Hardthöhen-KURIER
DAS MAGAZIN FÜR SOLDATEN UND WEHRTECHNIK

FÜR EIN STARKES EUROPA

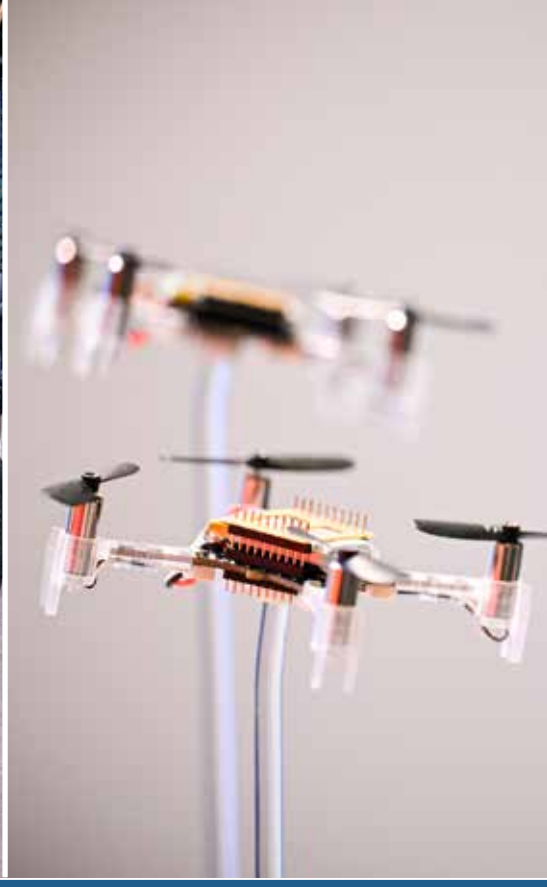
HHK w w w . h a r d t h o e h e n k u r i e r . d e AFCEA 2026

SONDERPUBLIKATION
zur AFCEA Fachausstellung 2026

AFCEA Bonn e.V.

39. AFCEA Fachausstellung – 12./13. Mai 2026

AFCEA Bonn e.V.



Was war los auf der AFCEA Fachausstellung?

©MRV/Socrates Tassos (6)

Die AFCEA Fachausstellung 2026 – Zahlen und Fakten

Von Jochen Reinhardt

Die 39. AFCEA-Fachausstellung 2026 hat am 12. und 13. Mai über 8.800 Teilnehmerinnen und Teilnehmer angelockt und damit gezeigt, dass sie eine der bedeutendsten IT-Messen für Verteidigung und öffentliche Sicherheit in Deutschland ist. Die Ausstellung stand mit 325 Ausstellern und 233 Ständen im World Conference Center unter dem Motto „Vernetzt denken & sicher handeln als Antwort einer gesamtstaatlichen Verteidigung".

Über 8.800 Teilnehmerinnen und Teilnehmer besuchten die 39. AFECEA-Fachausstellung.

General a. D. Jörg Vollmer bei seiner Keynote zur Eröffnung der Ausstellung.

Generalmajor Armin Fleischmann, Vorsitzender von AFCEA Bonn e. V., sagte auf dem begleitenden Symposium: „Verteidigung ist längst keine ausschließlich militärische Aufgabe mehr. Sie ist eine gesamtgesellschaftliche Verantwortung – von der kritischen Infrastruktur über den Katastrophenschutz bis hin zur Cybersicherheit. Vernetzte Systeme, digitale Souveränität und resiliente Kommunikation sind keine technischen Nischen. Sie sind strategische Voraussetzungen für die Handlungsfähigkeit unseres Staates." Dafür sei Bonn als Wiege der Bundeswehr auch ein Zentrum der IT, sagte Guido Déus, Oberbürgermeister von Bonn, in seinem Grußwort zur Eröffnung.

Wolfgang Quirin, Leiter der AFCEA Fachausstellung, ordnet die Ausstellung wie folgt ein: „Wir leben in einer Zeit, in der sich die sicherheitspolitische Lage weltweit spürbar verändert. Neue Bedrohungen entstehen und technologische Entwicklungen schreiten in rasantem Tempo voran. In diesem Umfeld kommt der Zusammenarbeit zwischen Industrie, Forschung und staatlichen Institutionen eine zentrale Bedeutung zu. Diese Messe ist mehr als nur eine Ausstellung moderner Technologien. Sie ist ein Ort des Austauschs, des Dialogs und der kritischen Auseinandersetzung. Die präsentierten Systeme und Lösungen stehen nicht nur für technischen Fortschritt, sondern auch für die Fähigkeit, Sicherheit verantwortungsvoll zu gestalten."

General a. D. Jörg Vollmer beschrieb in seiner Keynote Deutschlands Situation als Zwischenlage: Deutschland sei nicht im Krieg, aber auch nicht mehr im Frieden. Als Beispiele führt er unter anderem russische Drohnen über europäischen Luftwaffenstützpunkten und Flughäfen auf. Sabotage gegen Eisenbahnen und Logistikzentren für Ukraine-Lieferungen. Brandanschläge. Einschleusung von Geschäftsleuten in westliche Institutionen. Wahlbeeinflussung. Mordpläne. Störungen des Navigationssystems GPS im Ostseeraum. Der Verdacht, dass zivile Schiffe als Werkzeuge dienen, um Glasfaser- und Überwachungskabel in Nord- und Ostsee zu beschädigen.

Deutschlands Rolle im Bündnis ist die logistische Drehscheibe. Verstärkungskräfte müssen durch Deutschland. Material muss durch Deutschland. Verwundete müssen zurückgeführt werden. Häfen, Schienen, Straßen, Flughäfen, Brücken, Energienetze, Kommunikationssysteme und Verwaltungen werden Teil der Verteidigungsfähigkeit. Hier müssen Deutschlands Institutionen einfach schneller werden und alle die Situation ernster nehmen.

Brigadegeneral Michael Jäger, Abteilungsleiter Informationstechnik im BAAINBw, stellte dafür die neue Organisation seiner Behörde vor und stellte fest, dass genügend Geld vorhanden sei. Die Fachausstellung zeige außerdem, dass die notwendige Technologie bereitstehe. Das Zusammenspiel für gesamtstaatliche Sicherheit und Vernetzung untersucht AFCEA Bonn e.V. derzeit mit dem „Gesamtstaatlichen Sicherheitsökosystem 2030".

Die 40. AFCEA Fachausstellung findet am 25. und 26. Mai 2027 statt.

AFCEA Bonn e.V.

„Ich möchte nicht auf diese Location verzichten“

Interview mit Generalmajor Armin Fleischmann, Vorsitzender der AFCEA Bonn e.V. und Abteilungsleiter Planung CIR und Digitalisierung der Bundeswehr im Kommando Cyber- und Informationsraum

©MRV/Socrates Tasso (2)

Generalmajor Armin Fleischmann im Gespräch am Stand des Mittler Report Verlags auf der AFCEA Fachausstellung 2026.

Sehr geehrter Herr General, was ist Ihr Fazit der AFCEA Fachausstellung in diesem Jahr?
Wir haben gestern und heute über 8.800 Besucher gehabt, bei 325 ausstellenden Industriepartnern oder Behörden und 233 Ständen insgesamt. Denn wir bieten auch für die Teilstreitkräfte, regierungsnahe Organisationen oder Sozialverbände Ausstellungsfläche. Und die kommen gerne und erleben einen immer größeren Zulauf. Das Ergebnis freut mich sehr.
Wir haben in den letzten Jahren unheimlich viele Anfragen bekommen von Firmen, die gerne mit dabei sein wollen. Dafür mussten wir uns vergrößern, obwohl der Veranstaltungsort platzmäßig begrenzt ist. Also haben wir nach Lösungen gesucht, wie wir vor allem junge Unternehmen integrieren können. Darum haben wir eine Fläche für Start-ups gemacht, die wir kostengünstig zur Verfügung gestellt haben, sodass Start-ups sich einen Auftritt leisten können und ihre Produkte zeigen und vorstellen können.

Können Sie so überblicken, wie die Ausstellerzahl gegenüber dem letzten Jahr gewachsen ist und welchen Anteil davon Start-ups ausmachen?
Wir haben ungefähr 30 bis 40 Start-ups mehr als im letzten Jahr. Insgesamt muss man dazu sagen, dass die Zahl der Firmen stagniert, weil es einfach nicht mehr Platz gibt. Wir mussten etwa 100 Firmen absagen. Das ist natürlich auch ein schwerer Schlag für die Firmen.
Aber lieber klein und fein. Ich möchte nicht auf diese Location verzichten. Einerseits sind wir seit 39 Fachausstellungen hier in der Bundesstadt Bonn beheimatet. Auf der anderen Seite haben wir hier diesen ehemaligen Bundestags-Plenarsaal. Das ist einfach ein Juwel. Das haben wir woanders nicht. Und aus diesem Grund lieber hierbleiben und lieber begrenzen, aber dafür Hochwertwirtschaft und Hochwertbereiche einsetzen.

Sie haben das Thema Gesamtverteidigung in den Mittelpunkt gestellt. Wie hat sich das in der Durchführung konkretisiert?
Das Entscheidende bei der Gesamtverteidigung ist, dass man ein Netzwerk bildet, in dem sowohl die zivile als auch die militärische Verteidigung zusammenarbeitet. Dazu braucht man Industrie, Forschung und die komplette Community. AFCEA ist der Platz, wo wir Behörden, Organisationen für Sicherheit und Zusammenarbeit, Verteidigung und Forschungseinrichtungen zusammenbinden können. Das Schöne ist, dass hier in den Gesprächen Partnerschaften entstehen können. Da bin ich auch ein bisschen stolz drauf, dass wir das mittlerweile geschafft haben.

Was steht bei der AFCEA Bonn für den Rest des Jahres noch auf dem Programm?
Wir haben in diesem Jahr keine Mitgliederwahl, keine Vorstandswahl, von daher können wir unser Programm durchziehen. Wir arbeiten mit verschiedenen Verbänden wie dem BDSV zusammen. Wir haben unsere nächste Veranstaltung am 16. und 17. Juni in Berlin und wir werden am 7. und 8. Oktober im Maritim in Bonn die Gesamtverteidigung mit dem Bonner IT-Dialog noch mal deutlich stärken.
Da freuen wir uns schon auf viele andere Dienststellen wie das BBK und ähnliche, die dann kommen. Die Vizeministerpräsidentin von Nordrhein-Westfalen hat sich mit einer Keynote angekündigt. Da haben wir also mit Sicherheit ein tolles Programm. Ich glaube, es ist bitter notwendig in Deutschland, auch aufgrund der weltweit politischen Situation, dass wir diesen Bereich zivile Verteidigung mit militärischer Verteidigung sinnvoll vernetzen. Und dafür leistet die AFCEA gerne einen Beitrag.

Können Sie schon etwas zum Ausblick auf das nächste Jahr sagen, vielleicht thematisch zur nächsten AFCEA Fachausstellung?
Themen, die immer wieder von Interesse sind, sind neben Cybersicherheit mittlerweile der Bereich Welt-

General Fleischmann mit Burghard Lindhorst und Stefan Axel Boes vom Mittler Report Verlag (v. r.).

raum. Nachdem der Minister angekündigt hat, dort in den nächsten fünf Jahren 35 Milliarden ausgeben zu wollen, kümmern wir uns darum, dass dieses Geld vorzugsweise in die deutsche Industrie fließt. Wir wollen auch die Start-up-Community entsprechend bedienen, wenn sie denn in der Lage ist, das zu leisten. Denn ein Punkt, der insbesondere unserer Space-Community in Deutschland nicht so gefällt, ist, dass wir natürlich Leistung erwarten. Und zwar durch vorhandene Produkte und nicht durch PowerPoint und Ideen, die wir erst in fünf bis zehn Jahren bekommen. Da muss man dann auch realistisch sein.

Neben dem Thema Weltraum stehen insbesondere der Bereich KI und Daten. Daran arbeiten wir intensiv in den drei Bereichen Streitkräfte, Bundeswehrverwaltung und Personal. Angefangen beim Personal, versuchen wir jetzt die Streitkräfte mit digitaler Grundbefähigung auch im Bereich KI deutlich zu ertüchtigen. Wir investieren sehr, sehr viel in KI-Produkte wie KI-Procure, die wir in der Verwaltung einsetzen, zum Beispiel in Bundeswehrdienstleistungszentren, wo wir Beschaffungen automatisieren können.

Im Bereich der Streitkräfte haben wir natürlich auch entsprechende Projekte. Insgesamt hat sich die AFCEA Fachausstellung mittlerweile in Deutschland zu einer der wichtigsten Cyber-IT-Messen entwickelt. Das möchten wir weiterhin bleiben, und dafür werden wir weiterhin kämpfen.

Herr General, herzlichen Dank für das Gespräch.

Dr. Christian Marwitz, Chief Digital Officer während der diesjährigen AFCEA Fachausstellung im Gespräch mit Michael Horst, Chefredakteur des „Hardthöhenkurier".

Liefern, darauf kommt es jetzt an!

Interview mit Dr. Christian Marwitz,

Chief Digital Officer und Mitglied der Geschäftsführung der BWI GmbH

Friedrich Merz hat die Aussage getätigt, dass die Bundeswehr zur stärksten konventionellen Armee Europas werden soll. Da kommt also viel Arbeit auf die Bundeswehr und damit auch auf die BWI zu. Wie wollen Sie das stemmen?
Wir haben für die Bundeswehr bereits nach der Zeitenwende mehr Aufgaben übernommen, immer häufiger auch im Bereich der einsatznahen IT. In den letzten zwölf Monaten hat sich diese Entwicklung noch mal intensiviert. Wir verzeichnen ein deutliches Mehr an Beauftragungen, Tendenz weiter steigend. Eine Vielzahl an Themen, welche auf die Erhöhung der Verteidigungsfähigkeit einzahlen, können jetzt zum einen durch das Sondervermögen, aber auch durch die Erhöhung des Einzelplans 14 beauftragt werden.
Diese Beauftragungen führen zu einer deutlichen Steigerung des Umsatzes der BWI in den nächsten fünf Jahren. Die geopolitischen Rahmenbedingungen sorgen für zusätzlich steigende Anforderungen an die Qualität und vor allem die Liefergeschwindigkeit. Dazu kommen veränderte politische Rahmenbedingungen, auf die wir als IT-Systemhaus reagieren müssen, beispielsweise die Wiedereinführung der Wehrpflicht, die wir IT-seitig unterstützen. Es ist eine große Herausforderung, dieses deutliche Wachstum zu realisieren. Die BWI muss und wird alles tun, um die Bundeswehr bestmöglich bei der Erfüllung ihrer Aufgaben zu unterstützen. Liefern, darauf kommt es jetzt an!

Die BWI ist in den letzten Jahren bereits beträchtlich gewachsen und beschäftigt mittlerweile bereits über 8.000 Mitarbeitende. Wie wollen Sie das gerade erwähnte Mehr an Beauftragungen stemmen? Wird die BWI im bisherigen Tempo weiterwachsen, um die neuen Anforderungen der Bundeswehr zu erfüllen?
Dieses Wachstum war kein Selbstzweck, sondern erfolgte, um die wachsenden Aufgaben für die

Bundeswehr erfüllen zu können. Wir werden jedoch keinen Personalaufwuchs im gleichen Maße wie den Auftragszuwachs haben. Dies gibt der hart umkämpfte IT-Fachkräftemarkt schlicht nicht her, selbst wenn wir das wollten.
Aus dieser Situation heraus ergibt sich die Notwendigkeit, die Art unserer Leistungserbringung grundlegend zu verändern, um das kommende Mehr an Aufträgen bewältigen zu können. Unser klares Ziel ist es, die Leistungsfähigkeit der Organisation durch Effizienzsteigerung deutlich zu erhöhen. Das gilt auch für den gesamten Wirkverbund: Hier müssen wir gemeinsam überlegen, wie wir dieses Mehr an Aufträgen mit angemessenem Aufwand und in möglichst hoher Geschwindigkeit bewerkstelligen können.

Wie wollen Sie diese Effizienzsteigerung erreichen?
Dafür spielen zwei Themen eine zentrale Rolle: KI und Automatisierung. Mit dem geplanten verstärkten Einsatz von KI verfolgen wir das Ziel, die eigene Leistungsfähigkeit und Effizienz zu steigern. Mit Automatisierung streben wir eine sogenannte Zero-Touch-Operation an. Das bedeutet, dass der IT-Betrieb ohne händische Tätigkeiten auskommt. Das ist ein weiter Weg, den wir mit einem konsequenten Automation-Framework bereits begonnen haben. So benötigen wir weniger Menschen für betriebliche Aufgaben und können sie vor allem für die Bereitstellung von neuen IT-Lösungen und Projekten für die Bundeswehr einsetzen. Die BWI kann und wird die angesprochenen Leistungen nicht allein erbringen und wird deshalb an vielen Stellen ihre Rolle als Integrator noch weiter ausbauen.
Über all den genannten Maßnahmen steht das Ziel, die Bundeswehr bestmöglich dabei zu unterstützen die Sicherheit Deutschlands und Europas zu schützen.

Die BWI ist der primäre Digitalisierungspartner der Bundeswehr. Können Sie uns ein paar spannende Projekte nennen, an denen Sie bei der BWI gerade arbeiten?
Es gibt eine Vielzahl spannender Projekte. Drei Beispiele möchte ich davon nennen:
Zunächst das Krisenvorsorgeinformationssystem Bund (KVInfoSysBund): Das ist die erste von der BWI vollständig eigenständig entwickelte Softwarelösung, die auf der pCloudBw betrieben wird. Als ressortübergreifendes System zur Krisenvorsorge und -unterstützung trägt es wesentlich zur Sicherheit deutscher Staatsbürger im Ausland bei. Seit Ende April 2026 ist KVInfoySysBund ressortübergreifend im Einsatz für die Krisenvorsorge in Deutschland.
Dann das Health Information Management System (HIMS): Zentrale Voraussetzung für die Digitalisierung der Gesundheitsversorgung der Bundeswehr ist die Einführung eines Health Information Management System. Kernelement des HIMS ist eine zentrale Datenaustausch- und Integrationsplattform für eine durchgehende, medienbruchfreie sowie prozessorientierte Vernetzung der bundeswehreigenen Leistungserbringer der Gesundheitsversorgung. Da das HIMS auf Basis konsolidierter, validierter und selektierter Daten die Entscheidungsprozesse transparent, ebenen- und zeitgerecht unterstützt, dient es der bestmöglichen Digitalisierung der Gesundheitsversorgung der Bundeswehr und somit letztlich auch der Sicherstellung der Einsatz- und Dienstfähigkeit aller Soldatinnen und Soldaten. Wir haben HIMS auch auf der AFCEA Fachausstellung am Stand des BAAINBw präsentiert.
Drittens der Mission Enabling Service Bundeswehr (MESBw): Er ermöglicht die direkte Anbindung des BwMessengers an MESBw SitaWare HQ. Mit der MESBw-Lagemeldung kann jeder Nutzer ohne zusätzliche Tools oder Hardware mit der BwMessenger-App zu einem umfassenden Lagebild beitragen.

Durch die Phishing Kampagne gegen Nutzer des Messengerdienstes Signal ist aktuell das Thema Digitale Souveränität wieder in aller Munde. Wie stellt sich die BWI hier auf, um technologisch nicht in Abhängigkeiten zu geraten?
Das ist zunächst mal eine Definitionsfrage. Sicher ist, dass wir in der heutigen Zeit nicht technologisch autark agieren können. Die BWI muss sicherstellen, dass die Bundeswehr zu jeder Zeit die erforderlichen Kontroll-, Zugriffs- und Handlungsfähigkeiten im Cyber- und Informationsraum besitzt, um ihren verfassungsgemäßen Auftrag sicher, selbstbestimmt und frei von ungewollter Einflussnahme durch Dritte ausüben zu können. Die BWI muss Abhängigkeiten aktiv managen, eigenständig Entscheidungen treffen, zu einem hohen, akzeptierten Grad Kontrolle behalten und Risiken begegnen.

Können Sie dafür ein Beispiel nennen?
Die von uns eingesetzte Lösung „Google Distributed Cloud Air-Gapped“, die wir in den eigenen Rechenzentren physisch vollständig von anderen Google-Systemen oder Netzwerken isoliert (Red: air-gapped) installieren und betreiben, ist ein gutes Beispiel. Die Bundeswehr besitzt so zu jeder Zeit die Kontrolle über die eigenen Daten und kommt damit ihrer Anforderung nach Informations- und Datensicherheit nach. Durch unseren Multi-Cloud-Ansatz, also den Mix aus proprietären und offenen, Open Source-basierten Produkten, verringern wir einseitige Abhängigkeiten und können die Interoperabilität zu strategischen Partnern wie der NATO sicherstellen, zum anderen ermöglichen wir abhängig vom Anwendungsfall die sicherste und wirtschaftlichste Lösung einzusetzen.
Neben der Air-Gapped-Lösung mit Google-Technologie stellen wir in diesem Jahr auf der AFCEA Fachausstellung den Demonstrator für eine auf Open Source Software (OSS) basierende Cloud-Infrastruktur vor: die Open Defense Cloud (ODC). Wir bauen zunächst eine verlegefähige Lösung für die Bundeswehr. Die Vorarbeiten dafür haben bereits 2024 begonnen. Mit dieser können Soldatinnen und Soldaten zukünftig in Einsätzen auf Cloud-Dienste zugreifen. Der Demonstrator dieser Lösung wird bereits auf internationalen militärischen

Übungen erprobt und stetig weiterentwickelt. Später werden verlegefähige (Fog) und stationäre (Core) Infrastrukturen in den Rechenzentren der Bundeswehr folgen. Welche der technologischen Säulen in Zukunft bei der pCloudBw wann zum Einsatz kommen soll, haben Bundeswehr und BWI nun strategisch festgelegt. Langfristig konzentrieren sie sich beim Aufbau der Multi-Cloud-Plattform für Wehrverwaltung und Streitkräfte vermehrt auf Open-Source-Lösungen. Für den Aufbau setzen wir weiterhin auf die Zusammenarbeit mit Industriepartnern.

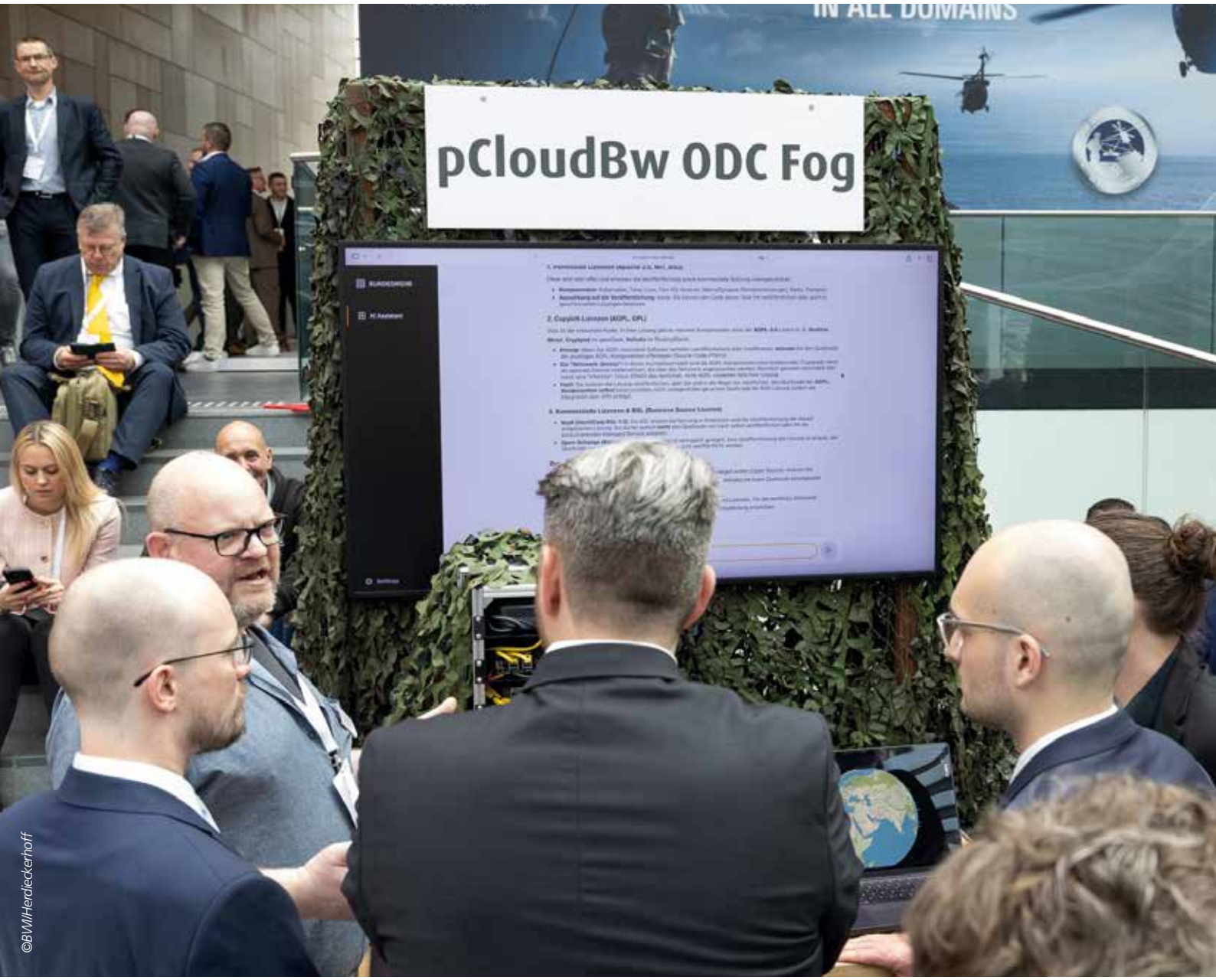
Man muss sich insgesamt aber klarmachen, dass es keinen Sinn macht, die zur Verfügung stehenden technischen Möglichkeiten, die beispielsweise die amerikanischen Hyperscaler bieten, nicht zu nutzen, nur um nach technischer Autarkie zu streben. Es gilt aber, parallel daran zu arbeiten, Alternativen zu entwickeln und Abhängigkeiten zu reduzieren.

Wie schätzen Sie das Interesse an der BWI auf der diesjährigen AFCEA ein?

So groß wie nie zuvor und weiter zunehmend. Den Trend beobachten wir schon die letzten Jahre. Das liegt natürlich auch an den eingangs erwähnten Haushaltsmitteln, es ist „viel Geld im System“. Es ist klar, dass an uns als diejenigen, die viel für die IT der Bundeswehr einkaufen, ein großes Interesse besteht. Das Interesse an der Zusammenarbeit ist groß und die Offenheit der Bundeswehr gegenüber unterschiedlichen Lösungsansätzen ebenfalls.

Wichtig ist: Wir sind weder Konkurrenten am Markt, wir nehmen als BWI niemandem etwas weg. Noch sind wir jemand, der sich ins System reindrängt. Als Inhouse-Gesellschaft sind wir für die Bundeswehr immer da. Das intensiviert die Zusammenarbeit, und das merkt man immer mehr.

Danke für das gute Gespräch und Ihre Zeit.



©BWI/Herclieckerhoff

Demonstrator der Open Defense Cloud auf der AFCEA Fachausstellung.

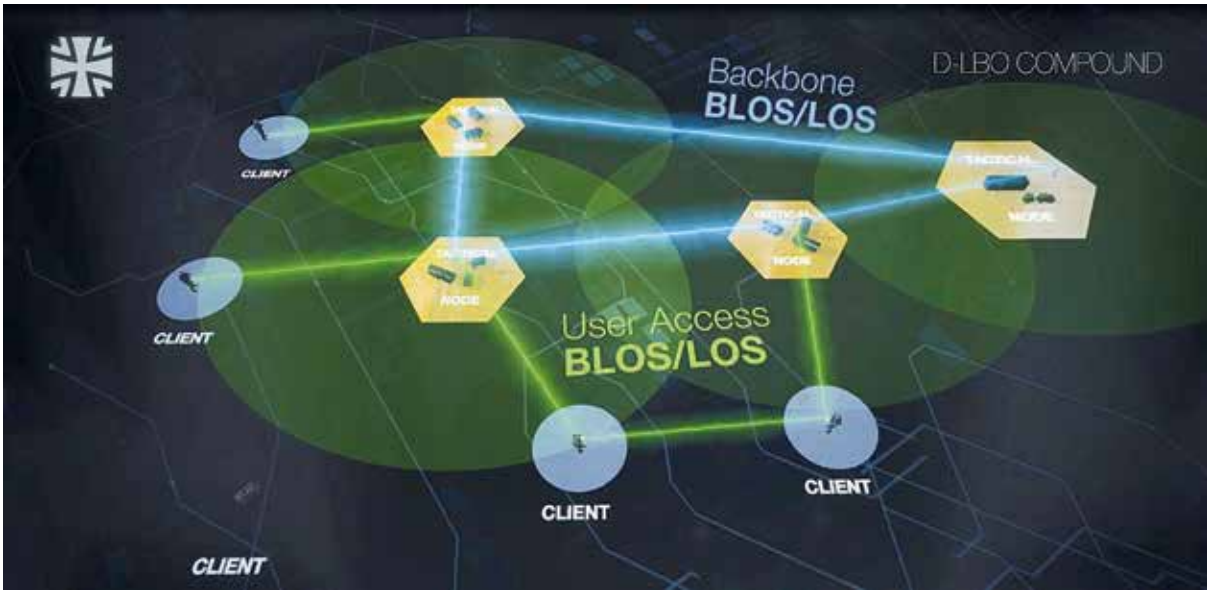
Realisierung D-LBO weiterhin im Mittelpunkt der IT-Beschaffungen

Milliardenschwere Verträge, aber konkrete Auswirkungen sind bisher kaum spürbar.

Von Gerhard Heiming

Mit der Bereichsausnahme im Bundeshaushalt und dem auslaufenden Sondervermögen Bundeswehr stellt die Finanzierung neuer Beschaffungs- und Dienstleistungsverträge für den Bereich Informationstechnik kein Hindernis mehr dar. Bei den Neuverträgen im vergangenen Jahr stand die Digitalisierung landbasierter Operationen (D-LBO) im Mittelpunkt.

D-LBO ist eines der wichtigsten Rüstungsprojekte der Bundeswehr. Soldaten, Fahrzeuge und Führungssysteme der Landstreitkräfte sollen umfassend digital vernetzt werden, um abhörsichere Kommunikation und ein gemeinsames Lagebild in Echtzeit zu gewährleisten. Dazu muss in Zehntausenden von Gefechts- und Unterstützungsfahrzeugen und Einrichtungen ein System aus moderner Hard- und Software installiert werden, um Daten und Sprache (Digitalfunk) zu übertragen.



©Amt für Heeresentwicklung

Informations- und Kommunikationsverbund D-LBO

Fortführung D-LBO

Mit zwei Verträgen in Höhe von zusammen 3,2 Milliarden Euro war Ende 2024 die Einrüstung von Funkgeräten und IT-Systemen in vorhandene Fahrzeuge der Truppe unter Vertrag genommen worden. Das Tactical Wide Area Network (TaWAN) wurde Anfang 2025 mit einem Rahmenvertrag im Wert von 5,5 Milliarden Euro gestartet. Obwohl die Projekte nicht recht von der Stelle kommen, soll die 10. Panzerdivision unter dem Stichwort „Division 2025“ bis Ende 2027 als erster Großverband vollständig digitalisiert werden.

Unterstützungsleistungen der BWI

Über einen Rahmenvertrag unterstützt die BWI die Rüstungsprojekte D-LBO, TaWAN und TEN, die deutsch-niederländische Kooperation Tactical Edge Networking. Der Vertrag wurde mit dem 13. Änderungsvertrag um 68 Millionen Euro aktualisiert und verlängert. Die technischen und logistischen Betreuungsleistungen durch die BWI laufen nahtlos weiter. Das Leistungsspektrum der BWI umfasst unter anderem die Unterstützung im Programm- und Projektmanagement D-LBO, die Durchführung des Releasebaus, Übernahme logistischer Tätigkeiten im Rollout, Unterstützung im IT-Betrieb sowie den Bau von Ausbildungsanlagen und die Durchführung der Ausbildung. Konkret sollen zum Beispiel Systemingenieure der BWI bei der Digitalisierung der Landstreitkräfte eingebunden werden. Darüber hinaus unterstützt die BWI weitere langfristige Projekte der Bundeswehr.

DND liefert Sender und Antennen für TaWAN D-LBO

Der Hauptauftragnehmer für TaWAN, Rheinmetall, hat mit DND Digital einen Vertrag zur Lieferung von Sendern und Antennen für das Taktische Wide Area Network abgeschlossen.

In den Systemanteilen TaWAN D-LBO Richtfunkmanagement groß, klein und tragbar werden jeweils die gleichen Sender und Antennen verwendet. Auf einem Antennenträger werden Antennen von Comrod, der Positioner von iMAR Navigation und der Sender/Empfänger BNet HCLOS (High Capacity Line of Sight) von DND Digital zusammengeführt. Für die Netzwerkkomponenten und das Netzwerkmanagement ist dainox vorgesehen.

Als ersten Teilauftrag hat DND Digital 2025 Trainings- und Referenzanlagen (eTuRA) für die Integration der Systeme in der Produktionsphase und später in der Truppe geliefert. Der Beginn der Serienlieferung ist für das erste Halbjahr 2026 terminiert. Um die kurzen Termine einhalten zu können, hat das Unternehmen seit Anfang 2025 einen weiteren Produktionsstandort für die TaWAN-Komponenten in Kiel Flintbek aufgebaut. Die Kapazität ist auf 30 Komponenten pro Monat ausgelegt, kann aber auf 120 Stück pro Monat gesteigert werden.

Zwei Richtfunkantennen von Comrod und ein Sender-/Empfänger von DND Digital sind auf einem Antennenträger zusammengeführt. Die Antennen werden von einem Positioner von iMAR Navigation in zwei Achsen positioniert.

©Gerhard Heiming

Gefechtsübungszentrum Heer wird D-LBO ready

Im Rahmen der Digitalisierung des Heeres müssen auch die Kommunikationssysteme des Gefechtsübungszentrums Heer in die Lage versetzt werden, mit den digital ausgerüsteten Gefechtsfahrzeugen zu kommunizieren. Die zentrale Ausbildungseinrichtung der Landstreitkräfte, in der vor allem die Kampftruppen in der höchsten Ausbildungsstufe trainiert und zertifiziert werden, erhält Führungs- und Kommunikationseinrichtungen nach dem Standard D-LBO.

Das BAAINBw hat Rheinmetall beauftragt, für knapp 61 Millionen Euro das Vorhaben D-LBO auch in das Gefechtsübungszentrum zu integrieren. Arbeitsbeginn war 2025. Die Integration soll bis Anfang 2028 abgeschlossen sein.

Nach Angabe von Rheinmetall wird im Rahmen des Vorhabens insbesondere der neue digitale Sprechfunk in das Gefechtsübungszentrum integriert. Zudem sollen alle Daten, die über das Battle Management System bereitgestellt werden, in der Übungsleitungszentrale des Gefechtsübungszentrums abgebildet werden können. Hierzu werde die vorhandene IT-Infrastruktur umfangreich erneuert und erweitert. Hierzu gehören die Anbindung der Software Tactical Core der Rheinmetall-Tochter Blackned und die Nutzung der in der Bundeswehr eingeführten Systeme SitaWare Frontline und HQ

©DSK, L3Harris

Funkgerät Falcon III AN/PRC-160(V) Wideband HF/VHF Manpack Radio von L3Harris.

Sprechsätze mit integriertem Gehörschutz

Die Bundeswehr erhält seit Mitte 2024 Sprechsätze mit Gehörschutzfunktion (SMG) aus einem Siebenjahresrahmenvertrag von Rheinmetall. Von der vereinbarten Gesamtmenge von 191.000 Stück sind die ersten 60.000 in zwei Losen abgerufen worden. Die Auslieferung wurde Ende 2025 abgeschlossen.

Im Dezember 2025 wurde mit erheblicher Verzögerung der dritte Abruf im Wert von 140 Millionen Euro vom Haushaltsausschuss gebilligt. Das entspricht etwa 60.000 Sprechsätzen, die derzeit ausgeliefert werden. Im Rahmenvertrag ist eine Obergrenze von 191.000 Sprechsätzen für rund 400 Millionen Euro vereinbart. Es bleibt also noch ein Rest von 81.000 Sprechsätzen und rund 114 Millionen Euro.

Nach Angabe von Rheinmetall umfasst der SMG einen modernen aktiven Kapselgehörschutz, welcher schädlichen Impulslärm dämpft und leise Geräusche verstärken kann. Weiterhin verfüge das System über ein Mikrofon und lasse sich an verschiedene Funkgeräte anschließen, sodass Sprechfunkverkehr möglich ist.

Funkgeräte für Spezialkräfte

Die Bundeswehr hat bei L3Harris Technologies eine große Anzahl an Funkgeräten mit einem Auftragswert von rund 190 Millionen Euro vor allem für D-LBO bestellt. Diese Aufträge umfassen die Lieferung von interoperablen Kommunikationssystemen zur Verbesserung der operativen Fähigkeiten der deutschen Streitkräfte, vor allem beim Heer, aber auch den anderen Teilstreitkräften. Funkgeräte von L3Harris waren bisher vor allem bei den deutschen Spezialkräften

in Nutzung und bei der Very High Readiness Joint Task Force (VJTF) 2023. Zunächst werden vor allem die Funkgerätmodelle Falcon III AN/PRC-117G(V)1(C) Multiband Networking Manpack Radio und AN/PRC-160(V) Wideband HF/VHF Manpack Radio geliefert.

Dezentrale Serversegmente Einsatz regeneriert
Im Dezember 2025 hat Hensoldt nach Abschluss der Regeneration die letzte Tranche der Dezentralen Serversegmente Einsatz (DSE) an die Bundeswehr übergeben. Einer Information von Hensoldt zufolge hat die Auslieferung der regenerierten DSE im September 2024 begonnen. Zur Lieferung gehören Transport- und Betriebsbehälter, inklusive der dazugehörenden Energieklimamodule und Segmentgrundausstattungen.
Nach der Beschreibung von Hensoldt sind die Serversegmente modulare, skalierbare und verlegefähige Einsatzsysteme. DSE sind für die Datenverarbeitung in beliebigen Client-Server-Infrastrukturen der Bundeswehr ausgelegt und können sowohl im Systemverbund als auch im Stand-alone-Betrieb (Offline) operieren.

SitaWare

Generallizenz SitaWare Edge für tragbare Geräte der Bundeswehr
Im September 2025 hat die Bundeswehr für die tragbaren Führungs- und Kommunikationsgeräte eine Generallizenz der Softwareapplikation SitaWare Edge des dänischen Softwareherstellers Systematics erworben. Diese wird im Rahmen der Digitalisierung der Streitkräfte auf Soldatenebene eingesetzt.
Im Mission Enabling Service Bundeswehr (MESBw), der IT-basierte Unterstützungs- und Betriebsleistungen für die Streitkräfte bereitstellt, ergänzt SitaWare Edge als Variante Portable die bereits vorhandenen Ausprägungen Command Post und Mountable.
Mit diesen Softwarevarianten lässt sich die digitale Operationsführung auf allen Ebenen durchgängig umsetzen vom stationären oder verlegefähigen Gefechtsstand über mobile Systeme in Fahrzeugen bis hin zu abgesessenen Kräften. SitaWare Edge nutzt dieselben Funktionen zur taktischen Datenkommunikation wie SitaWare Frontline. Mit durchgängiger Anwendung entsteht ein interoperabler und skalierbarer Kommunikationsverbund, der die IT-Systemanforderungen zur Landes- und Bündnisverteidigung erfüllt.
Zusammen mit der Generallizenz hat die Bundeswehr die zugehörigen Software Development Kits (SDKs) beschafft. Diese sind die Basis für ein offenes C4ISR-Ökosystem (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance) zum Sammeln, Verarbeiten und Verteilen von Informationen als Grundlage für Entscheidungen. Das Ökosystem kann durch die Bundeswehr selbst oder durch andere Unternehmen flexibel erweitert werden.

©Systematics

Die Führungsmittel der abgesessenen Kräfte werden mit SitaWare Edge ausgestattet.

SitaWare Battlefield Health für die Führung des Sanitätsdienstes

Mit Add-ons wird die eingeführte SitaWare Suite von Systematic nach den Anforderungen des Sanitätsdienstes der Bundeswehr erweitert. Unter dem Namen „SitaWare Battlefield Health" hat die Bundeswehr im September eine Generallizenz beim Hersteller in Auftrag gegeben. Die Softwarelösung findet Eingang in die Digitalisierung des Sanitätsdienstes. SitaWare Battlefield Health bietet der Bundeswehr eine digitale Lösung zur Verwundetensteuerung und notfallbezogenen Verwundetendokumentation, die das Tracking von Verwundeten sowie die Erstellung eines Lagebildes ermöglicht, schreibt Systematic in einer Mitteilung vom 31. Oktober.

In SitaWare Battlefield Health sind die bestehenden und bewährten EMR- und C4ISR-Lösungen (Elektronischer Kampf, Führung und Aufklärung) von Systematic kombiniert. Mit umfangreichem Fachwissen und langjähriger Erfahrung werden wichtige Entscheidungshilfen für den Gesundheits- und Verteidigungssektor geliefert.

Luftwaffe führt SitaWare ein

Im Februar 2026 hat die Luftwaffe ihre Entscheidung zur Nutzung von SitaWare bekannt gegeben. Die Nutzung wird im Rahmen der vorhandenen Generallizenz realisiert. Mit dieser Entscheidung der Luftwaffe wird SitaWare erstmals streitkräfteübergreifend bei Heer, Marine und Luftwaffe genutzt.

Die Einführung von SitaWare in der Luftwaffe ist Teil der Weiterentwicklung der interoperablen Führungsfähigkeit innerhalb der bestehenden Systemlandschaft der Bundeswehr. Ziel ist ein verbesserter, durchgängiger Informationsaustausch in einem gemeinsamen Lagebild über alle Dimensionen hinweg.

Marine

Link 22 für die „Sachsen"-Klasse

Im Juli 2025 hat das BAAINBw die Ausstattung aller drei Fregatten der Klasse F124 mit einem Ship-Shore-Ship Buffer on Ship (SSSB) ausgeschrieben. Diese externe Gateway-Lösung soll bis Mitte 2026 auf den Schiffen installiert werden und die Möglichkeit zur Nutzung

©Michael Nitz

Die „Sachsen"-Klasse wird mit Link 22 ausgerüstet für die taktische Datenanbindung in der NATO.

Fregatte „Hessen" und andere Schiffe in der Ostsee.

des modernen NATO-Datenlink Link 22 sowie das Joint Range Extension Applications Protocol C (JREAP-C) eröffnen. Die taktische Datenanbindung soll ohne tiefgreifende Eingriffe in das komplexe Führungs- und Waffeneinsatzsystem (FüWES) der „Sachsen"-Klasse auf den Stand der Allianz gebracht werden.
Bei Link 22 handelt es sich um ein taktisches Datenlinknetzwerk der NATO, das Kommunikation im HF- und UHF-Bereich erlaubt, auch bei störungsbehaftetem Umfeld oder über die Line of Sight hinaus. Damit eignet es sich für maritime Operationen in großer Raumaufteilung oder bei Kommunikationsbeeinträchtigung. Die Reichweite von Link 22 im HF-Bereich kann mehr als 1.000 Seemeilen betragen.

Standardisierung maritimes FüWES mit Kanada
Die seegehenden Plattformen der Deutschen Marine erhalten als einheitliches Führungs- und Waffeneinsatzsystem (FüWES), das Combat Management System CMS 330 von Lockheed Martin Canada. Für erste Maßnahmen hat der Haushaltsausschuss des Deutschen Bundestages am 5. November 2025 162 Millionen Euro bereitgestellt.
Die Integration des FüWES in Plattformen der Deutschen Marine erfolgt durch Hensoldt.
Das Projekt ist auf eine Laufzeit von 25 Jahren angelegt und mit einem Volumen von über einer Milliarde Euro geplant.
In der Initialisierungsphase, die unmittelbar nach Vertragsabschluss begonnen hat, sollen wesentliche fachliche und technische Grundlagen für die spätere Integration auf den Plattformen geschaffen werden. Darauf aufbauend werden zeitnah landgestützte Test-, Referenz- und Schulungsanlagen errichtet.
Ab dem Jahr 2027 sind die ersten Maßnahmen zur Einrüstung auf ausgewählten Schiffen und Booten vorgesehen. Langfristig sollen alle bestehenden und künftigen maritimen Überwasserfähigkeitsträger einschließlich der neuen Fregattenklasse F127 mit dem standardisierten Führungs- und Waffeneinsatzsystem ausgerüstet werden.

Cloud-Computing

IT-Unterstützung für Litauen-Brigade und Cloud-Computing
Mitte 2025 wurde der 13. Änderungsvertrag des Leistungsvertrags mit der BWI im HERKULES-Folgeprojekt mit einem Volumen von 1,5 Milliarden Euro unterzeichnet. Der Vertrag regelt die Weiterentwicklung und den Betrieb der Informations- und Kommunikationstechnik für die Bundeswehr.
Wesentliche Änderungen sind die IT-Unterstützung für die Stationierung der Brigade in Litauen, die Erweiterung des zu Jahresbeginn in Betrieb gegangenen Cloud-Computing und die bereits erwähnte Erweiterung für D-LBO. Nach Einschätzung des BMVg tragen die Fortführung und Weiterentwicklungen sowie die neuen Leistungen der IT-Services der BWI zur Resilienzsteigerung und zukunftsfähigen Digitalisierung der Bundeswehr bei.

Private Cloud der Bundeswehr erhält Google-Anteil
Für das Cloud-Computing ging ab 6. Januar die private Cloud der Bundeswehr (pCloudBw) in Betrieb. Bis Ende 2027 erhält die pCloudBw zwei neue Instanzen. Die BWI beschafft von der Google Cloud Public Sector – Deutschland GmbH die Lösung Google Cloud Air-Gapped. Bis Ende 2027 wird die BWI nach eigener Angabe damit eine weitere Cloud-Umgebung in den eigenen Rechenzentren aufbauen und als Teil der pCloudBw betreiben. Mit der Google Cloud Air-Gapped sollen zwei physikalisch getrennte Cloud-Instanzen aufgebaut werden: für die Verarbeitung offener sowie geschützter Daten.
Die BWI will die Lösung des Herstellers Google Cloud in den bundeswehreigenen Rechenzentren physisch vollständig von anderen Google-Systemen oder Netzwerken isoliert (air-gapped) installieren und betreiben. Die Bundeswehr besitze so zu jeder Zeit die Kontrolle über die eigenen Daten und komme damit ihrer Anforderung nach Informations- und Datensicherheit nach, schreibt die BWI.

Satellitenkommunikation

UniBw M erhält Q/V-Band-Satellitenbodenstation von SatService
Das terrestrische Labor der Universität der Bundeswehr München (UniBw M) wird mit einer Q/V-Band-Satellitenbodenstation von SatService, einer Tochtergesell-

©OHB Digital

Die neue UHF-Kontrollstation ist Teil des Programms SATCOMBw.

SatService

Das Vier-Meter-Hochleistungsantennensystem der Satellitenbodenstation.

schaft der kanadischen Calian Group, ausgestattet. Einer Unternehmenmitteilung vom 10. Februar zufolge hat der Auftrag einen Wert von mehr als circa 2,5 Millionen Euro. SatService werde dabei eine fortschrittliche Full-Service-Bodenstation für Satelliten im Q/V-Band-Bereich zur Unterstützung von Satellitenkommunikation (SATCOM) für wissenschaftliche und moderne militärische Zwecke bereitstellen.

Die Vereinbarung sieht vor, dass SatService die Satellitenbodenstation, einschließlich eines Vier-Meter-Hochleistungsantennensystems entwirft herstellt, testet und liefert. Nach Fertigstellung wird die Satellitenbodenstation im Q/V-Band für Anwendungen im geostationären Orbit (GEO) betrieben. Diese Möglichkeit stehe der Universität aktuell noch nicht zu Verfügung, so SatService.

©Lockheed Martin

Mensch-Maschine-Schnittstelle für CMS 3330.

Die Satellitenbodenstation soll im terrestrischen Labor der Universität die Kommunikation zwischen GEO-Satelliten und Bodeneinrichtungen für wissenschaftliche Anwendungen unterstützen. Für die Offiziersausbildung steht eine Satellitenkonnektivität mit hohem Durchsatz zur Verfügung, mit der die zahlreichen operativen Vorteile von SATCOM erfahren und erprobt werden können.

UHF-Kontrollstation für die Satellitenkommunikation

Die Bundeswehr hat seit November 2025 eine neue Schaltzentrale für ihre satellitengestützte Kommunikation: OHB Digital Connect hat die moderne UHF-DAMA-Kontrollstation an das BAAINBw sowie das Kommando IT-Services der Bundeswehr übergeben.

Die neue Kontrollstation ersetzt eine ältere Anlage und bietet leistungsfähigere Technik für die sichere Satellitenkommunikation der Streitkräfte. Herzstück ist das UHF-DAMA-System (Demand Assigned Multiple Access), das die dynamische Zuteilung von Sende- und Empfangskanälen ermöglicht. So kann die verfügbare Bandbreite optimal genutzt werden, selbst in abgelegenen Einsatzgebieten.

Bereits 2019 hatte OHB Digital Connect eine ähnliche Station erfolgreich fertiggestellt.

Die neue Kontrollstation ist Teil des Programms SATCOMBw, dem satellitengestützten Kommunikationssystem der Bundeswehr. Es ermöglicht sichere Verbindungen zwischen Truppen, Führungsstellen und Einsatzkontingenten weltweit. Eine Schlüsselressource für moderne militärische Kommunikation.

Weiterentwicklung ESSOR

Die europäische Beschaffungsagentur OCCAR hat im November 2025 mit dem multinationalen Joint Venture a4ESSOR S.A.S (Alliance for ESSOR, European Secure Software-Defined Radio) einen weiteren Vertrag zur Entwicklung interoperabler taktischer Kommunikationssysteme abgeschlossen. Dieser Vertrag ermöglicht nicht nur die Zusammenführung der Funknetzplanungsfähigkeiten zur Konfiguration und zum Betrieb der ESSOR-Wellenformen, sondern auch die Sicherheitsqualifizierung der nationalen Implementierungen, um multinationalen Funknetzen den Austausch von Informationen bis zur Geheimhaltungsstufe NATO RESTRICTED zu ermöglichen.

In dem Joint Venture arbeiten die Branchenführer der sechs beteiligten Länder (Deutschland – Rohde & Schwarz, Finnland – Bittium, Frankreich – Thales, Italien – Leonardo, Polen – Radmor, Spanien – Indra) zusammen, um neue Funktionen wie elektronische Schutzmaßnahmen und die Unterstützung moderner kryptografischer Standards hinzuzufügen.

Im Rahmen des neuen mit 47 Millionen Euro dotierten Vertrags wird a4ESSOR ein gemeinsames Missionsframework entwerfen, das auf die gemeinsame Planungsfähigkeit der Netzwerkparameter der ESSOR-Wellenform mit hoher Datenrate (ESSOR High Data Rate waveform, EHDRWF) abzielt, schreibt Rohde & Schwarz.

Nach Angabe der OCCAR ist 2028 eine ganzheitliche Demonstration unter Verwendung der ESSOR-Hoch-

geschwindigkeitswellenform (STANAG 5651) in Verbindung mit nutzerorientierten Diensten geplant, die in Frankreich durchgeführt werden soll.
Die Bundeswehr will die ESSOR-Wellenformen auf den Software-Defined Radios implementieren, die Rohde & Schwarz derzeit für die Ausstattung im Rahmen der Digitalisierung landbasierter Operationen liefert.

Ausblick
Nur gut zwei Milliarden Euro wurden in den letzten zwölf Monaten in neuen Verträgen gebunden. Aus dem Jahr davor laufen mehrere milliardenschwere Verträge vor allem für D-LBO und TaWAN. Konkrete Auswirkungen sind bisher kaum spürbar. Das zeigt, mit den Verträgen ist es nicht getan. Die Industrie muss liefern und die Bundeswehr muss abnehmen. Letzteres bedeutet schnelle, aber nicht weniger gründliche Prüfungen und Freigaben, damit die Truppe das Material nutzen kann. Zwei Termine drücken: Die Division 2025 (!), die jetzt bis 2027 vollständig digitalisiert werden muss, und 2029, das Jahr, ab dem Russland zum offenen Angriff auf NATO-Gebiet fähig sein könnte. Bis dahin muss die Verteidigungsfähigkeit Deutschlands sicher auf eine ausreichend und gut ausgerüstete Bundeswehr setzen können.

Das Bechtle Team und die Herstellerpartner auf der AFCEA Fachausstellung 2026

bechtle

Kontakt:
Bechtle AG
E-Mail: defence@bechtle.com
Telefon: 0228 6888 400
www.bechtle.com

Bechtle ist mit über 16.500 Mitarbeitenden und mehr als 120 Standorten in 14 europäischen Ländern immer in der Nähe seiner Kunden und einer der führenden IT-Dienstleister in Europa. Die Kombination aus Direktvertrieb von IT-Produkten mit umfassenden Services macht Bechtle zu einem starken IT-Zukunftspartner für den Mittelstand, Konzerne und den Public Sector. Das herstellerübergreifende Produkt- und Leistungsportfolio reicht von klassischen IT-Infrastrukturen über Digitalisierung, Multi Cloud, Modern Workplace und Security bis hin zu künstlicher Intelligenz und Managed Services. Seit mehr als 15 Jahren ist Bechtle zuverlässiger Rahmenvertragspartner diverser Rahmenverträge des BAAINBw, so auch seit 2009 durchgehend für die 2./3. Rechnerebene.

Bechtle auf der AFCEA Fachausstellung 2026.
Gemeinsam mit den Herstellerpartnern Dell Technologies, Ubiqconn Technology, Cloudera, NVIDIA und VMware by Broadcom präsentierte Bechtle vor Ort sein umfassendes Portfolio rund um Rechenzentrumsinfrastruktur, Speichersysteme, Netzwerk- und Funktechnik sowie Künstliche Intelligenz zur Verwaltung von Dokumenten- und Vorschriftenlagen. Im Mittelpunkt standen dabei aktuelle Herausforderungen der Digitalisierung sowie praxisnahe Lösungsansätze für moderne und sichere IT-Infrastrukturen im Public Sector.

MITTLER REPORT

Wehrtechnischer Report: **IT-Report 2026**

Themen-Highlights im Heft:

- **Fortschreitende Digitalisierung in sämtlichen Bereichen der Teilstreitkräfte**
- **Ansatz der Software Defined Defence**
- **Einsatz von Künstlicher Intelligenz in allen Domänen**
- **Multi Domain Operations**
- **Simulationstechnologien**
- **Cloud-Lösungen**
- **Der Elektromagnetische Kampf**

Jetzt QR-Code scannen und kostenlos den IT-Report 2026 downloaden!

mittler-report.de/WTR-ITReport26

dtec.bw –
Sechs Jahre Innovationskraft für Digitale Souveränität und Verteidigungsfähigkeit

Von Dr. Annika-Kathrin Belz, Referentin für Wissens- und Technologietransfer UniBw M

„Der Aufbau des dtec.bw war ohne Zweifel eine Herausforderung, bei der beide Universitäten der Bundeswehr gezeigt haben, was sie einzeln und vor allem gemeinsam imstande sind zu leisten." Dieses Resümee beschreibt präzise, was seit 2020 mit dem Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr (dtec.bw) entstanden ist: ein wissenschaftliches Leuchtturmprojekt, getragen von der Universität der Bundeswehr München (UniBw M) und der Helmut-Schmidt-Universität/Universität der Bundeswehr Hamburg (HSU/UniBw H), mit klarem Fokus auf Digitale Souveränität, technologische Resilienz und sicherheitsrelevante Innovationen.

©UniBw M/Wagener

Dr. Annika-Kathrin Belz

Gegründet im Rahmen des Konjunkturpakets zur Bewältigung der COVID-19-Krise und finanziert aus dem Deutschen Aufbau- und Resilienzplan der Europäischen Union mit insgesamt 700 Millionen Euro bis Ende 2026, verfolgt dtec.bw das Ziel, die Forschung an den Universitäten der Bundeswehr in Schlüssel- und Zukunftstechnologien strategisch zu bündeln. Bereits der Aufbau in kürzester Zeit stellte beide Universitäten vor enorme strukturelle Herausforderungen: Auswahl und Initiierung von Projekten, Gewinnung exzellenter Wissenschaftlerinnen und Wissenschaftler, Beschaffung moderner Forschungsinfrastruktur inmitten der Corona-Krise. Heute steht fest: Dieser Kraftakt hat sich gelohnt.

66 Forschungsprojekte mit mehr als 400 wissenschaftlichen Mitarbeitenden haben seitdem eindrucksvolle Ergebnisse erzielt: mehr als 4.000 Veröffentlichungen, rund 200 vertraglich etablierte Partnerschaften mit Akteuren aus Bundeswehr, Wissenschaft und Industrie, über 500 entwickelte Technologien, 20 Patentanmeldungen und mehrere erfolgreiche Start-ups. Hinzu kommen über 60 abgeschlossene Promotionen, ein starkes Signal für die Förderung des wissenschaftlichen Nachwuchses (Stichtag Zahlen 31. Dezember 2025). dtec.bw hat damit nicht nur technologische Innovationen hervorgebracht, sondern auch eine neue Generation von Expertinnen und Experten für sicherheitsrelevante Digitalisierung qualifiziert.

In der heutigen sicherheitspolitischen Lage zeigt sich, wie vorausschauend die thematische Ausrichtung des dtec.bw bereits mit seiner Gründung war: Künstliche Intelligenz, Cybersicherheit, quantensichere Kommunikation, autonome Systeme, Weltraumtechnologien oder die Resilienz kritischer Infrastrukturen sind zu zentralen Handlungsfeldern nationaler Sicherheitsvorsorge geworden. Bemerkenswert ist, dass sämtliche Projekte bereits 2020 und damit vor dem russischen Angriffskrieg gegen die Ukraine initiiert wurden. Die Evaluierung durch den Wissenschaftsrat bestätigte 2022 die hohe wissenschaftliche Qualität ausgewählter Projekte sowie die strategische Relevanz der Maßnahme.

Die Jahre 2025 und 2026 markieren eine Phase sichtbarer Reife und verstärktem Transfer. Auf der dtec.bw Jahrestagung 2025 an der HSU/UniBw H wurde die gesamte Bandbreite der Forschung in den Dimensionen Cyber, Weltraum, Luft, See, Land und Mensch präsentiert. Projekte wie SeRANIS im Bereich weltraumge-

©UniBw M/Wagener

Flugsimulator im dtec.bw Projekt MissionLab.

©UniBw M/Siebold

Präsidentin Prof. Eva-Maria Kern präsentiert Verteidigungsminister Boris Pistorius die dtec.bw-finanzierte Kleinsatellitenmission SeRANIS.

stützter Signalaufklärung oder GhostPlay mit KI-gestützter Simulation taktischer Entscheidungsprozesse verdeutlichten, wie eng Grundlagenforschung und operative Anwendung zusammengedacht werden. Die begleitende Fachausstellung sowie das ScienceForum stärkten den Dialog zwischen Forschenden, Bundeswehrdienststellen und Industriepartnern.

Auf dem Defence Innovation Pitch Day 2025 in München wurde das innovative Transferformat gemeinsam mit dem Behörden Spiegel sowie den Innovationselementen der UniBw M – dtec.bw, founders@unibw und dem Palladion Defence Accelerator bespielt. Ein herausragendes Beispiel für erfolgreichen Technologietransfer ist das Spin-off Orbint, hervorgegangen aus dem dtec.bw-Projekt SeRANIS. Durch die Beteiligung von Rohde & Schwarz wird satellitengestützte Signalaufklärung „Made in Germany" gezielt weiterentwickelt, ein konkreter Beitrag zur europäischen technologischen Souveränität. In diesem Jahr war dtec.bw bereits das vierte Mal auf der AFCEA als Aussteller ver-

©UniBw M/Petzold

Gemeinsames Grußwort der Präsidenten der beiden UniBw auf der dtec.bw Jahrestagung 2025.

©UniBw M/Petzold

Einführung in die dtec.bw Jahrestagung durch die beiden Vizepräsidenten Forschung beider UniBw.

treten und stellte unter anderem das dtec.bw Projekt SeRANIS und Orbint am Stand vor und die Ausgründung Scalable Propulsion.

Bereits zu Beginn des Jahres 2026 setzte dtec.bw starke Impulse im Innovationsökosystem der Bundeswehr. Beim Palladion-Event „SPARK 26“ im Umfeld der Munich Security Conference war dtec.bw vertreten. Auf der Enforce Tac in Nürnberg präsentierten Projekte wie SPARTA zur Analyse von Desinformation, MuQuaNet zur quantensicheren Kommunikation oder LogSimSanDstBw zur simulationsgestützten Optimierung militärischer Logistik ihre Fortschritte. Die enge Verzahnung von universitärer Forschung, industrieller Umsetzung und militärischer Bedarfsträgerseite wurde dabei als Erfolgsmodell sichtbar. Vom 15. bis 16. September 2026 findet mit der dtec.bw Jahrestagung 2026 bereits die dritte große Tagung des dtec.bw statt und markiert damit auch den feierlichen Abschluss des aktuellen Finanzierungszeitraums 2020 bis 2026.

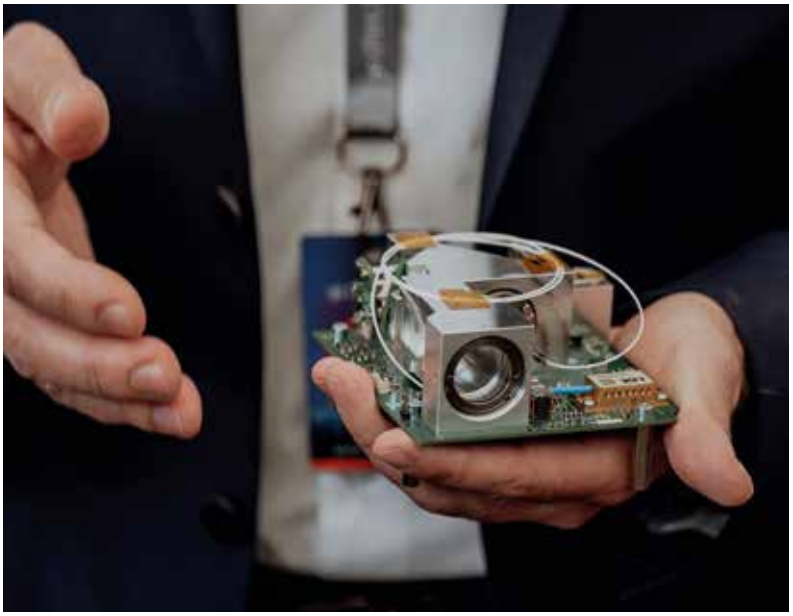
dtec.bw steht damit exemplarisch für eine neue Qualität der Kooperation zwischen ziviler und militärischer Forschung. Freie wissenschaftliche Arbeit liefert Impulse, die gezielt in verteidigungsrelevante Innovation überführt werden. Gleichzeitig bieten die besonderen Rahmenbedingungen der Universitäten der Bundeswehr inklusive militärischer Sicherheitsbereiche ein Umfeld, das auch eingestufte Forschung ermöglicht.

Mit Blick auf die Zeit ab 2027 richtet sich der Fokus auf die Verstetigung als „dtec.bw 2.0“. Der Wissenschaftsrat empfiehlt ausdrücklich, die Finanzierung der sicherheits- und verteidigungsrelevanten Digitalisierungsforschung fortzuführen, künftig noch stringenter am Bedarf der Bundeswehr ausgerichtet. Geplant ist eine klare Fokussierung auf universitäre Dual-Use-Forschung im Bereich Cyber/IT und diesbezüglicher Schlüsseltechnologien. Zukünftige Forschungsprojekte müssen gemeinsam mit mindestens einer Bundeswehrdienststelle durchgeführt und durch Industriepartner ergänzt werden, um eine schnelle Überführung in die Anwendung zu ermöglichen.

Ziel ist es, dtec.bw ab 2027 weiterzuführen als dauerhaftes wissenschaftliches Zentrum für sicherheits- und verteidigungsrelevante Digitalisierungsforschung. In einer Zeit geopolitischer Umbrüche gilt mehr denn je: Forschung ist kein Selbstzweck, sondern strategische Notwendigkeit. dtec.bw hat in den vergangenen Jahren bewiesen, dass die Universitäten der Bundeswehr mehr sind als Bildungseinrichtungen, sie sind Innovationstreiber, strategische Ressource und ein zentraler Baustein für eine resiliente, souveräne und einsatzbereite Bundeswehr.

©UniBw MWagener

Fahrsimulator im dtec.bw Projekt MORE.



©UniBw MWagener

Technikpräsentation im Rahmen der dtec.bw Jahrestagung.

©dtec.bw/Panzau

Digitale Ersthelferausbildung im dtec.bw Projekt Smart Health Lab.

Das Zentrum Digitalisierung der Bundeswehr und Fähigkeitsentwicklung Cyber- und Informationsraum

Strategische Steuerung, technologische Umsetzung und operative Nähe

Von Autorenteam Zentrum Digitalisierung der Bundeswehr

Stellen Sie sich vor, Sie müssten ein Unternehmen mit über 260.000 Mitarbeitern digitalisieren, während es sich weltweit im Einsatz befindet und gleichzeitig gegen Hackerangriffe verteidigen muss. Eine unmögliche Mission? Für das Zentrum Digitalisierung der Bundeswehr und Fähigkeitsentwicklung Cyber- und Informationsraum (ZDigBw) ist genau das der Auftrag.

Der Auftrag

Das ZDigBw mit dem Hauptsitz in Bonn sowie sechs weiteren deutschlandweit verteilten Standorten wurde 2022 aufgestellt und untersteht dem Kommando Cyber- und Informationsraum (KdoCIR).

Es koordiniert die zentralen Digitalisierungsvorhaben der Streitkräfte und sorgt dafür, dass aus militärischen Anforderungen konkrete digitale Fähigkeiten entstehen, die im Einsatz genutzt werden. Gleichzeitig verbindet das Zentrum in der Rolle als zentraler Bedarfsträger für Informationstechnik, vergleichbar mit dem Planungsamt für die Nicht-IT-Projekte, die militärischen Organisationsbereiche, die Teilstreitkräfte, den Bedarfsdecker Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAAINBw) sowie nationale und internationale Partner miteinander.

Darüber hinaus verantwortet das ZDigBw die Fähigkeitsentwicklung der Teilstreitkraft CIR in den Bereichen Militärisches Nachrichtenwesen, Elektronische Kampfführung sowie in der Operativen Kommunikation. Hier werden Innovation, Konzeption, Planung, Entwicklung und Integration sowie Nutzung zusammengeführt.

Das Zentrum stellt außerdem eigene Fähigkeiten zur Softwareentwicklung und für Integrationsleistungen von IT-Services in das IT-System der Bundeswehr bereit.

Gliederung

Die Struktur folgt diesem umfangreichen Auftrag. Hierzu nimmt die Dienststelle zum 1. Oktober 2026 eine an diesen Auftrag angepasste Struktur ein. Die Abteilungen greifen dabei wie Zahnräder ineinander und verbinden strategisches Denken mit operativer und taktischer Umsetzung.

Die Abteilung I verantwortet den Grundbetrieb des Zentrums. Sie bildet das organisatorische Rückgrat der Dienststelle. Sie stellt Führung und Steuerung über die Themen der Führungsgrundgebiete sicher.

Die Abteilung II ist der Taktgeber der Digitalisierung. In der Abteilung schlägt das konzeptionelle Herz der Dimension CIR und darüber hinaus steuert sie die Aufgaben als zentraler Bedarfsträger des Teilportfolios Cyber- und Informationstechnik (CIT) für die gesamte Bundeswehr. Hier werden nicht nur Zielbilder entwickelt und Fähigkeiten der Teilstreitkraft CIR geschärft, sondern die Digitalisierung der Bundeswehr aktiv gesteuert. Indem die Abteilung militärische Anforderungen in präzise planerische Vorgaben übersetzt, schafft sie das Fundament für die Wirksamkeit von morgen.

In der Praxis fungiert die Abteilung II als strategischer Taktgeber, der die komplexen digitalen Anforderungen aller militärischen Organisationsbereiche bündelt und mit der Expertise aus den Bereichen Anforderungsmanagement, Finanzplanung und IT-Bebauungsplanung in die Digitalisierungsplattform überführt. Durch moderne Architekturmethoden wird dabei sichergestellt, dass sich neue Lösungen nahtlos in die bestehende Systemlandschaft integrieren lassen. Zusätzlich nimmt die Abteilung die Rolle des Chief Information Officer wahr, wodurch die enge Verzahnung zwischen Informationstechnik und den klassischen Rüstungsprojekten sichergestellt wird. Dabei blickt das Team weit über den Tellerrand hinaus und vernetzt die Bundeswehr eng mit dem zivilen Innovationsökosystem, etwa durch die Kooperation mit dem Cyber Innovation Hub in Berlin, der Cyberagentur in Halle, das Forschungsinstitut CODE an der Universität der Bundeswehr in München und das neu gegründete Innovationszentrum in Erding. So wird sichergestellt, dass modernste Technologien aus der Start-up-Welt ihren Weg in die Truppe finden.

Ein besonderer Schwerpunkt liegt auf der Zukunftsfä-

higkeit im Cyber- und Informationsraum. Die Abteilung konzipiert und entwickelt die Fähigkeiten für Cyberoperationen, das Militärische Nachrichtenwesen, den Elektronischen Kampf, die Aufklärung sowie die Operativen Kommunikation. Dabei geht es nicht nur um deutsche Entwicklungen: Durch die aktive Mitgestaltung von NATO-Standards stellt die Abteilung sicher, dass unsere Systeme auf dem digitalen Gefechtsfeld nahtlos konzeptionell und technisch interoperabel mit denen unserer Partner sind.

Von der Sensortechnik in der Aufklärung bis hin zur hochkomplexen Sensor-to-Shooter-Kette begleitet die Abteilung II Rüstungsprojekte über ihren gesamten Lebenszyklus. Sie ist das Sprachrohr der Soldaten gegenüber der Beschaffungsseite und garantiert, dass die Technik im Einsatz genau das leistet, was die Truppe für ihre Auftragserfüllung benötigt. Kurzum: Hier wird das digitale Rückgrat geschmiedet, das die Bundeswehr im 21. Jahrhundert handlungsfähig hält.

Wie diese konzeptionelle Vorarbeit konkret Gestalt annimmt, zeigt sich an der Thematik hybride Kriegsführung und dem Projekt „Digitalisierung Operative Kommunikation“: Im 21. Jahrhundert ist Information selbst zum Gefechtsfeld geworden. Desinformation gehört zu den wirkungsvollsten Instrumenten moderner Konflikte. Mit gezielten Falschmeldungen, manipulierten Bildern oder KI-generierten Videos versuchen Gegner, Gesellschaften zu destabilisieren und Vertrauen in staatliche Institutionen zu untergraben. Genau hier setzt die Operative Kommunikation der Bundeswehr an: Sie soll falsche Narrative entlarven und eigene, faktenbasierte Informationen schnell und wirksam verbreiten.

Ein mögliches Szenario: Ein Dorf wird überfallen, Menschen werden aus ihren Häusern gezerrt und verschleppt. Doch der Angreifer weiß nicht, dass sein Vorgehen dokumentiert wird. Kameras halten das Geschehen fest, Tonaufnahmen sichern Details. Minuten später werden die Aufnahmen veröffentlicht. Nicht als Propaganda, sondern als Beleg für das tatsächliche Geschehen im Einsatzraum. Möglich macht das ein Rüstungsprojekt mit dem Namen „Digitalisierung Operative Kommunikation“. Herzstück ist unter anderem ein mobiles, voll ausgestattetes audiovisuelles Rundfunkstudio in Containerbauweise. Dort lassen sich Videos schneiden, Live-Sendungen produzieren, Podcasts aufzeichnen oder Social-Media-Beiträge erstellen. Das Material kann unmittelbar veröffentlicht oder internationalen Medien zur Verfügung gestellt werden.

Der Bedarf für diese Fähigkeiten ist offensichtlich: „Die Art und Weise, wie Menschen nicht nur in der westlichen Welt miteinander kommunizieren und sich informieren, hat sich seit dem Siegeszug des Internets und der mobilen Endgeräte hinsichtlich der Anzahl und der Tiefe in erheblichem Umfang verändert. Telefon, Zeitung, Fernsehapparat und Kneipentisch sind heute immer und jederzeit mit dabei“, erklärt Oberstleutnant Andreas B., Leiter im Dezernat Fähigkeitsentwicklung Operative Kommunikation und Digital Humanities. Gleichzeitig basierten viele Systeme der Operativen Kommunikation in früheren Auslandseinsätzen, etwa in Afghanistan, Mali oder auf dem Balkan, noch auf technischen Standards des 20. Jahrhunderts. Daher ist das klare Ziel der Digitalisierung OpKom: Schneller reagieren, mehr Menschen erreichen und die Deutungshoheit über Ereignisse behalten. Denn: „In einem medial nahezu vollständig erfassten Einsatzgebiet wird erfolgreiche Kommunikation, künftig vielleicht sogar mehr als je zuvor, zu einem entscheidenden Erfolgsfaktor werden“, so Oberstleutnant Andreas B.

Die Modernisierung umfasst daher mehr als nur neue Technik. Neben einem modularen Produktionssystem entsteht auch eine moderne Analyseumgebung für offene Quellen im Internet. Damit können Zielgruppen, Kommunikationsmuster und kulturelle Codes präziser ausgewertet werden. Eine Voraussetzung, um Botschaften in Fremdsprachen sowie mit regional verständlichen Symboliken und Narrativen zu platzieren.

©ZDigBw

Soldatinnen und Soldaten eines Audioteams im Einsatz schicken aus mobilen Studiokabinen die von ihnen produzierten Podcasts und Radiosendungen raus in den Äther.

Die Abteilung III ist Macher der Digitalisierung, sie ist das planerische Schwergewicht der Digitalisierungsplattform. Nach den Vorgaben der Abteilung II verantwortet sie insgesamt über 600 Projekte in neun sogenannten Clustern und die dazu gehörigen Clusterprogramme, erarbeitet Bedarfs- und Haushaltsunterlagen und ist in der Rolle des Bedarfsträgers für das Teilportfolio CIT in komplexen Projektstrukturen verantwortlich. Hier wird Planung konkret und steuerbar. Darüber hinaus entwickelt die Abteilung III die konzeptionellen Grundlagen für die Digitalisierungsvorhaben, definiert Zielbilder und stellt deren einheitliche Umsetzung über alle Projekte hinweg sicher. Sie schafft damit den inhaltlichen Rahmen für eine abgestimmte Ausrichtung und langfristig tragfähige Lösungen.

©ZDigBw

Fahrzeugintegriertes Funkgerät VR5500 als Teil des Systems D-LBO, eingebaut in einen ausgestatteten Kommunikationsarbeitsplatz für mobile Einsätze.

Ein Kernprojekt der Abteilung ist die Digitalisierung landbasierte Operationen (D-LBO). Ziel dieses Programms ist es, die Landstreitkräfte digital zu vernetzen und damit Führung, Informationsaustausch und Einsatzkoordination grundlegend zu verbessern. Statt überwiegend analoger Verfahren, wie Funkmeldungen oder papierbasierte Kartenarbeit, sollen digitale Systeme ein nahezu verzögerungsfreies Lagebild ermöglichen sowie Entscheidungsprozesse erleichtern und beschleunigen.
D-LBO umfasst dabei mehr als nur die Einführung neuer IT-Geräte. Es geht um die Integration moderner Kommunikationsnetze, vernetzter Fahrzeuge, digitaler Führungsinformationssysteme sowie die Einbindung von Sensoren und Aufklärungsmitteln. Informationen aus unterschiedlichen Quellen sollen zusammengeführt, ausgewertet und den Entscheidungsträgern strukturiert zur Verfügung gestellt werden. Damit reagiert das Programm auf die gestiegene Komplexität moderner Einsatzszenarien und die Notwendigkeit schneller und präziser Abstimmung.

Hier übernimmt das ZDigBw eine zentrale Rolle bei der Umsetzung. Es fungiert dabei als verbindendes Element zwischen militärischem Bedarf, technischer Entwicklung und praktischer Einführung in die Truppe. Das Zentrum begleitet Projekte von der konzeptionellen Planung über Erprobungsphasen bis zur Implementierung im Einsatzbetrieb.
Darüber hinaus unterstützt es die Standardisierung digitaler Prozesse und sorgt dafür, dass neue Systeme interoperabel und sicher betrieben werden können. Auch Ausbildung, Tests und organisatorische Anpassungen fallen in seinen Aufgabenbereich. So trägt das Zentrum entscheidend dazu bei, dass D-LBO nicht nur technische Modernisierung bedeutet, sondern eine nachhaltige Änderung in der militärischen Führungs- und Einsatzfähigkeit darstellt.
Die Abteilung IV sind die Programmierexperten des Zentrums. Hier erbringt das ZDigBw operative Leistungen. Die Abteilung verantwortet die qualitätsgesicherte Integration militärischer IT-Services in das IT-System der Bundeswehr und entwickelt in ausgewählten Bereichen eigene Software für den Geschäftsbereich BMVg. Damit schließt die Dienststelle bewusst die Lücke zwischen Planung und Umsetzung.
Um dies leisten zu können, verfügt die Abteilung IV über das nötige Know-how und die notwendige Ausstattung, um den kompletten Softwarelebenszyklus in Form von Test- und Entwicklungsanlagen abbilden zu können. Angefangen von der Steuerung und Priorisierung der gestellten Anfragen mittels IT-Service-Kompetenzleistungen (IT-SKL) als Leistungsvereinbarung mit anderen Bereichen des ZDigBw sowie anderen Stellen der Bundeswehr, hier insbesondere dem BAAINBw.
Auch die Spezialistinnen und Spezialisten für Anforderungserfassung und -management, der Grundlage für jede Entwicklung, sind hier verortet.
Die „Softwareschmiede" der Abteilung IV verfügt über eine leistungsfähige Softwareentwicklungs- und Integrationsanlage, mit der sie den Auftrag der agilen Softwareentwicklung verlässlich durchführt.
Neben der Eigenentwicklung verfügt die Abteilung über Fähigkeiten, IT-Services zu integrieren, um so neue IT-Services aus bestehenden zu schaffen oder auch Pro-

IRec hat eine Service-Mesh-orientierte Architektur, die es ermöglicht, einzelne Services in Pipelines zu verschachteln. Die Abbildung zeigt eine mögliche Pipeline über verschiedene KI-Services für eine Video-Extraktion. Alle Ergebnisse werden dann dem Artikel hinzugefügt und unterstützen den Analysten bei der Analyse und Lagebilderstellung.

©ZDigBw

totypen zu erstellen, um Anforderungen zu evaluieren oder Sofortbedarfe zu decken. In diesem Bereich findet auch die Integration von Sondersoftware für den Warenkorb der BWI statt. Kurz gesagt: keine Sondersoftware auf Herkules IT ohne die Abteilung IV.

Eine weitere wichtige Aufgabe der Abteilung ist die Bereitstellung des Bundeswehranteils am Digitalfunk BOS, ohne die eine Einbindung des Katastrophen- und Zivilschutzes nicht möglich wäre.

Zum Abschluss eines Softwarelebenszyklus gehört die Nachweisführung. Hierbei geht es zum einen darum, zu verifizieren, ob die Anforderungen, die an die zu entwickelnde Software gestellt wurden, durch das fertige Produkt erfüllt werden. Zum anderen wird bei der Validierung neuer Software und kompletter IT-Services geprüft, ob sie für die Nutzung in der Truppe geeignet sind und den Bedarf des Nutzers erfüllen. Darüber hinaus geht es auch um den Nachweis der Interoperabilität mit den Partnern. Dazu führt die Abteilung IV nationale sowie multinationale Tests durch.

Zur Unterstützung von experimentellen Untersuchungen, von Tests und zur Durchführung von über die Bundesrepublik Deutschland verteilten Übungen betreibt die Abteilung ihr eigenes Digitallabor, indem sie die notwendigen Services sowie nationale und multinationale Übungsnetze bereitstellt.

Abschließend beteiligt sich die Abteilung IV an der Operationalisierung des strategischen Leitprinzips Software-Defined Defence (SDD), bei dem es im Schwerpunkt um einheitlich definierte IT-Infrastruktur und agil entwickelte Softwareprodukte geht. Die Idee von SDD ist dabei in der Abteilung nichts Neues, sondern wird seit Jahren bereits von allen Angehörigen der Abteilung gelebt und in der täglichen Aufgabenerfüllung umgesetzt. Ein Beispiel dafür ist die Software Internet Reconnaissance (IRec) aus dem Bereich Open Source Intelligence (OSINT). Angesichts der aktuellen sicherheitspolitischen Lage gewinnt die Fähigkeit, aus öffentlich verfügbaren Daten aussagekräftige Lagebilder zu erstellen, zunehmend an Bedeutung. Die enorme Datenflut im Internet, die Filterung und Auswertung der darin enthaltenen relevanten Informationen stellen dabei eine zentrale Herausforderung dar. Social Media, Smartphones und andere digitale Quellen liefern heute mehr Daten als je zuvor, ein großes Potenzial für OSINT und die Analyse des Informationsumfelds im militärischen Kontext.

Mit der neuen Software IRec entwickelt das ZDigBw ein KI-gestütztes Werkzeug zur automatisierten Sammlung, Analyse und Visualisierung von offen zugänglichen Informationen. Durch den Einsatz moderner Statistik, Heuristik, Künstlicher Intelligenz sowie Bild- und Videoverarbeitung soll IRec Analysten dabei unterstützen, Bedrohungslagen schneller und präziser zu bewerten und so die Sicherheit eigener Kräfte zu erhöhen.

In dieser Struktur vereint das Zentrum Digitalisierung der Bundeswehr strategische Steuerung, technologische Umsetzung und operative Nähe und macht Digitalisierung für die Bundeswehr messbar wirksam.

KI-Spracherkennung stärkt die Digitalisierung der Rettungskette

Von Marco Schriek, Principal Consultant, Center of Excellence Consulting der BWI GmbH

©BwI/Patrick Grüterich (2)

Bei der medizinischen Erstversorgung verwundeter Soldaten zählt auf dem Gefechtsfeld nicht nur jede Minute, auch eine möglichst präzise Dokumentation der erfolgten Behandlungsschritte ist von enormer Bedeutung.
Im ersten Schritt der Rettungskette versorgt der Einsatzersthelfer B den verwundeten Soldaten, macht ihn transportfähig und übergibt ihn an das sanitätsdienstliche Personal. Auf dem Gefechtsfeld sind dabei die Rahmenbedingungen extrem schwierig: Zeitdruck, blutige Handschuhe oder die gleichzeitige Herstellung von Feuerüberlegenheit erschweren die bis dato handschriftliche Dokumentation der Behandlungsdaten.

Lösung:
Eine speziell trainierte KI zur Spracherkennung
Die BWI wurde von der Bundeswehr mit Vorarbeiten für Projekte zur Digitalisierung der Rettungskette beauftragt. Unter anderem sollen identifizierte Fähigkeitslücken mit digitalen Assistenzfunktionen geschlossen werden, wie in diesem Fall die digitale Dokumentation und Weitergabe von Verletzungen, Behandlungsschritten oder Vitalparametern. Für die spezifischen Anforderungen der Patientendokumentation auf dem Gefechtsfeld entwickelte die BWI folgende Idee: Eine notfallmedizinisch trainierte Spracherkennung auf Basis Künstlicher Intelligenz (KI) soll gesprochene Informationen unter Gefechtslärm automatisiert erfassen, transkribieren und strukturiert in die medizinische Standard-Dokumentation übertragen.
Hierfür entwickelte die BWI im Rahmen eines Experiments einen ersten Prototyp. Der Fokus lag dabei auf dem Einsatzersthelfer B am Ort der Verwundung bis zur Übergabe an den ersten medizinischen Experten. Eine von der BWI trainierte KI wurde so verfeinert, dass die Spracherkennung selbst unter Stress und hoher Gefechtslautstärke undeutlich gesprochene Worte im korrekten Sinnzusammenhang erkennt. Bei der Entwicklung wurde auch berücksichtigt, dass die Einsatzersthelfer auf dem Gefechtsfeld oft eigene, präklinisch-militärische Begriffe verwenden.

Mobiler Einsatz auch auf dem Gefechtsfeld
Die KI-Anwendung wird auf dem Standard Mobile Device des Einsatzersthelfers B installiert. Dieses ist ebenso wie das Headset ohnehin an der Ausrüstung des Soldaten befestigt und beeinträchtigt dessen Beweglichkeit somit nicht. Die KI-Anwendung ist insbesondere aufgrund taktischer Erfordernisse im Offline-Betrieb des Mobile Device einsatzfähig und erkennt nach Aktivierung die medizinischen Sprachspezifika, etwa in der Unterhaltung des Einsatzersthelfers B mit seinem Begleitsoldaten. Diese werden von der KI automatisiert erfasst, transkribiert und strukturiert in die Standard-Dokumentation übertragen. In diesem Schritt werden auch weitere relevante Zeitstempel dokumentiert, beispielsweise, wann ein Tourniquet angelegt wurde. Diese Daten werden mit GPS-Positionsdaten angereichert, sodass ein digitales Bild mit Verletzungen, Vitalwerten, Behandlungsmaßnahmen und exakten Zeitstempeln als weiterleitbare Datei entsteht. Diese Informationen erleichtern dem übernehmenden sanitätsdienstlichen Teil der Rettungskette die Beurteilung über die weiter zu treffenden medizinischen Maßnahmen.

Erfolgreiche Erprobung
Nachdem die BWI gemeinsam mit dem Sanitätsdienst der Bundeswehr das Experiment erfolgreich abschließen konnte, wurden der Prototyp und dessen Funktionalitäten auf der Informations- und Lehrübung des Sanitätsdienstes der Bundeswehr im Juli 2025 vorgestellt. Die Erkenntnisse aus der erfolgreichen Erprobung fließen nun in das für 2027 geplante Projekt „Patientenversorgungs-, Assistenz- und Dokumentationssystem Mobile Sanitätskräfte“ (PADMOS) ein, in dem die BWI die Bundeswehr unterstützt. Die generierten Daten könnten darüber hinaus in die Erstellung von Lagebildern auf verschiedenen Ebenen einfließen.

Die gesprochenen Informationen werden automatisiert in die medizinische Standard-Dokumentation übertragen.

Jens Reynders von Airbus Defence and Space (r.) im Gespräch mit Stefan Axel Boes, stellvertretender Chefredakteur des Hardthöhenkurier.

„Die AFCEA bietet uns ein hervorragendes Forum für den direkten Dialog mit der Bundeswehr“

Interview mit Jens Reynders, Vice President & Head of Defence Digital Germany & International bei Airbus Defence and Space

Sehr geehrter Herr Reynders, was alles gehört zum Aufgabenbereich Defence Digital bei Airbus Defence and Space?
Wir sind der Bereich innerhalb von Airbus Defence and Space, der sich mit Fokus auf Deutschland auf alle militärischen Programme ohne direkten Bezug zu den fliegenden Plattformen konzentriert. Unser Fokus liegt auf bodengebundener Verteidigungsinfrastruktur, vernetzten Systemen und integrierten Führungslösungen. Unser militärisches Portfolio deckt ein breites Spektrum ab: Es reicht von der Combat Cloud über mobile Systeme und die Shelter-Integration bis hin zu Software für Aufklärungs- und Führungsunterstützungssysteme.
Ein wesentlicher Schwerpunkt liegt zudem auf der bodengebundenen Luftverteidigung. Darüber hinaus verantworten wir große Anteile der Lösungen für die Control and Reporting Centres der Luftwaffe, sowohl in stationärer als auch in verlegefähiger Ausführung, sowie die Perimeter-Absicherung von Bundeswehrliegenschaften. Insgesamt präsentieren wir ein weitreichendes Portfolio mit klarem Fokus auf den deutschen Markt und einem komplementären Exportanteil.

Im Grunde sind Sie also ein primärer Dienstleister für die Bundeswehr. Wie unterstützen Sie die Bundeswehr bei der Digitalisierung und vor allem der immer stärkeren Nutzung von Künstlicher Intelligenz?
Wir sind in diesem Bereich sehr gut aufgestellt: Allein in dem Teilbereich von Airbus, in dem ich arbeite, verfügen wir über 100 Experten für Künstliche Intelligenz. Diese sind zwar dezentral organisiert, werden von uns aber sehr zielgerichtet eingesetzt.
Wir unterstützen die Bundeswehr bereits heute dabei, verschiedenste KI-Anwendungen in ihre Bestandssysteme zu integrieren. Aus meiner Sicht ist das eines der

wichtigsten Themen überhaupt; es geht hier nicht um den „Fight tomorrow“, sondern um den „Fight tonight“. Das bedeutet, bestehende Systeme schon jetzt durch gezielte Teilanwendungen zu optimieren, die erhebliche Kampfwertsteigerungen generieren. Während das bei Shelter-Systemen eine untergeordnete Rolle spielt, kann KI insbesondere in der Luftverteidigung heute schon aktiv zum Einsatz kommen.

Ein gutes Beispiel hierfür ist unser Luft- und Raketenabwehr-Managementsystem Fortion SAMOC. Dieses multinationale Operationszentrum führt Daten aus allen Dimensionen zu einem integrierten Lagebild zusammen und nutzt KI-gestützte Algorithmen, um die immense Datenflut in Sekundenschnelle auszuwerten, Bedrohungen automatisch zu priorisieren und optimale Entscheidungsvorschläge für die Abwehr zu liefern. Dadurch ermöglicht es die landesweite Koordination aller bodengestützten Luftverteidigungsressourcen bis hin zur Abwehr ballistischer Raketen.

Ein zweiter wichtiger Punkt ist die Verkürzung und Beschleunigung des Weges zur Serienreife. Unsere spezialisierte Studienabteilung führt hierzu verschiedene Projekte mit der Bundeswehr durch. Gerade in den letzten Jahren haben wir im Bereich der KI enorm an Fahrt aufgenommen, um experimentelle Technologien spürbar schneller direkt in die Truppe zu bringen. Im Rahmen der Studie KITCH, KI für Taktik-Chat in Simulationssystemen, entwickeln wir beispielsweise KI-Lösungen direkt mit dem Kunden und bringen diese über gehärtete On-Premise-Varianten wie „KITCH-in-a-Box“ oder „KITCH mobile“ unmittelbar in hochsichere, militärische Umgebungen.

Ein weiteres Thema, mit dem wir uns sehr intensiv beschäftigen, ist die Simulation. Die entsprechende Produktfamilie nennt sich PAXSEM und ist ein bereits lang etabliertes, agentenbasiertes Simulationsframework. Damit sind wir für die Bundeswehr sowie für befreundete Nationen in der Lage, Veränderungen der Bedrohungslage agil zu simulieren. Es werden neue Waffensysteme eingespielt, um darauf aufbauend optimale Reaktionsmuster zu analysieren. Dieses an sich deterministische System wird von uns zunehmend durch KI angereichert.

Der letzte wesentliche Punkt ist der gesamte Bereich der Drohnensteuerung. Hier haben wir schon früh Pionierarbeit geleistet, insbesondere bei der Frage, wie Drohnen intelligent im Schwarm gesteuert werden können. Das tun wir natürlich nicht im Alleingang,

Jens Reynders erläutert sein Portfolio als Vice President & Head of Defence Digital Germany & International bei Airbus Defence and Space.

Auf der AFCEA-Fachausstellung 2026 präsentierte Airbus unter anderem das unbemannte Hubschrauber-Aufklärungssystem VSR700.

sondern arbeiten eng mit Partnern wie Quantum-Systems zusammen. Auf Basis von Studien mit der Bundeswehr haben wir in diesem Segment bereits beachtliche Fortschritte erzielt.
Neben der erwähnten Kooperation mit Quantum-Systems im Drohnenbereich unterstützen wir die Bundeswehr vor allem durch diesen kontinuierlichen Dialog. So leiten wir unter anderem den BDSV-Expertenkreis KI. Zudem haben wir im vergangenen Jahr sehr erfolgreiche KI-Tage mit der Bundeswehr am Standort Immenstadt veranstaltet, ein Format, das wir am 6. und 7. Oktober dieses Jahres fortsetzen werden. Damit schaffen wir eine wertvolle Austauschbasis für diese noch sehr neue Technologie.

Welche Systeme und Produkte sind aktuell die wichtigsten Treiber im Bereich Verteidigung für Airbus? Sind das auch noch konventionelle Systeme, die ohne KI auskommen, oder ist das schon ein querschnittlicher Aspekt?
Persönlich glaube ich, dass KI über kurz oder lang alle Systeme betreffen wird. Selbst bei robusten Systemen wie einem Shelter wird es künftig smartere Anwendungsfälle geben. Wir müssen hier schlichtweg in Phasen denken. Am Boden bewegen wir uns vor allem im Bereich der Waffeneinsatzführungssysteme in Segmenten, in denen die KI maximale Unterstützung bietet. Hier sehen wir ganz klar, dass sich die Technologie bereits durch die gesamte Kette zieht, meist in Form von hochspezialisierten Teilfunktionen.

Im Rahmen eines Vertrags mit der französischen Beschaffungsbehörde DGA erweitern wir beispielsweise das Marineüberwachungssystem Spationav um KI-Elemente. Dort wurde der Prozess automatisiert, um Überwachungsdaten von Satelliten und maritimen Systemen schneller zu fusionieren und so deutlich effizienter ein integriertes Lagebild zu generieren. Auch die automatische Erkennung und Identifizierung ist ein zentrales Thema, das besonders für Drohnen relevant ist.
Da moderne Verteidigung aber längst auch im Informationsraum stattfindet, ist ein weiterer entscheidender KI-Treiber bei Airbus unsere Produktlösung Massive Intelligence. Als integrierte Multi-Intelligence-Lösung bündelt das System unter anderem OSINT, also Open Source Intelligence, GEOINT, Geospatial Intelligence, COMINT, Communications Intelligence, oder IMINT, Imagery Intelligence, und weitere Quellen.
Durch das intelligente Zusammenspiel dieser verschiedenen Bereiche lassen sich Deepfakes sowie manipulierte Videos, Bilder und Audiodateien präzise erkennen. Um diese Desinformation im Verteidigungskontext verlässlich zu identifizieren, nutzen wir wiederum KI-gestützte Verfahren. Gleichzeitig unterstützen diese KI-Tools unsere Analysten dabei, größere Zusammenhänge oder Desinformations-Narrative zu erkennen, die gegebenenfalls von bestimmten Akteuren oder Staaten gesteuert werden.
Im Bereich Cybersecurity nutzen wir KI zur Erkennung von Malware, für fortschrittliche Analyseverfahren in den Cyber Operation Centern sowie in den Cyber-Trainingsszenarien für die Streitkräfte. Zusammenfassend lässt sich sagen: Für uns ist KI bereits ein querschnittlicher Aspekt, der sich durch unser gesamtes Produktportfolio zieht. Bei einigen Systemen schreitet die Integration etwas schneller voran, bei anderen benötigt dieser Transformationsprozess noch etwas Zeit.

Warum ist die AFCEA Fachausstellung für Sie so interessant? Und wo liegt dieses Jahr der Schwerpunkt für Sie hier?
Die AFCEA Fachausstellung ist für uns deshalb so interessant, weil sie sich exakt an der Schnittmenge zwischen der Bundeswehr sowie IT- und Defence-Unternehmen bewegt. Für die Bereiche des Airbus-Portfolios, die ich verantworten darf, ist das ideal, da es bei uns im Kern immer um IT- und Software-Integrationsthemen geht. Die AFCEA bietet uns ein hervorragendes Forum für den direkten Dialog mit der Bundeswehr. Die räumliche Nähe in Bonn hilft dabei natürlich enorm, die relevanten Akteure kommen alle bei uns vorbei.
Gleichzeitig habe ich es ja bereits erwähnt: Wir setzen intensiv auf Partnerschaften. Das ist in diesem dynamischen Umfeld unumgänglich. Auch für diesen Austausch mit Partnern und Kunden ist die Messe eine perfekte Plattform. Was unsere diesjährigen Schwerpunkte betrifft, so steht Künstliche Intelligenz ganz klar im Vordergrund. Mein Kollege Daniel Kalfass hat hierzu einen Fachvortrag zum Thema „Taktischer KI-Assistent für den digitalen Gefechtsstand“ gehalten, und wir demonstrieren unsere KI-Anwendung KITCH direkt auf dem Stand des Unterstützungskommandos.
Darüber hinaus fokussieren wir uns auf drei weitere Kernthemen. Einmal der ganze Bereich Konnektivität und Interoperabilität. Hier zeigen wir sowohl unsere Lösungen im Bereich der Satellitenkommunikation als auch die Entwicklungen unserer Kollegen beim Bündelfunk. Das umfasst klassische TETRA-Netzwerke ebenso wie ein hochsicheres Overlay für 5G-Plattformen namens Airbus AGNET.
Ein weiterer wichtiger Kernbereich von uns ist die Cybersicherheit. Am Stand demonstrieren wir, wie ein Tactical SOC, Security Operations Center, in der Praxis funktionieren kann. Zudem stellen wir unsere Simulations- und Trainingsplattform CyberRange vor, mit der wir umfassende Cyber-Szenarien für Streitkräfte abbilden können.
Schließlich zeigen wir wegweisende Lösungen im Bereich der luftgestützten Aufklärung und Geodaten. Ein Beispiel hierfür ist die VSR700, ein unbemanntes Hubschraubersystem für maritime und terrestrische Aufklärungsmissionen. Dessen Fähigkeiten komplementieren wir direkt mit den hochauflösenden Geodaten unseres Airbus-eigenen Satellitenverbunds Pléiades Neo.

Sie sagen, Sie arbeiten mit vielen Partnerunternehmen wie Quantum-Systems zusammen. Das ist ja quasi schon eine etablierte Firma. Aber wir haben hier auf der AFCEA auch einen Start-up-Bereich …
Ich kann hier vor allem aus eigener Erfahrung sprechen: Aus der Perspektive eines Großkonzerns wie Airbus ist natürlich fast jedes andere Unternehmen etwas kleiner. Das Spektrum unserer Partner reicht dabei von agilen Start-ups bis hin zu klassischen KMU. In diesem Ökosystem arbeiten wir sehr erfolgreich zusammen. Vieles von dieser Kooperation findet bereits im reinen Engineering-Bereich statt, also noch vor dem direkten Kundenkontakt.
Dabei gilt ganz klar: Auch für kleinere Partner gelten exakt die gleichen, strengen Sicherheitsanforderungen. Wir arbeiten beispielsweise mit einem hochspezialisierten KMU zusammen, bei dem prozentual sogar noch mehr Mitarbeiter sicherheitsüberprüft sind als in unseren eigenen Teams. Grundsätzlich arbeiten wir unglaublich gerne mit agilen Start-ups und ihren visionären Ideen zusammen. Die eigentliche Kür liegt dann darin, diese innovativen Konzepte fit für die strengen behördlichen Auflagen und Zertifizierungen zu machen.
Dieser hohe Qualitätsanspruch ist am Ende unser gemeinsames Gütesiegel, auch wenn nicht jedes Start-up diesen intensiven und ressourcenstarken Zertifizierungsweg von Anfang an bis zum Ende mitgehen kann. Das ist aus meiner Sicht jedoch nichts Schlimmes, sondern schlicht ein notwendiger Qualitätsfilter im Defence-Bereich. Diejenigen Start-ups, die sich strategisch darauf fokussieren, lernen schnell, worauf es ankommt und wie man etwa erfolgreich den Dialog mit den Juristen des BAAINBw führt.

Herr Reynders, vielen Dank für das Gespräch.

Die Fragen stellten Burghard Lindhorst und Stefan Axel Boes.

Erkennungsraten von 99,9 Prozent der Cyber-Threats

Nachgefragt bei …

Michael Rimmele, Major Account Manager Defence bei Check Point Software in Deutschland

©MRV

Michael Rimmele, Major Account Manager Defence bei Check Point Software, stellte sich den Fragen von Michael Horst, Chefredakteur des „Hardthöhenkurier".

Sehr geehrter Herr Rimmele, gibt es neue Herausforderungen seit der letzten AFCEA Fachausstellung und worauf liegt zurzeit der Fokus?
Die Herausforderung für uns als Hersteller von Cybersecurity-Lösungen liegt selbstverständlich darin, dass wir Cyberattacken erkennen müssen, die zunehmend KI gesteuert sind. Das Thema Erkennungsrate ist ein ganz wichtiger Punkt, den wir aber seit jeher sehr gut lösen. Wir haben Anfang des Jahres durch ein unabhängiges Testinstitut erneut bestätigt bekommen, dass wir in den Erkennungsraten mit einem Ergebnis von 99,9 Prozent marktführend sind. Wenn man da unsere Wettbewerber wie zum Beispiel Fortinet, Palo Alto oder Cisco betrachtet, dann liegt der Zweitplatzierte bei lediglich 84 Prozent Erkennungsrate. Deshalb lösen wir diese Herausforderung, der wir uns durch KI-gesteuerte Cyberattacken konfrontiert sehen, im Vergleich zum Wettbewerb überdurchschnittlich gut. Die Herausforderungen, was das Geschäft in Deutschland anbelangt, sind natürlich die ganzen Zulassungsszenarien, wie zum Beispiel die VS-Zulassung. Wir haben seit dem letzten Jahr eine BSI-Zertifizierung für unsere Kernprodukte, also alles, was sich in dem Bereich Hybrid Mesh Firewalls bewegt.

An welchen zentralen Projekten zur Digitalisierung der Streitkräfte arbeitet Check Point Software gerade?
Das ist vielfältig, würde ich tatsächlich sagen. Wir sind aktuell in regem Austausch mit Vertretern der Rüstungsindustrie, wenn es um die Themen Software-Defined Defence und Multi-Domain Operations geht. Da gibt es ja einige interessante Player wie Airbus Defence and Space oder Hensoldt. Überall dort, wo Systeme vernetzt werden, gibt es Netzübergänge und diese müssen selbstverständlich entsprechend abgesichert werden. Ebenso mit Herstellern im Bereich Marinetechnik, in dem wir diverse Besonderheiten haben, wenn es um die Absicherung innerhalb der Domäne See geht. Dort finden wir besondere Anforderungen an Abluft, Platzmangel, an „Ruggedized" et cetera vor. Und auch hier sind wir ein bevorzugter Hersteller.

Welche Rolle nehmen Partner ein?
Wir sind eine hundertprozentige Partnerorganisation und treten in der Regel selten als Systemintegrator auf. Wir haben Partner, die für unsere Lösungen zertifiziert sind und diese sowohl beraten als auch implementieren. Wir selbst agieren beratend in Richtung Endkunde und unterstützen Partner bei Bedarf im Presales oder in der Technologie-Bereitstellung für Tests. Partner wie NTT, Bechtle, SVA oder Computacenter übernehmen dann das Fulfillment beim Endkunden.

Auf der AFCEA werden in der Regel Einblicke zu Projekten gezeigt, die dazu beitragen, die IT der Bundeswehr zu optimieren. Wo liegt in diesem Jahr der Schwerpunkt auf dem Check Point Software-Messestand?
Wir präsentieren in diesem Jahr die neue Rugged-X Security Appliance gemeinsam mit unserem Partner steep. Die Rugged-X ist ein Produkt der steep, wird auch von steep produziert und erfüllt alle relevanten militärischen und industriellen Standards. Steep hat das militärische Gehäuse mit individuell konfigurierbaren Anschlüssen gefertigt und unsere Security-Technologie, also Platine und Software Layer integriert. Hier sprechen wir quasi von einer Military off-the-shelf Security Appliance, die zum Beispiel für den Einsatz in Fahrzeugen oder in verlegbaren Systemen verwendet werden kann. Die Kombination aus militärischem Gehäuse, MIL-Zertifizierungen und den vorher erwähnten Erkennungsraten ist diese Appliance derzeit einzigartig im Markt.

Sind Sie mit dem Interesse der zivilen und besonders militärischen Besucher zufrieden?
Ja, in der Tat. Wir sind auch mit einer entsprechende Mannstärke hier auf dem Stand vertreten und der Zulauf von Bundeswehr und Industrie ist außerordentlich gut. Gerade in der aktuellen Diskussion zur europäischen Souveränität sind wir als israelisches Unternehmen Europa näher als die US-amerikanischen Wettbewerber. Das beeinflusst, denke ich, noch zusätzlich zu unserer Technologieführerschaft das erhöhte Interesse an uns. Insofern können wir jetzt schon sagen, dass wir sehr zufrieden mit dem bisherigen Verlauf sind.

Danke für das Gespräch und Ihre Zeit.

Dirk Walther, Leiter Geschäftsbereich Defence der ND SATCOM, stellte sich auf der diesjährigen AFCEA Fachausstellung den Fragen von Michael Horst, Chefredakteur des „Hardthöhenkurier".

Nachgefragt bei …

Dirk Walther, Leiter Geschäftsbereich Defence der ND SATCOM

Sehr geehrter Herr Walther, das Leitthema der AFCEA Fachausstellung 2026 lautet „Vernetzt denken & sicher handeln als Antwort einer gesamtstaatlichen Verteidigung". Sind wir bei der gesamtstaatlichen Verteidigung aus Ihrer Sicht in der digitalen Zeitenwende zu langsam, was muss sich ändern und welche wesentlichen Folgerungen hat das für ND SATCOM?
Die allseits beschworene Zeitenwende hält spürbar Einzug. Für ND SATCOM bedeutet das insbesondere, Technologien schneller skalierbar, resilient und interoperabel bereitzustellen. Allerdings sind Tempo und Pragmatismus, insbesondere in Bezug auf Beauftragungen in den Mittelstand hinein, noch nicht mit dem richtigen Elan spürbar. Der ebenfalls oft zitierte Pragmatismus des öffentlichen Auftraggebers ist für uns an einer der Scharnierstellen der Leistungserbringung nicht immer ersichtlich. Im Zweifel wird nach Prozess vorgegangen. Das gibt zwar gewissermaßen Leitplanken, hemmt aber auch häufig die Entscheidungsfreude und kostet damit wertvolle Zeit.

Wie hat sich die Lage bei ND SATCOM seit der letzten AFCEA Fachausstellung verändert? Gibt es neue Herausforderungen und worauf liegt zurzeit der Fokus?
Seit der letzten AFCEA hat sich einiges verändert. Durch das öffentlich gemachte Bereitstellen von Milliardensummen in die Digitalisierung, insbesondere in der Dimension Raum, ist eine gewisse „Goldgräberstimmung" spürbar. Dies hat nicht zuletzt zu einer Erweiterung auf LEO-Konstellationen geführt.

An welchen zentralen Projekten zur Digitalisierung der Streitkräfte arbeitet ND SATCOM gerade?
ND SATCOM richtet seine Entwicklungen an den Marktanforderungen aus und hat die richtungsweisenden Programme der EU, IRIS², und der Bundeswehr, SATCOMBw, fest im Blick. Dementsprechend fließen die Anforderungen dieses Marktsegmentes (Dimension Raum/Luft, Land, See) in die Weiterentwicklung der SKYWAN-Technologie ein.

Nach meiner Bewertung also ein deutliches Mehr an zeitkritischen Aufgaben für ND SATCOM. Was und wie planen Sie, um diesen Zuwachs an Aufträgen sicher zu bewältigen?
Wir müssen die sogenannte Skalierung organisch bewältigen und den Zuwachs stets beherrschbar halten. Dies betrifft sowohl die Allokation von Fachkräften als auch das Stärken von Partnerschaften hinsichtlich Infrastruktur sowie Engineering- und Fertigungskapazitäten. Unser Ziel ist dabei bewusst nachhaltiges Wachstum statt kurzfristiger Expansion.

Welche Rolle spielen dabei Partner Ihrer Firma?
Partnerschaften gewinnen zunehmend an Bedeutung, insbesondere bei Skalierung, Integration neuer Technologien sowie im Bereich Fertigung und Lieferfähigkeit.

ND SATCOM gibt auf dem Messestand in der Regel Einblicke zu Projekten, die dazu beitragen, die IT der Bundeswehr reaktionsschneller und resilienter zu machen. Wo liegt in diesem Jahr der Schwerpunkt?
Der Schwerpunkt liegt dieses Jahr ganz klar auf unserer Modemtechnologie, hierbei sowohl auf unserem aktuellen „Flaggschiff“, der SKYWAN 7X, als auch auf der technologischen Weiterentwicklung hinsichtlich LEO-Konstellationen.

Die AFCEA Bonn e.V. hat sich zu einer der etabliertesten Dialogplattformen für die IT- und Kommunikationsbranche entwickelt. Sind Sie zufrieden mit dem Interesse der zivilen und besonders militärischen Besucher oder spüren Sie noch Skepsis?
Das Interesse, insbesondere der militärischen Besucher, ist in diesem Jahr herausragend. Es gibt auf dieser Messe in den Gesprächen keine zwei Meinungen hinsichtlich der sicherheitspolitischen Herausforderungen für Europa, etwas, das ich im Übrigen im gesellschaftlichen Diskurs noch etwas vermisse. Das Interesse an Lösungen ist also groß, die Erfahrungswerte aus der Ukraine spielen dabei eine immer größer werdende Rolle. Waren früher noch reine Leistungsparameter von Interesse, so weichen diese immer mehr den Schlagworten „schnell verlegefähig“, „schwer aufklärbar“ und „mengenmäßig skalierbar“.
Die Anforderungen an militärische Kommunikation verändern sich derzeit schneller als jemals zuvor. Entscheidend wird sein, Technologien nicht nur leistungsfähig, sondern vor allem schnell verfügbar und skalierbar zu machen, auf Grundlage einer deutschen Lieferkette. Ebenso spielt die Feldverwendungsfähigkeit auf Basis der Erfahrungen aus dem Ukrainekrieg eine entscheidende Rolle.

Der auf der AFCEA präsentierte SKYWAN 7X.w

Fachpublikum auf dem AFCEA-Messestand der Firma ND SATCOM.

Blick auf den diesjährigen AFCEA-Stand der Firma ND SATCOM. Michael Horst im intensiven Gespräch mit Dirk Walther und Arzu Evlek, Director Marketing & Communication der Firma ND SATCOM.

©MRV/Socrates Tassos

Boris Hecker, Geschäftsführer Atos Deutschland und Leiter Public Sector & Defense Deutschland, im Gespräch mit Michael Horst, Chefredakteur „Hardthöhenkurier".

Zentraler Erfolgsfaktor ist die konsequente Zusammenarbeit in Partnerschaften!

Interview mit Boris Hecker, Geschäftsführer Atos Deutschland und Leiter Public Sector & Defense Deutschland

Sehr geehrter Herr Hecker, „Vernetzt denken & sicher handeln als Antwort einer gesamtstaatlichen Verteidigung", so lautet das Leitthema der AFCEA Fachausstellung 2026. Wie kann die Firma Atos bei der gesamtstaatlichen Verteidigung und der damit verbundenen digitalen Zeitenwende unterstützen?

Die gesamtstaatliche Verteidigungsfähigkeit wird heute nicht mehr allein durch materielle Kapazitäten bestimmt. Entscheidend sind zunehmend die Qualität, Resilienz und Souveränität digitaler Infrastrukturen und Architekturen.

Die Fähigkeit, Daten sicher zu verarbeiten, heterogene Systeme zuverlässig zu vernetzen und Entscheidungen nahezu in Echtzeit zu unterstützen, entwickelt sich zum zentralen Faktor militärischer und staatlicher Handlungsfähigkeit.

Als europäisches IT-Systemhaus und Integrator für digitale, KI-gestützte End-to-End-Services unterstützt Atos die digitale Transformation in sicherheitskritischen Bereichen von staatlichen Institutionen über kritische Infrastrukturen bis hin zu Bundeswehr und Einsatzkräften. Unsere Kernleistung als Systemintegrator besteht darin, isolierte Einzelsysteme zu vernetzen und Datenflüsse in einen gemeinsamen Informationsraum zu integrieren. Daraus entsteht ein übergreifendes, digitales Lagebild,eine zentrale Grundlage für eine funktionierende gesamtstaatliche Verteidigung.

Gibt es neue Herausforderungen seit der letzten AFCEA Fachausstellung und worauf liegt zurzeit der Fokus?

Der Handlungsdruck in der erforderlichen Geschwindigkeit zur Entwicklung von Technologien und Lösungen hat sich weiter erhöht.

Wir können es uns heute nicht mehr leisten, lange Grundsatzdiskussionen über Standards zu führen, bevor wir in die Umsetzung gehen. Stattdessen müssen bestehende, häufig proprietäre Systeme in ihrer aktuellen Form akzeptiert und schnell in vernetzte digitale Wirkverbünde integriert werden. Das erfordert konsequent offene Architekturen und standardisierte Schnittstellen.

Ein zweiter zentraler Aspekt ist die Digitale Souveränität. Architekturen und Lösungen müssen so gestaltet sein, dass die Kontrolle über Datenflüsse, die technologische Unabhängigkeit und die Fähigkeit zum

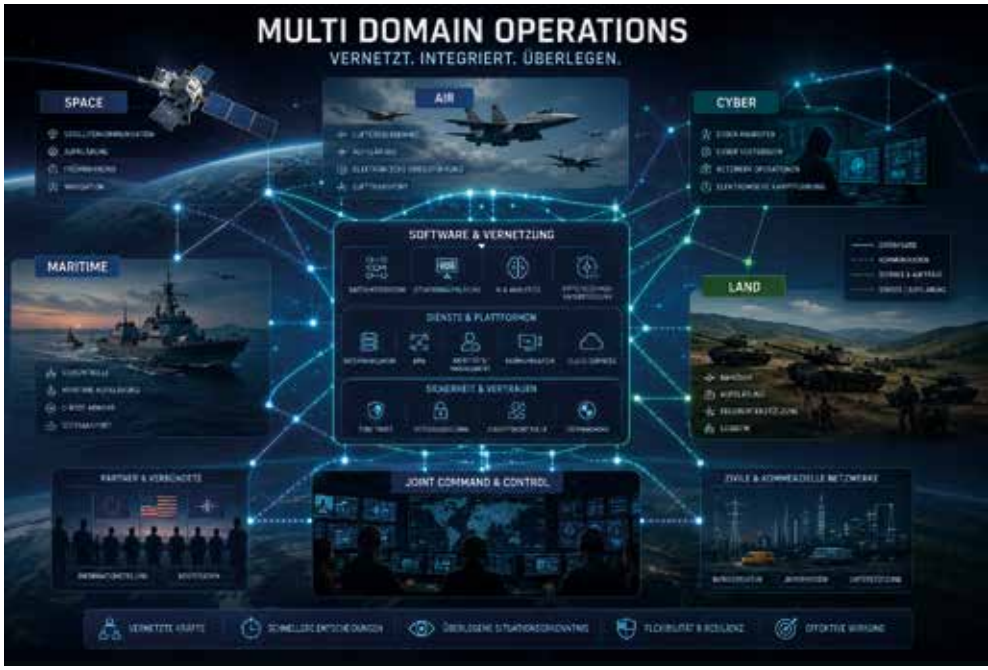
eigenständigen Betrieb und zur Weiterentwicklung jederzeit gewährleistet bleiben.

An welchen zentralen Projekten zur Digitalisierung der Streitkräfte arbeitet Atos gerade?
Ein wesentlicher Schwerpunkt liegt auf der Realisierung von Führungsinformationssystemen zur Erzeugung mehrdimensionaler Lagebilder. Dazu zählen unter anderem Projekte im Bereich der Weltraumlage sowie im Umfeld des German Mission Network. Hier bringt Atos jahrzehntelange Erfahrung in der Integration nationaler und multinationaler Systeme ein.
Ein weiterer Fokus ist die Entwicklung von Tactical Combat Clouds, die Sensoren und Effektoren über unterschiedliche Plattformen hinweg vernetzen. Durch offene Architekturen ermöglichen wir dabei die Integration moderner, digital vorbereiteter Systeme wie etwa Drohnen ebenso wie bestehender proprietärer Einsatzsysteme. Unsere Erfahrung aus Projekten wie dem Transparent Battlefield zeigt, dass sich so durchgängige Sensor-to-Shooter-Ketten realisieren lassen, ein entscheidender Schritt hin zu einem vernetzten Gefechtsfeld.

Was und wie planen Sie, um diesen Zuwachs an zeitkritischen Aufträgen sicher zu bewältigen?
Ein zentraler Erfolgsfaktor ist die konsequente Zusammenarbeit in Partnerschaften. Durch den gezielten Einsatz bewährter Services- und Lösungsbausteine aus dem Atos-Portfolio einschließlich ausgewählter Eviden-Produkte in Bereichen wie Cyberproducts und KI-gestützter Videoanalytik sowie aus unserem breiten Partnernetzwerk können wir Systeme schneller bereitstellen und gleichzeitig auf erprobte Komponenten zurückgreifen.
Zudem setzen wir konsequent auf Künstliche Intelligenz, um Entwicklungs- und Implementierungsprozesse zu beschleunigen von der Konzeption über die Entwicklung bis hin zum Roll-out.

Welche Rolle nimmt dabei Atos als Systemintegrator ein?
Unsere Stärke liegt in der Entwicklung leistungsfähiger IT-Plattformen und in der Integration KI-gestützter digitaler Wirkketten. Atos agiert dabei häufig als Generalunternehmer für komplexe IT-Gesamtsysteme. Dabei kommt es entscheidend auf zwei Aspekte an: die Auswahl geeigneter Technologien und die Orchestrierung der richtigen Partner. Gerade in hochkomplexen Projekten ist die Fähigkeit zur Integration der entscheidende Erfolgsfaktor, nur so lassen sich leistungsfähige, interoperable Systeme in kurzer Zeit realisieren.

Auf der AFCEA werden in der Regel Einblicke zu Projekten gezeigt, die dazu beitragen, die IT der Bundeswehr zu optimieren. Wo liegt in diesem Jahr der Schwerpunkt auf dem Atos-Messestand?
Im Mittelpunkt unseres Messeauftritts stehen Lösungen für Software-Defined Defense (SDD) auf Basis offener, modularer Architekturen und Cloud-Native-Technologien.
Ein wesentliches Element ist unsere **Sovereign Software Factory**, die eine sichere und integrierte Softwareentwicklung über den gesamten Lebenszyklus hinweg ermöglicht. Dabei unterstützen wir insbesondere die Realisierung von System-of-Systems-Ansätzen, etwa durch Daten- und KI-gestützte Entscheidungsunterstützung sowie durch die Vernetzung bestehender Systeme mit einer Tactical Combat Cloud.
Ergänzt wird dies durch eine **serviceorientierte Middleware-Technologie** der Atos als digitales Rückgrat für Multi-Domain Operations. Atos macht SDD damit greifbar und praktisch umsetzbar.
Darüber hinaus zeigen wir konkrete **Lösungen im Kontext OPLAN DEU**, insbesondere zur Schaffung vernetzter Datenräume für gesamtstaatliche, mehrdimensionale Lagebilder sowie zur Stärkung der Resilienz gegenüber hybriden Bedrohungen.



©Atos Deutschland, KI-generierte Konzeptgrafik 2026

Multi-Domain Operations.

Die AFCEA Bonn e.V. hat sich zu einer der etabliertesten Dialogplattformen für die IT- und Kommunikationsbranche entwickelt. Sind Sie mit dem Interesse der zivilen und besonders militärischen Besucher zufrieden?
Ja, absolut. Das Interesse war in diesem Jahr erneut sehr hoch, sowohl quantitativ als auch qualitativ. Besonders hervorzuheben ist die zunehmende Konkretisierung der Gespräche: Der Fokus liegt klar auf der schnellen Umsetzung und Realisierung konkreter Fähigkeiten.
Der große Mehrwert der Veranstaltung liegt im direkten Austausch über alle Ebenen hinweg vom Nutzer bis zum strategischen Entscheider.
Dieser Dialog ist entscheidend, um die tatsächlichen Bedarfe der Streitkräfte präzise zu verstehen und um Lösungen bereitzustellen, die nicht erst morgen, sondern idealerweise schon heute wirken.

©MRV/Socrates Tassos

Marc Schieder, CEO emproof, im Gespräch mit Michael Horst, Chefredakteur „Hardthöhenkurier".

Mit emproof Nyx härten wir Software auf Binärebene!

Nachgefragt bei …

Marc Schieder, CEO emproof

Sehr geehrter Herr Schieder, die Bundeswehr soll zur stärksten konventionellen Armee Europas werden. Wie kann die Firma emproof bei der damit verbundenen digitalen Zeitenwende unterstützen?
Die digitale Zeitenwende in der Bundeswehr entscheidet sich nicht allein durch neue Plattformen, sondern durch deren digitale Widerstandsfähigkeit. Plattformen, Sensoren, Funkgeräte und Effektoren sind heute in hohem Maß softwaredefiniert. Eingebettete Software wird damit zu einem sicherheitskritischen Bestandteil militärischer Handlungsfähigkeit. Hier setzt emproof an: Mit emproof Nyx härten wir Software auf Binärebene, also dort, wo Systeme ausgeliefert und betrieben werden. Wir erschweren Reverse Engineering, Code-Manipulation und Exploit-Entwicklung erheblich, ohne Quellcodes offenzulegen oder tief in Entwicklungsprozesse einzugreifen. So entsteht eine zusätzliche Schutzschicht für digitale Souveränität und operative Resilienz bis auf Geräteebene.

Gibt es zurzeit neue Herausforderungen und worauf liegt zurzeit der Fokus?
Die Bedrohungslage hat sich verdichtet. Angriffe richten sich zunehmend gegen eingebettete Systeme, Firmware, Updates und Lieferketten. Wehrtechnische Systeme bleiben oft lange im Feld, lassen sich nicht kurzfristig neu entwickeln, und der vollständige Quellcode ist nicht immer unmittelbar verfügbar oder wirtschaftlich nutzbar. Ein Schwerpunkt liegt deshalb auf der nachträglichen Härtung bestehender Systeme, also dort, wo klassische Security-by-Design-Ansätze nicht mehr greifen. Daneben adressieren wir Lieferkettenresilienz, damit Updates und ausgelieferte Geräte nicht selbst zum Einfallstor werden. Sicherheit muss so früh wie möglich, bei Bedarf aber auch nachträglich und automatisiert in bestehende Prozesse integrierbar sein.

An welchen zentralen Projekten zur Digitalisierung der Streitkräfte arbeitet emproof gerade?

Wir arbeiten mit Partnern aus Industrie und Systemintegration an Anwendungsfällen, bei denen eingebettete Software besonders schutzbedürftig ist. Ein Schwerpunkt sind unbemannte Systeme. Der Krieg in der Ukraine zeigt deutlich, dass Drohnen, Sensorik, KI-Modelle und autonome Funktionen zu entscheidenden technologischen Schlüsselfaktoren geworden sind. Gleichzeitig steigt das Risiko, dass der Gegner erbeutete Systeme ausliest, analysiert und gegen den ursprünglichen Betreiber wendet. Wir härten daher nicht nur Firmware, sondern auch die darin enthaltene technische Intelligenz: Algorithmen, Entscheidungslogik und, wo relevant, KI-Modelle. Der entscheidende Vorsprung liegt heute häufig nicht allein in der Hardware, sondern in der Software, die Navigation, Sensorfusion und Missionslogik ermöglicht.

Was und wie planen Sie, um diesen Zuwachs an zeitkritischen Aufträgen sicher zu bewältigen?
Wir wachsen personell, optimieren unsere Prozesse und bauen die Zusammenarbeit mit Partnern aus. Intern verstärken wir gezielt Kompetenzen in Binäranalyse, Compiler-Technologie und Embedded Security. Darüber hinaus automatisieren wir unsere Integrationsprozesse weiter, damit Projekte schneller und reproduzierbarer werden. Mit Systemhäusern und Industriepartnern arbeiten wir eng zusammen. Diese klare Rollenteilung erlaubt es, auch zeitkritische Anforderungen zu bedienen, ohne Abstriche bei Qualität, Nachvollziehbarkeit und Sicherheit.

Welche Rolle nimmt emproof als Partner der Systemhäuser ein?
emproof ist spezialisierter Technologiepartner, kein Plattformanbieter. Wir treten nicht in Konkurrenz zur Systemverantwortung der Generalunternehmer, sondern ergänzen ihre Lösungen um eine Schutzschicht für eingebettete Software. Das ist besonders relevant, weil viele Verteidigungssysteme aus komplexen Lieferketten bestehen, der Quellcode nicht immer vollständig vorliegt und bestehende Architekturen nicht grundlegend neu aufgesetzt werden können. So lassen sich Schutzmaßnahmen auch dort integrieren, wo klassische Security-Ansätze an Grenzen stoßen.

Wo liegt in diesem Jahr der Schwerpunkt auf dem emproof-Messestand?
Im Mittelpunkt steht emproof Nyx für sicherheitskritische Embedded-Anwendungen. Wir zeigen konkret, wie sich Firmware und Binärcode härten und in bestehende Auslieferungsprozesse integrieren lassen. Der Schwerpunkt liegt nicht auf abstrakten Folien, sondern auf konkreter technischer Anwendbarkeit. Mit Bedarfsträgern, Systemhäusern und Industriepartnern diskutieren wir, wie Schutz automatisierbar bleibt und wie sich bestehende Systeme nachträglich robuster machen lassen.

Die AFCEA Bonn e.V. hat sich zu einer der etabliertesten Dialogplattformen für die IT- und Kommunikationsbranche entwickelt. Sind Sie mit dem Interesse der Besucher zufrieden?
Ja, sehr. Die AFCEA ist eine der maßgeblichen Dialogplattformen für die Digitalisierung der Verteidigung im deutschsprachigen Raum. Besonders wertvoll ist die Qualität der Gespräche: Bedarfsträger, Beschaffung, Systemhäuser und Technologieanbieter treffen wir hier an einem Ort. Genau dort entfaltet unsere Technologie ihren Wert.

Impressum

Sonderpublikation
AFCEA Fachausstellung 2026
ISSN 0933-3355

MITTLER REPORT

Verlag · Herausgeber
Mittler Report Verlag GmbH
Beethovenallee 21 · 53173 Bonn
Telefon: +49 (0) 228 / 25 90 03 44
E-Mail: info@hardthoehenkurier.de
www.hardthoehenkurier.de

Ein Unternehmen der Gruppe TAMM Media

Geschäftsführer
Peter Tamm

Verlagsleiterin
Sylvia Fuhlisch

Redaktion
Chefredakteur: Michael Horst V.i.S.d.P. (mh)
Telefon: +49 (0) 228 / 35 00 881
Mobil: +49 (0) 173 / 28 91 728
E-Mail: m.horst@mittler-report.de
E-Mail: redaktion@hardthoehenkurier.de

Stellvertretender Chefredakteur:
Stefan Axel Boes (sab)
Telefon: +49 (0) 30 / 86 32 42 662
E-Mail: s.boes@mittler-report.de

Mitarbeiter Redaktion:
Friedrich K. Jeschonnek, Johann R. Fritsch, Knut Görsdorf (kg), Burghard Lindhorst, Dr. Gerd Portugall
E-Mail: redaktion@hardthoehenkurier.de

Fotograf: Socrates Tassos

Marketing · Head of Sales
Michael Menzer
Telefon: +49 (0) 228 / 35 00 866
Mobil: +49 (0) 151 / 15293872
E-Mail: m.menzer@mittler-report.de

Anzeigenkoordination: Karin Helmerath
Telefon: +49 (0) 228 / 25 900 344
E-Mail: k.helmerath@mittler-report.de

Marketing · Anzeigen
Stephen Barnard, Telefon: +49 (0) 228 / 35 00 886,
E-Mail: s.barnard@mittler-report.de

Stephen Elliott, Telefon: +49 (0) 228 / 35 00 872,
E-Mail: s.elliott@mittler-report.de

Thomas Liebe, M.A., Telefon: +49 (0) 228 / 25 900 350,
Mobil: +49 (0) 176 / 24 13 02 29,
E-Mail: t.liebe@mittler-report.de

Susanne Sinß, Telefon: +49 (0) 40 / 70 70 80 310,
E-Mail: s.sinss@hansa-online.de

Layout
AnKo MedienDesign GmbH
Telefon: +49 (0) 2225 / 608 67 42
E-Mail: info@anko-mediendesign.de

Offizieller Partner:

Marcel Taubert (m.) im Interview mit Stefan Axel Boes (l.) und Burghard Lindhorst vom Mittler Report Verlag.

„Wir können in Deutschland viel mehr, als wir uns zutrauen“

Interview mit Marcel Taubert, Vice President Defence & Space von secunet Security Networks

Sehr geehrter Herr Taubert, die NATO vollzieht gerade den Wandel vom Denken in Waffensystemen zu Software-Defined Defence und Data-Driven Defence. Unter anderem führt sie zurzeit das System Maven von Palantir ein. Was trägt secunet an Angeboten bei, und wie sehen die aus?

Bei Verschlusssachen geht es im Kern um einen Zielkonflikt zwischen maximaler Sicherheit und maximaler Teilbarkeit zugleich. Genau den lösen wir. Klassisch gilt das Need-to-know-Prinzip: Kenntnis nur, wenn notwendig. Mit software- und datengetriebenen Ansätzen wie dem Maven Smart System, das die NATO 2025 von Palantir beschafft hat, kommt ein zweites Prinzip hinzu: Need to share. General Stanley McChrystal hat den Wandel vom Need to know zum Need to share mal treffend mit „Share to win“ beschrieben.

In diesem Spannungsfeld arbeiten wir. Verschlusssachen so absichern, dass Informationen kollaborativ geteilt und genutzt werden können. Und zwar so reibungslos, wie man es von modernen kommerziellen Cloud-Diensten kennt und zugleich das Prinzip „Kenntnis nur, wenn notwendig“ wahrt. Dafür stellen wir hochsichere Infrastruktur bereit und haben bereits eine Softwarelösung, die Need to know in den entsprechenden Umgebungen abbildet.

Gleichzeitig reicht rein manuelles Arbeiten mit Informationen nicht mehr aus. Wir nutzen seit Jahren Machine-Learning-Algorithmen und Operations-Research-Ansätze, also mathematische Verfahren zur Optimierung komplexer Entscheidungen. Der KI-Schub der letzten Jahre hebt das auf ein neues Niveau. Hier entstehen praktisch von Woche zu Woche neue Möglichkeiten.

Palantir ist seit über zehn Jahren auch im nationalen Sicherheitsbereich aktiv, etwa bei Polizeibehörden. Das Unternehmen hat entsprechend viel Erfahrung darin, Plattformen dieser Art aufzubauen und in Organisationen zu verankern, vergleichbar mit den großen Hyperscalern im Office-Umfeld. Jeder weiß, wie schwer etablierte Lösungen zu ersetzen sind. Deshalb sind wir überzeugt: Solche Fähigkeiten muss man im Ökosystem denken, nicht isoliert.

Die Souveränitätsdebatte verschiebt sich gerade von politischen Schlagworten hin zur Frage, wie wir anfangen, sie ernsthaft umzusetzen. Dafür liefern wir das Fundament, nämlich eine sichere Plattform, auf der solche Anwendungen über alle Geheimhaltungsstufen hinweglaufen von offen über VS-NfD beziehungsweise RESTRICTED bis GEHEIM beziehungsweise SECRET. Anders als früher ziehen wir längst nicht mehr nur einen Zaun um ein Rechenzentrum. Wir bringen die Sicherheitsarchitektur in die Cloud.
Steht dieses Fundament, können wir Lösungsanbieter in ein souveränes Ökosystem integrieren. Mit Innosystec haben wir eine strategische Partnerschaft geschlossen. Deren Lösung SCOPE führt Massendaten, Open Source Intelligence und bereits verarbeitete Daten in einem System zusammen, damit sie analysiert werden können.

Geht es darum, der absolute Konkurrent von Palantir zu werden?
Nein, und das ist eine strategische Entscheidung, kein Verzicht. Den Wettlauf um die beste Analyseplattform führen andere. Den führen wir bewusst nicht. Unsere Rolle ist eine andere, und ich würde sagen die anspruchsvollere: die souveräne, zugelassene und herstellerunabhängige Schicht, auf der solche Plattformen überhaupt sicher betreibbar sind. Ich bin überzeugt, dass wir in Deutschland und Europa die Technologien haben, um Vergleichbares und in bestimmten Bereichen Besseres zu entwickeln.
Was uns manchmal fehlt, ist die Bereitschaft der Kunden, die Souveränität einfordern, diese europäischen Fähigkeiten dann auch konsequent zu nutzen. Denn auch ein marktdominanter Anbieter wie Palantir liefert keine Lösung von der Stange. Man braucht konkrete Use Cases und muss gemeinsam mit dem Kunden integrieren. Wir sollten nicht versuchen, Microsoft oder Palantir nachzubauen. Was zählt, ist die Frage, was unsere Stärken sind und wie wir sie so zusammenbringen, dass daraus echter Mehrwert entsteht.

Wenn Sie von so einem Sicherheits-Ökosystem in Deutschland reden, hat man den Eindruck, es gäbe ein System. Ist es nicht eher der Bund, dann hier ein Land, dann da ein Land, vielleicht mal zwei, drei zusammen? Wir reden von Gesamtverteidigung. Haben wir nicht eher Insellösungen?
Unsere Technologie ist in einer Welt groß geworden, in der Verschlusssachen bewusst nicht über offene Schnittstellen nach außen geöffnet wurden. Wer früher mit unserer SINA-Technologie gearbeitet hat, konnte innerhalb dieser geschützten Umgebung sehr gut zusammenarbeiten, auch wenn diese eine große nationale Insel war. Dieses Denken in geschützten, voneinander abgegrenzten Strukturen war in Deutschland über viele Jahre prägend und vielfach erfolgreich. Für die heutige Gesamtverteidigung reicht es nicht mehr aus. Und gerade weil wir die geschützte Insel perfektioniert haben, wissen wir, wie man sie öffnet, ohne die Sicherheit zu verlieren.
Jetzt brauchen wir genau dieses Teilen. Das bisherige Modell wird schon national schwierig, wenn ein Bundesland andere Technologien nutzt als das andere. Europaweit funktioniert es gar nicht. Wir müssen Kollaboration deutlich besser ermöglichen. Unsere Erfahrung der letzten Jahre zeigt, dass im Verschlusssachenbereich die NATO häufig der Taktgeber für Standardisierung war.
Diese Standardisierung war allerdings teilweise langwierig. Beim sicheren IP-Standard der NATO, NINE, zog sich der Prozess über viele Jahre hin. Erst jetzt wird er implementiert. Beim SCIP-Standard für sichere Sprachkommunikation waren wir einer der ersten, die ihn in unseren SINA Communicator H, das sogenannte „rote Kanzlertelefon", integriert haben. Wir wären interoperabel gewesen, hätte es weitere Anbieter gegeben, die diesen Standard ebenfalls unterstützen. Dies macht deutlich, dass, auch wenn wir mit geschützten Inseln groß geworden sind, unterschiedliche Lösungen künftig stärker verbunden werden müssen. Und das gelingt über Interoperabilität.

„Share to win": Marcel Taubert erläutert die Philosophie hinter den Lösungen von secunet.

Dazu passt das europäische Motto „In Vielfalt geeint". Vielfalt kann eine Stärke sein. Wer auf einen einzelnen, marktdominanten Anbieter wie Palantir setzt, macht sich langfristig abhängig und muss ihm sehr weitreichend vertrauen. Unser Anspruch ist ein anderer. Wir wollen zwischen die Systeme kommen, Verbindungen schaffen und Abhängigkeiten reduzieren. Das ist für uns nicht nur eine technische Aufgabe, sondern Teil unseres Purpose: „We are the Guardians of Europe's Digital Freedom".
Die Souveränitätsdebatte benennt das Problem, aber sie erfasst es nicht vollständig. Worum es letztlich geht, ist unsere digitale Freiheit. Und ja, das ist ein System der Systeme, kein durchorchestriertes Gesamtsystem. Die Ukraine hat das eindrücklich belegt. Menschen speisten mit handelsüblichen Smartphones Bilder mit Geotags in ein C2-System ein, woraus ein militärisches Lagebild entstand. Wenn der Druck groß genug ist, greifen solche Systeme zusammen.

Auf der AFCEA Fachausstellung 2026 präsentierte secunet seine sichere Kommunikationstechnologie SINA.

Kommen wir noch einmal zur Kombination von SCOPE und SINA. SINA ist Ihr System, SCOPE das Ihres Partners. SINA existiert zudem in verschiedenen Versionen: SINA-S, -E und -H. Können Sie kurz erklären, was SCOPE und was SINA in dieser Kombination leisten und wie die Abstufungen sind?
S, E und H bezeichnen unterschiedliche Klassifizierungsstufen, angelehnt an die NATO-Terminologie, also Standard, Enhanced und High. S reicht bis RESTRICTED beziehungsweise VS-NfD, E bis CONFIDENTIAL beziehungsweise VS-VERTRAULICH, H bis SECRET beziehungsweise GEHEIM. Wir haben Desktopgeräte und Laptops, die multisessionsfähig sind. Auf einem solchen Gerät kann man OFFEN sowie gleichzeitig auf VS-NfD- und auf GEHEIM-Niveau arbeiten. Nach unserer Kenntnis sind wir weltweit der einzige Anbieter von zugelassenen, multisessionsfähigen Clients, die das ermöglichen. Das ist zunächst die Hardwaregrundlage, um in diesem Ökosystem zu arbeiten.
Darüber hinaus verfügen wir über einen Cloud-Stack aus mehreren Modulen, die modular zugelassen sind beziehungsweise eine Einsatzempfehlung haben und sich zu einer verschlusssachenfähigen Cloud zusammensetzen lassen. Auf dieser Plattform läuft SCOPE, ein wichtiger Baustein für solche Analysen. So verbinden wir die Stärken souveräner Player und schaffen Mehrwert, ohne für das Gesamtsystem jedes Mal eine vollständig neue Zulassung zu benötigen. Ziel ist es, vorhandene Technologien sinnvoll zusammenzuführen, sodass das Ergebnis mehr leistet als die Summe seiner Einzelteile.

Auf der AFCEA Fachausstellung haben Sie auch einen Gemeinschaftsstand mit CGI zum Thema Operationsplan Deutschland. Wie sind Sie da engagiert?
Im Grunde handelt es sich um eine Lösung, welche die SINA-Technologie von secunet mit Managed Services von CGI kombiniert und die bei der NATO zum Einsatz kommt. Im Kern ist es ein gehärtetes Laptop von uns, integriert in einen Koffer der CGI, den man im Handgepäck in eine zivile Flugzeugkabine mitnehmen kann und der zusätzlich eine autonome Stromversorgung und eine Konnektivitätslösung mit unter anderem Kabelmodem, WLAN und 5G für terrestrische Netze sowie ziviles und militärisches SATCOM enthält. Egal welche Verbindung vor Ort verfügbar ist, man kann sie nutzen und weltweit auf mehreren Domänen bis GEHEIM- beziehungsweise NATO-SECRET-Ebene arbeiten.
Gemeinsam mit unserem Partner CGI wollen wir diese Fähigkeit as a Service anbieten, weil auch die NATO nicht mehr die Kapazität hat, alles selbst zu administrieren. Das wird besonders relevant, wenn im Ernstfall deutlich mehr Beteiligte mit VS-NfD oder höher eingestuften Informationen arbeiten müssen. Ein solches Angebot könnte auch national im Rahmen des Operationsplans Deutschland zum Zuge kommen, um unterschiedlichen Nutzern mobile Kommunikation mit hoch eingestuften Daten flexibel zu ermöglichen.

Zum Thema Kompatibilität und Interoperabilität, nicht nur in Deutschland, sondern auch in Europa mit NATO-Partnern: Auch Ihre Lösung wird am Ende nicht die einzige sein. Haben Sie beim Design dieses Systems von vornherein einberechnet, dass Sie mit unterschiedlichen Systemen zusammenarbeiten müssen?
Genau das ist die Architektur und die Idee dahinter. Klappt es mit jedem System sofort? Nein. Aber mit dem Federated Mission Networking, kurz FMN, und der großen jährlichen Übung CWIX, der Coalition Warrior Interoperability Exercise, gibt es etablierte Formate, um das zu erproben. Dabei geht es nicht nur um Interoperabilität auf Hardware- und Software-Ebene. Mission Networking hat auch eine soziale und organisatorische Komponente: Wie tauschen Menschen Informationen aus? Wie funktionieren gemeinsame Prozesse? Deshalb kommen die Beteiligten zusammen und zeigen in Übungen, ob die Zusammenarbeit tatsächlich funktioniert.
Manchmal müssen Lösungen auch ad hoc verbunden werden. Viel gelernt haben wir mit dem FMN während des Bundeswehreinsatzes in Afghanistan, wo solche Ansätze bereits erfolgreich erprobt wurden. Durch diese Erfahrungen sind wir heute deutlich weiter. Aber out of the box läuft in diesem Umfeld nichts.

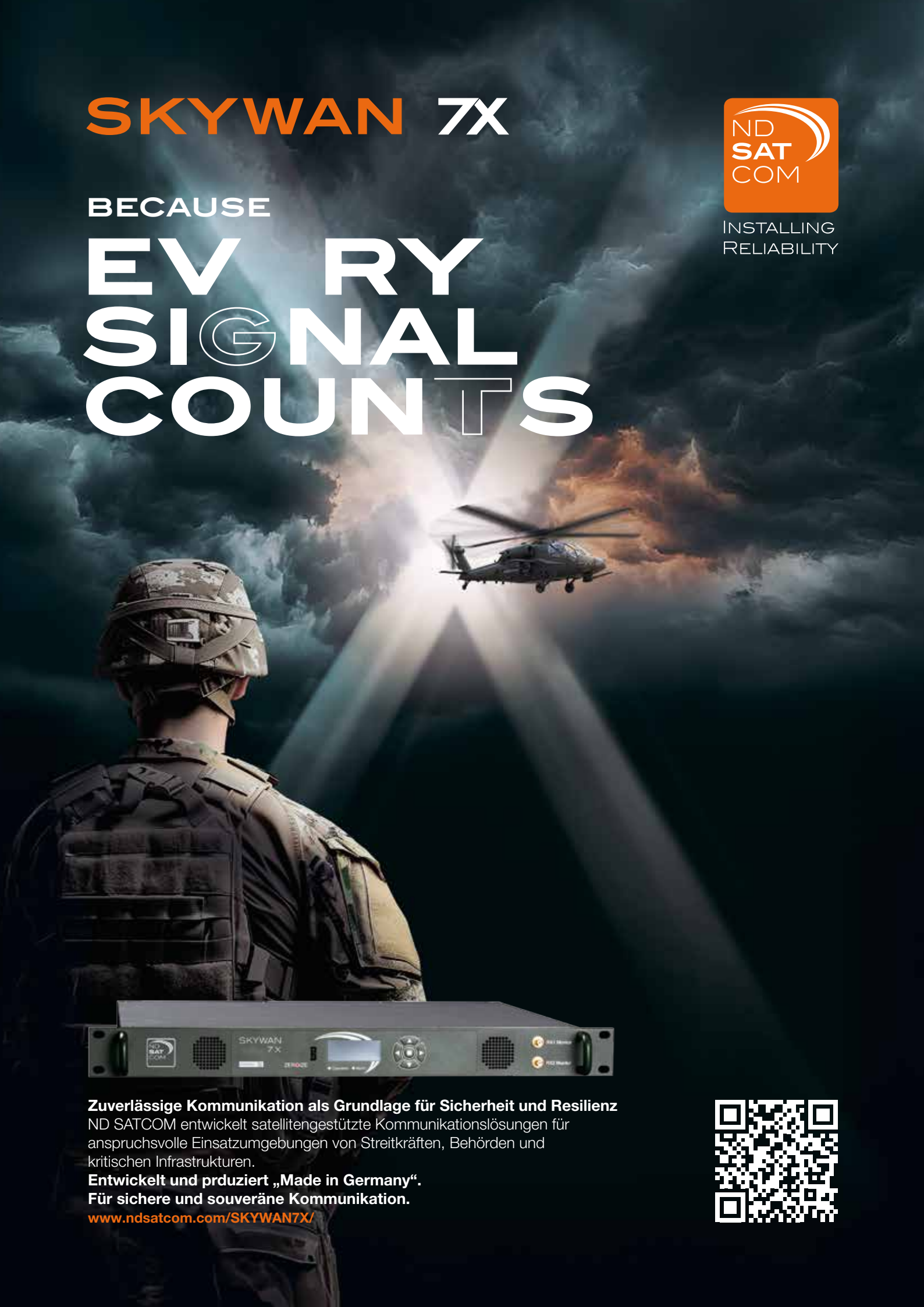
Wie sehen Sie unter dem IT-Aspekt die Lage in Deutschland insgesamt?
Wenn ich sehe, was wir als Community in Deutschland können, dann sind wir der Riese, der gerne ein Zwerg sein möchte. Wir können viel mehr, als wir uns zutrauen, und über Partnerschaften haben wir ein enormes Potenzial. Es fehlt nicht an Technologie, sondern an Mut, den Weg konsequent zu gehen. Das ist kein Vorwurf an Einzelne, sondern eine gemeinsame Bringschuld. Industrie wie öffentliche Hand dürfen mutiger werden. Unseren Teil dazu tragen wir bei.

SKYWAN 7X

ND SAT COM
INSTALLING RELIABILITY

BECAUSE

EV RY SIGNAL COUNTS



Zuverlässige Kommunikation als Grundlage für Sicherheit und Resilienz
ND SATCOM entwickelt satellitengestützte Kommunikationslösungen für anspruchsvolle Einsatzumgebungen von Streitkräften, Behörden und kritischen Infrastrukturen.
Entwickelt und prduziert „Made in Germany“.
Für sichere und souveräne Kommunikation.
www.ndsatcom.com/SKYWAN7X/

©MRI/Socrates Tassos (4)

Hardthöhen-KURIER

FÜR EIN STARKES EUROPA

Das Team des **Hardthöhenkuriers** bedankt sich bei den Organisatoren der AFCEA Bonn e.V. sowie den Ausstellern und Besuchern der Fachausstellung 2026 sehr herzlich für ihre Unterstützung und ihr Interesse!

©privat

Vielen Dank wiederum an unseren Fotografen Socrates Tassos für seine professionelle Arbeit!