AFCEA 2026

Fraunhofer-Leistungsbereich Verteidigung Vorbeugung und Sicherheit VS
dtec.bw – Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr

Behörden Spiegel in Zusammenarbeit mit AFCEA Bonn e. V.

TOUGHBOOK

TOUGH IS
JEDERZEIT ZUVERLÄSSIG DATENZUGRIFF ZU HABEN

12 HOURS

38999-CONNECTOR

IP66

Das **TOUGHBOOK 40** Tactical verfügt über ein spezielles Modul mit bis zu 3 militärischen Rundsteckern von roda computer und kann zusammen mit einem Shock-proof Mount nahtlos in militärische Ketten – und Radfahrzeuge integriert werden.

Kontaktieren Sie einen Panasonic-Spezialisten, um mehr über das **TOUGHBOOK 40** Tactical zu erfahren.

www.toughbook.eu

intel CORE ULTRA 7

Intel® Core™ i5-1345U vPro™ Processor

Windows 11

Panasonic CONNECT

Vorwort

Dr. Bernhard Günther, Geschäftsführer und CEO BWI GmbH

Dr. Bernhard Günther
Foto: BWI GmbH

Die deutsche Verteidigungsfähigkeit hängt maßgeblich davon ab, wie Deutschland die sicherheitspolitische Zeitenwende meistert. Dabei sind die größten Herausforderungen die schnellstmögliche Digitalisierung, um in künftigen Konflikten bestehen zu können, die Umstellung der digitalen Wirtschaft auf mehr Unabhängigkeit von ausländischer Hard- und Software und der Wandel der Sicherheits- und Verteidigungsindustrie von Manufakturleistungen zu standardisierter „Fließbandproduktion".

Das BMVg hat für das Jahr 2026 Investitionen von mehr als 108 Milliarden Euro in die äußere Sicherheit vorgesehen. Sondervermögen und der wachsende Verteidigungshaushalt außerhalb der Schuldenbremse sowie das NATO-Ziel machen in großem Umfang diese Ausgaben möglich. Gefordert werden neue Technologien und Lösungen für die volle Verteidigungsfähigkeit, aber vor allem auch resiliente und redundante Systeme. Dazu sollen die produktiven Systeme bis 2029 der Bundeswehr zur Verfügung stehen. In den kommenden Jahren soll die Summe auf rund 152 Milliarden Euro für den Haushalt des Verteidigungsministeriums steigen. Gegenüber dem Jahr 2023 entspricht das einer Verdreifachung.

Die Sicherheits- und Verteidigungsbranche wird so zu einem „Boomsektor" inmitten einer schwächelnden Wirtschaft. Doch wir sollten uns bewusst sein: Das Verteidigungsbudget steigt zwar, wird aber nicht eins zu eins wie bisher verwendet werden. Und dennoch werden wir aufgrund des schieren Umfangs an Anforderungen und Leistungen mit knappen Mitteln umgehen müssen.

Erfolgskritisch wird darum, wie dafür ein optimiertes Zusammenspiel zwischen Bedarfsträgern und Bedarfsdeckern in der Bundeswehr, zwischen Bundeswehr und Industrie gelingt. Das benötigt Mut und Willen zur Transformation sowie uns als Überzeugungstäter. Der Boom der Sicherheits- und Verteidigungsbranche hat auch eine staatsbürgerliche Bedeutung.

Die 39. AFCEA Fachausstellung bringt uns dafür zusammen und hoffentlich einen Schritt weiter. Geben wir unserem Land etwas zurück!

Inhalt

Impressum Sonderheft Behörden Spiegel „AFCEA 2026“
Redaktionelle Leitung Oberst a. D. Thomas Hönig, Behörden Spiegel
Herausgeber (presserechtlich verantwortlich) Dr. Eva-Charlotte Proll, Behörden Spiegel-Gruppe
Verlag ProPress Verlagsgesellschaft mbH, Friedrich-Ebert-Allee 57, 53113 Bonn, 0228/970970; Berlin, Kaskelstraße 41, 10317 Berlin, 030/55741200
Layout Yonca Bilgi, ProPress Verlagsgesellschaft mbH
Anzeigenleitung Dr. h.c. Jennifer Großblotekamp, Behörden Spiegel
Herstellung ProGov GmbH
Titelbild ProGov GmbH unter der Verwendung von BAIVECTOR, stock.adobe.com
Druck Köllen Druck + Verlag GmbH, Bonn
Magazinpreis 7,50 Euro

www.behoerdenspiegel.de

AFCEA als DefTech-Antwort in der gesamtstaatlichen Verteidigung

Generalmajor Armin Fleischmann, Vorsitzender AFCEA Bonn e.V., Abteilungsleiter Planung CIR und Digitalisierung der Bundeswehr und BEA Weltraum CIR

Generalmajor Armin Fleischmann

Foto: Bundeswehr

Die 39. AFCEA Fachausstellung stellen wir in diesem Jahr unter das Motto: „Vernetzt denken und sicher handeln als Antwort einer gesamtstaatlichen Verteidigung“. Als AFCEA Bonn e.V. gehen wir damit bewusst auf die Breite ein, die das Thema gesamtstaatliche Sicherheit und Verteidigung nach der Feststellung der sicherheitspolitischen Zeitenwende in 2022 erfahren hat. Wir erkennen an, dass es viele staatliche und gesellschaftliche Akteure benötigt, um das Ziel – die Antwort – einer gesamtstaatlichen Verteidigung zu erreichen. Es ist gleichzeitig nicht damit getan, nur darüber zu denken, sondern eben auch zu handeln. Gesamtstaatlich verteidigungsfähig zu werden, ist viel Arbeit, für die wir nur wenig Zeit haben.

„Vernetzt denken und sicher handeln als Antwort einer gesamtstaatlichen Verteidigung“. Das Thema hat AFCEA Bonn e.V. bewusst gesetzt, wohlwissend, dass AFCEA Bonn e.V. darin nur einen Beitrag rund um technologische Themen spielt und besetzt. Defence Tech ist „unser“ Betätigungsfeld. Als AFCEA sind wir die führende Austauschplattform für den Dialog von Bundeswehr, Sicherheitsbehörden, Verwaltung, Wissenschaft und Industrie. Übergeordnetes Ziel ist die erfolgreiche Umsetzung der digitalen Transformation unserer nationalen Sicherheitsarchitektur. Genauso bewusst ist uns, dass wir das Feld nicht alleine und nur gemeinsam mit anderen Akteuren bearbeiten können.

„Vernetzt denken und sicher handeln als Antwort einer gesamtstaatlichen Verteidigung“. Das ist auch nicht das Motto einer AFCEA Fachausstellung allein, sondern prägt unsere Veranstaltungen und andere Aktivitäten über das ganze Jahr. Mit unserem Jahresprogramm wollen wir für alle Beteiligten zusammenstellen, wie Sicherheit einerseits heute organisiert ist, anderseits welche technologischen Elemente, Wirkzusammenhänge und Ordnungsprinzipien erforderlich sind, um Sicherheit, Resilienz und Handlungsfähigkeit gesamtstaatlich künftig wirksam mit welchen Technologien und Lösungen zu ermöglichen.

Warum unser Blick auf „Defence Tech“? Wirksame gesamtstaatliche Sicherheit setzt nicht nur institutionelle Leistungsfähigkeit voraus, sondern auch auf gesellschaftliche Akzeptanz, Vertrauen, Mitwirkung und vorbereitetes Verhalten der Bevölkerung, ohne die staatliche Maßnahmen ihre Wirkung nicht entfalten können. Bei gesamtstaatlicher Verteidigung müssen wir immer mit Fähigkeiten und Technologien das Zusammenwirken staatlicher, ziviler, militärischer, wirtschaftlicher und gesellschaftlicher Akteure koordinieren und resilient sicherstellen. Fähigkeiten und Technologien sind essenzieller Teil von Sicherheit, Handlungsfähigkeit und Widerstandskraft des Staates vor, während und nach Krisen und Konflikten.

Ein solches Zusammenspiel – nennen wir es gesamtstaatliches Sicherheitsökosystem – ermöglicht frühere Lageerkennung, bessere und schnellere Entscheidungen sowie wirksameres Handeln über Organisations-, Ressort- und Ebenengrenzen hinweg, weil Fähigkeiten, Rollen und Technologien systemisch gekoppelt statt einzeln optimiert werden. AFCEA Bonn e.V. mit seinen Mitgliedsfirmen leistet seinen Beitrag, damit Gesellschaft, Staat und Bundeswehr die notwendige Resilienz gegenüber den Bedrohungen erreichen und unsere nationale Souveränität stark genug und technologisch führend ist.

In diesem Jahr tragen wir diesen Beitrag durch Fähigkeiten und Technologien mit einer Zusammenstellung eines technologischen Zielbilds eines solchen gesamtstaatlichen Sicherheitsökosystems zusammen. Das Ergebnis werden wir im Herbst zum zweiten Bonner IT-Dialog vorstellen. Das ist „Vernetzt denken und sicher handeln als Antwort einer gesamtstaatlichen Verteidigung“ – ganz konkret gemacht.

Das Sonderheft „AFCEA 2026“ gibt ebenfalls bereits Antworten aus verschiedenen Perspektiven, die traditionell unser Vorstand im ersten Teil des Hefts einbringt. Konkret listet Ron Simon, unser Leiter Programm, auf welche Themen der Informations- und Kommunikationstechnologie es jetzt ankommt (Seite 10). Als unsere Stimme der Industrie fordert Vorstand Marc Akkermann zur Umsetzung moderner Verteidigungsfähigkeit mehr Kooperation statt Bürokratie. Digitale Resilienz ist längst Teil der Abschreckungs- und Verteidigungslogik (Seite 12).

Weg von bunten Marketingdarstellungen gehen unsere Emerging Leaders unter Leitung von Anna-Lena Hohmann, die in diesem Heft einen Einblick gibt, wie unsere Nachwuchskräfte sich mit Künstlicher Intelligenz beschäftigen (Seite 18). Dass es jedoch ohne gezieltes Marketing nicht geht, zeigt Jochen Reinhardt, Vorstand für Presse- und Öffentlichkeitsarbeit (Seite 20).

AFCEA-Vorstandsmitglied Christopher Gaube spannt den Bogen zwischen Mensch und Technologie. Er zeigt auf, welche Faktoren für eine schnelle und wirksame Fähigkeitsentwicklung notwendig sind. (Seite 16)

Die 39. AFCEA Fachausstellung bündelt als Flaggschiffveranstaltung all diese Themen, Lösungen und bietet den Raum für den Austausch. Zum sechsten Mal öffnet sie

am 12. und 13. Mai 2025 im World Conference Center Bonn (WCCB) ihre Tore. Hier treffen mehrere tausend Teilnehmer aus Besuchern und Standpersonal von über 250 Ausstellern zusammen. Unser Symposium im Plenarsaal des alten Bundestages beschäftigt sich in Vorträgen und Podiumsdiskussionen mit unseren Themenfeldern, ergänzt durch fachliche Firmenvorträge. Das zeichnet die Ausstellung aus. Über die konkrete Ausgestaltung gibt Wolfgang Quirin, Leiter der Fachausstellung eine Orientierung (Seite 26).

„Vernetzt denken und sicher handeln als Antwort einer gesamtstaatlichen Verteidigung“ – das Wirken als gesamtstaatliche Sicherheitsökosystem zeigt sich auf der AFCEA Fachausstellung besonders, wenn Ämterseite, Industrie und Wissenschaft engagiert zusammen Lösungen entwickeln und umsetzen, damit die digitale Transformation unserer nationalen Sicherheitsarchitektur gelingt. Durch AFCEA Bonn e.V. als neutrale, nationale Austauschplattform kommen Bedarfsträger, Bedarfsdecker, Industrie und Wissenschaft zusammen.

Gemeinsam werden wir an diesen Tagen der 39. AFCEA Fachausstellung wieder viele Antworten auf gesamtstaatliche Verteidigung geben!

Ich freue mich auf Ihren Besuch und das Networking!

Jetzt Scannen!

Hier gehts zum Jahresprogramm 2026!

AFCEA Vorstand und Aufgaben

Unter Leitung des Vorsitzenden steuert der Vorstand in Abhängigkeit eines Jahresthemas die Aktivitäten des Vereins.

Vertretungsberechtigter Vorstand nach §26 BGB

Generalmajor Armin Fleischmann,
Vorsitzender

Ron Simon,
Stv. Vorsitzender und Leiter Programm

Marc Akkermann,
Stv. Vorsitzender und Leiter Industriebeirat

Weitere Mitglieder mit ihren Zuständigkeiten

Thomas Wirsching, Geschäftsführer,
Schatzmeister, Veranstaltungsmanagement

Christopher Gaube,
Ausbildung und Schulförderung

Generalleutnant a. D. Dr. Ansgar Rieks,
Internationale Zusammenarbeit

Kevin Thiele,
Sicherheitsbehörden

Jochen Reinhardt,
Presse & Medien

Wolfgang Taubert,
Berlin & Internationales

Dr. Michael Gerz,
Wissenschaft und Forschung

Nils Merkle,
Industrie

Anna-Lena Hohmann,
Emerging Leaders AFCEA Bonn e.V.

Christian Rösch,
Schriftführer

Christine Skropke,
Internationale Netzwerke

Annika Harpering,
Innovation & Mentoring

Brigadegeneral Tim Zahn,
Bundeswehr

Fotos: Homepage AFCEA Bonn e.V.

Die AFCEA-Geschäftsstelle

Das Team der Geschäftsstelle

Thomas Wirsching
Geschäftsführer, Schatzmeister, Veranstaltungsmanagement

Bernward Sondermann
Mitgliederbetreuung, Adressdatenbank, Veranstaltungsunterstützung

Beate Jaedicke
Buchhaltung, Veranstaltungsunterstützung

Gerhard Groth
Unterstützung Veranstaltungsmanagement

Das Team der Geschäftsstelle ist für Sie da

In allen Fragen zur Satzung, Geschäftsordnung, Mitgliedsbeitragswesen, Anmeldung/ Organisation von AFCEA-Veranstaltungen unterstützt Sie das Team der Geschäftsstelle in unserem Büro auf dem Hardtberg in Bonn.

AFCEA Bonn e.V. | Borsigallee 2, 53125 Bonn
Mo – Do 08:30 Uhr – 14:30 Uhr
Fr 08:30 Uhr – 12:30 Uhr

buero@afcea.de
+49 228 925 82 52
www.afcea.de

Day ZERO ist Jetzt! Wo stehen wir?

Ron Simon, AFCEA Bonn e.V. Stv Vorsitzender & Leiter Programm und Programmdirektor für die Digitalisierung militärischer IT-Systeme BWI GmbH

Ron Simon

Foto: privat

Die sicherheitspolitische Landschaft Europas hat sich dramatisch verändert, und die Herausforderungen, denen wir uns gegenübersehen, erfordern eine grundlegende Neuausrichtung unserer Verteidigungsstrategien. Die Zeit der isolierten nationalen Verteidigungsanstrengungen ist vorbei. Nur durch ein engeres Zusammenwachsen und eine verstärkte Zusammenarbeit können wir in der Lage sein, unsere Sicherheit effektiv zu gewährleisten. Ein Blick auf die aktuellen Konflikte zeigt, dass sich auch die Art der Kriegsführung verändert hat. Moderne Waffen wie die Panzerhaubitze, einst ein Symbol konventioneller Stärke, muss im oft asymmetrischen Kontext als Teil eines Gesamtsystemansatzes bestehen. Die Notwendigkeit, in innovative Technologien zu investieren, ist somit offensichtlicher denn je. Moderne Kriegsführung verlangt nach Lösungen, die nicht nur leistungsfähig, sondern auch anpassungsfähig und vernetzt sind. Der Einsatz von Technologien wie Künstlicher Intelligenz, automatisierter Systeme, gemeinsamer Informationsräume, mobiler sowie sicherer Infrastruktur und fortschrittlicher Sensorik kann einen entscheidenden Vorteil im Gefecht liefern.

Um diese technologischen Fortschritte voll auszuschöpfen, müssen wir auch unsere Bündnisse stärken. Ein zentraler Aspekt dabei ist die Entwicklung und der Einsatz multinationaler IT-Systeme. Durch die Vernetzung unserer Streitkräfte und die gemeinsame Nutzung von Informationen können wir eine effektivere und koordinierte Verteidigung aufbauen. Darüber hinaus müssen wir uns von der Vorstellung isolierter Teilsysteme verabschieden und stattdessen in vernetzten Gesamtsystemen denken. Nur so können wir die komplexen Herausforderungen der modernen Kriegsführung bewältigen. Dies erfordert eine enge Zusammenarbeit zwischen den Mitgliedstaaten, eine Harmonisierung von Standards und Verfahren sowie eine gemeinsame Vision für die Zukunft der europäischen Verteidigung.

Die aktuelle Situation erfordert von uns nicht weniger als einen Paradigmenwechsel. Wir müssen bereit sein, alte Denkmuster zu hinterfragen, neue Technologien zu nutzen und enger denn je zusammenzuarbeiten. Nur so können wir ein starkes, geeintes und verteidigungsfähiges Europa mit unseren Partnern schaffen. Dies alles darf aber nicht dazu führen, dass wir uns hinter Problembeschreibungen, Konzeptionen, Schuldzuweisungen und Definitionen verstecken. Wir müssen die Herausforderungen, die vor uns liegen akzeptieren, und die Herausforderungen eines Gesamtsystemansatzes überwinden.

Aufbruch in eine neue Ära der Verteidigung

Wir als Verein AFCEA Bonn e.V. treiben den Austausch von Themen der Informations- und Kommunikationstechnologie voran. Wir müssen zusätzlich zu der inkrementellen Verbesserung bestehender Systeme auch disruptive Innovationen zulassen und dabei Security by Design von Anfang an mitdenken, um somit einen entscheidenden Vorsprung zu erlangen. Die Vermaschung von IT-Systemen und eine uneingeschränkte Vernetzung sind dabei unerlässlich. Die Vision der Bundeswehr heißt Multi-Domain-Operations. Dies bedeutet, dass wir in der Lage sein müssen, Operationen über alle Domänen hinweg – Land, See, Luft, Weltraum und Cyberraum vom Sensor bis hin zum Effektor – nahtlos zu integrieren und zu koordinieren. Die Datenübertragung und Datenfusion spielen eine entscheidende Rolle in der modernen Kriegsführung. Ein multinational nutzbarer Informationsraum rückt in den Fokus, um die Zusammenarbeit mit unseren Partnern zu verbessern. AI-Enabled Automated Warfare wird ein weiterer Schwerpunkt sein, da künstliche Intelligenz das Potenzial hat, die Art und Weise, wie wir Kriege führen, grundlegend zu verändern.

Projekte wie D-LBO und FCAS bilden dabei einen wichtigen Startpunkt. Wir müssen diese Projekte nutzen, um die Verzahnung von Rüstung und IT voranzutreiben. Die Bundeswehr muss dabei klare Vorgaben an Schnittstellen definieren, um die Vernetzung, Vermaschung und Interoperabilität von Sensoren und Effektoren für die Zukunft zu gewährleisten. Der einschränkende Blick auf äußere Sicherheit ist bei der Umsetzung dabei nicht zielführend, denn nur der Ansatz eines Gesamtsicherheitsökosystems spannt den Lösungsraum über alle notwendigen Partner. Im Zuge dieser Entwicklungen müssen wir uns kritische Fragen stellen: Sind wir technologisch festgefahren? Halten wir zu viel an Altsystemen fest? Wo stehen wir in Bezug auf die Verteidigungsfähigkeit Europas mit unseren Partnern?

Day ZERO ist jetzt! Wo stehen wir im Gesamtsystemansatz?

Das Jahresprogramm 2026 wird sich dieser Fragestellung stellen und somit einen Beitrag zur Entwicklung einer zukunftsfähigen Verteidigung leisten.

Luftraumsicherheit im Fokus: Mit BOREADES wird ZMZ 4.0 wirklich wirkungsvoll

Der gesamtgesellschaftliche Ansatz der Zivil-Militärischen Zusammenarbeit (ZMZ) muss angesichts der neuen Bedrohung durch Drohnen systematisch um eine Dimension erweitert werden: die des Luftraums im Nah- und Nächstbereich von kritischen Anlagen (ZMZ 4.0). Drohnenabwehr wird damit ein integraler Baustein aller Stufen des ZMZ-Kontinuums (drei Stufen Frieden–Krise–Krieg). Im Zentrum steht die gezielte Erweiterung der Führungs- und Lagekompetenz auf den Luftraum.

Vier Erfolgsfaktoren sind für ZMZ 4.0 entscheidend:

- Ein behördenübergreifendes Echtzeit-Luftlagebild ermöglicht schnelle und fundierte Analysen sowie Entscheidungen.
- Moderne C-UAS-Lösungen lassen sich nahtlos in bestehende Leitstellen und Entscheidungsstrukturen integrieren.
- Eine klare rechtliche und organisatorische Verankerung der Drohnenabwehr muss jede Stufe des ZMZ-Kontinuums abdecken und durch zuverlässige Defence-as-a-Service-Modelle ergänzt werden.
- Der Schutz kritischer Infrastrukturen sowie von Großveranstaltungen erfordert interoperable C-UAS-Fähigkeiten in zentralen ZMZ-Handlungsfeldern wie Sicherheit und Logistik.

Mit **BOREADES** liefert **Sopra Steria** hierfür eine sofort verfügbare, skalierbare C2-Lösung: Sensorfusion (Radar, RF, EO/IR) und KI ermöglichen ein integriertes, behördenübergreifendes Luftlagebild und unterstützen durchgängige, koordinierte Entscheidungsprozesse auf taktischer Ebene. Eine weitere Stärke von BOREADES ist, dass sich die Lösung reibungslos in bestehende Systemlandschaften über die Standards SAPIENT und Link 16 integrieren lässt.

Sopra Steria unterstützt den Einsatz des Systems mit umfangreichen Services wie Beratung und Systemintegration, technischem Betrieb, Trainings und Simulationen sowie Projektmanagement über den gesamten Lebenszyklus. Damit stärkt BOREADES die Resilienz der staatlichen Sicherheitsarchitektur maßgeblich.

Verteidigungsfähigkeit als gesamtstaatliche und digitale Aufgabe

Marc Akkermann, Stv. Vorsitzender und Ltr IBR bei AFCEA Bonn e.V. und Head of Public Defense & Vice President bei Capgemini Deutschland GmbH

Marc Akkermann
Foto: privat

Deutschland erlebt eine sicherheitspolitische Zeitenwende, die längst über politische Willensbekundungen hinausgehen muss. Der Krieg gegen die Ukraine, hybride Bedrohungen in allen Sphären und die Verwundbarkeit kritischer Infrastrukturen (wie zuletzt beim Stromausfall in Berlin) haben die Begriffe der Resilienz und Verteidigungsfähigkeit wieder in den Mittelpunkt nationaler Verantwortung gerückt – ebenso wie die Tatsache, dass hier zwischen gewünschter Fähigkeit und aktuellem Status eine erhebliche Lücke besteht.

Der Kern dieser Lücke ist kein Mangel an Erkenntnis, sondern ein Mangel an Umsetzung Deutschland verfügt über das Wissen, die Strukturen und die Technologien, um sich und seine Partner effektiv zu schützen – doch es fehlt an Geschwindigkeit, an verbindlicher Koordination und an einer klaren gesamtstaatlichen Architektur der Verantwortung. AFCEA Bonn e.V. ist eine – wenn nicht DIE – Plattform, in der wesentliche Akteure zur Gestaltung und Umsetzung dieser Verantwortung zusammenkommen. Daher sollten wir die kommende Fachausstellung und die darauffolgenden Formate nutzen, um die folgenden Aspekte zu beleuchten und „anzupacken“ wo immer möglich. Verteidigungsfähigkeit ist kein exklusives Thema der Bundeswehr. Sie ist eine gesamtstaatliche und gesamtgesellschaftliche Aufgabe, die weit über die klassische militärische Dimension hinausgeht. Sie betrifft Versorgungssicherheit, Logistik, Cyberabwehr, digitale Souveränität, industrielle Resilienz und Krisenkommunikation gleichermaßen.

Ein Verteidigungsfall im digitalen Zeitalter wird nicht an der Landesgrenze beginnen, sondern im Netz, in Lieferketten, in Verwaltungsinfrastrukturen oder auf Desinformationsplattformen. Damit wird deutlich: Ohne funktionsfähige Zusammenarbeit zwischen Bund, Ländern, Wirtschaft und Zivilgesellschaft existiert keine verteidigungsfähige Nation.

Grenzen im Denken und Handeln, die aus Ressort-Gedanken oder verschiedenen föderalen Ebenen entstanden sind, verhindern eine neu gedachte und an die heutigen Herausforderungen angepasste Sichtweise auf Verteidigungsfähigkeit und die damit einhergehenden Maßnahmen in Digitalisierung, Innovation und Organisation.

Die Bundesrepublik hat seit Jahrzehnten Strukturen aufgebaut, die Stabilität garantieren, aber selten Dynamik fördern. Diese institutionelle Trägheit behindert in einem Umfeld, in dem Reaktionsgeschwindigkeit und Adaptionsfähigkeit zu Überlebensbedingungen werden.

Dabei ist Digitalisierung – also das Kern-Portfolio der AFCEA-Community – ein essenzieller Bestandteil. Sie ist damit der Schlüssel, die bestehenden organisatorischen Grenzen aufzubrechen und die Voraussetzung für gesamtstaatliche Führungsfähigkeit und Entscheidungsdominanz. Deutschland braucht eine gemeinsame digitale „Umgebung“, in der Lageinformationen, Entscheidungen und Kräfteverfügbarkeiten sektorenübergreifend geteilt werden können – nicht nach Behördenlogik, sondern nach Operationslogik und zugänglich für alle relevanten Parteien.

Ein weiteres Defizit liegt im Verhältnis zwischen Staat und Industrie. Wir haben in unseren Rüstungs- und Technologieunternehmen ein erhebliches Innovationspotenzial und die Möglichkeit einer enormen Wertschöpfung aus der Expertise und Erfahrung – auch aus anderen Branchen, welches sich in partnerschaftlicher Zusammenarbeit ideal entfalten könnte. Allerdings werden diese Unternehmen häufig als Lieferanten, nicht als Mitgestalter gesehen und behandelt. Damit wird das vorhandene Potenzial erheblich reduziert.

Moderne Verteidigungsfähigkeit entsteht in der Kooperation, nicht in der Vergabeakte

Digitale Resilienz ist längst Teil der Abschreckungs- und Verteidigungslogik. Ein Land, das seine Daten, Netze, Infrastruktur und Sensorik schützen kann, ist weit schwerer zu destabilisieren als ein Land, das über Panzer und Drohnen, aber keine digitale Resilienz verfügt. Darum müssen Cyberabwehr, Informationssicherheit und digitale Verwaltungskapazitäten als integrale Elemente der Verteidigungsfähigkeit behandelt werden – nicht als technische Unterstützungsfunktionen.

Hier liegen wesentliche Herausforderungen vor uns:

- Aufbau eines nationalen digitalen Lagezentrums, das militärische, zivile und wirtschaftliche Sicherheitsdaten vernetzt;
- Einführung einer verbindlichen Krisenkommunikationsarchitektur zwischen Bund, Ländern, Kommunen und Betreibern Kritischer Infrastruktur;
- Förderung eines europäischen Ansatzes für sichere Cloud- und Datenräume für Verteidigung;
- Angepasste Applikationen an die jeweilige Operationslogik;
- Regelmäßige Übungen über Grenzen von Ressorts und Ebenen hinaus.

Damit wird Digitalisierung zum Fundament der Verteidigungsfähigkeit – nicht im Sinne der Eskalation, sondern im Sinne der nachhaltigen Handlungsfähigkeit.

Die Debatte über Verteidigungsfähigkeit darf sich nicht in Strukturen und Technologiediskussionen erschöpfen. Am Ende entscheidet Haltung.

- **Führung** bedeutet, nicht auf eindeutig perfekte Lösungen zu warten, sondern Entscheidungen zu treffen, die Fortschritt ermöglichen.
- **Mut** bedeutet, neue Wege zu beschreiten und auch Risiken einzugehen, um Sicherheit zu schaffen.
- **Konsequenz** bedeutet, vereinbarte Strategien auch durchzuhalten, wenn die Aufmerksamkeitsschleifen der Öffentlichkeit sich bereits anderen Themen zuwenden.

Deutschland hat die politische Rückendeckung und die finanzielle Basis gelegt – das Sondervermögen und die wachsenden Verteidigungsetats. Jetzt braucht es den institutionellen Willen, diese Mittel sichtbar in Wirksamkeit umzusetzen. Die Unternehmen der AFCEA-Community und die deutschen und europäischen Wirtschaftsteilnehmer allgemein bringen das Portfolio mit, die notwendigen Schritte anzugehen, Fähigkeiten aufzubauen und nachhaltige Resilienz und Adaptionsfähigkeit aufzubauen. Die Zeit zu handeln ist jetzt. Dafür braucht es unter anderem

- ein klares Mandat zur ressortübergreifenden Krisenführung;
- die Digitalisierung der Kommunikations- und Führungsstrukturen über alle Ebenen;
- eine Beschleunigungskultur für Innovation im Verteidigungsfeld;
- und eine enge, vertrauensvolle Partnerschaft zwischen Staat, Wissenschaft und Industrie.

AFCEA Bonn e.V. leistet hier als Kommunikations- und Netzwerkplattform einen wesentlichen Beitrag. Die Mobilisierung der Behörden und Ämter, in einen solchen Diskurs zu treten, ist wesentlich, um die oben beschriebenen gesamtstaatliche und gesamtgesellschaftliche Aufgabe zu meistern. Gerade diese haben sich teilweise in den letzten Jahren aber aus dem Dialog zurückgezogen.

Erneut: moderne Verteidigungsfähigkeit entsteht in der Kooperation, nicht in der Vergabeakte.

Deutschland muss zu einer sicherheitspolitischen Reife finden, die es erlaubt, angesichts realer Bedrohungen entschlossen, modern und vernetzt zu agieren. Das bedeutet: weniger Zuständigkeitsdebatten, mehr Handlungseinheit, weniger Planungsvorbehalte, mehr Führungswillen, um die Lücke zur Verteidigungsfähigkeit zu schließen.

Erneut: Der Kern dieser Lücke ist kein Mangel an Erkenntnis, sondern ein Mangel an Umsetzung.

Verteidigungsfähigkeit ist kein Zustand, den man erreicht und abhakt – sie ist ein dauernder Prozess der Anpassung und Erneuerung. Wenn wir diesen Prozess jetzt mit Entschlossenheit gestalten, wird Deutschland nicht nur wieder verteidigungsfähig sein, sondern führungsfähig in einem Europa, das seine Sicherheit selbst gestaltet – mit Führung, Mut und Konsequenz.

Sichere Software-Lieferketten als zentrale Voraussetzung für Software Defined Defence

Dr. Michael Gerz, Vorstand AFCEA Bonn e.V für Wissenschaft und Forschung,
Abteilungsleiter am Freunhofer FKIE

Dr. Michael Gerz

Foto: privat

Die Weiterentwicklung wehrtechnischer Systeme wird zukünftig verstärkt durch intelligente Algorithmen und den Einsatz Künstlicher Intelligenz vorangetrieben. Für den Leitgedanken, kontinuierlich neue softwarebasierte Fähigkeiten auf vorhandenen (Hardware-) Plattformen auszubringen, wurde der Begriff »Software Defined Defence« geprägt. Voraussetzung für Software Defined Defence sind Prozesse und eine IT-Infrastruktur, die es ermöglichen, Anpassungsbedarf aus dem Einsatz zu identifizieren, Softwaresysteme zu adaptieren und zu testen sowie Updates auszurollen. Softwareentwicklungsprozesse werden dabei zunehmend komplexer. Die Entwicklung und das Deployment von Software erstrecken sich über eine Vielzahl von Akteuren (Open Source Communities, Zulieferer und Integratoren aus der Industrie, unterschiedliche Organisationsbereiche beim Kunden). Die Sicherstellung der Integrität über die gesamte Software-Lieferkette hinweg ist von zentraler Bedeutung und gleichzeitig eine große Herausforderung. Im Rahmen des AFCEA Zukunfts- und Technologieforums wurden daher Ende 2025 aktuelle Fragestellungen zum Thema »Secure Software Supply Chain« betrachtet: Wie kann eine Software-Lieferkette unter Einbeziehung verschiedener Stakeholder umgesetzt werden? Welche Methoden lassen sich zur Identifizierung und Bewertung von Risiken in der Software-Lieferkette einsetzen? Bei der AFCEA-Veranstaltung wurden in Beiträgen der Bundeswehr, der Industrie und der Wissenschaft technische wie auch organisatorische Aspekte betrachtet. Im Folgenden werden ausgewählte Erkenntnisse vorgestellt.

Mit Hilfe gezielter Lieferketten-Attacken können Angreifer nicht nur einzelne Systeme, sondern potenziell eine Vielzahl von Systemen gleichzeitig ausschalten. In Zeiten der Künstlichen Intelligenz lassen sich dabei sehr schnell Exploits für neue Schwachstellen automatisiert erstellen. Die Bedeutung von digitalen Technologien und die Cyber-Risiken in Zusammenhang mit Software-Lieferketten hat auch die Europäische Union erkannt. Mit der zweiten Richtlinie zur Sicherung von Netz- und Informationssystemen (NIS-2) fordert sie Risikomanagementmaßnahmen in Bezug auf die Sicherheit der Lieferketten kritischer Informations- und Kommunikationsdienste und -Produkte. Um die Sicherheit von Software bewerten zu können, muss man zunächst wissen, was überhaupt darin enthalten ist. Während es in der Lebensmittelbranche selbstverständlich ist, dass für alle Produkte die Inhaltsstoffe detailliert ausgewiesen sind, gibt es eine entsprechende Kennzeichnungspflicht in der Softwareentwicklung bislang nicht. Dabei ist es von zentraler Bedeutung, alle verwendeten Module und Bibliotheken einer Software zu kennen. Eine der größten Schwachstellen in der Geschichte der Softwareentwicklung betraf die Bibliothek „Log4j“, die für die Protokollierung in Java-Anwendungen sehr populär ist. Sie ist in unzähligen Bibliotheken im Einsatz, die wiederum Teil von größeren Modulen oder Anwendungen sind. Als im Jahr 2021 eine kritische Sicherheitslücke identifiziert wurde, trieb alle Verantwortlichen nur eine Frage um: „Ist „Log4j“ in meiner Software verbaut und wenn ja, in welcher Version?“

Die Erstellung einer sogenannten „Software Bill of Materials“ (SBOM), also einer maschinenlesbaren Stückliste aller Softwarekomponenten und ihrer Versionen, ist keine triviale Aufgabe. Der Build-Prozess für eine Software kann sehr komplex sein und verschiedene Programmiersprachen umfassen. Und was, wenn die Software gar nicht im Quellcode vorliegt, sondern nur als Installer oder Container-Image? Dann muss eine SBOM in jedem Fall durch eine Analyse der Binärdateien ermittelt werden. Dabei können verschiedene Erkennungsverfahren eingesetzt werden. Neben Datei-Hashes können Zeichenketten im Datensegment und Byte-Folgen im Code-Segment von Binärdateien ausgewertet werden. Bei der Anwendung entsprechender Analysetools kommt es nicht nur darauf an, dass alle Komponenten und deren Versionen korrekt und vollständig erfasst werden. Es ist ebenso wichtig, dass die Werkzeuge auf Softwarebestandteile hinweisen, die sie nicht eindeutig identifizieren können.

Dynamische und statische Analyse von Firmware

Eine besondere Form der Software stellt Firmware dar, die in unterschiedlichsten Systemen – von Firewalls und Druckern über Funkgeräte und Telefone bis hin zu Sensoren – verbaut ist. Firmware kann sowohl unbeabsichtigte Schwachstellen als auch Schadsoftware und Hintertüren für gezielte Angriffe enthalten. Für die Analyse von Firmware bieten sich sowohl statische als auch dynamische Verfahren an. Zur statischen Analyse zählt etwa die Suche nach hinterlegten Passwörtern. Bei einer dynamischen Analyse wird untersucht, welche Funktionen/Dienste der Firmware in welcher Konfiguration aufgerufen werden, um dann zu entscheiden, ob potenzielle Schwachstellen ausgenutzt werden können. Firmware stellt eine besondere Herausforderung für sichere Lieferketten dar. In der Regel verfügt nur der Hersteller über den Quellcode. Dies erschwert die Analyse, zumal Firmware nicht auf Standard-IT-Systemen ausführbar ist. Ebenso ist die Dokumentation typischerweise unvollständig vorhanden.

Daher ist bei Verträgen mit Integratoren und Zulieferern ein transparenter und gewissenhafter Umgang bei der Erkennung und Behebung von Schwachstellen sicherzustellen.

Bedeutung von Governance und Lifecycle-Management von Daten

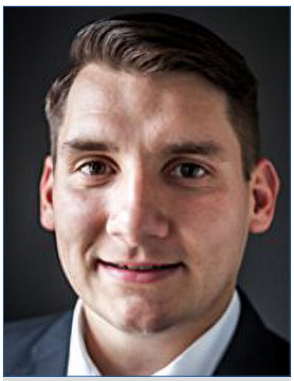
Auch auf die spezifischen Anforderungen an Lieferketten bei KI-Anwendungen, die z. B. ein regelmäßiges Nachtraining erfordern, wurde in verschiedenen Vorträgen eingegangen. Bei der Erstellung von KI-Modellen durch maschinelles Lernen ergeben sich eine Vielzahl neuer Risiken entlang der Entwicklungskette, die sowohl eigenes Fehlverhalten als auch Angriffe durch Dritte betreffen. So können bereits bei der Erhebung von Trainingsdaten falsche Annahmen über den operationellen Einsatz getroffen werden oder die Daten können einen Bias enthalten. Auch das bewusste Poisoning (Manipulation) von großen KI-Modellen birgt eine große Gefahr. Bereits mit wenigen manipulierten Trainingsdaten kann dabei erheblicher Schaden erzeugt werden. Eine wichtige Rolle spielt daher die Governance und das Lifecycle-Management von Daten, das die Phasen „Erfassung“, „Validierung“, „Speicherung & Versionierung“, „Nutzung“ und „Archivierung“ umfasst.

Konzept für die kontinuierliche Adaptierung souveräner KI-Infrastruktur

Wie eine souveräne KI-Infrastruktur für den Einsatz und im Einsatz aussehen kann, wurde anhand eines aktuellen Bundeswehrprojekts dargestellt. Die Infrastruktur soll es ermöglichen, KI-Modelle der Industrie nicht nur auszurollen, sondern auch anhand aktueller Daten nachzutrainieren, um sie kontinuierlich an veränderte operationelle Anforderungen zu adaptieren. Grundidee ist dabei ein sogenanntes Stage-Konzept, das die Schritte „Entwicklung & (Nach-) Training“, „Verifikation und Validierung“, „Integration in Systeme“, „KI-Modell- und Datenmanagement“, „Einsatz/Übungen“ und „Einsatznahes Nachtraining“ umfasst und bei dem die Verantwortung und die Entwicklungsumgebung je nach Stage bei der Industrie oder der Bundeswehr liegt. Hierbei sind technische Voraussetzungen wie z. B. eine sichere Trainingsumgebung, Zugriffskontrolle, Daten-Sanitarisierung und Auditierung sowie reproduzierbare Trainingspipelines zu erfüllen. Darüber hinaus ist einerseits eine klare Rollenverteilung zwischen den verschiedenen Stakeholdern erforderlich. Andererseits ist eine kooperative Übernahme von Aufgaben durch Industrie und Bundeswehr für den Erfolg zentral. So muss beispielsweise die wehrtechnische Industrie für die Entwicklung KI-basierter Systeme kontrollierten Zugang zu hochwertigen, kuratierten Daten der Bundeswehr bekommen. Vor der Nutzung von KI-Modellen im Einsatz sind diese einer umfangreichen Validierung und Verifizierung zu unterziehen. Dabei ist die Einhaltung von Einsatzvorschriften und geltendem Recht ebenso zu prüfen wie ethische Fragestellungen.

Faktoren für eine schnelle und wirksame Fähigkeitsentwicklung: Mensch und Technologie

Christopher Gaube, Vorstand AFCEA Bonn e.V. und Country Lead Defense Germany Capgemini und
Gero Wülfken, Business Analyst Defense Capgemini Deutschland GmbH

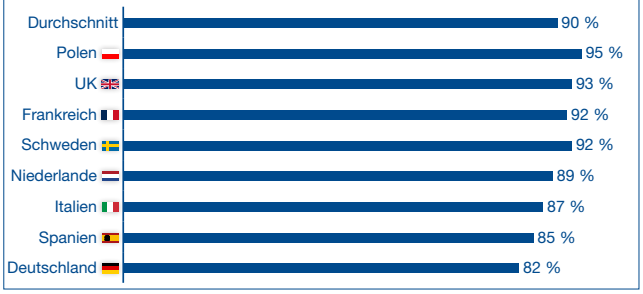


Christopher Gaube
Foto: privat

Gero Wülfken
Foto: privat

Wenn Schwärme günstiger Kleindrohnen Angriffe im Minutentakt ermöglichen, entscheidet nicht mehr allein pure Masse über Schutz und Wirkung, sondern das Tempo, in dem Hardware, Sensorik, Software und Menschen gemeinsam reagieren. Deutschlands Verteidigungsfähigkeit wird sich daher weniger an zusätzlicher Hardware messen lassen, sondern daran, wie schnell Fähigkeiten aus Daten, Code und Ausbildung in den Einsatz gelangen. „Code over steel" heißt in der Praxis: Die Softwarekomponente gibt den Takt vor und wertet Systeme laufend auf – im Feld, in der Instandsetzung, in der Produktion. Dabei bleibt der Mensch im Prozess immer die relevante Instanz. In Europa steigen dafür die Investitionen; politisch flankiert wird dies durch das Ziel, die Verteidigungsbereitschaft bis 2030 deutlich zu erhöhen. Entscheidend bleibt jedoch, wie schnell softwaredefinierte Ansätze Wirkung entfalten. Passend dazu findet jährlich die AFCEA Fachausstellung statt: Sie bringt Menschen aus Bundeswehr, Behörden, Industrie und Forschung zusammen, fördert den Austausch und beschleunigt Kooperationen.

Prozent der aktiven Soldaten in verschiedenen Ländern, die der Aussage zustimmen: „Die Zusammenarbeit von Mensch und Maschine wird in den nächsten zehn Jahren einen Vorteil auf dem Schlachtfeld bringen"



Umfrage zu den europäischen Streitkräften, Oktober 2025, N = 555 aktive Militärangehörige
Quelle: Capgemini Research Institute

Was „Code over steel" für Deutschland bedeutet, lässt sich klar beschreiben: Personal, Zeit und Budget sind endlich; die Komplexität wächst. Der skalierbare Hebel ist Software Defined Defense – Systeme, die über modulare Architekturen, offene Schnittstellen und verlässliche Datenflüsse kontinuierlich verbessert werden. Damit rückt der Mensch als Entscheider in den Mittelpunkt. Technologie soll ihn nicht ersetzen, sondern augmentieren: durch bessere Lagebilder, schnellere Auswertung, Assistenz bei Disposition und Versorgung sowie realitätsnahe, datenbasierte Ausbildung. In europäischen Streitkräften gilt Human Machine Teaming bereits als Schlüssel für den Vorsprung im Gefecht der verbundenen Kräfte; viele sehen darin den Treiber künftiger Abschreckung, während softwaredefinierte Technologien wichtiger werden als reine Truppenstärke. Die Drohnenabwehr, Counter Unmanned Aircraft Systems (C-UAS), ist dafür die härteste Schule. Die Ukraine hat gezeigt, wie Dynamik und Skalierung im Drohnenkrieg Spielregeln verschieben – von der Aufklärung über elektronische Kampfführung bis zu Abwehrketten, die sich laufend anpassen. Für Deutschland folgt daraus zweierlei. Erstens: Es braucht echte Entscheidungsüberlegenheit – Datenfusion aus Sensoren am Boden, auf Fahrzeugen und in der Luft, KI-gestützte Mustererkennung und robuste Führungs- und Kommunikationsnetze, die selbst in umkämpften Umfeldern funktionieren. Zweitens: Iterationen müssen radikal kürzer werden – Updates, Taktikanpassungen und Zulassungen in Wochen statt Jahren, flankiert von Trainingszyklen, die neue Verfahren unmittelbar in die Truppe tragen. Softwaredefinierte Technologien sind hier der Hebel, um Komplexität zu beherrschen, Entscheidungszyklen zu verkürzen und knappe personelle Ressourcen spürbar zu entlasten.

Drei Hebel machen den Unterschied:

- Entlastung der Truppe: Automatisierung repetitiver Tätigkeiten – von Datensichtung über First-Level-Support bis Logistik – schafft Zeit für Kernaufgaben, reduziert Fehler und erhöht die Verfügbarkeit. KI-gestützte Assistenzsysteme senken die kognitive Last; agentische KI kann Routineprozesse in sicheren Grenzen übernehmen, bleibt aber menschlich beaufsichtigt.
- Beschleunigte Entscheidungen: Mit Datenfusion, Simulation und Szenarioplanung werden OODA-Loops (Beobachten, Orientieren, Entscheiden, Handeln) verkürzt. Einsatzführung, Sensor-to-Shooter-Ketten und Wirkmitteldisposition laufen kohärenter – ein Vorteil in Lagen, in denen Minuten zählen. Softwaredefinierte Systeme erlauben schnelle, risikobegrenzte Anpassungen „over the air".

- Skalierbare Industrie: Digitale Zwillinge, additive Fertigung, vorausschauende Instandhaltung und vernetzte Lieferketten erhöhen die Ausbringung ohne jahrelange Neubauten und halten Systeme länger einsatzbereit. Viele Entscheider sehen KI und Daten als Schlüssel für den Produktionshochlauf, auch wenn die breite Umsetzung noch hinter den Ambitionen zurückliegt.

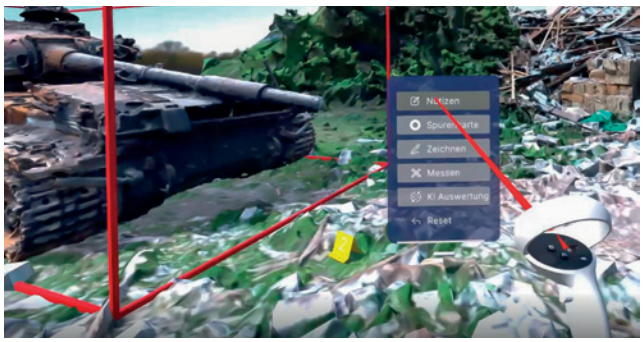
Wer „Code over steel“ operationalisieren will, muss Piloten schnell in Fähigkeiten überführen. Das ist eine doppelte Aufgabe: Zum einen braucht es mehr softwarezentrierte, updatefähige Produkte, die über offene Standards anschlussfähig sind und in kurzen Zyklen reifen. Zum anderen muss die Produktion selbst smarter werden – mit digitalen Zwillingen, datengestützten Prüfpfaden und automatisierten, rückverfolgbaren Releaseprozessen. Beides gelingt nur, wenn Bedarfsträger, Beschaffung, Nutzer und Industrie ein gemeinsames digitales Rückgrat aufspannen: modellbasierte Anforderungen statt monolithischer Pflichtenhefte, durchgängige Datenmodelle vom Entwurf bis zur Truppe sowie klare Regeln für Sicherheit und Interoperabilität; ergänzt um effect based Procurement, das Wirkung misst statt Dokumente zu verwalten.

Konkrete Ableitungen für die C-UAS-Fähigkeitsentwicklung liegen auf der Hand. Ein vernetztes Lagebild muss optische, akustische, RF- und Radarquellen zusammenführen und durch KI priorisieren – von Objekterkennung bis Störsignalkorrelation. Offene Schnittstellen sichern die Anschlussfähigkeit neuer Sensoren und erleichtern das Zusammenspiel mit bestehenden Führungs- und Wirksystemen. Elektronische Abwehr und Effektoren sollten als Softwareprodukt gedacht werden: Parameter- und Profilupdates „over the air“ passen Taktiken an neue gegnerische Verfahren an, erhöhen die Wirksamkeit pro investiertem Euro und verlängern die Nutzungsdauer der Hardware. In der Ausbildung heben Mixed-Reality- und Simulationsumgebungen das Training auf ein neues Niveau, wenn reale Telemetriedaten einfließen und Operatorinnen und Operatoren mehrere Sensor- und Wirkmittelsysteme als Team mit KI-Unterstützung führen. Im Betrieb senken digitale Zwillinge sowie prädiktive Analytik Ausfallraten und entlasten das Personal – spürbar gerade in verteilten Komponentenketten.

Diese Prinzipien tragen über den Verteidigungsbereich hinaus. Wer Lagen schnell bewerten und Maßnahmen priorisieren muss – ob im Bevölkerungsschutz oder bei der polizeilichen Lageverarbeitung – profitiert von digitaler Kontinuität entlang des Einsatzprozesses, von iterativen, kleinteiligen Auslieferungen mit klaren Wirkungshypothesen und von systematischer Befähigung der Mitarbeitenden. Menschen machen heute und auch zukünftig den Unterschied, weil sie Technik in Wirkung übersetzen.

Für Deutschland verdichtet sich daraus ein Dreisatz: erstens ein einheitliches digitales Rückgrat von der modellbasierten Anforderung bis in den Betrieb; zweitens integrierte, nutzerzentrierte Teams, in denen Erprobungsdaten unmittelbar in Designentscheidungen fließen; drittens eine Industrie, die sich selbst augmentiert – mit KI-gestützter Planung, adaptiven Produktionszellen, durchgängiger Qualitätssicherung und digitalen Zwillingen.

Am Ende entscheidet die Zeitenwende sich nicht an der Frage, wie viel beschafft wird, sondern wie. Wer Fähigkeiten als Zusammenspiel von Mensch, Daten und Software denkt, entfaltet schneller Wirkung – im C-UAS-Schutz, in der Führung, in der Logistik und darüber hinaus. „Code over steel“ ist ein Arbeitsprinzip: updaten statt umrüsten, integrieren statt isolieren, befähigen statt überlasten. Und bei allem gilt: Der Mensch behält die Kontrolle. Genau diesen Austausch über Technik, Verfahren und Menschen fördert die AFCEA Fachausstellung – sie bringt die Akteure zusammen, die diese Entwicklung mit Leben füllen.



Training mit VR-Brille, Capgemini Deutschland GmbH.
Bild: Demonstrator Augmented Reality

Ein Blick in den KI-Maschinenraum

Anna-Lena Hohmann, Vorstand AFCEA Bonn e.V. Emerging Leaders und Senior Managerin at PwC Deutschland

Anna-Lena Hohmann
Foto: PwC

Schluss mit bunten Marketingdarstellungen. Es ist längst Zeit für eine technische, detaillierte Auseinandersetzung mit Künstlicher Intelligenz (KI). Denn KI verändert die Spielregeln im Bereich Sicherheit und Verteidigung. Sie ermöglicht adaptive, lernfähige Systeme, die Bedrohungen antizipieren und Entscheidungen in Echtzeit treffen können. Diese Transformation erfordert mehr als nur technologische Entwicklung: Sie verlangt Vertrauen, unternehmerische Exzellenz und eine klare Einbettung in demokratische Werte. Mit dieser Vision im Blick haben die Emerging Leaders des AFCEA Bonn e.V. in Zusammenarbeit mit GovTech Deutschland und Bitkom e.V. die Fachveranstaltung zum Thema „Defense & Security AI uncovered – ein Blick in den KI-Maschinenraum“ ausgerichtet. Das etablierte Veranstaltungsformat der Emerging Leaders entwickelt sich zu einem festen Treffpunkt für die DefTech Community.

Am GovTech Campus in Berlin kamen Vertreterinnen und Vertreter aus Bundeswehr, Behörden, Wissenschaft und der Tech-Szene zusammen, um die Chancen und Herausforderungen von KI im sicherheitskritischen Umfeld zu diskutieren. Die zentrale Frage: Wie verändert Künstliche Intelligenz sicherheitsrelevante Aufgaben in Staat und Verteidigung? Die Veranstaltung bot Raum für Antworten und Debatten rund um technologische Grundlagen, strategische Implikationen und organisatorische Fragen an konkreten Anwendungsfällen. Das Ziel: Brücken bauen zwischen etablierten Expertinnen und Experten sowie innovativen Unternehmen. Der Vorsitzende des AFCEA Bonn e.V., Generalmajor Armin Fleischmann, eröffnete die Veranstaltung und bezeichnete KI als den größten „Game Changer“ in der modernen Verteidigung. In seiner Eröffnungsrede rief er dazu auf, gemeinsam an einer intelligenten Verteidigungsfähigkeit „Made in Germany“ zu arbeiten.

Diesem Aufruf folgten die Teilnehmenden in vier parallelen Working Sessions, die konkrete Anwendungsfälle Künstlicher Intelligenz in den Mittelpunkt stellten: HENSOLDT demonstrierte, wie KI-gestützte Detektion und Multi-Kamera-Tracking von Landfahrzeugen die Lageerfassung verbessern. Capgemini & Edgeless Systems stellten vor, wie semantische Auswertung von Satellitenbildern mithilfe von KI-Agenten neue Möglichkeiten für die Geodatenanalyse eröffnet. Sopra Steria präsentierte gemeinsam mit der Polizei Niedersachen den Einsatz moderner Computer-Vision-Technologien zum Schutz kritischer Infrastrukturen. Walaris zeigte, wie Drohnenerkennung und -verfolgung bei Nacht durch KI-basierte Bildverarbeitung die Überwachung sensibler Bereiche verbessert. Die Demonstrationen und anschließenden Diskussionen machten deutlich, dass KI längst mehr als ein Buzzword ist. Sie ist ein Werkzeug, das – richtig eingesetzt – Sicherheit neu definiert. Neben den inhaltlichen Impulsen war die Veranstaltung ein Ort des Austauschs. Die ausgebuchte Veranstaltung und das positive

Generalmajor Fleischmann eröffnet die Fachveranstaltung „Defense & Security AI uncovered – ein Blick in den Maschinenraum“. *Foto: AFCEA Bonn e.V.*

Teilnehmerinnen und Teilnehmer der Fachveranstaltung. *Foto: AFCEA Bonn e.V.*

Feedback zeigen: Dieses Format fernab von Frontbeschallung trifft einen Nerv. Vielen Dank für die Gastfreundschaft von GovTech Deutschland, die Unterstützung von Bitkom und allen Vortragenden sowie Teilnehmenden. Die nächste Ausgabe für das Jahr 2026 ist bereits in Planung.

Über die Emerging Leaders von AFCEA Bonn e.V.: Die Emerging Leaders sind die junge Generation von AFCEA Bonn e.V.: Mitgliedern bis zum 40. Lebensjahr bieten wir eine Plattform zum Aufbau des beruflichen Netzwerks und zum fachlichen Austausch und leisten dadurch einen Beitrag zur Modernisierung, Digitalisierung und Souveränität von Bundeswehr und Sicherheitsbehörden. Kontakt für Fragen und Interessensbekundungen: ela@afcea.de

Organisation: AFCEA Bonn e.V. Emerging Leaders – Teresa Ritter, Justus Groth, Nemo Buschmann, Jakob Lennertz, Anna Lena Hohmann (Vorsitzende).

Gesamtstaatliche Sicherheit zwischen Marktschreiern und Dialog

Jochen Reinhardt, AFCEA Bonn e.V. Vorstand Presse & Medien, Leitung Communications & Marketing BWI GmbH

Jochen Reinhardt
Foto: BWI GmbH

Die eigene und die öffentliche Wahrnehmung ist für die Verbesserung der gesamtstaatlichen Verteidigung Deutschlands ein mächtiger Gegner. Die Situation ist klar: Um auf die „Zeitenwende“ zu reagieren, muss zügig und über die kommenden Jahre in „Resilienz“, „Kriegstüchtigkeit“ und höhere „Verteidigungsfähigkeit“ investiert und die nationale Sicherheitsarchitektur neu ausgerichtet werden. Erreicht ist das Ziel einer neuen, besseren gesamtstaatlichen Verteidigung bislang nicht.

Nicht nur in der Medienberichterstattung folgen der Ukraine-Krieg und die sicherheitspolitische Zeitenwende dem typischen Wahrnehmungszyklus. War zu Beginn das Thema durch hohes Interesse und intensive Berichterstattung geprägt, flacht sie über die Zeit deutlich ab und wird auch kritisch hinterfragt. Das ist unabhängig davon, wie sich etwa der tatsächliche Krieg in der Ukraine entwickelt. Oder wenn Resilienzmaßnahmen aus der Sicherheitsstrategie außerhalb dieses Wahrnehmungszyklus stattfinden, drohen sie überhaupt nicht wahrgenommen zu werden. Das Thema „nutzt“ sich ab, ohne dass es in der Realität erledigt wäre.

Die diesjährige AFCEA Fachausstellung widmet sich dem Thema „Vernetzt denken & sicher handeln als Antwort einer gesamtstaatlichen Verteidigung“ und versucht damit, dem ermüdenden Blick auf dieses große Thema zu begegnen. Doch vernetzt denken, wenn dies jahrzehntelang nicht der eigenen Erfahrung und Notwendigkeit entsprach, teils sogar nicht gewünscht war und der Fokus nur begrenzt liegt, ist schwierig, sicheres Handeln als Antwort auf multiple Krisen und Unsicherheiten zu geben, eine herausfordernde Aufgabe.

In den achtziger Jahren prägten die beiden Forscher James Grunig und Todd Hunt ein vierphasiges Modell der Kommunikation. Es beschreibt ursprünglich die Entwicklung von Kommunikation, wurde jedoch schnell genutzt, die Art von Kommunikation zu beschreiben, da verschiedene Phasen gleichzeitig zu finden sind und ineinander übergehen.

1. Phase „Publicity“: Hier ist die erste und einzige Aufgabe Aufmerksamkeit zu erreichen, der Wahrheitsgehalt ist nachrangig. Das ist marktschreierische Propaganda.
2. Phase „Information“: Hier geht es um die Vermittlung von Inhalten. Die Informationen sind korrekt, jedoch ausschließlich als Ein-Weg-Kommunikation vom Sender zu den Empfängern ausgerichtet.

In den beiden folgenden Phasen des Kommunikationsmodells entsteht auch ein Rückkanal, hier handelt es sich um eine Zwei-Wege-Kommunikation.

3. Phase „Asymmetrische Kommunikation“: Hier ist das Ziel, zu überzeugen, der Sender geht dafür tatsächlich in den Austausch, als Sender jedoch ohne die Absicht, sich und sein Verhalten zu ändern.
4. Phase: „Symmetrische Kommunikation“: Hier ist das Ziel ein echter Dialog mit der Bereitschaft, Rückmeldungen in sein eigenes Verhalten umzusetzen.

Öffentlichkeitsarbeit gilt dabei als erfolgreich, wenn sie für beide Seiten einen Nutzen generiert. In der Wahrnehmung und Kommunikation rund um die gesamtstaatliche Verteidigung zeigt sich eine hohe Gleichzeitigkeit dieser Phasen – weswegen ich dieses „alte“ Modell in diesem Beitrag aus dem Methodenkoffer ziehe.

„Publicity“ prägt viele Themen und die Wahrnehmung in der politischen Diskussion und auf Social-Media-Plattformen. Der Wahrheitsgehalt spielt keine Rolle, 2017 prägte eine Beraterin des US-Präsidenten dafür treffenderweise den Begriff der „alternative facts“. Dadurch erodiert in der politischen Debatte der gemeinsame, akzeptierte Grund, was Tatsachenrealität ist. Meinung ersetzt Fakten, Wissenschaft wird ein Interpretationsangebot unter vielen. Was bleibt, ist ein reiner Kampf um Aufmerksamkeit, befeuert durch die Logik der Medienberichterstattung und der Reichweite in den Sozialen Medien, die ausschließlich Aufmerksamkeit belohnt. Verschärfend kommt hinzu, dass Akteure sich Publicity und Propaganda bedienen, um gegen das Ziel besserer gesamtstaatlicher Verteidigung zu agieren. Gleichzeitig sind Bereiche unserer Gesellschaft in den vergangenen Jahren vom Austausch und dem gemeinsamen

Der Autor im Austausch mit jungen Teilnehmern der AFCEA Fachausstellung 2025. *Foto: AFCEA Bonn e.V.*

Finden von Lösungen geprägt. Die Zwei-Wege-Kommunikation ist fundamentaler Bestandteil von politischen Aushandlungsprozessen und gesellschaftlicher Teilhabe ohne Basta-Ansagen. In der gesamtstaatlichen Verteidigung, wo Organe der inneren und äußeren Sicherheit in neuer Intensität zusammenwirken müssen – insbesondere ohne zentral steuernde Instanz, ist diese Form der Kommunikation unerlässlich.

Was bedeutet das für die kommunikative Begleitung des Themas gesamtstaatliche Verteidigung und sicheres Handeln? Ziel kann es nicht sein, selbst auf Publicity ohne Wahrheitsgehalt zu setzen oder damit darauf zu reagieren. Mit dem Anspruch auf Wahrheit kann – oder gar muss – jedoch das „mächtige Schwert" der Aufmerksamkeit auch einmal gezogen werden. Niemals sollte es als alleiniges Mittel zum Zweck eingesetzt werden, sondern als Auftakt zur Aufmerksamkeitsgewinnung, um dann schnell in eine der Folgephasen der Kommunikation einzutreten. Das kann „Information" oder „Dialog" sein. Der Wechsel in einer inhaltlich geprägten Kommunikationsphase setzt voraus, dass dafür Vorbereitungen getroffen worden sind: Die zu kommunizierenden Inhalte müssen recherchiert und zielgruppengerecht aufbereitet sein, die Kanäle und ihre Formate müssen ausgewählt und bespielbar sein, kurzum: Ein Plan muss stehen und umgesetzt werden können. Aufmerksamkeitsspannen sind heute kurz, Algorithmen darauf ausgerichtet. Das Fenster zur Wahrnehmung beträgt nicht selten nur noch wenige Stunden.

Ein Beispiel einer solchen Vorbereitung von Inhalten bietet „Deutschland macht Alarm". Diese Initiative stellt ein unabhängiges, nicht-kommerzielles Onlineportal zur Verfügung, das die wichtigsten öffentlichen Informationsangebote zum Thema ziviler und militärischer Krisen-, Zivil- und Katastrophenschutz übersichtlich bündelt – ohne eigene inhaltliche Wertung oder redaktionelle Einordnung. Die wichtigsten öffentlichen Informationen zum Krisen- und Katastrophenschutz sind dort übersichtlich und schnell verfügbar (https://www.deutschland-macht-alarm.de/index.html). Auch AFCEA Bonn e.V. widmet sich inhaltlich in diesem Jahr stärker dem Thema „Gesamtstaatliches Sicherheitsökosystem". Dabei geht der Verein über das reine Plattformangebot seiner Veranstaltungen hinaus und untersucht und beschreibt selbst, wie gesamtstaatliche Sicherheit wirkt. Die sicherheitspolitischen und sicherheitsrelevanten Herausforderungen unserer Zeit werden komplexer, dynamischer und systemischer. Immer deutlicher zeigt sich: Entscheidend ist nicht allein die technologische Leistungsfähigkeit, sondern die Fähigkeit zur Orchestrierung von Akteuren, Rollen und Fähigkeiten über Organisations- und Ressortgrenzen hinweg. Mit Tiefeninterviews, Auswertungen und Befragungen entwickelt AFCEA Bonn e.V. das Bild eines „Sicherheitsökosystem 2030" vor, während und nach Krisen. Im Mittelpunkt stehen Wirkungslogiken statt Zuständigkeiten, Fähigkeiten statt Produkte sowie Orchestrierung statt Einzeloptimierung.

Damit wird AFCEA Bonn e.V. bewusst in den Dialog gehen und neue Player für die gesamtstaatliche Sicherheit integrieren. In dem anfangs geschilderten Kommunikationsmodell bewegen wir uns damit in der „Symmetrischen Kommunikation", wo AFCEA Bonn e.V. in echten Dialog mit der Bereitschaft Rückmeldungen in Verhalten umzusetzen, geht. Das ist gesamtstaatliche Sicherheit, Verteidigung und Verantwortung einmal nicht marktschreierisch gedacht.

AFCEA Bonn e.V.

39. AFCEA Fachausstellung 2026

Technologiekompass für ein gesamtstaatliches Sicherheitsökosystem 2030

AFCEA Bonn e.V. widmet sich 206 mit einer eigenen Untersuchung den sicherheitspolitischen und sicherheitsrelevanten Herausforderungen unserer Zeit. Zum Bonner IT-Dialog am 6. und 7. Oktober wird der Verein dann einen Defence Tech Guide mit Technologiekompass vorstellen, der Wirkungslogiken, kritische Technologiedomänen und Fähigkeiten sowie die Orchestrierung vor, während und nach Krisen aufzeigt.

Die Publikationen und ihre Inhalte werden unabhängig, neutral und AFCEA-nah erstellt. Verschiedene Partner ermöglichen die inhaltliche Tiefe des Defence Tech Guides, sichern die breite Beteiligung relevanter Akteure in Tiefeninterviews und sichern die Qualität durch kurarierte Beiträge.

Die Partner sind (Stand April 2026):

Strategic Partner

ARVATO SYSTEMS · Google Cloud

Solution Partner

AIRBUS · CGI · secunet · bechtle · aws

Supporting Partner

infodas connect more. be secure. · CONET · roda RUGGED IT & ELECTRONICS

AFCEA Bonn e.V.

39. AFCEA Fachausstellung 2026

Breit angelegtes Begleitprogramm

Gemeinsam mit den Emerging Leaders der AFCEA Bonn e.V. gestaltet die AFCEA Fachausstellung 2026 ein vielseitiges Programm, das jungen Fach- und Führungskräften sowie Innovationsakteuren eine zentrale Plattform für Austausch, Impulse und Vernetzung bietet. Von Pre-Opening bis Pitch Session prägen sie zahlreiche Formate, die die Themen Innovation, Verteidigungsfähigkeit und Nachwuchsgewinnung in den Mittelpunkt stellen.

So findet bereits am Vortag der Fachausstellung ein exklusives Pre-Opening statt. Im Mittelpunkt stehen die inhaltliche Einstimmung auf die Messetage sowie informelles Networking. Besonders der Austausch zwischen jungen Fach- und Führungskräften aus Bundeswehr, Verwaltung, Industrie, Forschung und dem Innovationsökosystem erhält hier eine zentrale Plattform.

Auf der Ausstellungsfläche für Startups im Foyer des Plenargebäudes präsentieren an beiden Messetagen 17 Startups ihre innovativen Lösungen für die Verteidigungs- und Sicherheitsbranche. Die jungen Unternehmen wurden durch die Emerging Leaders ausgewählt. Begleitend dazu findet die Pitch & Panel Session statt: Vier ausgewählte Startups stellen im Plenarsaal sich und ihre Lösungen vor.

Vorträge von Behördenvertretern außerhalb der Industrievortragsreihe finden an beiden Ausstellungstagen statt. Dabei geben Vertreter des öffentlichen Dienstes Fachimpulse aus Behörden, Bundeswehr und BOS. Im Saal Berlin steht das Recruiting-Element zur Verfügung. Werben können Unternehmen aus dem Verteidigungs- und Sicherheitssektor um Nachwuchskräfte.

Die DefTech Night im GOP Varieté bildet eine exklusive Abendveranstaltung, bei der Austausch zu technologischen Innovationen und die Vernetzung zwischen Bundeswehr, Industrie, Forschung und Startup-Szene im Vordergrund stehen.

Einer der Höhepunkte der Fachausstellung bietet die Digital Defense Debate, ebenfalls organisiert und geleitet von den Emerging Leaders. Führende Personen des Verteidigungsökosystems diskutieren zentrale Herausforderungen der nationalen Verteidigungsfähigkeit und formulieren Impulse, um diese weiter zu stärken.

ELLEM – Ein immersiver KI-Assistent auf der AFCEA Fachausstellung 2026

Daniela Rittmeier, Head of AI Accelerator bei Capgemini Deutschland GmbH,
Stefan Pollack, Delivery Executive Public Defense bei Capgemini Deutschland GmbH

Daniela Rittmeier
Foto: Capgemini

Stefan Pollack
Foto: Capgemini

Im Eingangsbereich stellt er Informationen rund um die AFCEA Fachausstellung zur Verfügung und macht gleichzeitig Künstliche Intelligenz in Aktion erlebbar. Der von Capgemini bereitgestellte Avatar ELLEM ermöglicht diesen Zugang und unterstützt die Vermittlung der Inhalte durch dialogbasierte Interaktion.

Wie souveräne, dialogbasierte KI den Zugang zu Wissen neu gestaltet

Nachdem Künstliche Intelligenz bereits tagtäglich im Alltag genutzt wird, hält die Technologie zunehmend Einzug in Bereiche, in denen hohe Anforderungen an Sicherheit, Transparenz und Datenhoheit gelten. Während erste Anwendungen vor allem textbasierte Assistenzfunktionen abbilden, stellt sich die Frage, wie komplexes Fach- und Prozesswissen so bereitgestellt werden kann, dass es verständlich, vertrauenswürdig und sicher nutzbar ist.

Mit ELLEM wurde ein Ansatz entwickelt, der diese Fragestellung neu adressiert. ELLEM ist eine multimodale, immersive KI-Assistenz, die Sprache, Wissensverarbeitung und visuelle Darstellung kombiniert. Im Mittelpunkt steht nicht die Automatisierung um ihrer selbst willen, sondern der niedrigschwellige, kontrollierte Zugang zu kuratiertem Wissen.

Wer oder was ist ELLEM?

ELLEM ist Capgeminis sogenannte AI[wo]man: eine holografisch dargestellte, generative KI-Assistenz, mit der Nutzerinnen und Nutzer per Sprache interagieren. Anders als klassische KI-Assistenten greift ELLEM nicht auf offene Internetquellen, sondern auf vordefiniertes, organisations- oder branchenspezifisches Wissen zurück.

Dadurch wird ELLEM zu einem dialogorientierten Wissenssystem, das Inhalte nicht nur ausgibt, sondern sie auch kontextbezogen auf Basis des trainierten Wissens erklärt. Die visuelle Repräsentation in Form eines comicartigen Avatars dient dabei nicht dem Selbstzweck, sondern unterstützt die Verständlichkeit, Aufmerksamkeit und Akzeptanz – insbesondere bei komplexen Sachverhalten. Auf eine fotorealistische Repräsentation wurde bewusst verzichtet, um Irritationen wie Deepfakes oder das Uncanny-Valley-Phänomen zu vermeiden und Vertrauen aufzubauen sowie um mehr über die Zukunft der Mensch-Maschine-Interaktion zu erfahren. Zentral ist der Aspekt der Souveränität: Die zugrunde liegenden Daten verbleiben in der kontrollierten IT-Umgebung, werden von energieoptimierten, europäischen Small Language Models (SLM, Mistral AI) prozessiert und vollständig on premise, also lokal, betrieben. Für Verwaltungen ist dies ein entscheidender Unterschied zu vielen marktgängigen KI-Anwendungen und insbesondere für die Prozessierung von hochsicherheitsrelevanten Daten entscheidend.

Wie funktioniert ELLEM?

Technisch basiert ELLEM auf einer modularen Microservices-Architektur, die flexibel on premise, hybrid oder in der Cloud betrieben werden kann. Die Mensch-Maschine-Interaktion folgt einem klar strukturierten Ablauf: Gesprochene Anfragen werden zunächst lokal erfasst und mittels Sprach-zu-Text-Verfahren verarbeitet. Anschließend wird die Anfrage semantisch analysiert und mit relevanten Inhalten aus einer Vektor-Datenbank angereichert. Dieses als Retrieval-Augmented Generation (RAG) bekannte Verfahren stellt sicher, dass Antworten auf geprüften, nachvollziehbaren Quellen beruhen. Auf dieser Basis erzeugt das kleine, energieschonendere Sprachmodell, ein sogenanntes Small Language Model (SLM, LLM) eine Antwort, die wiederum in Sprache umgewandelt und von ELLEM ausgegeben wird. Der gesamte Prozess folgt dem Prinzip: Zuhören – Verstehen – Verarbeiten – Antworten. Sind keine Daten zu den Inhalten vorhanden, wird im Gegensatz zu klassischen AI-Anwendungen

Foto: Capgemini

ELLEM stieß auch auf dem Generative AI Summit 2025 auf das Interesse der Besucher. *Foto: Capgemini*

keine Antwort generiert, um Halluzinationen zu verhindern. Für den öffentlichen Sektor besonders relevant: Der Betrieb kann auf dedizierter Hardware erfolgen, ohne externe Datenabflüsse oder Abhängigkeiten von Drittanbietern.

Relevanz für Verwaltung und öffentliche Organisationen

ELLEM ist weniger Produkt, sondern ein Demonstrator, der einen Ausblick in die Zukunft der Mensch-Interaktion gibt und gleichzeitig das Antizipieren potenzieller KI-Anwendungsfälle unterstützt. Gerade in Verwaltungen mit stark regulierten Prozessen und umfangreichen Regelwerken zeigt sich das Potenzial dialogbasierter Systeme:

- Beschleunigung der Erschließung und Verarbeitung von Fachwissen;
- Nachvollziehbarkeit der Antworten auf Basis kuratierter Daten;
- Verringerung der Einstiegshürden vor und Steigerung des Vertrauens in KI-Anwendungen;
- Reduktion der Komplexität durch menschenähnliche Interaktion.

Insbesondere vor dem Hintergrund des Fachkräftemangels, der zunehmenden Arbeitsverdichtung und der notwendigen Wissenssicherung kann dieser Ansatz einen Beitrag zur organisationalen Stabilität leisten.

Entwicklung und Ausblick

ELLEM wurde seit Anfang 2024 kontinuierlich weiterentwickelt und für zahlreiche Innovations-, Branchen- und Verwaltungsveranstaltungen trainiert. Ziel ist, generative KI greifbar, erklärbar und vertrauenswürdig zu gestalten. ELLEM wurde so konzipiert, dass sie sowohl on-premises, in der Cloud als auch hybrid betrieben werden kann. Ihre modulare Architektur bildet die Grundlage für eine Vielzahl von KI-Systemen in allen Industrien und entlang der Wertschöpfungskette. Dieser Ansatz zeigt, wie KI-Systeme im öffentlichen Sektor in Zukunft aussehen könnten: interaktiv statt abstrakt, souverän statt intransparent und unterstützend statt ersetzend.

Infobox: Warum On Premise?

Der performante, lokale Betrieb von KI-Systemen ist sowohl für das produzierende Gewerbe als auch für die Bereiche Verteidigung, innere Sicherheit und öffentliche Organisationen keine Ausnahme, sondern eine Voraussetzung.

- Daten-Souveränität: Sensible sowie hochsicherheitsrelevante Fach und Personaldaten verlassen nicht die eigene Infrastruktur.
- Performanz und Nachhaltigkeit: Sogenannte Small Language Models (SLM) liefern vergleichbare, jedoch energieoptimierte Ergebnisse.
- Compliance: Bestehende Vorgaben zu Datenschutz, Geheimschutz und IT-Sicherheit bleiben uneingeschränkt einhaltbar.
- Nachvollziehbarkeit: Datenflüsse, Modelle und Wissensquellen sind transparent kontrollierbar.
- Unabhängigkeit: Keine Abhängigkeit von externen Plattformen, kurzfristigen Lizenzmodellen oder regulatorisch bedingten Änderungen.

Weitere Informationen zu ELLEM, ihren Anwendungsbereichen und ihrer technischen Architektur stehen über den Link: https://go.capgeminigroup.com/ellem oder QR-Code zur Verfügung:

AFCEA Fachausstellung 2026 für den Verteidigungs- und Sicherheitsbereich

Wolfgang Quirin, Oberst a.D., Leiter AFCEA Fachausstellung

Wolfgang Quirin
Foto: AFCEA Bonn e.V.

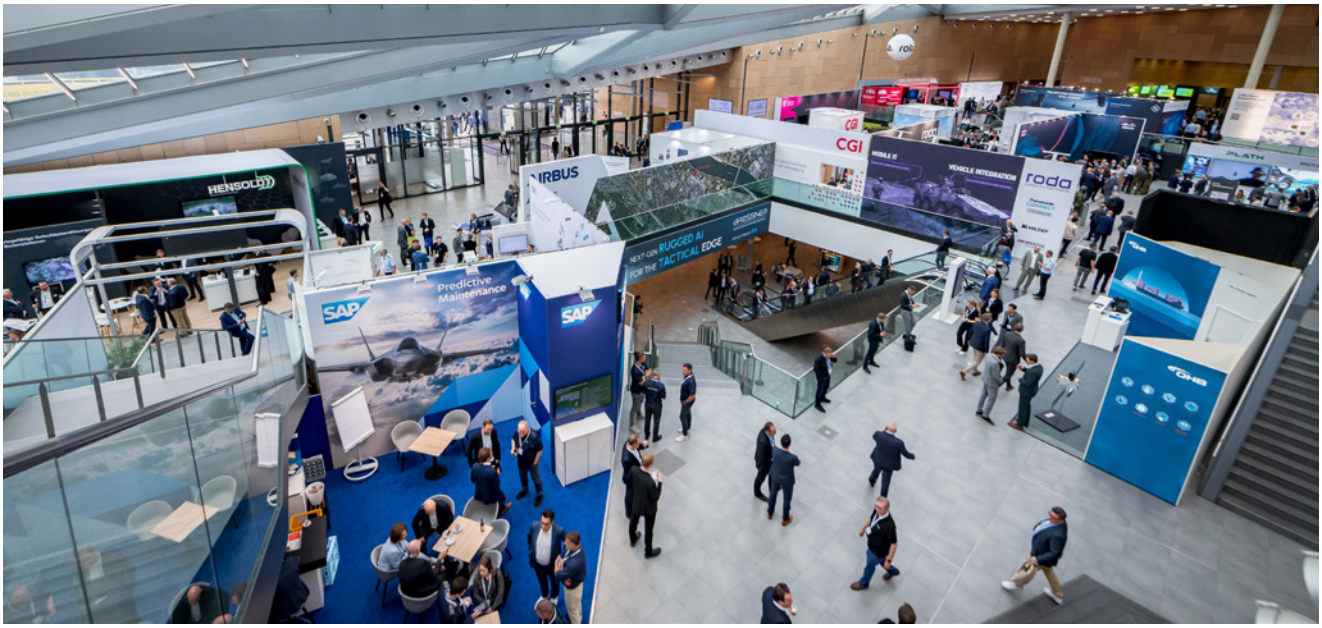
Unter der Überschrift „Vernetzt denken & sicher handeln als Antwort einer gesamtstaatlichen Verteidigung“ startet die AFCEA Fachausstellung 2026. Dabei stellt sich natürlich die Frage, was man unter vernetzt denken versteht und was eine gesamtstaatliche Verteidigung bedeutet. Vernetztes Denken in der Verteidigung ist der Ansatz, militärische Sicherheit als Teil eines komplexen Systems aus Politik, Wirtschaft und Gesellschaft zu verstehen. Dabei reicht rein konventionelle militärische Stärke nicht mehr aus. Benötigt wird eine gesamtstaatliche Strategie, die alle Bereiche eines States einbezieht und diese so vernetzt, dass eine sich ergänzende und nicht widerstrittige Symbiose in der Verteidigung des Staates und seiner Werte entsteht, um eine einheitliche Gefahrenabwehr zu erreichen.

Und gerade hier sehe ich die größte Herausforderung: Wie gelingt es, eine Gesellschaft so aufzustellen, dass sie trotz unterschiedlicher Denkansätze ein einheitliches Verständnis für die Verteidigung ihres Staates aufbringt, und dann auch Willens ist, diesen Staat zu verteidigen sowie die dazu erforderlichen Schlüsse zu ziehen und diese auch mit entsprechenden Gesetzen und Verordnungen umzusetzen.

So stellt sich nicht nur die Frage, ob unsere Gesellschaft auch verteidigungswillig ist, sondern auch, wie wir mit den modernen Herausforderungen eines Krieges umgehen. Angefangen von der zivilen, auch eigenverantwortlichen Vorsorge, über hybride Kriegsführung bis zu KI-gesteuerten Waffen. So experimentieren russische Firmen bereits am Einsatz von Tauben mit implementierten Chips zur Flugsteuerung oder chinesische Firmen mit dem Beeinflussen von Kleinlebewesen wie Schaben durch Mikrochips zur Bewegungssteuerung. Ein weiteres Feld der Bedrohung liegt in der Abhängigkeit von Rohstoffen und eingesetzten Techniken. Bei Rohstoffen gilt es schnellstmöglich alternative Bezugsquellen zu erschließen, keine einfache Sache, wenn die Zivilgesellschaft verlangt, auch hohe moralische Ansprüche in den Kriterienkatalog mit aufzunehmen. Anders bei der Abhängigkeit von Techniken und Softwareanwendungen. Wie schwer man sich tut, sahen wir bei der Diskussion um die Verwendung von Huawei-Produkten in der Informationstechnik. Nicht zu unterschätzen ist das Risiko der Abhängigkeit von Produkten der US-Tech-Konzerne. Was wäre, wenn plötzlich der Zugriff auf beispielsweise die Clouddienste von Microsoft oder Google nicht mehr möglich, der E-Mail-Verkehr etwa über Outlook betroffen oder Amazon plötzlich nicht mehr erreichbar wäre? Firmendokumente wären nicht mehr abrufbar, Lieferketten wären unterbrochen, Bestellungen wären nur noch eingeschränkt möglich und Termine sind nicht mehr auffindbar. Stellen wir uns dann noch vor, WhatsApp wäre gesperrt. Wie viele Chatgruppen laufen darüber, die nicht nur privaten Charakter haben. Und, nicht zu vergessen, den Stress, den Eltern zu Hause haben, wenn ihre Kinder plötzlich vom digitalen Leben abgeschnitten sind! Natürlich gibt es für alles Alternativen, diese müssen aber geplant und vom Willen getragen auch umgesetzt werden. Alternativen und Lösungsansätze zu technischen und militärischen Herausforderungen werden auf der AFCEA Fachausstellung 2026 vom 12. und 13. Mai 2026 im World Conference Center Bonn (WCCB) vorgestellt. Über 250 nationale und internationale Aussteller aus verschiedenen Branchen präsentieren ihre Lösungen – von großen Unternehmen bis hin zu spezialisierten Softwareanbietern. Start-ups erhalten erneut die Möglichkeit, auf einer neuen Ausstellungsfläche im Bereich des Plenargebäudes dem Fachpublikum und den etablierten Unternehmen ihre innovativen Ideen von Produkten und Dienstleistungen zu präsentieren.

Die Vortragsveranstaltungen werden auch in diesem Jahr wieder auf großes Interesse der Besucher treffen. *Foto: AFCEA Bonn e.V.*

Unbemannte Systeme fanden bereits bei der letzten Fachausstellung großes Interesse. *Foto: AFCEA Bonn e.V.*



Wie in den Vorjahren ist die Fachausstellung erneut voll ausgebucht. *Foto: AFCEA Bonn e.V.*

Seit ihrer Gründung im Jahr 1986 hat sich die Veranstaltung zu einer der wichtigsten Plattformen für Informations- und Kommunikationstechnologien in den Bereichen Verteidigung und innere Sicherheit in Deutschland entwickelt. Die Ausstellung wird 2026 bereits zum 39. Mal durchgeführt und bringt für zwei Tage Experten aus Bundeswehr, Behörden, Industrie und Wissenschaft zusammen.

Schwerpunktthemen der Fachausstellung

Die AFCEA Fachausstellung 2026 steht im Zeichen aktueller Herausforderungen:

- Cyberabwehr und Resilienz: Schutzmaßnahmen und Frühwarnsysteme sind angesichts zunehmender Cyberangriffe zentrale Themen.
- Künstliche Intelligenz und autonome Systeme: Es werden KI-basierte Anwendungen für Lagebilder, Entscheidungsunterstützung und unbemannte Systeme vorgestellt.
- Vernetzte Führungsfähigkeit: Im Fokus stehen Lösungen für interoperable Kommunikation und Datenintegration zwischen Streitkräften und Behörden.
- Digitale Transformation: Von Cloud-Architekturen bis zu sicheren Software-Supply-Chains – die Digitalisierung prägt sämtliche Bereiche.

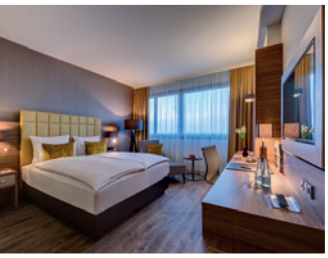
Rahmenprogramm und Services

Das WCCB bietet mit seinen modernen Räumlichkeiten die ideale Umgebung für die Präsentation neuester Technologien. Neben der Ausstellung erwartet die Besucher ein umfangreiches Vortragsprogramm mit Fachvorträgen und Paneldiskussionen. Ein besonderes Highlight sind die Veranstaltungen im alten Plenarsaal. Die Vortragsveranstaltungen werden auch in diesem Jahr wieder auf großes Interesse der Besucher treffen. Die Fachausstellung ist nicht nur eine Leistungsschau, sondern auch ein wichtiger Ort für Networking und Austausch. Über 6.000 Besucher, darunter Vertreter der Bundeswehr, von Behörden und aus der Industrie, nutzen die Gelegenheit, Kooperationen zu vertiefen und gemeinsame Projekte zu initiieren. So wird der Wissensaustausch gefördert und die nationale Sicherheitsarchitektur gestärkt. Mit der AFCEA Fachausstellung 2026 setzt der AFCEA Bonn e.V. erneut Maßstäbe für den Dialog zwischen Technologie und Sicherheit. Die Messe zeigt anschaulich, wie Innovationen die Einsatzfähigkeit der Streitkräfte und die Sicherheit öffentlicher Institutionen nachhaltig verbessern. Im neu gestalteten StartUp-Bereich zeigen junge Firmen innovative Ideen, denken Altbekanntes neu und präsentieren ihre Produkte und Dienstleistungen. Zur Orientierung stellt AFCEA Bonn e.V. auch 2026 wieder die „e-Kompetenzmatrix“ unserer Mitgliedsfirma CGI zur Verfügung. Damit können Besucher gezielt jene Aussteller finden, die zu spezifischen Themen die passenden Lösungen bieten. Diese Matrix erleichtert die Planung insbesondere angesichts der Vielzahl von über 250 Ausstellern. Als weiteren Service steht auch wieder die AFCEA-MesseApp, programmiert von unserer Mitgliedsfirma Capgemini, bereit. Sie bietet einen Überblick über das Programm, die Aussteller und Lagepläne – ein hilfreiches Tool zur Planung und Gestaltung des Messebesuchs. Wie auch im letzten Jahr findet auch diesem Jahr wieder ein Recruiting-Event statt. Berufsanfänger, Young Professionals sowie ausscheidende Zeit- und Berufssoldaten haben die Möglichkeit, attraktive Einstiegsoptionen in einem hochspezialisierten und zukunftsorientierten Sektor zu entdecken und direkt mit den Firmen in Kontakt zu kommen.

Wichtige Informationen im Überblick

Die Öffnungszeiten der Fachausstellung sind am 12. Mai von 09:00 bis 18:00 Uhr und am 13. Mai von 09:00 bis 17:00 Uhr. Am 12. Mai 2026 lädt AFCEA Bonn e.V. von 18:00 bis 22:00 Uhr zu einem Get-Together ein.
Der Eintritt ist nach Registrierung kostenfrei möglich.

MARRIOTT
BONN



MEHR ERFAHREN:

RAUM FÜR ENTSCHEIDUNGEN. ZUKUNFT BRAUCHT VERTRAUEN.

Business-Events und Tagungen erfordern ideale Bedingungen: Verlässlichkeit, Diskretion, moderne Technik und ein Umfeld, das konzentriertes Arbeiten ermöglicht.

Das Bonn Marriott Hotel bietet optimale Voraussetzungen für Konferenzen, Meetings und Business-Events.

Moderne, lichtdurchflutete Tagungsräume mit direktem Außenzugang, flexiblen Bestuhlungsvarianten und zeitgemäßer Veranstaltungstechnik schaffen Raum für Austausch, Strategie und Vernetzung. Ein erfahrenes Convention Sales Team begleitet Veranstaltungen professionell, von der Planung bis zur erfolgreichen Umsetzung. Vertraulich, zuverlässig und in sicheren Händen.

Kulinarisch eröffnen mehrere Restaurants und Bars vielfältige Möglichkeiten. Besondere Akzente setzt Konrad's Restaurant & Skybar: Private Dinner oder exklusive Meetings mit Blick über Bonn und den Rhein – vom Empfang auf der Dachterrasse über Snacks in der Bar bis hin zum Fine-Dining-Dinner.

Mit 336 Zimmern, Spa-Bereich mit Pool sowie einem 24/7-Fitnessstudio ist das Hotel zugleich ein optimaler Rückzugsort für Geschäftsreisende – funktional, komfortabel und zukunftsorientiert.

IHR BUSINESS. UNSER RAUM.

KONRAD'S
BONN

Platz der Vereinten Nationen 4 | 53113 Bonn | marriotthotels.com | www.konrads-bonn.de

BONNER IT DIALOG

by AFCEA Bonn e. V.

THEMA 2026

„Die Resilienz Deutschlands auf dem Prüfstand“

Aufbrechen von Grenzen im Sicherheitsökosystem einer gesamtgesellschaftlichen Verantwortung

WANN?	7. und 8. Oktober 2026
WO?	Maritim Hotel Bonn
WER?	Bis zu 1.200 Teilnehmende aus dem Umfeld Bundeswehr, Behörden, Organisationen mit Sicherheitsaufgaben, Sicherheits- und Verteidigungsindustrie
WAS?	Vorträge, Panels und Showcases im Kontext gesamtgesellschaftlicher Verantwortung
SCHIRMHERRIN	Mona Neubaur, Ministerin für Wirtschaft, Industrie, Klimaschutz und Energie sowie stellvertretende Ministerpräsidentin des Landes Nordrhein-Westfalen

AFCEA Bonn e.V.

- Deutschland übernimmt eine neue Schlüsselrolle in der europäischen Sicherheitsarchitektur. Aber sind wir darauf vorbereitet?
- In der sicherheitspolitischen Lage Europas nimmt Deutschland eine wichtige Rolle als „Drehscheibe Logistik“ wahr. Die mit dieser Rolle verbundene Verantwortung als Transitland und logistisches Rückgrat der NATO lässt sich nicht allein militärisch bewältigen.

  Sicherheit ist eine gesamtgesellschaftliche Aufgabe.
- IT ist ein wesentlicher Enabler für einen gesamtgesellschaftlichen Ansatz zur Erlangung einer hinreichenden Resilienz. Die Veranstaltung bringt alle dafür wichtigen Stakeholder einer resilienten Gesellschaft zusammen.
- Die zentrale Frage lautet: Wie halten Bundeswehr und Zivilgesellschaft gemeinsam die politische und gesellschaftliche Handlungsfähigkeit unter den Bedingungen einer hybriden Bedrohungslage aufrecht?

BONNER IT-DIALOG
by AFCEA Bonn e. V.

Tel. +49 (0) 228 925 82 52
E-Mail: buero@afcea.de

Informationen:
www.afcea.de

Software Defined Defence – Wie Systeme von menschlicher Kognition lernen können

Dr. Pascal Marquardt, Abteilungsleiter Kognitive Verfahren, Fraunhofer FHR

Dr. Pascal Marquardt
Foto: Fraunhofer FHR/Hardy Welsch

Wenn von Software Defined Defence (SDD) die Rede ist, ist häufig der Einsatz von künstlicher Intelligenz (KI) gemeint. Das zeigen Positionspapiere von BDSV, BDLI, Bitkom und BMVg (2023) sowie des Cyber Innovation Hub (2025). Auch das Pentagon spricht von einer „AI Adoption Strategy“. Das wirft regelmäßig Fragen nach einem sicheren Einsatz von KI in militärischen Systemen auf. Wie vertrauenswürdig ist das Ergebnis der KI? Kann die Korrektheit der Entscheidung bewiesen oder zumindest erklärt werden? Und wie hoch kann und darf der Autonomiegrad der KI sein?

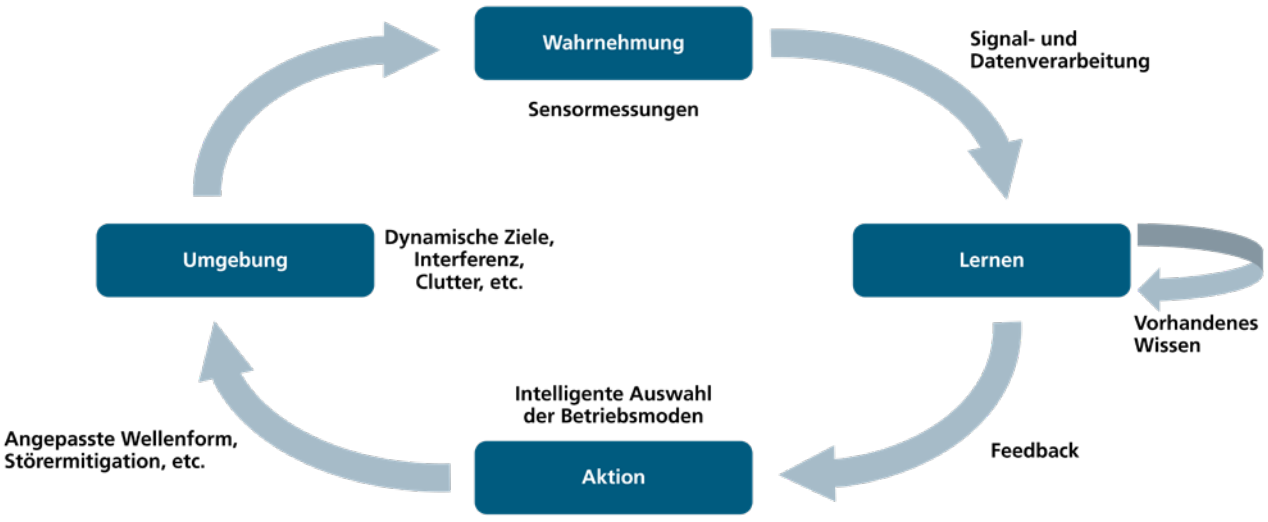
Allerdings wird eine zentrale Frage nur sehr selten gestellt. Sollte der Begriff Software Defined Defence auf den Einsatz von KI reduziert werden? Konkreter gefragt: sollte ein Verteidigungssystem das Wissen, das es zur Entscheidungsfindung nutzt, nicht auch verwenden, um daraus für die Zukunft zu lernen?

Das Fraunhofer-Institut für Hochfrequenzphysik und Radartechnik FHR erforscht Methoden, die es Radar- und EloKa-Systemen ermöglichen, Informationen aus der Umgebung und der eigenen (Mess-)Historie zu verarbeiten, und daraus Schlussfolgerungen zu ziehen. Diese Schlussfolgerungen sorgen dann für eine kontinuierliche Anpassung des Systems an die aktuelle Situation. Die grundlegende Idee für diese Methoden ist dabei angelehnt an die menschliche Kognition.

Menschliche Kognition als Vorbild für Software Defined Defence

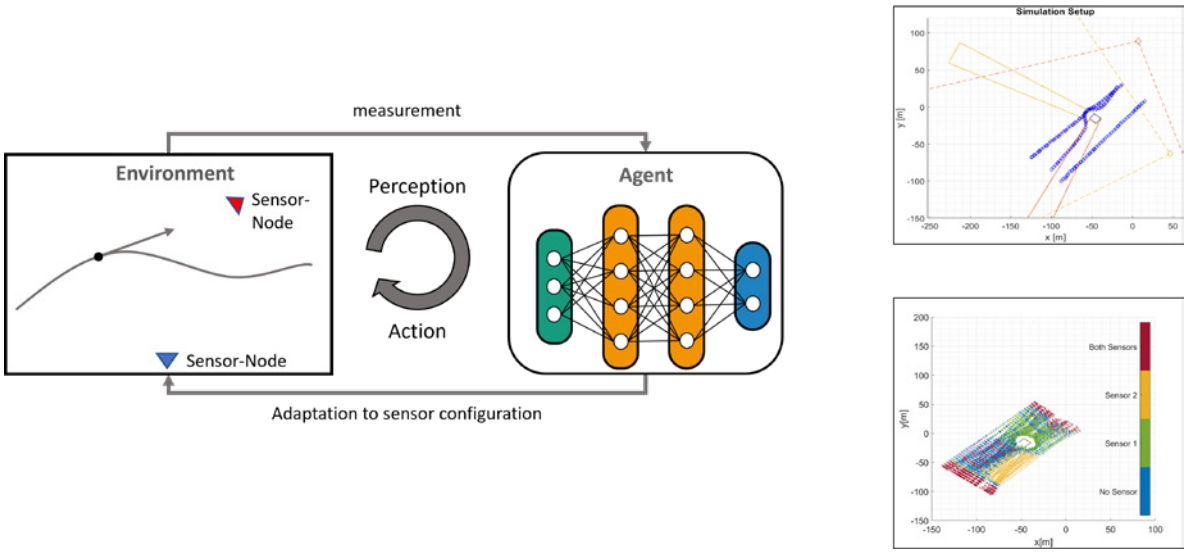
In der Neurowissenschaft wird Kognition häufig als Kreislauf aus Wahrnehmen und Handeln beschrieben. Ein Organismus nimmt seine Umgebung über Sinnesorgane wahr, verarbeitet diese Informationen im Gehirn, trifft eine Entscheidung, handelt – und die Wirkung dieser Handlung verändert wiederum die Umgebung. Diese Rückkopplung wird als Perception-Action-Cycle bezeichnet und läuft kontinuierlich ab. So entsteht die Fähigkeit, aus Erfahrung zu lernen und Verhalten laufend anzupassen.

Kognitive RF-Systeme nutzen diesen Kreislauf gezielt: Sie werten nicht nur einzelne Messungen aus, sondern berücksichtigen ihre Messhistorie, nehmen ihre elektromagnetische Umgebung wahr und bewerten damit die aktuelle Situation und bisherige Erfahrungen, um ihr Verhalten fortlaufend zu verbessern. Damit übertragen sie grundlegende Ideen der menschlichen Kognition – Wahrnehmen, Bewerten, Handeln, Lernen – direkt auf Radarsensoren und EloKa-Systeme. Aus Radar-Sicht bedeutet dies, dass ein klassisch ausgelegtes System, dessen Parameter auf ein bestimmtes Szenario optimiert sind, durch kognitive Verfahren deutlich flexibler wird. Ein kognitives Radar beobachtet fortlaufend, wie gut seine aktuellen Ziele erreicht werden, etwa in Bezug auf Detektionswahrscheinlichkeit oder Trackqualität,



Perception-Action-Cycle in einem Sensorsystem.

Grafik: Fraunhofer FHR



Framework für ein kognitives Tracking von Drohnen. Durch den Einsatz eines Agenten können Radarressourcen gespart werden.

Grafik: Fraunhofer FHR

und passt daraufhin seine Betriebsweise an. Besonders im Verbund mehrerer Sensoren kommt ein kognitives Ressourcenmanagement ins Spiel: Ein lernender Agent entscheidet, welche Sensoren zu welchem Zeitpunkt wirklich benötigt werden, um zum Beispiel eine geforderte Trackqualität sicherzustellen – und spart so Sensorressourcen, ohne die Verfolgung der Ziele zu gefährden. In der elektronischen Kampfführung zeigt sich die gleiche Struktur mit anderer Zielsetzung. Hier geht es darum, fremde Emissionen zu erkennen, zu trennen und zu identifizieren. Ein kognitives EloKa-System bewertet kontinuierlich, wie zuverlässig diese Schritte sind, welche Signale besonders relevant erscheinen und wo Unsicherheiten bestehen – und passt seine Strategien entsprechend an, etwa durch die gezielte Beobachtung bestimmter Frequenzbereiche. Aufbauend darauf kann es Täuschungsmaßnahmen wie die Erzeugung von Falschzielen anstoßen und auf Basis seiner Erfahrung entscheiden, welche Art von Täuschung in welcher Situation voraussichtlich am wirkungsvollsten ist. Radar- und EloKa-Systeme verschiedener Akteure richten sich typischerweise gegeneinander: Radarsysteme sollen ein möglichst verlässliches Lagebild erzeugen, während EloKa-Systeme des Gegners genau diese Aufklärung stören, täuschen oder ausnutzen. Beide Seiten beobachten dabei fortlaufend das Verhalten des jeweils anderen, ziehen Rückschlüsse und passen ihre eigenen Verfahren an. In modernen, vernetzten Systemverbünden kommt eine zweite Perspektive hinzu: Radar und EloKa existieren nicht nur als Gegenspieler, sondern auch als Komponenten eines gemeinsamen technischen Umfelds. In dieser Koexistenz werden die unterschiedlichen Sichtweisen beider Systeme genutzt, um ein umfassenderes Bild der Lage zu gewinnen und die Gesamtarchitektur an neue Bedingungen anzupassen.

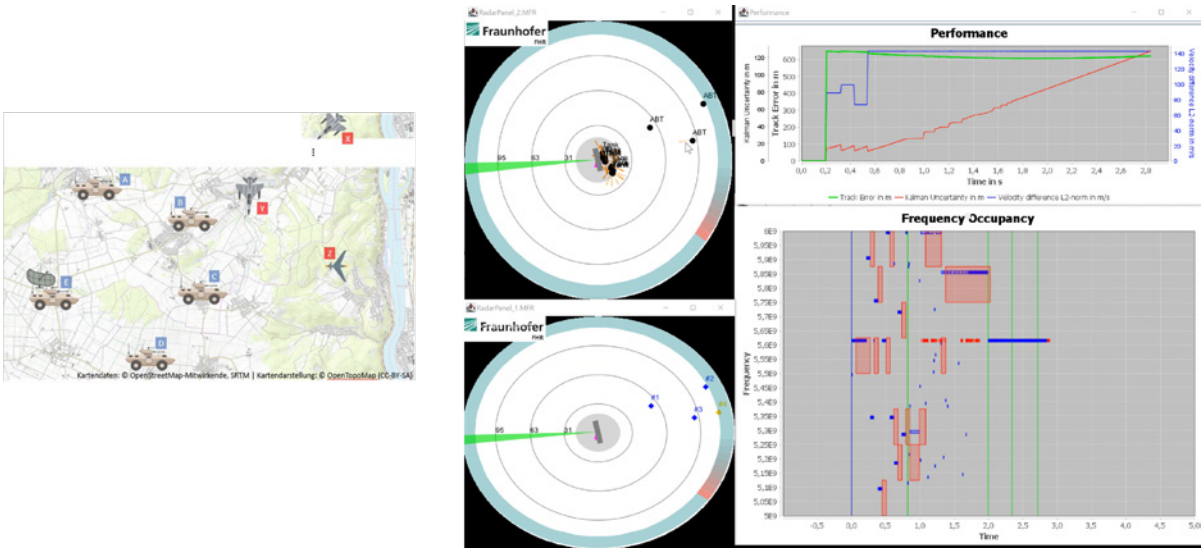
Daten und Simulation als Grundlage kognitiver Verfahren

Kognitive Verfahren benötigen große Mengen an Daten, um den Perception-Action-Cycle in RF-Systemen zu ermöglichen. Algorithmen müssen unter möglichst vielen, möglichst realistischen Bedingungen trainiert und getestet werden. Reale Messdaten stehen dafür oft nur begrenzt zur Verfügung oder sind aufwändig zu gewinnen. Simulationen werden damit zu einem zentralen Werkzeug: Sie liefern kontrollierbare, reproduzierbare und gezielt variierbare Datensätze für die Entwicklung und Bewertung kognitiver Methoden. Am Fraunhofer FHR stehen dafür sowohl Simulationswerkzeuge für EloKa-Szenarien als auch für Radarsysteme zur Verfügung. ESM-Simulatoren bilden komplexe elektromagnetische Umgebungen mit unterschiedlichen Plattformen in drei Dimensionen ab und ermöglichen eine realistische Parametrisierung der beteiligten Systeme. Radarsimulatoren erlauben die Abbildung einer Vielzahl von Radaren und die Simulation komplexer Szenarien mit mehreren Zielen, Störern und wechselnden Umgebungsbedingungen. In beiden Fällen können synthetische Daten erzeugt werden, die sowohl für klassische Verfahren als auch für Methoden des maschinellen Lernens genutzt werden, um Detektion, Klassifikation, Ressourcenmanagement und andere kognitive Komponenten systematisch zu untersuchen.

Werden Radar- und EloKa-Modelle in einer gemeinsamen Simulationsumgebung zusammengeführt, lassen sich typische Wechselwirkungen realitätsnah nachbilden und kognitive Anpassungsstrategien auf beiden Seiten erproben. Simulationen liefern damit nicht nur Trainingsdaten für Lernverfahren, sondern auch ein geschütztes Experimentierfeld, in dem SDD-Konzepte sicher und systematisch weiterentwickelt werden können.

KI im Kontext von Software Defined Defence

Natürlich spielt KI auch bei kognitiven Systemen eine wichtige Rolle. Wo Systeme ihre Umgebung nicht nur erfassen, sondern auch Muster erkennen, Situationen einordnen und aus Erfahrung lernen sollen, stoßen klassische Algorithmen manchmal an Grenzen. Das gilt insbesondere für Aufgaben wie die automatische Zielerkennung (ATR): Hier haben sich neuronale Netze als sehr leistungsfähig erwiesen. Sie können aus Radardaten komplexe Strukturen herausarbeiten und unterschiedliche Zielklassen zuverlässig unterschei-



Simulation eines komplexen Szenarios mit Radarsystemen, Kommunikationsknoten und feindlichen Jammern. Das kognitive Radar reagiert hier sowohl auf die befreundeten Kommunikationssignale (Koexistenz) als auch auf die feindlichen Störungen durch die Änderung des Sendeverhaltens.

Grafik: Fraunhofer FHR

den. Damit sind KI-Methoden ein naheliegender Baustein für kognitive Systeme: Sie liefern schnell und automatisiert Informationen, auf deren Basis weitere Schritte im Perception-Action-Cycle geplant werden können.

Gerade weil KI für SDD so attraktiv ist, stellt sich eine zentrale Frage: Wie soll sie eingesetzt werden? Soll KI in der Lage sein, eigenständig Entscheidungen zu treffen, oder soll sie vor allem als Assistenzsystem dienen, das den Menschen unterstützt, aber nicht ersetzt? Eine Metis-Studie zur Rolle von KI in Streitkräften macht deutlich, dass es hier nicht nur um Technik geht, sondern auch um Verantwortung, Kontextwissen und Urteilskraft. Eine Gestaltung, bei der die Maschine Daten sammelt, fusioniert, aufbereitet und Optionen vorschlägt, während der Mensch den Überblick behält, bewertet und entscheidet, unterscheidet sich grundlegend von einem Ansatz, bei dem die Maschine faktisch Entscheidungen vorgibt und der Mensch nur noch formal verantwortlich bleibt. Die aktuellen Konflikte zeigen aber auch, dass eine menschliche Entscheidung aufgrund von hoher Auslastung teilweise nicht mehr möglich ist.

Hinzu kommt, dass KI-Systeme nicht unfehlbar sind. Immer wieder zeigen Beispiele, dass neuronale Netze auf für Menschen schwer nachvollziehbare Weise falsche Entscheidungen treffen können oder gezielt getäuscht werden, etwa durch minimale, kaum sichtbare Veränderungen in den Eingangsdaten (Fooling). Ein wichtiger Schritt, Vertrauen in KI-gestützte Verfahren aufzubauen, besteht daher darin, die Robustheit der Modelle zu erhöhen und ihre Entscheidungen erklärbarer zu machen. Spezielle Netzwerkarchitekturen können dazu beitragen, Ausgaben stabiler gegenüber Störungen zu machen, während Methoden der „Explainable AI“ helfen, die Entscheidungsgrundlage eines Netzes besser zu verstehen. Robustheit und Erklärbarkeit ersetzen keine politische oder ethische Bewertung des KI-Einsatzes, sie schaffen aber eine technische Grundlage dafür, dass KI in SDD verantwortungsvoll genutzt werden kann.

Kognitive Verfahren als Schlüssel für Software Defined Defence

Software Defined Defence ist mehr als maschinelles Lernen: Im Zentrum steht die Fähigkeit von Systemen, ihre Umgebung fortlaufend wahrzunehmen, die eigene Lage zu bewerten, auf dieser Grundlage zu handeln – und aus den dabei gesammelten Erfahrungen zu lernen.

Für RF-Systeme entsteht daraus ein konsistentes Konzept: Radar- und EloKa-Systeme stehen sich oft als Gegner gegenüber und lernen dabei aus dem Verhalten der jeweils anderen Seite. Gleichzeitig koexistieren sie in Systemverbünden und tragen mit ihren unterschiedlichen Perspektiven zu einem gemeinsamen Lagebild bei. Kognitive Architekturen und KI-Methoden verbinden diese Rollen, indem sie Muster in den Daten erkennen, Entscheidungen vorbereiten und Anpassungen im Perception-Action-Cycle unterstützen. Simulationen und synthetische Daten liefern dafür die notwendige Grundlage, um neue Verfahren sicher zu entwickeln, zu trainieren und gegeneinander zu testen.

Damit wird deutlich, dass es bei Software Defined Defence nicht nur darum geht, „irgendwo KI einzubauen“, sondern darum, das Zusammenspiel von Algorithmik, Datenbasis und Systemarchitektur bewusst zu gestalten. Fragen nach Verantwortlichkeit, nach dem zulässigen Autonomiegrad von Systemen sowie nach Robustheit und Erklärbarkeit von KI sind keine Randaspekte, sondern bestimmen mit, welche Lösungen sich am Ende durchsetzen. Kognitive Verfahren sind in diesem Sinne eine Schlüsseltechnologie: Sie entscheiden mit darüber, ob software-definierte Verteidigungssysteme tatsächlich lernfähig, anpassbar und vertrauenswürdig sind.

Digitale Souveränität, Resilienz und Echtzeitfähigkeit als sicherheitspolitische Notwendigkeiten.

Thomas Teitge, Geschäftsführer Bechtle IT-Systemhaus Bonn.

Thomas Teitge

Foto: Bechtle

Die Anforderungen an staatliche IT- und Netzwerkinfrastrukturen wachsen rasant. Digitale Souveränität, Resilienz und Echtzeitfähigkeit sind sicherheitspolitische Notwendigkeiten. Vor diesem Hintergrund zeigt sich, welches Potenzial in der engen Zusammenarbeit zwischen Bechtle als führendem deutschen IT-Systemhaus und seinem spezialisierten Partnernetzwerk steckt.

Verlässliche IT-Lösungen aus einer Hand.

„Wir haben uns in den Bereichen Sicherheit und Verteidigung mehrfach als innovationsgetriebener, leistungsstarker und herstellerunabhängiger IT-Partner bewiesen und etabliert. Einer, der maßgeschneiderte Konzepte und zuverlässige Lösungen aus einer Hand anbietet“, erklärt Thomas Teitge, Geschäftsführer im Bechtle IT-Systemhaus Bonn, die Stärke von Bechtle. Das belegt unter anderem der Rahmenvertrag 2./3. Rechnerebene R1753 über IT-Komponenten und Dienstleistungen vom Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAAINBw). „Darüber hinaus sind wir auch beim Einsatz von KI-Anwendungen, No-Code-Lösungen und Open-Source-Produkten führend“, ergänzt Teitge.

Einsatzfähigkeit durch resiliente Netze.

Mit Blick auf verlegefähige und mobile Rechenzentrumslösungen kann Bechtle mit seinen Partnern Netz 33 und infodas dieses Ziel mit der benötigten Hard- und Software zur Sicherstellung der Verlegefähigkeit an Land unterstützen. „Gerade im Kontext von Landes- und Bündnisverteidigung ist eine stabile Kommunikationsinfrastruktur elementar“, bringt Teitge die Relevanz moderner IT-Lösungen auf den Punkt.

Echtzeit-Lagebilder durch intelligente und geschützte Vernetzung.

„Das Projekt TerrHub stellt einen bisher einzigartigen Baustein dar, mit dem es möglich sein wird, die Führungsfähigkeit im Krisen- und Katastrophenfall durch ressortübergreifende Erzeugung und Nutzung aktueller Lagebilder weiterzuentwickeln“, so Teitge. „Ein schneller und sicherer Informationsaustausch ist entscheidend. Die Umsetzung könnte in einem Konsortium erfolgen, zu dem neben uns auch infodas und Systematic zählen und dem künftig auch Netz 33 angehören könnte.“

Digitale Transparenz für strategische Entscheidungen.

Um digitale Souveränität mess-, vergleich- und steuerbar zu machen, hat Bechtle den Bechtle Index of Sovereignty (BIoS) entwickelt. Das wissenschaftlich fundierte, softwarebasierte Assessment analysiert eine reale Ausgangslage datenbasiert, objektiv und herstellerunabhängig. Dazu Teitge: „Der Fokus liegt dabei auf drei kritischen Domänen – Datenhoheit, technologische Unabhängigkeit und Kompetenz. Das stellt die Grundlage für ein präzises sowie belastbares Lagebild des aktuellen Souveränitätsgrads dar. Auf dieser Basis lassen sich dann für Organisationen und Unternehmen konkrete, strategische Handlungsempfehlungen ableiten, die für eine noch bessere Souveränität sorgen. Und diese beruhen somit nicht mehr auf einem Bauchgefühl, sondern auf Fakten.“

Fazit

Digitale Infrastruktur ist strategische Infrastruktur. Eine vertiefte Partnerschaft zwischen Bechtle und seinem Partnernetzwerk könnte sich dabei als Modell für die Entwicklung, Bereitstellung und den Betrieb zukunftsfähiger, souveräner IT-Ökosysteme etablieren – leistungsfähig, resilient und ganzheitlich gedacht.

Über Bechtle

Der IT-Zukunftsgestalter ist mit über 100 IT-Systemhäusern immer nah an seinen Kunden und zählt darüber hinaus mit IT-E-Commerce-Gesellschaften in 14 Ländern zu den führenden IT-Unternehmen in Europa. Das herstellerübergreifende Produkt- und Leistungsportfolio reicht von Hard- und Software, Open Source Produkten, Hybrid- und Multi-Clouds, Managed Service hin bis zu disruptiven digitalen Lösungen.

Bechtle begleitet zudem die Öffentliche Hand und Unternehmen bei der Planung und Inbetriebnahme von KI-Lösungen, Quantentechnologien und Cybersicherheit.

Edge AI für effiziente taktische Datenübertragung

Norman Jansen, Fraunhofer FKIE, Abteilung Informationstechnik für Führungssysteme

Norman Jansen
Foto: Fraunhofer FKIE

Unter der Bezeichnung „Edge AI“ versteht man den Einsatz von Algorithmen der Künstlichen Intelligenz auf lokaler Hardware anstelle der Verarbeitung der Daten in einer zentralisierten Cloud. Bei mobilen, militärischen Systemen denkt man dabei zunächst an die Auswertung von großen Sensordatenströmen, zum Beispiel die Objekterkennung in Videos. Edge AI kann jedoch auch dazu eingesetzt werden, um die auf der mobilen Ebene begrenzten Kommunikationsmöglichkeiten möglichst effizient zu nutzen. Dies kann einerseits durch intelligente Cross-Layer-Ansätze erreicht werden, bei denen Anwendungen ihren Datenaustausch dynamisch an den Zustand des Kommunikationsnetzes anpassen und anderseits durch KI-basierte Verfahren zur Datenkompression. Am Fraunhofer FKIE werden beide Ansätze seit Jahren intensiv beforscht. Die Wissenschaftler tragen mit ihren Arbeiten maßgeblich zu Forschungsgruppen der NATO Science & Technology Organisation (NATO STO) bei.

Perfektes Zusammenspiel von militärischen Services mit taktischen Funksystemen – Cross-Layer-Optimierung mit Multi-Agent Reinforcement Learning

Drahtlose, mobile Funknetze sind physischen Randbedingungen unterworfen. Auf dem Gefechtsfeld ist zudem mit elektromagnetischen Störungen zu rechnen. Beides führt zu instabilen Verbindungen und geringen Datenübertragungsraten. Militärische Funknetze werden daher häufig als sogenannte DIL-Netze bezeichnet („Disconnected, Intermittent and Limited“). Sie stellen eine erhebliche Herausforderung für einen zuverlässigen Informationsaustausch und eine Real-Time Situational Awareness in taktischen Führungssystemen dar.

Das Zusammenspiel von militärischen Services mit taktischen Funksystemen kann mittels Cross-Layer-basierten Optimierungsansätzen verbessert werden. Aufgrund der Komplexität der Netzwerkumgebung und der Abhängigkeiten zwischen verschiedenen Services bzw. Serviceinstanzen ist es praktisch jedoch nicht möglich, eine optimale Lösung zu bestimmen. Stattdessen kommen einfache Heuristiken zum Einsatz. In solchen komplexen Umgebungen bietet sich der Einsatz von künstlicher Intelligenz – insbesondere des Reinforcement Learning (RL) – an, um Strategien für die Optimierung der Services und der militärischen Netzwerke zu erlernen. Das Fraunhofer FKIE untersucht hierzu einen Multi-Agent Reinforcement Learning (MARL)-Ansatz, bei dem dezentrale Agenten die Ressourcennutzung über Netzschichten hinweg optimieren. Dabei kommen moderne Deep-RL-Verfahren zum Einsatz, darunter ein stabiler Optimierungsalgorithmus sowie neuronale Netze, die militärische Kommunikationsnetze in Form von Graphen abbilden können.

Der Ansatz wurde anhand der klassischen Aufgabe des Blue-Force-Tracking (BFT) untersucht. Die trainierten Agenten legen dynamisch die jeweils zu nutzende Datenrate für lokale BFT-Service-Instanzen fest. Die BFT-Service-Instanzen passen daraufhin die Senderate von Eigenpositionsmeldungen entsprechend an. Als Optimierungsmetrik dient die Quality of Experience (QoE); im Fall von BFT ist dies die Aktualität der Positionen auf der Lagekarte.

Das Fraunhofer FKIE hat eine Trainings- und Testumgebung entwickelt, um die militärische Umgebung realistisch nachzubilden (vgl. Abb. 1). Sie basiert auf einer virtualisierten Infrastruktur, in der Experimente innerhalb von virtuellen Maschinen (VM) durchgeführt werden. Innerhalb der VMs wird jede militärische Einheit durch einen Docker-Container repräsentiert, der einen Netzwerkknoten mit emuliertem Funkgerät, der Grundfunktionalität eines taktischen Routers (OLSRv2-Routing) sowie einer Instanz des Blue-Force-Tracking (BFT)-Service abbildet. Ein Resource Manager steuert die lokalen Ressourcen eines Knotens, indem er über Cross-Layer-Schnittstellen Informationen aus dem Routingprotokoll und dem BFT-Service auswertet und zur dynamischen Konfiguration des lokalen BFT-Service nutzt. Die Funkübertragung wird mittels des echtzeitfähigen Netzwerkemulators EMANE nachgebildet. Eine zentrale Machine Learning & Monitoring-Komponente auf dem Host-System koordiniert das Training und die Überwachung der dezentralen Agenten. Hierbei kommen etablierte Werkzeuge wie Telegraf, InfluxDB, MLflow, MongoDB und Grafana zum Einsatz.

Für das Training der RL-Agenten wurde ein phasenbasierter Ansatz verwendet. In der ersten Phase lernen die Agenten mittels Behavioral Cloning zunächst, das grundlegende Verhalten eines Experten nachzuahmen. Als Experte wird eine einfache Heuristik verwendet, die die aktuell verfügbare Datenrate im Netzwerk gleichmäßig auf die Netzwerkteilnehmer (militärische Einheiten) verteilt. Die Ausgabe des Agenten ist in diesem Fall also eine vorgegebene Datenrate für die lokale Instanz des BFT Service. In einer weiteren Phase lernen die Agenten, ihr Verhalten so anzupassen, dass die Zielmetrik (QoE) maximiert wird und die Heuristik übertroffen werden kann. Hierbei wirkt die Heuristik als eine Art Ratgeber, welcher den Möglichkeitsraum für Aktionen des Agenten einschränkt (Aktions-

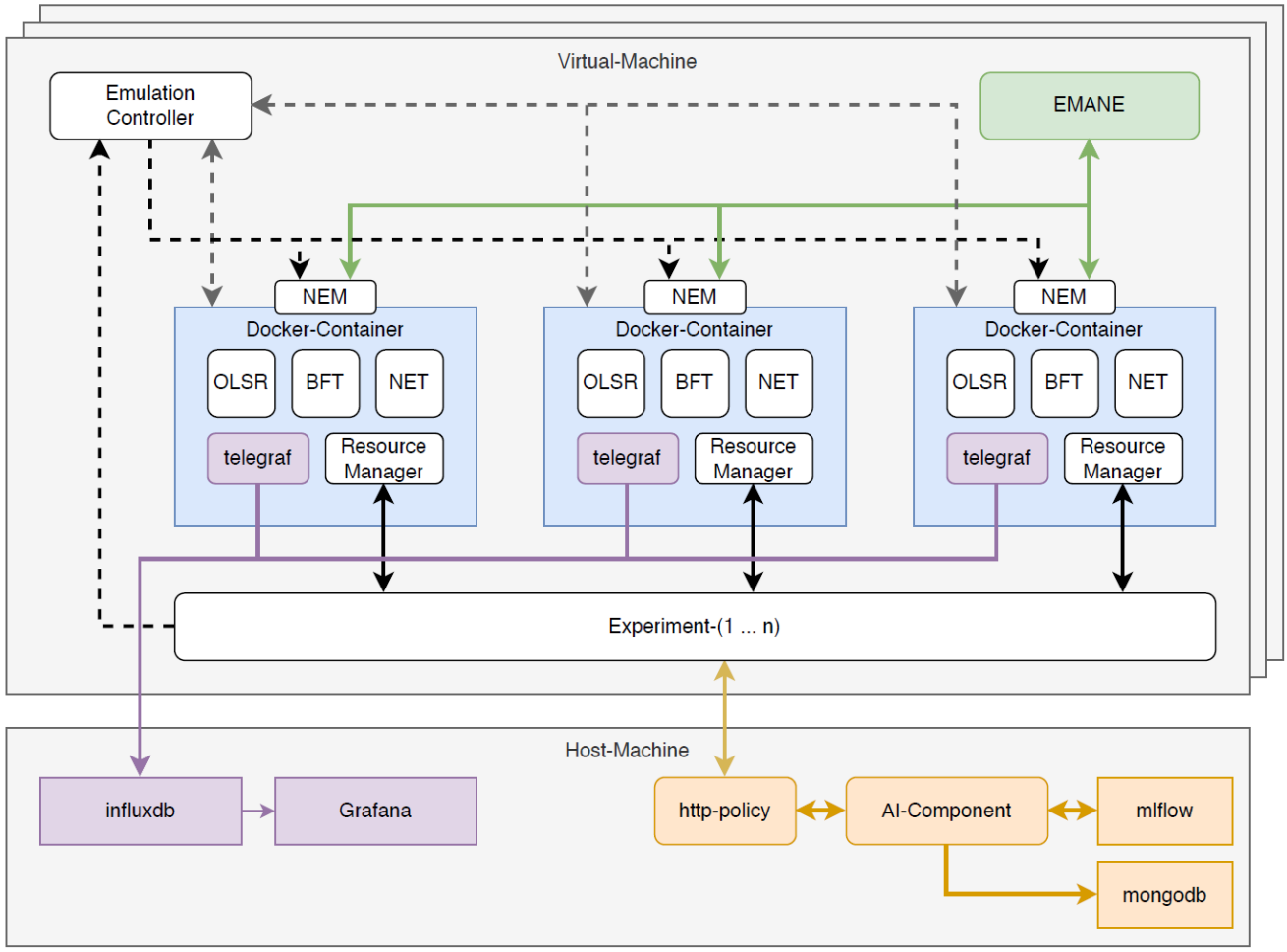


Abb. 1: Trainingsarchitektur für Multi-Agent Reinforcement Learning. *Grafik: Fraunhofer FKIE*

maskierung), um nicht erfolgsversprechende Aktionen auszuschließen. In der abschließenden Phase lernt der Agent völlig selbständig, da er bereits robust genug ist.

Die Integration eines marktverfügbaren Führungssystems für die mobile Ebene in die Emulationsumgebung stellt einen wichtigen Schritt zur Verbesserung der Realitätsnähe der Simulation dar. Das Führungssystem wird auf separaten virtuellen Maschinen (VMs) ausgeführt, die in die Emulation bzw. die jeweiligen Container eingebunden werden.

Unsere Evaluation hat gezeigt, dass mit Hilfe von Multi-Agent Reinforcement Learning eine Verbesserung der Quality of Experience beim Blue Force Tracking gegenüber einer einfachen Heuristik für die Datenratenverteilung erreicht werden kann. Die Ergebnisse wurden auf der ICCRTS 2023 und MILCOM 2024 vorgestellt. Die Lösung lässt sich als KI-App in eine Battlesuite integrieren. Der MARL-Ansatz bietet weitergehendes Potenzial, da er sich auf andere taktische Anwendungen übertragen lässt.

Speech-to-Text-to-Speech: Effiziente Sprachkommunikation in DIL-Netzen

Digitale Sprach-Kommunikationsdienste stellen besondere Anforderungen an die zugrunde liegende Kommunikationsinfrastruktur. Geringe Datenraten, eingeschränkte Reichweiten sowie häufige und teils länger anhaltende Verbindungsunterbrechungen prägen jedoch die eingesetzten Netze auf der taktischen Ebene und erschweren den Einsatz klassischer kontinuierlicher Sprachübertragung.

In der NATO STO-Forschungsgruppe IST-201 „Federated Collaboration Services at the Tactical Edge“ werden unter Leitung des Fraunhofer FKIE audio-basierte Dienste untersucht. Frühere Untersuchungen verglichen klassische militärische Sprachcodecs wie MELPe mit generativen Low-Bitrate-Ansätzen wie Google Lyra. Trotz qualitativer Verbesserungen bleibt die kontinuierliche Übertragung von Audiodaten eine strukturelle Schwäche bei stark eingeschränkter oder intermittierender Konnektivität.

Vor diesem Hintergrund wurde ein alternatives Kommunikationsparadigma untersucht, bei dem nicht das Audiosignal selbst, sondern dessen semantischer Inhalt übertragen wird. Sprache wird beim Sender mittels Speech-to-Text (STT) automatisch in Text überführt, als kompakte Nachricht verteilt und beim Empfänger mittels Text-to-Speech (TTS) wieder mit originalgetreuer Modulation synthetisch erzeugt. Ziel ist es, die erforderliche Datenrate für Sprachkommunikation signifikant zu reduzieren und die Robustheit gegenüber Unterbrechungen in taktischen Netzen zu erhöhen. Als Metriken für die Evaluierung dienen Delay

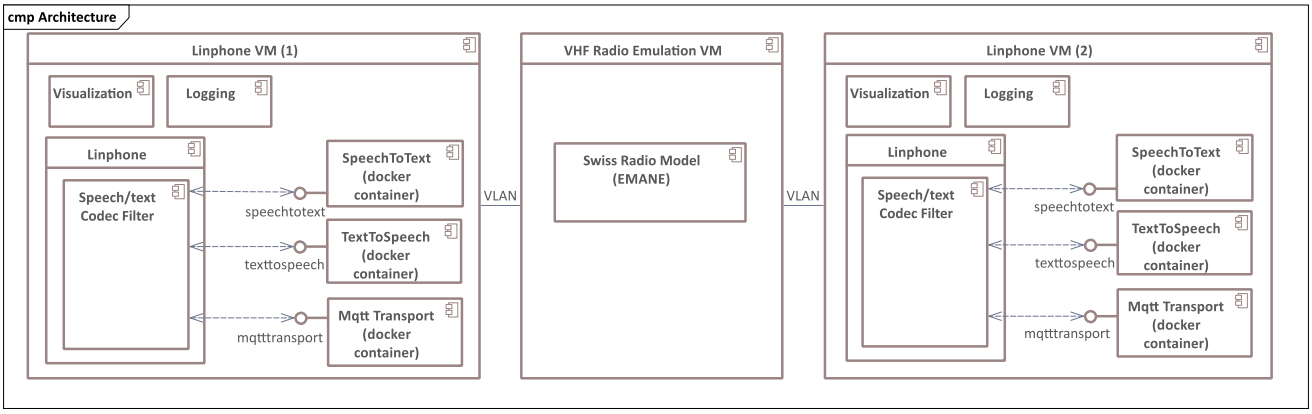


Abb. 2: Systemarchitektur für die STT-TTS-Pipeline. *Grafik: Fraunhofer FKIE*

und Word Error Rate per Sentence. Für die experimentelle Untersuchung des STT-TTS-Ansatzes wurde eine Systemarchitektur entworfen und umgesetzt (vgl. Abb. 2). In dem Demonstrator wurden zwei Kommunikationsknoten mit dem VoIP-Softphone Linphone über ein emuliertes taktisches Funknetz verbunden. Die Netzemulation erfolgte mithilfe des Swiss Radio Model, das von den Schweizer Partnern entwickelt wurde und innerhalb des Emulationsframeworks EMANE TDMA-basierte VHF- und UHF-Funkgeräte mit begrenzter Datenrate realitätsnah emuliert. STT und TTS wurden lokal auf den Netzwerkknoten (als Microservices) ausgeführt. Zur Evaluation wurde die Verzögerung vom Ende eines gesprochenen Satzes bis zum Beginn der Wiedergabe am empfangenden Knoten gemessen und in ihre vier Bestandteile zerlegt: Satzdetektion, STT-Verarbeitung (Vosk bzw. Whisper), Transport via MQTT/UDP und TTS-Synthese (FastPitch + HiFi-GAN). Abbildung 3 zeigt die Verzögerungen bei Nutzung einer schmalbandigen VHF-Wellenform mit einer Gesamtdatenrate von 10 kbit/s (geteilt zwischen beiden Teilnehmern). Die Medianwerte lagen bei ca. 340 ms für die Satzdetektion, 366–399 ms für die STT-Verarbeitung, 580–655 ms für den MQTT-Transport und ca. 320 ms für die TTS-Synthese. Die kumulative Gesamtverzögerung lag zwischen 1,6 s und 1,8 s und blieb damit unter zwei Sekunden. Der Datenverbrauch konnte gegenüber MELPe um bis zu 93,7 %

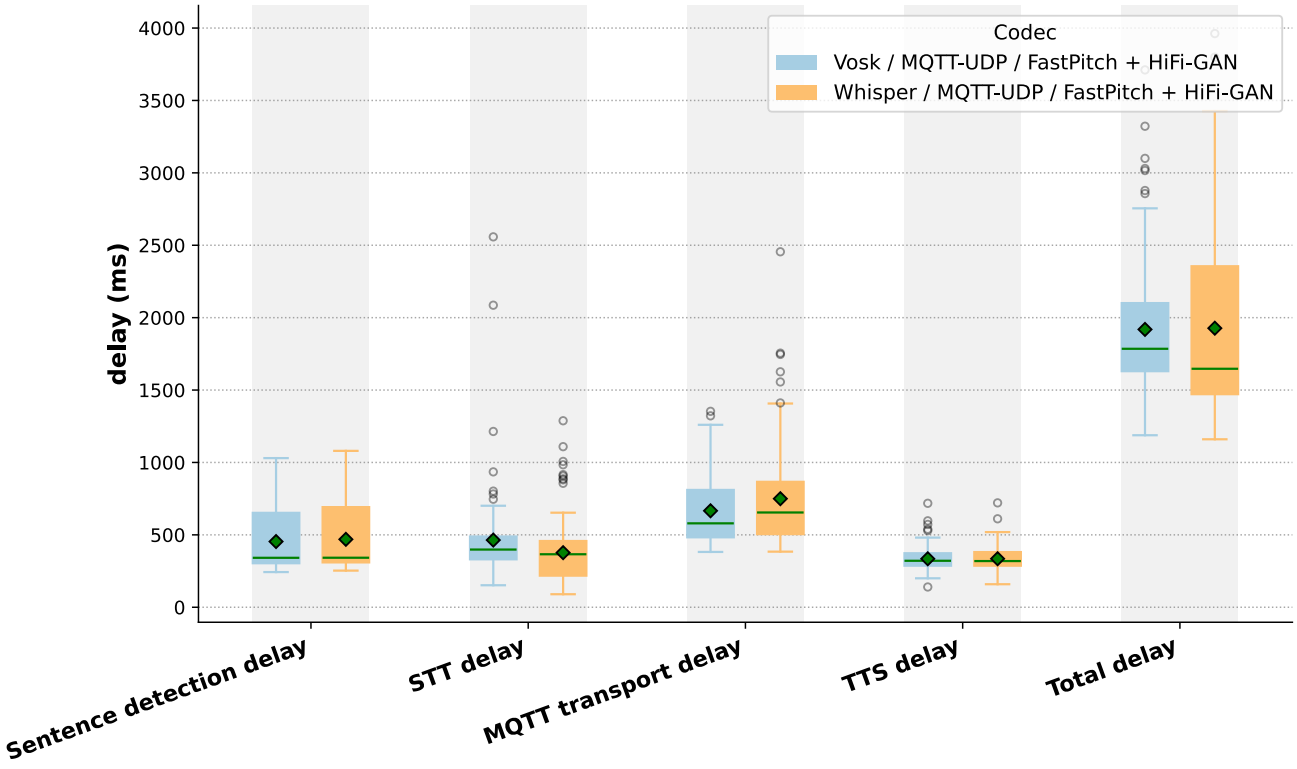


Abb. 3: Latenz des STT-TTS-Ansatzes. *Grafik: Fraunhofer FKIE*

(72 % inkl. Protokolloverhead) reduziert werden. Selbst unter stark datenratenbeschränkten DIL-Bedingungen blieb verständliche Sprachkommunikation möglich.

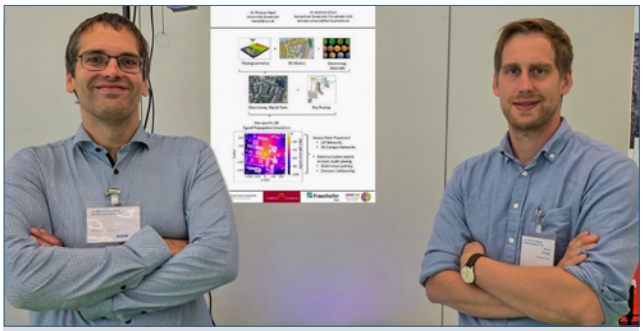
In einem weiteren Schritt wurde die TTS-Komponente um mehrere Zero-Shot-Voice-Cloning-Modelle erweitert. Beim Zero-Shot-Voice-Cloning werden Stimmen anhand von 5–10 Sekunden Audiomaterial des Sprechers imitiert. Ziel war dabei ein geringer Delay und eine hohe Voice-Cloning-Qualität.

Objektive Evaluierungsmetriken für Natürlichkeit (UTMOSv2) und Stimmähnlichkeit (ECAPA-TDNN) wurden auf die Kategorien Weiblich, Männlich und Nicht-Muttersprachler angewendet. Zur subjektiven Bewertung wurde zudem ein webbasiertes Hörtestverfahren durchgeführt, bei dem Teilnehmende aus verschiedenen Nationen die synthetisierten Sprachproben hinsichtlich Natürlichkeit und Sprecherähnlichkeit im Vergleich zu Referenzaufnahmen bewerteten. Das Modell Chatterbox erzielte mit die höchsten Natürlichkeitswerte, wies jedoch eine deutlich erhöhte Syntheseverzögerung auf, was seine Eignung für echtzeitkritische Anwendungen einschränkt. Die Analyse ergab, dass F5-TTS — insbesondere in der optimierten Variante F5-TTS-TRT — insgesamt das beste Verhältnis aus Natürlichkeit, Sprecherähnlichkeit und Performanz aufweist und damit als führendes Modell in der Gesamtbetrachtung bewertet werden kann. Die Ergebnisse zeigen die Machbarkeit des STT-TTS-Ansatzes selbst in stark eingeschränkten DIL-Umgebungen mit sehr niedriger Datenrate (10 kbit/s, geteilt zwischen den Kommunikationsknoten). Durch die semantische Repräsentation des Audiosignals als Text kann die benötigte Datenrate drastisch reduziert werden, während gleichzeitig eine akzeptable Ende-zu-Ende-Verzögerung erreicht wird. Der Ansatz stellt somit eine strukturelle Alternative zur kontinuierlichen Audioübertragung dar. Die Integration von Zero-Shot Voice Cloning ermöglicht darüber hinaus die Nachbildung der Sprecheridentität und verbessert die wahrgenommene Qualität der rekonstruierten Sprachsignale. Dank modularer Architektur lässt sich die Sprachlösung leicht in bestehende Systeme integrieren. Die Forschungsergebnisse werden bei der IEEE-Konferenz ICMCIS 2026 präsentiert.

Als nächster Schritt soll eine echte Streaming-basierte Variante der STT-TTS-Pipeline untersucht werden, um die Ende-zu-Ende-Verzögerung weiter zu reduzieren. Ziel ist eine nahezu echtzeitfähige Sprachrekonstruktion bei vergleichbarer Word Error Rate. Ebenso sollen Experimente mit Hintergrundgeräuschen bzw. zur Geräuschunterdrückung durchgeführt werden. Durch die semantische Repräsentation des Audiosignals als Text ergeben sich zusätzliche Möglichkeiten. Beispielsweise kann beim Empfänger vor der Sprachsynthese bei Bedarf eine Übersetzung in die Muttersprache des Soldaten erfolgen. Hierfür müssen Anpassungen der TTS-Modelle für spezifische Sprachen untersucht werden. Erste Untersuchungen eines angepassten Chatterbox-Modells für die deutsche Sprache lieferten bereits vielversprechende Ergebnisse.

Ortsspezifische Simulation von Funksignalausbreitung mittels Ray Tracing in Digitalen Zwillingen

Dr. Bertram Schütz, Wissenschaftlicher Mitarbeiter am Fraunhofer FKIE in der Abteilung Kommunikationssysteme mit Tandem-Professur in der Talentakademie „Smart Factory und Products“ an der Hochschule Osnabrück.



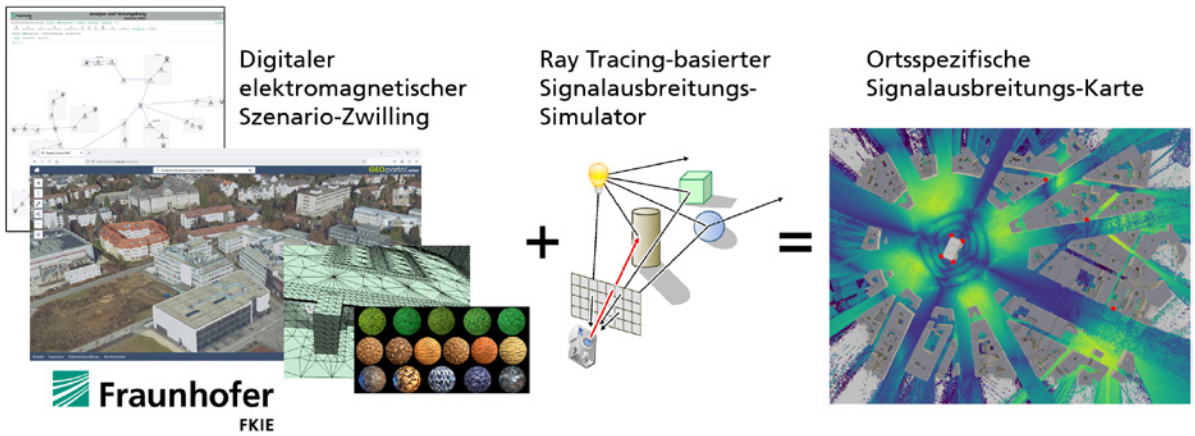
Dr. Bertram Schütz (rechts) (Fraunhofer FKIE) und **Dr. Thomas Hänel** (links) (Joint Lab Universität Osnabrück), Interaktive Demonstration, VDE Mobilfunktagung 2025 *Foto: Fraunhofer FKIE*

„Radiowellen zum Anfassen“
Auf der VDE Mobilfunktagung 2025 wurde in Kooperation mit Dr. Thomas Hänel vom Joint Lab der Universität Osnabrück eine interaktive Demonstration des Verfahrens gezeigt. Dabei konnten interessierte Veranstaltungsbesucher einen Funksender beliebig auf einem 3D-Modell des Universitätscampus platzieren. Mittels eines Projektors wurde live die simulierte Signalausbreitungskarte unter Berücksichtigung der ortsspezifischen Effekte auf das 3D-Modell projiziert.

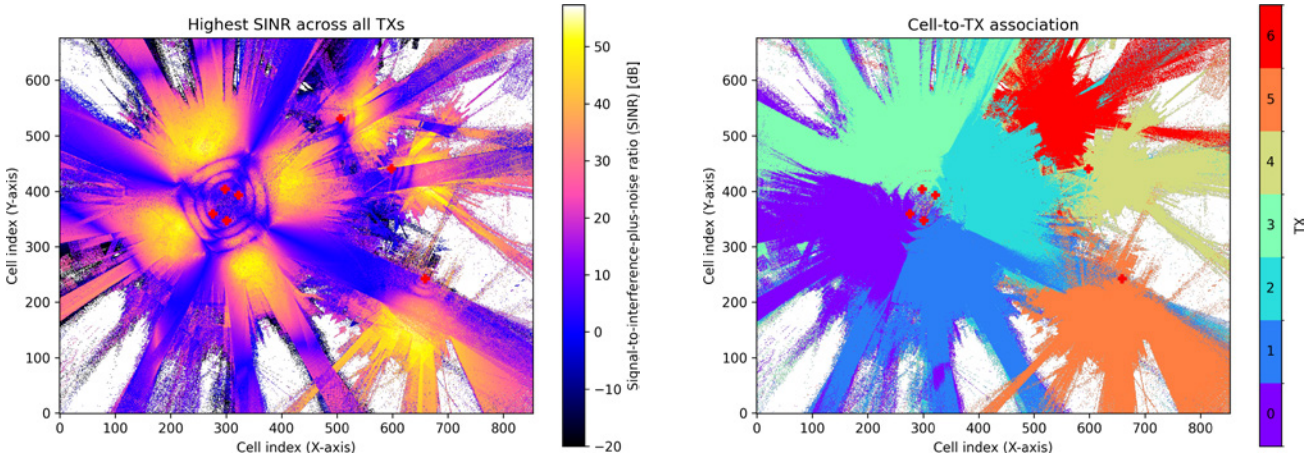
Robuste Funkverbindungen sind unerlässlich für zuverlässige Kommunikation. Insbesondere in komplexen, urbanen Umgebungen haben ortsspezifische Effekte jedoch einen starken Einfluss auf die Kommunikationsfähigkeit. Hierzu zählt insbesondere die Abschattung durch Terrain, Biomasse und Gebäude. Ob sich zwischen zwei Kommunikationsteilnehmern ein modernes Gebäude aus Stahlbeton, ein zweischaliges Altbau-Mauerwerk oder ein landwirtschaftliches Gebäude befindet, hat einen signifikanten Einfluss auf die Signalausbreitung. Somit ist der direkte Umgebungseinfluss nicht nur für die grundsätzliche Erreichbarkeit einer Einheit relevant, sondern hat auch signifikanten Einfluss auf Bitfehlerrate, Latenz und den Durchsatz des verwendeten Funkmittels.

Mit den Augen des Funkmittels sehen

Aufgrund ihrer empirisch-statistischen Natur können traditionelle Funksignalausbreitungsmodelle ortsspezifische Effekte nur bedingt berücksichtigen. Ray Tracing-basierte Simulatoren hingegen nutzen einen digitalen elektromagnetischen Zwilling des konkreten Ziel-Szenarios, um ein realistisches Lagebild der Kommunikationsfähigkeiten zu berechnen. Dabei wird auf Basis von 3D-Daten eine geometrisch möglichst exakte virtuelle Umgebung erzeugt und so modifiziert, dass die elektromagnetischen Eigenschaften der vorkommenden Objekte und Materialien berücksichtigt werden. Insbesondere wird so die material- und frequenzabhängige Dämpfung von unterschiedlichen Konstruktionsmaterialen, wie etwa Holz, Beton und Metall, modelliert. In diesem elektromagnetischen digitalen Zwilling werden anschließend die ortsspezifischen Pfadverluste mittels hoch-performanten Ray Tracing-Algorithmen berechnet. Während traditionelles Ray Tracing fotorealistische Renderings durch die Simulation von Lichtstrahlen im sichtbaren Frequenzspektrum erzeugt, wurde das hier beschriebene Verfahren speziell für relevante Frequenzen von taktischen Funkmitteln angepasst. Somit werden auch komplexe physikalische Effekte wie Mehrpfadreflektionen, Beugung und Brechung realistisch berücksichtigt. Der Simulator „sieht“ somit die Signalausbreitung des Funkmittels, ähnlich wie ein Mensch sichtbares Licht wahrnimmt. Die berechneten Pfadverlustwerte werden anschließend zu Signalausbreitungskarten des Szenarios zusammengesetzt und komprimiert gespeichert.



Übersichtsgrafik ortsspezifische Simulation von Funkmitteln *Grafik: Fraunhofer FKIE*



SINR-Simulation für ein 5G Netz (links) und simulierte Zellenzuordnung für Endgeräte (rechts) (erzeugt mit NVIDIA Sionna, s. https://nvlabs.github.io/sionna/index.html) [BS1.1].

Grafik: Fraunhofer FKIE

Eine „strahlende“ Zukunft

Aufgrund des erhöhten Realismus eröffnen strahlenbasierte Signalausbreitungssimulationen neue Fähigkeiten und Kompetenzen, insbesondere im Bereich der Evaluation und Optimierung von Kommunikationsmitteln. So können die berechneten Pfadverlustwerte genutzt werden, um realistische Testszenarien zu generieren, beispielsweise zur Unterstützung der Digitalisierung Landbasierter Operationen (D-LBO) sowie der wichtigen NATO- und Federated Mission Networking (FMN) Bemühungen. Ein besonders interessanter Use Case ist die Generierung von realistischen Pfadverlustwerten für Vignette 3 „Urban Operation“ des NATO Referenzszenarios „Anglova“ der NATO IST-124 Research Task Group on Heterogeneous Networks: Improving Connectivity and Network Efficiency (s. https://anglova.net/). Bei der Planung von 5G-Netzen werden Ray Tracing-basierte Simulationen bereits zur Optimierung der Abdeckung und Evaluation der Zellzuordnung von Endgeräten eingesetzt (s. Foto). Auch für den Zivilschutz bietet ortsspezifische Signalausbreitungssimulation großes Potenzial. Beispielsweise kann so die Funkabdeckung von kritischer Infrastruktur (KRITIS) und von Rettungskräften für mobile Kommunikationslösungen im Katastrophenfall simuliert und optimiert werden. Insbesondere bei Starkregen- und Hochwasserereignissen, wie der Ahrtalflut 2021, kann so das Lagebild um die Kommunikationsfähigkeit ergänzt werden. Hierzu ist aufgrund der herausragenden Auflösung besonders die Verwendung der 3D-Daten des öffentlich verfügbaren „Digitalen Zwilling NRW“ interessant. Durch die Verwendung solch detailgetreuer Digitaler Zwillinge können in Zukunft ortsspezifische Effekte noch deutlich feingranularer simuliert werden – wie der Name also bereits sagt, hat strahlenbasierte Funksignalausbreitung mittels Ray Tracing also tatsächlich eine „strahlende“ Zukunft.

Screenshot Digitaler Zwilling NRW Fraunhofer FKIE, Standort Wachtberg, vgl. www.dz.nrw.de

Foto: Fraunhofer FKIE

Hochenergielaser als vernetzte Wirksysteme – Fraunhofer IOSB stärkt technologische Souveränität

Prof. Dr. Marc Eichhorn, Direktor Ettlingen und Bereichsleiter Verteidigung am Fraunhofer IOSB

Prof. Dr. Marc Eichhorn
Foto: Fraunhofer IOSB / Fotosassa

Die sicherheitspolitische Lage in Europa hat die Anforderungen an neue militärische Fähigkeiten grundlegend verändert. Gefragt sind Systeme, die schnell reagieren, präzise wirken und sich in vernetzte Führungs- und Aufklärungsketten einfügen lassen. Hochenergielaser (HEL) gehören in diesem Zusammenhang zu den Technologien, die für Bundeswehr, Beschaffung und Industrie gleichermaßen an Bedeutung gewinnen. Zugleich berührt ihre Entwicklung eine strategische Frage, die über die einzelne Fähigkeit hinausweist: die technologische Souveränität Deutschlands und Europas. Wer solche Systeme künftig wirksam, sicher und unabhängig nutzen will, muss ihre Schlüsseltechnologien verstehen, bewerten und weiterentwickeln können. Entscheidend ist dabei der Blick auf das Gesamtsystem. Hochenergielaser sind keine isolierten Effektoren, deren Leistungsfähigkeit sich allein aus der optischen Ausgangsleistung ableiten ließe. Ihre Wirksamkeit entsteht erst im Zusammenspiel von Sensorik, Tracking, Strahlquellen, Strahlformung, atmosphärischer Ausbreitung, Sicherheitskonzepten und der Wirkung auf unterschiedliche Ziele. Genau an dieser Schnittstelle arbeitet das Fraunhofer IOSB: Wir betrachten HEL end-to-end, analysieren ihre Leistungsgrenzen, entwickeln Modelle für ihr Verhalten in realen Umgebungen und schaffen die wissenschaftlichen Grundlagen für belastbare Bewertungen und Systementscheidungen.

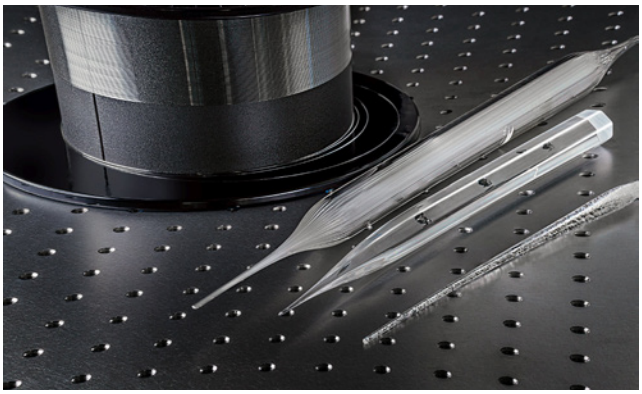
Systemverständnis statt Einzeltechnologie

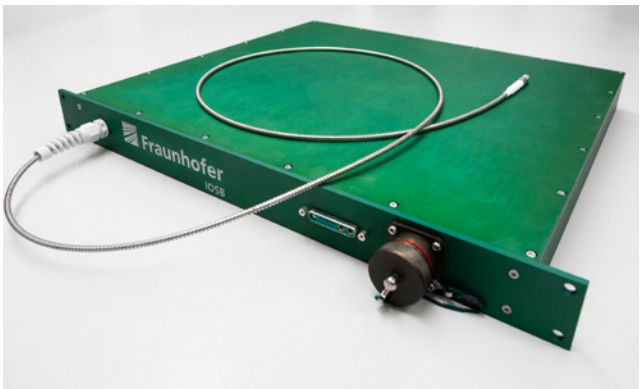
Für militärische Anwender ist diese Systemperspektive von zentraler Bedeutung. Ein Hochenergielaser muss Ziele nicht nur erreichen, sondern sie unter realen Bedingungen zuverlässig erfassen, verfolgen und mit ausreichender Energiedichte beaufschlagen. Das setzt eine mehrstufige Kette voraus: von der großräumigen Detektion über die optische Feinverfolgung bis zur präzisen Stabilisierung des Zielpunkts. Schon kleine Abweichungen in der Sensorik, in der Regelung oder in der Ausbreitung des Strahls können die Wirkung auf dem Ziel deutlich verringern. Wer die Einsatzreife solcher Systeme beurteilen will, braucht daher belastbare Aussagen über das Zusammenspiel aller Teilsysteme.

Unsere Arbeit zielt genau auf diese belastbaren Aussagen. Wir entwickeln und koppeln Simulationsmodelle, Messmethoden und Erprobungsansätze, um Hochenergielaser-Systeme nicht nur in Teilaspekten, sondern als vernetzte Wirksysteme zu verstehen. Das schafft eine Grundlage für Industriepartner, die Technologien weiterentwickeln, ebenso wie für öffentliche Auftraggeber, die Leistungsversprechen einordnen und Entwicklungsrisiken bewerten müssen. Damit leisten wir einen Beitrag, der für die Fähigkeitsentwicklung ebenso relevant ist wie für die Vorbereitung späterer Beschaffungsentscheidungen.

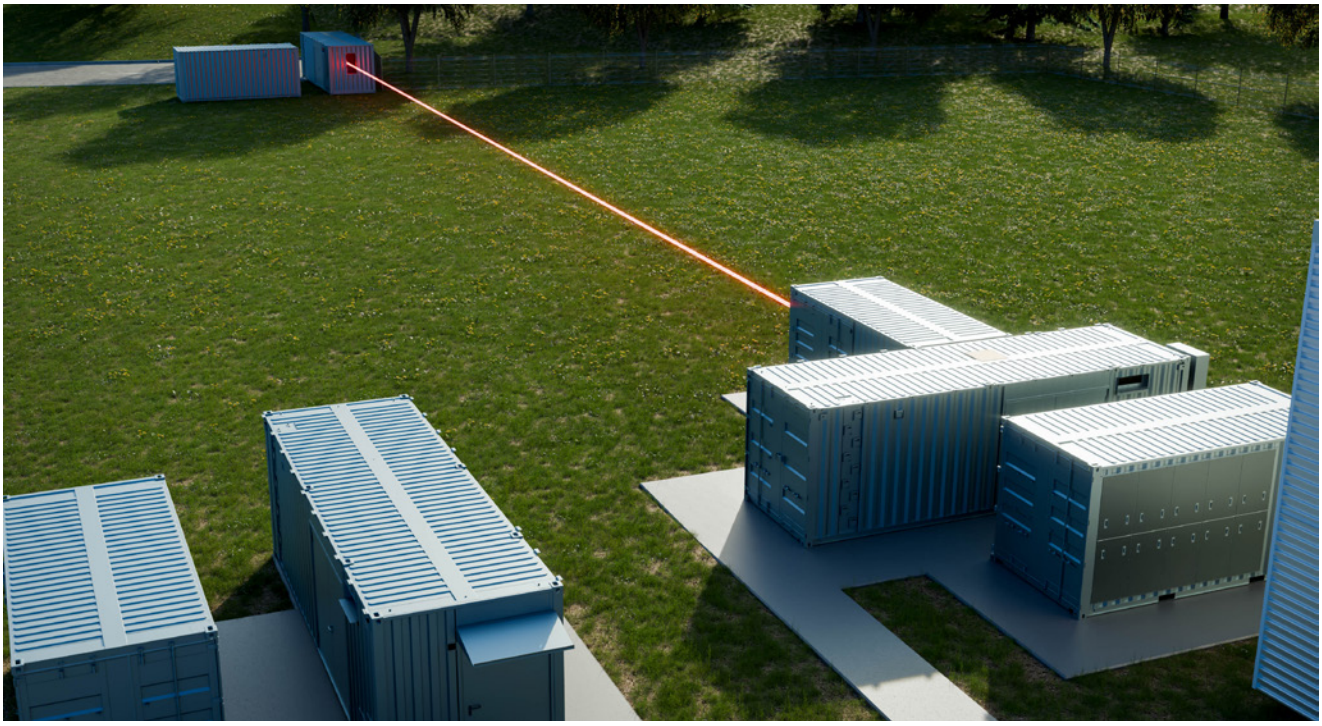
HELIKS als Brücke zwischen Labor und realer Umgebung

Ein zentrales Element dieser Arbeit ist HELIKS („HEL-Investigationsanlage mit kohärenter Strahlkopplung“), unsere mobile Forschungs- und Erprobungsplattform für Hochenergielaser. Das auf mehrere Standard-Transportcontainer verteilte System verbindet hohe Flexibilität mit realitätsnaher Untersuchung komplexer Zusammenhänge.





Von der Herstellung von Preformen für das Faserziehen bis zum hochintegrierten Prototypen eines Faserlasers: Das Fraunhofer IOSB beherrscht die gesamte Wertschöpfungskette.
Foto: Fraunhofer IOSB / indigo



Die derzeit in Aufbau befindliche HEL-Versuchsanlage HELIKS, hier noch als Rendering: HEL-Quelle, Energieversorgung, Kühlung, Command-and-Control-Center und Messstationen sind über mehrere Transportcontainer verteilt. *Rendering: Fraunhofer IOSB*

Durch seine mobile, in weiten Teilen autarke Auslegung kann es in unterschiedlichen Umgebungen eingesetzt werden und ermöglicht Messungen dort, wo sich entscheidende Effekte tatsächlich zeigen: unter wechselnden atmosphärischen Bedingungen, bei realen Entfernungen und in Szenarien, die sich nicht vollständig in klassische Laborumgebungen übertragen lassen.

HELIKS dient dabei nicht allein als technologischer Demonstrator, sondern vor allem als wissenschaftliche Plattform. Mit der kohärenten Kopplung von mehr als 90 Laserkanälen und einer nominalen Ausgangsleistung von über 100 Kilowatt eröffnet das System einen Untersuchungsraum, der in dieser Form in Deutschland derzeit einzigartig ist. Es ermöglicht uns, Fragen der Strahlkopplung, der atmosphärischen Ausbreitung, der Laserwirkung und der Sicherheit in einem konsistenten Gesamtansatz zu untersuchen. Gerade für militärische Anwendungen ist diese Verknüpfung entscheidend, weil sich die Leistungsfähigkeit von HEL-Systemen erst im Zusammenwirken aller Komponenten realistisch bewerten lässt.

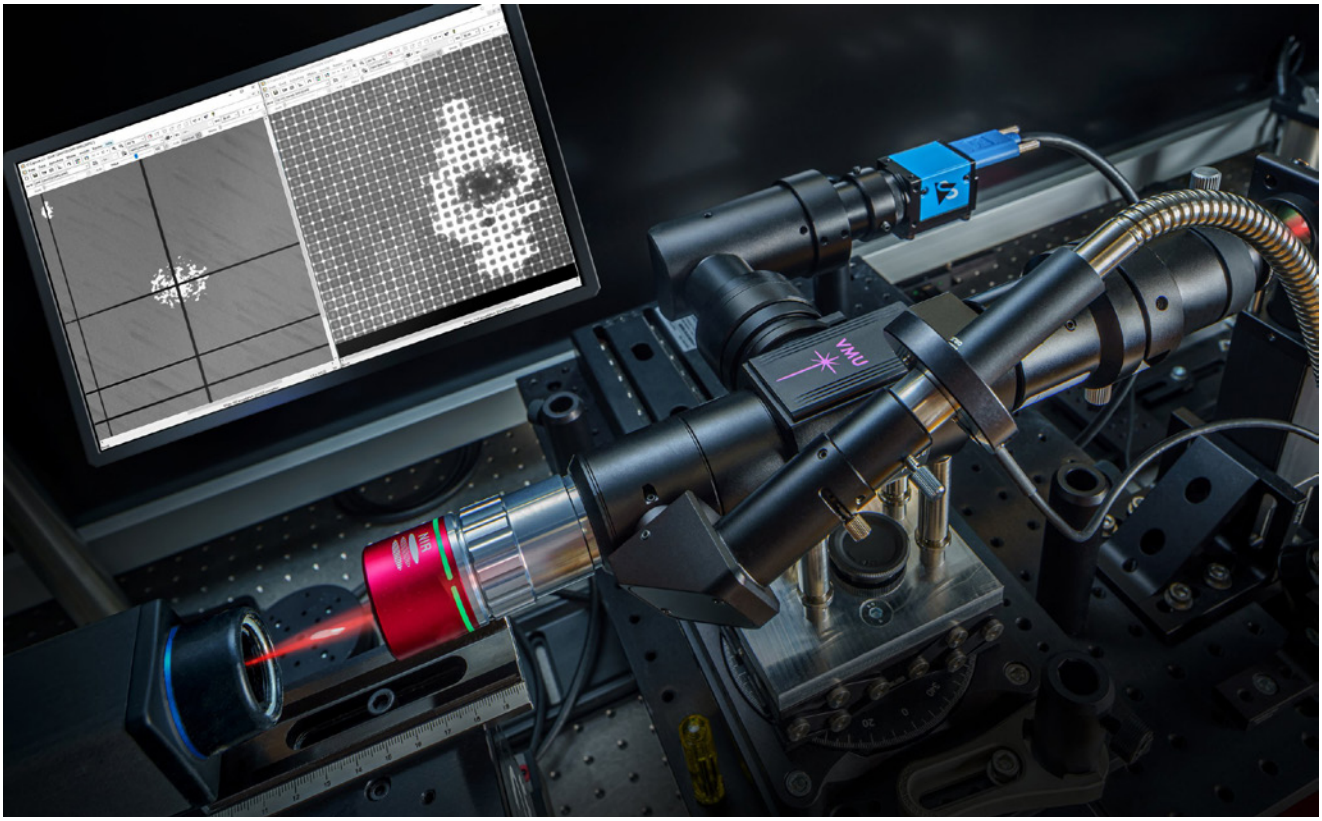
Präzision beginnt bei Sensorik und Ausbreitung

Eine Schlüsselrolle spielt dabei die Zielerfassung und Zielverfolgung. In einem militärischen Kontext geht es häufig um kleine bis mittelgroße, dynamisch bewegte Ziele vor komplexem Hintergrund und unter eingeschränkten Sichtbedingungen. Deshalb erforschen wir mehrstufige Tracking-Ketten, in denen verschiedene Sensortypen ihre jeweiligen Stärken einbringen. Neben elektrooptischen und infraroten Verfahren gehören dazu aktive bildgebende Ansätze wie Gated Viewing und LiDAR. Sie verbessern den Ziel-Hintergrund-Kontrast, liefern zusätzliche Distanz- und Bewegungsinformationen und schaffen damit die Voraussetzung für präzises Feintracking. Denn unabhängig von der verfügbaren Laserleistung gilt: Ohne robuste Zielverfolgung ist keine belastbare Wirkung erreichbar.

Ebenso zentral ist die Frage, wie sich der Strahl auf seinem Weg durch die Atmosphäre verändert. Turbulenz, thermisches Blooming, Absorption, Streuung und mechanischer Jitter beeinflussen die Intensitätsverteilung auf dem Ziel teils erheblich. Für die militärische Praxis ist das keine theoretische Randbedingung, sondern ein maßgeblicher Leistungsfaktor. Deshalb koppeln wir Modellierung und Messung eng miteinander. Wir entwickeln Simulationswerkzeuge, die alle relevanten physikalischen Effekte der Ausbreitung zusammenführen, und validieren diese Modelle mit eigenen Messkampagnen. Ergänzt wird dieser Ansatz durch kontrollierte Untersuchungen in einer eigens entwickelten adiabatischen Wolkenkammer, in der sich Nebel- und Wolkenbedingungen reproduzierbar einstellen lassen. So lassen sich Aussagen über Reichweite, Wirkung und Einsatzgrenzen unter unterschiedlichen Umweltbedingungen deutlich fundierter treffen.

Adaptive Optik und souveräne Schlüsselkomponenten

Um atmosphärisch bedingte Verzerrungen nicht nur zu beschreiben, sondern aktiv zu kompensieren, arbeiten wir an Lösungen der adaptiven Optik. Dazu gehören Hochgeschwindigkeitssensoren zur Wellenfrontmessung ebenso wie Verfahren, mit denen sich Verzerrungen in Echtzeit korrigieren lassen. Besonders anspruchsvoll ist dies bei unkooperativen Zielen, wie sie im militärischen Umfeld typisch sind. Hier entwickeln wir eigene sensorische Ansätze, die auch unter schwierigen Rückstreubedingungen nutzbare Informationen liefern. Ziel ist es, die auf dem Ziel verfügbare Leistungsdichte zu stabilisieren und die Präzision des Gesamtsystems zu erhöhen.



Versuchsaufbau für die Untersuchung von Zerstörschwellen (LIDT) optoelektronischer Komponenten. *Foto: Fraunhofer IOSB / indigo*

Von besonderer strategischer Bedeutung ist außerdem der Bereich Laserquellen, Strahlkopplung und Komponenten. Hier wird technologische Souveränität besonders konkret. Wer bei kritischen Schlüsselkomponenten dauerhaft von externen Lieferketten, eingeschränkter Verfügbarkeit oder nicht transparenten Entwicklungswegen abhängt, bleibt auch bei der Fähigkeitsentwicklung verwundbar. Deshalb forschen wir an kohärenter Strahlkopplung, faserbasierten Laserarchitekturen und spezialisierten Komponenten wie Kopplern, Strippern und neuartigen Fasern. Das gilt sowohl für Systeme um 1 Mikrometer als auch für den Wellenlängenbereich bei 2 Mikrometern, der große Vorteile sowohl bei der Wirkung auf Kunststoff als auch hinsichtlich der Augensicherheit mit sich bringt.

Unser Ziel ist es, zentrale Technologien nicht nur anwenden, sondern auch in Deutschland und Europa bewerten, gestalten und gemeinsam mit Partnern weiterentwickeln zu können. Gerade im militärischen Kontext schafft diese Fähigkeit die Voraussetzung für Resilienz, Weiterentwicklung und glaubwürdige Unabhängigkeit.

Wirkung und Sicherheit gemeinsam denken

Zur Einsatzreife von Hochenergielaser-Systemen gehört schließlich immer auch die belastbare Untersuchung ihrer Wirkung und ihrer Risiken. Wir analysieren, wie Laserstrahlung mit unterschiedlichen Materialien, optischen Komponenten und optronischen Systemen interagiert. Dabei geht es sowohl um die Wirkung auf feste Materialien als auch um die Verwundbarkeit von Sensorik und Optiken. Solche Untersuchungen sind wichtig, um Leistungsgrenzen realistisch einzuordnen, Schutzmaßnahmen abzuleiten und Einsatzkonzepte technisch fundiert zu bewerten.

Ebenso wichtig ist die Sicherheitsbetrachtung. Hochenergielaser stellen besondere Anforderungen an Gefährdungs- und Risikoanalysen, etwa im Hinblick auf Streustrahlung, Reflexionen an Zieloberflächen oder maritime Umgebungen. Wir entwickeln dafür Mess- und Simulationsmethoden, mit denen sich Risiken systematisch erfassen und in künftige Sicherheitskonzepte überführen lassen. Auch hierin liegt ein wesentlicher Beitrag für Bundeswehr, Beschaffung und Industrie: Hochenergielaser als militärische Fähigkeit nicht nur leistungsfähig, sondern auch verantwortbar, beherrschbar und in reale Systemumgebungen integrierbar zu machen.

Das Fraunhofer IOSB bringt damit Kompetenzen zusammen, die für die militärische Nutzung von Hochenergielaser-Systemen entscheidend sind: von Sensorik und Tracking über Ausbreitungsmodellierung und adaptive Optik bis hin zu Quellen, Komponenten, Wirkung und Sicherheit. Unser Beitrag liegt darin, Zusammenhänge sichtbar zu machen, Technologien belastbar zu bewerten und eine wissenschaftliche Grundlage für die Weiterentwicklung vernetzter Wirksysteme zu schaffen. So stärken wir nicht nur die Einsatzreife künftiger Hochenergielaser-Systeme, sondern auch die technologische Souveränität Deutschlands und Europas in einem sicherheitspolitisch hochrelevanten Zukunftsfeld.

BDSV

Bundesverband der Deutschen
Sicherheits- und Verteidigungsindustrie e.V.

innovativ, leistungsfähig, wettbewerbsstark.
Die deutsche SVI.

Der BDSV ist die Stimme der deutschen Sicherheits- und Verteidigungsindustrie (SVI) in Berlin und Brüssel.

Als zentraler Verband bündeln wir die Interessen von Ausrüstern staatlicher Sicherheitsorgane mit dem Ziel, die Wettbewerbsfähigkeit unserer Mitgliedsunternehmen auszubauen.

Unser Netzwerk lebt vom gegenseitigen Austausch mit Politik und Verwaltung, dem intensiven Dialog und dem gemeinsamen Streben nach der Sicherung unseres freiheitlichen Lebens.

SVI-CONNECT

UNSERE WEBSITE

KI-gestützte Drohnenerkennung mit Infrarot- und Videosensorik für Lagebild und Priorisierung

Norbert Heinze und Dr. Alina Lindner, Abteilung Videoauswertesysteme des Fraunhofer IOSB

Norbert Heinze
Foto:Fraunhofer IOSB/indigo

Dr. Alina Lindner
Foto: Fraunhofer IOSB/Fotosassa

Drohnen prägen zunehmend das Gefechtsfeld und sind zudem ein Mittel hybrider Bedrohung: Sie werden im Umfeld kritischer Infrastrukturen, militärischer Sicherheitsbereiche und anderer sensibler Einrichtungen zu einem wachsenden Risiko. Ihre Detektion, Erkennung, Analyse und Bekämpfung sind deshalb wesentliche Fähigkeiten für den Schutz von Truppe, Liegenschaften und ziviler Sicherheit. Passiven Infrarot- und Videosensoren kommt dabei eine wichtige Rolle zu, weil sie im Verbund mit anderen Systemen einen entscheidenden Beitrag zur Situationsanalyse leisten können.

Für die Drohnenabwehr reicht es jedoch nicht aus, ein Objekt nur zu entdecken. Entscheidend ist, anfliegende Drohnen in Echtzeit zu erkennen, von Verwechslungsobjekten wie Vögeln zu unterscheiden und zusätzliche Informationen über Art und mögliche Nutzung zu gewinnen. Genau hier setzen unsere KI-Verfahren an: Sie werten Bilddaten aus dem visuellen und infraroten Spektralbereich aus und führen von der bloßen Erstdetektion zu einer fundierten Lagebewertung als Grundlage für Priorisierung und weitere Maßnahmen in der Drohnenabwehr.

Vom Sensorsignal zur belastbaren Einordnung

Infrarot- und Videosensoren liefern Bilddaten anfliegender Objekte, die von unseren KI-Verfahren in Echtzeit analysiert werden. Auf diese Weise lassen sich Drohnen detektieren, verfolgen und analysieren. Die Verfahren müssen dabei in der Lage sein, kleine Drohnen auch vor unterschiedlichen Hintergründen wie Vegetation oder Bebauung zu erkennen und sie nicht mit anderen Objekten wie Vögeln oder aufgewirbelten Gegenständen zu verwechseln. Ebenso müssen sie mit variierenden Beleuchtungssituationen und unterschiedlichen Blickwinkeln zurechtkommen. Der Mehrwert der KI-Auswertung geht dabei deutlich über die reine Erkennung hinaus. Wir realisieren Verfahren zur Unterscheidung verschiedener Klassen von Drohnen und insbesondere zur Detektion von Nutzlasten. Dabei kann es sich etwa um Sensorik, Funkausstattung, abwerfbare Munition oder fest verbaute Sprengkörper handeln. Solche Informationen ermöglichen es, das Gefährdungspotenzial eines Objekts deutlich besser einzuschätzen und bei mehreren gleichzeitig auftretenden Zielen weitere Maßnahmen zu priorisieren.

Robuste Verfahren trotz knapper Trainingsdaten

Damit diese KI-Verfahren zuverlässig arbeiten, benötigen sie große Mengen annotierter Bilddaten, in denen die relevanten Objektklassen aus verschiedenen Blickwinkeln, bei unterschiedlichen Beleuchtungssituationen und in unterschiedlichen Umgebungen enthalten sind. Schon im visuellen Bereich ist der Aufbau solcher Datensätze auf-

Die am Fraunhofer IOSB entwickelten Videoauswerteverfahren detektieren Drohnen auch vor schwierigen Hintergründen und unterscheiden sie zuverlässig von anderen Objekten wie etwa Vögeln. *Foto: Fraunhofer IOSB*

Die Erkennung von Nutzlasten ermöglicht die Einschätzung der Gefährlichkeit.

Foto: Fraunhofer IOSB

Unterschiedliche Drohnen, variierende Beleuchtung, verschiedene Blickwinkel: Trainingsdaten für die KI-Detektion. *Foto: Fraunhofer IOSB*

wändig. Im Infrarot-Bereich ist die Verfügbarkeit geeigneter Trainingsdaten noch stärker eingeschränkt. Genau deshalb erforschen und nutzen wir spezielle Techniken des frugalen Lernens, also des Lernens mit wenigen Trainingsdaten. Dazu gehören die gezielte Variation vorhandener Daten, die Adaption visuell-optischer Daten für Infrarot-Verfahren und das Lernen mit kleinen annotierten Datensätzen.

Diese Forschungsarbeit ist eng mit unseren Erfahrungen aus anderen Echtzeitverfahren der videobasierten Aufklärung verbunden. Auch dort müssen Objekte und ihr Verhalten in variabler Umgebung und unter wechselnden Beleuchtungsbedingungen in visuellen und infraroten Bildern analysiert werden. Für die Drohnenabwehr bedeutet das: Die Leistungsfähigkeit eines Systems hängt nicht nur von der Sensorik ab, sondern in hohem Maß von der Qualität der trainierten KI-Modelle und ihrer Robustheit unter realen Einsatzbedingungen.

MODEAS als integrierter Systemrahmen

Diese Verfahren integrieren wir in MODEAS, unser modulares Drohnenerfassungs- und Assistenzsystem. Auf Basis einer Erstdetektion – vorzugsweise per Radar oder per Weitwinkelkamera, um auch für autonome Drohnen wirksam zu sein, die keine Funksignale aussenden – erfolgt eine Voreinweisung und eine Tele- bzw. Zoomkamera schwenkt automatisch auf das potenzielle Ziel ein. Anschließend detektieren, klassifizieren und verfolgen KI-Verfahren die Drohne im Videostrom weiter. Der multisensorische Ansatz verbindet damit die Reichweite der Erstdetektion mit der Genauigkeit optischer Auswertung. MODEAS ist dabei modular, multisensorisch und offen ausgelegt. Unterschiedliche Sensoren und nachgelagerte Systeme lassen sich einbinden, ihre Daten zu einem einheitlichen Lagebild zusammenführen. Für den menschlichen Entscheidungsträger werden relevante Informationen übersichtlich aufbereitet – etwa Position auf der Karte bzw. in einem 3D-Lagebild, Entfernung, Höhe, Geschwindigkeit, Typ und das zugehörige Live-Videobild.

MODEAS-Experimentalsystem in Aktion: Nach Erstdetektion durch eine Weitwinkelkamera visieren die Tele-Zoomkamera und der Laser-Entfernungsmesser auf dem Schwenk-Neigekopf (großes Bild) die Drohne automatisch an und liefern detailliertere Daten. *Foto: Fraunhofer IOSB*

Dokumentation und Nachvollziehbarkeit von Überflügen

Ein zusätzlicher Mehrwert liegt in der Speicherung und Dokumentation erkannter Ereignisse. Bei der Erkennung einer fliegenden Drohne werden automatisch Bilder und Ergebnisse der KI-Auswertung im Bild eingestanzt und in einem Videoclip gesichert. Sichtungen und Überflüge lassen sich dadurch im Nachhinein analysieren und nachvollziehen. Diese Fähigkeit ist nicht nur für die unmittelbare Lagebewertung relevant, sondern auch für die Nachbereitung von Vorfällen.

Gerade im Umfeld kritischer Infrastrukturen, militärischer Sicherheitsbereiche oder anderer sensibler Lagen kann eine solche forensische Dokumentation einen wichtigen Zusatznutzen bieten. Sie macht Ereignisse nachvollziehbar, unterstützt die spätere Bewertung und schafft eine belastbare Grundlage für weiterführende Analysen. Damit erweitert sich der Nutzen des Systems über die reine Echtzeitdetektion hinaus.

Im Gesamtkontext der Drohnenabwehr ist die KI-gestützte Auswertung mit Infrarot- und Videosensorik damit ein besonders wertvoller Baustein. Sie überführt passive Bilddaten in operative Information, reichert Tracks mit zusätzlichen Erkenntnissen an und verbessert die Einschätzung von Bedrohungen. Aus einer Erstdetektion wird eine belastbare Entscheidungsgrundlage – und damit ein wesentlicher Beitrag zu einer wirksamen und differenzierten Drohnenabwehr.

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

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

Dr. Annika-Kathrin Belz
Foto: UnIBw M/Wagener

„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.

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. 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, Cyber-Sicherheit, 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.

Reifephase und verstärkter Transfer

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 weltraumgestützter 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

Präsidentin Prof. Eva-Maria Kern präsentiert Verteidigungsminister Boris Pistorius die dtec.bw-finanzierte Kleinsatellitenmission SeRANIS.
Foto: UniBw M/Siebold

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 techno-

Gemeinsames Grußwort der Präsidenten der beiden UniBw an der dtec.bw Jahrestagung 2025. *Foto: UniBw M/Petzold*

Einführung in die dtec.bw Jahrestagung durch die beiden Vizepräsidenten Forschung beider UniBw. *Foto: UniBw M/Petzold*

logischen Souveränität. In diesem Jahr wird dtec.bw bereits das vierte Mal auf der AFCEA als Aussteller vertreten, sein und u.a. das dtec.bw Projekt SeRANIS und Orbint am Stand vorstellen (siehe Artikel auf Seite 46).

Neue Impulse und Projektpräsentationen

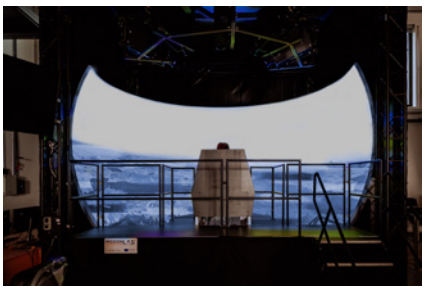
Bereits zu Beginn des Jahres 2026 setzte dtec.bw starke Impulse im Innovationsökosystem der Bundeswehr. Beim Palladion-Event „SPARK 26“ im Umfeld der Munich Security Conference war dtec.bw vertreten. Auf der Enforce Tac in Nürnberg präsentierten Projekte wie SPARTA zur Analyse von Desinformation, MuQuaNet 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 15.09.-16.09.2026 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 2020–2026.

Die Anmeldung zur dtec.bw Jahrestagung 2026 ist hier möglich: https://dtecbw.de/home/jahrestagung

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.



Flugsimulator im dtec.bw Projekt MissionLab. *Foto: UniBw M/Wagener*

Fahrsimulator im dtec.bw Projekt MORE. *Foto: UniBw M/Wagener*

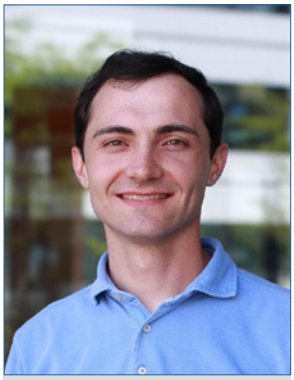
Digitale Ersthelferausbildung im dtec.bw Projekt Smart Health Lab. *Foto: UniBw/Panzau*

Vom In-Orbit-Labor zur einsatznahen Fähigkeit: SeRANIS und Orbint bringen Tempo ins elektromagnetische Lagebild

Apl. Prof. Dr.-Ing. Christian Hofmann, Stellv. Direktor Munich Center for Space Communications und Projektleiter GENA-OT Mission; **Dr.-Ing. Robert Schwarz,** Leiter Forschungsgruppe Satellitennetzwerke; **Simon Heine,** Co-founder & Co-CEO Orbint

Apl. Prof. Dr.-Ing. Christian Hofmann
Foto: UniBw M, Sabrina Simone

Dr.-Ing. Robert Schwarz
Foto: UniBw M, Sabrina Simone



Simon Heine
Foto: UniBw M, Sabrina Simone

Im elektromagnetischen Spektrum entscheidet sich zunehmend, was Streitkräfte und Sicherheitsbehörden sehen und wie schnell sie handeln können. GNSS-Störungen, aktive Radargeräte, Funkteilnehmer oder Störsender hinterlassen Signaturen, aus denen sich Lageinformation gewinnen lässt. Gleichzeitig steigen die Anforderungen der Nutzer: Erkenntnisse müssen zeitnah, belastbar und über große Räume verfügbar sein, damit sie in Führungs- und Entscheidungsprozesse einfließen können.

Genau an dieser Schnittstelle setzt SeRANIS (Seamless Radio Access Networks for Internet of Space) an. Als dtec.bw-Projekt der Universität der Bundeswehr München ist ein Technologie- und Demonstrationsprogramm entstanden, das nicht isoliert Einzelkomponenten betrachtet, sondern ein „Netzwerk von Netzwerken“: Mission, Bodenstationen, Auswertung und Betriebsprozesse. Leitgedanke ist „vom Einsatz her denken“, das heißt der Nutzer wird in den Fokus gestellt. Gleichzeitig schafft SeRANIS offene Schnittstellen, über die Start-ups und Industrie neue Technologien im Verbund testen und auch der Bundeswehr demonstrieren wollen.

Übertragung in die Praxis

Dass dieser Ansatz nicht im Labor endet, zeigen die jüngsten Fortschritte im Orbit. Am 28. November 2025 wurde die CubeSat-Plattform GENA-OT auf SpaceX’ Transporter-15 gestartet. Die UniBw M nutzt sie im SeRANIS-Kontext als Testplattform für Schlüsseltechnologien wie Kommunikation, Erdbeobachtung, Strahlungsschutz und Künstliche Intelligenz. Rapid Prototyping kommt damit in der Praxis an: Die Universität betont, dass es auch für die Bundeswehr möglich ist, eine Satellitenmission in kürzester Zeit von der Idee bis zur Einsatzbereitschaft im Weltall durchzuführen und sogar kurzfristig zusätzliche Nutzlasten zu integrieren, um einen Bedarf zu decken. Für 2026 ist mit dem Satelliten ATHENE-1 eine weitere Mission mit über 15 Experimenten geplant.

Tests unter realen Bedingungen

SeRANIS verbindet In-Orbit-Demonstration mit Bodentests, dazu wird unter anderem auf dem Campus der UniBw M ein 5G/6G-Testbed mit Satellitenanbindung aufgebaut. Außerdem wird eine für Europa einzigartige Forschungsbodenstation für Satellitenkommunikation durch ein Laserkommunikationsterminal erweitert, um terrestrische Kommunikationstechnologien in Kombination mit ATHENE-1 „in den Weltraum zu verlängern“. Damit lassen sich neue Endgeräte, Netzwerkkomponenten oder Softwarefunktionen früh unter realen Bedingungen testen und demonstrieren, ein entscheidender Faktor, wenn Technologien später unter Zeitdruck in den Betrieb überführt werden sollen.

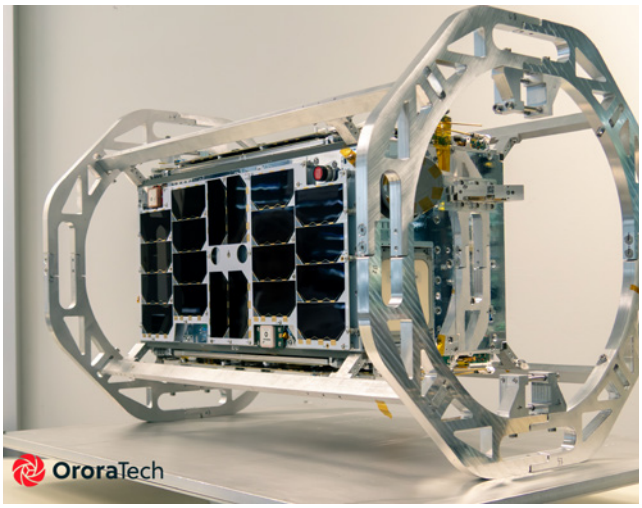
Zu einsatznaher Bewertung gehört außerdem professioneller Missionsbetrieb. Die UniBw M erprobt hierfür innerhalb SeRANIS Verfahren, Werkzeuge und End-to-End-Tests, die den parallelen Betrieb vieler Nutzlasten erlauben. Für Behörden ist dieser Aspekt besonders relevant: Weltraumsysteme müssen nicht nur leistungsfähig, sondern auch sicher und robust betrieben werden. Orientierung geben dabei Standards wie die Technische Richtlinie BSI TR-03184 zur Informationssicherheit für Weltraumsysteme.

Aus dieser Plattform und der daraus resultierenden Erfahrung heraus ist die Ausgründung Orbint entstanden. Das Spin-off aus dem SeRANIS-Programm entwickelt einen neuen Ansatz für satellitengestützte Signalaufklärung: Ein verteiltes Satellitennetz soll verschiedenste Emitter detektieren, identifizieren und präzise geolokalisieren. Ein Kernpunkt ist die Datenverarbeitung bereits an Bord, um schneller von Rohdaten zu verwertbaren Erkenntnissen

zu kommen mit dem Ziel, nahezu in Echtzeit ein aktuelles elektromagnetisches Lagebild bereitzustellen. Ein wichtiger Schritt Richtung Industrialisierung folgte im November 2025: Rohde & Schwarz beteiligte sich an Orbint. Die Partnerschaft bündelt Start-up-Tempo mit industrieller Umsetzungskraft und adressiert explizit technologische Souveränität. Anspruch ist es, der Bundeswehr eine souveräne Lösung mit nationalen Kapazitäten für signalerfassende Aufklärung aus dem All zu bieten und diese innovativ weiterzuentwickeln.

SeRANIS liefert die nutzerorientierte Demonstrationsumgebung im Orbit und am Boden; Orbint übersetzt Forschungsergebnisse in eine skalierbare, anschlussfähige Lösung. Wer am gemeinsamen Stand auf der AFCEA Fachausstellung das Gespräch sucht, findet damit ein konkretes Beispiel dafür, wie Forschung der UniBw M – gestützt durch dtec.bw – zügig in operative Wirkung überführt werden kann.

Das Projekt SeRANIS läuft bis Ende 2026 und wird aus Mitteln des dtec.bw finanziert. Das dtec.bw – Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr – ist ein an beiden Universitäten der Bundeswehr gemeinsam getragenes wissenschaftliches Zentrum. Es unterliegt der akademischen Selbstverwaltung. Die Mittel, mit dem das dtec.bw ausgestattet wurde, werden an beiden Universitäten der Bundeswehr zur Finanzierung von Forschungsprojekten und Projekten zum Wissens- und Technologietransfer eingesetzt. dtec.bw wird von der Europäischen Union – NextGenerationEU finanziert.



Die von OroraTech entwickelte Nanosatellitenplattform GENA dient als standardisierte Trägerstruktur für unterschiedliche Nutzlasten. Ähnlich dem Fahrgestell eines Autos stellt GENA die grundlegende Satelliteninfrastruktur bereit, auf der Kunden ihre Experimente und Technologien im Orbit betreiben und testen können, ohne einen eigenen Satelliten entwickeln zu müssen.
Foto: OroraTech

Software Supply Chain Management: Ein „neuer“ Blick auf Bedeutung, Risiken, Transparenz und Resilienz von Software-Lieferketten für moderne Produkte

Maximilian Holzner; Andreas Glas; Michael Eßig, Universität der Bundeswehr München, Arbeitsgebiet Beschaffung

Maximilian Holzner
Foto: privat

Andreas Glas
Foto: privat

Michael Eßig
Foto: privat

Software als zentrales Wertschöpfungselement

Software wird zunehmend zum zentralen Wertschöpfungselement moderner Produkte. Ob im Kontext von Software Defined Defence, Software Defined Vehicle oder Software Defined Power Grids, immer mehr Funktionen physischer Systeme werden durch Software implementiert und gesteuert. Mit dieser Entwicklung steigt nicht nur die funktionale, sondern auch die ökonomische Bedeutung der Software für die Wertschöpfung moderner Systeme. So ist die Zahl der Codezeilen in Fahrzeugen bereits auf über 100 Millionen angestiegen und wird Prognosen zufolge bis 2027 auf mehr als 600 Millionen anwachsen. Auch in der Militärtechnik, wie modernen Kampfflugzeugen, hat sich der Softwareumfang seit den frühen 2000er-Jahren um rund 1.300 % auf etwa 24 Millionen Codezeilen erhöht. Selbst die Leistungsfähigkeit kritischer Infrastrukturen wie Stromnetze hängt maßgeblich von Software ab.

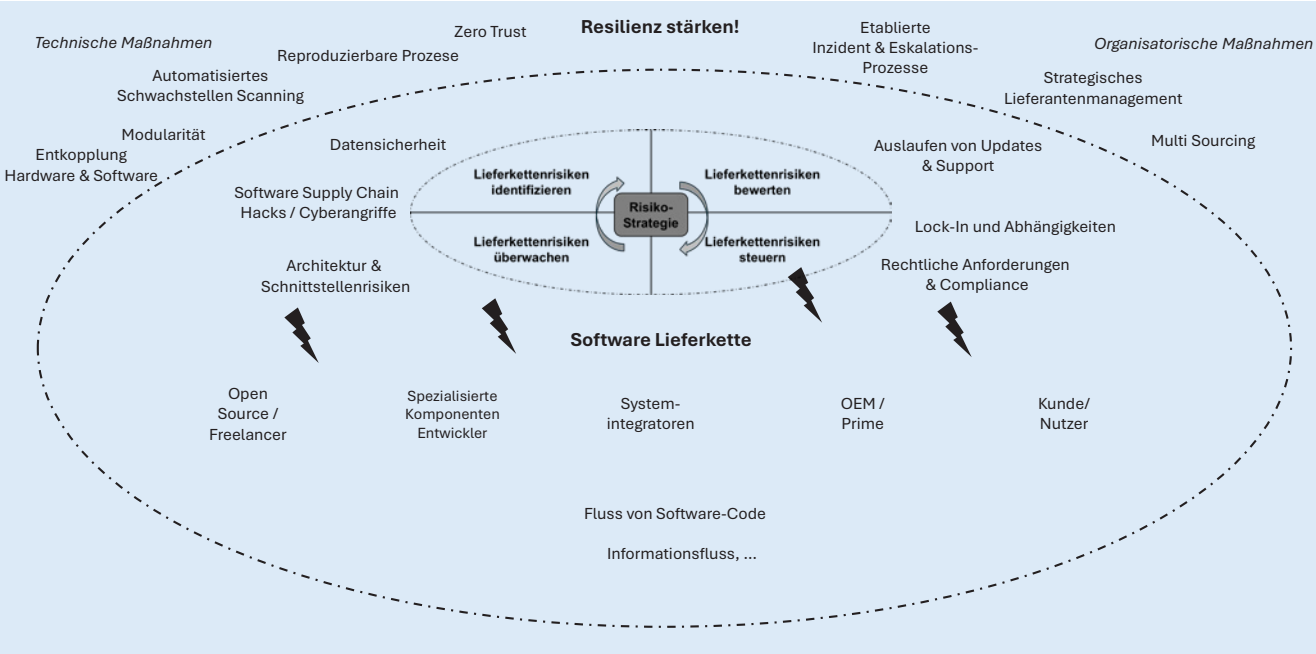
Entstehung von Software-Lieferketten

Diese Entwicklung verändert die Organisation von Wertschöpfung grundlegend. Wie physische Produktionssysteme sind auch softwarebasierte Wertschöpfungsprozesse arbeitsteilig organisiert und beruhen auf der Kooperation spezialisierter Akteure, von Open-Source-Entwicklern über Freelancer bis hin zu globalen Technologiekonzernen. So beträgt der Anteil extern entwickelter Software bei Automobilherstellern Berichten zufolge bis zu 90 %. Eine Befragung der Universität der Bundeswehr München bei 104 Unternehmen der deutschen Sicherheits- und Verteidigungsindustrie hat ergeben, dass der Anteil digitaler Komponenten bei Rüstungsgütern schon heute bei über 55 % liegt und sogar auf über ⅔ steigen wird. Die Hälfte der eingesetzten Software stammt dabei von externen Lieferanten, ist also das Ergebnis einer Lieferkette. Das betrifft nicht nur die Interaktion von Software in und zwischen Waffensystemen, sondern auch vielfältige Unterstützungsdienste wie Lagerbewirtschaftungs- und ERP-Systeme sowohl der Bundeswehr als auch ihrer Lieferanten (SAP, SASPF). Durch die Integration zahlreicher externer Softwarekomponenten entstehen zunehmend komplexe, hochgradig vernetzte Softwarelieferketten mit vielfältigen Abhängigkeiten. Software Defined Defence muss das Problem der Software Supply Chains adressieren, wenn es erfolgreich implementiert bzw. weiterentwickelt werden soll.

Neue Risikodimensionen

Softwarelieferketten weisen spezifische Verwundbarkeiten auf und können gezielt als Angriffsvektor genutzt werden. Zwei prominente Fälle verdeutlichen diese Problematik. Im Jahr 2020 kompromittierten Angreifer ein Softwareupdate des Unternehmens SolarWinds, das anschließend an tausende Kunden, darunter US-Bundesbehörden und Technologieunternehmen wie Microsoft, ausgeliefert wurde. Die Angreifer erhielten dadurch Zugriff auf Systeme zahlreicher Organisationen. Ein weiteres Beispiel betrifft die Open-Source-Bibliothek xz-utils: Angreifer bauten über mehrere Jahre hinweg Vertrauen innerhalb der Entwicklergemeinschaft auf, erlangten Maintainer-Rechte und integrierten eine Hintertür in eine neue Version der Bibliothek. Diese hätte potenziell verdeckten Zugriff auf zahlreiche Linux-Systeme ermöglicht. Die Manipulation wurde jedoch während der Testphase entdeckt.

Diese Fälle verdeutlichen die Anfälligkeit von Softwarelieferketten gegenüber gezielten Cyberangriffen. Gleichzeitig steigt die Zahl solcher Angriffe, laut Sonatype, jährlich um über 740 %. Das Risikoprofil von Softwarelieferketten ist je-



Softwarelieferkette mit ausgewählten Risiken und Ansatzpunkten zur Stärkung der Resilienz. *Grafik: UniBw München*

doch deutlich breiter. Neben bösartigen Angriffen bestehen weitere Risiken, etwa rechtliche Anforderungen aus Open-Source-Lizenzen, zunehmende Regulierung, die Insolvenz von Softwarelieferanten oder strukturelle Abhängigkeiten von wenigen dominanten Technologieanbietern. Beispielsweise kontrollieren die drei größten US-Cloud-Anbieter allein zwei Drittel des weltweiten Cloud-Markts. Hinzu kommen auslaufende Wartungs- und Updateleistungen sowie Abstimmungsprobleme bei Schnittstellen und Architekturen über Unternehmensgrenzen hinweg.

Bedarf an neuen Lösungsansätzen

Im Vergleich zu physischen Lieferketten weisen Softwarelieferketten eine andere Qualität von Komplexität auf. Kurze Innovationszyklen erzeugen eine hohe Dynamik, sodass sich Lieferstrukturen kontinuierlich verändern oftmals ohne, dass alle Beteiligten umfassende Transparenz besitzen. In einer Umfrage von JFrog im Jahr 2025 gaben 75 % der Unternehmen an, nicht oder nur bedingt zuversichtlich zu sein, ausreichende Transparenz und Kontrolle über ihre eigene Softwarelieferkette zu besitzen. In einem Software Defined-Produkt trifft „updatefähige“ Software auf weiter nutzbare, weitgehend unveränderte Hardware. Dadurch entwickeln sich derartige Produkte zu Systemen zweier Geschwindigkeiten. Dies erhöht die Integrationsanforderungen erheblich, da externe Komponenten laufend in Architekturen, Entwicklungsprozesse und Sicherheitskonzepte eingebunden werden müssen. Hinzu kommt eine andere Kostenlogik. Software kann vereinfacht ohne großen Einsatz von Zeit und Ressourcen reproduziert werden. Folglich erfordern Software Supply Chains schnellere und adaptivere Steuerungsmechanismen, als dies bislang der Fall war. Gleichwohl existieren bereits zahlreiche technische Maßnahmen zur Reduktion von Risiken in Softwarelieferketten, darunter automatisierte Schwachstellenanalysen, Threat Modelling oder Zero-Trust-Architekturen. Diese Maßnahmen tragen dazu bei, Sicherheitsniveaus zu erhöhen, können jedoch vollständige Sicherheit nicht garantieren. Auch nicht bösartige Risiken, etwa Lieferantenausfälle oder starke Abhängigkeiten, lassen sich mit etablierten Instrumenten des Supply Chain Managements adressieren, beispielsweise durch Beschaffung aus mehreren unabhängigen Quellen oder durch gezielte Weiterentwicklung von Zulieferern. Da Sicherheitsmaßnahmen stets mit Kosten und Ressourcen verbunden sind, ist vollständige Risikovermeidung in der Praxis nicht realisierbar. Ziel ist vielmehr, Angriffe ökonomisch unattraktiv zu machen und die Eintrittswahrscheinlichkeit und Auswirkungen von Störungen zu begrenzen.

Resilienz als zentrale Zielgröße

Resilienz wird zur zentralen Zielgröße eines Software Supply Chain Management. Resilienz bezeichnet die Fähigkeit einer Lieferkette, sich auf unerwartete Ereignisse vorzubereiten, auf diese zu reagieren und sich anschließend zu erholen. Resilienz ist dabei keine isolierte Eigenschaft einzelner Organisationen, sondern eine gemeinsame Aufgabe aller Akteure innerhalb der Softwarelieferkette. Sicherheitslücken oder Störungen müssen dort adressiert werden, wo sie entstehen – häufig bei vorgelagerten Lieferstufen. Während Risikominderungsstrategien primär darauf abzielen, die Eintrittswahrscheinlichkeit und potenzielle Schadenshöhe einzelner Risiken zu reduzieren, fokussieren Resilienzstrategien auf die Fähigkeit der Softwarelieferkette, auch bei Eintritt unvermeidbarer Störungen funktionsfähig zu bleiben oder sich schnell zu erholen. Resilienz ergänzt damit klassische Risikosteuerung, ersetzt diese jedoch nicht. Eine zentrale Voraussetzung für Software Supply Chain Resilienz ist Transparenz. Werkzeuge wie Software Bills of Materials (SBOMs) gewinnen hierbei zunehmend an Bedeutung und finden inzwischen auch Eingang in regulatorische Anforderungen. Eine Studie von ONEKEY aus dem Jahr 2024 zeigt, dass lediglich 24 % der befragten

deutschen Industrieunternehmen eine vollständige SBOM führen. Im internationalen Vergleich weist eine Erhebung der Linux Foundation darauf hin, dass bereits 47 % der befragten Organisationen im Jahr 2021 SBOMs erzeugten und 78 % planten, dies künftig zu tun. Gleichzeitig zeigt eine Umfrage von Lineaje aus dem Jahr 2025, dass 47 % der befragten Unternehmen noch gar nicht mit der SBOM-Integration begonnen haben oder sich erst in Testphasen befinden.

Auf Basis der Transparenz ist eine systematische Risikobewertung erforderlich. Lösungsansätze entstehen dabei iterativ durch Risikoidentifikation, Risikobewertung, Risikosteuerung sowie kontinuierliche Kontrolle. Die Risikosteuerung umfasst dabei Maßnahmen zur Risikovermeidung, Risikoübertragung oder Risikoakzeptanz. In der Praxis handelt es sich dabei um eine Kombination technischer und Managementmaßnahmen. Wer Software als zentrales Wertschöpfungselement versteht, muss seine Softwarelieferkette aktiv gestalten und steuern.

Eine mögliche Resilienzstrategie ist die Reduktion kritischer Abhängigkeiten, etwa durch Mehrquellenstrategien für zentrale Softwarekomponenten oder durch modulare Softwarearchitekturen, die Austauschbarkeit von Komponenten ermöglichen. Ergänzend erhöhen reproduzierbare Prozesse Integrität und Nachvollziehbarkeit von Softwareartefakten und reduzieren Manipulationsrisiken entlang der Lieferkette. Darüber hinaus sind vordefinierte Notfall- und Eskalationsprozesse mit Softwarelieferanten erforderlich, die Zuständigkeiten, Kommunikationswege und Wiederanlaufmechanismen im Störungsfall klar regeln. Eine weitere Strategie liegt im strategischen Lieferantenmanagement, das über kurzfristige Vertragsbeziehungen hinausgeht und auf langfristige Partnerschaften, ein gemeinsames Verständnis kritischer Abhängigkeiten sowie die gezielte Entwicklung besonders relevanter Softwarelieferanten abzielt. Ziel ist es, die Funktionsfähigkeit und Anpassungsfähigkeit der Softwarelieferkette auch unter Störungsbedingungen sicherzustellen.

Die Rolle der Beschaffung

Der Beschaffung kommt in diesem Kontext eine zentrale Rolle zu. Externe Softwarekomponenten gelangen über Beschaffungsprozesse in die Organisation. Dadurch verfügt der Einkauf über einen strukturellen Überblick über die Lieferantenlandschaft. Anforderungen an Transparenz, etwa die Bereitstellung von SBOMs – auch durch Vorlieferanten – lassen sich daher wirksam in der Beschaffung verankern. Dies erfordert eine Kombination von Technologie- und Marktwissen. Beschaffung wird damit zu einer strategischen Steuerungsfunktion für Software-Lieferketten und geht weit über eine „passive“ Auftragsvergabe hinaus – und gleichzeitig erfordert „echtes“ Software Supply Chain Management funktions- wie organisationsübergreifendes Arbeiten.

Diese Forschungsarbeit wird durch dtec.bw – Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr finanziert. dtec.bw wird von der Europäischen Union – NextGenerationEU finanziert.

Drone Resilience Day

Die technologische Entwicklung macht vor dem Luftraum nicht halt – und damit wachsen auch die Herausforderungen für die deutsche Sicherheitsarchitektur. Am 7. Juli 2026 wird das geschichtsträchtige Gelände des Infocenters Berlin TXL am Flughafen Tegel zum Epizentrum für eines der drängendsten Sicherheitsthemen unserer Zeit: der Abwehr unbemannter Luftfahrtsysteme (UAV). Der Drone Resilience Day, bringt die entscheidenden Akteure aus Politik, Behörden und Streitkräften zusammen, um Lösungen für eine neue Ära der Bedrohung zu finden.

Vom Helfer zum Hochrisiko: Die neue Bedrohungslage

Lange Zeit konzentrierte sich die öffentliche Debatte über Drohnen an zwei Polen: Katastrophen-Hilfe auf der einen und militärische Einsatzszenarien auf der anderen Seite. Doch dieses Bild ist überholt. Längst sind UAV Mittel hybrider Kriegsführung – dienen zur Destabilisierung und Provokation. Drohnen ungeklärter Herkunft kreisen über Krankenhäusern, Energieinfrastruktur und Bildungseinrichtungen. Auch Liegenschaften der Bundeswehr sind vor ihnen nicht sicher. Die Gefahr ist in Deutschland angekommen.

Die Bundesregierung reagiert und bringt erste Gegenmaßnahmen auf den Weg. Änderungen im Luftfahrtgesetz, neues Material und Ausbildungsinhalte für die Polizeien sollen rechtliche Rahmenbedingungen schärfen und den Sicherheitsbehörden Mittel in die Hand geben. Doch rein normativ ist dem Problem nicht beizukommen. Ein holistischer Ansatz, der Recht, Technologie, Kultur und Operation zusammenbringt ist gefragt. Der Drone Resilience Day bietet den Rahmen diese zu entwickeln.

Theorie und Praxis verknüpft

Am Flughafen Tegel kommt der strategische Dialog mit operativer Anschaulichkeit zusammen. Deshalb startet der Tag direkt dort, wo die Theorie auf die Realität trifft: auf dem Flugfeld.

Technik im Live-Einsatz

- In mehreren Demo-Slots präsentieren Partner wie Globe Flight, wie moderne Detektions- und Abwehrsysteme im operativen Umfeld funktionieren.
- Die Teilnehmer erleben hautnah, wie Drohnen im Luftraum identifiziert und – falls nötig – unschädlich gemacht werden können.
- Parallel dazu bietet die „Testing Time II“ am Nachmittag Raum für vertiefende praktische Beispiele, während das Catering den Rahmen für informelles Networking bietet.

Aus dem Nebel zur Einsicht

Eine zentrale Herausforderung der Drohnenabwehr ist der Umgang mit Daten. Wie kann die relevante Information aus dem sensorischen Grundrauschen herausgefiltert werden? – Wie eine effiziente Auswertung der Datenflut gelingen? Prof. Dr. Wolfgang Koch*, Chief Scientist des Fraunhofer-Instituts für Kommunikation, Informationsverarbeitung und Ergonomie (FKIE), nimmt sich dieser Frage an. Ergänzt werden diese technischen Einblicke durch die Anwender-Perspektive:

- Thomas Vieweg*, Leiter des Drohnenkompetenzzentrums Bayern, berichtet aus der Praxis der Länderpolizeien.
- Die Bundeswehr stellt ihre Expertise durch Vertreter der Steuergruppe „Aufbau Innovation“ und des Drohnenabwehrzentrums vor.
- Grit Tüngler*, Präsidentin des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe (BBK), beleuchtet die zivile Komponente der Resilienz.

Die politische und rechtliche Dimension

Auch die potenteste Technologie bleibt ohne klare gesetzliche Vorgaben zahnlos. Eine der Kernfragen der Veranstaltung lautet daher: Reicht die geplante Änderung des Bundespolizeigesetzes aus, oder braucht es einen judikativen Paradigmenwechsel?

Unter dem Titel „Aufgabenkritik für eine rechtliche und technische Ertüchtigung“ nehmen sich dieser Frage an:

- Andreas Schmenkel-Backhoff*, Inspekteur der Bereitschaftspolizeien der Länder im BMI.
- Marcel Emmerich* (Bündnis 90/Die Grünen), Alexander Throm* (CDU) und Dr. Johannes Fechner* (SPD) als innenpolitische Experten des Deutschen Bundestages.
- Vertreter des Operativen Führungskommandos der Bundeswehr.

**angefragt*

www.drone-resilience.de

AFCEA Bonn e.V.

39. AFCEA Fachausstellung 2026

12. – 13. Mai 2026 | World Conference Center Bonn

Vernetzt denken & sicher handeln als Antwort einer gesamtstaatlichen Verteidigung

Der Treffpunkt der IT-Community, Bundeswehr und BOS

Programm
der AFCEA Fachausstellung 2026

Ausstellerverzeichnis
AFCEA Fachausstellung 2026

Industrievorträge
AFCEA Fachausstellung 2026

Programm AFCEA FA 2026

Vorträge der Keynotes und Symposien finden im ehemaligen Plenarsaal des Bundetages statt

Vernetzt denken & sicher handeln als Antwort einer gesamtstaatlichen Verteidigung

12. – 13. Mai 2026 | World Conference Center Bonn

Dienstag, 12. Mai 2026 | 09:00 Uhr – 18:00 Uhr	
09:50 Uhr	**Begrüßung/Eröffnung der 39. AFCEA Fachausstellung** Generalmajor Armin Fleischmann, Vorstandsvorsitzender AFCEA Bonn e.V. Oberst a.D. Wolfgang Quirin, Leiter der AFCEA Fachausstellung
10:00 Uhr	**Grußwort** des Oberbürgermeisters der Bundesstadt Bonn, Guido Déus
10:10 Uhr	**Key Note:** General a.D. Jörg Vollmer, ehem. Befehlshaber des Allied Joint Forces Command der NATO in Brunssum (NL)
18:00 Uhr – 22:00 Uhr	**Get-together der AFCEA Fachausstellung 202**

Mittwoch, 13. Mai 2026 | 09:00 Uhr – 17:00 Uhr	
10:00 Uhr – 11:00 Uhr	**Digital Defence Debate** **Organisation und Moderation:** Emerging Leaders der AFCEA Bonn e.V.
11:05 Uhr – 12:00 Uhr	**Startup Pitch & Panel Session** **Moderation:** Emerging Leaders der AFCEA Bonn e.V. **Ablauf:** Impulsvortrag (ca. 10 Minuten) mit aktuellem Sachstand zur Durchlässigkeit von Innovation in der Bundeswehr. Beginn der Pitch-Session mit 4 Startups (2 Minuten Pitch), die anschließend im Rahmen einer Fishbowl-Diskussion von der Jury und interaktiv mit dem Publikum bewertet werden.
14:00 Uhr	**Key Note: Prominenter Gast**
anschließend	**Abschluss des Symposiums und Schlusswort** Generalmajor Armin Fleischmann, Vorstandsvorsitzender AFCEA Bonn e.V.

Ausstellerverzeichnis AFCEA FA 2026

Standabkürzungen:
A= Aussenbereich
AA= Saal Addis Abeba
B= Saal Bangkok
F= Foyer Eingangsbereich
G= Foyer Galerie
N= Saal Nairobi
R= Rheinebene
S= Saal NewYork/Genf
P= Plenargebäude
W= Saal Wien
X= Eingangsbereich
EL= Startup-Fläche Emerging Leaders im Plenargebäude

Aussteller (Stand 17.04.2026)	Standnr.
:em engineering methods AG	B01
]init[AG	B12
21strategies GmbH	P07
A. WEIDELT Systemtechnik GmbH & Co. KG	S60
abat AG	P36
Accenture	W07
adesso	G02
Adva Network Security GmbH	N04
Airbus Defence and Space	F03
Akkodis Edge Germany GmbH	N07
Akkodis Germany AS&D GmbH	N07
ALE Deutschland GmbH	S15
Allied Vision Technologies GmbH	R48
Almato AG	S73
Alteva Technologies GmbH	EL01
Amphenol Precision Optics GmbH	F30
Amphenol-Air LB GmbH	R12, F30
Ansys part of Synopsys	P16
Arbit Cyber Defence Systems	P05
ARIS GmbH	S20
ARX Robotics GmbH	P13
Atos	F31
Autonomous Teaming Solutions ATS GmbH	EL03
AVS Systeme GmbH	S21
B&T Solutions GmbH (Mosolf Group)	F14
B&W International GmbH	F14
BAKO Systemintegration GmbH & Co. KG	S84
BAPersBw/HRLab	R62
Barco Control Rooms GmbH	S21
Bareways GmbH	EL03
Barricadix GbR	EL01
BDSV e.V.	S41
bebob defense - a division of bebob factory GmbH	F14
Bechtle GmbH & Co. KG, IT-System-haus Bonn	S18 & Q01b
Behörden Spiegel / ProPress Verlag GmbH	F34
Bernd Richter GmbH	R12
Bertrandt AG	R71
best Systeme GmbH	R48
blackned GmbH	S40
Bosch Sicherheitssysteme GmbH	B06b
Bren-Tronics International Solutions	S83
BRESSNER Technology GmbH	B05
Bundesstadt Bonn - Amt für Wirtschaftsförderung	R26
Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr	N05
BWI GmbH	F07
CAE GmbH	W05
Capgemini Deutschland GmbH	N02
Carl-Cranz-Gesellschaft e.V.	R24
Carmenta Germany GmbH	W11
Cellebrite GmbH	R47
CEOTRONICS AG	F26
CGI Deutschland B.V. & Co. KG	F04, A03
Check Point Software Technologies GmbH	S15, W02
Chora GmbH	S76
Cisco Systems GmbH	F08
citema group GmbH	F11
Cloudera Germany GmbH	S18
Computacenter AG & Co. oHG	W02
Comrod Communication AS	FF17
CONDOK GmbH	S01
CONET Technologies Holding GmbH	S45
Conrad Electronic SE	F35
CPI Vertex Antennentechnik GmbH	R27
CPM Verlag GmbH	N06
Cradlepoint GmbH	S35
Cyber Innovation Hub Bundeswehr GmbH	EL03
dainox GmbH	S33
Dassault Systemes Deutschland GmbH	R11
Dataciders GmbH	B12
DATAGROUP Business Solutions GmbH	A04, S73
Dataminr Germany GmbH	R52
Data-Warehouse GmbH	F36
DCON GmbH	F32
deepset GmbH	R48
DELINFO, spol. s r.o.	S86
Dell Technologies	R51, A19
Deloitte Consulting GmbH	P01, A01
DESAPRO AG	R73
Deutsche Gesellschaft für Wehrtechnik e.V	R28
Deutsche Telekom Geschäftskunden GmbH, PG1432	F06a1, F06a2
Dreger Group GmbH	A12
DTC, a Codan Company	F14
dtec.bw – Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr	N03
D-Trust GmbH	S25
Dynamit Nobel Defence	S31
EAL Leidel GmbH	S42
ECOS Technology GmbH	S25
Edgeless Systems	W02
EGL Elektronik Vertrieb GmbH	S57
EIZO Europe GmbH	S82
Elbit Systems Deutschland GmbH & Co. KG	F23
eleQtron GmbH	R48
Elma Electronic	R46
ELP GmbH European Logistic Partners	R72
Emerging Leaders AFCEA	EL04
Emproof B.V.	EL03
Enercon Technologies	B04
EPAK GmbH	S07
Epson Deutschland GmbH	R18
Eraneos Germany GmbH	A17b
Esri Deutschland GmbH	F22
FERCHAU Management GmbH	R56
fiveD GmbH	EL02
Fortinet GmbH	S04
Fraunhofer FKIE	F15
Fraunhofer IOSB	W01
Frequentis Deutschland GmbH	S75
Fujitsu Germany GmbH	F13
GBS TEMPEST & Service GmbH	S03
genua GmbH	S25, F27, A16
GEOSYSTEMS GmbH	S85
Getac Technology GmbH	R41
Glenair GmbH	S72
Global RadioData Communications Europe Ltd.	S16
GMC TASSTA GmbH	F14
Google Germany GmbH	G01
Gretchen AI GmbH	EL04
Griffity Defense GmbH	F14
HARTING Deutschland GmbH	B08
HAT.tec GmbH	R14
Helsing Germany GmbH	S71
hema electronic GmbH	B09c
HENSOLDT AG	A05, F01
Hewlett Packard Enterprise	F25, R48
Hirt Systemtechnik GmbH	F24

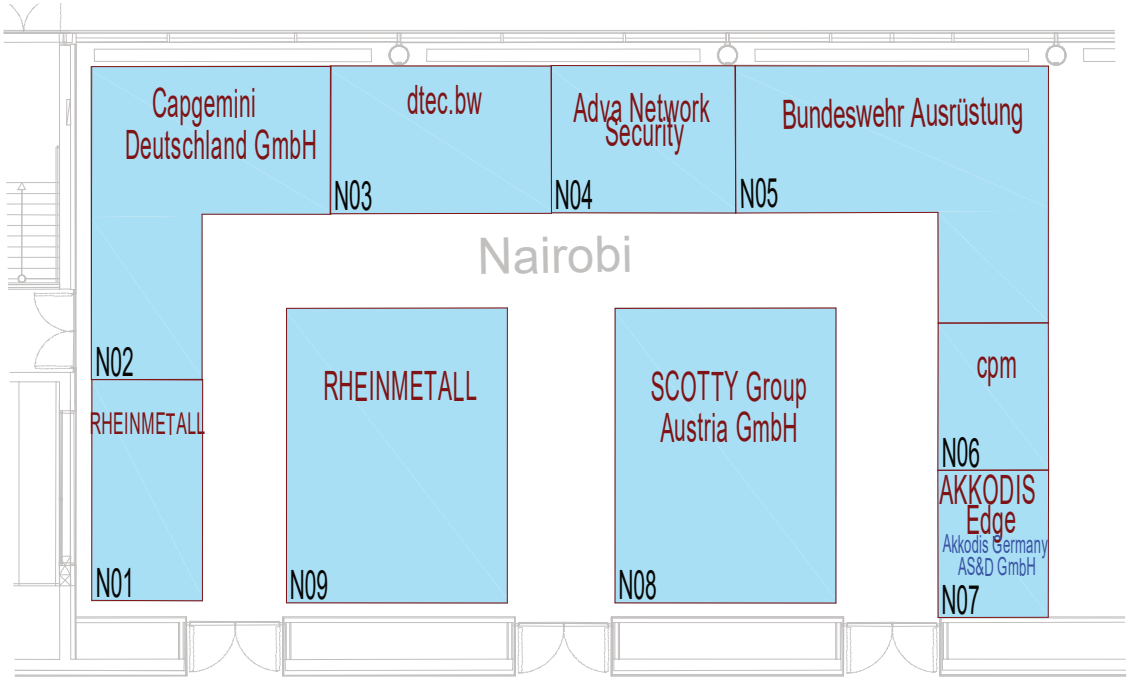
IABG mbH	W06
IABG Teleport GmbH	W06
IBM Deutschland GmbH	F02
iesy GmbH	S63
Ihse GmbH	S81
iMAR Navigation GmbH	F14
Imtradex Hör- und Sprechsysteme GmbH	F14
Indicium Technologies GmbH	EL03
Indra Avitech GmbH	S11
INFODAS GmbH	S46
INNOSYSTEC GmbH	S34
Intracom Defense S.A.	F14
inxire GmbH	F37
itemis AG	P14
itWatch GmbH	S10
Jane's Group UK Ltd	F09
JK Defence & Security Products GmbH	S30
JOWO - Systemtechnik AG	W10
Kappa optronics	R19
KIX Service Software GmbH	P03
Klepsydra Technologies AG	R48
Knapp Service Koblenz GmbH	W09
KNDS Deutschland GmbH & Co. KG	A11
KNDS Deutschland Mission Electronics GmbH	S48
Kobra Infosec GmbH	F29
Kommando Cyber- und Informationsraum	B03
Kommando Heer	S65
Kommando Luftwaffe	G03b
Kontron Hartmann Wiener GmbH	P15
KPMG AG Wirtschaftsprüfungsgesellschaft	S26
L3Harris Technologies	S30
Laokoon Security GmbH	EL02
Lateration GmbH	P10
LEONARDO Germany GmbH	R54, A06
LiveDrop B.V.	EL01
LS telcom	Q04
LWL Sachsenkabel	F30
M4Com System GmbH	R61
Marble Imaging GmbH	EL02
Marinekommando/Marineinnovationsmanagment	G03a
Materna Information & Communications SE	S52
Materna Virtual Solution GmbH	S56
MBS GmbH	S29
MICCAVIONICS GmbH	P04
Micropol Fiberoptic GmbH	F33
Microsoft Deutschland GmbH	R57
Milexia Deutschland GmbH	P09
Mittler Report Verlag GmbH	R13
ML Eingabesysteme GmbH	B01b
MÖNCH Verlag GmbH	R10
Motorola Solutions Germany GmbH	S32
Narda Safety Test Solutions GmbH	F14
ND SATCOM GmbH	S43
NEOSAT GmbH	S74
NetApp Germany GmbH	W02
Newsletter Verteidigung	R08
NewTec GmbH	P32
NI Network Innovations	B20
Nokia Solutions and Networks GmbH & Co. KG	S05
NTT Germany AG & Co. KG	S15
Nürnberg Messe - itsa	R09
NVIDIA GmbH	R48, S18
Octave	S14
ODM GmbH	F28
OHB SE	F20
ONTIME NETWORKS AS	P35
Opternus GmbH	W10
OPSWAT GmbH	P06
ORACLE Deutschland B.V. & Co. KG	P37
P3 Group GmbH	Q05
Palladion Defence Accelerator	EL03
Panasonic	F05
Paradigm	P02
PEC project engineers & consultants GmbH	P06
Peli Products Germany GmbH	S02
Pexip Germany GmbH	R22
PHYSEC GmbH	F04
Planungsamt der Bundeswehr	Q02
PLATH GmbH & Co KG	F18
ProCase GmbH	R23
Project Q GmbH	R14
promegis Gesellschaft für Geoinformationssysteme mbH	S13
PROSTEP Gruppe	R16
Pure Storage GmbH	B10
QGroup GmbH	R42
Quantum-Systems GmbH	A13
Qvest Group GmbH	A18
rasdaman GmbH	R55
Raydiant RF GmbH	EL03
RECONIQ Software GmbH	F18
Reflex Aerospace GmbH	EL03
rfe-global GmbH	P33
RHEINMETALL AG	M01, N09, A20
Rick Location Solutions GmbH	F22
roda computer GmbH	F05
Rohde & Schwarz GmbH & Co. KG	F10
rola Security Solutions GmbH	F06b
Rosenberger Hochfrequenztechnik GmbH & Co. KG	R17
RUAG AG	S70
RuggON	S18
Safran Electronics & Defense Germany GmbH	Q03
Sagio GmbH	EL03
SailPoint Technologies GmbH	R15
SaltRock GmbH	S56
SAP Deutschland SE & CoKG	F21
Satcube	F16
Schönhofer Sales and Engineering GmbH	S54
Schwarz Digits Defense GmbH & Co. KG	S61
SCOPE Engineering GmbH	R63
SCOTTY Group Austria GmbH	A02, N08
S.E.A. Datentechnik GmbH	Q01a
secunet Security Networks AG	F19
Secusmart GmbH	S51
secuvera GmbH	P11
SELECTRIC Nachrichten-Systeme GmbH	S35
Sepura Deutschland GmbH	S35
ServiceNow	W02, P08
SES SPACE & DEFENSE	B11
Shieldex	S22
Sicherheitsforum Deutschland	R75
Siemens Industry Software GmbH	G04
Skylance GmbH	EL04
Skyline Europe GmbH	S85, S86
soffico GmbH	R43
Solidplex GmbH	R23
Solifos Deutschland GmbH	S27
Sophos Technology GmbH	S62
Sopra Steria SE	S12
ST Connect GmbH	P12
steep GmbH	S39
Stellar PCS GmbH	F14
SThree GmbH	S52
SVA System Vertrieb Alexander GmbH	S53
Systematic A/S	S47
systerra computer GmbH	S64
TechniSat Digital GmbH	S66
tde - trans data elektronik GmbH	S06
tecnotron elektronik gmbh	P34
TEKSAM GMBH	W03
Thales Deutschland	S23
Thinklogical LLC	F14
TKMS Hagenuk Marinekommunkation GmbH	B07
TQ Systems GmbH	B22
Trend Micro Deutschland GmbH	S36
Treo - Labor für Umweltsimulation GmbH	S55
Twentyfour Industries GmbH	EL04
UniBw München	N03
UNITE+ Consulting GmbH	P03
Unterstützungskommando der Bundeswehr	R64
Utimaco Managment Services GmbH	S19
Veeam Software UK Holdings Limited	S62
Verband der Reservisten der Bundeswehr e.V.	B02
Veteranenbüro der Bundeswehr	A40
VISS UG	EL03
VITEC GmbH	W04
VMware	S18
Willert Software Tools GmbH	B06a
WORK Microwave GmbH	F12
Xecuro GmbH	S25
Zarges GmbH	W08
Zebra Technologies Germany GmbH	S35

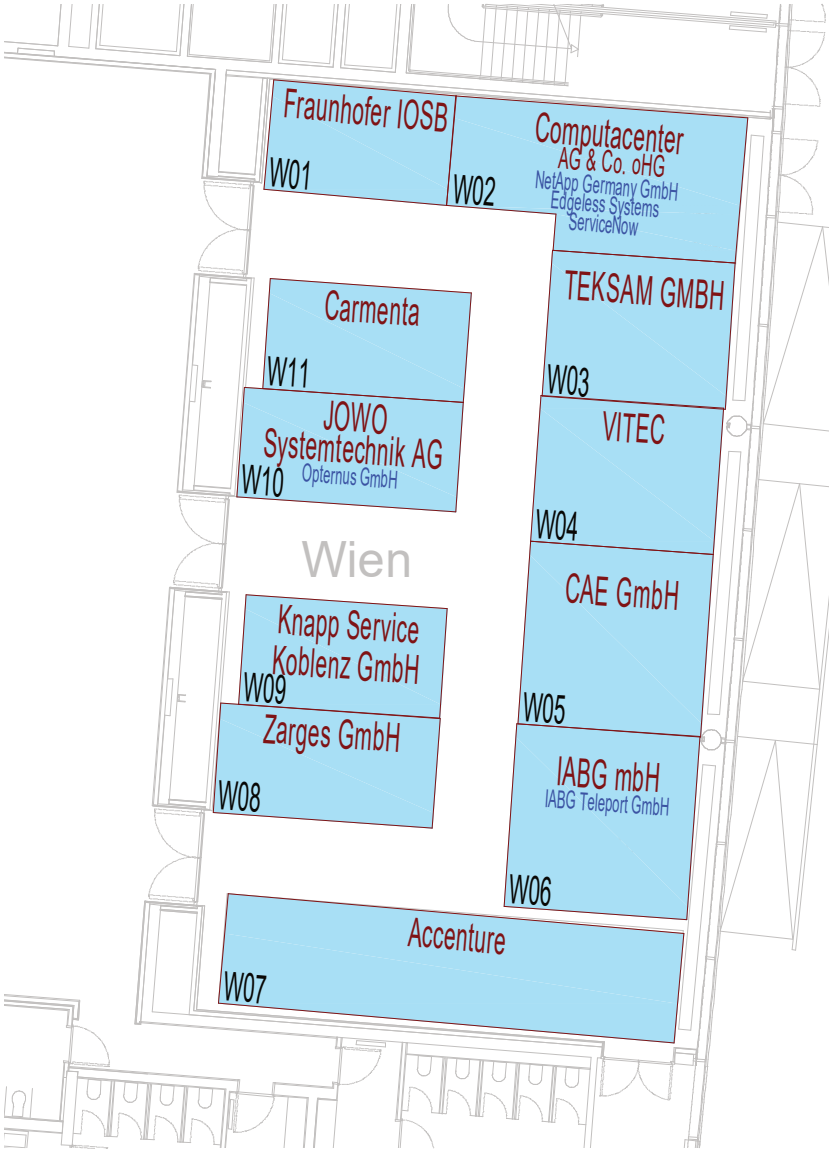
Standpläne im World Conference Center Bonn

Foyer Eingangsbereich

Saal New York / Genf

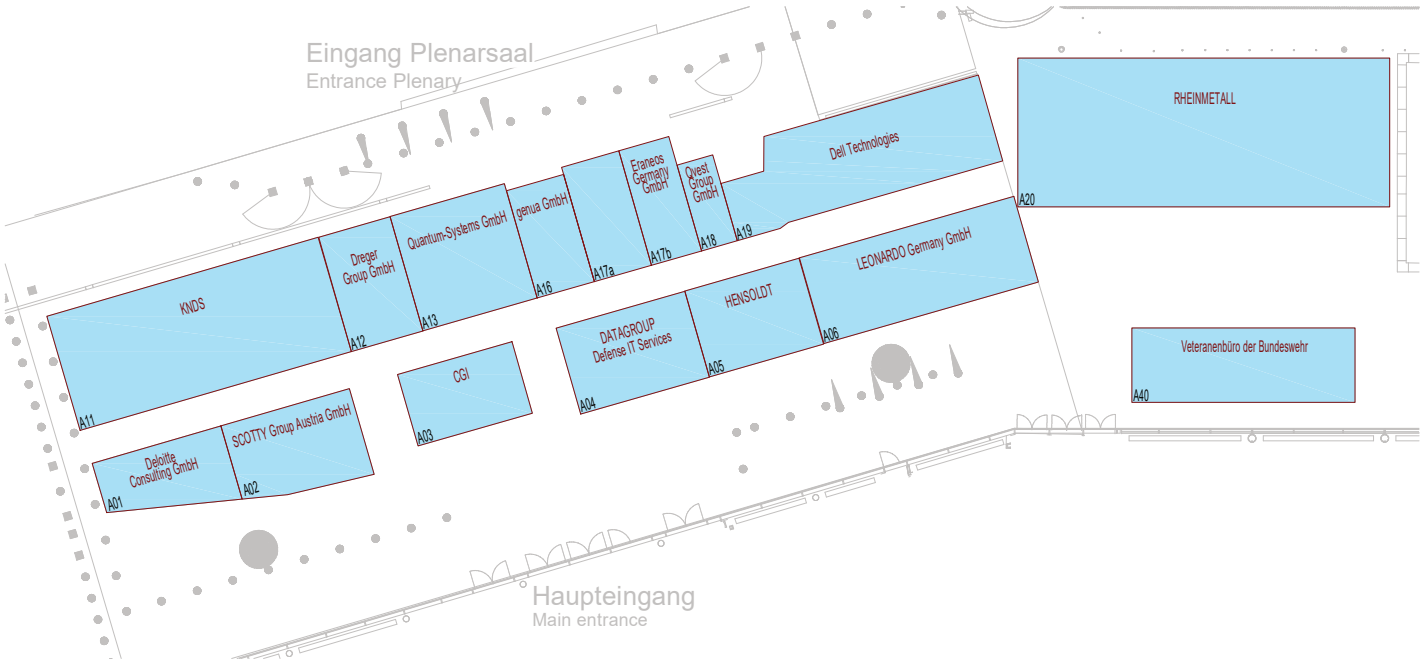
Saal Nairobi & Saal Wien



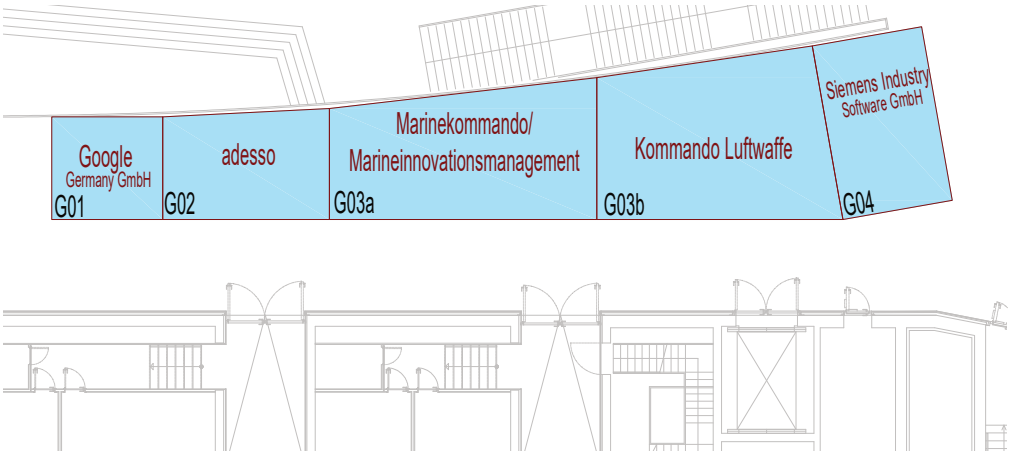


Rheinebene & Saal Bangkok & Saal Addis Abeba

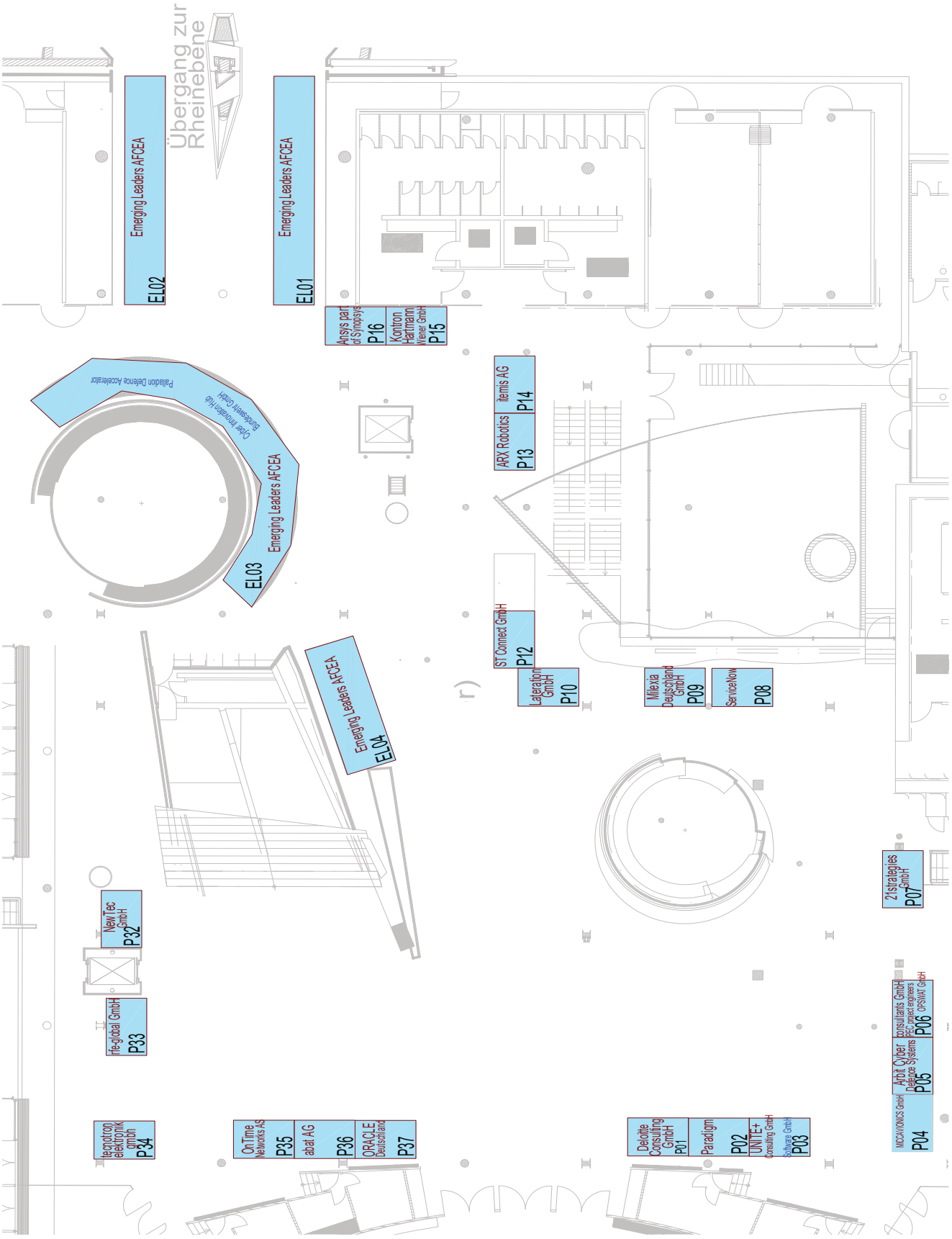
Außenbereich



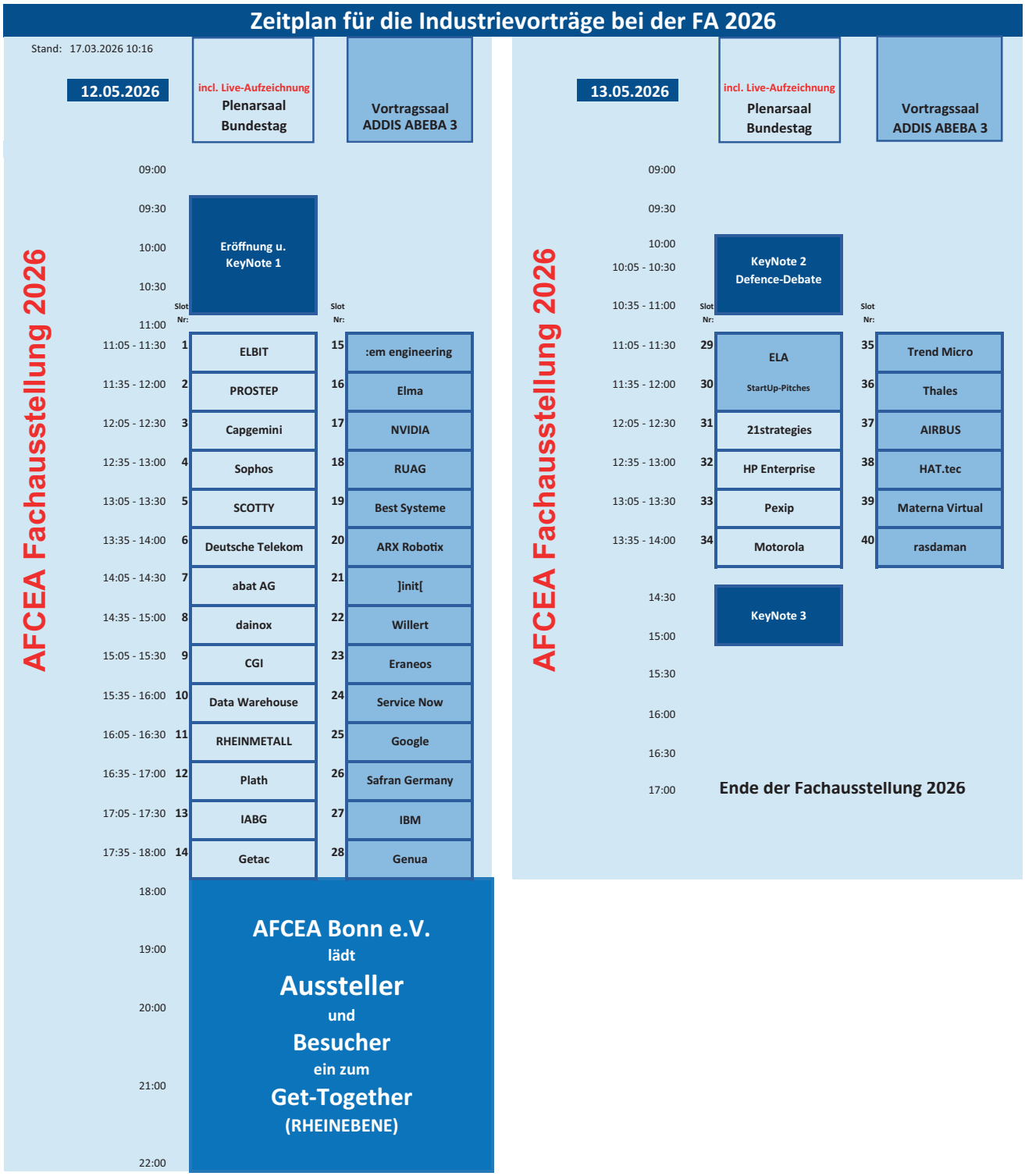
Galerie Foyer



Plenarsaal (Foyer)



Symposium und Industrievorträge



Themen der Industrievorträge

Slot	Aussteller	Thema des Industrievortrages
1	Elbit Systems Deutschland GmbH & Co. KG	Digitale Kommunikation im Einsatz
2	PROSTEP Gruppe	Von der Anforderung zur Einsatzreife: Beschleunigung von Verteidigungsprogrammen durch Digital Engineering, den Digital Thread und das Konzept des Digital Twin
3	Capgemini Deutschland GmbH	Code over Steel: Der entscheidende Hebel für Fähigkeitsaufbau bis 2030
4	Sophos Technology GmbH	Cyberlage 2026: Aktuelle Bedrohungen und Wege zu belastbarer Cyber Resilienz)
5	SCOTTY Group Austria GmbH	Secure Communication
6	Deutsche Telekom Geschäftskunden GmbH	Digitale Souveränität sichern: Wehrtaugliche IT-Architekturen 2035
7	abat AG	Resiliente Lieferketten – Robuste, IT-gestützte Prozesse für verteidigungsfähige Logistik
8	dainox GmbH	Vernetzungsfähigkeit im Einsatzgebiet aufs Neue definieren und differenzieren
9	CGI Deutschland B.V. & Co. KG	Organisationsübergreifende sichere Kommunikation: Wie HERMES als NATO-Projekt zur Resilienz und Gesamtverteidigung in Deutschland beiträgt
10	Data-Warehouse GmbH	Post Quantum - Internationaler Status, Handlungsempfehlungen und Lessons Learned für Defence und Sicherheit
11	RHEINMETALL	Battlespace Dominance is Digital – Sensor-to-Shooter Ketten im Realitätscheck
12	PLATH GmbH & Co KG	Closing the gap - Meshed Unmanned EW Core
13	IABG mbH	Open-Source-Software (OSS) allein reicht nicht für digitale Souveränität!
14	Getac Technology GmbH	Vom Soldaten zum Systemknoten: Digitale Befähigung des modernen Infanteristen.
15	:em engineering methods AG	Zukunftsorientierte IT-Architekturen für die Digitale Durchgängigkeit – von Model Based Engineering zum Digital Twin
16	Elma Electronic	(*) Unlocking the Potential of VNX+: High-Performance Embedded Computing for Next-Generation Defense Systems
17	NVIDIA GmbH	Anwendung und Betrieb agentischer KI für die Verarbeitung klassifizierter Daten
18	RUAG AG	Resiliente Kommunikation für den «Tactical Edge»
19	best Systeme GmbH	Don't Panic: A Small Company's Guide to Airworthiness
20	ARX Robotics	UGV´s als Enabler im Aufklärungs- und Wirkverbund
21	]init[AG	Die vernetzte Planungsgemeinschaft: Digitalisierung als Schlüssel der Zivil-Militärischen Zusammenarbeit
22	Willert Software Tools GmbH	KI-gestütztes Model-Driven Engineering für missionskritische Embedded-Systeme: System- und Softwaremodelle als autonome Engineering-Agenten
23	Eraneos Germany GmbH	Vernetzt denken, offensiv handeln: Gesamtstaatliche Verteidigung im Zeitalter permanenter Hybridangriffe
24	ServiceNow	Schutz kritischer Infrastrukturen im Krisen- und Konfliktfall
25	Google Germany GmbH	Souverän, resilient, skalierbar: Hybride Cloud-Lösungen als Rückgrat der digitalen Verteidigung
26	Safran Electronics & Defense Germany GmbH	(*) Resilient positioning, navigation and timing solutions are key to operate in GNSS-Denied-Areas
27	IBM Deutschland GmbH	Vom Datenstrom zur Entscheidungsfähigkeit. Wie softwarebasierte Architekturen MDO beschleunigen
28	genua GmbH	Trau Schau Wem: Hybride Clouds für Resilienz und strategische Autonomie
29-30	Emerging Leaders AFCEA Bonn e.V.	Digital Defence Debate und Startup-Pitches
31	21strategies GmbH	JATOC – Taktikfähigkeiten für agil agierende unbemannte Systeme
32	Hewlett Packard Enterprise	Datenhoheit im Gefecht der Zukunft: Das souveräne HPE Defense-Ökosystem
33	Pexip Germany GmbH	Kommunikations- und Kollaborationsplattformen in der Verteidigung: Kernanforderungen an Souveränität. Resilienz. Interoperabilität.
34	Motorola Solutions Germany GmbH	Warum die nächste Generation verlegbarer Netze das Gefechtsfeld verstehen muss
35	Trend Micro Deutschland GmbH	Digitale Souveränität im Zeitalter globaler Cyberkonflikte – Handlungsfähigkeit trotz Abhängigkeiten
36	Thales Deutschland	Algorithms at War: Wie KI und Cyber das vernetzte Gefechtsfeld bis 2030+ transformieren
37	Airbus Defence and Space	MissionAI-Bw - Der souveräne taktische KI-Assistent für den digitalen Gefechtsstand
38	HAT.tec	Komplexität, KI, Kooperation: Über integrierte Lagebilder in multi-domain Missionen
39	Materna Virtual Solution GmbH	Von der Smartcard zur mobilen PKI-Wallet: Souveräne digitale Identitäten im sicherheitskritischen Bereich
40	rasdaman GmbH	KI-gestützte Föderation für Multi-Domain GEOINT: Was geht, Stand heute?

Aussteller AFCEA-Fachausstellung 2026

Die folgenden Angaben wurden von den jeweiligen Anbietern geliefert. Sie tragen für diese Eigenangaben und deren Wahrheitsgehalt die Verantwortung.

Standabkürzungen:
A= Aussenbereich
AA= Saal Addis Abeba
B= Saal Bangkok
F= Foyer Eingangsbereich
G= Foyer Galerie
N= Saal Nairobi
R= Rheinebene
S= Saal NewYork/Genf
P= Plenargebäude
W= Saal Wien
X= Eingangsbereich

:em engineering methods AG — B01a

Die :em AG entwickelt innovative Methoden und Softwarelösungen für das Engineering und verfügt als Integrator von IT-Systemen über ein umfassendes branchenübergreifendes Portfolio. Getreu der Vision „Wir liefern die digitale Zukunft für das Engineering & Manufacturing." unterstützt die :em AG mit ihren Dienstleistungen und Software-Applikationen die konkrete Umsetzung der Digitalen Transformation bei ihren Kunden. Dazu entwerfen die Mitarbeiter*Innen Digitalisierungsstrategien und Roadmaps und helfen bei der Realisierung einer modellbasierten, digitalen Entwicklung.

]init[AG — B12

Die]init[AG für digitale Kommunikation ist der umsetzungsstärkste Experte für Digitalisierung im öffentlichen Sektor und regulierten Branchen. Das 1995 gegründete Unternehmen beschäftigt rund 1.400 Mitarbeitende. Zum Kundenkreis gehören zahlreiche Bundes- und Landesministerien, insbesondere im Innenwesen und Blaulichtorganisationen.Mit Ende-zu-Ende-Digitalisierung vereinfacht]init[Prozesse und stärkt staatliche Handlungsfähigkeit durch eine moderne, digitale Wehrverwaltung. Unser Fokus: Daten strukturiert nutzbar machen, Verfahren standardisieren und eine sichere digitale Zusammenarbeit über Organisationsgrenzen hinweg ermöglichen.

21strategies GmbH — P07

21strategies – Ihr Partner für technologische Souveränität
21strategies entwickelt seit 2020 in München die Künstliche Intelligenz, die Systeme erst wirklich wirksam macht. Mission: Taktische Überlegenheit im Gefecht wie in der Industrie – durch den klugen Einsatz von Entscheidungswissenschaft und Spieltheorie.

Lösungen:
- tactics21: Defense Metaverse mit KI-Agenten, die Millionen Gefechte simulieren inkl. Red Teaming
- JATOC: Das „KI-Gehirn" für kontextbewusste Entscheidungen und adaptive Reaktionen militärischer Plattformen
- flow21: Resilienz für die Supply Chain mit bis zu 20% Produktivitätsgewinn.

Ihr Vorteil: Maximale Effizienz und Handlungsfähigkeit selbst in kritischen Momenten.
21strategies liefert Logik für echte Souveränität – aus komplexen Signalen klare Handlungsoptionen.

A. WEIDELT Systemtechnik GmbH & Co. KG — S60

Die A. WEIDELT Systemtechnik verfügt über langjährige Erfahrungen in der Entwicklung, Fertigung, Integration und Dokumentation von Einbausätzen:
- mobile Fernmeldekabinen mit Informationsausstattungen
- TuLB (Betriebs-, Transport- und Lagerbehälter) für verschiedenste Anwendungsgebiete.

Aufgrund der neuesten Sicherheitslage in Europa ergeben sich für die Bundeswehr neue Aufgaben und Anforderungen an die Instandsetzung, Verfügbarkeit und Kampfwertsteigerung des Wehrmaterials. Hier liefert die A. WEIDELT Systemtechnik als mittelständisches Unternehmen maßgeschneiderte und kundenspezifische Lösungen.

Das Leistungsspektrum umfasst:
- Projektmanagement und -planung
- Konstruktion und Entwicklung
- Fertigung und Einrüstung
- Dokumentation und Schulung
- Instandsetzungsrahmenverträge Werk und Standort

abat AG — P36

abat ist SAP-Dienstleister, innovativer Softwareentwickler und Lösungsanbieter für softwaregestützte Geschäftsprozesse in den Kernbranchen Aerospace & Defence, Automotive, Diskrete Fertigung sowie für Unternehmen mit logistischen Prozessen oder Fertigungssteuerung. Im Leistungsbereich consult beraten wir von Konzeption über Implementierung bis zum Betrieb eines SAP-Systems. abat manufacture stellt digitale Hochverfügbarkeitslösungen zur Produktionssteuerung bereit.
abat transform bietet innovative Lösungen: von KI über Cloud-Services bis zu RPA. Der Bereich plm hält übergreifende Prozessberatung bereit, um durchgängigen Datenfluss zu erreichen. abat protect hilft, Informationen zu schützen sowie Vertraulichkeit, Verfügbarkeit und Integrität in Geschäftsbeziehungen zu bewahren.

Accenture — W07

Accenture ist ein weltweit tätiges Beratungsunternehmen, das führende Organisationen dabei unterstützt, einen digitalen Geschäftskern aufzubauen und Mehrwert durch Künstliche Intelligenz auf allen Ebenen zu schaffen. Die rund 784.000 Mitarbeitenden, unsere eigenen Ressourcen und Plattformen sowie tiefgehende Beziehungen in unserem Ökosystem bilden die Pfeiler unserer Strategie, der Transformationspartner der Wahl für unsere Kunden sowie weltweit der Arbeitgeber mit der größten Kundenorientierung und KI-Erfahrung zu sein.
In unseren Reinvention Services bündeln wir Kompetenzen aus den Bereichen Strategie, Beratung, Technologie, Operations, Song und Industry X mit umfassender Branchenerfahrung, um Lösungen und Services für unsere Kunden zu entwickeln und bereitzustellen.
www.accenture.de

adesso G02

AgenticAI: #KI #sichereSWE #Kern-Prozessunterstützung #Projekt&Portfoliomanagement #FüInfoSys #DualUse #BestOfBreed. Im Verteidigungssektor bündeln adesso, cplace und die Riedel Gruppe ihre Expertise für sichere, zukunftsfähige Lösungen im Anwendungsbereich: adesso optimiert Kerngeschäftsprozesse mit passgenauer IT und über 11.000 Spezialist:innen, um Organisationen und nationale Sicherheit zu stärken.
cplace liefert ein Next Generation Project & Portfolio Management mit adaptiver, KI gestützter Plattform und Single Source of Truth für hochkomplexe F&E Programme.Riedel steht für Mission-Critical Communication und hochverfügbare End-to-End-Lösungen für globale Daten-, Audio- und Videosysteme mit Echtzeit-Übertragung. Gemeinsam zur Stärkung der nationalen Residenz und souveränen Sicherheit!

Adva Network Security GmbH N04

Adva Network Security ist ein führendes deutsches IT-Sicherheits-Unternehmen. Wir bieten optische und Ethernet-Netzwerklösungen sowie ein umfassendes Dienstleistungsangebot.
Unsere ConnectGuard-Technologie gewährleistet eine quantensichere Verschlüsselung zum Schutz essenzieller Netzwerke. Kunden in den Bereichen kritische Infrastruktur, Regierung, Verteidigung und Privatwirtschaft schätzen unsere technische Kompetenz.
Diese einzigartige Kombination ist wesentliche Grundlage für die Resilienz und Sicherheit der IT- und OT-Infrastruktur. Unser Serviceteam unterstützt sie vom ersten Entwurf bis zum sicheren Betrieb. Die Design- und Fertigungsprozesse sowie unsere cyberresilienten Lösungen sind von führenden staatlichen Sicherheitsbehörden zugelassen.

Airbus Defence and Space F03

Airbus pioneers sustainable aerospace for a safe and united world. The Company constantly innovates to provide efficient and technologically-advanced solutions in aerospace, defence, and connected services. In commercial aircraft, Airbus offers modern and fuel-efficient airliners and associated services.
Airbus is also a European leader in defence and security and one of the world's leading space businesses. In helicopters, Airbus provides the most efficient civil and military rotorcraft solutions and services worldwide.

Akkodis Edge Germany GmbH N07

Akkodis is a global digital engineering company and Smart Industry leader. We enable clients to advance in their digital transformation with Consulting, Solutions, Talent, and Academy services. Headquartered in Switzerland and part of the Adecco Group, Akkodis is a trusted tech partner to the world's industries. We co-create and pioneer solutions that help to solve major challenges, from accelerating the clean energy transition and green mobility, to improving user and patient centricity.
Empowered by a culture of inclusion and diversity, our 50,000 tech experts across 30 countries combine best-in-class technologies and cross industry knowledge to drive purposeful innovation for a more sustainable tomorrow. We are passionate about Engineering a Smarter Future Together.

ALE Deutschland GmbH S15

Alcatel-Lucent Enterprise, europäischer Hersteller mit Fokus auf gehärtete Netzwerkinfrastrukturen, Embedded Switche, gesicherte UC-Kommunikation und KI Integration im eigenen Rechenzentrum, bietet speziell für den Verteidigungs- und Sicherheitsbereich entwickelte Kommunikationslösungen.
Die Systeme gewährleisten hochverfügbare, verschlüsselte und automatisierte Kommunikation für stationäre, mobile und remote Einsatzszenarien. Robuste, militärgeeignete Technologien sichern die digitale Zusammenarbeit auch unter extremen Einsatzbedingungen – zuverlässig, skalierbar und auf die Anforderungen von Streitkräften und Rüstungsindustrie abgestimmt.

Allied Vision Technologies GmbH R48

Allied Vision ist Ihr Partner für anspruchsvolle Vision-Systeme im militärischen Einsatz, Made in Germany. Wir entwickeln und fertigen robuste Hochleistungskameras für Situational Awareness, C4ISR und Countermeasures, passgenau für Ihre Plattform.
Wir arbeiten für führende Rüstungsfirmen, darunter 22 der SIPRI Top 100. Bewährte Qualität durch strenge Tests, ausgereiftes QMS und eine sichere Lieferketten mit Optionen für non-China-Komponenten und lange Verfügbarkeit.
Von Entwicklung bis Support liefert unser globales Team zuverlässige Lösungen termingerecht und gemäß Spezifikation.

Alteva Technologies GmbH EL01

alteva is developing ultralight, next-generation batteries using entirely European resources and production. Our battery technology unlocks unprecedented range, payload, and performance for UAVs, robotics, and front-line operations, while shoring up NATO supply chains to be independent of foreign actors. After more than 15 years of research and development, the next generation of battery technology, Made in Europe, is available today.

Amphenol-Air LB GmbH F30 & R12

Amphenol gilt weltweit als führender Steckverbinder- & Systemhersteller in den Bereichen Luftfahrt und Verteidigung.
Unser Lieferspektrum umfasst elektrische und fiberoptische Steckverbindungen sowie Verkabelungen, für High-Speed, Ethernet, Audio, Datenübertragung & Power.
Unsere Steckverbinder und Leitungen eignen sich für harte Bedingungen und können hohe Übertragungsraten auch größer als 10 Gigabit bieten.
Unsere Produkte sind MIL- bzw. VG-zugelassen und gelten als bevorzugte Lösungen für Sicherheits- und Verteidigungsapplikationen Europaweit.

Kontakt: Amphenol-Air LB GmbH, Am Kleinbahnhof 4, D-66740 Saarlouis, Tel. +4968319810-0, info@amphenol-airlb.de, www.amphenol-airlb.de.

Amphenol Precision Optics GmbH F30

Linsensteckverbinder EUROLENS und euMicron von Amphenol Precision Optics kommen überwiegend in anspruchsvollen militärischen Anwendungen zum Einsatz – darunter Radar- und Flugabwehrsystemen sowie unterschiedlichen Fahrzeugplattformen.
Die Steckverbinder haben sich darüber hinaus auch in extremen zivilen Einsatzbereichen wie dem Bergbau, dem Offshore-Sektor und der Broadcast-Technologie bewährt. Dort überzeugen sie durch ihre außergewöhnliche Robustheit, Zuverlässigkeit und Widerstandsfähigkeit gegenüber rauen Umweltbedingungen.
EUROLENS und euMicron Linsensteckverbinder sind die ideale Lösung überall dort, wo eine zuverlässige Hochgeschwindigkeits-Datenübertragung unter extremen Bedingungen unverzichtbar ist.

Atos F31

Die Atos Group ist ein weltweit führender Anbieter im Bereich der digitalen Transformation. Mit ca. 63.000 Mitarbeitenden und einem Jahresumsatz von ca. 8 Mrd. EUR agiert das Unternehmen in 61 Ländern unter zwei Marken: Atos für Services und Eviden für Produkte. Als europäische Nummer eins in den Bereichen Cybersicherheit, Cloud und High-Performance-Computing arbeitet die Atos Group für eine sichere und dekarbonisierte Zukunft und bietet maßgeschneiderte KI-gestützte End-to-End Lösungen für alle Branchen.
Das Ziel von Atos ist es, die Zukunft der Digitalisierung mitzugestalten. Die Erfahrungen und Dienstleistungen des Konzerns unterstützen die Wissensentwicklung, Bildung und Forschung in einer multikulturellen Welt und tragen zur Entwicklung technologischer Spitzenleistungen bei.

Ansys part of Synopsys P16

Our Mission is to Empower Innovators to Drive Human Advancement
We live in a world where intelligent technology is everywhere, shaping our daily lives. This pervasive intelligence is driven by three major trends: artificial intelligence, software-defined systems and silicon proliferation. For decades we've been a driving force of the technologies that make pervasive intelligence possible.
Synopsys is the leader in engineering solutions from silicon to systems, enabling customers to rapidly innovate AI-powered products. We deliver industry-leading silicon design, IP and simulation and analysis solutions. We partner closely with our customers across a wide range of industries to maximize their R&D capability and productivity, powering innovation today that ignites the ingenuity of tomorrow.

AVS Systeme GmbH S21

Die AVS Systeme GmbH hat sich auf die Planung und Realisierung von hoch technisierten audiovisuellen Visualisierungssysteme und Systemanlagen in Leitstellen und Führungsräumen spezialisiert – deutschlandweit, europaweit und über zahlreiche Märkte und Branchen hinweg. Dank über 30 jähriger Unternehmenserfahrung mit eigener Forschung und Entwicklung, kann AVS Technologien und Lösungen garantieren, die zukunftsweisend, faszinierend und zuverlässig sind.
Hinter AVS steckt nicht nur ein Team von hochqualifizierten Fachkräften mit exzellenten Branchenkenntnissen, sondern Menschen, die mit persönlichem Einsatz und Begeisterung für ihre Kunden über das Mögliche hinausdenken. Nur so hat sich AVS in den letzten Jahren zum Markführer entwickelt.
AVS Systeme GmbH, tobias.baader@avs.ch, www.avs.ch

Arbit Cyber Defence Systems P05

Arbit Cyber Defence Systems, based in Copenhagen, Denmark, was founded in 2006 by Rasmus Borch and celebrates its 20th anniversary this year. Arbit is a 100% Danish owned company, with all development and production taking place in Denmark.
The company specializes in Cross Domain Solutions for governments, military, intelligence, police and critical infrastructure. The core products include highly certified and accredited network protection solutions such as the EAL7+ certified Data Diode, approved for up to COSMIC TOP SECRET environments. These ensure unidirectional communication, improved security, and reduced risks. Arbit solutions enable secure information exchange between classified networks and have been proven in Bold Quest exercises from Georgia (US) to Finland.

B&W International GmbH F14

B&W International ist der verlässliche Partner für die Verteidigungsbranche, wenn es um robuste und sichere Verpackungslösungen geht. Unsere zertifizierten Koffer bieten kompromisslosen Schutz für empfindliche Ausrüstung – selbst unter extremen Bedingungen.
Mit höchsten Standards wie MIL-STD-810 und DEF STAN 81-41 entwickelt, kombinieren unsere Produkte Langlebigkeit, Widerstandsfähigkeit und Präzision. Individuell anpassbare Schaumeinsätze und hochstabile Polymergehäuse gewährleisten einen perfekten Schutz und optimale Funktionalität. Wir arbeiten weltweit mit Verteidigungskräften und -unternehmen zusammen, um maßgeschneiderte Lösungen zu liefern, die zuverlässig und einsatzbereit sind – für heutige und zukünftige Missionen. Plug & Protect mit B&W International.

ARIS GmbH S20

Innovativ, leistungsstark, Partners der Bundeswehr
Die ARIS Gmbh, ein produkt von SoftwareAG Gmbh , ist einer der führenden Anbieter von Prozess-Lösungen für die Verteidigungsindustrie. Mit unserer Lösung „Made in Germany" steigern Streitkräfte die Effizienz und optimieren ihre Prozesse, um qualifizierte Entscheidungen in Echtzeit zu treffen. Als Innovationspartner unterstützt die ARIS GmbH die Bundeswehr, ihre Prozesse an neue Herausforderungen anzupassen: agil, modern und ergebnisorientiert.
Alfabet – ein Produkt von Bizzdesign – hilft Entscheidungsträgern, bessere Investitionsentscheidungen zu treffen und Transformationsrisiken zu reduzieren, indem sie verstehen, wann, wo, wie und warum Änderungen im IT-Portfolio vorg

BAPersBw R62

Das Bundesamt für das Personalmanagement der Bundeswehr (BAPersBw) gewährleistet das Personalmanagement und die Personalführung des überwiegenden Anteils der militärischen und zivilen Angehörigen der Bundeswehr. Die Bundeswehr braucht deutlich mehr Personal. Um der aktuellen Bedrohungslage gerecht zu werden und die aktuellen NATO-Fähigkeitsziele zu erreichen, muss die Bundeswehr wachsen, und sie wird das schaffen.
Dazu führt das BAPersBw umfassende Digitalisierungsmaßnahmen durch, setzt im Rahmen des WDModG die ersten Befragungen zum neuen Wehrdienst um und unterstützt mit innovativen Ansätzen in der Personalgewinnung den Auftrag des BAPersBw: Aufwuchs

Kontakt:
BAPersBw, Militärringstraße 1000, 50737 Köln, Christian Otten, Tel.: +49 221 9571 6574, eMail: BAPersBwI3@bundeswehr.org

Bareways GmbH — EL03

Bareways entwickelt eine digitale Koordinationsplattform für Krisen, Einsatz und Verteidigung. Organisationen führen Kräfte, Fahrzeuge und Ressourcen in Echtzeit, teilen Lagebilder, planen Aufträge und Routen, und kommunizieren sicher. Die Lösung funktioniert auch bei schwacher Konnektivität, ist schnell integrierbar, und unterstützt Behörden, Blaulicht, kritische Infrastruktur, sowie Logistik und Sicherheitsakteure.

bebob defense - a division of bebob factory GmbH — F14

Battery Manufactory from Munich. We operate in industries where system failures or interruptions are simply not an option. That's why we take "Made in Germany" as a genuine commitment to quality. We design batteries that combine reliable power, ease of use, and long service life – complemented by certified safety and rapid service.
Our batteries deliver uninterrupted power for mission-critical mobile operations. They are deployed in tactical soldier systems, drones, robotic platforms, and communication systems, as well as in radiation detection and advanced measurement technology. Yet their range of applications extends well beyond these areas. Whenever specific requirements arise, we design and develop customized solutions tailored to demanding operations with high energy needs.

Barricadix GbR — EL01

BarricadiX entwickelt eine geodatenbasierte, KI-gestützte Plattform, die Zufahrtsrisiken erkennt, Fahrzeugdynamik und Aufprallenergie bewertet und daraus Schutzkonzepte inkl. Produktabgleich ableitet. Wir unterstützen KRITIS, Kommunen, Veranstalter sowie den militärischen Bereich bei der Planung von Zufahrts- und Perimeterschutz – standardisiert, nachvollziehbar und schnell umsetzbar, bis hin zu vergabefähigen Unterlagen.

Bechtle GmbH & Co. KG, IT-Systemhaus Bonn — S18

Als einer der führenden IT-Dienstleister in Europa gestalten wir zukunftsfähige IT-Architekturen – von klassischer IT-Infrastruktur über Multi Cloud, Modern Workplace und Cyber-Resilienz bis Künstliche Intelligenz und Managed Services. Zusätzlich bieten wir intelligente Finanzierungen und nachhaltiger Circular-IT-Konzepte. Und mit unseren Tochterunternehmen zählen wir zu den führenden Spezialisten für Business Applications. Unsere Multichannel-Strategie verbindet persönliche Betreuung an über 120 Standorten in 14 europäischen Ländern mit digitalen Services. Wir sind mit mehr als 16.000 Mitarbeitenden immer in der Nähe unserer Kunden – ob Mittelstand, Konzern oder Public Sector.
Bechtle ist im MDAX und im TecDAX notiert. 2025 lag der Umsatz nach vorläufigen Zahlen bei rund 6,4 Mrd. €.

Behörden Spiegel F34

Der Behörden Spiegel ist Deutschlands größte unabhängige Zeitung für den Öffentlichen Dienst, gehört zur Pro-Press Verlagsgesellschaft mbH und erscheint mit einer monatlichen Auflage von 101.000 (ivw-geprüft) Exemplaren. Die ProPress Verlagsgesellschaft mbH mit Sitz in Bonn ist ein Medienunternehmen mit rund 55 Mitarbeiterinnen und Mitarbeitern, dessen Zielgruppe der öffentliche Sektor ist. Neben mehreren Publikationen veranstaltet der Verlag rund 30 Kongresse sowie jährlich mehr als 530 Webinare und Seminare für Fach- und Führungskräfte aus dem Öffentlichen Dienst. Zum Portfolio gehören weitere Printmagazine, eine Homepage, mehrere digitale Newsletter und vier Podcasts, darunter der Podcast „Public Sector Insider".

blackned GmbH S40

Die blackned GmbH hat sich seit ihrer Gründung im Jahr 2009 auf die Entwicklung von softwarebasierten Verteidigungslösungen spezialisiert. Mit der taktischen Middleware RIDUX und dem Führungssystem XONITOR bildet das Unternehmen den Kern einer fortschrittlichen Architektur für die Digitalisierung von Landstreitkräften. Das von blackned entwickelte digitale Ökosystem TACTICAL CORE bietet einen zukunftssicheren und offenen Rahmen für die Umsetzung von Digitalisierungsprojekten innerhalb der NATO-Streitkräfte.

Bernd Richter GmbH R12

Als langjähriger Hersteller von kundenspezifischen Kabelsystemen für Healthcare-, Defense- und Industrie liegt unsere Stärke in der Entwicklung von individuellen Komplettlösungen. Professionell und leidenschaftlich arbeiten über 250 Mitarbeiter:innen an innovativen Lösungen.
Der Bereich Wehrtechnik fordert Belastbarkeit auf höchstem Maß, welcher unsere Systeme standhalten und so eine einwandfreie Kommunikation sicherstellen. Unsere Kabelsysteme werden im Defense-Bereich bei jeglicher Art von Verkabelung des Soldaten oder im Fahrzeug eingesetzt. Mit unserem Werkzeugbau schaffen wir Möglichkeiten für umspritzte und geschützte Kabelsysteme, die anspruchsvollen Anforderungen entsprechen. Unsere Entwicklung ist vom ersten Tag an in Ihrem Projekt involviert und bietet vollumfänglichen Support.

Bosch Sicherheitssysteme GmbH B06b

Performance built on Partnership
Ihr Gebäude kann mehr – mit unseren smarten Lösungen. Seit über 100 Jahren verbinden wir technisches Know-how mit Leidenschaft, um Menschen und ihre Umgebung zu schützen. Als einer der weltweit führenden Systemintegratoren bieten wir maßgeschneiderte Lösungen für Gebäudesicherheit, Brandschutz, Gebäudeautomation und Energieeffizienz. Neben unseren eigenen Brandschutztechnologien und digitalen Services setzen wir dabei auf die besten Produkte am Markt.
Von der Beratung bis zum Service begleiten wir Sie über den gesamten Gebäudelebenszyklus – immer an Ihrer Seite. Bosch Building Technologies

Bertrandt AG R71

Durch Entwicklungsleistungen beschleunigt Bertrandt den technologischen Fortschritt und leistet einen relevanten Beitrag zu einer nachhaltigen Zukunft. Als eigenständiger und internationaler Engineering Dienstleister mit langjähriger Aerospace- und Defence-Expertise verfügt Bertrandt über branchenübergreifendem Know-how sowie einem ganzheitlichen System- und Produktverständnis. Mit rund 13.000 Mitarbeitenden an über 50 Standorten ist Bertrandt einer der größten Engineering Service Provider Europas und der bevorzugte Entwicklungspartner für Hersteller und Systemzulieferer der Luftfahrtindustrie. Ob Defence, Space, zivile und militärische Luftfahrt oder Helicopter – Bertrandt entwickelt innovative Lösungen für die aktuellen und künftigen Herausforderungen in allen Bereichen der Branche.

Bren-Tronics International Solutions S83

Bren-Tronics is a global leader in advanced portable power solutions for military platforms, dismounted soldiers, and mission-critical systems. We design and manufacture Li-ion batteries, multi-chemistry smart chargers, and high-voltage energy systems meeting MIL-STD environmental and electromagnetic requirements. Our portfolio includes BB-2590 batteries, 6T Li-ion vehicle solutions, UAV power modules, and custom packs. Bren-Tronics solutions deliver high energy density in compact, lightweight formats, enabling seamless integration into C4ISR networks, unmanned platforms, electronic warfare systems, and soldier modernization programs. Trusted by armed forces worldwide, our technologies provide reliable, efficient, interoperable power to ensure operational superiority across all theaters.

best Systeme GmbH R48

Die best Systeme GmbH ist Ihr Partner für ruggedized IT-Systeme, zu Land, zu Wasser und in der Luft. Wir entwickeln in enger Abstimmung mit Ihnen und Ihren speziellen Bedürfnissen IT-Systeme für raue Umgebungen und extreme Umwelteinflüsse wie Temperatur, Vibration, Schmutz oder Stöße. Selbst kleinste Lose oder Einzelanfertigungen sind möglich. Neue Technologien wie Digital Twins unter Anwendung von Artificial Intelligence verkürzen dabei den Zeitrahmen für die Entwicklung signifikant. Seit mehr als 30 Jahren steht bei der best Systeme GmbH der Kunde und seine IT-Lösungen im Fokus.

BRESSNER Technology GmbH B05

Als Systemintegrator und Value-Added Distributor hat sich BRESSNER Technology in den letzten 30 Jahren ein umfangreiches Produkt- und Service Portfolio im Bereich industrieller Hardware-Lösungen aufgebaut. Mit unseren hoch spezialisierten Hardware-Systemen und Komponenten bedienen wir die Branchen, in denen Standard-Hardware an ihre Grenzen stößt. Durch unser stetig wachsendes Partnernetzwerk und dem Gespür für technologischen Fortschritt, sind wir in der Lage, Ihnen State-of-the-Art Hardware-Lösungen für nahezu jedes Anwendungsgebiet zu liefern.

Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr N05

AUSRÜSTUNG

Der Organisationsbereich Ausrüstung, Informationstechnik und Nutzung (OrgBer AIN) gliedert sich in das Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAAINBw) und seinen Geschäftsbereich; sechs Wehrtechnische Dienststellen, zwei Wehrwissenschaftliche Institute, das Marinearsenal und die Deutsche Verbindungsstelle des Rüstungsbereichs in Reston, USA.
Hauptaufgabe ist die bedarfs- und forderungsgerechte Ausstattung der Bundeswehr mit leistungsfähigem und sicherem Material, auch im Bereich der Informationstechnik. Im Mittelpunkt stehen die Entwicklung, Erprobung, Beschaffung und das Nutzungsmanagement von Wehrmaterial; vom hochkomplexen Waffen- und IT-System, über Panzer, Flugzeuge und Schiffe bis hin zur Bekleidung der Truppe.

Bundesstadt Bonn - Amt für Wirtschaftsförderung R26

Bonn for sure!
EUROPEAN IT & CYBERSECURITY HUB

Bonn for sure! European IT- und Cybersecurity Hub.

- 1.000 IT-Unternehmen in der Region
- 11 Prozent IT-Beschäftigte
- 10 sicherheitsrelevante Bundesbehörden und Institutionen
- 700 neue Arbeitsplätze im IT-Sektor allein im Jahr 2024

Ob Unternehmen wachsen möchten oder Fachkräfte neue Perspektiven suchen – Bonn for sure! macht das einzigartige digitale Ökosystems sichtbar. Die Bonner Wirtschaftsförderung unterstützt die Kultur des Miteinanders der gesamten IT- und Cybersicherheitsbranche. Die Wirtschaftsförderung lädt Unternehmen, Organisationen, Fachkräfte und ihre Familien ein, Teil dieser Bewegung zu werden – einer Bewegung, die die digitale Souveränität Europas stärkt, nachhaltige Werte schafft und so wichtig für die gesamte Standortsicherung ist.

Bundesverband der Deutschen Sicherheits- und Verteidigungsindustrie e.V. S41

BDSV
Bundesverband der Deutschen Sicherheits- und Verteidigungsindustrie e.V.

Der Bundesverband der Deutschen Sicherheits- und Verteidigungsindustrie vertritt über 500 privatwirtschaftlich organisierte Unternehmen aus den Bereichen Sicherheit, Verteidigung & Digitales und unterstützt in seiner Arbeit den Erhalt und die Stärkung der Wettbewerbs- und Zukunftsfähigkeit der deutschen Sicherheits- und Verteidigungsindustrie und des Technologie- und Wirtschaftsstandortes Deutschland. Wir sind Ansprechpartner für Politik, Ministerien, andere Staaten sowie Medien und Öffentlichkeit. Der Verband agiert als branchenübergreifende Interessenvertretung, sowohl national als auch international. In diesem Sinne übernimmt der BDSV auch die Koordination der Aktivitäten innerhalb der AeroSpace & Defence Industries Association of Europe (ASD).
www.bdsv.eu

BWI GmbH F07

BWI
IT für Deutschland

BWI GmbH – primärer Digitalisierungspartner der Bundeswehr. Die BWI ist eines der größten IT-Service-Unternehmen in Deutschland. In Frieden, Krise und Krieg erbringt sie für die Bundeswehr mit über 8.000 Mitarbeitenden stabile, sichere und effiziente IT-Services im Inland und Ausland. So trägt sie zur kontinuierlichen Erhöhung der Führungs- und Einsatzfähigkeit sowie Kampfkraft der Streitkräfte bei.
Seit ihrer Gründung 2006 hat die BWI ihr Leistungsportfolio enorm erweitert. Sie berät kompetent, entwickelt IT-Lösungen für die Bundeswehr – „innovativ by design“, und sie ist zentrale Kraft beim Auf- und Ausbau eines resilienten Partner-Ökosystems. Als attraktiver Arbeitgeber gewinnt und bindet die BWI hochqualifizierte Kräfte, welche die Bundeswehr-IT aus Überzeugung voranbringen.
bwi.de

CAE GmbH W05

CAE

CAE Defense & Security ist führend in der digitalen Innovation und bietet breitgefächerte, individuelle Trainingslösungen und Mission Support für militärische Kunden und Einsatzbereiche, wie Luft, Land, See, Weltraum und Cyber. Unser Trainingsangebot unterstützt Kunden, die in komplexen, hochsensiblen Umgebungen operieren, in denen Einsatzbereitschaft und erfolgreiche Missionen entscheidend sind. CAE Defense & Security ist das weltweit führende, plattformunabhängige Trainings- und Simulationsunternehmen für den globalen Verteidigungsmarkt.

Capgemini Deutschland GmbH N02

Capgemini

Capgemini ist ein globaler Partner für KI-gestützte Geschäfts- und Technologietransformation. Wir gestalten die Zukunft unserer Kunden durch die Verbindung von KI, Technologie und Mensch mit messbaren Mehrwert. Unser End-to-End-Leistungsspektrum basiert auf Branchenexpertise, einem starken Partner-Ökosystem sowie Kompetenzen in Strategie, Technologie, Design, Engineering und Operations. Wir setzen auf Innovation, Zusammenarbeit und europäische Werte. Mit unseren Lösungen sichern wir die Einsatzbereitschaft und Entscheidungsfähigkeit unserer Soldatinnen und Soldaten auch in herausfordernden Situationen. Auf der Fachausstellung zeigen wir, warum und wie Softwarebasierte Fähigkeitsentwicklung sowie Domänen- /Plattformenübergreifende Vernetzung wesentlich zur Verteidigungsfähigkeit beitragen.

Carmenta Germany GmbH W11

carmenta

Carmenta ist ein weltweit führender Anbieter leistungsstarker Geospatial-Software für missionskritische Anwendungen in den Bereichen Verteidigung und öffentliche Sicherheit. Mit über 40 Jahren Erfahrung bieten wir fortschrittliche Visualisierungs- und Analysefunktionen für Land-, Luft- und Seeeinsätze. Unsere Produkte unterstützen Echtzeit-Geoanalysen, Gelände- und Wetterbewertungen, Sensorfusion sowie dynamische 2D/3D-Visualisierungen und lassen sich nahtlos in moderne C2- und Missionssysteme integrieren. Führende Systemintegratoren weltweit vertrauen auf unsere zuverlässigen, flexiblen und leistungsstarken Lösungen.
Wichtige Produkte:

- Carmenta Engine: Ein leistungsstarkes, zuverlässiges und flexibles geospatial SDK.
- Carmenta Server: Webmapserver für die Verteilung von Geodaten

CEOTRONICS AG F26

CEOTRONICS
when it counts

Kommunikation ist ein Schlüssel zum Erfolg. Aber was passiert in Situationen, in denen schwierige äußere Umstände eine einwandfreie Kommunikation beinahe unmöglich machen? Im Einsatz von Polizei-, Feuerwehr-, Rettungs- und Verteidigungskräften oder in der Industrie sind solche Situationen Alltag. Eine störungsfreie Kommunikation sichert hier nicht nur reibungslose Abläufe, sondern rettet im Ernstfall Leben. Im Wissen darum wurde CEOTRONICS gegründet.
Unser Antrieb: Für diejenigen Menschen Kommunikationslösungen zu entwickeln, auf die es ankommt. Und für die Situationen, wenn es darauf ankommt. When it counts.

Das Fundament für die Verteidigung von morgen.

Vom Informationsvorsprung zum Wirkungsvorteil – Mission Critical Infrastructure als Basis für militärische Fähigkeiten.

CGI Deutschland B.V. & Co. KG — F04 & A03

CGI Deutschland B.V. & Co. KG ist die unabhängige deutsche Tochter von CGI Inc., einem der größten globalen Dienstleister für IT- und Geschäftsprozesse. Für unsere Kunden entwickeln unsere über 4.500 Mitarbeitenden in Deutschland ergebnisorientierte Strategien für ihre digitale Transformation und unterstützen sie mit End-to-End-Services. Mit Bundeswehr und NATO arbeiten wir seit 50 Jahren im Grundbetrieb wie in Übungen und Einsätzen zusammen. Gemeinsam stärken wir unsere Verteidigungsfähigkeit: Bewährte Lösungen wie CGI eGov360 in DokMBw und KI sowie unsere Secure Managed Services wie SINA Managed Service und Betrieb HIL ermöglichen Streitkräften, Industrie und anderen Organisationen die sichere Bearbeitung ihrer Verschlusssachen – für eine zügige Umsetzung des Operationsplans Deutschland.

Chora — S76

Chora liefert einzigartige Lösungen, die speziell für Streitkräfte, Nachrichtendienste und Sicherheitsbehörden entwickelt wurden. Als anerkannte Experten auf dem Gebiet der Satellitenkommunikation und des PNT setzen wir auf Innovation, Leistung und Vertraulichkeit, um die Erwartungen der Endnutzer zu erfüllen. Unser praxiserprobter Erfolg basiert auf engen Beziehungen zu unseren Kunden, deren Feedback und Ideen unsere wichtigste Inspirationsquelle für die Entwicklung präziser, robuster und benutzerorientierter Produkte sind.
Unsere taktischen und strategischen Lösungen werden in Dänemark entwickelt und hergestellt und weltweit über unsere Tochtergesellschaft in Deutschland, ein Netz lokaler Vertriebshändler und eine begrenzte Anzahl enger Partner vermarktet.

Check Point Software Technologies GmbH — S15 & W02

Check Point Software Technologies GmbH ist ein führender Anbieter von KI-gestützten Cybersicherheitsplattformen. Weltweit schützen Check Point Technologien über 100.000 Unternehmen, darunter Ministerien und Organisationen der inneren- und äußeren Sicherheit sowie Unternehmen der Rüstungsindustrie. Proaktive Bedrohungserkennung ermöglicht eine schnellere Reaktionszeit im Falle einer Cyberattacke. Die Ekennungsraten von Check Point werden von unabhängigen Stellen global als führend in der Branche eingestuft. In seinen 4 Kernbereichen „Hyrid Mesh“, „Workspace Security“, „Exposure Managament“ und „AI-Security“ nutzt Check Point die Leistungsfähigkeit von KI, um den Wirkungsgrad der Cybersicherheit u. a. beim Schutz von mobilen- und verlegefähigen Netzen essentiell zu erhöhen.

Cisco Systems GmbH — F08

Cisco Systems hilft Unternehmen, Behörden, Organisationen und dem deutschen Staat als strategischer Partner sichere, leistungsfähige Netzwerke zu schaffen, mit denen effizient zusammengearbeitet werden kann, so dass entscheidende Prozesse schneller gelingen und sich die Digitalisierung unserer Gesellschaft im KI-Zeitalter geschützt weiterentwickeln kann.
Cisco ist ein seit Jahrzehnten verlässlicher Partner der Bundeswehr und der Verteidigungsindustrie auf allen Ebenen. Dazu entwickelt Cisco Produkte und Lösungen rund um das Netzwerk, Netzwerkinfrastrukturen, Cybersicherheit, Rechenzentrumsausrüstung, Videokommunikations- und Kollaborationslösungen, Cloud/Software und Services.

Computacenter

EINSATZFÄHIG. SOFORT.

Performante und moderne Lösungen für eine hochsichere Infrastruktur.

citema group GmbH — F11

Die citema group GmbH steht für Digitalisierung im sicherheitsrelevanten Systemumfeld. Wir beraten und unterstützen mit unseren Group-Unternehmen citema consulting GmbH, citema experts GmbH und citema systems GmbH unsere militärischen, behördlichen und zivilen Kunden in deren Entwicklungsprojekten und Produktivsystemen sowie bei Cyber Security- und KI-Vorhaben.
Unsere festangestellten Experten verfügen über langjährige Projekterfahrung sowie fundiertes technisches und organisatorisches Know-how. Diese Expertise können wir basierend auf Werkverträgen, Dienstverträgen und Arbeitnehmerüberlassungsverträgen bereitstellen.
Die citema group gewährleistet Ihnen als inhabergeführte und deutsche Unternehmensgruppe ein Höchstmaß an Stabilität, Vertraulichkeit und Sicherheit

CONDOK GmbH — S01

Das Systemhaus für technische Dienstleistungen, Technik und Logistik. Das Leistungsspektrum der CONDOK umfasst die Bereiche Systementwicklung und Dienstleistungen im Rahmen des Integrated-Logistics-Support. Dazu gehören u.a. die Technische Dokumentation, die Produkt- und Betriebssicherheit, die logistische Betreuung von Produkten und Systemen sowie die Software-Entwicklung für das logistische Datenmanagement. Als Systemhaus entwickelt und realisiert CONDOK Einrüstungs- und Umrüstungsmaßnahmen in Kabinen und Fahrzeugen und führt Instandsetzungsleistungen durch.
Die CONDOK GmbH beschäftigt an den Standorten Kiel, Hamburg und Koblenz ca. 400 Mitarbeiter. Kontakt: www.condok.org

Computacenter AG & Co. oHG — W02

Computacenter ist ein führender, unabhängiger Technologie- und Servicedienstleister, dem öffentliche Auftraggeber und große Unternehmen vertrauen. Wir helfen unseren Kunden bei der Beschaffung, der Weiterentwicklung und dem Betrieb ihrer IT-Infrastruktur, um eine digitale Transformation zu ermöglichen, die Menschen und deren Geschäft erfolgreich macht.
In Deutschland sind wir mit rund 7.000 Mitarbeiter:innen einer der führenden ICT-Anbieter. An unserem Hauptsitz in Kerpen betreiben wir eines der modernsten Integration Center. Weltweit beschäftigt Computacenter über 20.000 Menschen und wir arbeiten global mit den führenden Technologiepartnern zusammen, um unseren Kunden jederzeit die sichersten und besten Lösungen, maßgeschneidert auf ihre Anforderungen, zur Verfügung zu stellen.

Conrad Electronic SE — F35

Conrad Electronic steht als zuverlässiger Partner seit 1923 für Technik und Elektronik und bietet heute als Sourcing Platform alle Teile für die erfolgreiche Beschaffung von technischem Bedarf. Geschäftskunden, Behörden und die Bundeswehr bekommen bei Conrad genau das, was ihre Projekte oder ihr Business zum Erfolg führt: Ein breites und tiefes Sortiment mit zehn Millionen Produktangeboten, kundenzentrierte Lösungen und Services sowie fachkompetente Betreuung von Mensch zu Mensch. Mithilfe von maßgeschneiderten E-Procurement-Lösungen vereinfacht Conrad komplexe Beschaffungsprozesse und hilft Unternehmen aller Branchen und Größen, Zeit und Kosten zu sparen.

CPI Vertex Antennentechnik GmbH — R27

Antennentechnik, die verbindet. Werte, die tragen.
CPI Vertex Antennentechnik GmbH ist ein international führender Anbieter von Hochleistungsantennensystemen für wissenschaftliche, kommerzielle und sicherheitsrelevante Anwendungen. Von der Konzeption über die Fertigung bis zur weltweiten Installation begleiten wir Projekte end-to-end. Wir ermöglichen modernste Antennensysteme, präzise zugeschnitten und von dauerhafter Qualität.
Unsere Mission: Zukunftsorientierte Technologie auf höchstem Niveau, getragen von internationaler Ingenieurskunst, Kundenorientierung, starker Mitarbeiterkultur, ökologischer Achtsamkeit und fairer Zusammenarbeit. CPI Vertex ist Teil der Communications & Power Industries (CPI), einem globalen Anbieter innovativer Elektronik- und Hochtechnologielösungen.

DATAGROUP — S73 & A04

DATAGROUP betreut seit vielen Jahren behördliche und industrielle Kunden aus dem Rüstungsbereich sowie der Luft- und Raumfahrt. Dies umfasst ebenfalls die wehrtechnische Zulieferindustrie sowie Unternehmen mit kritischer Infrastruktur (KRITIS).
Als Full-Service Provider bietet DATAGROUP im Rahmen von flexiblen und hybriden Liefermodellen einen modular skalierbaren, state-of-the-art IT-Betrieb „as-a-Service“ an. Diese Betriebsmodelle decken sowohl VS-NfD-Umgebungen als auch Mischsysteme aus regulären Netzen und VS-NfD-Umgebungen ab. Darauf aufbauend bildet die semantische Datenplattform Bardioc, eine optimale Ergänzung. Zudem präsentieren wir in diesem Jahr Cyber Security „made by DATAGROUP“.

Cradlepoint GmbH — S35

Ericssons hochleistungsfähige, programmierbare Netze bieten täglich Konnektivität für Milliarden von Menschen. Seit fast 150 Jahren sind wir Pioniere bei der Entwicklung von Kommunikationstechnologien. Wir bieten mobile Kommunikations- und Konnektivitätslösungen für Dienstanbieter und Unternehmen. Gemeinsam mit unseren Kunden und Partnern lassen wir die digitale Welt von morgen Wirklichkeit werden.
www.ericsson.com

Dataminr Germany GmbH — R52

Dataminr First Alert enables public sector organizations to detect breaking events and extract actionable insights faster than ever before possible so they can maintain situational awareness, accelerate decision-making, and respond faster—ultimately saving time, resources, and lives. Powered by agentic AI, Dataminr First Alert provides early warnings and essential context for breaking events and unexpected risks across the physical and digital domains. Stay ahead of evolving risks with Dataminr First Alert, the trusted AI-powered real-time event, threat & risk intelligence solution for the public sector.

dainox GmbH — S33

Wir sind ein etabliertes und innovatives Hightech IT-Unternehmen. Unsere Schwerpunkte sind IT-Architekturen (IP-Netzwerke & IT-Sicherheit, Collaboration und Digitalisierung), Software-Entwicklung (Automation & Orchestrierung) sowie IT-Systeme (Entwicklung & Fertigung). dainox unterstützt Kunden dabei im gesamten Workflow, beginnend bei der Machbarkeitsbetrachtung über die Realisierung bis hin zum Betrieb. Dabei setzen wir auf nachhaltige und kostenoptimierte Lösungen auf Basis aktueller Technologien. Der Schlüssel zu unserem Erfolg sind unsere hoch qualifizierten Mitarbeiter, die auf langjährige Erfahrung zurückgreifen können. Unsere Produkte und Lösungen sind innovativ, effizient und langlebig. Gebündeltes Fachwissen auf den Punkt gebracht – dainox.
www.dainox.net | info@dainox.net

Data-Warehouse GmbH — F36

Die Data-Warehouse GmbH ist als inhabergeführtes, Münchner Mittelstandsunternehmen seit 1987 am Markt aktiv. Unser Firmenmotto „Use Your Information“ setzen wir erfolgreich mit Produkten in den Bereichen Datenmanagement, Cybersecurity, Softwareentwicklung und Datenschutz für unsere Kunden aus Verteidigung (Luftwaffe, Armee, Marine), Banken, Logistik, Luftfahrt, Automobilbau etc. ein. Aktuelle Mitarbeit im US-NIST und MITRE in der Post Quantum Workinggroup mit unseren Produkten PCert und IQIMS.
Homepage: www.dwh.info

Dassault Systemes Deutschland GmbH — R11

Dassault Systèmes ist ein Katalysator für den menschlichen Fortschritt. Durch virtuelle Umgebungen ermöglichen wir Unternehmen und Menschen, nachhaltige Innovationen zu realisieren. Mit der 3DEXPERIENCE Platt-form und fortschrittlichen Lösungen erstellen unsere Kunden virtuelle Zwillingsabbilder der realen Welt, um Prozesse für die Entwicklung, die Produktion und das Lebenszyklusmanagement neu zu definieren. Dassault Systèmes unterstützt über 350.000 Kunden in mehr als 150 Ländern.

DCON GmbH — F32

Wir sind DCON. Wir denken das Enterprise Service Management öffentlicher Organisationen weiter.
Wie genau? Wir sehen die Anforderungen an Automatisierung und Digitalisierung durch die Augen unserer Public-Kunden. Und diesen begegnen wir mit Servity – unserer Enterprise Service Management Plattform. Dafür bringt Servity wertvolle Features mit, wie bspw. mehrstufige Genehmigungen, Verlegefähigkeit, Mandantenfähigkeit und ein umfassendes Best Practice Framework zum Start ins automatisierte und digitalisierte Enterprise Service Management.
Wer sich für Servity entscheidet, dem stellen wir Public- und Defense-Consultants zur Seite, die die anspruchsvollen Prozesse der Branche in der Tiefe beherrschen. Und: die Servity wie ihre Westentasche kennen.

deepset GmbH — R48

Haystack von deepset ist die KI-Plattform für den Verteidigungssektor – entwickelt für missionskritische Anwendungen und KI-Agenten unter höchsten Anforderungen an Präzision, Sicherheit und Compliance. Mit unserem ergebnisorientierten Ansatz und der Stärke unseres Open-Source-Frameworks ermöglichen wir schnelle Wertschöpfung bei komplexen Herausforderungen. On-Premise oder Cloud – volle Flexibilität bei maximaler Sicherheit. Unsere Technologie unterstützt zentrale Verteidigungskompetenzen: von KI-gestützter Cyberabwehr bis zur intelligenten Automatisierung elektronischer Systementwicklung. Ministerien und Partner wie Airbus setzen bereits auf deepset. Integriert mit NVIDIA AI Enterprise für skalierbare, hochperformante KI. Mehr unter deepset.ai

DELINFO, spol. s r.o. — S86

DOLPHIN Staff C2 Information System
The subsystem of DELINFOS is dedicated to support command and control on the workstations within the LAN on the command posts of the task force. SC2IS contains modules and applications enabling effective data preparation, processing, sharing and distribution within the command post or among them SAMET BMS Situational Awareness and Message Terminal. The key advantage of this module is maximal automation of the Situational Awareness generation, simplified operation, which allows information exchange among tactical units and platforms. BADIAN BMS Battle Digital Assistant. It has been dedicated to support basic command and control functions of Dismounted soldiers. BADIAN's applications can be operated on a commercial or ruggedized smartphone or tablet.

Dell Technologies — R51 & A19

Dell Technologies unterstützt weltweit Unternehmen bei der Gestaltung ihrer digitalen Zukunft, der Transformation ihrer IT und dem Schutz ihrer Daten. In 180 Ländern bietet Dell das umfangreichste Technologie- und Services-Portfolio für das KI-Zeitalter, von Clients über Server- und Speichersysteme bis hin zu Software- und IT-Security-Lösungen. Mit speziellen Finanzierungs- und Leasing-Optionen sowie der Möglichkeit, das gesamte Infrastrukturportfolio „as a service" über APEX zu beziehen, bietet Dell maximale Flexibilität, Skalierbarkeit, Planungssicherheit und Kostenkontrolle.

Deloitte Consulting GmbH — P01 & A01

Deloitte bietet führende Prüfungs- und Beratungsleistungen für nahezu 90 % der Fortune Global 500® sowie zahlreiche private Unternehmen. Unsere Mitarbeitenden liefern messbare, langfristige Ergebnisse, stärken das Vertrauen in Kapitalmärkte und unterstützen Kunden bei Wandel und Wachstum. Auf einer 180 jährigen Geschichte aufbauend entwickeln wir zukunftsorientierte Lösungen für den öffentlichen Sektor, um Sicherheitsinfrastruktur und Verteidigungsfähigkeit zu optimieren. Deloitte unterstützt Streitkräfte, Polizeien und Justiz mit globaler Expertise bei digitaler Transformation, Resilienz und Logistik. Mit methodischer Stärke gestalten wir praktikable Sicherheits- und Verteidigungsstrategien und setzen sie gemeinsam mit unseren Mandanten um.

DESAPRO GmbH — R73

DESAPRO ist führend in der Entwicklung, Produktion und Integration von Spezial-Gehäusen wie Aluminium- und Composite 19 Zoll-Gehäuse und Transportbehälter.
Die Gehäuse und Behälter schützen deren Inhalt vor mechanischen, klimatischen oder elektrischen Einwirkungen wie Schock, Vibration, Wasser, Staub, Korrosion und EMV. Die Firma hat eine breite Palette von Produkten bestehend aus MILEX & COMEX 19 Zoll Gehäusen, STANEX Transportbehälter, PORTEX Behälter für sensitive Messinstrumente sowie KOOLEX AC-Kühlungselementen. DESAPRO verfügt über einzigartige Erfahrungswerte in der Entwicklung von kundenspezifischen massgeschneiderten Lösungen zum Schutz von kostbaren Gütern. Neu verfügen wir auch über einen Standort mit Integrations-Fähigkeiten im EU-Raum.

DEUTSCHE GESELLSCHAFT FÜR WEHRTECHNIK e. V. (DWT) — R28

Die DEUTSCHE GESELLSCHAFT FÜR WEHRTECHNIK e. V. (DWT) wirkt als neutrale Dialog- und Informationsplattform für Fragen der Sicherheits- und Verteidigungspolitik, der Wehr- und Sicherheitstechnik sowie der Verteidigungswirtschaft. Die DWT und ihre Tochtergesellschaft, die Studiengesellschaft der DWT mbH (SGW), führen Entscheidungsträger aus Politik, Wirtschaft, Industrie und Dienstleistungssektor, Bundeswehr und anderen Behörden sowie Wissenschaft, Forschung und Öffentlichkeit zusammen, um Ausrüstungs- und Ausstattungsfragen der Bundeswehr unter Berücksichtigung nationaler und internationaler Interessen und Rahmenbedingungen zu erörtern. In der Fläche wird die DWT in zahlreichen regional wirkenden Sektionen und in Wehrtechnischen Arbeitskreisen tätig.
www.dwt-sgw.de.

Deutsche Telekom Geschäftskunden GmbH — F06a

Gemeinsam die öffentliche Infrastruktur des Digitalzeitalters schaffen
Damit das öffentliche Gemeinwesen funktioniert, braucht es verlässliche digitale Lösungen. Für Bund, Länder und Kommunen. Für Bildung und Forschung wie für Gesundheit, Soziales und Sicherheit. Wir unterstützen öffentliche Dienstleistende dabei, ihre Digitalisierung nachhaltig umzusetzen – bei Planung, Implementierung und Betrieb. Und mit hoher Expertise bei dem Schutz vor Cyber-Angriffen. Wir kennen gesetzlichen Rahmenbedingungen und die Begebenheiten vor Ort. Unsere Service-Teams sind landesweit unterwegs. Egal welche Dienste von der öffentlichen Hand erwartet werden – sie kann sich auf ein stabiles Netz und performante IT verlassen. Weitere Informationen finden Sie hier: https://public.telekom.de/

Dreger Group GmbH — A12

Mobiler Krisenleitstand für Führungsfähigkeit und Reaktionskraft im Normalbetrieb und in der hybriden Lage – für Militär, BOS, KRITIS und Unternehmen. Unser situatives Krisenmanagementsystem bündelt alles, was Sie im Ernstfall brauchen:

- Autarke, vorinstallierte Führungsstelle
- Visuelles Lagebild & Aufgabensteuerung
- Kommunikation online & offline
- Zugriff auf SOPs, Checklisten, Kontakte, Verträge, Sensorik
- Gehärtete Datenbereitstellung – kompatibel mit Windows, Linux, Android, iOS, macOS
- Ballistischer Schutz mit QUICKBLOCK, Wärmebild- & EM-Tarnung
- Sofort einsatzbereit – mit strategischer Beratung & operativer Begleitung

Jeder braucht heute einen Krisenleitstand – wir liefern ihn.
MISSION READY – ONLINE AND OFFLINE.

dtec.bw - Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr (Universität der Bundeswehr München) N03

Das dtec.bw – Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr – ist ein gemeinsam getragenes wissenschaftliches Zentrum der Universität der Bundeswehr München (UniBw M) und der Helmut-Schmidt-Universität/Universität der Bundeswehr Hamburg (HSU/UniBw H). Mit der Aufnahme in den Deutschen Aufbau- und Resilienzplan (DARP) wird dtec.bw von der Europäischen Union – NextGenerationEU finanziert. Mit über 60 finanzierten Forschungsprojekten zu Schlüssel- und Zukunftstechnologien, mehr als 3.500 Publikationen und Beiträgen, 300 Partnerschaften, über 500 entwickelten Technologien und Prototypen sowie mehreren Patenten und Start-ups stärkt das dtec.bw die technologische Resilienz Deutschlands und schafft Mehrwert für Gesellschaft und Bundeswehr.

D-Trust GmbH S25

Die D-Trust GmbH mit Sitz in Berlin ist ein Unternehmen der Bundesdruckerei-Gruppe und mit ihren technologisch ausgereiften Lösungen ein Vorreiter für sichere digitale Geschäftsprozesse und Identitäten. Als unabhängiger und qualifizierter Vertrauensdiensteanbieter ist D-Trust bereits seit 2016 im Rahmen der eIDAS-Verordnung bei der Bundesnetzagentur gelistet. Das Unternehmen übersetzt Vertrauen in konkrete Produkte: Es stellt rechtssichere und zertifizierte Vertrauensdienste wie digitale Zertifikate und elektronische Signaturen sowie Lösungen zum sicheren Datenmanagement wie Datentreuhänder-Plattformen zur Verfügung. Sie entsprechen den höchsten Sicherheitsstandards moderner Infrastrukturen und ermöglichen sichere digitale Identitäten für Unternehmen, Behörden und im privaten Umfeld.

Dynamit Nobel Defence S31

Die Dynamit Nobel Defence GmbH (DND) ist ein mittelständischer Systemanbieter der Verteidigungsindustrie mit Hauptsitz in Burbach (NRW). Weitere Standorte liegen in Berlin, Leipzig und Kiel. Das Unternehmen beschäftigt über 600 hochqualifizierte Mitarbeiterinnen und Mitarbeiter. Das Portfolio ist breit diversifiziert und umfasst schultergestützte Mehrzweck-Waffensysteme, Reaktivschutz-Systeme für Landplattformen, Counter Mobility Lösungen, Digitalisierungskapazitäten für Landstreitkräfte sowie Brandschutzsysteme für zivile und militärische Anwendungen. Zudem bietet DND Testladungen sowie Umwelt- und Qualifizierungsdienstleistungen und umfassende Forschungs- und Entwicklungsleistungen im grundlagenorientierten wie auch im angewandten Bereich an und unterstützt damit Kunden weltweit.

ECOS Technology GmbH S25

ECOS ist ein deutscher Softwarehersteller für Cybersecurity-Produkte, spezialisiert auf: Homeoffice, mobiles Arbeiten. BYOD Der ECOS SecureBootStick ermöglicht hochsicheren Zugriff auf VS-NfD-eingestufte Daten & Anwendungen, von einem ungemanagten Endgerät aus.
Videokonferenzen & Fernausbildung. Das ECOS SecureConferenceCenter bietet alle Funktionen einer Videokonferenzlösung. Für den Zugriff außerhalb gesicherter Netze erlaubt die Kombination mit dem Secure Boot Stick VS-NfD-konforme Videokonferenzen.
Identitäten, Schlüssel & Zertifikate. Die ECOS TrustManagementAppliance ist eine PKI- & Key-Management-Lösung zur Erstellung, Verteilung und Validierung digitaler Zertifikate und Schlüssel für IT, OT und IoT, inklusive Certificate Lifecycle Management – mit BSI-Einsatzerlaubnis für VS-NfD.

EGL Elektronik Vertrieb GmbH S57

Ihr Partner für Abstrahlsicherheit. Vielen Nutzern ist es nicht bekannt, dass bei einer Daten-Verarbeitung unweigerlich kompromittierende Abstrahlung direkt an der aktuell genutzten Hardware auftritt. Diese Abstrahlung kann zur Wiederherstellung der Daten genutzt werden und somit zum Verlust der Vertraulichkeit der zu schützenden geheimen Information führen.
Mit geeigneten Abschirmmaßnahmen kann diese kompromittierende Abstrahlung auf ein nicht auswertbares Maß reduziert werden. Auf diese Schirmung und Entstörung hat sich die Firma EGL Elektronik Vertrieb GmbH spezialisiert.Gerne stehen wir Ihnen für Fragen zur Verfügung. Tel.: 06051-71838 E-Mail: info@eglgmbh.de

EIZO Europe GmbH S82

EIZO ist ein weltweit führender Anbieter visueller Lösungen mit COTS- und MCOTS-Produkten für extreme Einsatzbedingungen. Das Portfolio umfasst TEMPEST-konforme Low-Emission-Monitore zum Schutz vor digitaler Abstrahlung sowie MIL-STD-konforme Lösungen für Verteidigung, Avionik, Luft- und Raumfahrt, ISR, Marine, EW und SIGINT. Dazu zählen rugged LCD-Monitore, Hochleistungsgrafikkarten, GPGPU-Verarbeitung und Videoerfassung sowie rugged Video-Encoder. Mit Hauptsitz in Japan und Niederlassungen u.a. in den USA und Europa entwickelt EIZO Produkte in-house und kann selbst nach MIL-Standards testen. Spezifische Kundenanforderungen, erweiterter Lebenszyklus-Support und ein hohes Maß an Zuverlässigkeit können durch strenge Kontrollprozesse gewährleistet werden.

eleQtron GmbH R48

eleQtron entwickelt skalierbare Quantencomputer auf Basis gefangener Ionen.
Mithilfe der patentierten MAGIC-Technologie (Magnetic Gradient Induced Coupling) werden Qubits mit präziser Mikrowellentechnik statt komplexer Lasersysteme gesteuert. Ziel ist es, Quantencomputing aus der Forschung in reale industrielle Anwendungen zu überführen. Bereits heute betreibt eleQtron Quantencomputer in enger Zusammenarbeit mit den Projektpartnern DLR (Deutsches Zentrum für Luft- und Raumfahrt) und dem Forschungszentrum Jülich.

Elma Electronic R46

Elma Electronic ist ein weltweit führender Anbieter von Embedded-Computing-Lösungen, darunter integrierte Gehäusesysteme, Platinenprodukte, modulare Gehäuse, Geräteschränke und Präzisionshardwarekomponenten in Standard- und kundenspezifischen Konfigurationen. Als globales Unternehmen sind wir mit Vertriebs-, Design- und Produktionsstätten auf drei Kontinenten eng mit unseren Kunden und Partnern weltweit verbunden.
Zuverlässigkeit und langfristiger Support mit einer langen Geschichte von fundiertem technischem Fachwissen und Präzisionstechnik. Das ist Elma.

Emerging Leaders AFCEA — EL01 - EL04

Die Startup-Ausstellungsfläche der AFCEA Emerging Leader auf der 39. AFCEA-Fachausstellung 2026 bietet jungen, innovativen Unternehmen eine einzigartige Bühne, um ihre Ideen, Technologien und Lösungen einem hochkarätigen Fachpublikum aus Verteidigung, öffentlichem Sektor, Wissenschaft und Wirtschaft zu präsentieren. In einem dynamischen, inspirierenden Umfeld erhalten Startups die Chance, neue Märkte zu erschließen, strategische Partnerschaften aufzubauen und ihre Sichtbarkeit nachhaltig zu erhöhen. Gemeinsam stärken wir die Resilienz Deutschlands – durch Innovation, Vernetzung und unternehmerischen Mut.

Eraneos Germany GmbH — A17b

Eraneos ist eine vollständig europäische Beratung, die als skalierte Boutique etablierte Denk- und Handlungsweisen hinterfragt. Das Ziel: Erfolg der Kunden im Umfeld permanenter Veränderung.
Um das zu erreichen, transformiert Eraneos Unternehmen und gestaltet den technologischen Wandel mit einem Schwerpunkt auf KI aktiv mit. Mit unternehmerischem Weitblick hilft Eraneos seinen Kunden, zu wachsen und effizienter zu werden.
Der aktuelle Wachstums-Superzyklus im Verteidigungsbereich bildet die Grundlage des paneuropäischen Verteidigungsteams, das Prozesse skaliert, Markteintritte ermöglicht und Wertschöpfungsnetzwerke schafft.

Emproof B.V. — EL03

In der Verteidigung bestimmen zunehmend Software und KI-Modelle die militärische Überlegenheit, weit mehr als die reine Hardware. Genau diese digitalen Fähigkeiten sind jedoch ein zentrales Ziel von Angreifern und Hackern. Embedded Software wird ausgelesen, nachgeahmt und zur Entwicklung von Gegenangriffsmodellen missbraucht. Genau dies verhindert Emproof mit seiner Embedded-Security-Lösung Emproof Nyx, um technologische und militärische Überlegenheit wirksam zu schützen.

Esri Deutschland GmbH — F22

Für raumbezogenes Analysieren, Planen und Entscheiden sind Geoinformationslösungen basierend auf ArcGIS von Esri die erste Wahl für Privatwirtschaft, Verwaltung und Wissenschaft. Anpassungsfähigkeit, Intuitivität und Integrationsfähigkeit kennzeichnen den Industriestandard ArcGIS: mobil, auf dem Desktop und auf Serverebene. Mehr als eine Million Anwender weltweit wissen dies zu schätzen.
Die Esri Deutschland GmbH mit Sitz in Kranzberg bei München vertreibt als Distributor die Produkte von Esri Inc. exklusiv über acht Standorte in Deutschland. Esri unterstützt die Anwender mit einem breit gefächerten Schulungs-, Support- und Consultingangebot und dem gesamten Erfahrungsreichtum von mehr als 250 Mitarbeitern.

Enercon Technologies LTD — B04

Bel Aerospace & Defense designs and delivers advanced power conversion, power management, and rugged networking solutions for aerospace and defense applications. Part of Bel Fuse Inc., we combine deep engineering expertise with global resources and innovation capabilities.
Our solutions support airborne, naval, and ground platforms, helping enable reliable, mission-ready performance in demanding environments. With decades of military-grade design and production experience, we serve customers across Europe with local support and close alignment to regional standards and program requirements.

FERCHAU GmbH — R56

FERCHAU (Aerospace/Defence) und RST Rostock System-Technik präsentieren sich auf der AFCEA als schlagkräftiger Verbund für die technologische Souveränität der Bundeswehr und Sicherheitsorgane. Wir vereinen die Skalierbarkeit eines Marktführers mit der tiefen Systemkompetenz eines spezialisierten Entwicklungshauses.
Unser Fokus liegt auf ganzheitlichem Systems Engineering, der Entwicklung missionskritischer Software und Embedded Systems sowie hochspezialisiertem Prüfstandsbau. Von der Luftfahrt-Expertise über Simulationslösungen (VR/AR) bis hin zum Integrated Logistics Support (ILS) bieten wir zertifizierte Prozesse und Innovationen „Made in Germany“. Gemeinsam transformieren wir komplexe Anforderungen in einsatzbereite Hochtechnologie für die Verteidigung der Zukunft.

EPAK GmbH — S07

Die EPAK GmbH, 2000 in Leipzig gegründet, hat sich als führender deutscher Entwickler und Hersteller von automatisch nachführenden Satellitenantennen etabliert. Mit jahrelanger Kompetenz in Hard- und Softwareentwicklung, konzipiert und integriert EPAK komplexe Kommunikationssysteme der Zukunft.
Speziell für den behördlichen Markt wurde ein passives Radarsystem entwickelt. Auch als Bodenstation für Kleinsatelliten im LEO/ MEO Orbit oder zur Kommunikation mit nicht-terrestrischen Netzwerkknoten können die Parabolantennen maßgeblich zur technologischen Souveränität beitragen. Durch jahrelange Forschung & Entwicklung in diesem Spezialgebiet hat die EPAK eine einzigartige Nischenkompetenz aufgebaut, die sie zu einem gefragten Partner für anspruchsvolle Satellitenkommunikationslösungen macht.

fiveD GmbH — EL02

fiveD wurde 2024 in Kooperation mit Rohde&Schwarz gegründet und entwickelt eine physikbasierte Radarsimulationsplattform für die effiziente Entwicklung moderner Radare. Die Software ermöglicht realistische Simulationen von Sensoren, Wellenformen, Signalverarbeitung, Interferenzen und Jamming in komplexen Szenarien inklusive Material- und Mehrwegeeffekten. So können Systeme früh virtuell bewertet, Entwicklungsrisiken reduziert und Zyklen verkürzt werden. Gleichzeitig können Signale hochpräzise gelabelt werden was bisher unerreichte Möglichkeiten für Radar-KI bietet.

Fortinet GmbH — S04

Fortinet, weltweit führend im Bereich Cybersecurity, bietet das branchenweit größte Portfolio an Netzwerk- und Cybersecurity-Lösungen auf der innovativsten und leistungsstärksten Netzwerk-Sicherheitsplattform. Unser Ziel ist es, IT-Infrastrukturen abzusichern und zu vereinfachen und sie gleichzeitig vor den modernsten Cyber-Bedrohungen wie Malware, Ransomware und Phishing-Angriffen zu schützen. Unsere KI-gestützten Lösungen umfassen Firewalls, Intrusion-Prevention-Systeme, Endpunktschutz und E-Mail-Sicherheit, Cloud- und Application-Journey-Lösungen sowie Work-from-Anywhere-Technologien, die die Sicherheit und Konnektivität für entfernte Standorte und Mitarbeiter verbessern.

Fujitsu Germany GmbH — F13

Fujitsu ist ein weltweit führender Technologieanbieter mit über 60 Jahren Erfahrung in der Bereitstellung sicherer und zuverlässiger Lösungen für Militär und Regierungen. Wir unterstützen die Verteidigungsindustrie bei den Herausforderungen der modernen Kriegsführung mit innovativen, maßgeschneiderten Lösungen für die digitale Transformation – stets unter Einhaltung höchster Sicherheitsstandards.
Unsere Expertise erstreckt sich auf die gesamte Wertschöpfungskette, von der Beratung und Planung bis hin zur Implementierung und dem Support. Als global agierendes Unternehmen mit rund 113.000 Mitarbeitern in über 100 Ländern verfügt Fujitsu über die Ressourcen und das Know-how, um auch die komplexesten Herausforderungen der Verteidigung zu meistern.

Fraunhofer FKIE — F15

Das Fraunhofer FKIE entwickelt Technologien und Prozesse mit dem Ziel, existenzbedrohende Risiken frühzeitig zu erkennen, zu minimieren und beherrschbar zu machen. Das Institut deckt dabei sämtliche Domänen der Verteidigung und Sicherheit ab – sei es zu Land, in der Luft, zur See, unter Wasser, im Cyberspace oder im Weltall. In enger Kooperation mit strategischen Partnern widmet sich das Institut hierbei der gesamten Verarbeitungskette von Daten und Informationen: vom Gewinn, der Übertragung und Verarbeitung bis hin zu ihrem zuverlässigen Schutz. Seinen Auftrag sieht das Fraunhofer FKIE hier sowohl im zivilen Sektor als auch bei Führungs- und Aufklärungsprozessen im wehrtechnischen Bereich.

GBS TEMPEST & Service GmbH — S03

Die GBS GmbH, mit Sitz in Diepholz, betreibt ein vom BSI anerkanntes Abstrahlprüflabor. Für das Geschäftsfeld TEMPEST, verfügt die GBS GmbH über vier firmeneigene TEMPEST-Labore.
Neben der Berechtigung zur Durchführung von Zulassungsmessungen sowie Kurzmessverfahren nach dem Nationalen Zonenmodell besteht auch die Berechtigung zur Durchführung von Zulassungsmessungen und Kurzmessverfahren nach SDIP 27 Level A, Level B und Level C (International).

Fraunhofer IOSB — W01

Beratung und Technologie für die Verteidigung: In seinem Geschäftsfeld Verteidigung und Sicherheit forscht das Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung IOSB auf den Gebieten der Bildgewinnung durch optronische Systeme, der Bild- und Signalauswertung in Echtzeit sowie Informations- und Simulationssystemen. Wichtige Themen sind dabei auch KI sowie unbemannte Systeme. Mit unserer Analyse- und Bewertungsfähigkeit, in konkreten Technologieprojekten sowie durch Auftragsforschung und Entwicklung unterstützen wir das Bundesministerium der Verteidigung mit seinen nachgeordneten Ämtern und Dienststellen sowie die wehrtechnische Industrie. An erster Stelle steht die rasche Umsetzung aktueller Forschungsergebnisse für die Befähigung der Bundeswehr und zum Schutz der Soldaten.

genua GmbH — F27 & S25 & A16

Mit ihren IT-Sicherheitslösungen „Made in Germany“ ist die genua GmbH eine Wegbereiterin für digitale Souveränität. Behörden, geheimschutzbetreute Organisationen und KRITIS-Unternehmen vertrauen auf genua zum Schutz ihrer digitalen Infrastrukturen. genuas Portfolio umfasst u.a. Firewalls, Gateways, quantenresiliente VPNs, Fernwartungssysteme und Komplettlösungen für VS-NfD-konformes mobiles Arbeiten. Virtualisierte Varianten ermöglichen eine flexible Cloud-Integration. Regelmäßige Zertifizierungen und Zulassungen durch das Bundesamt für Sicherheit in der Informationstechnik belegen das hohe Sicherheits- und Qualitätsniveau.
Kontakt: Tel +49 89 991950-902 | vertrieb@genua.de | www.genua.de

Frequentis Deutschland GmbH — S75

Frequentis ist ein weltweit führender Anbieter sicherheitskritischer Applikationen für Operationszentralen. Die Systeme kommen überall dort zum Einsatz, wo höchste Anforderungen an Zuverlässigkeit, Verfügbarkeit und Sicherheit bestehen.
Im Geschäftsbereich Defence unterstützt Frequentis verbündete Streitkräfte mit technologischen Lösungen für Führung, Kommunikation und Lagebild. Seit über 30 Jahren vertraut die Bundeswehr auf die Lösungen von Frequentis im Bereich militärische Flugsicherung und Sprachkommunikationssystemen. Für die Bundeswehr realisierte Frequentis mit dem MilRADNET ein landesweites militärisches Radardatennetz zur Verteilung von Flugüberwachungsdaten und zur Überwachung des deutschen Luftraums.

GEOSYSTEMS GmbH — S85

GEOSYSTEMS ist Lösungs- und Servicepartner für GeoIT und unterstützt Behörden und Organisationen mit Sicherheitsaufgaben bei der Gewinnung, Analyse und Visualisierung raumbezogener Informationen. Mit über 35 Jahren Erfahrung entwickelt das Unternehmen hochautomatisierte Downstream-Services, die Satellitenbilddaten mit weiteren Datenquellen verknüpfen und die Ergebnisse geräteübergreifend, auch in 3D, bereitstellen. Das Leistungsspektrum umfasst Fernerkundung, Photogrammetrie, GIS, Datenmanagement sowie browserbasierte Applikationen und 4D-Echtzeitlösungen zur Erstellung einsatzrelevanter Lagebilder. Im Fokus auf der AFCEA steht das Mapping von Drohnendaten mit PhotoMesh Drone von Skyline Software Systems. GEOSYSTEMS ist ein Tochterunternehmen der OHB-Gruppe.

Getac Technology GmbH R41

Getac ist ein weltweit führender Anbieter robuster, KI fähiger mobiler Technologie und intelligenter Videolösungen, darunter Laptops, Tablets, Software, tragbare Kameras, Kfz-Videosysteme, digitales Beweismittelmanagement sowie Videoanalyselösungen für Unternehmen. Getacs Dienstleistungen und Lösungen sind so konzipiert, dass sie allen Anwendern an vorderster Front und in anspruchsvollen Umgebungen erstklassige Erfahrungswerte bieten. In über 100 Ländern versorgt Getac derzeit Kunden in den Bereichen Verteidigung, öffentliche Sicherheit, Rettungsdienste, Feuerwehr, sowie Versorgung, Automobil- und Prozessindustrie, Rohstoffe, Fertigung, Transport & Logistik. Getac wurde von Newsweek als eines der „Verlässlichsten Unternehmen der Welt“ für 2024 ausgezeichnet.

Griffity Defense GmbH F14

griffity defense steht, neben Aktivitäten im Bereich der Geschäftsentwicklung und Marketing-Services, für die Beratung von Unternehmen und dem öAG bei der Lösung komplexer Herausforderungen. Unser Fokus liegt auf der Entwicklung von umfassenden, zukunftssicheren Strategien und integrierten technischen Lösungen, um für die unterschiedlichen Einsatzszenarien bestmögliche Werkzeuge und Infrastruktur bereitzustellen. Unter dem Motto „Vernetzt denken - Kommunikation, Integration, Kollaboration“ zeigen wir mit unseren Partnern modulare Lösungen die einen wesentlichen Beitrag zur Ausgestaltung von Soldatensystemen und mobilen Führungs- und Gefechtsständen für die Digitalisierung der Landstreitkräfte in der taktischen Ebene leisten können.

Glenair GmbH S72

Glenair is a leading manufacturer of cutting-edge connector technologies including both Mil-Spec qualified as well as commercial circular and rectangular connectors. All interconnect designs are available in environmental, filter, hermetic, and fiber optic configurations. Interconnect technologies may be supplied as either discrete components or integrated into turnkey assemblies. In addition to electrical and fiber optic interconnects, Glenair produces and supplies backshells, dummy stowage receptacles, protective covers, and shield termination designs in a variety of materials and a leader in composite accessories. Glenair is also a market leader in cabling systems and lightweight EMI/RFI braid for the military/Aerospace marketplace.

HAT.tec R14

HAT.tec – Human Autonomy Teaming Technologies ist Europas führendes Softwareunternehmen für plattform-unabhängiges Missionsmanagement militärischer und sicherheitsrelevanter Einsätze. Mit Hauptsitz bei München entwickelt das Team umfassende modulare Softwarelösungen für Sicherheits- und Verteidigungskräfte in ganz Europa. Zur optimalen Entscheidungsunterstützung menschlicher Operatoren werden Daten aus den Domänen Land, See und Luft mittels Automatisierung nahtlos integriert, verarbeitet und angezeigt. Durch die Zusammenführung der Daten zu einem einzigen Lagebild bieten die Lösungen bestmögliches Situationsbewusstsein und automatisierte Entscheidungsunterstützung. HAT.tec startete 2018 als Ausgründung der Universität der Bundeswehr von zwei promovierten Luft- und Raumfahrttechnikern.

Global Radio Data Communications Europe Ltd. S16

As GRC Ltd. we are specialists in satellite, RF, cloud and IP networking solutions. We design, integrate and support critical communication systems used globally by defence and government and are a main SATCOM supplier for NATO MoDs.

GRC's 6-SAT service provides managed, flexible worldwide connectivity with multi-orbit (LEO, MEO and GEO), multi-domain hardware and airtime solutions, design, monitoring, training and 24/7 helpdesk support. SCYTALE is our rapidly deployable connectivity solution, scalable from a single user to a welfare deployment or entire HQ. Utilising SD-WAN and supporting any bearer of opportunity, SCYTALE can provide a pop-up network, delivering Wi-Fi, data and VoIP telephones, with options for next-generation encryption, VPN, end-to-end security and cloud routing.

Helsing Germany GmbH S71

Helsing ist ein KI- und Softwareunternehmen der neuesten Generation im Verteidigungsbereich. Es wurde als inhabergeführtes Technologie-Unternehmen gegründet, um KI-Fähigkeiten im Sicherheitssektor zu entwickeln und einzuführen.

Als europäischer Technologievorreiter befähigt Helsing demokratische Gesellschaften, souveräne Entscheidungen zu treffen und eigene ethische Standards durchzusetzen. Unsere Teams entwickeln Technologien, die operative Fähigkeiten neuer und bestehender Verteidigungssysteme in ein neues Zeitalter führen. Wir entwerfen und entwickeln neue Arten autonomer Systeme und arbeiten mit Regierungen und der Industrie zusammen, um bestehende Hardware in ein KI-gestütztes Netzwerk zu integrieren. Unsere Mission: „Künstliche Intelligenz zum Schutze unserer Demokratien“.

Gretchen AI GmbH EL04

Moderne Verteidigungsoperationen sind zunehmend hochentwickelten zivil-militärischen Desinformationskampagnen ausgesetzt, die synthetische Medien, Fälschungen und irreführende Narrative als Waffe nutzen, um Lagebeurteilungen zu verfälschen sowie Entscheidungsträger und Öffentlichkeit zu manipulieren. Gretchen AI – preisgekröntes Startup aus dem DFKI – entwickelt KI-agentenbasierte Tools zur Erkennung synthetischer Inhalte, Informationsintegrität und zur web-weiten Kontextverifikation. Unsere Analysen ermöglichen schnelle, belastbare Entscheidungen und sichern Überlegenheit im C4ISR-Umfeld.

hema electronic GmbH B09c

Embedded Vision Elektroniken für die Wehrtechnik. Der Wunsch nach schneller Beschaffung und Integration neuester Technologien trifft in der Wehr- und Verteidigungsindustrie auf höchste Anforderungen an Zuverlässigkeit und Langzeitverfügbarkeit. hema electronic entwickelt und produziert Elektroniken, die für Driver Vision Enhancer, Systeme für Situational Awareness und andere Anwendungen zum Einsatz kommen, bei denen zahlreiche Sensor- und Signaldaten in Echtzeit verarbeitet werden müssen. Dafür setzt hema auf modulares Design und proaktives Obsoleszenzmanagement. Mit über tausenden Installationen in Kampfpanzern und geschützten Fahrzeugen bewähren sich die Elektroniken unter härtesten Umweltbedingungen.

Klarheit in jeder Mission.

HENSOLDT Ceretron ist die software- und KI-basierte Missionsassistenz für Gefechtsfahrzeuge:
Die CERETRON Software fusioniert Multisensor-Daten in nahezu Echtzeit, erkennt und klassifiziert Bedrohungen automatisiert und priorisiert die entscheidungsrelevanten Informationen – für ein sofort nutzbares Lagebild im BMS.
Dank modularer, containerisierter Software-Architektur lassen sich neue Funktionen schnell integrieren und sicher aktualisieren. Im Einsatz bedeutet das schnellere Entscheidungen, weniger kognitive Belastung der Besatzung und höhere Wirksamkeit in vernetzten Missionen.

Heute einsatzbereit.

www.hensoldt.net

HENSOLDT
Detect and Protect.

HENSOLDT AG — F01 & A05

HENSOLDT
Detect and Protect.

HENSOLDT ist ein führendes Unternehmen der europäischen Verteidigungsindustrie mit globaler Reichweite. Das Unternehmen mit Sitz in Taufkirchen bei München entwickelt Sensorlösungen für Verteidigungs- und Sicherheitsanwendungen.
Als Neo-Systemhaus bietet HENSOLDT plattformunabhängige, vernetzte Sensoren an. Zugleich treibt das Unternehmen die Entwicklung der Verteidigungselektronik und Optronik voran und investiert in neue Lösungen auf Grundlage von Software-Defined Defence. Außerdem erweitert das Unternehmen sein Angebot um neue Service-Modelle und baut sein Portfolio an Systemlösungen aus.
2025 erzielte HENSOLDT einen Umsatz von 2,46 Milliarden Euro. Das Unternehmen beschäftigt circa 9.500 Mitarbeiter. HENSOLDT ist an der Frankfurter Wertpapierbörse im MDAX notiert.

Hirt Systemtechnik GmbH — F24

Hirt
SYSTEMTECHNIK GMBH

Die Firma Hirt Systemtechnik GmbH entwickelt seit über 30 Jahren innovative Lösungen für Kunden in den Bereichen Verteidigung, Luft- und Raumfahrt, Medizintechnik und viele mehr.
Von der Entwicklung, Fertigung und Montage bis zur Auslieferung erhalten unsere Kunden eine maßgeschneiderte Komplettlösung aus einer Hand.
Ob LWL- und Blitzschutz-Module oder Lade- bzw. Netz-Anschaltkästen, die Montage von komplexen Geräten nach höchsten Qualitätsstandards ist neben der Fertigung anspruchsvoller Präzisionsteile eine unserer Kernkompetenzen. Unsere qualifizierten Mitarbeiter erfüllen höchste Anforderungen bei der Montage von Baugruppen und hochkomplexen Geräten.
Die Konfektionierung von Kabeln und Leitungen nach VG 96927-2 im LWL und Kupferbereich runden unsere Kompetenzen ab.

Hewlett Packard Enterprise — F25 & R48

HPE

HPE ist ein führender Anbieter von essenziellen Technologien und bündelt die Stärken von KI, Cloud und Networking, um Unternehmen und öffentliche Einrichtungen voranzubringen. Als Wegbereiter des Fortschritts verbessern wir mit Innovation und Fachkompetenz das Leben und Arbeiten von Menschen. Wir befähigen unsere Kundinnen und Kunden aus allen Branchen, ihre betriebliche Leistung zu optimieren, Daten in wertvolle Prognosen zu verwandeln und ihre Wirkung zu maximieren. Verwirklichen Sie Ihre ambitioniertesten Ziele mit HPE. www.hpe.com

IABG mbH — W06

IABG

Die IABG bietet ganzheitliche Lösungen rund um sichere Digitalisierung, IT-Unterstützung, sichere und souveräne Cloud-Lösungen inkl. Kollaborationsplattformen für den Einsatz von VS-IT, IT-Services und Kommunikation von Streitkräften und BOS. Wir verfügen über einzigartige Kompetenzen für Grundbetrieb, Einsatz und querschnittliche Aufgaben in allen Dimensionen und Fähigkeitsdomänen - von Enterprise Architecture, IT-Unterstützung in der Planung über Konzeption von Aufklärungs- / Wirkungsverbünden, Technologie- und Innovationsmanagement, Optimierung in der Nutzung sowie Cyber Security / Resilience bis zur Erstellung von ganzheitlichen Informationssicherheitskonzepten oder Einführung des Galileo Public Regulated Service.
info@iabg.de

IBM Deutschland GmbH F02

IBM ist ein führender Anbieter in den Bereichen globale Hybrid-Cloud und KI sowie Consulting. Das Lösungsportfolio reicht vom Supercomputer und Software über Dienstleistungen inklusive Beratung bis hin zur Finanzierung. Software Defined Defense ist für IBM Basis und Schlüssel für die effektive und effiziente Transformation der Bundeswehr. Bei der Software-getriebenen Digitalisierung kommen standardisierte, offene und wiederverwendbare Software-Komponenten zum Einsatz, die in einem interoperablen Ökosystem kompatibel nutzbar sind. Die eigens für Kunden aus dem Verteidigungsbereich eingerichtete IBM Garage for Defense in Bonn ist ein Ort, an dem diese digitale Transformation konzipiert und gestaltet wird. Mehr Informationen: https://software-defined-defense.de/

iesy GmbH S63

Wir sichern und stärken digitale Souveränität.
Die iesy GmbH entwickelt und fertigt seit 60 Jahren hochspezialisierte, komplette Embedded-Systemlösungen für sicherheitskritische Defense-Anwendungen. Unsere Systeme kommen in taktischen Führungsfahrzeugen, geschützten Kommunikations- und Kryptoeinheiten, unbemannten Plattformen sowie in Sensor- und Aufklärungssystemen zum Einsatz. Hard- und Software werden bei uns als untrennbare, validierte Gesamtsysteme entwickelt und geliefert. Ausgelegt für Schock, Vibration, extreme Temperaturen und elektromagnetische Belastung – mit kontrollierter Lieferkette und Langzeitverfügbarkeit, vollständig entwickelt und gefertigt in Deutschland.

IHSE GmbH S81

Die IHSE GmbH ist ein weltweit führender Entwickler und Hersteller hochsicherer IT-Infrastruktur. IHSE-Lösungen ermöglichen es, mehrere Computer mit nur einer Tastatur, einer Maus und ein oder mehreren Monitoren zu steuern. Durch diese Technologie können der eigentliche Computer und der Arbeitsplatz über mehrere hundert oder tausend Meter voneinander getrennt sein. So werden ein komfortables und effizientes Arbeitsumfeld und optimierte Arbeitsabläufe geschaffen.
In sicherheitskritischen Umgebungen spielen IHSE-Lösungen eine Schlüsselrolle, da sie höchsten Sicherheitsanforderungen entsprechen und umfassenden Schutz der Systeme garantieren. Unbefugter Zugriff oder das Einschleusen von Malware werden verhindert und Datensicherheit gewährleistet.

iMAR Navigation GmbH F14

Die iMAR Navigation GmbH, ein deutsches Unternehmen, ist seit über 30 Jahren ein anerkannter Spezialist und Innovator für führende Inertialsysteme und Lösungen.
Dank unserer langjährigen Erfahrung in der Produktion, Entwicklung, Wartung und im Support von Inertialsystemen für Positionierung, Navigation, Vermessung, Führung, Stabilisierung, Steuerung und Kommunikation (PNT/PNTC) bieten wir leistungsstarke Systeme und Lösungen für ein breites Anwendungsspektrum unbemannter und bemannter Plattformen in Industrie, Automobilbranche, Luft- und Raumfahrt, Geodäsie sowie Verteidigung – sowohl ab Lager als auch als kundenspezifische Lösung. iMAR Navigation wurde 1992 gegründet und hat seinen Sitz in St. Ingbert im Saarland.

Imtradex Hör- und Sprechsysteme GmbH F14

Seit über 30 Jahren ist Imtradex ein verlässlicher Partner für Behörden und Organisationen mit Sicherheitsaufgaben, u.a. auch für die Bundeswehr. Mit der Produktion und Entwicklung in Deutschland bieten wir Kommunikationslösungen für verschiedene Einsatzbereiche. Von der Leitstelle bis zum Soldaten im Feld. Seit 2017 sind wir der vertrauensvolle Ansprechpartner, wenn es um taktische Kommunikationssysteme der Firma INVISIO geht. Seit 2021 auch für Headsets im CVC Bereich der Firma Racal Acoustics. Auf der Messe zeigen wir u.a. den marktführenden In-Ear Gehörschutz X7 mit 39 dB Dämpfung. Weiterhin gibt es verschiedene Lösungen im Bereich Leitstelle, u.a. die innovative Mobile Sprechstelle MDU/MVU.

Indicium Technologies GmbH EL03

Indicium Technologies steht für Vertrauen durch Transparenz und Technologie. Wir bieten KI-gestützte, DSGVO-konforme Background Checks für Mitarbeiter, Partner und sensible Rollen - entwickelt für Organisationen mit höchsten Sicherheits- und Compliance-Anforderungen. Unsere Plattform prüft Identität, Werdegang und relevante Risiken schnell, rechtssicher und nachvollziehbar.
Gegründet 2020 und geführt mit juristischer wie technologischer Expertise, unterstützen wir Behörden, kritische Infrastrukturen und sicherheitsrelevante Unternehmen dabei, fundierte Entscheidungen ohne Grauzonen zu treffen.

Indra Group S11

Die Indra Group bietet sichere und effiziente Lösungen in den Bereichen ATM, Verteidigung und Raumfahrt. Von der Luftfahrtinformationsverwaltung über Kommunikationslösungen bis hin zu missionskritischen Verteidigungsoperationen und Satellitenkommunikation unterstützt unsere Technologie komplexe, sicherheitskritische und militärische Einsätze. Zusätzlich nehmen dieses Jahr Indra Park Air (UK) und Indra Air Traffic (USA) mit ihren Lösungen teil.
www.indragroup.com

infodas GmbH S46

Die INFODAS GmbH zählt seit über 50 Jahren zu den führenden Lösungsanbietern für Cyber- und Informationssicherheit in Deutschland. Als Airbus Tochterunternehmen, spezialisiert auf Cyber und IT, begleitet und berät die infodas das Militär, öffentliche Verwaltungen, Behörden und Unternehmen mit Dienstleistungen in der Konzeption und Umsetzung umfassender Ansätze von sicherheitsrelevanten Themen. Mit der auf höchstem Sicherheitslevel zertifizierten SDoT Produktfamilie liefert die infodas erstklassige Lösungen zur Sicherung der digitalen Datennutzung und Kommunikation. Durch Umfassende und maßgeschneiderte Dienstleistungsangebote von zertifizierten Experten aus dem Bereich Cybersecurity-Consulting wird das Unternehmen individuellen Kundenansprüchen gerecht.

INNOSYSTEC GmbH — S34

Seit der Firmengründung im Jahr 2000 entwickelt INNO Softwarelösungen Made in Germany für Sicherheitsbehörden, zivile Nachrichtendienste und Militär. Unser Produkt SCOPE bietet eine einzigartige Plattform für die Korrelation und Analyse von Milliarden von Datensätzen aus unterschiedlichsten Quellen. Wir helfen Ihnen dabei, riesige Datenmengen in entscheidende Erkenntnisse zum richtigen Zeitpunkt zu verwandeln. Erkenntnisse, durch die Terroranschläge verhindert, Verbrechen aufgeklärt und der Frieden erhalten werden kann. Darauf sind wir stolz.
In den kommenden 25 Jahren haben wir noch einiges vor: In unserem neu gebauten Firmensitz in Salem/Bodensee ist genügend Platz, um unser 100-köpfiges Experten-Team zu verdoppeln.
INNO | NOW YOU KNOW

inxire GmbH — F37

inxire ist ein führender Produkt- und Serviceanbieter für Enterprise Digitalization mit Sitz in Frankfurt am Main. Das Unternehmen entwickelt maßgeschneiderte Software für Content Management, Datensicherheit und Intelligent Decision Support, die als Basis für innovative digitale Geschäftsmodelle dient.
Ein Kernprodukt ist inxire Classified: ein digitales VS-Registratursystem für die medienbruchfreie und VSA-konforme Handhabung von Verschlusssachen bis zur Einstufung GEHEIM. Internationale Top-Kunden wie die Deutsche Bahn, die Bundeswehr und die National Ignition Facility beschleunigen mit inxire bereits heute ihre digitale Transformation.
Weitere Informationen finden Sie unter www.inxire.com.

INTEC Group — R63

Die INTEC Gruppe – Ihr unabhängiger Partner für Technologie, Systemintegration und Dokumentation
Die INTEC Gruppe vereint die Kompetenzen von vier etablierten Unternehmen: INTEC Industrie-Technik GmbH, OSW, TECO und SCOPE Engineering. Unter dem Dach der INTEC Holding bündeln wir herstellerunabhängige und hardwareneutrale Engineering-, Systemintegrations- und Dokumentationsexpertise für ganzheitliche Lösungen aus einer Hand. Gemeinsam bieten wir ein einzigartiges Leistungsportfolio über den gesamten Lebenszyklus komplexer Systeme – von Konzeption, Software- und Systemdesign über Systemintegration und Technische Dokumentation bis zu ILS- und Lifecycle-Support.

itemis AG — P14

itemis supports organizations in the development and compliance of complex digital and cyber-physical systems. As a technology enabler and engineering partner, we combine software and systems engineering with high requirements for safety, cybersecurity, and the responsible use of artificial intelligence.
In addition to project-based support, we contribute our own products and modular solution components – ranging from model-based integration and migration concepts to extensions of existing development environments and entirely new, innovative tools that increase efficiency across the system lifecycle. Our goal is to make technological innovation transparent, resilient, and better manageable.

itWatch GmbH — S10

itWatch stellt patentierte IT-Sicherheit her. Im Fokus stehen Schutz gegen Datendiebstahl (Data Loss Prevention - DLP), technische Vertrauensketten von der Tastatur bis zu den Daten und deren organisatorische Einbettung durch rechtsverbindliche Dialoge, Endpoint Security, Datenschleuse mit Datenwäsche – itWash (Data Sanitizing) sowie Mobile Security und Verschlüsselung.
Die seit 1997 entwickelten Produkte zeichnen sich durch hohe Sicherheit aus, belegt durch den Einsatz in VS-NfD und GEHEIM klassifizierten Umgebungen. Diese sind höher als CC EAL 4+ zu bewerten, da nicht gegen ein vom Hersteller definiertes Protection Profile geprüft wird, sondern alle Produkt-Facetten in real vernetzten Einsatzumgebungen professionellen Angriffsszenarien ausgesetzt werden.
Mehr unter: https://itwatch.de

JK Defence & Security Products GmbH — S30

Seit über 30 Jahren liefert JK Defence als zuverlässiger Partner der Bundeswehr Funkkommunikationssysteme der Spitzenklasse. Marktverfügbare Lösungen bieten dem Anwender robuste und sichere Vernetzung in anspruchsvollen Szenarien. Mit unseren Partnern L3Harris, Nantenna, Rolatube, Rowden, Spectra, Ultralife und ViaSat finden wir stets die passende Lösung. Kompetentes Systemengineering und Projektmanagement begleitet unsere Kunden von Bedarfsanalyse bis Inbetriebnahme und darüber hinaus.
In eigenen Werkstätten führen wir kompetent, schnell und zuverlässig Befundungen, Regelinstandsetzungen und Reparaturen durch. So steht unseren Kunden ein kompetenter, zuverlässiger und schnell agierender Partner in Deutschland zur Verfügung.
www.jkdefence.de, milcom@jkdefence.de, 02152/1445-207

Janes — F09

In a complex global landscape, leaders need accurate information and full context quickly. Janes equips defence, government, and industry leaders with validated intelligence to act quickly and confidently. Our experts combine advanced technology with a proven tradecraft, to collect, analyse, and validate millions of data points to deliver intelligence our customers use for assessing threats, accelerating decisions and staying ahead of emerging challenges. We deliver this intelligence as a single, contextual view that is system-ready and easy to integrate into any workflow.

JOWO - Systemtechnik AG — W10

Die JOWO - Systemtechnik AG ist Hersteller und Distributor von elektrischen und optischen Steckverbindern, LWL- und elektrischen Verkabelungen, sowie kundenspezifischen Lösungen seit 1995. In Zusammenarbeit mit namenhaften Herstellern erstellen wir für sie stets die besten Lösungen. Wir bieten:

- Elektrische Steckverbinder für Militär, Industrie, Luft- u. Raumfahrt,
- Marine, Öl und Gas (Ex-Lösungen)
- Endgehäuse, Schutzkappen, Werkzeuge
- LWL-Steckverbinder Multimode/Singlemode
- Reinigungs- und Testkoffer
- Kabelbäume militärisch/zivil in LWL, Signal, Leistung, HF, Hybrid
- Systemlösungen
- Konstruktion kundenspezifischer Lösungen
- Drucktests bis 1000 Bar
- Schnellfertigungslinie Marinebronzestecker MIL/VG
- Zugelassen nach EN9120, NATO C6689 und VG96927 Typen C, D, E, M und E

Kappa optronics GmbH R19

The world's safest vision systems for defense mobility and autonomous machines

Kappa optronics bietet skalierbare Driver Vision Enhancer (DVE) und Situational Konzept basiert auf flexiblen Kamerakonfigurationen mit hochwertigen Tag- und Nachtsichtsensoren, einem leistungsstarken digitalen Videomanagement sowie robusten Displays. Vorteile: eine nahtlose Rundumsicht von bis zu 360° bei extrem niedriger Latenz, Image Fusion VIS/LWIR und Stitching. Die Systeme sind erfolgreich auf verschiedenen Plattformen im Einsatz. Ergänzt wird das Portfolio durch laser- und kamerabasierte Systeme zur Rohrinspektion.

Mit über 45 Jahren Erfahrung steht Kappa für einsatzbewährte Lösungen in Verteidigung und Luftfahrt. Seit 2026 ist Kappa Teil der THEON Gruppe.

KIX Service Software GmbH P03

KIX ist die digital souveräne Open-Source-Plattform für Service Management aus Deutschland – mit Support in Deutschland. Die moderne, skalierbare Architektur ermöglicht den flexiblen OnPrem-Betrieb oder als SaaS im eigenen Rechenzentrum.

KIX ist mit 16 ITIL® 4 Practices im Gold-Level zertifiziert und verfügt damit über die höchste Zertifizierung einer Open-Source-ITSM-Software. IT Service Management, Asset-Management für IT- und Non-IT-Equipment, Wartungsplanung für technisches Equipment, Workforce-, Field Service- und Workflow Management sowie Vertrags- und Wissensmanagement werden durch KIX unterstützt. Die moderne REST-API ermöglicht umfassende Integrationen. Anpassungen erfolgen vollständig per grafisch unterstützter Konfiguration (No-Code- und Low-Code) – ohne Programmierung.

Klepsydra Technologies AG R48

Klepsydra entwickelt fortschrittliche, patentierte Edge-KI-Softwarelösungen für Embedded Systeme. Wir konzentrieren uns auf die Entwicklung von Software, die das Potenzial von KI und Edge-Datenverarbeitung auf verschiedensten Prozessoren maximiert und dadurch hohe Leistung und Effizienz liefert.

Klepsydra Technologies hat sich zum Ziel gesetzt, ein weltweit führender Anbieter von KI- und Edge-Datenverarbeitungslösungen zu sein. Unsere Partnerschaften mit Herstellern von Edge-Prozessoren und Betriebssystemen stärken diese Vision. Unsere Software wurde im Rahmen mehrerer Projekte erfolgreich mit der Europäischen Raumfahrtagentur ESA getestet, was ihre Zuverlässigkeit und Innovation unter Beweis stellt.

Knapp Service Koblenz GmbH W09

Knapp Service Koblenz GmbH - Als bodenständiger Mittelständler sind wir seit Jahrzehnten Lieferant für Bundeswehr, BAAINBw, HIL, BwFPS sowie für wehrtechnische Systemhäuser. Wir sind spezialisiert auf die Entwicklung, Fertigung und Instandsetzung von Einbausätzen für Funk- und Führungsmittel und Kabelbäumen sowie für die Serieninstandsetzung von Baugruppen. Derzeitiger Schwerpunkt sind u.a. Einrüstungen in MERCEDES G- Modelle einschließlich D-LBO. Auch Musterintegrationen und Kleinstserien können von uns in höchster Qualität bearbeitet werden. Unser Standort in Koblenz bietet modernste Infrastruktur in einer KWKg gesicherten Umgebung. Wir haben etablierte und zuverlässige Lieferanten, wachsen gerne und suchen Verstärkung.

www.knapp-service.de | info@knapp-service.de

KNDS Deutschland GmbH & Co. KG A11

KNDS ist ein führender europäischer Anbieter militärischer Landsysteme mit mehr als 11.000 Mitarbeitern, einem Umsatz von 3,8 Milliarden Euro im Jahr 2024, einem Auftragsbestand von rund 23,5 Milliarden Euro und einem Auftragseingang von 11,2 Milliarden in 2024. Als Hauptauftragnehmer und führender Systemintegrator entwickelt, liefert und wartet KNDS modernste bemannte und unbemannte 'system-of-systems', komplette Missionslösungen und deren Haupt- und Subsysteme, einschließlich der dazugehörigen Munition und Service. Das Produktportfolio umfasst Kampfpanzer, gepanzerte Fahrzeuge, Artilleriesysteme, Waffensysteme, Munition, Robotik, militärische Brücken, Kundendienst, Battle Management Systeme, Ausbildungslösungen, Schutzlösungen und eine breite Palette von Ausrüstungen.

KNDS Deutschland Mission Electronics GmbH S48

KNDS Deutschland Mission Electronics GmbH (ehemals ATM ComputerSysteme GmbH) ist Spezialist für gehärtete IT- und Kommunikationssysteme. Als langjähriger Partner der Bundeswehr bilden die Systemlösungen das digitale Rückgrat der Heeresfahrzeuge. Als Systemhaus konzipiert, entwickelt und programmiert KNDS Deutschland Mission Electronics alle Systemlösungen am Standort in Konstanz. „Von der ersten Idee, über die Entwicklung und Integration bis zur Serie" lautet die Philosophie von KNDS Deutschland Mission Electronics. Zum Portfolio gehören gehärtete Computersysteme, Displays, Panel-PCs, Ethernet-Switche, mobile und stationäre Kommunikationsanwendungen sowie Kommunikations- und Life-Cycle-Software. KNDS Deutschland Mission Electronics ist eine Tochterfirma von KNDS Deutschland GmbH & Co KG.

Kobra Infosec GmbH F29

KOBRA VS Datenträger beinhalten externe verschlüsselte Festplatten und USB-Sticks mit BSI-Zulassung bis VS-NfD, NATO- und EU-RESTRICTED. Diese Datenträger sind vorwiegend für Behörden und Unternehmen mit Geheimschutzbetreuung entwickelt und hergestellt. Die Vertraulichkeit der Daten wird durch die AES-Verschlüsselung mittels Verwendung zweier 256-Bit-Kryptoschlüssel, die Zwei-Faktor-Authentifizierung mittels Smartcard und PIN sowie die Verwaltung der Krypto-Schlüssel gewährleistet.

Die Verwaltungssoftware Kobra Client VS unterstützt Administratoren bei der Einrichtung und Verwaltung von KOBRA VS Datenträger. Die Software steht kostenfrei zur Verfügung und ermöglicht die Nutzung zusätzlicher Funktionen dieser Datenträger.

Kobra Infosec GmbH: +49/345/2317350; info@kobra-infosec.de

Kommando Cyber- und Informationsraum B03

In aktuellen und zukünftigen militärischen Konflikten spielt der Cyber- und Informationsraum (CIR) eine entscheidende Rolle. Auf dem gläsernen Gefechtsfeld zählt jede Sekunde: Informationen müssen schnell und sicher gewonnen, ausgewertet und übermittelt werden. Sie sind Voraussetzung für ein Lagebild in Echtzeit. Die Vernetzung der Streitkräfte trägt maßgeblich zum Erfolg von Multi Domain Operations bei. Die Teilstreitkraft (TSK) CIR stellt hierfür als „zentrales Nervensystem" wesentliche Fähigkeiten wie IT-Services, Aufklärung, Einsatzunterstützung aus dem Weltraum, Cyberoperationen, Elektromagnetische Kampfführung, Operative Kommunikation und Geoinformationen bereit.

Geführt wird die jüngste TSK der Bundeswehr aus dem Kommando CIR heraus – dem Dienstsitz des InspCIR in Bonn.

Laokoon Security GmbH — EL02

Laokoon Security wurde von ehemaligen Hackern der Bundeswehr und anderen Bundessicherheitsbehörden gegründet, um offensive Cybersicherheitsdienstleistungen wie Red Teaming und Penetrationstests anzubieten.
Aus den Erfahrungen als Angreifern entstand HoneyGuard360, einem Honeypot-as-a-Service, der trotz extrem niedriger False-Positive Rate laufende Angriffe bereits in einem frühen Stadium aufklären kann und so Verteidigungsmaßnahmen besonders wirksam sind. Laokoon Security befindet sich derzeit im LEVELHUB Acceleratorprogramm, welches Start-Ups auf die internationale Skalierung vorbereitet.

Lateration GmbH — P10

Lateration develops the next-generation soldier system. By providing soldiers with reliable information exactly when and where it is needed, our technology reduces uncertainty on the battlefield, strengthens decision-making under pressure, and ultimately helps save lives by ensuring the right decisions are made at the right moment.

LEONARDO Germany GmbH — R54 & A06

LEONARDO Germany GmbH ist eine Tochter des Leonardo-Konzerns, einem der weltweit führenden Produzenten von Systemen der Luftfahrtbranche und im Verteidigungsmarkt. Als innovatives Technologieunternehmen sind wir auf hochmoderne Technologieprodukte, Dienstleistungen und Lösungen für die internationalen Meteorologie- und Militärmärkte spezialisiert. Wir liefern Wetterradar- und Lidarsysteme für die Meteorologie sowie Luftüberwachung und Präzisionsanflugradare für die deutschen Verteidigung. Ergänzt wird unser Produktportfolio durch funkbasierte Kommunikationssysteme, Shelter-Integration sowie durch Software, Dienstleistungen und Lösungen für den Schutz und die Sicherheit kritischer Infrastrukturen. Bei der AFCEA 2026 zeigen wir unsere maßgeschneiderten Containerlösungen für den IKT-Bedarf.

LiveDrop B.V. — EL01

LiveDrop B.V. ist ein niederländisches Deep-Tech-Unternehmen mit Sitz in Eindhoven. Das Unternehmen entwickelt eine innovative Technologie für sichere, vollständig offlinebasierte Datenübertragung. LiveDrop ermöglicht den verschlüsselten Austausch von Informationen ohne Funk, Kabel oder Netzwerke, indem Daten visuell über Displays und Kameras übertragen werden. Dadurch wird eine echte Air-Gap-Kommunikation geschaffen, die Abhören, Stören und Cyberangriffe verhindert. Die Technologie richtet sich insbesondere an sicherheitskritische Bereiche wie Verteidigung, Behörden und Cybersecurity.

LS telcom AG — Q04

VERWALTEN, ÜBERWACHEN und VERTEIDIGEN Sie Ihr Spektrum - Das elektromagnetische Spektrum (EMS) ist zu einer entscheidenden Domäne moderner militärischer Operationen geworden. Die sichere, störungsfreie & effiziente Nutzung des Spektrums ist eine zentrale Voraussetzung für erfolgreiche Missionen. Elektronische Kampfführung (EloKa) ermöglicht Streitkräften, das elektromagnetische Umfeld zu beherrschen, Bedrohungen frühzeitig zu erkennen und die Einsatzfähigkeit eigener Sensoren, Komm.-Systeme & Plattformen zu sichern. LS telcom ist führender Lösungsanbieter für elektromagnetische Spektrums-Operationen (EMSO):

- Spektrumsmanagement & -planung
- Spektrumsüberwachung, Peilung und Geolokalisierung
- Funknetz- & Missionsplanung
- Elektronische Unterstützungsmaßnahmen, Signal Intelligence (SIGINT)

Marble Imaging GmbH — EL02

Marble Imaging ist ein europäisches Start-Up für hochauflösende Erdbeobachtung und sicherheitsrelevante Datenservices. Mit einer eigenen VHR-Satellitenkonstellation liefert Marble zeitkritische, verlässliche Daten für strategische, operative und taktische Aufklärung. Der Fokus liegt auf Defense- und Security-Use-Cases wie Lagebildgenerierung, Infrastrukturüberwachung sowie Krisen- und Konfliktmonitoring. KI-gestützte Analysen, souveräner Datenzugang und missionsorientierte Services ermöglichen eine schnelle, belastbare Entscheidungsunterstützung für staatliche und militärische Nutzer.

Marinekommando / Marineinnovationsmanagement — G 03a

Die Gruppe Marineinnovationsmanagement, als ein Teil des Marinekommandos, fungiert als Ansprechpartner für die Erarbeitung und Weiterentwicklung von Innovationsvorhaben der Marine. Wir identifizieren Bedarfe, entwickeln daraus konkrete Lösungsansätze und überführen Ideen in umsetzbare Projekte.
Dazu stehen wir in engem Austausch mit internen und externen Partnern aus Wissenschaft, Industrie und Streitkräften. Der Schwerpunkt in diesem Jahr liegt auf Operational Exercises (OPEXe). Ziel ist es, mithilfe zukunftsrelevanter Technologien und Innovationen die Einsatz- und Leistungsfähigkeit der Marine nachhaltig zu stärken.

Materna Information & Communications SE — S52

Materna entwickelt und stellt professionelle IT-Lösungen bereit, die den Bereich Defence bei der Erfüllung ihrer Pflichten und Aufgaben im In- sowie Ausland verlässlich unterstützen und in die Zukunft der digitalen Souveränität begleitet. Zu den intelligenten IT-Lösungen zur Unterstützung des Einsatzes gehören dynamisch-operative Lagebilder, Military Logistics, Military Mobility, Sanität und Software Defined Defence. Zu den digitale Enablern gehören Prozess- und IT-Service-Management, Architekturmanagement Defence, KI-gestützte Datenanalyse, digitale Infrastruktur, ultramobiles Arbeiten (VS-NfD) und die digitale Verwaltung der Bundeswehr. Im Umfeld Schutz und Resilienz fokussieren wir auf Cyber Security, KRITIS, Zivil- und Bevölkerungsschutz sowie Digitale Souveränität.

Mittler Report Verlag GmbH R13

Der Mittler Report Verlag ist ein führender Fachverlag für Sicherheitspolitik, Streitkräfte, Wehrtechnik und Rüstung. Das Portfolio umfasst Zeitschriften, Broschüren, Informationsdienste und Fachtagungen. Dazu zählen die in Zusammenarbeit mit dem Bundesministerium der Verteidigung herausgegebene Monatszeitschrift „Europäische Sicherheit & Technik“ in Verbindung mit dem vielbeachteten Online-Auftritt „esut.de“, der Hardthöhenkurier, als Magazin aus der Bundeswehr und für die Bundeswehr, die internationale Fachzeitschrift „European Security & Defence“, die Fachzeitschrift „MarineForum“, die Broschürenreihe „Wehrtechnischer Report“, der Newsletter „Wehrwirtschaft“ und die Online-Plattform „soldat-und-technik.de“.
www.mittler-report.de

ML Eingabesysteme GmbH B01b

An unserem Standort in Sinsheim fertigen wir mit ca. 60 Mitarbeiterinnen und Mitarbeitern qualitativ hochwertige und individuelle Eingabesysteme.
Haben Sie Bedarf an beleuchteten Folientastaturen, an kapazitiven oder resistiven Touchlösungen, an oberflächenbehandelten Fronten, an edel bedrucktem Glas oder einer Kombination aus anderen technischen Modulen? Dann sind wir Ihr Ansprechpartner für die Umsetzung und Entwicklung Ihrer Ideen und Produkte! Wir freuen uns auf ein persönliches Gespräch mit Ihnen! Ihr Team der ML Eingabesysteme GmbH

Narda Safety Test Solutions GmbH F14

Tactical radio communications surveillance / reconnaissance and emission control in battlefield, border control scenarios and intelligence applications require lightweight and portable Radio Direction Finding equipment. This allows also covert operation if necessary. NARDA is a market leader in electromagnetic spectrum analysis. NARDA designs wrist controlled, handheld, man portable and vehicle integrated Radio DF equipment. Our AOA / TDOA hybrid technologies are using „Made In Germany“ High Dynamic Range (HDR) SignalShark receivers and NARDA's unique Automatic Direction Finding Antenna (ADFA). NARDA equipment is exempted from time consuming export control procedures and can be used highly effective also in autonomous Outdoor Remote Monitoring stations.

ND SATCOM GmbH S43

ND SATCOM ist ein führender Anbieter von Satellitenkommunikationslösungen für sicherheitskritische und militärische Anwendungen. Unsere Technologien ermöglichen zuverlässige, flexible und hochverfügbare Kommunikationsnetze für jede Mission. Mit der SKYWAN 7X stellt ND SATCOM die nächste Generation der bekannten SKYWAN Technologie vor. Entwickelt für militärische Einsatzszenarien mit anspruchsvollsten Bedingungen, zertifiziert nach AECTP-Standards wird robuste Hardware mit höchster Cybersicherheit kombiniert.
Die intelligente Steuerung MeshIQ. sorgt für maximale Leistung für jede Topologie und jedes Netzwerkdesign. Höchste Verfügbarkeit durch einen selbstoptimierenden und adaptiven Durchsatz. Besuchen Sie uns an unserem Stand S43 und erfahren Sie mehr über die Vorteile der SKYWAN 7X.

NEOSAT GmbH S74

NEOSAT entwickelt wegweisende Übertragungstechnologien für Satellitenkommunikation. Mit UCSS hat NEOSAT eine Wellenform entwickelt, die im Segment Military Internet-of-Things - wie z.B. Blue Force Tracking - neue Standards vor allem im Bezug auf Detektierbarkeit und Störfestigkeit setzt. Wir ermöglichen eine jederzeit verfügbare, weltweite Verbindung mit autonomen Kleinstsendern über LEO- und GEO-Satelliten. Durch die Nutzung vorhandener geostationärer Satelliten erlaubt UCSS hoheitlichen Bedarfsträgern den autarken Betrieb eigener IoT Lösungen. Neben Hard- und Software für SATCOM IoT, bietet NEOSAT auch Schnittstellen für die Anbindung von nachfolgenden Systemen (Lagesysteme), sowie Lösungen für die Vernetzung von Kleinsatelliten bzw. Satellitenkonstellationen.

NewTec GmbH P32

NewTec ist ein führender Spezialist für die Entwicklung von Elektronik- und Softwaresystemen mit besonderem Fokus auf funktionaler Sicherheit (Safety) und Informationssicherheit (Embedded Security). In den Bereichen Automotive, Industrie, Medizintechnik, Avionik, Defense und Railway bietet das Unternehmen umfassende Leistungen vom Konzept über Elektronik- und Softwareentwicklung sowie Testing bis zur Unterstützung bei Zulassung und Betrieb. Verschiedene sofort einsatzfähige Plattformen von NewTec ermöglichen zudem Herstellern und Entwicklern einen schnelleren Produktlaunch sicherer Systeme. Darüber hinaus unterstützt NewTec seine Kunden mit Technologieberatung und Trainings sowie bei der Integration von KI-Technologie in sicherheitsgerichtete Systeme (Safe AI).

Nokia Solutions and Networks GmbH & Co. KG S05

Nokia Defense delivers cutting-edge communication solutions that provide a decisive advantage for armed forces. With secure, resilient, and high-performance networks, we support defense organizations in gaining information superiority, making rapid decisions, and securing their operations – even in the most challenging environments. Our end-to-end technologies, including quantum-safe networks and tactical communication solutions, enable seamless collaboration across land, air, sea, cyber, and space domains. Trust Nokia to empower your missions and shape the future of defense. Learn more: https://www.nokia.com/industries/defense/.

NTT DATA S15

NTT DATA ermöglicht Verteidigungsorganisationen, Innovation zu beschleunigen und kritische Assets zu sichern. Als strategischer Partner transformieren wir Defense Engineering und modernisieren resiliente Infrastruktursysteme. Wir steigern Produktionseffizienz mit AI und Machine Learning, nutzen Digital Twins zur Echtzeit-Simulation und modernisieren Legacy-Systeme durch 5G- und IoT-Integration für Smart Manufacturing und Smart Military Bases. Software-defined Infrastructure schafft selbstheilende Infrastrukturen mit Cybersecurity. Unsere Europa-basierten Private Clouds gewährleisten Datensouveränität und Speicherung klassifizierter Daten. Mit über 30 Jahren Cybersecurity-Erfahrung und als Leader im Everest Group 5G PEAK Matrix 2025 liefern wir zukunftssichere Lösungen.

NVIDIA GmbH — R48 & S18

NVIDIA ist der Architekt der vierten industriellen Revolution und liefert die Basis für KI-zentrierte Rechenzentren. Über die NVIDIA Jetson-Plattform ermöglicht das Unternehmen hochperformante unbemannte Systeme, die mittels Edge-Computing in Echtzeit navigieren. Ein Fokus liegt auf der Absicherung kritischer Infrastrukturen: KI-gestützte Netzwerkeinheiten (DPUs) integrieren Cybersecurity direkt in die Hardware, um Datenströme in Zero-Trust-Umgebungen zu schützen. Mit physikalisch exakten digitalen Zwillingen schafft NVIDIA zudem die Grundlage, um autonome Systeme sicher zu trainieren und industrielle Prozesse datenzentriert zu optimieren.

ODM GmbH — F28

Wenn es darauf ankommt, zählt Technik ohne Kompromisse: ODM steht für robuste, missionskritische Systeme in Kommunikation, Aufklärung und Einsatzlogistik – für Behörden und Spezialkräfte. Made in Germany.
Portfolio: Kommunikation: IR33-Headset für Schutz bei Impuls- und Dauerlärm (auch niederfrequent) sowie robuste, modular anschließbare Komponenten. Einsatzlogistik: CROW-Drohnenlösungen für Transport, Versorgung und Aufklärung. Passive Aufklärung: Paradect zur verdeckten Luftraumüberwachung (Detektion und Ortung ohne eigene Emissionen). Human Performance: KARIBUX kombiniert Ganganalyse per Sensorsohlen mit individuell angepassten Aktivsohlen, gleicht Fehlstellungen aus und reduziert Schmerzen für leistungsfähige Einsatzkräfte.

Octave — S14

Octave (vormals Hexagon) ist ein global führender Anbieter für das Verteidigungs- und Nachrichtenwesen. Auf der AFCEA Fachausstellung präsentiert Octave innovative Produkte zur Erfassung, Verarbeitung, Analyse und Simulation digitaler Informationen. Das Spektrum umfasst Geoinformationssysteme, mobile Mapping, Sensordatenverarbeitung, Angebote zur Visualisierung und Lageerfassung in Echtzeit sowie KRITIS-Lösungen. Diese Technologien verbessern die situative Wahrnehmung, verwandeln die Komplexität des Einsatzgebiets in klare, umsetzbare Informationen und optimieren so die Planung und Durchführung von Einsätzen. Mit den digitalen Produkten von Octave erhalten Sie die erforderlichen Einblicke, um schneller handeln, Risiken reduzieren und mit hoher Präzision führen zu können. www.octave.com

OHB SE — F20

Die OHB SE ist einer der führenden Anbieter von Raumfahrtsystemen in Europa. Mit der Expertise von mehr als 3.500 hochqualifizierten Mitarbeitenden in Europa und Übersee ist der Konzern hervorragend im internationalen Wettbewerb positioniert und hat sich als verlässlicher Partner für staatliche Institutionen und private Unternehmen etabliert.
Mit den drei Geschäftsbereichen Space Systems, Access to Space und Digital bietet OHB Raumfahrttechnologie aus einer Hand – von der Entwicklung kompletter Satellitensysteme über die Fertigung von Komponenten für die Luft- und Raumfahrt bis hin zu Bodeninfrastruktur, Missionsbetrieb und Nutzbarmachung von Satellitendaten für vielfältige Anwendungen. We.Create.Space.

Ihr Systemhaus für die Dimension Raum.

We. Create. Space.

OnTime Networks AS P35

OnTime Networks liefert robuste, leistungsstarke Netzwerk- und Timinglösungen, die für missionskritische Systeme entwickelt wurden. Unsere Ethernet-Switches, Router, Missionscomputer sowie Zeitserver und Synchronisierungslösungenermöglichen deterministische Kommunikation und präzise Synchronisation durch Technologien wie IEEE 1588 und Time-Sensitive Networking (TSN). Alle Produkte werden in Norwegen entwickelt und hergestellt, was außergewöhnliche Qualität, Zuverlässigkeit und langfristige Verfügbarkeit gewährleistet. Seit über 25 Jahren ist OnTime Networks ein verlässlicher Partner führender globaler Unternehmen und unterstützt die anspruchsvollsten Verteidigungs- und Luftfahrtprogramme weltweit.

PEC project engineers & consultants GmbH P06

Die PEC Project Engineers & Consultants GmbH unterstützt Sie dabei, komplexe IT- und Projektvorhaben sicher zu steuern und wirksam umzusetzen. Mit unserer Expertise in IT-Services, Governance, Risk & Compliance Services sowie Produkt- und Projektmanagement schaffen wir für unsere Kund:innen Strukturen, Transparenz und messbaren Fortschritt. So helfen wir Organisationen dabei, Anforderungen belastbar umzusetzen und sich zukunftsfähig aufzustellen, insbesondere in anspruchsvollen und regulierten Umfeldern. Für AFCEA-Besucher:innen besonders relevant sind unsere Leistungen in MIL-Project Management, MIL-IT Project Management sowie Governance, Risk & Compliance Services. Besuchen Sie uns an unserem Stand. Wir freuen uns auf den persönlichen Austausch.

Opternus GmbH W10

Opternus ist deutscher Marktführer in der Glasfaser-Einblas-, -Spleiß- und -Messtechnik für den Glasfaserausbau sowie für Anwendungen in Forschung, Fertigung, Fahrzeug- und Flugzeugbau und Datacentern. Auch Lösungen für den Sicherheits-/militärischen und Harsh-Bereich bilden einen – immer wichtigeren – Teil unseres Portfolios.
Wir begleiten unsere Kunden von der Idee bis zur Umsetzung mit den passenden Glasfaserbearbeitungsgeräten, Prüf- und Messmitteln. Neben individuellen Glasfaserlösungen bieten wir Expertenberatung, umfassenden Service und Support sowie ein breites Spektrum an Anwenderschulungen. Besuchen Sie uns am Stand W10, unserem gemeinsamen Stand mit JOWO – Systemtechnik, und entdecken Sie die Spleiß- und hochauflösende Messtechnik unserer Partner Fujikura, EXFO und Luciol!

Peli Products Germany GmbH S02

Peli Products is the global leader in design and manufacture of both advanced portable lighting systems and high-performance case solutions including protective cases and containers for security equipment, weapons and ammunition.
With over 500 standard sizes as well as bespoke case solutions, Peli cases provide the highest quality protection for any equipment: from critical high-tech equipment and firearms to rescue operations equipment. Our extensive portfolio of transport cases is complemented by robust mobile military products, like our portable 19-inch rackmount cases and field desks. Peli cases are virtually indestructible, designed to meet global military packaging standards and are watertight, heat- and impact-resistant. Peli cases have been tested and proven in the field since 1976

P3 Group Q05

P3 ist ein deutsches, inhabergeführtes Technologieberatungs- und Softwareentwicklungsunternehmen mit über drei Jahrzehnten Erfahrung und einer globalen Präsenz auf allen Kontinenten. Wir unterstützen Unternehmen und staatliche Institutionen im Verteidigungs- und öffentlichen Sektor mit einem breiten Spektrum an spezialisierten Leistungen, darunter:

- Individuelle Softwareentwicklung auch für hochkritische Anwendungen
- App-Store-Lösungen für alle Anwendungsfälle
- CI/CD-Pipelines für effiziente, sichere Entwicklungsprozesse
- Skalierung von Produktion und Entwicklung
- Drohnenkompetenz in Luft- und Bodenanwendungen
- Umfassendes Testing für höchste Qualität und Zuverlässigkeit
- Cyber Security für den Schutz sensibler Systeme und Daten
- Funktionale Sicherheit & System Safety

Pexip Germany GmbH R22

Missionskritische Videokommunikation mit Pexip: Souverän, resilient, interoperabel - Pexip ist ein börsennotierter europäischer Hersteller von Videokonferenzlösungen mit Hauptsitz in Oslo. Die Pexip Videokommunikationsplattform ermöglicht eine nahtlose Kommunikation über verschiedene Technologieplattformen unter Berücksichtigung höchster Sicherheitsanforderungen:

- Souveränität: Self-hosted und air-gapped für vollständige Daten- und Betriebssouveränität
- Resilienz: Höchste Zuverlässigkeit und flexible Integration in Zero-Trust-Umgebungen
- Interoperabilität: Nahtlose Videokommunikation über verschiedenste Technologieplattformen, auch bei Satellitenverbindungen.

Erfahren Sie hier mehr:
www.pexip.com; Kontakt: Dr. Dirk Fischer, Country Manager DACH, contact-dach@pexip.com

Paradigm P02

Paradigm makes the world's most advanced satcom, simple. Our range of secure, rapid deploy, low-SWaP terminals are field-proven by military, special forces, government, intelligence agencies and NGOs. With all terminals powered by the PIM®, everything needed for communication is managed through a simple user interface.
Certified for use on all major satellite networks, the PIM can operate as part of Paradigm's own VSAT range or be integrated across existing terminals and antennas.

PLATH GmbH & Co KG F18

PLATH ist ein international tätiger Anbieter von integrierten Systemen zur datenbasierten Krisenfrüherkennung. Das innovative Portfolio deckt den gesamten Aufklärungszyklus ab und hat sich weltweit in strategischen und taktischen Operationen bewährt. Als familiengeführtes Unternehmen mit 70 Jahren Branchen-Erfahrung unterstützt PLATH seine Kunden bei der Erfüllung ihres Sicherheitsauftrags – mit dem Ziel, die Welt zu einem sichereren Ort zu machen.
PLATH S & I operiert als vollständig neutraler Systemintegrator unter dem Dach der PLATH Group eigenständig am Markt.

ProCase GmbH — R23

HIGH PERFORMANCE TRANSPORT CASES
ProCase wurde 1987 gegründet. Als Markenhersteller von Flightcases ist ProCase ein europaweit tätiges, mittelständisches Unternehmen in der Verpackungs-Branche. Mehr als 10.000 Flightcases und Koffer verlassen pro Jahr unter der Marke ProCase die Produktion. Zu den Kunden zählen Unternehmen wie Bose, ZDF, SWR, Siemens, Carl Zeiss, Audi und Mercedes. Hohe Flexibilität und Zuverlässigkeit, kompetente und motivierte Mitarbeiter sowie die Qualifizierung des eigenen Nachwuchses zählen - neben unseren innovativen und hochwertigen Produkten - zu den Erfolgsfaktoren von ProCase. Ein zertifiziertes Qualitätsmanagementsystem nach ISO 9001 bestätigt unseren hohen Anspruch. Lassen auch Sie sich begeistern von den ProCase Produkten und unserem Service!

promegis Gesellschaft für Geoinformationssysteme mbH — S13

Als Spezialist für Geoinformatik, Geoinformationssysteme, Bildverarbeitung, Bildauswertung, Softwareentwicklung und IT-Servicedienstleistungen entwickelt unser Unternehmen Anwendungen und fachspezifische Systemlösungen für die Bereiche der öffentlichen Verwaltung, der Behörden und Organisationen mit Sicherheitsaufgaben (BOS), des militärischen Nachrichtenwesens (MilNW) und der militärischen Aufklärung sowie der Energie- und Versorgungswirtschaft. Darüber hinaus unterstützen wir unsere Kunden bei der Umsetzung umfangreicher IT-Projekte.
Die promegis setzt auf innovative und zukunftssichere Lösungen und nutzt moderne Technologien wie Künstliche Intelligenz zur Analyse und Auswertung großer Daten- und Bilddatenbestände sowie zur Realisierung komplexer, integrationsfähiger Systemlösungen.

PROSTEP Gruppe — R16

Die PROSTEP Gruppe ist der führende unabhängige Anbieter für Beratung und Software rund um PLM und ALM. Mit über 30 Jahren Erfahrung unterstützen wir Unternehmen beim Aufbau von Enterprise Architecture Management und digitaler Durchgängigkeit. Im Sinne der DoD Digital Engineering Strategy (DODI 5000.97) entwickeln und implementieren wir einen „Digital Thread“, der Informationen entlang des Systems-Engineering-V-Modells über alle Lebenszyklusphasen hinweg verknüpft und Datenintegrität sicherstellt.
Gemeinsam mit unseren Kunden entwickeln wir PLM/ALM-Strategien, führen digitale Zwillinge ein und stärken so Innovationskraft und Wettbewerbsfähigkeit. Internationale Joint Ventures und Unternehmenskooperationen beraten wir bei der Erarbeitung Ihrer PLM-Strategie.

Pure Storage GmbH — B10

Datenmanagement als strategischer Vorteil und Souveränität in der KI-Ära. Daten sind das Nervensystem moderner Sicherheitsstrategien. Doch wenn Informationen in Millisekunden entscheiden, bremst veraltete Infrastruktur den Fortschritt. Wir bei Everpure haben das herkömmliche Verständnis von Speicherung hinter uns gelassen. Wir definieren Storage und Datenmanagement als eine Einheit—ein intelligentes System für missionskritische Anforderungen.
Die Everpure Platform sichert Ihre Handlungsfähigkeit durch höchste Resilienz. Wir brechen Datensilos auf und schaffen eine intuitive Umgebung, die sich automatisch aktualisiert. Dies sichert die digitale Souveränität und ermöglicht präzise Entscheidungen in Echtzeit. Everpure schafft die technologische Freiheit für Ihre Mission.

QGroup GmbH — R42

QGroup als IT-Security Hersteller/-Dienstleister überträgt mit Produkten und Services die Grundsätze militärischer IT-Sicherheit auf ihre Auftraggeber. Die QTrust-Plattform erfüllt die Voraussetzungen für Security-by-Design. Sie ermöglicht separationsfähigen Sicherheitsaufbau und integriert Sicherheitslösungen Dritter.
QGroup S1EDROP kombiniert KI-gestützte EDR-Technologie mit strikter Datenhoheit. Die Lösung erlaubt Angriffserkennung, automatisierte Reaktion und Threat Hunting in isolierten Umgebungen – ohne Abfluss von Betriebsdaten in externe Cloud-Infrastrukturen (On-Premise). Unser Portfolio umfasst eigenentwickelte Penetrationstests, Passwortaudits, Schwachstellenanalysen, Implementierung von Endgeräteschutz, Netzwerküberwachung und Systemintegritätssicherung.
www.qgroup.de

Qvest Group GmbH — A18

Qvest ist Systemintegrator für Medien-, IT- und Kommunikationsinfrastrukturen. Wir begleiten Sicherheitsbehörden und Betreiber kritischer Infrastrukturen herstellerneutral bei der Transformation von Leitstellen und Kontrollräumen. Mit Beratung, Technologie und Systemintegration schaffen wir Führungsstände, die effiziente Entscheidungsprozesse in einsatzkritischen Umgebungen sicherstellen.
AFCEA-Schwerpunkte: Leitstellen für kritische Infrastrukturen: Moderne Kontrollraumlösungen für sichere Kommunikation, integrierte Lagebilder, fundierte Entscheidungen. Mobiles Videostudio: Broadcast-Qualität aus dem Flight Case – in Minuten einsatzbereit für Ausbildung, Übungsreviews, Lagekommunikation und als mobile Leitstelle. Schon beim Reservistenverband der Bundeswehr im Einsatz.
qvest.com

rasdaman GmbH — R55

Rasdaman definiert GEOINT neu durch verteiltes Management und Auswertung von raumzeitlichen „Big Geo Data“. Es nutzt AI-Cubes™, ein disruptives Konzept für ISR und taktische Datenverfügbarkeit insbesondere im Federated Mission Networking (FMN). Zu den Alleinstellungsmerkmalen von rasdaman zählen maximale Performance und Skalierbarkeit, Datenwürfel mit KI-Integration, orts-transparente Föderation, verteilte Echtzeit-Datenfusion, nahtlose Cloud/Edge-Integration, und „Security by Design“. Volle Interoperabilität, als offizielle Referenzimplementierung, erlaubt die direkte Nutzung eines weiten Spektrums an Dritt-Clients. Eine Serie von Innovationspreisen, darunter NATO Defence Innovation Challenge und Tech Connect Award, dokumentiert den technologischen Vorsprung von rasdaman.

Raydiant RF GmbH — EL03

Raydiant RF entwickelt innovative gerichtete Antennensysteme für UAVs, Defense und New-Space. Mit maßgeschneiderten, skalierbaren Lösungen sichern unsere Kunden maximale Robustheit, Energieeffizienz und kurze Markteinführungszeiten – für zuverlässige Sensor- und Kommunikationsanwendungen der Zukunft.

RECONIQ Software GmbH — F18

RECONIQ bietet hochmoderne Software und Softwaremodule für Aufklärungssysteme. Automatisierung und Echtzeit-Datenverarbeitung sind zentrale Elemente unserer KI-gestützten Lösungen, um schnelle und fundierte Entscheidungsfindungen zu unterstützen. Dank unserer umfangreichen Expertise in der Softwareentwicklung und unserem tiefgehenden Domänenwissen gewährleisten wir nahtlose Integration und Interoperabilität und bieten unseren Kunden somit langfristige operationelle Vorteile.

Reflex Aerospace GmbH — EL03

Reflex Aerospace, ein 2021 in Deutschland gegründetes NewSpace-Startup mit Sitz in München und Berlin, bietet schnelle und sichere Kleinsatellitenlösungen, die sowohl für zivile als auch militärische Zwecke genutzt werden können. Durch die Anwendung von generativem Design, additiver Fertigung und optimierten Systemdesignprozessen beschleunigt Reflex die Lieferung von Satelliten und ermöglicht seinen Kunden blitzschnelle Innovationen.

rfe-global GmbH — P33

"The modern way to reduce cost and time to market for all of us" das ist rfe-global, ihr spezialisierter Anbieter von Mess-, Analyse- und Softwarelösungen für sicherheitskritische Kommunikationssysteme. Wir bieten Ihnen Softwarelösungen zur Analyse von Protokolldaten (TETRA&DMR) sowie zur Visualisierung und Überwachung von Netzstrukturen.

Den Bereich der Mess- und Testhardware decken wir mit Funkmessplätzen (Testlösungen für taktische Funkgeräte und PMR), Echtzeit-Spektrumanalysatoren bis 40 GHz, Radar-Signalgeneratoren (zum Testen von RWR/MWR/EW), PIM-Testern sowie handlichen und robusten HF-Messgeräten ab. Sprechen Sie uns auch gerne zu Funkinteroperabilität (PMR- / PoC-Systemen) sowie für Sonderlösungen in der proprietären Protokoll-Stack-Entwicklung oder für HF-Komponenten an.

RHEINMETALL — N01 & N09 & A20

Die börsennotierte Rheinmetall AG mit Sitz in Düsseldorf steht als integrierter Technologiekonzern für ein ebenso substanzstarkes wie international erfolgreiches Unternehmen, das mit einem innovativen Produkt- und Leistungsspektrum auf unterschiedlichen Märkten aktiv ist. Rheinmetall ist ein führendes internationales Systemhaus der Verteidigungsindustrie. Die Ausrichtung auf Nachhaltigkeit ist integraler Bestandteil der Rheinmetall-Strategie.

Durch unsere Arbeit auf unterschiedlichen Feldern übernehmen wir bei Rheinmetall Verantwortung in einer sich dramatisch verändernden Welt. Mit unseren Technologien, unseren Produkten und Systemen schaffen wir die unverzichtbare Grundlage für Frieden, Freiheit und für nachhaltige Entwicklung: Sicherheit.

Rick Location Solutions GmbH — F22

Rick Location Solutions bietet als deutscher Handelspartner internationale Lösungen im Bereich Advanced Geospatial Analytics. Die angebotenen Softwareprodukte sind bei Sicherheitsbehörden (BOS) am globalen Markt etabliert und integrieren sich medienbruchfrei in die Geoinformationssysteme (GIS) der Nato und ihrer Mitglieder. Durch die Interoperabilität mit dem bestehenden IT-Ökosystem wird die durchgängige Verfügbarkeit der Analyseergebnisse auf allen Führungsebenen sichergestellt.

Inhaltlicher Fokus sind in diesem Jahr die räumliche Analysen im elektromagnetischen Spektrum (EW) und die standardisierte Erstellung von Sicherheitskonzepten für kritisches Infrastrukturen (KRITIS) gegen Gefahren durch Drohnen (c-UAV), schultergestützte Flugabwehrwaffen (MANPADS) und direkten/indirekten Beschuss

roda computer GmbH — F05

roda computer GmbH ist ein führender Anbieter von gehärteten IT und Elektronik Lösungen im europäischen Verteidigungstechnischen Umfeld. Seit 2025 sind wir Teil der MilDef – Unternehmensgruppe. Das Produktportfolio umfasst robuste Notebooks, Tablets, Displays, mobile Serverlösungen und Steuerungsgeräte. Zusätzlich entwickelt die Unternehmensgruppe maßgeschneiderte Lösungen, die exakt auf die individuellen Anforderungen der Kunden abgestimmt werden und bieten so gemeinsame IT- Lösungen aus einer Hand.

Als Teil der schwedischen MilDef Gruppe ist roda computer ein zuverlässiger Partner für Streitkräfte, Behörden und industrielle Anwender, die auf robuste und missionsgeprüfte IT-Systeme angewiesen sind.

Rohde & Schwarz GmbH & Co. KG — F10

Rohde & Schwarz – technologisch und partnerschaftlich führend

Rohde & Schwarz ist ein weltweit führender Konzern für drahtlose, vertrauenswürdige, störfeste und sichere Kommunikation, Verschlüsselung und digitale Protokolle. Seit Jahrzehnten gestaltet das Unternehmen die taktische Kommunikationsarchitektur und deren Realisierung in Deutschland und in vielen NATO Ländern an wesentlichen Stellen mit. Besonders zu nennen ist hier das umfassende Modernisierungs- und Digitalisierungsprogramm D-LBO; die Beteiligung im transeuropäischen Interoperabilitätsprojekt ESSOR; und die Ausstattung von mehr als 40 Marinen weltweit.

rola Security Solutions GmbH — F06b

ZUSAMMENARBEIT STÄRKEN. SICHERHEIT SCHAFFEN.

Die Lagebearbeitung in militärischen Organisationen erfordert das Verdichten großer Informationsmengen aus diversen Quellen. Angesichts steigender Datenflut sind moderne Systeme unverzichtbar. Unsere Softwarelösungen bieten dynamische Lagebilder, effiziente Datenfusion, KI-gestützte Analyse, OSINT-Recherchen, biometrische Analysen und praxiserprobten Datenschutz bei nachvollziehbarer Datenhaltung – für digitale Souveränität und maximale Sicherheit.

www.rola.com

Rosenberger Hochfrequenztechnik GmbH & Co. KG R17

Rosenberger ist einer der weltweit führenden Hersteller von Verbindungslösungen in der Hochfrequenz-, Fiberoptik- und Hochvolt-Technologie. Rund 15.500 Mitarbeitende entwickeln und produzieren Steckverbinder und Kabelassemblies für Luftfahrt, Raumfahrt und militärische Anwendungen gemäß DIN EN 9100. Viele unserer Produkte sind seit Jahren erfolgreich im militärischen Einsatz. Renommierte Hersteller vertrauen auf unsere Qualität und die vollständige Rückverfolgbarkeit aller Komponenten. Zum Portfolio gehören u. a. SMP, WSMP, Mini-SMP, TNC, RPC-SP (BMA) und SMA, kundenspezifische HF- und HV-Kabelassemblies, Double-Bandpass-Filter, hermetische Steckverbinder sowie Lösungen für Fiberoptik und Test & Measurement. Militärische Komponenten sind nach MIL-PRF 39012 qualifiziert.

RUAG AG S70

RUAG ist der zukunftsorientierte Technologiepartner für internationale Streitkräfte und Sicherheitsorganisationen. Wir fokussieren uns auf Life Cycle Management, Betrieb und langfristige Verfügbarkeit militärischer Land- und Luftsysteme. Unser umfassendes Portfolio reicht von interoperablen Informations- und Kommunikationslösungen über moderne Wartungs- und Instandhaltungsleistungen bis hin zu individuellen Systemanpassungen. Mit maßgeschneiderten, durchgängigen und effizienten Gesamtlösungen sorgen wir für höchste Einsatzbereitschaft. In einem komplexen und dynamischen Umfeld sind nahtlose Integration und höchste Qualitätsstandards essenziell. Als verlässlicher Partner schaffen wir mit unseren Dienstleistungen die Voraussetzungen für erfolgreiche Missionen und Einsatzsicherheit.
ruag.de

Safran Electronics & Defense Germany GmbH Q03

Safran Electronics & Defense bietet innovative PNT-Lösungen (Positioning, Navigation, Timing), die präzise und verlässliche Daten für militärische und zivile Anwendungen liefern. Sie kombinieren modernste Trägheitsnavigationssysteme mit Satellitennavigation und ergänzenden Technologien, um auch in GPS-gestörten oder -verweigerten Umgebungen volle Einsatzfähigkeit sicherzustellen. Safran entwickelt modulare Systeme für Land-, Luft- und Seestreitkräfte, die eine robuste Lagebestimmung, Synchronisation und Missionskontinuität ermöglichen. Dank jahrzehntelanger Erfahrung, starker Integration in internationale Programme und kontinuierlicher Innovation unterstützt Safran Streitkräfte weltweit bei der sicheren Durchführung komplexer Operationen.

Sagio GmbH EL03

SAGIO ist ein AI Spin-off der Universität der Bundeswehr München und entwickelt intelligente Sensor- und Entscheidungsunterstützungssysteme für autonome Plattformen. Von anwendungsnaher Forschung bis zum Engineering modularer UAV-Sensorlösungen verbinden wir modernste AI mit realen Einsatzszenarien. Unter dem Leitsatz „AI where it matters“ entstehen skalierbare, robuste Lösungen vom Digital Twin der Einsatzumgebung bis zum Deployment heterogener Sensorik auf unbemannten Systemen.

SailPoint Technologies GmbH R15

SailPoint definiert adaptive Identitätssicherheit mit einer KI-gestützten Plattform, die Identität, Sicherheit und Datenintelligenz vereint. Durch den Schutz menschlicher und nicht-menschlicher Identitäten mit risikobewusstem Echtzeitzugriff verwandelt SailPoint Identitäten von einer Schwachstelle in einen strategischen Sicherheitsvorteil.

SAP Deutschland SE & CoKG F21

Mithilfe eines weltweiten Netzwerks aus Kunden, Partnern, Mitarbeitern und Vordenkern verbessert SAP die Abläufe in der weltweiten Wirtschaft und das Leben der Menschen. Als Marktführer für Unternehmenssoftware unterstützt die SAP Unternehmen und Organisationen jeder Größe und Branche dabei, erfolgreicher zu sein: 87% des weltweiten Handelsvolumens werden von SAP-Kunden generiert. Unsere Technologien für maschinelles Lernen, das Internet der Dinge (Internet of Things, IoT) und fortschrittliche Analysen unterstützen unsere Kunden auf ihrem Weg zum intelligenten Unternehmen. Unsere durchgängige Suite mit Anwendungen und Services ermöglicht es unseren Kunden, rentabel zu arbeiten sowie sich kontinuierlich anzupassen und vom Wettbewerb abzuheben.

Satcube AB F16

Satcube is a disruptive satellite communications company that develops game-changing terminals and data services to enable high-performance broadband – any time, quickly and cost-effectively. Our portable Satcube Ku is a highly compact & intuitive device that delivers seamless connectivity anywhere in the world, empowering people to communicate at any time.

Schönhofer Sales and Engineering GmbH S54

Die 1983 gegründete Schönhofer Sales and Engineering GmbH (SSE), seit 2022 ein Mitglied der Rohde & Schwarz Gruppe, ist Wegbereiter für fortschrittliche analytische Lösungen und hochrangige IT-Systeme mit dem Fokus auf den Sicherheits- und Verteidigungssektor. Entwickelt von einem deutschen Team aus Sicherheitsexperten, gewährleistet SSE, dass Kundensysteme den strengen Sicherheitsanforderungen entsprechen. Die vom Unternehmen entwickelte, KI-unterstützte Datenanalyseplattform wandelt multi-level Sensordaten in Lösungen zur Entscheidungsunterstützung und Cybersicherheit um. Als führendes Technologieunternehmen entwickelt, konstruiert und integriert die SSE maßgeschneiderte Lösungen, die durch wirkungsvolle Beratung, Unterstützung und Schulung ergänzt werden.

SCOTTY Group Austria GmbH — N08 & A02

SCOTTY ist ein Unternehmen, welches landmobile, maritime als auch aeronautische Kommunikationslösungen für sicherheitskritische Anwendungen realisiert. Diese Lösungen unterstützen das gemeinsame Situationsbewusstsein durch den hochzuverlässigen, nativen und multimedialen Informationsaustausch, basierend auf resilienten Draht-, Funk- und Satellitennetzen.
Weltweit vertrauen zivile und militärische Organisationen auf Technologien von SCOTTY, um jederzeit, überall und unter allen Umständen kommunizieren zu können.

Secusmart GmbH — S51

Secusmart entwickelt hochsichere mobile Kommunikationslösungen für Regierungen, Behörden und KRITIS-Unternehmen. Besonders für das BMVG und die Bundeswehr sind vertrauenswürdige, souveräne Kommunikationsplattformen entscheidend, um sensible Informationen sicher und effizient austauschen zu können. Mit SecuSUITE for Samsung Knox und SecuSUITE for iOS bietet Secusmart Lösungen für sicheres mobiles Arbeiten. Alle Lösungen verfügen über eine Einsatzerlaubnis des BSI bis zu den Geheimhaltungsstufen VS-NfD. Wie sich diese Technologien zu einer modernen, sicheren Kollaborationsplattform für Behörden und Streitkräfte weiterentwickeln, zeigt Dr. Christoph Erdmann in unserem Vortrag am 12. Mai um 14 Uhr im Raum Business I / H-1-01.
Wir freuen uns auf Ihren Besuch

secunet Security Networks AG — F19

secunet ist Deutschlands führendes Cybersecurity-Unternehmen. In einer zunehmend vernetzten Welt sorgt das Unternehmen mit der Kombination aus Produkten und Beratung für widerstandsfähige, digitale Infrastrukturen und den höchstmöglichen Schutz für Daten, Anwendungen und digitale Identitäten. secunet ist dabei spezialisiert auf Bereiche, in denen es besondere Anforderungen an die Sicherheit gibt – wie z. B. Defence, Cloud, IIoT, eGovernment und eHealth. Mit den Sicherheitslösungen von secunet können Behörden, Streitkräfte und Unternehmen höchste Sicherheitsstandards in Digitalisierungsprojekten einhalten und damit ihre digitale Transformation vorantreiben.
Über 1000 Expert*innen stärken die digitale Souveränität von Regierungen, Unternehmen und der Gesellschaft.

secuvera GmbH — P11

secuvera ist ein unabhängiger Cybersicherheitsberater und vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifizierter IT-Sicherheitsdienstleister mit über 30 Jahren Erfahrung. Seit 1988 unterstützen wir Behörden, Unternehmen und Betreiber kritischer Infrastrukturen beim Aufbau und der Prüfung wirksamer Informationssicherheit.
Im sicherheitskritischen Umfeld von Behörden und Unternehmen der Verteidigungsindustrie begleiten wir Projekte bei der Entwicklung und Bewertung von Sicherheitskonzepten nach A960/1. Darüber hinaus führen wir technische Sicherheitsprüfungen von Systemen im Rahmen von Akkreditierungsverfahren durch.

SELECTRIC Nachrichen-Systeme GmbH — S35

Die SELECTRIC Gruppe ist eines der führenden Dienstleistungs- und Serviceunternehmen im Bereich der kritischen Infrastrukturen für Funk- und Mobilfunk.
Vertrieb und Wartung von Telekommunikationssystemen jeglicher Größenordnung und Anwendung sind unsere Spezialität, und für Entwicklungen im Bereich der mobilen Kommunikation bieten wir Ihnen richtungsweisende Dienstleistungs- und Servicekonzepte an. Besonders bei Spezialzubehör mit oftmals beratungsintensiven Anwendungsfällen finden Sie bei uns professionelle Lösungen.
Mehr Informationen: SELECTRIC.DE

Sepura Deutschland GmbH — S35

Sepura ist ein global führender Anbieter für digitale Funkgeräte Lösungen, ergänzender Zubehörprodukte, Applikationen sowie der zum Support notwendigen Hard- und Softwarewerkzeuge.
Im Zentrum britischer Hightech-Schmieden, in Cambridge beheimatet, ist Sepura weltweit ein verlässlicher Partner und Anbieter professioneller Funkgeräte für Nutzer aus den Bereichen öffentliche Sicherheit, Industrie und Gewerbe. Als ein weltweit anerkanntes Unternehmen konstruiert, entwickelt und liefert Sepura innovative Lösungen für einsatzkritische und sicherheitsrelevante Anwendungen.

SES SPACE & DEFENSE — B11

SES bietet weltweit integrierte End-to-End-Satellitenlösungen für kommerzielle Kunden, Regierungsbehörden und militärische Anwender. Grundlage dafür sind eine Flotte von über 120 Satelliten in verschiedenen Umlaufbahnen (GEO und MEO), ein leistungsfähiges Multi-Operator-Netzwerk sowie eine globale terrestrische Infrastruktur. Mit unseren integrierten Satelliten- und Technologielösungen unterstützen wir den nachhaltigen Erfolg anspruchsvoller Missionen.
Besuchen Sie uns am Stand [B11] und erfahren Sie, wie wir auch Ihre Mission zum Erfolg führen.

Siemens Industry Software GmbH — G04

Siemens Digital Industries Software unterstützt Unternehmen jeder Größe bei der digitalen Transformation mit Software, Hardware und Services der Siemens Xcelerator Business Platform. Die Software von Siemens und der umfassende digitale Zwilling ermöglichen es Unternehmen, ihre Entwurfs-, Konstruktions- und Fertigungsprozesse zu optimieren, um die Ideen von heute in nachhaltige Produkte der Zukunft zu verwandeln. Vom Chip bis zum Gesamtsystem, vom Produkt bis zum Prozess, über alle Branchen hinweg. Siemens Digital Industries Software– Accelerating transformation.

Skylance GmbH — EL04

Die Firma Skylance entwickelt einen der kleinsten Lenkflugkörper der Welt, den DroneHammer, zur Abwehr von Drohnen der Klasse 1 (u.A. FPV). Dieser misst grade einmal 50cm und fliegt bis zu 500km/h schnell, bei einer Reichweite bis zu 2km. Die Skylance GmbH, gegründet 2025 von Philipp Bohne, Dr. Tobias de Taille und Dr. Olaf Wollersheim beschäftigt mittlerweile 15 Mitarbeiter und hat ihren Hauptsitz in Hürth, bei Köln und eine Außenstelle in Oldenburg.

Skyline Europe GmbH — S85 & S86

Skyline Europe GmbH mit Sitz in Diessen bei München ist eine Niederlassung der Firma Skyline Software Systems Inc. mit Sitz in Herndon, Virginia, USA. Als führender Anbieter von 3D-Erdvisualisierungssoftware und -diensten bietet Skyline eine umfassende Plattform von Anwendungen, Tools und Services, die die Erstellung und Verbreitung interaktiver, fotorealistischer 3D-Umgebungen ermöglichen. Die Produkte von Skyline haben sich im Verteidigungsmarkt bewährt. Aktueller Themenschwerpunkt in der Ausstellung ist das Mapping mit Drohnen (PhotoMesh Drone).

soffico GmbH — R43

Die soffico GmbH ist Hersteller von Standardsoftware für KRITIS und sicherheitsrelevante Branchen. Mit der Low-Code-Plattform Orchestra gewährleisten wir als commercial off the shelf-Lösung die sichere und redundante Bereitstellung von Daten, interoperabel in heterogenen zivilen, dual-use und militärischen Umgebungen, auch auf taktischer Ebene. Orchestra erfüllt höchste NATO-Standards, ermöglicht unterbrechungsfreie Datenflüsse und unterstützt KI-gestützte Analysen, effiziente Lieferkettensteuerung und präzise Einsatzentscheidungen.

Solidplex GmbH — R23

SINORA ist eine Marke der Solidplex GmbH mit Hauptsitz in Miltenberg, im bayerischen Regierungsbezirk Unterfranken. Bereits seit 1990 beschäftigt sich unser Unternehmen mit der Herstellung von Transportkoffern für sensibles Equipment der unterschiedlichsten Branchen. Mit unserer langjährigen Erfahrung, Kompetenz und Kreativität in der Kunststofftechnik erschaffen wir maßhaltige Schutz- und Transportkoffer im Spritzgussverfahren aus robustem Polypropylen (PP). SINORA Schutzkoffer stehen für erstklassige Qualität und maximale Sicherheit. Unsere Koffer sind nach verschiedenen Umwelttests zertifiziert, wie beispielsweise nach IP67 oder der Militärnorm MIL-STD-810.

Sophos Technology GmbH S62

Sophos ist ein weltweit führender Next-Gen-Cybersecurity-Anbieter und schützt über 500.000 Organisationen und Millionen von Kunden in mehr als 150 Ländern vor komplexen Cyberbedrohungen. Mit Threat Intelligence, KI und Machine Learning aus den SophosLabs und SophosAI bietet Sophos ein breites Portfolio modernster Produkte und Services. Diese schützen Benutzer, Netzwerke und Endpoints zuverlässig vor Malware, Exploits, Phishing und anderen Cyberangriffen. Mit Sophos Central hat Sophos eine zentrale, cloudbasierte Management-Konsole im Angebot. Sie bildet das Herzstück unseres adaptiven Cybersecurity-Ökosystems. Teil dieses Systems ist ein zentralisierter Data Lake. Er nutzt eine Vielzahl offener APIs, die Kunden, Partnern, Entwicklern und anderen Cybersecurity-Anbietern zur Verfügung stehen

SVA System Vertrieb Alexander GmbH S53

Die SVA System Vertrieb Alexander GmbH ist einer der führenden deutschen System-Integratoren. Das unternehmerische Ziel des Unternehmens ist, hochwertige IT-Produkte der jeweiligen Hersteller mit dem Projekt-Know-how und der Flexibilität von SVA zu verknüpfen, um so optimale Lösungen für die Kunden zu erzielen. Kernthemen des Unternehmens sind Datacenter-Infrastruktur – wie Speicher-, Server- und Netzwerk-Lösungen sowie Virtualisierungstechnologien – und auch Business Continuity, Digital Process Solutions und SAP. Darüber hinaus bietet SVA nicht nur Unterstützung im Betrieb der Infrastruktur durch Operational Services, sondern auch Managed Services. Mit dem Angebot zu Strategischem IT-Consulting stehen auch Experten für eine ganzheitliche und umsetzungsorientierte Beratung zur Verfügung.

Sopra Steria SE S12

Sopra Steria ist ein führender europäischer Tech-Player mit 51.000 Mitarbeitenden in fast 30 Ländern und anerkannter Expertise in den Geschäftsfeldern Consulting, Digital Services und Solutions. Die Gruppe bietet umfassende End-to-End-Lösungen, die große Unternehmen und Behörden wettbewerbs- und leistungsfähiger machen – und zwar auf Grundlage tiefgehender Expertise in einer Vielzahl von Branchen, innovativer Technologien und eines kollaborativen Ansatzes.
Sopra Steria stellt die Menschen in den Mittelpunkt seines Handelns mit dem Ziel, die Digitalisierung für seine Kunden zu nutzen, um eine positive Zukunft für alle zu gestalten. Der Konzern erzielte 2025 einen Umsatz von 5,6 Milliarden Euro.

Systerra Computer GmbH S64

Systerra Computer GmbH ist seit mehr als 20 Jahren Anbieter industrieller Computer und Netzwerklösungen, sowie von MIL_STD konformen, robusten Rechner-, Speicher- und Netzwerkplattformen. Unser Schwerpunkt liegt auf Spitzentechnologie mit hoher Verfügbarkeit in anspruchsvoller Umgebung (mobiler und stationärer Einsatz). Wir setzen dabei auf bewährte und neueste Hard- und Software-Standards.
Mit unserer Erfahrung und Expertise erstellen wir in enger Zusammenarbeit mit Kunden und Herstellern applikationsspezifische Hardware- Sonderlösungen und beraten bei der Projektierung.
Unsere Produktpartner: MPL AG, Moxa, RTD, Acromag;
Kontakt: Systerra Computer GmbH, Kreuzberger Ring 22, 65205 Wiesbaden,
Tel. 0611 / 44 88 9 – 400, E-Mail: info@systerra.de, Internet: www.systerra.de

steep GmbH S39

Zur 39. AFCEA-Fachausstellung zeigen wir Ihnen an unserem Messestand S39 im Saal New York/Genf unsere aktuellen Leistungen und Lösungen.
Wir sind ein international erfolgreiches technisches Dienstleistungsunternehmen mit mehr als 35 Standorten und rund 800 Mitarbeiterinnen und Mitarbeitern in Deutschland und Europa. Ob hochmobile Kommunikations- oder verlegbare Containerlösungen – unsere Leistungen gehen weit über die Fertigstellung hinaus: Wir liefern, in enger Abstimmung mit dem Kunden, alle erforderlichen Prozesse aus einer Hand. Bei Bedarf übernehmen wir auch Transport und Logistik, bieten Auf-, Abbau sowie Inbetriebnahme im Einsatzgebiet oder bei Übungen und führen auf Kundenwunsch maßgeschneiderte Trainings zur Einarbeitung des Bedienpersonals am System durch.
www.steep.de

tde - trans data elektronik GmbH S06

Als führender deutscher Netzwerkexperte und global erfolgreiches Unternehmen entwickelt und produziert tde – trans data elektronik GmbH seit über 30 Jahren skalierbare Verkabelungssysteme für höchste Packungsdichten. Wir entwickeln Lösungen für die vernetzte, digitalisierte Welt von morgen: hochwertig, Made in Germany und zu 100 Prozent ausfallsicher.
Unser Produktportfolio umfasst komplette Systemlösungen mit Schwerpunkt Plug & Play für Highspeed-Anwendungen in den Bereichen: Datacom, Telecom, Industry, Medical und Defence. Ein Highlight, welches wir auf der 39. AFCEA Fachausstellung präsentieren, ist das innovative tMA System, unser high-density tde Verkabelungssystem für mobile Applikationen, gewichtsoptimiert und bestens geeignet für den mobilen Einsatz in Harsh Environments.

Stellar PCS GmbH F14

Stellar PCS steht seit über 25Jahren für zuverlässige und sichere Kommunikation weltweit. Unsere Teleports in Deutschland, Zypern und Fidschi verbinden Menschen und machen Forschung im All möglich, unsere Kunden profitieren von einem globalen terrestrischen Transportnetzwerk. In der deutschen Satelliten-Mission Heinrich Hertz spielen wir eine zentrale Rolle in der Satellitensteuerung und betreiben auf unserem Gelände ebenfalls eine Antenne zur Betreuung technischer Experimente.
Die Heinrich-Hertz-Satellitenmission wird vom DLR im Auftrag des BMWK und mit Beteiligung des Bundesministeriums der Verteidigung (BMVg) durchgeführt. Zusammen mit der schwedischen Firma Ovzon bietet Stellar optimierte Lösungen für verschiedene Einsatzfälle im Bereich Katastrophenschutz, Polizei, Militär.

tecnotron elektronik gmbh P34

tecnotron elektronik gmbh - unabhängiger zertifizierter Elektronik-Komplettdienstleister (E^2MS) für Hightech-Projekte. Wir entwickeln und fertigen komplexe Elektronikprojekte für Verteidigung, Luft- und Raumfahrt, Medizin und Industrie – für anspruchsvolle Anforderungen und extreme Einsatzbedingungen.
Unsere hochqualifizierten, gut verzahnten Fachabteilungen und zertifizierten Prozesse (EN 9100, ISO 13485, ISO 14001) stehen für Qualität und Zuverlässigkeit. Ob Entwicklung, PCB-Layout und Fertigung elektronischer Baugruppen, Geräte und Systeme, wir erarbeiten intelligente und individuelle Gesamtlösungen – von der Idee bis zur Serienfertigung. Familiengeführt, seit über 47 Jahren sicher im Markt etabliert. Qualität „Made in Germany“, alles aus einer Hand, von unserem Standort am Bodensee.

TEKSAM GMBH — W03

Die Teksam GmbH ist die deutsche Vertriebstochter des belgischen Herstellers Teksam Company NV und bearbeitet den D-A-CH Bereich. Unter den Markennamen Teklite, Clark Masts und TekMast bieten wir eine große Auswahl an Beleuchtungsmasten und pneumatischen sowie mechanischen Teleskopmasten für eine Höhe von bis zu 50m und einer max. Kopflast von 300kg an.
Kundenbezogene Anforderungen umzusetzen, sowie eine ständige Weiterentwicklung unserer Produkte, sind unsere Stärke.

TQ Systems GmbH — B22

TQ-Systems mit Hauptsitz in Seefeld bei München ist ein Lösungsanbieter für Elektronik mit starken Wurzeln als E²MS-Dienstleister. Zum Kundenstamm des inhabergeführten Unternehmens gehören nationale wie internationale Firmen aus Industrie, Medizintechnik, Sicherheit und Verteidigung, Luft- und Raumfahrt, Energiemanagement u.v.m. Seit mehr als 30 Jahren bietet TQ in jeder Phase des Produktlebenszyklus' kompetente Unterstützung in den Bereichen Hardware, Software und Mechanik bei Baugruppen, Geräten und Systemen. Antriebs- und Automatisierungslösungen sowie Mikrocontrollermodule ergänzen das Portfolio. Nah am Kunden mit 5 Produktionsstandorten allein in Bayern. Zertifiziert und mehrfach ausgezeichnet.

Thales Deutschland — S23

Wir unterstützen Streitkräfte zuverlässig gegenüber Bedrohungen jeder Art und helfen ihnen, taktische Überlegenheit und strategische Unabhängigkeit zu erreichen und diese auch zu behaupten.In komplexen militärischen Szenarien müssen weitreichende Entscheidungen in kürzester Zeit richtig getroffen werden. Thales unterstützt dies mit innovativen und integrierten Lösungen für Überwachung, Aufklärung und Einsatz. Unser umfassendes internationales Portfolio bietet die größtmögliche Bandbreite für jede Mission in den Wirkdimensionen Land, See, Luft und Cyber. Von intelligenten Sensoren, über moderne Verteidigungssysteme für das Gefecht im Verbund, bis hin zur Anbindung und Ausrüstung von Soldaten auf dem digitalen Gefechtsfeld sorgen unsere Systeme für Informationsüberlegenheit.

Treo - Labor für Umweltsimulation GmbH — S55

Testing? Treo. Umwelteinflüsse wie Hitze, Kälte oder Feuchtigkeit, Vibrationen oder elektromagnetische Strahlung – Produkte und Komponenten sind verschiedenen Belastungen ausgesetzt. Treo untersucht, ob sie diesen standhalten.
Als akkreditiertes Prüflabor unterstützen wir unsere Kunden vom Umsetzen konkreter Prüfspezifikationen über entwicklungsbegleitende Tests bis zu akkreditierten Zulassungsprüfungen. Unser Service umfasst die Bereiche Umweltsimulation, Materialprüfung sowie elektromagnetische Verträglichkeit (EMV). Expertise haben wir vor allem in Verteidigung, Luftfahrt, Schiffbau und Bahn. Für militärische Produkte bieten wir nahezu alle benötigten Prüfungen aus einer Hand an. Wir prüfen z. B. gemäß MIL-STD 810, MIL-STD 461 und diversen AECTP- und VG Normen.

Twentyfour Industries GmbH — EL04

Twentyfour Industries designs, manufactures, and deploys drones for European and allied partners — cost-effectively, at scale, and with end-to-end operational support. Amongst others, we offer a market-available, European-made 10-inch quadcopter for training and everyday operations. Its multi-mission payload concept and rugged, repeatable design make it ideal for cost-effective operation at scale, enabling realistic unit-level training and frequent field use. The platform is already in use across multiple European countries, supporting civil operators and military units alike.

Veeam Software GmbH — S62

Souveräne Datenverfügbarkeit für eine vernetzte Verteidigung - Veeam ist führender Anbieter für Daten- und KI-Sicherheit. Das Unternehmen bietet umfassende Einblicke in Daten, Identitäten und KI-Modelle, steuert den Zugriff, automatisiert Datenschutz und Compliance und schützt somit kritische Infrastrukturen vor Bedrohungen wie Ransomware, Katastrophen und KI-Fehlern. Über 550.000 Kunden weltweit, darunter 82 % der Fortune 500 schützen ihre Daten mit Veeam.
Mehr unter www.veeam.com.
Ihr Ansprechpartner: Gerd-Uwe Sachse, Enterprise Account Manager, gerd-uwe.sachse@veeam.com

UniBw München — N03

Das Forschungszentrum SPACE (FZ SPACE) an der Universität der Bundeswehr München deckt Kerngebiete der Raumfahrt wie Satelliten- und Raketentechnologie oder die Erforschung des Sonnensystems und Weltalls ab, aber auch Anwendungen auf der Erde wie Kommunikation, Navigation und Erdbeobachtung gehören zu seinen Kompetenzen. Die Mitglieder vom FZ SPACE arbeiten fakultätsübergreifend zusammen und bündeln ihre Expertise, um interdisziplinär Lösungen für komplexe Problemstellungen zu finden. Gemeinsam gestalten sie Innovationen und treiben das Thema Raumfahrt voran.

Veteranenbüro der Bundeswehr — A40

Das Veteranenbüro der Bundeswehr mit Sitz in Berlin ist die zentrale Anlauf-, Beratungs-, Informations- und Vermittlungsstelle für Veteraninnen und Veteranen. Wir sind die Ansprechstelle für Verbände und Organisationen, die sich in der Veteranenarbeit der Bundeswehr engagieren oder engagieren möchten. Wir unterstützen den Beauftragten für Veteranenangelegenheiten der Bundeswehr, bauen das Netzwerk zu militärischen und zivilen Stellen auf und pflegen es. Wir informieren die Öffentlichkeit über die Veteranenarbeit der Bundeswehr.
Das Veteranenbüro ist von Montag bis Donnerstag von 08:00 Uhr – 16:00 Uhr und Freitag von 08:00 Uhr – 12:00 Uhr telefonisch unter +49 160 90 363 527 oder unter Veteranenbuero@Bundeswehr.org erreichbar.

UNITE+ Consulting GmbH — P03

Wir designen Visionen und entwickeln daraus nachhaltige Web- und IT-Erlebnisse. UNITE+ ist ein zuverlässiger und erfahrener Partner für seine Kunden in unterschiedlichsten Branchen – insbesondere im öffentlichen Sektor. Gemeinsam mit unseren Kunden analysieren wir Prozesse, entwickeln tragfähige Konzepte und setzen diese von der Idee bis zum stabilen Produktivbetrieb um.
UNITE+ begleitet die Bundeswehr seit über 20 Jahren bei der digitalen Zukunftsgestaltung. Wir realisieren bedarfsorientierte Anwendungen basierend auf Anforderungen von Heer, Luftwaffe und Marine. Mit der Digitalisierung von Prozessen unterstützen wir die neue Dienststelle CAMOBw beim Aufbau in sicherheitsrelevanten Bereichen. So schaffen wir effiziente, sichere und zukunftsfähige Fachanwendungen mit nachhaltigem Mehrwert.

VISS UG — EL03

Viss's mission is to make endpoint security effortless, universal, and unbreakable. By delivering a plug-and-play hardware solution that cannot be bypassed by zero-days or nation-state malware, we empower governments, industries, and individuals to carry out their work without the fear of compromise.

Unterstützungskommando der Bundeswehr — R64

Der Unterstützungsbereich ist mit rund 55.000 militärischen und zivilen Angehörigen der zweitgrößte militärische Organisationsbereich der Bundeswehr. Heer, Luftwaffe, Marine sowie Cyber- und Informationsraum werden mit seinen Kernkompetenzen Logistik, Sanitätsdienst, ABC-Abwehr, Feldjägerwesen und Zivil-Militärische Zusammenarbeit unterstützt. Die bei uns im Unterstützungsbereich gebündelten Kräfte und Fähigkeiten stehen der Bundeswehr begrenzt zur Verfügung, sind aber kriegsentscheidend. Sie stärken die Einsatzfähigkeit der Streitkräfte und gewährleisten flexible Unterstützung in Frieden, Krise und Krieg. Die gesamten Unterstützungskräfte werden geführt und koordiniert durch das Unterstützungskommando der Bundeswehr in Bonn.

VITEC — W04

VITEC bietet ISR- und Situational-Awareness-Lösungen und deckt den gesamten Videoworkflow ab – von Erfassung und Encoding bis zu Streaming, Verteilung und Archivierung in militärischen und behördlichen Umgebungen. Die TOUGH-Serie liefert robuste, energieeffiziente Encoder für anspruchsvolle FMV-Einsätze. Die VSN-Serie ermöglicht missionskritische Visualisierung in Leitstellen, während EZ TV ISR eine End-to-End-Lösung für Ansicht, Aufzeichnung, Indexierung und sichere Verteilung von ISR-Videos und Metadaten bietet. VITEC verbessert Echtzeit-Lagebilder, Entscheidungsfindung und multisensorische Videofusion.

Willert Software Tools GmbH — B06a

SodiusWillert is a global software tools vendor specialized in developing powerful extensions for leading systems and software engineering tools. We help customers in highly regulated industries deliver products to market faster by integrating their engineering tools, boosting engineers' productivity, and fostering team collaboration. Our focus is on enhancing the engineering and development of large, mission-critical systems and software.
For over 30 years we are helping our customers succeed through efficient use of requirements management, system and software engineering, quality assurance, and methods and processes required for the development of advanced products, including safety-critical systems.

Zarges GmbH — W08

ZARGES steht seit über 90 Jahren für kompromisslose Qualität verbunden mit kontinuierlichen Innovationen in den Bereichen Steigen, Verpacken und Transportieren sowie Speziallösungen. Als erstes Leichtmetallbau-Unternehmen Europas ist ZARGES heute international tätig – mit rund 800 Mitarbeitern und drei Produktionsstätten in Europa.
Als Innovations- und Marktführer bietet ZARGES seinen Kunden Produkte und Services, die bei Sicherheit, Haltbarkeit und Ergonomie die Maßstäbe im Markt setzen. In ZARGES-Produkten vereinen sich die vielfältigen Vorteile des Leichtmetall-Werkstoffs Aluminium, wie hohe Stabilität bei geringem Gewicht, Korrosionsfestigkeit sowie Flexibilität im Einsatz. ZARGES hat für jeden das geeignete Produkt und bietet individuelle Lösungen an.

Xecuro GmbH — S25

Die Xecuro GmbH ist eine hundertprozentige Tochter der Bundesdruckerei Gruppe GmbH. Sie wurde im November 2021 gegründet, um neue digitale Systeme für die Verschlusssachen-Kommunikation des Bundes mit aufzubauen, zu betreiben und weiterzuentwickeln. Die Systeme reichen von verschlüsselter Telefonie- und Videokonferenz-Technologie bis zum sicheren Datenaustausch zwischen Ministerien, Behörden und Unternehmen. Xecuro betreibt dafür die Infrastruktur, betreut die Endgeräte und ist für den Service verantwortlich. Das Unternehmen soll auf rund 120 Beschäftigte wachsen. Standorte der Xecuro sind derzeit Berlin und Bonn.

Zebra Technologies Germany GmbH — S35

Zebra Technologies: Smarte Geräte für den öffentlichen Dienst.
Zebra besitzt große Expertise in Bereichen, in denen man sich Technologieausfälle nicht leisten kann, und unterstützt geschäftskritische Betriebsabläufe weltweit. In den Kernmärkten bietet Zebra führende Lösungen für die Verfolgung und Digitalisierung von Assets und Prozessen sowie für Kommunikation und Datenerfassung an. Dies sind auch Schwerpunkte für Rettungsdienste und Sicherheitsorgane. Der Begriff „Enterprise-Klasse" grenzt die Produkte und Lösungen von Zebra dabei von herkömmlicher Technologie für Endverbraucher ab. Das bedeutet mehr Sicherheit, Support, längere Lebensdauer und Serviceoptionen. Zebra besitzt ein umfangreiches Portfolio und Lösungen für Behörden und Organisationen mit Sicherheitsaufgaben.

Inserentenverzeichnis

Behörden Spiegel

Militärattachés in Deutschland – kompakt im Überblick

Verteidigungs- und Militärattachés aus über 100 Nationen sind in Deutschland vertreten. Dieses einzigartige Nachschlagewerk bietet einen umfassenden Einblick in ihre Arbeit und die sicherheitspolitischen Strukturen ihrer Länder.

- **Demografische und wirtschaftliche Kerndaten**
- **Mitgliedschaften in internationalen Bündnissen und Organisationen**
- **Kompakte Porträts der nationalen Streitkräfte**

Jetzt bestellen:

www.behoerden-spiegel.de/sonderpublikationen

BSC Berlin Security Conference

25th Congress on European Security and Defence

The Berlin Security Conference is one of the largest European security and defence policy events.

The congress and exhibition, held every autumn since 2001 in Berlin, draw participants from European and non-European countries, the European institutions, and NATO. The 25th Berlin Security Conference will take place at the Vienna House Andel's Berlin on 3-4 November 2026. The event is free of any government influence. It is not supported by public budgets and is therefore at liberty to take an objective stance.

Tuesday – Wednesday

3 – 4 November 2026

SAVE THE DATE

Vienna House Andel´s

Landsberger Allee 106, 10369 Berlin

www.euro-defence.eu

#BSC26

PARTNER LAND

LITAUEN

VORANKÜNDIGUNG

40. AFCEA Fachausstellung

25.05. – 26.05.2027

World Conference Center Bonn

www.afcea.de