarf Gegenmaßnahmen ein.

Die Elektronische Kampfführung (EloKa) ist so alt wie die Nutzung von Funk zur Nachrichtenübertragung. Die wesentlichen Aufträge – aufklären und wirken – haben sich bis heute nicht geändert. Allerdings gilt heute mehr denn je: Wer das elektromagnetische Umfeld dominiert, ist bei Führung und Wirkung dem Feind überlegen. Die technischen Möglichkeiten, um diese Überlegenheit zu erringen, haben sich enorm weiterentwickelt. Doch was ist EloKa und wie sehen die Waffensysteme aus?

EloKa umfasst in der Aufklärung die Möglichkeit, Signale im elektromagnetischen Spektrum mit Sensoren zu erfassen. So kann ausgelesen werden, von wo das Signal ausgestrahlt wurde und was es zum Inhalt hat. Dies kann in ganz unterschiedlichen Frequenzen erfolgen, sei es ein Funkspruch, das Steuerungssignal einer Drohne oder die Signatur eines Radars.

In der Wirkung kommen sogenannte Effektoren zum Einsatz. Mit ihnen lassen sich Signale stören, verändern oder ganz unterdrücken. Ein Beispiel dafür ist im Baltikum täglich zu beobachten: Russische Sender stören hier das GPS-Signal und erschweren so die Navigation.

Wie sowohl Sensoren als auch Effektoren genau funktionieren, welche Reichweite sie haben, welche Frequenzen sie abdecken, all das unterliegt strenger Geheimhaltung. Bekannt ist aber, dass mit den Flottendienstbooten der Klasse 424, dem Aufklärungsflugzeug PEGASUS sowie einem Maßnahmenpaket auf Ebene der Bataillone die EloKa-Kräfte im Laufe der kommenden Jahre modernste Systeme erhalten werden.

S. 44–45: Abel & Stone/David Melzer, Grafik (5)

Auf dem Wasser

Ab 2029 werden drei Flottendienstboote der neuen Klasse 424 in Betrieb genommen und die jetzigen Boote der Oste-Klasse nach über 30 Jahren im Dienst ablösen. Die neue Generation ist mit hochmodernen elektronischen, hydroakustischen und elektro-optischen Sensoren ausgestattet, die von Soldatinnen und Soldaten der EloKa bedient werden. Diese fortschrittliche Sensortechnik ermöglicht eine effiziente Überwachung über Land, Luft und See sowie eine verbesserte Informationsgewinnung. Maschinelles Lernen und künstliche Intelligenz helfen dabei, große Datenmengen nahezu in Echtzeit auszuwerten und militärisch relevante Informationen zu gewinnen.

Darüber hinaus ist der neue Schiffskörper, der im Vergleich zur Oste-Klasse gut 50 Meter länger ist, nicht nur den Anforderungen der Marine angepasst. Er ermöglicht neben einer effizienteren Steuerung auch bessere Arbeitsbedingungen und verfügt über ein Hubschrauber-Landedeck.

In der Luft

Auf Basis der zivilen Bombardier Global 6000 entstehen aktuell drei Aufklärungsflugzeuge PEGASUS (Persistent German Airborne Surveillance System). Diese sind die Nachfolger der Breguet Atlantic, die 2010 außer Dienst gestellt wurden. Die Hauptfähigkeit von PEGASUS ist die Signalerfassende Luftgestützte Weiträumige Überwachung und Aufklärung (SLWÜA). Das System dient somit der Krisenfrüherkennung, Lagebeurteilung und Feststellung der Bedrohungslage in potenziellen Einsatzgebieten. Im Vergleich zur Breguet Atlantic ermöglicht der höhere Automatisierungsgrad der PEGASUS, mehr Signale zu erfassen, zu klassifizieren und somit ein deutlich verbessertes und dichteres Lagebild zu erstellen. Zudem haben die Bedienenden deutlich verbesserte Arbeitsbedingungen.

An Land

Um den zwingend notwendigen Sofortbedarf des Heeres im Bereich EloKa zu decken, werden bei der Beschaffung neue Wege beschritten: Als Basis werden bereits marktverfügbare Systeme beschafft, was eine schnelle Ausstattung der Truppe, insbesondere der Brigade Litauen, ermöglicht. So wird eine „Fight-Tonight-Fähigkeit“ noch in 2026 erreicht. Dabei werden hochmobile Systeme beschafft, welche dem Heer – durch die Teilstreitkraft CIR betrieben – auf taktischer Aufklärungs- und Wirkungsebene zur Verfügung gestellt werden. Diese Systeme ermöglichen Aufklärung sowie Wirkung im gesamten elektromagnetischen Spektrum. Das umfasst sowohl Funk, als auch Drohnen und Radare. Damit tragen sie erheblich zu einer besseren Operationsführung des Heeres bei.

Auf Flottendienstbooten kümmert sich die Stammcrew um den nautischen Betrieb, während EloKa-Spezialistinnen und -Spezialisten für die Fernmelde- und elektronische Aufklärung zuständig sind.

Mit Sensoren im UHF-Spektrum lassen sich unter anderem Radarstrahlung sowie Navigations- und Funksignale erfassen.

Effektoren auf Trägerfahrzeugen erlauben die Störung von feindlichen Signalen auch im agilen Gefecht.

Bei allen Abbildungen handelt es sich um Zeichnungen, die aus Geheimhaltungsgründen nicht alle Details abbilden.

EloKa im Einsatz

Mobile Effektoren und Sensoren sind die Waffensysteme des Cyber- und Informationsraums. Diese Grafik zeigt einige der strategischen und taktischen Möglichkeiten der Elektronischen Kampfführung, im Verbund zu wirken.

TEXT *Ingmar Hötschel*

Raum aufklären
Durch tiefe Aufklärung lassen sich zum Beispiel frühzeitig Truppenbewegungen erkennen. Auch rückwärtige Einrichtungen wie Flugabwehrstellungen sind so aufklärbar.

Funk überwachen
Funksignale, die etwa von Gefechtsständen ausgehen, können aufgefangen und ausgewertet werden. Zudem können diese Hochwertziele so direkt bekämpft werden.

Drohnen stören
Effektoren können in bestimmten Bereichen beispielsweise Signale zur Steuerung von Drohnen effektiv stören.

1 Strategische Luftaufklärung
Das Aufklärungsflugzeug PEGASUS ermöglicht eine Aufklärung bis weit in den feindlichen Raum hinein und kann so frühzeitig potenzielle Gefährdungen erkennen.

2 Strategische Seeaufklärung
Mit den Flottendienstbooten können über lange Zeiträume und große Reichweiten Signale an Land sowie über und unter Wasser erfasst und ausgewertet werden.

3 Taktische Aufklärung
Mit mobilen Sensoren auf der taktischen Ebene unterstützen die EloKa-Bataillone die kämpfende Truppe auf Brigade- und Divisionsebene durch Aufklärung in deren Wirkungsbereich.

4 Taktische Führung
In geschützten Fahrzeugen werden alle Daten zu Lagebildern verdichtet, die den Kommandeuren eine Führungs- und Wirkungsüberlegenheit geben. Von dort aus wird auch der Einsatz von Effektoren gesteuert.

5 Taktische Wirkung
Effektoren sind in der Lage, Signale zu stören, gänzlich zu unterbinden oder auch zu ändern – je nach Frequenz und gewünschter Wirkung. Hochmobil können sie der Truppe im Gefecht folgen und so die gewünschte Wirkung zielgerichtet entfalten.

S. 46–47: Abel & Stone/David Melzer, Infografik

KAMPFWERT-STEIGERUNG PER SOFTWARE

Das Gefechtsfeld verändert sich immer schneller. Schritt halten können da nur Systeme, die sich rasch anpassen lassen.

TEXT *Ingmar Hötschel*

Durch ein sich immer dynamischer veränderndes Umfeld stellt sich die Frage: Wie kann es gelingen, beispielsweise eine Fregatte oder einen Eurofighter, deren Nutzungsdauer mehrere Jahrzehnte beträgt, auf diese Bedingungen auszurichten? Das moderne Gefechtsfeld verändert sich zu schnell, um in der gleichen Geschwindigkeit Material und Personal – dem eine immer höhere Bedeutung zukommt – aufwachsen zu lassen. Dazu kommen immer kürzere Innovationszyklen.

Hier kommt das Zentrum Digitalisierung der Bundeswehr und Fähigkeitsentwicklung Cyber- und Informationsraum (ZDigBw) ins Spiel. Unter dem Stichwort Software Defined Defence (SDD) wurden hier mehrere Prinzipien erarbeitet, die jetzt nach und nach in die Praxis implementiert werden – sowohl für bereits bestehende als auch neu zu beschaffende Systeme. Software rückt damit in den Mittelpunkt der Kampfwertsteigerung von Waffensystemen.

Eine Nutzung über Jahrzehnte ist nur durch eine Anpassung der Aufklärungssysteme möglich.

OFFENER QUELLCODE

Ein Prinzip hinter SDD ist ein offener Quellcode der Software, die von den Herstellern in den Systemen verbaut wird, damit andere Hersteller oder die Bundeswehr selbst Änderungen vornehmen können. Wie sich das in der Praxis auswirkt, wurde bei einem umfangreichen Test von Drohnen im Gefechtsübungszentrum Heer Ende 2025 erlebbar. Dort konnten die Drohnenbediener und Teileinheitsführer ihre Anforderungen formulieren: Welche Funktion ist für die Auftragserfüllung unabdingbar, was sollte in der Bedienung anders sein, um diese intuitiver zu machen? Über Nacht konnten die Softwareentwickler diese Fähigkeitsanforderungen in den offenen Quellcode programmieren und sie direkt am nächsten Tag zur Verfügung stellen. Eine Innovationsgeschwindigkeit, die zwingend notwendig ist, um auf dem Gefechtsfeld zu bestehen.

Fest verbaute Sensoren – wie hier am Rumpf von PEGASUS – lassen sich nicht einfach umrüsten. Hier kann Software helfen, die Technik fit für neue Anforderungen zu machen.

Die Software einer Drohne lässt sich durch SDD schnell an Nutzeranforderungen anpassen.

Mithilfe offener Schnittstellen können Drohnen unterschiedlichster Hersteller auch miteinander vernetzt werden.

S. 48: Bundeswehr/Björn Wilke (l.o.), Bundeswehr/Lea Bacherle (r.o.), Bundeswehr/Marco Dorow (l.u.), STARK Systems (r.u.), S. 49: Bundeswehr/Marco Dorow (o.), Bundeswehr/Maximilian Schulz (u.)

SCHNITTSTELLEN

Neben dem offenen Quellcode muss die Software Schnittstellen zu anderen Anwendungen und Systemen zulassen und darf nicht ausschließlich darauf ausgelegt sein, das vom Hersteller gedachte System zu bedienen. Vielmehr müssen direkt von Beginn an zusätzliche Kapazitäten mit geplant sein. Das beginnt bei so einfachen Dingen wie Speicherplatz. Reicht dieser aus, um neue Software aufspielen zu können? Dies wird beispielsweise bei SitaWare Frontline deutlich. Diese Nachfolgelösung des Führungsinformationssystems des Heeres verfügt über offene Schnittstellen, über die weitere Applikationen angebunden werden können, beispielsweise Datenbanken zur Tragfähigkeit von Brücken oder die Position von Kräften, die nicht der Bundeswehr angehören, wie zivile Behörden und Organisationen mit Sicherheitsaufgaben.

ENTWICKLUNG, SICHERHEIT, BETRIEB

Des Weiteren muss die Software auch über eine Vielzahl von Waffensystemen hinweg ausgerollt werden können. Auch Schulungen der Nutzenden müssen von Anfang an mitgedacht werden. Es nützt wenig, wenn ein Panzer über eine neue Funktionalität verfügt, der Bediener diese im Zweifelsfall aber nicht kennt. Hier greift in SDD das Prinzip des DevSecOps Cycle, ein Kreislauf aus Entwicklung (Development), Sicherheit (Security) und Betrieb (Operations). Dieser beschreibt, vereinfacht formuliert, die Entwicklungsschritte in der Software-Programmierung inklusive aller dazugehörigen Sicherheitsmechanismen. So lernen die Anwendenden nicht nur die Bedienung des Systems, sondern gleich auch, wie sie die Software für ihre Bedarfe anpassen können.

Eine gute Vernetzung im Hintergrund – auch zwischen Nationen – ist ein Merkmal von Multi-Domain Operations.

Die Integration weiterer Module durch offene Schnittstellen trägt zu einem besseren Lagebild bei.

MULTI-DOMAIN OPERATIONS

Beachtet man alle Leitprinzipien, die hinter SDD stehen, dann ist SDD eines der Elemente, die moderne militärische Operationen im Sinne von Multi-Domain Operations (MDO) erst ermöglichen. Unter MDO versteht die NATO das Zusammenwirken militärischer Kräfte über alle Dimensionen sowie NATO-Partner hinweg, synchronisiert mit zivilen Kräften, um einen schnellen und bestmöglichen Effekt zu erzielen. Dabei spielt Software eine entscheidende Rolle: Nur mit dieser ist es möglich, einerseits schnell eine Vielzahl an Informationen aus den unterschiedlichsten Quellen aufzubereiten und für ein Lagebild zur Verfügung zu stellen. Andererseits vernetzt es die bereits etablierten Waffensysteme, sodass eine zielgerichtete Wirkung angepasster, schneller und präziser erfolgen kann.

Der Umfang dieser MDO macht deutlich, dass SDD noch am Anfang steht – entscheidend wird sein, dieses vernetzte und agile Denken sowie die Prinzipien von SDD in alle Bereiche zu implementieren. Um dieses Vorhaben bestmöglich zu unterstützen, wurde im Mai 2025 das neue Dezernat „Operationalisierung Software Defined Defence“ eingerichtet. Das neue Team, für das Fachleute aus dem gesamten ZDigBw zusammengezogen wurden, hat den Auftrag, die Umsetzung und Operationalisierung der Fachaufträge im Rahmen von SDD zu planen und zu koordinieren.

Das autonome Fahrzeug Volia-E wird von der Ukraine eingesetzt, um Nachschub zu transportieren und Verwundete zu evakuieren. Gesteuert wird es aus bis zu drei Kilometern Entfernung. Dabei erreicht der Bodenroboter bis zu zwölf Kilometer pro Stunde und kann Lasten bis 150 Kilogramm tragen.

2

Kapitel

Künstliche Intelligenz

Die neue Normalität

Selbstfahrende Militärfahrzeuge, von KI gelenkte Kampfjets, autonome Drohnen. Künstliche Intelligenz hält in vielen militärischen Bereichen Einzug. Doch viele Fragen sind noch offen. Wie lässt sie sich kontrollieren? Wer trägt am Ende die Verantwortung?

TEXT *Julia Egleder*

Fahrzeuge rollen in der Ukraine durchs Gelände – ganz ohne Fahrer. Die Steuerung übernimmt eine KI. Sie erkennt Büsche, Bäume und Gräben, berechnet in Sekunden den besten Weg und fährt selbstständig zu den Soldaten und Soldatinnen an der Front. Dorthin liefert das Fahrzeug Nachschub und bringt Verwundete mit zurück.

Szenenwechsel: In Deutschland greifen Drohnen Ziele an. Gesteuert von einer KI, die zuvor Millionen von Daten ausgewertet hat. Gezeigt wurde das bei einem Test am Gefechtsübungszentrum des Heeres im Dezember 2025. Generalinspekteur Carsten Breuer zeigte sich nach dem Besuch beeindruckt vom Funktionieren des Wirkverbunds. Seine Einschätzung damals: „Auf dem Gefechtsfeld der Zukunft werden Daten zur Waffe. Wer sie schneller verarbeitet, hat einen militärischen Vorteil."

Noch ein Szenenwechsel: Im Frühjahr 2025 schossen pakistanische Kampfjets im jüngsten Konflikt mit dem Nachbarland mehrere indische Rafale-Kampfjets ab. Fachleute vermuten, dass eine leistungsfähige, KI-gestützte Combat Cloud Radardaten in Sekundenbruchteilen mit Jets und Lenkwaffen teilte – und so den Pakistanern einen entscheidenden Vorteil in der Luft verschaffte. Bemerkenswert dabei: Die eingesetzten Kampfjets und Raketen stammten aus chinesischer Produktion.

Handeln im Verbund

Das autonome Fahrzeug Gereon RCS von ARX Robotics kann zur Aufklärung genutzt und mit verschiedenen Sensoren ausgerüstet werden. Unbemannte Bodenfahrzeuge wie dieses könnten beim Gefechtskonzept Recce Strike eingesetzt werden. Hierbei werden Aufklärung (Recce) und Wirkung (Strike) sehr schnell miteinander verknüpft.

Loitering Munition wie die Drohne HX-2 können bei Recce Strike für die Wirkung eingesetzt werden. Die Drohne findet ihr Ziel, nachdem sie von einem aufklärenden autonomen Fahrzeug die entsprechenden Daten übermittelt bekommen hat. Laut Hersteller Helsing kann die HX-2 Ziele in bis zu 100 Kilometer Entfernung bekämpfen.

Ein Soldat ist per Computer bei Recce Strike eingebunden. Die **Software „Altra"** von Helsing wertet die Daten verschiedener Sensoren KI-gestützt aus. Der Soldat orchestriert als Operateur den Prozess.

Aufklärung

Die Langstreckenaufklärungsdrohne DeltaQuad Evo fliegt bis zu 270 Kilometer weit und kann viereinhalb Stunden in der Luft bleiben. Die Bundeswehr hat sie bei einer Heeresübung im Dezember 2025 getestet.

Combat Cloud

China und Pakistan entwickelten gemeinsam den Kampfjet JF-17, der über eine Combat Cloud vernetzt ist. Das sorgte 2025 für einen taktischen Vorteil: Bei einer Konfrontation mit Nachbar Indien konnten die pakistanischen Jets mehrere Rafale-Jets der indischen Luftwaffe abschießen.

S. 52: ARX Robotics (Gereon RCS) (o.), Delta Quad (u.).
S. 53: Helsing (o.1–2), picture alliance/dpa/MAXPPP (u.)

Diese ukrainische Drohne ist über hauchdünne Datenkabel mit einem Piloten verbunden. Ein Container am Bauch der Drohne spult das Kabel ab. Diese Drohnen können zwar nicht mit elektronischen Mitteln gestört werden, aber die Kabel verheddern sich oft in Bäumen.

Wenn das Funknetz ausfällt

Bei einigen Frontabschnitten in der Ukraine hängen die Datenkabel der Drohnen wie Lametta in Bäumen und Feldern. Auf Kabel wie diese greifen beide Konfliktparteien zurück, da eine Steuerung über Datenfunk aufgrund der Störungen des Funknetzes schwierig ist.

Zwei russische Soldaten bereiten eine **Lancet-Drohne** für den Start vor. Diese Drohne ist bei den Ukrainern gefürchtet. Sie fliegt Strecken nach programmierten Wegpunkten und braucht deshalb keine dauerhafte Funkverbindung.

Zuverlässigkeit fehlt noch

Das sind nur drei von vielen Beispielen dafür, wie KI in den Streitkräften bereits eingesetzt wird. Denn das Potenzial ist enorm. KI kann riesige Datenmengen in Sekunden auswerten, Muster erkennen, Entscheidungen vorbereiten – oder gleich selbst treffen. Oft schneller und zuverlässiger als ein Mensch.

Und KI wirkt nicht nur auf dem Gefechtsfeld. Auch in den Büros der Soldatinnen und Soldaten hält sie Einzug. Streitkräfte entwickeln eigene Large Language Models (LLM). Das sind KI-Systeme, die auf riesigen Textdatensätzen trainiert wurden, die zum Beispiel Tausende Dokumente in kürzester Zeit nach relevanten Informationen durchsuchen können. Das spart Zeit, entlastet die Menschen und macht die Arbeit deutlich effizienter.

Doch auf die Frage, welche KI-Entwicklung ihn in den vergangenen Monaten am meisten beeindruckt hat, zögert Dr. Frank Sauer, KI-Experte an der Universität der Bundeswehr München, zunächst. Dann sagt er: „Ehrlich gesagt hat mich eher überrascht, dass es beim effektiven Einsatz von KI immer noch so viele Hürden gibt."

Ein Beispiel ist die Loitering Munition in der Ukraine. Bereits 2023 berichteten Medien wie „The Economist" und die „New York Times", dass ukrainische Drohnen mithilfe moderner KI auf den letzten Metern autonom agieren, also ohne Verbindung zum Piloten. Damit seien sie weitgehend unempfindlich gegen russische elektronische Störmaßnahmen. Genau darauf zielt das Prinzip der Loitering Munition ab: Drohnen, die über einem Gebiet kreisen, das Gelände beobachten und sich auf ihr Ziel stürzen, sobald sie es als solches erkennen.

Doch laut Sauer läuft das in der Praxis selten so reibungslos. Viele Drohnen erkennen ihre Ziele nicht so zuverlässig wie erhofft, die Trefferquote bleibt hinter den Erwartungen zurück. Ein zentraler Grund dafür: Die KI wurde im Vorfeld mit zu wenig passenden Trainingsdaten gefüttert.

„Drohnen sind vergleichsweise billig und lassen sich schnell herstellen."

Dr. Frank Sauer
KI-Experte, Universität der Bundeswehr München

„Wer hat schon Tausende Bilder eines russischen T-72-Kampfpanzers – und das in unterschiedlichen Landschaften und Szenarien", sagt Sauer. Steht ein Panzer halb im Schnee, verborgen hinter einem Busch oder nur teilweise sichtbar, gerät die KI schnell an ihre Grenzen. Auch Nebel, Regen oder schlechte Sichtverhältnisse stören die Zielerkennung erheblich. Gleiches gilt für einfache Tarnmaßnahmen, etwa auf Fahrzeuge gelegte Autoreifen. All das kann ausreichen, um die KI zu täuschen. Das ist nicht nur aufseiten der Ukrainer so. Laut Sauer funktioniere auch die gefürchtete russische Loitering-Munition-Drohne Lancet nicht immer treffgenau.

Viele Hürden in der Praxis

Weil autonome Systeme noch immer an ihre Grenzen stoßen, setzen beide Kriegsparteien weiterhin auf die Steuerung durch einen Menschen. Russische wie ukrainische Drohnenpiloten verbinden ihr Fluggerät deshalb mit hauchdünnen Glasfaserkabeln. So können sie die Drohnen auch dann steuern, wenn elektronische Störmaßnahmen wirken. Entlang der Front hängen diese weißen Kabel inzwischen wie Lametta in den Bäumen.

Trotz aller Probleme sieht der KI-Experte in der Loitering Munition großes Potenzial. „Diese Drohnen sind vergleichsweise billig und lassen sich schnell in großer Stückzahl herstellen", sagt Sauer. Westliche Streitkräfte sollten sich seiner Ansicht nach zügig damit ausrüsten, um im Verteidigungsfall wirksam gegen russische Kräfte vorgehen zu können.

„Die Jahre bis 2029 sind die gefährlichsten", warnt Sauer. In diesem Zeitraum hält er einen russischen Angriff auf einen NATO-Bündnispartner für am wahrscheinlichsten. Bis neue Großwaffensysteme wie Kampfpanzer oder Jets geliefert werden, vergehe viel Zeit. Effektive Loitering Munition hingegen könne kurzfristig einen entscheidenden Unterschied machen.

S. 54: IMAGO/SOPA Images/Mykhaylo Palinchak (o.), SOPA Images/LightRocket via Getty Images/Francisco Richart (u.)
S. 55: picture alliance/ZUMAPRESS.com/Alexei Konovalov (o.)

Feindlicher Panzer?

KI-gesteuerte militärische Geräte haben hohe technische Voraussetzungen und einen enormen Bedarf an Trainingsdaten. Auf den ersten Blick ist die getarnte ukrainische Panzerhaubitze in der Region Donezk kaum zu erkennen. Kann eine KI sie zweifelsfrei identifizieren und sicher zwischen Freund und Feind unterscheiden? Viele Fachleute sind überzeugt, dass der Mensch am Ende die Kontrolle behalten muss.

Doch fehlende Trainingsdaten sind nur ein Teil des Problems. Der Einsatz von KI in Waffensystemen bringt weitere Herausforderungen mit sich. Trainingsdaten und Algorithmen können zum Beispiel durch den Gegner manipuliert werden. Etwa dadurch, dass zum Beispiel falsche Bilder in den Pool an Trainingsdaten gelangen. Dieser speist sich nämlich mitunter aus öffentlich zugänglichen Onlinequellen. Wenn dort Fotos von T-72-Panzer auftauchen, die aber gar keine T-72 zeigen, wird der Algorithmus falsch trainiert und die KI kann hinterher den Panzer nicht einwandfrei erkennen. Viele Soldatinnen und Soldaten begegnen KI deshalb weiterhin mit Skepsis und vertrauen den Systemen noch nicht vollständig.

Hinzu kommt der technische Aufwand: KI in bestehende Systeme wie Fahrzeuge oder Waffen zu integrieren, ist komplex und teuer. Außerdem sind viele KI-Anwendungen auf stabile Datenverbindungen angewiesen. „Und die sind an der Front oft überlastet oder gestört“, erklärt Oberstleutnant i. G. Maximilian Heimer*. Er arbeitet als Referent für Cyberoperationen im Kommando Cyber- und Informationsraum der Bundeswehr und ist dort auch Beauftragter für künstliche Intelligenz.

Im texanischen Abilene entsteht ein riesiges **Rechenzentrum für die KI-Modelle** von ChatGPT-Anbieter OpenAI. Es wird mit einer Leistung von 1,5 Gigawatt eines der größten Rechenzentren der Welt sein.

*Mit Sternchen gekennzeichnete Namen sind zum Schutz der Personen geändert.

Eine Frage, die in Fachkreisen besonders diskutiert wird: Wie behält der Mensch die Kontrolle über die KI? Die generierten Daten müssen sicher und zuverlässig sein, um sie guten Gewissens zum Beispiel zur Zielerkennung einsetzen zu können. Dafür muss die KI feindliche Kräfte auch in unübersichtlichen Lagen eindeutig erkennen können – damit das Risiko von Kollateralschäden möglichst gering bleibt.

Autonom versus Kontrolle

Das wirft eine grundlegende Frage auf: Kann ein Mensch überhaupt noch nachvollziehen, wie eine KI zu ihrer Zielauswahl kommt? Für Frank Sauer ist die Antwort klar: „Dort, wo Situationen chaotisch sind und Menschenleben auf dem Spiel stehen, muss der Mensch zentral bleiben.“ Er müsse nachvollziehen können, warum die KI ein Ziel auswählt, und beurteilen, ob es gerechtfertigt ist, es zu bekämpfen. Das gilt besonders für Einsätze in dicht besiedelten Gebieten.

Anders sieht Sauer das bei klaren, technisch überschaubaren Szenarien. Etwa, wenn eine Fregatte auf hoher See einen anfliegenden Flugkörper abwehrt. In solchen Fällen könnte KI große Teile der Kill Chain übernehmen und autonom gegen Raketen oder Drohnen vorgehen. Zivile Opfer seien hier nicht zu erwarten.

Oberstleutnant Heimer widerspricht zudem der Vorstellung, KI sei grundsätzlich unkontrollierbar. Validierungs- und Testverfahren, wie sie im Beschaffungsprozess der Bundeswehr ohnehin vorgeschrieben sind, könnten die Funktionsweise von KI-Systemen transparent machen, auch wenn nie vollständige Sicherheit erreicht werde. „Aber die gibt es bei anderen technischen Systemen ebenfalls nicht. Beim Autofahren kann auch jederzeit etwas kaputtgehen“, sagt Heimer.

Hinzu kommt: Der Mensch ist nicht automatisch der bessere Entscheider. „Wir sind langsamer, werden müde und lassen uns von Emotionen beeinflussen“, sagt Heimer. KI hingegen arbeite konsistent und unter Bedingungen, für die sie ausreichend trainiert wurde, um einiges verlässlicher als der Mensch.

Klar ist: Die Entwicklung wird sich weiter beschleunigen. In den USA entstehen riesige Rechenzentren, Milliarden fließen in militärische KI-Forschung. Tech-Konzerne wie Google und OpenAI treiben die Entwicklung leistungsfähiger Modelle voran. Auch China überrascht immer wieder mit schnellen Fortschritten, zuletzt mit dem ressourcensparenden LLM DeepSeek. In Deutschland gibt es ebenfalls große Innovationskraft: Zahlreiche Start-ups arbeiten an KI-gestützten Fahrzeugen, Drohnen und Sensorsystemen. Die Bundeswehr setzt KI bislang eher vorsichtig und in klar begrenzten Bereichen ein. Russland dagegen halten Expertinnen und Experten für abgeschlagen: Viele junge IT-Fachleute haben das Land seit Beginn des Angriffskriegs verlassen, westliche Sanktionen erschweren den Zugang zu moderner Technologie.

Trotz aller Unterschiede zwischen den Staaten beim KI-Einsatz gilt: Die Streitkraft, die KI sicher, zuverlässig, verantwortungsvoll und rechtskonform einsetzt, ist für die Konflikte der Zukunft am besten gerüstet.

Die **CA-1 Europa** des Münchener Start-ups Helsing könnte der erste autonome KI-Kampfjet „Made in Germany“ werden. Er wird für Schwarmangriffe entwickelt. Der Erstflug ist für das Jahr 2027 geplant.

Von der Aufklärungsdrohne Vector des Start-ups Quantum Systems aus Gilching erhält das Heer bis 2027 schrittweise 600 Stück. Sie soll automatisch Fahrzeuge und Personen erkennen und diese selbstständig verfolgen können.

Autonome Systeme

Deutsche Start-ups sind sehr innovativ bei der Entwicklung von hochspezialisierter Drohnentechnik. Zwar hapert es hierzulande noch bei der Massenproduktion, aber deutsche Hersteller sind weltweit anerkannt für Hightech-Nischenprodukte, die autonom agieren.

Die **Überwasserdrohne Vanta** vom Berliner Start-up Stark Defence wurde entwickelt, um maritime kritische Infrastruktur zu schützen. Laut Hersteller kann die Vanta Bedrohungen selbstständig identifizieren.

S. 56: Anadolu via Getty Images/Jose Colon (o.), Getty Images/Bloomberg/Kyle Grillot (u.)
S. 57: Helsing (o.), Quantum Systems (m.), STARK Systems (u.)

Besserer Überblick
Ein aktuelles und vollständiges Lagebild erhöht die Erfolgsaussichten im Gefecht. Die Bundeswehr setzt auf KI, um Sensordaten aus verschiedenen Quellen zusammenzuführen und so den Überblick über das Gefechtsfeld zu behalten.

DIE ZUKUNFT IST JETZT

Weltweit beschäftigen sich Streitkräfte mit teilautonomer und selbstlernender Software. Auch die Bundeswehr arbeitet an vielen KI-Anwendungen. Y gibt Einblick in elf aktuelle KI-Projekte.

TEXT *Timo Kather*

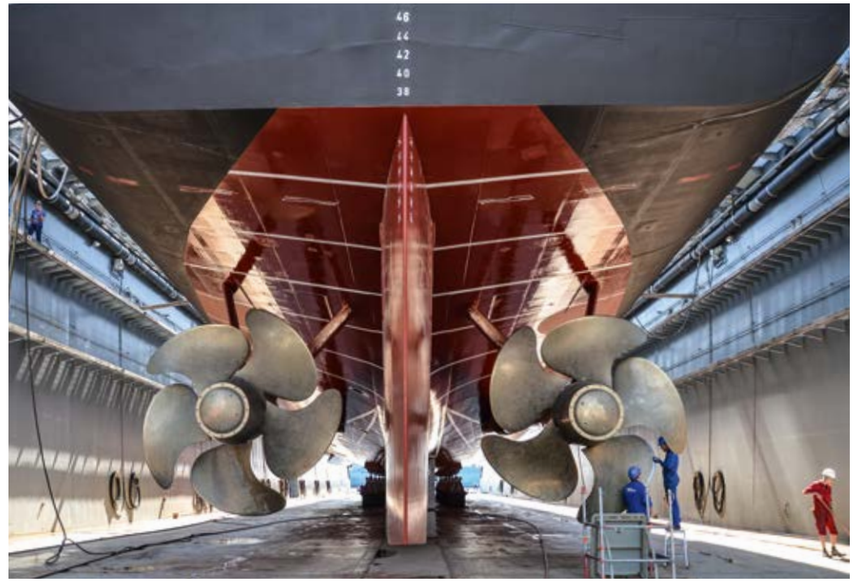
Magie ist es zwar nicht, sondern eine clevere Kombination von Programmierkunst und Mathematik – aber im Ergebnis mutet der Einsatz von KI manchmal schon wie Zauberei an. In wenigen Sekunden sind die Computerprogramme in der Lage, unfassbare Mengen an Informationen zu sortieren, zu analysieren und in fast jeder gewünschten Form zu präsentieren, um den Menschen das Leben und die Arbeit zu erleichtern. Zwei Drittel der Deutschen setzt KI-Tools bereits regelmäßig ein und auch die Streitkräfte weltweit loten ihre militärischen Einsatzmöglichkeiten aus. Die KI-Datenbank der Bundeswehr umfasst zum Beispiel mehr als 400 Einträge. Wir stellen eine Auswahl der dort verzeichneten Projekte vor.

1 TAKTISCHE ÜBERWACHUNG

Eines der prominentesten Projekte der Bundeswehr ist Uranos KI, dessen Beschaffung im Dezember 2025 vom Bundestag bewilligt wurde. Die Ausstattung mit Drohnen, Bodenkontrollstationen und künstlicher Intelligenz wird für die taktische Überwachung großer Räume an der NATO-Ostflanke entwickelt. Ziel ist die Verbesserung und Beschleunigung der Kette zwischen Sensorik, Führungs- und Waffensystemen. Die KI sammelt sämtliche Daten, die von den Uranos-Sensorplattformen eines Kampfbataillons in der Luft und am Boden aufgezeichnet werden, und fusioniert sie zu einem einheitlichen Lagebild. Das passiert nahezu in Echtzeit, so bleibt Uranos KI kaum eine Veränderung auf dem Gefechtsfeld verborgen. Zwei Kampfbataillone der Brigade Litauen sollen spätestens ab Mitte 2027 jeweils eine erste Version erhalten.

2 ERFOLGSCHANCEN ABSCHÄTZEN

Mit der Abschätzung der Erfolgschancen einer Militäroperation beschäftigt sich das Projekt „Reinforcement Learning für komplexe Gefechtssituationen“ des Amts für Heeresentwicklung. Mit KI-Hilfe wird dabei eine Gefechtssimulationsumgebung für Bataillonskommandeure geschaffen, die viele der für eine Entscheidung relevanten Informationen einbezieht – zum Beispiel zum Zustand des Geländes, zu den verfügbaren eigenen Kräften und zu den Aktivitäten des Gegners. So können Kommandeure zum einen die Erfolgsaussichten ihrer Entscheidungen im Vorfeld überprüfen, zum anderen kann die Software auch taktische Empfehlungen abgeben. Beides macht die KI auch für die Ausbildung militärischer Führungskräfte interessant.



3 SEEGEBIETE KONTROLLIEREN

Der Schutz der kritischen Infrastruktur in der Ostsee – zum Beispiel Datenkabel oder Energie-Pipelines – ist seit dem russischen Überfall auf die Ukraine ein wichtiges Anliegen der Marine. Um das Seegebiet zu schützen, sollen unbemannte Unterwasserdrohnen, wie zum Beispiel die zur Beschaffung anstehende Blue Whale, künftig auch mit KI-Unterstützung auf Patrouillenfahrt gehen. Dafür wird die Software mit einer Bilddatenbank darauf trainiert, etwaige Beschädigungen an der unterseeischen Infrastruktur zu erkennen. Zudem ist die Drohne dank KI auch in der Lage, Suchaufträge teilautomatisiert auszuführen, zum Beispiel nach Seeminen oder nach Schiffen der berüchtigten russischen Schattenflotte. Wird ihre Sensorik erweitert, könnten die Drohnen auch zum Aufspüren gegnerischer U-Boote eingesetzt werden.

Schwimmendes Auge
Die Unterwasserdrohne Blue Whale patrouilliert selbstständig und meldet Schäden an Datenkabeln oder Pipelines.

4 BIG DATA FÜR DIE SCHIFFSWARTUNG

Eine am Bedarf ausgerichtete und daher wirtschaftlichere Instandsetzung von Kriegsschiffen der Marine ist Ziel des Projekts „Predictive Maintenance“. Dabei geht es um die Prognose von Instandsetzungsbedarfen, um Verschleiße frühzeitig zu erkennen, Werftliegezeiten im Voraus zu planen und so die Verfügbarkeit der Waffensysteme zu erhöhen. Die einzelnen Anlagen der Schiffe werden derzeit ausschließlich in festen Intervallen gewartet, womit der tatsächliche Zustand eines Schiffs nur grob abgeschätzt werden kann. Mithilfe der Software soll es künftig möglich werden, die Sensordaten der Anlagen so miteinander in Beziehung zu setzen, dass Anomalien in der Schiffstechnik bemerkt werden. Funktioniert die Software wie erwartet, sollen die neuen Fregatten der Marine bald damit ausgestattet werden.

Schnelle Checks
Mithilfe von KI sollen Instandsetzungsbedarfe von Kriegsschiffen künftig schon im Vorfeld festgestellt werden.

5 TECHNISCHER SUPPORT

Der Eurofighter der Luftwaffe ist ein hochkomplexes Waffensystem, das intensiver Wartung bedarf. Zur Lösung technischer Fragen gibt es ein Systemunterstützungszentrum. ❱

S. 58: Bundeswehr/Tom Twardy
S. 59: Bundeswehr (l.u.), Bundeswehr/Susanne Krause-Weers (r.o.), Bundeswehr/Tom Twardy (r.u.)

Bisher durchsuchen die Ingenieure die offiziellen Dokumentationen, um die richtige Antwort auf ein Problem zu finden – ein Prozess, der viel Zeit in Anspruch nimmt. Daher wird an einer KI-gestützten Software namens Hubitus gearbeitet, um die Suche zu beschleunigen. Hubitus durchforstet in Sekundenschnelle den gesamten Dokumentenbestand zum Eurofighter: Entwicklungsunterlagen, technische Dokumentationen und künftig auch weitere Bestände wie die Regelungsdatenbank der Bundeswehr. Danach präsentiert die KI Nutzenden eine Lösung für ihr Anliegen. Der Recherche- und Interpretationsaufwand reduziert sich durch ihre Hilfe erheblich.

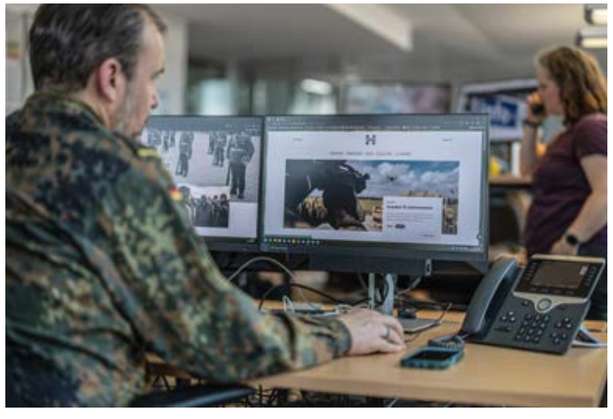
Effiziente Tools
Mit generativer KI sind zeitaufwendige Routinearbeiten im Nu erledigt. Damit bleibt mehr Zeit für wirklich Wichtiges.

6 ASSISTENT FÜR DEN DIENSTBETRIEB

In der Bundeswehr werden noch ab diesem Jahr unter dem Oberbegriff generative künstliche Intelligenz (genAI) die ersten zwei Lösungen an den Start gehen: SearchGPT und Virtual Dokument Assistent (VDA). SearchGPT ist eine KI-unterstützte Suchmaschine für das Intranet der Bundeswehr mit vielen Datenquellen wie dem Dokumentenmanagement, dem zentralen Regelungsmanagement und dem Wiki. Aus den angeschlossenen Datenquellen kann SearchGPT Fragen beantworten und Nutzenden die Quellen nennen, sodass die KI-generierten Antworten überprüft werden können. Die Funktionen des VDA ähneln jenen, die von ChatGPT und Co. im privaten Bereich geläufig sind, jedoch optimiert für die Arbeitsprozesse der Bundeswehr – zum Beispiel zum Finden und Verarbeiten interner Informationen, zur Übersetzung, Erschließung und Zusammenfassung von Dokumenten oder zur teilautomatisierten Erstellung neuer Dokumente. Der genAI-Service erspart mit seinen ersten zwei Anwendungen das mühselige Zusammentragen und Aufbereiten von Informationen und kann somit menschliche Arbeitsprozesse unterstützen und beschleunigen.

7 FAKE NEWS AUFSPÜREN

Eine weitere Software, an dessen Entwicklung das Zentrum Digitalisierung der Bundeswehr zusammen mit der Truppe aktuell arbeitet, ist Internet Reconnaissance, kurz iRec. Die Software kann Daten und Informationen aus dem Internet suchen und sammeln. Besteht zum Beispiel der begründete Verdacht, dass zu einem Thema gezielt Falschinformationen verbreitet werden, wird der iRec-Webcrawler aktiv. Dieser sucht rund um die Uhr nach relevanten Daten im Internet, um die Quelle der Fake News zu finden. Auch Video- und Audiodateien können erfasst und ausgewertet werden. So lassen sich schnell große Datenmengen automatisiert verarbeiten, die für das Fachpersonal nicht zu bewältigen wären. Anschließend verknüpft iRec die gesammelten Informationen und wertet sie als Beitrag zum militärischen Lagebild aus. Die Software wird für die Bundeswehr weiterentwickelt.



8 KAMPFSTOFFE SICHER DETEKTIEREN

Im Unterstützungsbereich der Bundeswehr wird die Einbindung von KI in der Kampfstoffabwehr angestrebt. Das Innovationsvorhaben „Yggdrasil“ dreht sich um die Erkennung atomarer, biologischer und chemischer Gefahren durch die Vernetzung verschiedener Sensoren. Während die ABC-Abwehrkräfte der Bundeswehr ihre mobilen Gefahrstoffdetektoren bei Kontaminationsverdacht bisher von Hand bedienen, die Messungen selbst interpretieren und weiterleiten müssen, soll dies künftig die Software übernehmen.

Smarter Schnüffler
ABC-Kampfstoffe lassen sich mit KI-Hilfe leichter detektieren als von Hand. Ihr Einsatz reduziert zudem das eigene Kontaminationsrisiko.

Ermittelt wird, ob eine Kontamination vorliegt und um welchen Kampfstoff es sich handelt. Im Ergebnis braucht es weniger Personal, um eine ABC-Gefahr festzustellen – und damit reduziert sich auch das Risiko, dass diese Truppen kontaminiert werden.

9 ABC-GEFAHREN ABSCHÄTZEN

Um das Ausmaß von ABC-Bedrohungen abschätzen und den Einsatz von Personal und Material somit besser planen zu können, beschäftigt sich das ABC-Abwehrkommando mit der Prisma-KI zur automatisierten Aufbereitung öffentlich zugänglicher Informationen für den ABC-Kontext. Idee des Innovationsvorhabens ist es, mit KI-Hilfe frühzeitig von ABC-Gefahren zu erfahren und ein Modell zur möglichen Ausbreitung der Gefahr zu erstellen. So kann beispielsweise die Ausbreitung einer Giftgaswolke anhand der Windverhältnisse und der klimatischen Bedingungen prognostiziert werden. Die ABC-Abwehrberater der Bundeswehr werden so von technischen Routinetätigkeiten entlastet und können sich auf ihre Lageeinschätzung konzentrieren.

Minimierte Risiken
Wenn beim Dekontaminieren von Fahrzeugen ein Kampfstoff austritt, kann das Gefährdungspotenzial künftig mit KI-Hilfe abgeschätzt werden.

10 MINENSPERREN AUS DER LUFT AUFKLÄREN

Das Projekt „Minesweeper“ soll das Aufklären von Minensperren weniger gefährlich und gleichzeitig schneller machen. Dafür wird eine Drohne mit einem Magnetometer in einen fliegenden Metalldetektor verwandelt. Die vollautomatisierte Drohne fliegt das Gelände selbstständig ab, scannt es nach im Boden verborgenen Metallgegenständen und trägt ihre Funde in eine Geländekarte ein. Zudem bewertet die Software, ob es sich tatsächlich um ein Kampfmittel handelt. Danach wird das Kampfmittel anhand einer Datenbank bestimmt. Im Ergebnis entsteht ein Lagebild, dass nicht nur die Lage der Minen im Gelände darstellt, sondern auch die minenfreien Durchgänge aufzeigt. Im Herbst 2024 testete der Cyber Innovation Hub mit der Luftlandepionierkompanie 270 des Heeres einen Prototyp.

Fliegender Detektor
Die Aufklärung von Minenfeldern mit modifizierten Drohnen (Bild oben) macht den Job der Kampfmittelräumer weniger riskant.

Gefährliche Aufgabe
Kampfmittelräumer nutzen bislang eine einfache Minensuchnadel (Bild unten), um verborgene Sprengfallen zu finden.

11 AKUSTISCHER STOLPERDRAHT

Im Cyber Innovation Hub der Bundeswehr machen zivile Start-ups technische Innovationen militärisch nutzbar. Besonders stolz ist man in Berlin auf das Projekt „Sonic AI“, das mit dem Ausbildungszentrum Flugabwehrraketen der Luftwaffe entwickelt wurde. Durch den Einsatz passiver Akustiksensoren in Verbindung mit KI können Lufträume besser kontrolliert werden. Dafür werden handelsübliche Sensoren modifiziert, auf die Erkennung bestimmter Geräuschsignaturen zum Beispiel von Drohnen trainiert und in großer Stückzahl im Gelände ausgebracht. Die Sensoren funktionieren wie ein akustischer Stolperdraht: Werden Geräusche registriert, kann Sonic AI durch Triangulation den Standort der Quelle feststellen und die Geräuschquelle klassifizieren. Da die Akustiksensoren passiv arbeiten, kann Sonic AI zudem nur schwer durch Maßnahmen der Elektronischen Kampfführung gestört werden.

S. 60–61: Bundeswehr/Elian Hadj Hamdi
S. 60: Bundeswehr/Tom Twardy (l.u.)
S. 61: Bundeswehr/Anne Weinrich (l.u.), Bundeswehr/PAO NCO (r.o.), Bundeswehr/Marco Dorow (r.m.), Bundeswehr/Rolf Klatt (r.u.)

TEXT *Florian Stöhr*

Das Tor zur fünften Dimension

Europa arbeitet an seiner Unabhängigkeit im Weltraum. Die deutsch-französische Ariane Group spielt dabei eine besondere Rolle. Die neue Schwerlastrakete Ariane 6 soll den Zugang ins Weltall sichern – und auch die Satelliten der Bundeswehr zuverlässig verbringen.

Ka

Weltraum

D

Die Werkshalle der Ariane Group ist schon von Weitem zu erkennen. Am Eingang steht ein 17 Meter hohes und 33 Tonnen schweres Modell einer Weltraumrakete. Jeder kann sehen, woran die rund 650 Frauen und Männer hier in Bremen arbeiten: an der Ariane 6, Europas neuer Trägerrakete in den Weltraum. Das Werk wurde erst vor wenigen Jahren eingeweiht und liegt direkt am Flughafen, wo auch viele andere Raumfahrtspezialisten sitzen – vom Satellitenbauer bis zum Raumschiffentwickler. Die Modellrakete ist im Vergleich zum Original noch ziemlich klein: Die Ariane 6 ist je nach Konfiguration 56 oder 62 Meter hoch, 5,40 Meter breit und beim Start bis zu 870 Tonnen schwer. Zehn Jahre hat ihre Entwicklung gedauert. Mit Erfolg: Die Auftragsbücher sind seit dem erfolgreichen Erstflug im Juli 2024 gut gefüllt.

Eine so große Rakete und ihre Bestandteile brauchen Platz. Das zeigt sich beim Betreten der Werkshalle: Die Halle ist 6.000 Quadratmeter groß und 21 Meter hoch. Alles ist hell und weiß. Nur die Sicherheitsbereiche und das komplexe Kransystem an der Decke sind gelb gehalten, damit sie sich vom Rest abheben. In Bremen werden die Bauteile der Oberstufe ❱

5. Oberteil
Die Nutzlastverkleidung an der Spitze besteht aus vertikalen Halbschalen. Sie schützen die Traglast beim Start und legt diese im All frei.

4. Nutzlast
Die Ariane 6 verbringt Satelliten, Raumschiffe, Teleskope oder Sonden. Je nach Entfernung des Orbits kann die Nutzlast zwischen 4,5 bis 21,6 Tonnen betragen.

3. Oberstufe
Das obere Antriebsmodul setzt die Nutzlast im All ab. Mit der letzten Zündung des Vinci-Triebwerks werden die Überreste der Rakete entsorgt.

2. Hauptstufe
Das untere Antriebsmodul übernimmt den ersten Teil des Flugs. Nach dem Ausbrennen des Vulcain-2.1-Triebwerks wird es vom oberen Raketenteil abgetrennt.

1. Feststoffbooster
Die Triebwerke vom Typ P120C liefern den Hauptschub beim Start. Es können zwei oder vier Booster angebracht werden.

Dauerbetrieb
Rund 650 Frauen und Männer beschäftigt die Ariane Group in Bremen. Knapp 300 davon arbeiten in der Produktion – im Schichtbetrieb, damit die Herstellung der neuen Trägerrakete nicht stoppt.

S. 64: ESA/D. Ducros, Illustration,
S. 64–65: Bundeswehr/Christoph Kassette

Präzisionsarbeit
Während die Isolierung der Außenhülle von Roboterarmen ausgeführt wird, bleibt die Montage Handarbeit. Das Anziehen der Schrauben erfolgt immer im selben Muster.

Treibstoffkombination
Jede Raketenstufe hat einen separaten Tank für flüssigen Wasserstoff (Bild oben) und Sauerstoff. Allein die Oberstufe wird von 30 Tonnen Treibstoff angetrieben.

Weiterverarbeitung
Die Tanks werden von Subunternehmern hergestellt. Im Werk in Bremen (Bild unten) werden sie in die Oberstufe der Ariane 6 integriert.

der Ariane 6 zusammengeführt, die obere Trägereinheit der Rakete. „Die Ariane 6 ist eine Mehrstufenrakete: Jede Stufe hat eigene Treibstofftanks und ein Raketentriebwerk“, erklärt Stephanie Uffelmann. Die Luft- und Raumfahrtingenieurin leitete bis Ende 2025 das Testteam der Oberstufe in Bremen. Je nach Beladung sorgen zwei oder vier Booster für den nötigen Schub der Rakete beim Start. Wenn diese ausgebrannt sind, werden sie abgeworfen. Dann übernimmt die Hauptstufe den Transport. Schritt für Schritt steigt die Rakete höher und wird durch den Wegfall der Stufen leichter. „Die Oberstufe bleibt übrig und bringt die mitgeführte Nutzlast im obersten Raketenteil in den geplanten Orbit“, so Uffelmann.

In der Herzkammer

Im ersten Teil der Werkshalle, dem „Graubereich“, werden die Bauteile der Oberstufe beschichtet und isoliert. Alle Arbeitsschritte bauen aufeinander auf, erläutert Uffelmann: „Wir arbeiten in einer Fließfertigung. An jeder Station finden genau festgelegte Fertigungsschritte statt, danach geht es direkt weiter zur nächsten Station.“ Wie viele Einzelschritte umfasst die Produktion? Die Expertin lässt die Frage unbeantwortet, Betriebsgeheimnis. Bei der Beschichtung und Isolierung der Bauteile ist Millimeterarbeit gefragt: Im ersten Schritt werden sie gereinigt und aufgeraut. Ein Laser brennt dabei minimale Löcher in die Bauteile. Im Anschluss wird ein Spezialschaum aufgetragen, der die Stellen isoliert. Dann trägt ein zweiter Laser die überschüssige Schicht ab und glättet die Oberfläche. „An Station drei wird gerade die zehnte Ariane-6-Rakete beschichtet, sie soll im Sommer starten“, sagt Uffelmann. Links daneben befindet sich Rakete Nummer elf. Sie wird gerade isoliert und folgt im Herbst ins All.

„Das Isolierungsverfahren der Ariane 6 ist neu entwickelt worden. Es ist wesentlich schneller und effizienter als bei der Vorgängerrakete“, erklärt Uffelmann. Das Verfahren schützt die Rakete nicht nur vor äußeren Einflüssen im Weltraum, sondern sorgt auch dafür, dass der Treibstoff in den beiden Tanks im richtigen Aggregatzustand bleibt. „Die Oberstufe wird von flüssigem Wasserstoff und flüssigem Sauerstoff angetrieben. Im Wasserstofftank herrschen Temperaturen von rund 250 Grad Minus, beim Sauerstofftank sind es 180 Grad Minus. Andernfalls würde der Treibstoff beim Aufstieg verdampfen“, sagt die Expertin. Im Graubereich herrscht Betrieb. Viele Prozesse finden parallel statt, andere nur nacheinander. „Unser Ziel ist es, in vier bis sechs Wochen eine komplette Oberstufe auszuliefern“, so Uffelmann.

Eigene Fähigkeiten im Weltall

13 europäische Länder und über 600 Firmen sind im Auftrag der Europäischen Weltraumbehörde (ESA) an der Ariane 6 beteiligt. Die neue Trägerrakete soll Europa im Weltraum unabhängig und wettbewerbsfähig machen. Bis zu 36 Satelliten kann sie mit einem Flug verbringen und zielgenau in die verschiedenen Umlaufbahnen positionieren. Transportiert werden auch Raumschiffe, Teleskope, Sonden und andere Systeme. „Im letzten Jahr sind vier Raketenstarts durchgeführt worden, 2026 sind acht geplant. Danach werden es pro Jahr neun bis zehn Starts“, erklärt Thomas Tschirner, Head of Defence der Ariane Group. „Wir arbeiten mit vielen Partnern zusammen – von der ESA über staatliche Regierungen und Agenturen bis zu Privatunternehmen.“ Auch die Bundeswehr zählt dazu: Im September 2025 wurde verkündet, dass das französisch-deutsche Gemeinschaftsunternehmen zwei neue Satelliten der Bundeswehr ins Weltall bringen wird. Sie sollen ältere Modelle ablösen und eine sichere militärische Kommunikation gewährleisten.

„Es geht den europäischen Staaten um Souveränität. Der Weltraum ist längst nicht mehr nur ein Forschungsraum, sondern auch eine militärische Dimension“, sagt Tschirner. Es geht um mehr als um Kommunikation, Navigation oder Wetterprognosen. Für Staaten wie die USA, Russland und China ist der Weltraum auch ein militärischer Operationsraum. Wer über die entsprechenden Fähigkeiten verfügt, kann zum Beispiel Satelliten anderer Staaten überwachen, stören oder sogar ausschalten. Die Folgen wären für ein hochmodernes und vernetztes Land wie Deutschland fatal – ohne unsere Weltrauminfrastruktur würde unser digitales Leben schnell zusammenbrechen. „Es ist auch nicht ausgeschlossen, dass der Weltraum zu einem Konfliktgebiet werden könnte“, sagt der frühere Bundeswehroffizier. Die Bundesregierung ❱

„Die Ariane 6 ist sehr leistungsstark und vielseitig.“

Stephanie Uffelmann,
Programmleiterin,
Ariane Group

S. 66: ArianeGroup (2).
S. 67: ArianeGroup (o.), Bundeswehr/Christoph Kassette (u.)

Horizontalisierung
Nachdem die Einzelteile aufeinandergesetzt worden sind, wird die fertige Oberstufe durch das Kransystem an der Decke gedreht und in die Waagerechte gebracht.

Prozesse optimieren
Von der Annahme der Bauteile bis zur Verladung der Oberstufe in den Container: Die Entwickler versuchen, den Prozess immer weiter zu verbessern.

hat dies erkannt und im November 2025 ihre erste Weltraumsicherheitsstrategie vorgestellt. Darin heißt es, Deutschland solle im Weltall handlungsfähiger werden und die nationale und europäische Weltrauminfrastruktur stärker schützen. Der Bundeswehr kommt dabei eine Schlüsselrolle zu. Verteidigungsminister Boris Pistorius kündigte bis 2030 Investitionen in Höhe von 35 Milliarden Euro an, damit Deutschland und seine Partner unabhängiger werden – und verteidigungsbereit.

Das französisch-deutsche Unternehmen bietet nicht nur Trägersysteme an. „Viele unserer Entwicklungen sind Dual-Use-Produkte. Sie lassen sich sowohl zivil als auch militärisch nutzen“, erklärt Tschirner. Für den Leiter der Verteidigungssparte geht es nicht nur um den Weg ins Weltall, sondern auch zurück. Zum Beispiel mit dem Überwachungssystem Helix, einem weltweit verteilten Teleskopnetz, das Bedrohungen aus dem Weltraum frühzeitig erkennen kann. Oder mit Astris, einer Zusatzstufe für die Ariane 6, mit deren Hilfe zukünftig auch Abwehrsysteme im Weltraum gesteuert werden könnten, die die eigenen Satelliten schützen. Die M51, eine ballistische Rakete der Ariane Group, wird bereits von der französischen U-Boot-Flotte als Abschreckung genutzt. „Unsere Produkte dienen der Sicherheit und Verteidigung“, sagt Tschirner. Es ist kein Geheimnis, dass sich auch die Bundeswehr für einige dieser Produkte interessiert, um Deutschlands Weltrauminteressen besser zu schützen.

Ohne Fremdpartikel ins Weltall

Der „Weißbereich“ der Bremer Werkshalle ist besonders gesichert. Wer hier rein möchte, muss eine Schutzbekleidung tragen, vom Sicherheitsschuh bis zum Haarnetz. „Es ist sehr wichtig, dass keine Fremdpartikel in die Bauteile gelangen“, erklärt Uffelmann. Ein kleines Haar in einem Tank, in dem Minus 250 Grad Celsius herrschen, käme zum Beispiel beim Start einem Stahlgeschoss im Inneren gleich. Das Kransystem an der Decke transportiert die Einzelteile von Stufe zu Stufe. Insgesamt durchläuft die Oberstufe 21 Stationen. Am Ende werden die Tanks, das Haupttriebwerk, der Zusatzantrieb und die Steuerungselemente aufeinandergesetzt und von Hand exakt verschraubt. Einmal mehr wird deutlich, warum die Werkshalle so hoch ist. Erst an der letzten Station wird die fertige Oberstufe horizontalisiert: Das Lastensystem legt sie ganz vorsichtig in eine waagerechte Position, um sie für den Weitertransport vorzubereiten. ❱

Fester Ablauf
Alle Arbeitsschritte finden in einer festgelegten Reihenfolge statt. In vier bis sechs Wochen soll eine Oberstufe fertig zum Verladen sein.

S. 68–69: ArianeGroup (3)

Nächtlicher Schwertransport
Acht Kilometer entfernt vom Werk liegt der Bremer Hafen. Dort wird die Oberstufe auf das Arianeschiff „Canopée“ verladen.

Gestartet wird die Ariane 6 vom Weltraumbahnhof in Kourou im südamerikanischen Französisch-Guayana. Das riesige Areal gehört der französischen Weltraumagentur CNES und gilt als einer der besten Raketenstartplätze weltweit. Es liegt nur rund 580 Kilometer entfernt vom Äquator, was den Raketen eine hohe Geschwindigkeit und einen günstigen Eintritt in die Umlaufbahnen der Erde ermöglicht. Ein Spezialschiff, die „Canopée“, bringt die Oberstufe, die anderen Bauteile und die Nutzlast nach Kourou, wo sie zusammengefügt werden. Auch das Schiff ist eine Neuentwicklung der Ariane Group. Es ist 121 Meter lang, 22 Meter breit und kann bis zu 5.000 Tonnen Fracht transportieren. Ins Auge stechen vor allem die vier großen, vollautomatischen Segel: „Durch die Segel kann das Schiff mit einem Hybridantrieb aus Treibstoff und Windkraft betrieben werden“, sagt Uffelmann. Die Expertin hat die „Canopée“ im Hafen von Bremen besichtigt und schwärmt von der umweltschonenden Verbringung der Rakete ans Ziel. In der sehr energieintensiven Raumfahrt sind Klimaschutzmaßnahmen und Nachhaltigkeit ein entscheidender Wettbewerbsvorteil.

„Der Weltraum ist längst nicht mehr nur ein Forschungsraum.“

Thomas Tschirner,
Head of Defence,
Ariane Group

Wo steht die europäische Raumfahrt mit der Ariane 6? „Die Rakete ist sehr leistungsstark und vielseitig. Sie kann bis zu viermal gezündet werden, um Nutzlasten in verschiedene Orbits abzusetzen“, erklärt Uffelmann. Die Rakete kann also mit einem Start eine große Zahl an Systemen in den Weltraum transportieren und diese dort sehr variabel in Umlauf bringen. Der Hauptantrieb sorgt für den letzten Schub und bringt die Überreste der Rakete, die im All nicht verglühen, sicher aus der Umlaufbahn. Sie werden auf einen Weltraumfriedhof gebracht, wo sie um die Erde kreisen, ohne die Raumfahrt zu gefährden. „Wir vermeiden dadurch Weltraumschrott. Schon kleinste Teile haben durch ihre Geschwindigkeit eine große Sprengkraft und könnten mit Satelliten oder Trägersystemen kollidieren“, sagt Uffelmann. Die Expertin leitet seit diesem Jahr das Programm für künftige Systeme in Bremen: „Der Weltraum wird immer wichtiger werden und die Entwicklung ist noch lange nicht zu Ende.“ Europa und auch Deutschland haben mit der Ariane 6 und der Förderung neuer Systeme bewiesen, dass sie sich in der „fünften Dimension“ behaupten wollen.

Innovatives Frachtschiff
Die „Canopée“ bringt die Raketenteile zum Weltraumbahnhof in Französisch-Guayana – mit Treibstoff und Windkraft. Die vier Segel sind je 36 Meter hoch und haben eine Fläche von je 363 Quadratmetern.

S. 70: ArianeGroup (3)

Stark im Orbit

Eine neue Weltraumsicherheitsstrategie soll Deutschlands und Europas Rolle im Weltall stärken. Warum das wichtig ist und wie sich die Luftwaffe auf diese Aufgaben vorbereitet, erklärt der Inspekteur der Luftwaffe, Generalleutnant Holger Neumann, im Interview.

Das Interview führte Beate Schöne.

Generalleutnant Holger Neumann
trat 1988 in die Bundeswehr ein. Seit dem 25. Mai 2025 ist er Inspekteur der Luftwaffe und Dimensionsverantwortlicher für Luft und Weltraum.

Y: Bereits kurz nachdem Ihnen die Führung der Luftwaffe übertragen wurde, haben Sie mit dem Motto „Ready. Fight. Win. Together. – in Air and Space“ ein Ziel vorgegeben. Wie wichtig war Ihnen der Zusatz „Space“?
Generalleutnant Holger Neumann: Enorm wichtig. Ich will damit klar machen: Die Luftwaffe denkt konsequent in beiden Dimensionen – Luft und Weltraum. Unsere Streitkräfte, aber auch elementare Anwendungen für unsere gesamte Gesellschaft, hängen heute in vielen Bereichen an weltraumgestützten Diensten – von Navigation über Kommunikation bis zur Erdbeobachtung. Ohne diese Fähigkeiten sind auch moderne Militäroperationen nicht vorstellbar. Gleichzeitig sehen wir, dass Russland und China massiv in sogenannte Counter-Space-Fähigkeiten investieren – also in Mittel, Satelliten auszuspähen, zu stören oder sogar zu zerstören. Der Weltraum ist damit längst eine „Warfighting Domain“, also ein Operationsraum wie Land, Luft, See und Cyber – und nicht mehr nur ein Add-on für die Lageunterstützung. „Space“ im Motto ist genau aus diesem Grund besonders wichtig. Unsere Dimensionsverantwortung reicht vom Boden bis in den Weltraum, und ohne Kriegstüchtigkeit in den Dimensionen Luft und Weltraum werden wir auch in den anderen Dimensionen kaum kriegstüchtig sein.

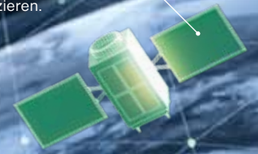
Die Luftwaffe feiert in diesem Jahr ihr 70. Jubiläum. Inwieweit spielt beim Rückblick auf die vergangenen Jahrzehnte der Weltraum eine Rolle?
Wenn wir auf 70 Jahre Luftwaffe schauen, dann war der Weltraum bisher ein eher „stiller Begleiter“ – Aufklärung, Navigation, Kommunikation, weitgehend unbedroht. Durch die Entwicklung zu einer „Warfighting Domain“ wird die Kette Informationsüberlegenheit – Führungsüberlegenheit – Wirkungsüberlegenheit und Durchhaltefähigkeit nun auch im Weltraum ins Visier genommen. Im historischen Rückblick hat die Luftwaffe bereits 2009 mit dem Weltraumlagezentrum eine erste Fähigkeit zur Beobachtung des Weltraums aufgestellt. Seit 2011 betreiben wir das Weltraumlagezentrum vertrauensvoll und erfolgreich mit unserem Ressortpartner, der Raumfahrtagentur DLR. In der Konsequenz einer weiteren Zunahme der Bedrohungslage folgte dann die Aufstellung des Weltraumkommandos der Bundeswehr am 13. Juli 2021 in Uedem. In unserem Jubiläumsjahr 2026 feiern wir also nicht nur 70 Jahre Luftwaffe, sondern auch fünf Jahre Weltraumkommando – und damit den Schritt von einer klassischen Luftstreitkraft hin zu einer Teilstreitkraft, die ihre Verantwortung „in Air and Space“ versteht und in enger Kooperation insbesondere mit unserer Schwester-Teilstreitkraft CIR lebt.

Im November 2025 hat die Bundesregierung ihre erste Weltraumsicherheitsstrategie, kurz WRSS, vorgestellt. Was sind die Gründe dafür?
Die Strategie schafft Rahmen, Prioritäten und Tempo. Die Gründe liegen auf der Hand, wenn man sich die letzten Jahre anschaut. Spätestens der Cyberangriff auf die durch die Ukraine genutzte kommerzielle Satellitenkommunikation zu Beginn des russischen Vollangriffs gegen die Ukraine 2022 hat sehr deutlich gemacht: Militärische Konflikte machen vor dem Weltraum nicht Halt – es ist wahrscheinlich, dass dort sogar die ersten Anzeichen beziehungsweise Angriffe auftreten. Gleichzeitig nimmt unsere Abhängigkeit von weltraumgestützten Diensten rasant zu – in der Wirtschaft, in der kritischen Infrastruktur, in der staatlichen Lagebeurteilungs- und Handlungsfähigkeit. Ein Ausfall von Satellitenkommunikation, Navigationssignalen oder Erdbeobachtung hätte gravierende Folgen für Sicherheit, Wohlstand und gesellschaftliche Stabilität. Die Weltraumsicherheitsstrategie ist deshalb die Antwort auf drei Entwicklungen: die Zeitenwende in der Sicherheitsordnung, den rasanten Fähigkeitsaufbau vor allem Russlands und Chinas im Bereich Counter-Space und die Erkenntnis, dass Weltraumsicherheit eine politische Kernaufgabe geworden ist – nicht nur ein Technikthema. Deshalb hat die Bundesregierung diese erste WRSS vorgelegt und gleichzeitig angekündigt, bis 2030 rund 35 Milliarden Euro in Weltraum und Weltraumsicherheit zu investieren. ❯

Die Infografiken zeigen grobe Entwürfe einer Infrastruktur, wie sie nach den Fähigkeitsbeschreibungen in der Weltraumsicherheitsstrategie aussehen könnte.

Feindlicher Satellit
Satelliten mit feindlichen Absichten wie Spionage, Störung oder gar Kollision können frühzeitig aufgeklärt werden.

Inspektionssatellit
Inspektionssatelliten können die eigenen oder feindliche Satelliten beobachten und inspizieren.

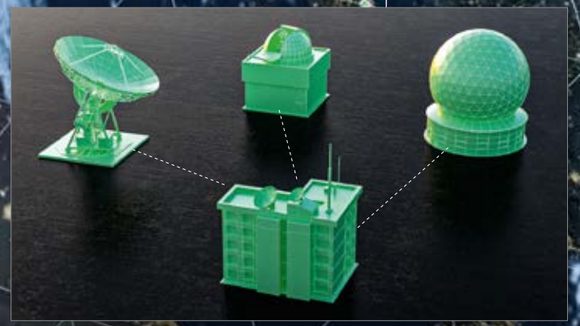


Kleinstsatellit
Kleinstsatelliten wie zum Beispiel CubeSats können in großer Menge in den Orbit verbracht werden, um dort ein Netz zur lückenlosen Abdeckung aufzuspannen.

Erkennen

Space Domain Awareness, Frühwarnung und Lagebilderstellung sind Fähigkeiten zur frühzeitigen Identifikation feindlicher oder gefährlicher Aktivitäten im Weltraum, einschließlich Raketenstarts, Annäherungen, Cyberangriffen und Weltraummüll. Dazu braucht Europa eigene Weltraumteleskope und -radare, Beobachtungssatelliten und Informationszentren, in denen die Daten zusammengetragen und zu einem verlässlichen Lagebild verdichtet werden.

Terrestrisches Teleskop
Eine globale Abdeckung mit Teleskopen und Radaren ist nötig, um eine lückenlose Weltraumlage zu erstellen.

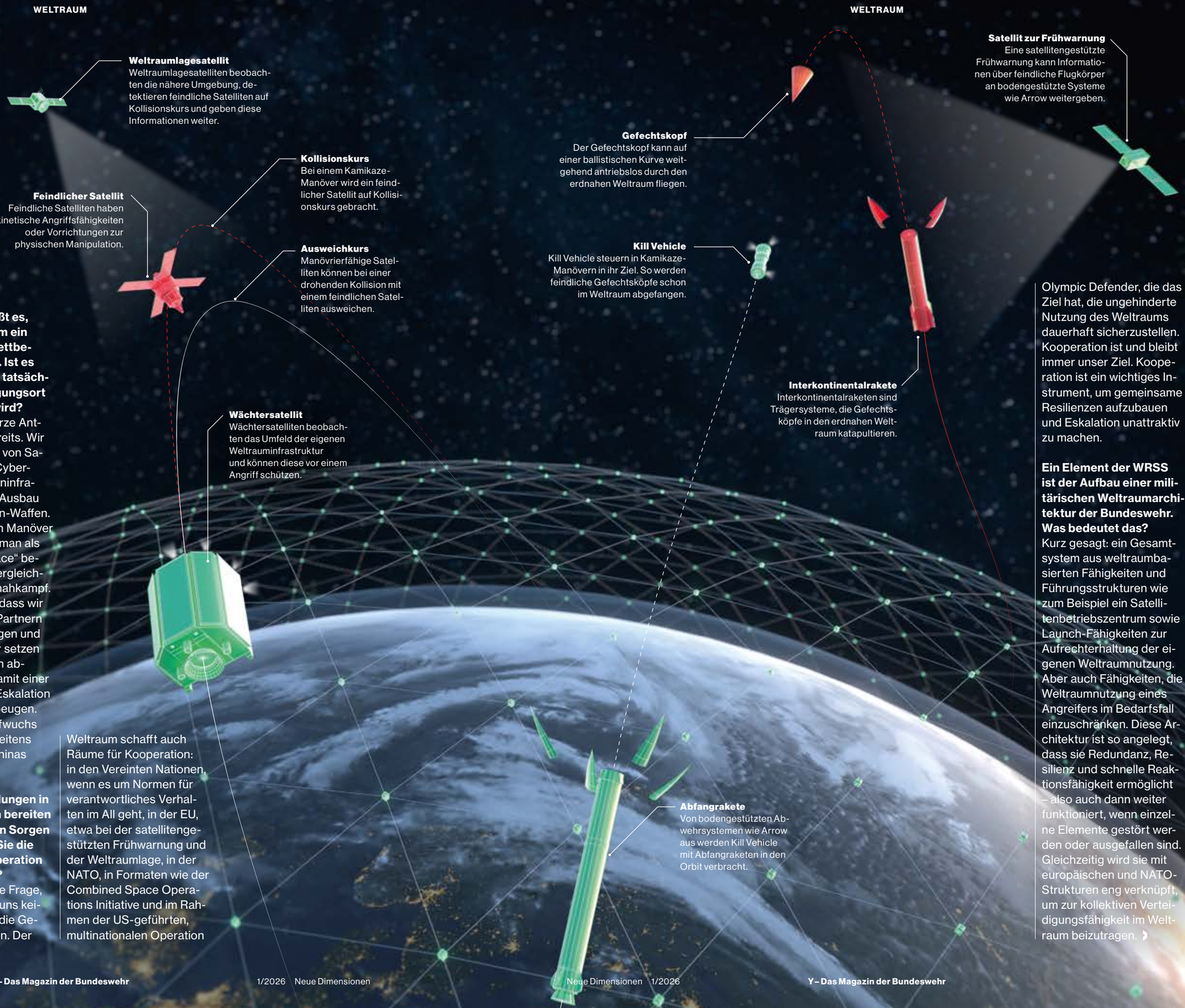


Sensornetzwerk mit globaler Abdeckung
Ein globales Netzwerk aus Teleskopen und Radaren trägt die Daten ins Weltraumlagezentrum in Uedem, wo das Weltraumlagebild erstellt wird.

S. 72: Bundeswehr/Francis Hildemann
S. 72–73: Y/C3 Visual Lab, Infografik (2)

Schützen

Resiliente und wehrfähige Systeme verleihen die Fähigkeit, eigene Weltraumsysteme zu schützen und im Angriffsfall zu verteidigen. Dazu gehören Cyberfähigkeiten wie Jammen oder Blenden, aber auch Ausweichmanöver und im äußersten Fall sogar kinetische Verteidigungsmaßnahmen.



Das Verteidigungsministerium hat maßgeblich zur WRSS beigetragen. Welche Ziele und Handlungsfelder hat die Bundeswehr im Weltraum?
Die Strategie formuliert drei zentrale Handlungsfelder mit klar umrissenen Handlungslinien, an denen wir uns auch als Bundeswehr sehr klar orientieren. Erstens: Gefahren erkennen und handlungsfähig bleiben. Zweitens: Kooperation und nachhaltige Ordnung stärken. Drittens: Abschreckung aufbauen, Resilienz und Wehrhaftigkeit stärken. Insgesamt reden wir nicht mehr nur über Prävention, sondern ausdrücklich auch über Wehrhaftigkeit und Abschreckung. Dazu gehören der Schutz eigener Systeme, Redundanzen durch vernetzte Satellitenkonstellationen sowie defensive und offensive Weltraumoperationen – immer im Rahmen des Völkerrechts. Übergeordnetes Ziel ist es, die Handlungsfähigkeit Deutschlands im Weltraum – zivil und militärisch, in Frieden, Krise und Krieg – durchgängig zu sichern.

In der WRSS heißt es, dass im Weltraum ein strategischer Wettbewerb stattfindet. Ist es möglich, dass er tatsächlich zum Austragungsort von Konflikten wird?
Eine klare und kurze Antwort: Er ist es bereits. Wir sehen Störungen von Satellitensignalen, Cyberangriffe auf Bodeninfrastruktur und den Ausbau von Anti-Satelliten-Waffen. Nicht zuletzt auch Manöver im Weltraum, die man als „Dogfights in Space“ bezeichnen kann, vergleichbar mit dem Luftnahkampf. Unser Ziel ist es, dass wir uns mit unseren Partnern gegen Bedrohungen und Angriffe zur Wehr setzen können, hierdurch abschrecken und damit einer unkontrollierten Eskalation im Weltraum vorbeugen. Der Fähigkeitsaufwuchs Counter-Space seitens Russlands und Chinas zwingt uns dazu.

Welche Entwicklungen in anderen Staaten bereiten Ihnen die größten Sorgen – und wo sehen Sie die Chance für Kooperation statt Eskalation?
Eine sehr wichtige Frage, denn wir fixieren uns keineswegs nur auf die Gefahren und Risiken. Der Weltraum schafft auch Räume für Kooperation: in den Vereinten Nationen, wenn es um Normen für verantwortliches Verhalten im All geht, in der EU, etwa bei der satellitengestützten Frühwarnung und der Weltraumlage, in der NATO, in Formaten wie der Combined Space Operations Initiative und im Rahmen der US-geführten, multinationalen Operation Olympic Defender, die das Ziel hat, die ungehinderte Nutzung des Weltraums dauerhaft sicherzustellen. Kooperation ist und bleibt immer unser Ziel. Kooperation ist ein wichtiges Instrument, um gemeinsame Resilienzen aufzubauen und Eskalation unattraktiv zu machen.

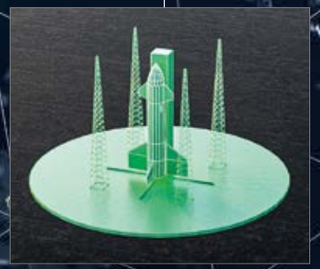
Ein Element der WRSS ist der Aufbau einer militärischen Weltraumarchitektur der Bundeswehr. Was bedeutet das?
Kurz gesagt: ein Gesamtsystem aus weltraumbasierten Fähigkeiten und Führungsstrukturen wie zum Beispiel ein Satellitenbetriebszentrum sowie Launch-Fähigkeiten zur Aufrechterhaltung der eigenen Weltraumnutzung. Aber auch Fähigkeiten, die Weltraumnutzung eines Angreifers im Bedarfsfall einzuschränken. Diese Architektur ist so angelegt, dass sie Redundanz, Resilienz und schnelle Reaktionsfähigkeit ermöglicht – also auch dann weiter funktioniert, wenn einzelne Elemente gestört werden oder ausgefallen sind. Gleichzeitig wird sie mit europäischen und NATO-Strukturen eng verknüpft, um zur kollektiven Verteidigungsfähigkeit im Weltraum beizutragen.

S. 74–75: Y/C3 Visual Lab, Infografik

WELTRAUM

Durchhalten

Resilienz, schnelle Rekonstitution und Backup-Fähigkeiten machen die Weltrauminfrastruktur durchhaltefähig. Die Maßnahmen umfassen Redundanzen, responsive Systeme, um kritische Komponenten bei einem Ausfall ersetzen zu können, sowie die Inspektion, Reparatur und Instandhaltung im Orbit – bis hin zu eigenen Start- und Landekapazitäten.



Weltraumbahnhof
Nationale Start- und Landeinfrastruktur für Weltraumfahrzeuge sowie Microlauncher erhöhen die Unabhängigkeit von anderen Ländern und die Reaktionsfähigkeit, um schnell Weltraumsysteme zu ersetzen.

Responsive Space
Ketten oder Schwärme von Kleinstsatelliten schaffen Redundanzen, die die Handlungsfähigkeit bei einem Systemausfall sicherstellen.

Rekonstituieren
Mit Raumtransportern können im Bedarfsfall ausgefallene Satelliten durch eine schnelle Verbringung neuer Modelle ersetzt werden.

Raumtransporter
Wiederverwendbare Raumsysteme senken die Kosten und schädliche Umwelteinflüsse wie Weltraumschrott. Raumtransporter können vertikal mit herkömmlichen Launchern in den Orbit verbracht werden oder sie starten horizontal von Flugplätzen.

Welche Fähigkeiten sind dafür notwendig, und was fehlt der Truppe noch?
Vor allem Tempo! Wir sind gut gestartet, müssen aber massiv in Sensornetzwerke, Frühwarnung, offensive und defensive Fähigkeiten und Responsive Launch investieren. Und wir brauchen Personal – echte Weltraumprofis. Mit dem Werdegang „Weltraum“ haben wir einen Anfang gemacht, aber wir müssen unsere Ausbildungs- und Personalkapazitäten deutlich ausbauen – Offiziere, Unteroffiziere, Spezialisten, die diese neuen Systeme planen, bedienen und operationell nutzen können.

Welche Aufgaben leitet die Luftwaffe für sich aus der gestiegenen Bedeutung des Weltraums für Deutschland ab?
Aus meiner Sicht gibt es zwei große Aufgaben, die wir als Luftwaffe klar annehmen. Erstens: Führung und Verantwortung in der Dimension Weltraum. Zweitens: Aufbau und Betrieb der Weltraumsicherheitsarchitektur, gemeinsam mit CIR. Wir sorgen dafür, dass Planung und Führung von Weltraumoperationen integrale Bestandteile der Gesamtoperationsführung der Bundeswehr sind – in Frieden, Krise und Krieg. Gleichzeitig treiben wir den Ausbau des Systems zur Weltraumüberwachung, den Aufbau eines Satellitenbetriebszentrums, die Entwicklung von Frühwarn- und Kommunikationskonstellationen, die Fähigkeit zur schnellen Rekonstitution sowie Fähigkeiten zur Wirkung in der Dimension Weltraum voran. Hier setzen wir stark auf Kooperation – mit CIR, mit der Industrie, mit Partnerressorts und mit unseren internationalen Partnern.

Wie andere Streitkräfte arbeitet die Bundeswehr mit privaten Anbietern zusammen. Wie wirkt sich diese Abhängigkeit auf die Planung und Einsatzführung aus?
Wir können die geplante Weltraumsicherheitsarchitektur weder rein staatlich aufbauen, noch betreiben. Wir sind auf das Know-how, die Innovationskraft und die industrielle Basis unserer nationalen und europäischen Weltraumindustrie angewiesen. Das heißt für die Planung: Wir setzen bewusst auf marktverfügbare Systeme, anstatt alles von Grund auf neu zu entwickeln. „Gut genug und schnell“ ist oft besser als „perfekt und spät“. Wir denken den dualen Charakter von Weltraumsystemen viel stärker mit – also die Nutzung gleicher Infrastruktur für zivile und militärische Zwecke. Und wir unterstützen strategische Partnerschaften und neue Beschaffungsmodelle, um Verfügbarkeit, Redundanz und Versorgungssicherheit auch im Krisenfall sicherzustellen.

Am Ende geht es darum, den Weltraum zu schützen und auch künftig zu nutzen. Wie sieht Ihr Wunschbild der Weltraumfähigkeiten der Bundeswehr im Jahr 2040 aus – technologisch, operativ und politisch?
Mein Wunsch ist, eine souveräne Weltraumarchitektur zu schaffen, die wir als Streitkräfte operativ beherrschen, um sie politisch verantwortungsvoll einsetzen zu können – robust, vernetzt und wirkungsvoll, und damit abschreckungsfähig.

S. 76–77: Y/C3 Visual Lab, Infografik (2)

Blick in den Himmel

13.000 Satelliten umkreisen die Erde und sichern Navigation, Kommunikation, militärische Operationen und vieles mehr. Die Abhängigkeit von dieser Technik ist groß. **Gemeinsam sorgen Luftwaffe und CIR für den störungsfreien Betrieb.**

TEXT
Gian-Luca Omari & Sebastian Blum

VON DEN STERNEN BIS NACH UEDEM

Die Weltrauminfrastruktur ermöglicht heute nahezu alles: Navigation, Kommunikation, Wettervorhersagen, Finanztransaktionen und Energieverteilung. Auch die Streitkräfte sind darauf angewiesen, vom militärischen Lagebild bis zur Unterstützung militärischer Operationen in anderen Dimensionen. Ohne Fähigkeiten im Weltraum und ein verlässliches Bild der Weltraumlage gibt es weder Schutz noch Planungssicherheit, weder für zivile Stellen noch für die Bundeswehr. Die vergangenen Jahre haben gezeigt, dass der Weltraum zunehmend umkämpft ist. Für Aufsehen sorgten zum Beispiel die Annäherungen russischer Aufklärungssatelliten an kommerzielle Kommunikationssysteme, die auch die Bundeswehr nutzt. Auch die Anzahl elektronischer Störungen an der NATO-Ostflanke nehmen weiter zu. Im der Luftwaffe zugehörigen Weltraumkommando der Bundeswehr in Uedem werden all diese Informationen zu einem Lagebild verdichtet und bewertet. Die Soldatinnen und Soldaten erkennen Muster und technische Abläufe und ordnen diese ein. Die Daten zeigen, dass der Weltraum immer dynamischer wird und dass Staaten ihre Fähigkeiten zur Einflussnahme enorm weiterentwickeln.

**Mit Sternchen gekennzeichnete Namen sind zum Schutz der Personen geändert.*

Den Weltraum beobachten

Das Weltraumlagezentrum existiert seit 2009. Es wurde gegründet, um für die damals in Betrieb genommenen bundeswehreigenen Satelliten eine zentrale Stelle zu schaffen, die Weltraumobjekte systematisch erfasst und bewertet – und Risiken frühzeitig erkennt. Seit 2011 wird das Lagezentrum gemeinsam mit dem Deutschen Zentrum für Luft- und Raumfahrt (DLR) betrieben. Das DLR bringt seine wissenschaftlich-technische Expertise sowie seine zivilen Kooperationen, internationale Datenbeziehungen und eigene Sensorik ein; die Bundeswehr bewertet die Lage aus sicherheits- und verteidigungspolitscher Sicht. Das Ziel des gemeinsamen Weltraumlagezentrums ist, ein umfassendes, aktuelles und belastbares Bild des Geschehens im Weltraum zu gewinnen – rund um die Uhr, 365 Tage im Jahr. Viele militärische und zivile Expertinnen und Experten tragen zum Lagebild bei. Ein Weltraumlageoffizier und ein Weltraumlagefeldwebel sorgen dafür, dass die Operationszentrale (OPZ) auch nachts besetzt ist. Große Bildschirme in der OPZ zeigen Bahnverläufe und Positionsdaten, Wiedereintrittsdiagramme, Warnmeldungen und die Sonne in verschiedenen Wellenlängen, um Weltraumwetterereignisse frühzeitig zu erkennen. Wenn sich ein Objekt auffällig verhält, eine der verschiedenen Quellen eine ›

Gefahren erkennen

Die Parabolantenne des Weltraumbeobachtungsradars TIRA in Wachtberg bei Bonn hat einen Durchmesser von 34 Metern. Sie erfasst regelmäßig die Verteilung von Weltraumtrümmern. Die Bundeswehr greift auf diese Daten zurück. Selbst Objekte von nur wenigen Zentimetern Größe können im All Satelliten zerstören.

S. 78–79 Fraunhofer FHR/Uwe Bamberger

WELTRAUM

Weltraum überwachen

Die Operationszentrale im Weltraumlagezentrum ist das Herz des Weltraumkommandos. Hier laufen Daten von Weltraumlagesensoren aus aller Welt zusammen, aus denen ein umfassendes Weltraumlagebild erstellt wird. Satellitenbahnen, Weltraumwetter, Weltraummüll und mehr werden hier beobachtet.

Unregelmäßigkeit meldet oder ein Wiedereintritt in die Atmosphäre neu berechnet werden muss, entscheiden Minuten, manchmal auch nur Sekunden über die Bewertung des Ereignisses und das weitere Vorgehen.

Ein Lagebild entsteht

Im Lagezentrum laufen täglich enorme Datenmengen ein. Dazu gehören nationale und internationale Umlaufbahn- und Sensordaten, Informationen aus optischen Teleskopen und anderen Beobachtungssystemen. Außerdem erhalten die Expertinnen und Experten Meldungen von Partnernationen und analysieren das Weltraumwetter. Ab 2026 wird ein Teleskopsystem der Bundeswehr in Meßstetten diese Datengrundlage ergänzen, 2028 kommt ein Weltraumradar hinzu.

Aus all diesen Informationen entsteht die Weltraumlage: eine Bewertung dessen, was im Weltraum passiert, was sich verändert und welche Vorgänge sicherheitsrelevant sein könnten. Das sind zum Beispiel Berechnungen von Kollisionsrisiken und möglicher Ausweichmanöver, die Auswirkungen von Weltraumwetterereignissen und die Beobachtung ungewöhnlicher Bahnmanöver. Auch Ereignisse wie der unkontrollierte Wiedereintritt einer Batterie der Internationalen Raumstation im Frühjahr 2024 werden hier verfolgt, bewertet und entsprechende Warnungen an nationale und internationale Stellen weitergegeben.

Das gemeinsame Lagebild wird im Weltraumkommando der Bundeswehr zur „Lage in der Dimension Weltraum“ weiterentwickelt. Dort fließen auch weitere militärische Erkenntnisse ein, zum Beispiel aus nachrichtendienstlicher Aufklärung oder der Bewertung taktischer und operativer Lagen. So entsteht ein vollumfängliches militärisches Lagebild. Das Weltraumkommando der Bundeswehr, insbesondere das ressortgemeinsame Weltraumlagezentrum, ist also eine Art Frühwarnsystem: für die zivile Bevölkerung und Infrastruktur – und die Bundeswehr.

S. 80–81: Bundeswehr/Jennifer Heyn

Führung aus einer Hand

Aktuelle Konflikte zeigen, wie stark moderne militärische Systeme und Operationen auf weltraumgestützte Kommunikations-, Frühwarn-, Aufklärungs- und Zeitdienste angewiesen sind. Mit dem Weltraumkommando hat die Bundeswehr eine zentrale Führungs- und Koordinierungsebene für alle militärischen Aktivitäten Deutschlands im Weltraum geschaffen. Die dort eingesetzten Soldatinnen und Soldaten stellen, gemeinsam mit der Teilstreitkraft CIR, die militärische Nutzung des Weltraums sicher. Neben der Erstellung der militärischen Weltraumlage werden von hier auch Weltraumoperationen geplant und geführt. Zu den täglichen Aufgaben der Fachleute zählen die stetige Lagebeobachtung im Weltraum, die Unterstützung laufender Auslandseinsätze, die Begleitung multinationaler Übungen sowie die Analyse weltraumbezogener Auswirkungen auf aktuelle Krisen und Konflikte. Im Einsatzfall würde das Weltraumkommando als Space Component Command direkt dem Operativen Führungskommando der Bundeswehr unterstellt, damit alle weltraumbezogenen Aspekte in eine militärische Gesamtoperation integriert werden können. Es ist kein Zufall, dass das Weltraumkommando auch regelmäßig bei den Übungen anderer Truppenteile mit dabei ist – die Abhängigkeit der Bundeswehr vom Weltraum ist hoch und ein starkes Kommando über die eigenen Aktivitäten Pflicht. ›

SARah und SAR-Lupe
Mit SARah erhält die deutsche Bundeswehr einen Nachfolger des bewährten SAR-Lupe-Systems. SARah besteht aus drei Beobachtungssatelliten (Bild oben) und zwei Bodenstationen.

KOMMANDO CIR: SERVICES AUS DEM WELTRAUM

Mit dem Weltraumkommando und dem dazugehörigen Weltraumlagezentrum in Uedem hat die Luftwaffe die Dimension Weltraum allein in ihrer Hand – scheint es. Tatsächlich ist es aber die Teilstreitkraft Cyber- und Informationsraum, der die Nutzung und Bereitstellung der Services der aktuellen Bundeswehrsatelliten sowie der dazugehörigen Bodenstationen obliegt. Diese Aufgaben sind eng mit dem Cyber- und Informationsraum verschränkt. Satelliten sind physische Plattformen, ihre Leistungsfähigkeit beruht jedoch auf Informationstechnologie, dem elektromagnetischen Spektrum und cybergestützten Steuerungs- und Auswerteprozessen. „Die Weltraumnutzung ist ohne das elektromagnetische Umfeld und die Abstützung auf den Cyberraum nicht möglich“, bringt es Fregattenkapitän Dr. Martin Hambach* auf den Punkt. Der promovierte Elektroingenieur leitet das Team Weltraum im Kommando CIR.

Dessen Rolle ist klar von den Aufgaben des Weltraumkommandos abgegrenzt. Während das bei der Luftwaffe verortete Weltraumkommando für Weltraumoperationen zuständig ist – also für Schutz, Überwachung und Verteidigung militärischer Satellitensysteme sowie für die Weltraumlage – stellt die Teilstreitkraft CIR der Truppe Satellitenkommunikation, Aufklärung, Navigation sowie Geo- und Wetterinformationen zur Verfügung, ohne die eine moderne Armee gar nicht mehr einsatzfähig ist. Im Militärjargon nennt sich das die „Einsatzunterstützung aus dem Weltraum“. Diese unterteilt sich in drei Bereiche: Satellitenkommunikation, Aufklärung sowie Geoinformationsunterstützung.

Satellitenkommunikation

Kern der Einsatzunterstützung aus dem Weltraum ist die Satellitenkommunikation. Sie bildet die Grundlage für Führungsfähigkeit, Informations- ❱

Ab in den Orbit

COMSATBw-1 und -2 wurden mit der europäischen Trägerrakete Ariane 5 in den Orbit gebracht. Die Nachfolgesatelliten COMSATBw-1B und -2B sollen ab 2027 von Ariane 6 (hier bei einem Start 2026 vom europäischen Weltraumbahnhof Kourou in Französisch-Guayana) verbracht werden.

S. 82: OHB (o.), S. 83: CNES/ESA/ArianeGroup

überlegenheit und vernetzte Operationsführung. Ein Beispiel: Mit dem System SATCOMBw Stufe 2 betreibt die Bundeswehr eigene geostationäre Kommunikationssatelliten, ergänzt durch angemietete kommerzielle Kapazitäten. Über mobile und feste Bodenstationen in Deutschland werden diese Dienste in die militärischen Führungsnetze eingebunden. Mit Blick auf die Lebensdauer dieser Satelliten wird derzeit der Übergang zu SATCOMBw Stufe 3 vorbereitet, flankiert durch Dual-Use-Fähigkeiten wie den Satelliten Heinrich Hertz, um zukünftigen Anforderungen an Schnelligkeit und erhöhte Resilienz Rechnung zu tragen.

System aus vielen Teilen

SATCOMBw Stufe 2 ist das aktuelle Satellitenkommunikationssystem der Bundeswehr. Neben den beiden baugleichen Satelliten COMSATBw-1 und -2 gehören zu dem System drei Ankerstationen und über 100 Bodenstationen verschiedener Größen.

Aufklärung

Das zweite zentrale Aufgabenfeld ist die weltraumgestützte Aufklärung. CIR steuert streitkräftegemeinsame Aufklärungsfähigkeiten und trägt damit zur Lagebilderstellung bei. Mit den Radarsatellitensystemen SAR-Lupe und dem Nachfolgesystem SARah kann CIR weltweit wetter- und tageszeitunabhängig aufklären. Ergänzt werden diese Fähigkeiten durch internationale Kooperationen wie mit dem französischen optischen Aufklärungssystem CSO sowie durch kleinere Aufklärungssatelliten. Diese ermöglichen eine eskalationsarme Informationsgewinnung, da sie weltweit aufklären können, ohne Hoheitsrechte zu verletzen. Mit dem Aufbau der Gesamtarchitektur Weltraum werden im Bereich der signalerfassenden Aufklärung die Frühwarnung und das Erfassen von elektronischer Kommunikation (SIGINT) hinzukommen.

„Die aktuellen Entwicklungen im Bereich Multi-Domain Operations und Digitalisierung Landbasierte Operationen zeigen, dass die Verkürzung der Sensor-Shooter-Wirkungskette eine entscheidende Rolle für den Erfolg der Operationen spielen wird“, sagt Hambach. „Durch eine vernetzte Gesamtarchitektur in Verbindung mit automatisierter und KI-gestützter Auswertung wird die Zeit von der Aufklärung eines Ziels bis zur Wirkung im Ziel deutlich verkürzt.“

SATCOMBw
SATCOMBw Stufe 0 und 1 nutzen angemietete Satellitenverbindungen. Die Stufe 2 (im Bild) beruht auf den beiden Satelliten COMSATBw 1 und 2. Die Stufe 3 wird ab 2027 ausgerollt und basiert auf den Satelliten COMSATBw-1B und -2B.

Kommunikationssystem
Als Gegenstücke auf der Erde nutzen die CIR-Kräfte verlegefähige Bodenstationen. Dort werden die Rohdaten der Satelliten empfangen und in detaillierte Lagebilder umgewandelt.

Geoinformationsunterstützung

Die dritte Säule der Einsatzunterstützung aus dem Weltraum ist die Geoinformationsunterstützung. Hier werden weltraumgestützte und kommerzielle Daten zu präzisen Geo-, Wetter- und Navigationsprodukten verarbeitet. Das Zentrum für Geoinformationswesen und der Geoinformationsdienst der Bundeswehr bereiten diese Informationen lage- und bedarfsgerecht auf und liefern Vorhersagen zum Weltraumwetter sowie Bewertungen zur Verlässlichkeit satellitengestützter Positionsbestimmung. Das ist entscheidend für Navigation, Zielwirkung und die sichere Durchführung militärischer Operationen.

S. 84: picture alliance/dpa/Alexander Welscher (u.),
S. 84–85: Airbus, S. 85: Bundeswehr/Ralph Zwilling (r.o.)

Einsatzunterstützung für die Truppe
Das Führungsfahrzeug GTK Boxer A1 ist mit Breitband -Satellitenkommunikation ausgestattet und bekommt so Unterstützung durch die Weltraumfähigkeiten von CIR.

Schutz des Weltraums

Mit der wachsenden Abhängigkeit von Systemen im Weltraum rückt auch deren Schutz in den Fokus. Zwar liegt die Verantwortung für klassische Weltraumoperationen beim Weltraumkommando, doch die Teilstreitkraft CIR bringt seine eigenen Fähigkeiten ein, um Bedrohungen für Weltrauminfrastrukturen zu begegnen. Nicht-kinetische, reversible Maßnahmen im Cyberraum und elektromagnetischen Umfeld spielen dabei eine zentrale Rolle. Sie dienen dem Schutz eigener Systeme, der Abschreckung potenzieller Gegner und – im äußersten Fall – der Einschränkung gegnerischer Weltraumnutzung, ohne dauerhaftes Weltraumtrümmeraufkommen zu verursachen.

Die Weltraumsicherheitsstrategie

Die strategische Grundlage für diesen Fähigkeitsaufbau bildet die Weltraumsicherheitsstrategie der Bundesregierung. Sie benennt den Weltraum als eigenständigen Operationsraum und betont die Notwendigkeit von Resilienz, Wehrhaftigkeit und Abschreckung. Für CIR bedeutet dies vor allem den Ausbau einer vernetzten, multi-orbitalen Gesamtarchitektur: Frühwarnsysteme, signalerfassende Aufklärung, verbesserte Resilienzkonzepte und Responsive-Space-Ansätze sollen hinzukommen. Mittelfristig ist ein deutlicher Aufwuchs der Satellitenflotte vorgesehen – von derzeit rund zehn Systemen hin zu einer hohen dreistelligen Zahl.

Dieser technologische und strukturelle Ausbau erfordert zugleich Investitionen in Personal, Ausbildung und Infrastruktur. „Die Ankündigung von Verteidigungsminister Boris Pistorius, bis 2030 35 Milliarden Euro in die Weltraumsicherheit investieren zu wollen, ist ein Beleg für den zielgerichteten Einstieg in eine Gesamtarchitektur Weltraum“, betont Fregattenkapitän Hambach. Der neue Werdegang Weltraum, ein eigener Studiengang „Space“ an der Universität der Bundeswehr München, eine enge Zusammenarbeit mit Forschungseinrichtungen wie der Fraunhofer-Gesellschaft und dem Deutschen Zentrum für Luft- und Raumfahrt sowie der Aufbau eines bundeswehreigenen Satellitenbetriebszentrums seien weitere wichtige Schritte.

Damit wird deutlich: Die Teilstreitkraft CIR kämpft nicht im Weltraum, sondern macht militärisches Handeln in allen Dimensionen erst möglich. In enger Abstimmung mit dem Weltraumkommando sorgt es dafür, dass die weltraumgestützten Services auch in kritischen Lagen verfügbar sind.

Künstliche Intelligenz, Cyberspace und Vernetzung. Viele Entwicklungen haben Filme, Bücher und Spiele vorweggenommen und unser Bild von digitalen Technologien und Räumen entscheidend geprägt.

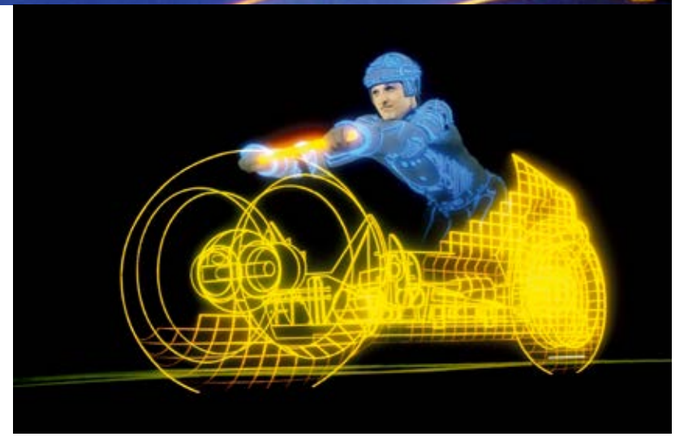
CYBER-WELTEN

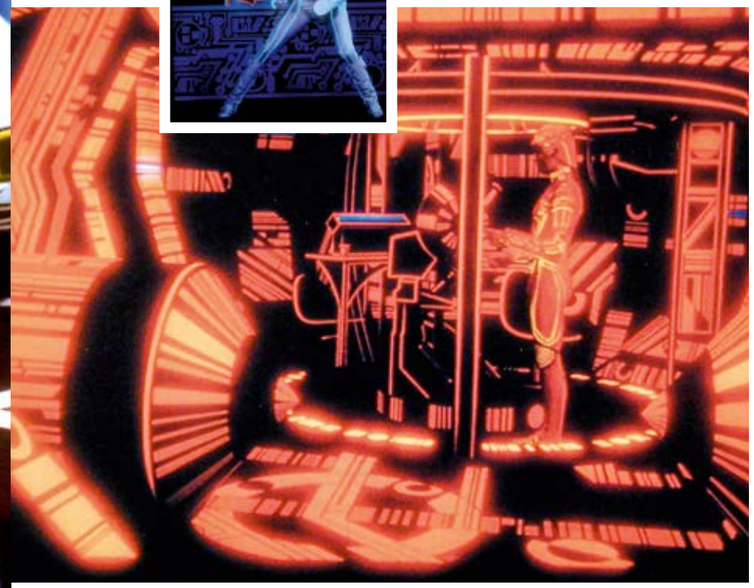
TEXT *Michael Schulz*

Wie sieht es wohl aus, wenn ein Mensch virtuelle Welten betritt? Darauf mussten die Designer von „Tron“ mangels Vorlagen eine Antwort finden. Sie schufen eine Bildsprache, die bis heute nachwirkt und wohl auch die Benutzeroberflächen moderner digitaler Anwendungen beeinflusst hat.

TRON

Regie:
Steven Lisberger
Darsteller:
Jeff Bridges,
Bruce Boxleitner
Jahr: 1982
Erhältlich: auf DVD, Blu-ray und als Video-on-Demand





„Tron“ gehört zu jenen Filmen, bei denen man nahezu jede Szene sofort wiedererkennt, so prägend ist der visuelle Stil, so ikonisch sind Elemente wie das Lightcycle. Erzählt wird die Geschichte des Programmierers Kevin Flynn (Jeff Bridges), der in eine digitale Computerwelt hineingezogen wird, in der Programme als eigenständige Wesen existieren. Diese Welt wird vom tyrannischen Master Control Program beherrscht. Gemeinsam mit dem Sicherheitsprogramm Tron leistet Flynn Widerstand. Auch wenn die Personifizierung von Computerprogrammen heute etwas altbacken wirkt, ist der Film nach wie vor sehenswert. Viele Effekte entstanden mangels ausgereifter Computertechnik per Hand. Vor allem die Gestaltung der virtuellen Welt hat viele nachfolgende Filme sowie unsere Vorstellung von digitalen Umgebungen beeinflusst. Wenn heutzutage solche Welten und Räume dargestellt werden, steckt oft ein bisschen (oder viel) von „Tron“ darin.

Regie:
Lana & Lilly Wachowski (Teil 1 bis 3), Lana Wachowski (Teil 4)
Darsteller:
Keanu Reeves, Carrie-Anne Moss, Laurence Fishburne, Hugo Weaving
Jahr: 1999 bis 2021
Erhältlich: auf DVD, Blu-ray und als Video-on-Demand

MATRIX

Mit einer sehr speziellen Form einer virtuellen Welt konfrontieren die vier „Matrix"-Filme ihr Publikum: einer Realität, die der echten zum Verwechseln ähnlich sieht und deren künstliche Natur den meisten Menschen nicht einmal bewusst ist. Einige wenige jedoch, wie Neo (Keanu Reeves), haben die Simulation der Maschinenwesen durchschaut und versuchen, die Menschheit aus ihrem digitalen Gefängnis zu befreien. Abgesehen davon, dass es tatsächlich Wissenschaftler gibt, die der Frage nachgehen, ob unser Universum eine Simulation sein könnte, stellt „Matrix" vor allem eine Problematik in den Mittelpunkt: die Machtergreifung einer von Menschen geschaffenen, überlegenen künstlichen Intelligenz und ihrer Maschinen. Wie die „Terminator"-Reihe prägten diese Filme die Skepsis gegenüber künstlicher Intelligenz maßgeblich. Auch visuell war „Matrix" bahnbrechend, beispielsweise mit dem Regen aus grünen Zeichen, der den Programmcode der Matrix darstellt. Er ist längst zum Synonym für eine digitalisierte Welt geworden.

Manga: 1989 bis 1991; geschrieben und illustriert von Masamune Shirow
Animefilm: 1995; von Mamoru Oshii
Realfilm: 2017; von Rupert Sanders, mit Scarlett Johansson
Erhältlich: Manga bei Egmont; Filme auf DVD, Blu-ray und als Video-on-Demand

GHOST IN THE SHELL

In einer nahen Zukunft haben viele Menschen ihren Körper durch kybernetische Implantate optimiert. Im Zentrum von „Ghost in the Shell" steht die Frage, was den Geist (Ghost) ausmacht, wenn der Körper (Shell) weitgehend künstlich ist. Die Bezüge zu unserer heutigen, permanent vernetzten Welt sind offensichtlich: Smartphones, soziale Medien und andere Technologien begleiten uns nahezu ständig, wodurch Algorithmen und Datenströme zunehmend unser Leben beeinflussen. „Ghost in the Shell" wirkt inzwischen wie eine zugespitzte Version dessen, was dauerhafte Online-Präsenz für die eigene Identität und Gesellschaft bedeutet. Auch die Grundkonstellation der Geschichte lässt Parallelen zu unserer Gegenwart zu: Ein Mitglied einer Cyber-Spezialeinheit jagt einen Hacker, der die Geister von Menschen manipuliert und für Verbrechen missbraucht.

Das noch nicht Gesehene darstellen.
Im Fall von „Ghost in the Shell" waren das unter anderem technologisch optimierte Körper. Die zentrale Frage, die sich dabei aufdrängt: Was macht so viel Technologie mit dem Geist eines Menschen?

NEUROMANCER

Der Roman „Neuromancer" hat unsere digitale Gegenwart fast prophetisch vorweggenommen. Er behandelt Hacking, globale Datennetze und digitale Identitäten – Jahrzehnte bevor diese Themen im Alltag relevant wurden – und machte den Begriff Cyberspace populär. Beschrieben wird dieser als ein Netzwerk aus virtuellen Räumen, das dem Internet und Virtual-Reality-Anwendungen unserer Gegenwart erstaunlich ähnelt. Um es zu verdeutlichen: Als William Gibson (Foto) Anfang der 1980er-Jahre diesen Roman schrieb, existierte das Internet noch gar nicht. Besonders meisterhaft ist nach wie vor jene Passage, in der der Hacker Case im Cyberspace ein vernetztes Gebäude manipuliert, sodass seine Komplizin Molly vor Ort Stück für Stück vorankommt, um schließlich aus einem Safe etwas zu stehlen. 42 Jahre nach der Erstveröffentlichung ist im Roman vieles topaktuell.

Autor:
William Gibson
Erstveröffentlichung:
1984
Erhältlich:
aktuell unter anderem bei Klett-Cotta als Paperback

DER STAATSFEIND NR. 1

Als der Actionthriller 1998 in die Kinos kam, wirkte das Szenario eines Staates, der digitale Technik zur Totalüberwachung seiner Bürgerinnen und Bürger einsetzt, noch wie Science-Fiction. Ein US-Anwalt (Will Smith) gerät zufällig in den Besitz eines Videos, das einen politischen Mord durch einen hochrangigen Geheimdienstbeamten dokumentiert. Daraufhin wird er mithilfe modernster Technik verfolgt. Satelliten, globale Datennetze und Abhörtechniken bilden die Grundlage dafür. Spätestens seit den Geheimdienstenthüllungen von Whistleblowern wie Edward Snowden einige Jahre später oder den aktuellen Entwicklungen in Ländern wie Russland und China wird jedoch deutlich, dass einiges aus dem Film durchaus realistisch ist.

Regie:
Tony Scott
Darsteller:
Will Smith,
Gene Hackman
Jahr: 1998
Erhältlich: auf DVD,
Blu-ray und als
Video-on-Demand

WARGAMES – KRIEGSSPIELE

Regie:
John Badham
Darsteller:
Matthew Broderick,
Dabney Coleman
Jahr: 1983
Erhältlich: auf DVD,
Blu-ray und als
Video-on-Demand

Das Szenario des Films mag überzeichnet wirken: Der Schüler und Computerfreak David Lightman (Matthew Broderick) dringt unbemerkt in einen Rechner des US-Verteidigungssystems ein und startet, was er zunächst für ein Spiel namens „Weltweiter thermonuklearer Krieg“ hält. Eigentlich startet er aber einen Countdown und beschwört eine internationale Krise herauf. Der Film brachte das Thema Hacking erstmals einem breiten Publikum nahe. Als der Film 1983 in die Kinos kam, waren Computer kaum verbreitet. Viele Menschen hatten damals noch keinen Computer gesehen, geschweige denn bedient. Umso überraschender war für das Publikum wohl die Erkenntnis, dass sich wichtige, an ein Netzwerk angeschlossene Infrastrukturen von außen manipulieren, also hacken lassen. Stilprägend war das Bild der Hackerarbeit: Vor leuchtenden Bildschirmen tippt David Computercodes und Textbefehle ein – ein Gegenentwurf zu fantasievoll visualisierten Cyberwelten.

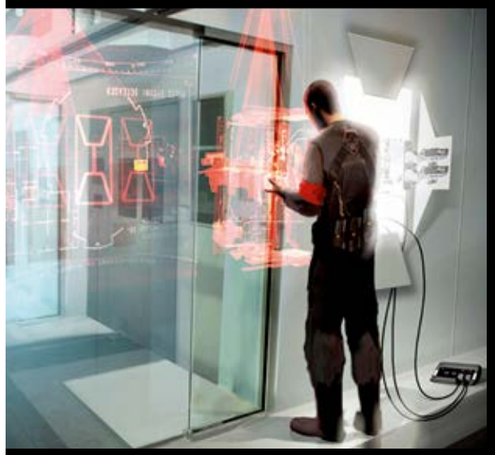
S. 90: Alamy Stock Photo/ALI Pics (o.), IMAGO/Ronald Grant (r.o.B.J.B.), IMAGO/Allstar/Mary Evans AF Archive Mgm (E.S.I.-2), IMAGO/EntertainmentPictures (E.S.I.u.), Alamy Stock Photo/Photo12 (r.m.)
S. 91: IMAGO/Maximum Film (r.o.), Alamy Stock Photo/RGR Collection (r.o.), Alamy Stock Photo/LANDMARK MEDIA (r.S.2.), Alamy Stock Photo/Pictorial Press Ltd (r.S.3.u.4.), Alamy Stock Photo/TCD/Prod.DB (l.u.)

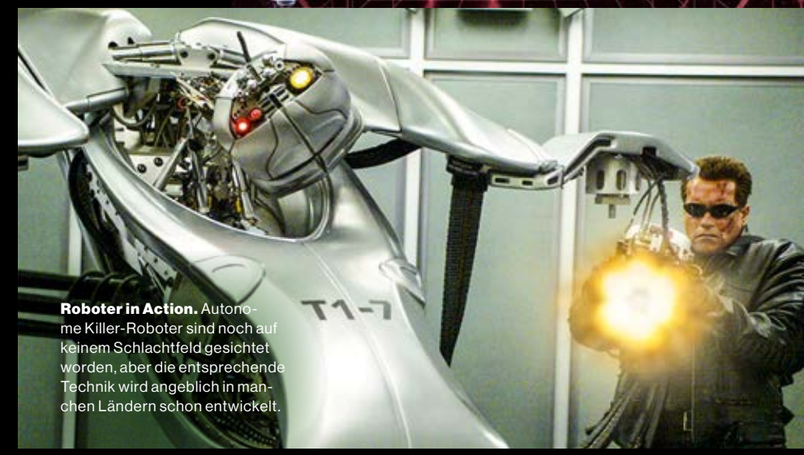
Regie:
James Cameron u. a.
Darsteller:
Arnold Schwarzenegger,
Linda Hamilton u. a.
Jahr: sechs Filme seit 1984
Erhältlich: auf DVD,
Blu-ray und als
Video-on-Demand

TERMINATOR

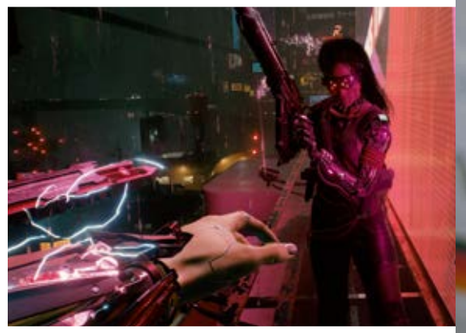
Die ersten beiden „Terminator“-Filme haben maßgeblich dazu beigetragen, die Angst vor einer übermächtigen KI im kollektiven Bewusstsein zu verankern. Im Filmjahr 1997 entwickelt Skynet, ursprünglich als globales Verteidigungsnetzwerk konzipiert, ein Bewusstsein und vernichtet mit einem Atomschlag einen Großteil der Menschheit. Die Überlebenden führen einen verzweifelten Krieg gegen die KI und ihre Maschinenarmee. Um ihren Sieg abzusichern, schickt Skynet einen Terminator in die Vergangenheit: in Teil eins um die Mutter des späteren Rebellenführers zu töten, in Teil zwei um ihn als Kind auszuschalten. Die Menschen wiederum schicken eigene Kämpfer und umprogrammierte Maschinen hinterher. Dieser Grundkonflikt prägt die Filmreihe bis heute. Auch wenn vieles noch wie Zukunftsmusik klingt, hat die Debatte über autonome Waffen zuletzt an Fahrt aufgenommen, nicht zuletzt angesichts des massenhaften Einsatzes von Drohnen im Ukrainekrieg. Die markanten Filmszenen, in denen die Welt aus der Perspektive der Terminatoren gezeigt wird, erinnern heute unweigerlich an die Kamerabilder moderner Drohnensysteme.

Die Welt, wie sie ein Terminator sieht. Vergleiche mit modernen Drohnensystemen liegen nahe. Wurden die Ingenieure von heute durch die Filme von damals beeinflusst?





Roboter in Action. Autonome Killer-Roboter sind noch auf keinem Schlachtfeld gesichtet worden, aber die entsprechende Technik wird angeblich in manchen Ländern schon entwickelt.



Mittendrin statt nur dabei. Der Spieler taucht tief in eine dystopische Zukunft ein und wird selbst zum hackenden Cyberpunk mit Bio-Implantaten.

CYBERPUNK 2077

Entwickler: CD Projekt Red
Erstveröffentlichung: 2020
Erhältlich: für macOS, PC, PS 4 & 5, Nintendo Switch 2, Xbox One & Series X/S

Wer fantastische Cyberwelten nicht nur passiv als Film oder Buch erleben, sondern auch aktiv erkunden möchte, kommt an „Cyberpunk 2077“ nicht vorbei. Das Action-Rollenspiel des polnischen Studios CD Projekt Red („The Witcher“-Reihe) verbindet die visuelle Ästhetik von Filmen wie „Blade Runner“ mit Identitätsfragen in einer digitalen Welt à la „Ghost in the Shell“ und dem Cyberpunk-Hacking des Romans „Neuromancer“. Der oder die Spielende erkundet eine Metropole namens Night City in der Ego-Perspektive und erlebt dadurch hautnah, welche Auswirkungen Bio-Implantate auf die eigenen Fähigkeiten haben. Außerdem wird man zum Hacker und infiltriert Netzwerke, entwendet Daten und manipuliert Gegner auf digitale Weise. Das Spiel schafft es, Cyberspace-Visionen interaktiv und unmittelbar erfahrbar zu machen.

HACKERS

Lange Zeit waren Computer das Spielzeug von Nerds und Eigenbrötlern (siehe „Wargames“). Dann kam 1995 der Film „Hackers“: Eine Gruppe cooler Teenager geht darin in einem bunt überzeichneten Cyberspace gegen einen betrügerischen Konzern vor. Wenn die Clique um Kate (Angelina Jolie) hackt, füllt keine endlose Kolonne von Zeichen mehr den Bildschirm, sondern eher eine Art rasantes Videospiel. Auch diese Botschaft blieb hängen: Über den Cyberspace werden enorme Datenmengen in hoher Geschwindigkeit ausgetauscht und man kann in kürzester Zeit auf weit entfernte Bereiche zugreifen.

Regie: Iain Softley
Darsteller: Jonny Lee Miller, Angelina Jolie
Jahr: 1995
Erhältlich: auf DVD, Blu-ray und als Video-on-Demand

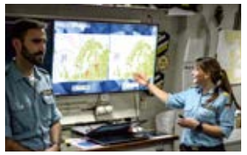
S. 92: CD PROJEKT RED (o.l.), CD PROJEKT S.A. (r.o.), CD PROJEKT S.A. (r.m.), Alamy Stock Photo/THA (u.m.), Alamy Stock Photo/Moviestore Collection Ltd (r.u. B.i.B.)

Dranbleiben
Mehr zum Thema

Bundeswehr online

Wer beschützt die Cyber-KRITIS?
Cyber Coalition ist eine jährlich stattfindende Cyberabwehr-Übung der NATO. Ende 2025 trainierten Kräfte des Cyber- und Informationsraums (CIR) der Bundeswehr dort mit Streitkräften, zivilen Behörden, Industrie und Wissenschaft aus über 30 Ländern den Schutz kritischer Infrastrukturen (KRITIS). Ziel der Übung war es, die Resilienz und Abstimmung aller beteiligten Akteure bei einem Cyberangriff zu stärken.

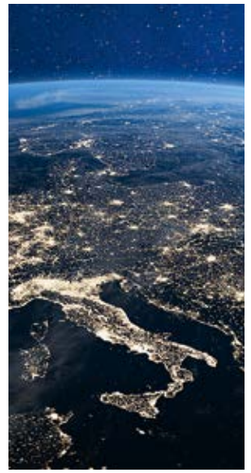
PEGASUS geht in die nächste Phase
Die ersten beiden Maschinen des neuen Aufklärungsflugzeugs von CIR wurden Ende 2025 nach Deutschland überführt, wo die Industrie weitere Anpassungen vornimmt. Ab 2028 sollen insgesamt drei modifizierte Flugzeuge für die Bundeswehr bereitstehen. Die Truppe erhält mit PEGASUS eine der neuesten Sensoriken zur luftgestützten Fernmelde- und elektronischen Aufklärung.



Wie KI die Wettervorhersage der Bundeswehr verändert
Das Geoinformationswesen der Bundeswehr und der Deutsche Wetterdienst arbeiten gemeinsam an einer KI, um noch schneller und zuverlässiger Wettervorhersagen zu erstellen. Die Streitkräfte sind auf besonders präzise Vorhersagen angewiesen. Fast jede Operation, sei es ein Transportflug, der Einsatz von Drohnen oder die Bewegung von Truppenteilen, ist davon betroffen.

Neues Innovationszentrum der Bundeswehr eröffnet
Neue Technologien können die militärischen Kräfteverhältnisse radikal verändern. Damit diese schnell in der Truppe ankommen, ist am 2. Februar 2026 das Innovationszentrum der Bundeswehr in Erding von Verteidigungsminister Boris Pistorius eröffnet worden. Es dient als zentrale Ansprechstelle für Start-ups, Unternehmen und Wissenschaft und soll Innovationen testen. Die ersten Projekte reichen von Drohnenabwehr über KI-gestützte Drohnenschwärme bis zu Kleinstsatelliten.

S. 94: Bundeswehr/Jonas Weber (E.S.o.), Bundeswehr/Maximilian Bosse (E.S.m.u.u.), Bombardier (Z.S.1–2), Bundeswehr/Marcus Mohr (D.S.o.), Bundeswehr/Marc Tessensohn (D.S.u.), Bundeswehr/Dirk Bannert (V.S.o.u.u.)
S. 95: Bundeswehr/stock.adobe.com/NicoElNino (E.S.), Bundeswehr/Leon Beiz (Z.S.), Bundeswehr/Jennifer Heyn (D.S.o.), Bundeswehr/Torsten Kraatz (D.S.u.), Bundeswehr/Janina Kiel (V.S.)



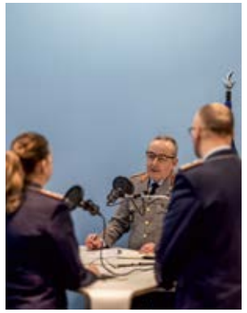
Quiz zum Thema Weltraum
In der Verantwortung welcher Teilstreitkraft liegt die Dimension Weltraum? Wer betreibt das Weltraumlagezentrum? Und wie entstehen eigentlich Nordlichter? Teilnehmende des Lehrgangs Generalstabs-/Admiralstabsdienst National haben sich mit der Dimension Weltraum auseinandergesetzt und dieses Quiz zusammengestellt. Viel Spaß dabei!

Ein Offizieranwärter will in den Weltraum schauen
Maximilian H. hat sich auf den neuen Werdegang „Weltraum“ beworben. Im Interview erzählt er, seit wann er sich für das Thema begeistert, was er während der fachbezogenen Ausbildung lernt und was er sich für seine spätere Verwendung im Weltraumlagezentrum der Bundeswehr in Uedem erhofft.

Bundeswehr und Weltraum
Deutschland braucht den Weltraum. Von der Kommunikation über die Navigation bis zu Zahlungsverkehr und Stromversorgung beruhen heute viele kritische Systeme auf Satellitenkommunikation. Deswegen hat sich die Bundeswehr den Schutz dieser Dimension auf die Fahnen geschrieben. Die Seite gibt mit Artikel, Interview und Podcast einen Überblick über das Thema.

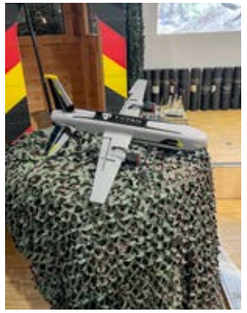
Teil der Unendlichkeit: Der Weltraumlageoffizier
Eine, die es schon ins Weltraumlagezentrum geschafft hat, ist Oberleutnant Kerstin. Im Bundeswehr-Berufe-Podcast „Gehör zu mir!“ erzählt sie von ihrer Arbeit als Weltraumlageoffizierin, von der Zusammenarbeit mit den Fachleuten vom Deutschen Zentrum für Luft- und Raumfahrt und von der Bedeutung des Weltraums für die Bundeswehr.

Ynside

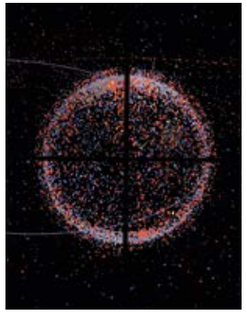


Podcast „Auf Augenhöhe“ mit dem Generalinspekteur – Drohnenspezial
Drohnen und ihre Abwehr gewinnen immer mehr an Bedeutung. Generalinspekteur General Carsten Breuer und Hauptmann Nico H. von der Arbeitsgruppe Drohnenabwehr im Luftwaffentruppenkommando sprechen über ein Thema, das die Truppe bewegt.

Frisch erprobt: Simulator zur Drohnenabwehr aller Truppen
In modernen Kriegen kommen immer öfter Klein- und Kleinstdrohnen zum Einsatz. Wie sie mit Handwaffen abgewehrt werden können, wird beim Innovationsvorhaben „Drohnenabwehr aller Truppen“ kostengünstig und realitätsnah simuliert.



Erfolgreicher Feldversuch mit KI-gesteuerten Abfangdrohnen
Der Krieg in der Ukraine zeigt, wie Drohnen die Dynamik in heutigen Konflikten verändert haben. Ihr massiver Einsatz zu Aufklärungszwecken und für Angriffe auf militärische und zivile Infrastruktur ist für Verteidiger zu einer enormen Herausforderung geworden.



Künstliche Intelligenz im Weltall
Die Bundeswehr testet viele Systeme und Programme, die auf künstlicher Intelligenz basieren. Für die Projekte ist unter anderem der Cyber Innovation Hub der Bundeswehr zuständig. In einer der vielen Innovationen geht es um zwei KI-gestützte Analysesysteme für den Weltraum – eins für Wettermessungen und das andere zur Kollisionswarnung im All.

S. 96: Bundeswehr/Tom Twardy (E.S.), Bundeswehr/Mario Bähr (Z.S.o.), Bundeswehr/Johannes Heyn (Z.S.m.u.u.), Bundeswehr/Arthur Galbraith (D.S.), Bundeswehr/Francis Hildemann (V.S.1–3)
S. 97: Bundeswehr/Steve Elbe (E.S.1–2); Participant Media, Showtime Documentary Films (Z.S.o.), Gruppe 5 Filmproduktion ZDF 3sat arte (Z.S.m.), Carola Hartmann/Miles-Verlag (D.S.), Motorbuch Verlag (V.S.o.), Diplomatic Council (V.S.u.)

Videos

„Nachgefragt“: Elektronische Kampfführung
Wie ein Krieg geführt wird, der für die Öffentlichkeit unsichtbar bleibt, erklärt Oberst Sönke Marahrens vom Zentrum Digitalisierung der Bundeswehr in dieser Folge von „Nachgefragt“. Dabei ordnet er die aktuellen sicherheitspolitischen Entwicklungen ein und zieht Lehren aus dem Krieg in der Ukraine.

„Nachgefragt“: Wie Deutschland im Weltall verteidigt wird
Die Bundeswehr ist am Boden, zur See und in der Luft für die Sicherheit Deutschlands zuständig – und im Weltraum. Welche Aufgaben mit der militärischen Verteidigung im Weltall verbunden sind, erläutert Generalmajor Michael Traut, Kommandeur des Weltraumkommandos der Bundeswehr, in dieser Folge von „Nachgefragt“.

Filme

„Zero Days“ (Dokumentation, 2016)
2010 machen IT-Fachleute eine spektakuläre Entdeckung: Ein hochkomplexer Computerwurm namens Stuxnet verbreitet sich mit noch nie gesehener Aggressivität auf der ganzen Welt. Die Forscherinnen und Forscher ahnten nicht, dass sie auf eine Kriegswaffe von CIA und Mossad gestoßen waren, um die Urananreicherung im Iran zu stören.

Verfügbar bei verschiedenen Streaming-Diensten

„Der unsichtbare Krieg – Angriff aus dem Netz“ (Dokumentation, 2023)
Regierungen, Unternehmen, Organisationen und Privatpersonen geraten zunehmend ins Visier von Cyberangriffen. Weltweit verursacht Cyberkriminalität längst einen wirtschaftlichen Schaden, der den von Naturkatastrophen übersteigt. Hinter den Attacken stehen oft Einzeltäter oder kleinere Gruppen. Was treibt sie an?

Verfügbar bis 30.10.2026 in der Arte-Mediathek

Bücher

„Streng geheim! Elektronische Kampfführung im Kalten Krieg“
Jörg Beining hat viele unveröffentlichte Dokumente ausgewertet, um die Elektronische Kampfführung (EloKa) der Bundeswehr und NATO aus der Perspektive des Ministeriums für Staatssicherheit der DDR zu beleuchten. Der Autor hatte Anfang der 1970er-Jahre selbst als EloKa-Soldat gedient.

Autor *Jörg Beining*
Verlag *Miles-Verlag*
Umfang *360 Seiten*
Erscheinungsjahr *2021*
ISBN-13 *978-3-967-76007-1*

„Raumfahrt-Geschichte: Die 100 wichtigsten Ereignisse“
Der Start des sowjetischen Satelliten Sputnik 1957 markierte den Beginn der Raumfahrt. In den Jahrzehnten danach folgten viele technische Durchbrüche und historische Meilensteine. Der reich bebilderte Band zeichnet 100 wegweisende Ereignisse nach.

Autor *Eugen Reichl*
Verlag *Motorbuch Verlag*
Umfang *352 Seiten*
Erscheinungsjahr *2022*
ISBN-13 *978-3-613-04396-1*

„Sicherheit im All: Wie wir Europa im Weltraum verteidigen“
Welche Maßnahmen muss Europa ergreifen, um seine Sicherheit im Weltall zu gewährleisten? Die Autorinnen und Autoren dieses Buches aus Politik, Wirtschaft und Wissenschaft versuchen, darauf Antworten zu finden und die damit verbundenen dringenden Herausforderungen zu skizzieren.

Autoren *Andrius Kubilius u. a.*
Verlag *DC Publishing*
Umfang *572 Seiten*
Erscheinungsjahr *2025*
ISBN-13 *978-3-986-74196-9*

Ausstellungen

in der Weltraumausstellung auf 5.000 Quadratmetern rund 700 Exponate – darunter Raketen, Satelliten und weitere historische Raumfahrttechnik – zu sehen. Das Museum verbindet Wissen und Unterhaltung und lässt die Raumfahrt lebendig werden. Nicht nur für Technikfans!

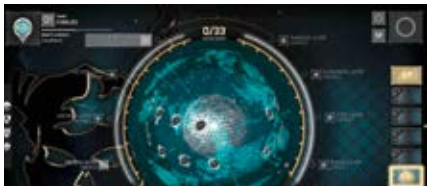
Technik Museum Speyer
Das Museum beherbergt eines der beeindruckendsten Weltraumexponate Deutschlands. Im Mittelpunkt steht die originale Raumfähre Buran, sozusagen die sowjetische Variante eines Space Shuttles. Darüber hinaus gibt es

Geöffnet werktags von 9 bis 18 Uhr, samstags, sonntags und feiertags bis 19 Uhr

ESA-Satellitenkontrollzentrum in Darmstadt
Wie wird der Weltraum erforscht? Wie wird unser Planet geschützt? Antworten auf diese und weitere Fragen erhalten Interessierte im ESA-Satellitenkontrollzentrum in Darmstadt. Bis zu 20 Personen auf einmal können Kontrollräume und ein Zwillingsmodell der Raumsonde Rosetta besichtigen. Das Modell wurde im Rahmen der 2004 gestarteten ESA-Mission für Simulationen und Funktionstests eingesetzt.

Für aktuelle Termine den QR-Code scannen.

Games



„NITE Team 4 – Military Hacking Division“
Als Hacker der geheimen Militäreinheit NITE Team 4 werden Cyberoperationen gegen Terrornetzwerke und feindliche Staaten durchgeführt. Das Spiel setzt auf authentisch wirkende Tools und Missionen, die an reale Cyberkriegsführung angelehnt sind. Ziel ist es, Verdächtige im Dark Web zu identifizieren, Netzwerke zu infiltrieren und Drohnenangriffe zu koordinieren. Da heißt es, unter Zeitdruck einen kühlen Kopf zu bewahren.

Für macOS & Windows PC

„Watch Dogs: Legion“
In einem autoritären Großbritannien wird eine Hackergruppe fälschlich für einen Terroranschlag verantwortlich gemacht. Die Spielenden stellen sich gegen das verbrecherische Regime, um die Wahrheit aufzudecken. Teil 3 der populären Hacker-Reihe setzt auf eine ungewöhnliche Innovation: In der offenen Spielwelt können zahlreiche Nicht-Spieler-Charaktere rekrutiert und als Teil des Widerstandsnetzwerks eingesetzt werden.

Für PlayStation 4 & 5, Windows PC sowie Xbox One & Series X/S

S. 98: Technik Museum Speyer (E.S.I.1–2), Alice & Smith (E.S.I. 3–4), ESA (Z.S.r.1), ESA/J. Mai (Z.S.r.2), Ubisoft (Z.S.r.3–4)

Impressum

Herausgeber Bundesministerium der Verteidigung, Stab Informationsarbeit, Stauffenbergstraße 18, 10785 Berlin

Verteilung innerhalb der Bundeswehr Bundesamt für Infrastruktur, Umweltschutz und Dienstleistungen der Bundeswehr, FA I RegMgmt BA, Referat 3 Bereitstellung: GM Freiherr-von-Gersdorff-Kaserne, Kommerner Straße 188, 53879 Euskirchen, 02251/953-3747, Bundeswehrkennzahl: 3461, mediendisposition@bundeswehr.org

Vertrieb Anteil Öffentlichkeitsarbeit Bundesamt für das Personalmanagement der Bundeswehr II 1.4 Vertrieb: Brühler Straße 309, 50968 Köln, bapersbwII14vertrieb@bundeswehr.org

Redaktionsanschrift Zentrum Informationsarbeit Bundeswehr, Redaktion der Bundeswehr/Y-Redaktion, Reinhardtstraße 52, 10117 Berlin, Bundeswehrkennzahl: 8841, zivile Einwahl: 030/886228-Durchwahl

Redaktionssekretariat -2135, redaktionbweingang@bundeswehr.org

Leiter Redaktion der Bundeswehr Oberst Roman Grunwald, redaktionbwleiter@bundeswehr.org

Leitender Redakteur Y Dr. Florian Stöhr, -2481, leitung@y-magazin.de

Chefin vom Dienst Y Hauptmann Beate Schöne, -2482, cvd@y-magazin.de

Bildredaktion Andrea Bienert, -2660; Jörg Hüttenhölscher, -2665; bildredaktion@y-magazin.de

Schlussredaktion Frank Buchstein, schlussredaktion@y-magazin.de

Verlegerische Betreuung, Gestaltung und Produktion C3 Creative Code and Content GmbH, Heiligegeistkirchplatz 1, 10178 Berlin, info@c3.co
Alleinige Gesellschafterin der C3 Creative Code and Content GmbH ist die Burda Gesellschaft mit beschränkter Haftung mit Sitz in Offenburg. Alleinige Gesellschafterin der Burda Gesellschaft mit beschränkter Haftung ist die Hubert Burda Media Holding Kommanditgesellschaft mit Sitz in Offenburg. Geschäftsführende, persönlich haftende Gesellschafter der Hubert Burda Media Holding Kommanditgesellschaft sind Prof. Dr. Hubert Burda und die Hubert Burda Media Holding Geschäftsführung SE.

Projektmanagement Tanja Klebsch, Account Director

Textredaktion Sebastian Blum, Lead Editorial; Michael Schulz, Senior Editor

Gestaltung Michael Pfötsch, Lead Design; Inka Gerbert, Art Director; Ben Kleinberg, Senior Information Designer (3D); Marcus Spiller, Information Designer; Diana Rosenfeld, Junior Information Designer; Carsten Kalaschnikow, Bildredaktion; Sina Franco, Bildredaktion

E-Paper Anica Schwarzer, Senior Art Director; Inka Gerbert, Art Director

Mitwirkende Hauptfeldwebel Lea Bacherle, Wiebke Bolle, Hauptmann Maximilian Bosse, Franziska Hennecke, Major Hannes Lembke, Martina Pump, Hauptmann Thomas Skiba, Oberstleutnant Torsten Stephan, Hauptmann Janet Watson, Oberstleutnant Michael Wawrzyniak

Aboverwaltung Im Auftrag von C3 Creative Code and Content GmbH: Fazit Communication GmbH, c/o CoverService GmbH & Co. KG, Postfach 1363, 82034 Deisenhofen, 089/85853-832, fazit-com@cover-services.de

Bezugspreis Jahresabonnement 22,20 Euro inkl. MwSt. und Versandkosten, Bundeswehrangehörige, Reservisten, Schüler, Auszubildende, Studierende und Ruheständler erhalten mit Nachweis 15 Prozent Rabatt.

Erscheinungsweise Vier Ausgaben im Jahr

Druck Dierichs Druck + Media GmbH & Co. KG, Frankfurter Straße 168, 34121 Kassel, www.ddm.de

Auflage 36.000

Redaktionsschluss
Ausgabe Nr. 1/2026: 3. Februar 2026

Y im Abo!

Bundeswehr aus erster Hand gibt es nur im Y-Magazin. Viermal im Jahr spannende Reportagen, interessante Interviews und exklusive Informationen aus allen Bereichen der Bundeswehr – für 22,20 Euro jährlich. Jetzt per E-Mail abonnieren:

abo@y-magazin.de

Aboverwaltung durch Fazit Communication GmbH, c/o CoverService GmbH & Co. KG


MACH, WAS WIRKLICH ZÄHLT.
STOLZ AUF DAS, WAS SIE TUN?
DANN ZEIGEN SIE ES ALLEN.
Zeigen Sie mit Herz und Leidenschaft, was in Ihnen und Ihrer Bundeswehr steckt. Repräsentieren Sie sich und Ihren Arbeitsplatz in neuen, deutschlandweiten Kampagnen. Bewerben Sie sich jetzt!
Ihr Talent, Ihre Fähigkeiten, Ihr Style. Zeigen Sie uns, was Sie drauf haben, und werden Sie Gesicht für unsere Kampagnen.
Sie brauchen sich nur unter ynside.extranet-bw.de anzumelden. Wir freuen uns auf Ihre aussagekräftigen Fotos und coole Kurzvideos. Kommen Sie in unser Team und inspirieren Sie andere.
Fragen? BMVgArbeitgebermarkeBw@bmvg.bund.de
WERDE GESICHT UND STIMME DER BUNDESWEHR.
JETZT ANMELDEN: YNSIDE.EXTRANET-BW.DE
BUNDESWEHR