AFCEA 2025

BDSV – Bundesverband der Deutschen Sicherheits- und Verteidigungsindustrie

ISBN 978-3-934401-81-5

Behörden Spiegel-Gruppe
in Zusammenarbeit mit AFCEA Bonn e.V.

.INNO
NOW YOU KNOW

ZUKUNFT BRAUCHT HERKUNFT.

Setzen Sie auf 25 Jahre Expertise im Bereich Massendatenanalyse.

SCOPE ist der hoch performante Analyse- und Knowledge Hub Made in Germany. Mit SCOPE kumulieren Sie Ihre Daten und Informationen in einem System und schaffen damit die Grundlage für Wissen, das durch effiziente Auswertung gezielt zur Einleitung konkreter Maßnahmen genutzt werden kann.

All-source Massendatenanalyse mit SCOPE: das sind 25 Jahre Domänenerfahrung für datenbasierte Entscheidungsfindung Made in Germany.

AFCEA | 27.-28.06. | Stand S34

ERPROBT.
EFFIZIENT.
PERFORMANT.

INNOSYSTEC.DE

Deutschland befindet sich in stürmischen Gewässern: 24 Stunden pro Tag, sieben Tage die Woche schlagen Cyberangriffe auf Behörden, Unternehmen und kritische Infrastrukturen wie hohe Wellen gegen den Bug unserer digitalen Sicherheit. Die nicht nur sicherheitspolitische, sondern auch technologische Zeitenwende hat das traditionelle Gefechtsfeld über Land, Luft und See hinaus erweitert – hin zu einem digitalen und „gläsernen“ Gefechtsfeld, auf dem Informationen zu strategischen Ressourcen werden.

Vizeadmiral Dr. Thomas Daum

Foto: Bundeswehr/Uj

Die Antwort auf diese neue Realität ist nicht mehr nur eine Frage der Kriegstüchtigkeit einzelner Teilstreitkräfte (TSK). Mit der Betrachtung des Cyber- und Informationsraums (CIR) als eigenständiges Gefechtsfeld und mithin der Aufwertung des bisherigen Organisationsbereiches zur Teilstreitkraft CIR setzt die Bundeswehr ein klares Signal: Deutschland muss im CIR genauso entschlossen verteidigt werden wie in den traditionellen Dimensionen. Die Raumverantwortung des Cyber- und Informationsraums ist damit klar zugewiesen. Doch die effektive Verteidigung gegen hybride Bedrohungen kann nur durch gesamtstaatliche Anstrengungen gelingen.

Die TSK CIR setzt daher auf einen übergreifenden Ansatz: Kooperationen mit Behörden, internationalen Partnern und der Wirtschaft. Vernetzung wird so zum Leuchtturm, der inmitten der stürmischen See hybrider Bedrohungen Orientierung bietet.

Doch welche Schlüsseltechnologien sind nötig, um Daten sicher, schnell und intelligent zu nutzen?

Unsere Verteidigung wird zunehmend durch Software bestimmt. Diese muss „by design“, also bei der Entwicklung der Schiffe, Flugzeuge und Panzer mitberücksichtigt werden, um bruchfreie, sichere Kommunikation in Echtzeit durch einheitliche Datenformate und standardisierte Schnittstellen auch dimensionsübergreifend zu gewährleisten.

Zudem wird Innovation bei traditionellen Einsatzverfahren durch das Zusammenwirken von Legacy-Systemen und die Einbindung in einen gemeinsamen Führungssystemverbund ermöglicht. Modulare Softwarebausteine müssen optimal aufeinander abgestimmt sein, sodass eine Systemlandschaft für alle TSK entsteht.

Daten, die durch die Vielzahl von Sensoren generiert werden, müssen dezentral an der (Sensor)quelle ausgewertet werden. So ist es möglich, die für das Überleben notwendige Geschwindigkeit der Kill-Chain zu erhöhen. Große Datenmengen werden im „rückwärtigen Raum“ in der Cloud gespeichert und so für langfristige Nutzung und Entscheidungsprozesse nutzbar gemacht.

Unterstützt werden diese Prozesse durch Künstliche Intelligenz (KI), denn diese ermöglicht die Auswertung der massiv gestiegenen Datenmengen im Bereich der Sensoren, beispielsweise bei der elektronischen Signalerfassung oder der raumgestützten abbildenden Aufklärung.

Schiffe, Panzer und Flugzeuge sind über lange Jahre im Einsatz, Umbauten und Umrüstungen auf diesen Plattformen sind stets baulich aufwändig und häufig auf die regelmäßigen Instandsetzungsphasen beschränkt. Software kann dagegen kurzfristig erweitert und auf den Systemen aktualisiert werden. Je weniger „hardware heavy“ und je mehr „software driven“ die Systeme gestaltet werden, umso mehr lassen sich auch die Vorteile von „software defined defence (SDD)“ erzielen.

Die TSK CIR ist der Treiber der Digitalisierung der Bundeswehr. Jedoch nur im Zusammenwirken von politisch-strategischer Steuerung aus dem BMVg, den Nutzerforderungen aus den TSK Heer, Luftwaffe und Marine und der Industrie als Partner wird es gelingen, die „digitale Kriegstüchtigkeit“ vollständig zu erreichen.

Die 38. AFCEA-Fachausstellung stellt hierzu eine Plattform des Austauschs von unschätzbarem Wert dar, in dem sich Experten aus verschiedenen Bereichen treffen, um gemeinsam die Routen für die digitale Zukunft der Streitkräfte zu kartieren.

Es geht nur gemeinsam.

Vizeadmiral Dr. Thomas Daum führt als Inspekteur CIR aus seinem Kommando in Bonn den Kampf in der Dimension CIR und treibt mit seiner Teilstreitkraft die Digitalisierung der Bundeswehr voran.

Impressum Sonderheft Behörden Spiegel „AFCEA 2025“ **Redaktionelle Leitung** Thomas Hönig, Behörden Spiegel, Telefon: 0228/970 970 **Herausgeber** (presserechtlich verantwortlich) Dr. Eva-Charlotte Proll, Behörden Spiegel-Gruppe **Verlegt** von der ProPress Verlagsgesellschaft mbH, Friedrich-Ebert-Allee 57, 53113 Bonn, 0228 / 970 970; Berlin, Kaskelstraße 41, 10317 Berlin, 030 / 55 74 12 0 **Anzeigen** Jennifer Großblotekamp **Herstellung** ProGov GmbH **Satz und Layout** Yonca Bilgi / ProGov GmbH **Fotos** Autoren, AFCEA Bonn e.V., BWI, Behörden Spiegel-Archiv **Druck** Köllen Druck + Verlag GmbH, Bonn **Heftpreis** 7,50 Euro

www.behoerdenspiegel.de

Die digitale Transformation umsetzen

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

Als AFCEA Bonn e.V. haben wir in diesem Jahr darauf verzichtet, uns ein neues Jahresthema zu suchen. Das ist keine Bequemlichkeit, sondern hat gute Gründe. Das vergangene Jahr haben wir unter das Motto „Zeitenwende in der nationalen Sicherheit – Resilienz durch disruptive digitale Lösungen“ gestellt. Daran orientieren wir uns auch 2025 weiter. Denn Zeitenwende ist nichts, das einmal kommt und schnell wieder geht. Der russische Angriff auf die Ukraine befindet sich seit geraumer Zeit in einer brachialen Abnutzungsphase, die Krisenregion Naher Osten ist weiterhin fragil. Verbündete wie die USA, auf die Deutschland und die NATO lange setzten, richten sich neu aus.

Armin Fleischmann Generalmajor

Bild: AFCEA

Die Zeitenwende in der nationalen Sicherheit ist eine doppelte: Sie wird sowohl durch die neue sicherheitspolitische Lage vorangetrieben als auch durch disruptive und digitale Lösungen. 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. Aufgrund dieser Vision wollen wir einen Beitrag leisten, damit Gesellschaft, Staat und Bundeswehr die notwendige Resilienz gegenüber den Bedrohungen erreichen und unsere nationale Souveränität stark genug und technologisch führend ist.

Heute sind wir auf dem Weg, die notwendigen Schritte zu gehen, die sich aus der Erkenntnis dieser doppelten Zeitenwende ergeben. Der Weg ist lang und erfordert Ausdauer. Es ist ein Marathon, den AFCEA als neutrales und nationales Netzwerk weiter begleiten will. Durch Formate wie Veranstaltungen und Nachwuchsförderung leisten wir einen relevanten Beitrag zur Modernisierung, Digitalisierung und Souveränität von Bundeswehr und Sicherheitsbehörden.

In unseren Veranstaltungen werden wir in diesem Jahr verstärkt auf die Umsetzung von Lösungen zur besseren Einsatzbereitschaft und gesellschaftlicher Resilienz schauen. Wir tun das mit unserem Jahresprogramm. Zu unseren Veranstaltungen gehört als Flaggschiff die AFCEA Fachausstellung, die Gesamtstruktur des Programms stellen wir auch in diesem Heft vor (Seite 26).

In diesem Heft betrachten wir schwerpunktmäßig, was Deutschland, die Bundeswehr und die verschiedenen Akteure bisher beim Zeitenwende-Marathon erreicht haben. Das gilt sowohl für die Beiträge des AFCEA-Vorstands als auch für die unseres Partners BDSV (ab Seite 29). Dabei betrachten wir ausgewählte Themen aus den neun Feldern, die wir für unsere IT-Community der Verteidigung und Sicherheit im vergangenen Jahr konkret benannt haben, um Wirkung für Resilienz und nationale Sicherheit zu entfalten. Es sind Frühwarnsysteme, Cybersicherheit, Krisenkommunikation, Datenmanagement, Künstliche Intelligenz (KI), Quantentechnologien, Software Defined Defence, Weltraumtechnologien und Innovationsförderung.

Brigadegeneral Rainer Beeck, AFCEA-Vorstand für Bundeswehrthemen, gibt durch den Leiter der Projektgruppe Digitalisierung aus dem Amt für Heeresentwicklung einen Einblick in die Experimentalserie Land. Die Serie ist ein zentraler Baustein zur Modernisierung der Landstreitkräfte, in denen sich nahezu alle Felder wiederfinden. Hier werden bestehende und zukünftige Systeme und Technologien integriert und auf die spezifischen Anforderungen der Landstreitkräfte abgestimmt, um die Bedürfnisse der Landstreitkräfte schneller und besser zu bedienen (Seite 10).

Unser Vorstand Generalleutnant a.D. Dr. Ansgar Rieks trägt für den Einsatz von künstlicher Intelligenz zehn konkrete Vorschläge Schritt hin zu einer verantwortungsvollen Anwendung von KI in militärischen Fähigkeiten der Zukunft zusammen, um die Leistungsfähigkeit von KI-Anwendungen zu nutzen und gleichzeitig ein ‚Legal Design‘ und ethische Überlegungen einzubeziehen (Seite 14).

Lieutenant General (Ret) Ben Hodges, ehemaliger Oberbefehlshaber der US Army in Europa war Gastredner bei der 37. AFCEA Fachausstellung 2024.

Foto: AFCEA Bonn e.V

Herkömmliche Ansätze zur Fähigkeitsentwicklung und -bereitstellung allein können den Anforderungen an die aktuellen Anforderungen nicht mehr gerecht werden. Soft-

ware Defined Defence (SDD) ermöglicht eine bessere Anpassungsfähigkeit. Sie ist aber auch eine notwendige Voraussetzung, um Fähigkeiten adäquat und einsatzbereit den Herausforderungen anzupassen. Hier ist laut unserem Industrie-Vorstand Marc Akkermann bereits viel erreicht. Gleichzeitig blickt er auf die Potenziale, die es in den nächsten Schritten zu nutzen gilt (Seite 16).
Die Umsetzung solch neuer Themen benötigt Mut, Zeit und Kraft. Wie hier Veranstaltungen helfen können, die „Mutigen“ zusammenzubringen und Mehrwerte zu schaffen, zeigt Justus Groth, Vorstand für unsere Emerging Leader AFCEA (ELA) am Beispiel zu einer Veranstaltung zum Einsatz von KI in der Krisenkommunikation (Seite 18).
Die zunehmende Technologisierung stößt dabei jedoch auf die große Herausforderung Fachkräftemangel. Um Ressourcen effizienter zu nutzen und technologischen Anforderungen gerecht zu werden, benötigt es einen effizienten und effektiven Technologieeinsatz, um diese Herausforderung zu meistern. Wie dies mit einer KI-Lösung gelingen könnte, beschreibt unser Ausbildungsvorstand Christopher Gaube (Seite 20).
Es ist weniger Krisenkommunikation als vielmehr Kommunikations- und Führungsaufgabe, was zur Fortsetzung und Umsetzung der Zeitenwende in der gesellschaftlichen Wahrnehmung vor uns liegt. Medienvorstand Jochen Reinhardt zeigt die Herausforderungen für Führung und Wahrnehmung einer resilienteren Gesellschaft auf und stellt Lösungsansätze zusammen, mit denen wir als Industrie, Wissenschaft und Bundeswehr, diese das Ziel gesellschaftlicher Resilienz nachhaltig verankern und erfolgreich begleiten können (Seite 22).

Mehrere tausend Teilnehmende werden auch in diesem Jahr bei der 38. AFCEA Fachausstellung erwartet. *Foto: AFCEA Bonn e.V*

Die 38. AFCEA Fachausstellung ist auch thematisch unsere Flaggschiffveranstaltung. Zum fünften Mal öffnet sie am 27. und 28. Mai 2025 im World Conference Center Bonn (WCCB) ihre Tore. Wir erwarten wieder mehrere tausend Teilnehmer aus Besuchern und Standpersonal. Rund 250 Aussteller werden auf acht Ausstellungsflächen dabei sein. Unser Symposium im Plenarsaal des alten Bundestages beschäftigt sich in Vorträgen und Podiumsdiskussionen mit unseren Themenfeldern, ergänzt durch fachliche Firmenvorträge. Natürlich wird auch der gesellige Austausch mit dem traditionellen Get-together am ersten Messeabend wieder stattfinden. Zeitenwende konkret und greifbar – in Lösungen und im Gespräch. Das zeichnet die Ausstellung aus. Über die konkrete Ausgestaltung gibt Wolfgang Quirin, Leiter der Fachausstellung eine Orientierung (Seite 24).
Im vergangenen Jahr habe ich an dieser Stelle im Heft die Frage gestellt: Sind wir hier bereits am Ziel?
Die Antwort war: Sicher nicht!
Und heute? Die Community hat geliefert. Wir sehen – und wir zeigen hier mit unseren Beiträgen im Heft, auf unseren Veranstaltungen und auf den Messeständen der Fachausstellung – dass Ämterseite, Industrie und Wissenschaft engagiert zusammen Lösungen entwickeln und umsetzen können, damit wir die digitale Transformation unserer nationalen Sicherheitsarchitektur erfolgreich umsetzen. AFCEA Bonn e.V. bietet als neutrales, nationales Netzwerk mit seinem Jahresprogramm auch 2025 wieder die Austauschplattform, auf der sich Bedarfsträger, Bedarfsdecker, Industrie und die Wissenschaft austauschen können. Unser Beitrag ist ein sachlicher Dialog mit frühzeitiger Information, in dem der Bedarfsträger seine Interessen darstellen, der Bedarfsdecker Lösungsräume identifizieren und die Industrie den Sachstand und das Entwicklungspotential darstellen kann. Auch die Wissenschaft lässt ihre Erkenntnisse in Konzeptionen einfließen.
Unser gesellschaftliches Ziel ist damit noch lange nicht erreicht. Gemeinsam laufen wir die Marathonstrecke. Es ist noch ein langer Weg zu gehen, der von Herausforderungen geprägt ist: Weiterhin destabilisieren uns Desinformationskampagnen und Extremismus unsere Gesellschaft und setzen tagtäglich unsere freiheitliche demokratische Grundordnung unter Druck. In einer angespannten finanziellen Situation erfordert die zunehmende militärische Bedrohung weiterhin Investitionen in unsere Verteidigungsfähigkeit.
Neben allen fachlichen Themen, für die AFCEA Bonn e.V. eine Plattform bietet, wollen wir mit der Fachausstellung, allen anderen Veranstaltungen, unserem Ausbildungsengagement und der Mitgliedschaft im Verein zeigen: Niemand kämpft dafür allein! Gemeinsam laufen wir diesen Marathon! Für diese Gemeinschaft lade ich Sie zur AFCEA Fachausstellung ein: Team Marathon, Team doppelte Zeitenwende, Team AFCEA Fachausstellung!

AFCEA-JAHRESPROGRAMM

www.afcea.de/veranstaltungen/jahresprogramm.html

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

Henry Günter Neumann,
Stv. Vorsitzender und Leiter Programm

Franz Bernd Möllers,
Stv. Vorsitzender und Leiter Industriebeirat

Weitere Mitglieder mit ihren Zuständigkeiten

Thomas Wirsching, Geschäftsführer,
Schatzmeister, Veranstaltungsmanagement

Andreas Höher,
Bundesressorts (ohne BMVg)

Christoph Gaube, Ausbildung

Generalleutnant a. D. Dr. Ansgar Rieks,
Schulförderung

Kevin Thiele, BOS

Jochen Reinhardt,
Presse & Medien

Wolfgang Taubert, Berlin & Internationales,
Regional Vice President Central Europe,
Director of the Board AFCEA International

Dr. Michael Gerz,
Wissenschaft und Forschung

Marc Akkermann, Industrie

Justus Groth, Emerging Leaders AFCEA
Bonn e.V.

Christian Rösch, Schriftführer

Christine Skropke, Cybersicherheit,
Member of the Board of Directors and
Executive Committee AFCEA International

Marianna Schwarz, Innovation/Mentoring

Brigadegeneral Rainer Beeck, Bundeswehr

Fotos: AFCEA Bonn e.V.

Die AFCEA-Geschäftsstelle

Die AFCEA Geschäftsstelle steht in allen Fragen des Vereins, insbesondere zur Satzung, Geschäftsordnung, Mitgliederfragen und -beitragswesen, Anmeldung/Organisation von AFCEA-Veranstaltungen im Büro auf dem Hardtberg in Bonn bereit.

Das sind Ihre Ansprechpartner:
Thomas Wirsching: Geschäftsführer, Schatzmeister, Veranstaltungsmanagement
Beate Jaedicke: Buchhaltung, IT-Unterstützung, Veranstaltungsunterstützung
Bernward Sondermann: Mitgliederbetreuung, Veranstaltungsunterstützung
Gerhard Groth: Adressdatenbank, Veranstaltungsunterstützung
Die Geschäftsstelle ist Montag bis Donnerstag von 08:30 bis 14:30 Uhr und freitags von 08:30 bis 12:30 Uhr besetzt. Sie können auch gerne, zu jeder Zeit, eine Nachricht über die Emailadresse versenden.
Der Geschäftsführer und alle Mitarbeiter sind über die folgenden Kontaktdaten zu erreichen:

AFCEA Bonn e.V.
Borsigallee 2
53125 Bonn
Tel.: +49 228 925 82 52
E-Mail: buero@afcea.de

Wie die Landstreitkräfte auf die Zeitenwende reagieren

Brigadegeneral Rainer Beeck, AFCEA Vorstand Bundeswehr, Stellvertretender Kommandeur Operationen und J6 Bundeswehr, Kommando CIR

Brigadegeneral Rainer Beeck

Foto: privat

AFCEA Bonn e.V. hat sich in den vergangenen beiden Jahren intensiv mit Themen beschäftigt, die sich aus der von Bundeskanzler Olaf Scholz ausgerufenen sicherheitspolitischen Zeitenwende und der digitalen Zeitenwende bei der Bundeswehr ergeben. Als neutrales, nationales Netzwerk werfen wir einen Blick darauf, wo und wie Modernisierung, Digitalisierung und Souveränität von Bundeswehr und Sicherheitsbehörden schneller vorankommen können. Welchen Wirkbeitrag kann Digitalisierung zu einer kriegstüchtigen Bundeswehr als Instrument glaubwürdiger Abschreckung leisten?

Welcher Blick auf die Entwicklung könnte konkreter sein als derjenige der Denker und Macher, deren tägliche Arbeit die Zeitenwende konkret prägt. Aus diesem Grund gibt uns das Amt für Heeresentwicklung einen Sachstand zu ihrer Experimentalserie Land. Die Serie ist ein zentraler Baustein für eine beschleunigte, harmonisierte und bedarfsorientierte Modernisierung der Landstreitkräfte, um bestehende und zukünftige Systeme auf ihre Integrationsfähigkeit zu testen. Hier werden Technologien aufeinander und auf die spezifischen Anforderungen der Landstreitkräfte abgestimmt, um die Bedürfnisse der Landstreitkräfte schneller und besser zu bedienen.

Das „Labor im Gelände“ – Die Experimentalserie Land

Oberst Mario Brux, Leiter Projekt Gruppe Digitalisierung, Amt für Heeresentwicklung

Oberst Mario Brux

Foto: Bundeswehr/Schulze

Die Verteidigungspolitischen Richtlinien (VPR) 2023 betonen unter dem Aspekt „Grundlagen für eine leistungsfähige Bundeswehr der Zukunft“, dass die umfassende Einsatzfähigkeit der Bundeswehr oberstes Ziel ist. Gleichzeitig müssen Modernisierungen den immer kürzeren Innovationszyklen und der Entwicklung der Industrie 4.0 gerecht werden. Dabei fordern die VPR auch eine regelmäßige Überprüfung von Fähigkeiten in Test- und Versuchsumgebungen. Hier knüpft die Experimentalserie Land an und liefert proaktiv Antworten auf diese Anforderungen.

Im Herbst 2023 hatte die „Experimentalserie Land“ (ExpS La) ihre Premiere. Übergeordnetes Ziel muss es sein, die Zukunft der Landstreitkräfte zu gestalten. Das Format dient dazu, Technologien gezielt aufeinander und auf die spezifischen Anforderungen der Landstreitkräfte abzustimmen. Zudem soll dieses Experimentierfeld als fortlaufende Serie etabliert werden, um Fähigkeitsforderungen frühzeitig in Entwicklungs- und Beschaffungsprozesse einbringen zu können und damit alle Möglichkeiten bestehender Verfahren auszuschöpfen, um schneller und besser auf die Bedürfnisse der Landstreitkräfte abgestimmte Projekte / Programme einführen zu können.

Zippermast auf Fahrzeug

Foto: Bundeswehr/Schulze

Zippermast mit Wirkmittel auf UGV Gereon (ARX Landsysteme), Drohne in der Luft *Foto: Bundeswehr/Schulze*

Grundgedanke der Experimentalserie Land

Mit Blick auf die Landes- und Bündnisverteidigung und die rasanten technologischen Entwicklungen stellt sich das Amt für Heeresentwicklung im Rahmen seines Mottos „Das Heer weiter denken“ unter anderem folgende zentrale Fragen:

- Wie können Innovationen – sei es neues Material, Software oder Einsatzgrundsätze – schneller in die Truppe gelangen?
- Wie lässt sich sicherstellen, dass Material und Software reibungslos sowohl in den Informations- und Kommunikationsverbund, als auch in „Sensor-to-Effector“-Prozesse integriert werden?
- Wie können wir als Nutzer frühzeitig unsere perspektivischen Bedarfe kommunizieren und so in den Entwicklungsprozess einbinden, dass passende Demonstratoren und kriegstaugliche, marktverfügbare Produkte betrachtet und - bei Bedarf durch Anpassungen - zur Marktreife gebracht werden können?

Der Grundgedanke sieht eine enge Verknüpfung von Anwenderinnen und Anwendern in Forschung, Entwicklung und Nutzung zu einem frühen Zeitpunkt in bestehenden Prozessen vor. Hierbei tritt das Heer als Nutzer auf, definiert basierend auf militärischen Szenarien Anforderungen und stellt Testumgebungen sowie Expertise bereit. In enger Abstimmung mit dem Planungsamt der Bundeswehr (PlgABw), dem Zentrum Digitalisierung der Bundeswehr (ZDigBw) und dem Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAAINBw) werden Demonstratoren oder marktverfügbare Testmuster sowohl über Forschung und Technologie (F&T) Studien als auch als Markterkundung mit Vertrag oder als Teil bestehender Projekte in die ExpS La eingebracht. Getestet werden diese Produkte dann in durch die Truppengattungsgruppen des Amtes erarbeiteten militärischen Testvignetten, die somit als „Leistungsanforderung“ verstanden werden können. Die unmittelbar stattfindenden Auswertungen werden mit Blick auf potenzielle Strukturanpassungen, technische Herausforderungen, möglichen Anpassungsbedarf von Einsatzgrundsätzen oder der Dokumentenlandschaft durchgeführt. Dabei sollen auch kurzfristige Erkenntnisgewinne, die direkt für die Truppe nutzbar sind, identifiziert werden. Hierzu tragen alle Teilnehmer der Experimentalserie Land aus Forschung & Entwicklung, wehrtechnischen Dienststellen, teilnehmende Firmen gemeinsam mit Soldatinnen und Soldaten bei.

Praktische Anwendung der Experimentalserie Land

Die Experimentalserie wird genutzt, um:

- Informations- und Kommunikationsverbünde auszubauen, zu betreiben und weiterzuentwickeln,
- bestehendes wie auch neu zulaufendes Material als auch Software in das System Land zu integrieren, anzupassen bzw. weiterzuentwickeln,
- Einzelsysteme bis hin zum komplexen Systemverbund in einem digitalen Umfeld taktisch und technisch zu erproben,
- gezielt neue Studien zu initiieren und bestehende bei Bedarf zu harmonisieren,
- innovative Lösungen zu integrieren und so frühzeitig zielgerichtete und am Bedarf der Nutzer ausgerichtete Lösungen der Truppe zur Verfügung zu stellen.

Das Konzept wird bildlich als „Labor im Gelände“ beschrieben. Damit wird der Vorgabe der VPR 2023 nach einer dauerhaften zyklischen Anpassung von Fähigkeiten, der begleitenden experimentellen Überprüfung in Test- und Versuchsstrukturen sowie der anschließenden Umsetzung in der Fläche grundsätzlich Rechnung getragen [VPR 2023, Seite 32]. Dabei erstreckt sich die Experimentalserie über das ganze Jahr und bildet einen kontinuierlichen Rahmen.

Gäste der Veranstaltung mit AFCEA zur Integrationstestung. *Foto: Bundeswehr/Hoermann*

Sie gipfelt zum Jahresende in die Integrationstestung, bei der neue und bestehende Systeme zusammengeführt und in militärischen Vignetten ebenfalls getestet werden. Dadurch entsteht der Dreiklang Einzeltestung, Vernetzung, Integrationstestung.
Bei der Integrationstestung im vergangenen Jahr wurde zudem am 29. Oktober ein „Distinguished Visitors Day“ unter Schirmherrschaft von AFCEA e.V. Bonn durchgeführt. Hier waren in der AFCEA organisierte Vertreterinnen und Vertreter aus Industrie, Wissenschaft und militärischen Dienststellen vor Ort im Gefechtsübungszentrum des Heeres, um live dabei zu sein, wie und in welchem Ausmaß das Heer neue und alte Systeme miteinander vernetzt, integriert und testet. Ziel war zudem auch der wichtige Informationsaustausch mit dem Nutzer.

Der Fokus der „Experimentalserie Land“ liegt darauf, möglichst nur noch solche Produkte für die Einführung in die Landstreitkräfte in Erwägung zu ziehen, die bereits in der Entwicklung eine Einbindung und Kompatibilität mit dem Programm „Digitalisierung Landbasierter Operationen“ (D-LBO) nachweisen können. Schwerpunkt hierbei ist es, die verwendete Soft- und Hardware in das Battlemanagementsystem (BMS) integrieren zu können. Damit wird der „Sensor-to-Effector“-Prozess gestaltbar und kann letztendlich bruchfrei schneller ablaufen. Ziel ist eine digitale Gefechtsführung, die über die Informationsüberlegenheit zur Führungsüberlegenheit und letztendlich zur Wirkungsüberlegenheit im Gefecht führen soll.

Verschiedene Teilnehmer *Foto: Bundeswehr/Hoermann*

BOXER im Hintergrund, niederländisches UGV TheMIS im Vordergrund

Foto: Bundeswehr/Schulze

Zukunftsperspektiven der Experimentalserie Land

Im Jahr 2023 war die „Experimentalserie Land“ ein erster Schritt und eine Erprobung des Konzeptes. 2024 wurde die Experimentalserie ausgeweitet und komplexer gestaltet. Ziel ist es, die Serie kontinuierlich weiterzuentwickeln, um die Landstreitkräfte, gestellt von Heer, Unterstützungsbereich und Teilstreitkraft Cyber- und Informationsraum (CIR) auf geopolitische Herausforderungen und technologische Entwicklungen vorzubereiten. Somit soll sichergestellt werden, dass eine stetige Adaption in Bezug auf moderne und effiziente Technologien vorgenommen werden kann. Sie ist integraler Bestandteil eines zyklischen Prozesses, der auf die fortlaufende Modernisierung des Heeres abzielt.

Multinationale Zusammenarbeit spiegelte sich ebenfalls in der Experimentalserie 2024 wider. So testeten die Einheiten der „Robotics and Autonomous Systems“ (RAS) der niederländischen Streitkräfte zusammen mit deutscher Beteiligung den Einsatz eines „Combat Unmanned Ground Vehicle“ (Combat-UGV). Für 2025 sind weitere internationale Kooperationen in Planung.

Eine Notwendigkeit für die Zukunft der Landstreitkräfte

In einer Zeit, in der Innovations- und Adaptionsfähigkeit entscheidend sind, ist die „Experimentalserie Land“ ein zentraler Baustein für eine beschleunigte, harmonisierte und bedarfsorientierte Modernisierung der Landstreitkräfte. Die „Experimentalserie Land“ stellt aus Sicht des Amtes für Heeresentwicklung ein hervorragend geeignetes Verfahren dar, um die Integrationsfähigkeit in bestehende und zukünftige Systeme zu testen und damit schneller und bessere Fähigkeiten für erfolgreiche Landstreitkräfte bereitstellen zu können.

Verantwortliche Nutzung von KI

Dr. Ansgar Rieks, Generalleutnant a.D., Vorstand AFCEA Bonn e.V.

Dr. Ansgar Rieks, Generalleutnant a.D. *Foto: AFCEA*

Eigentlich müsste man gar keinen Beitrag über verantwortliche Nutzung von Künstlicher Intelligenz schreiben, weil sie sich selbst erklärt. Verantwortlich mit Dingen, Anvertrautem, Daten, Ämtern oder Waffensystemen umzugehen, ist nicht nur rechtlich klar geregelt, sondern auch moralisch gefordert. Und man sollte auch auf sich selbst dabei achtgeben. Schwierig wird es zumeist dann, wenn man diese Verantwortung in einem fachlich komplexen und neuen Umfeld definieren soll. Immerhin ist hierbei zu erwähnen, dass eine Vielzahl von "Playern" sich dieses Themas angenommen hat. Das Bemühen um die Definition eines "Code of Conduct" im Umgang mit Künstlicher Intelligenz (KI) mag aus unterschiedlichen Beweggründen erfolgen, es ist jedenfalls international feststellbar und dokumentiert. Zunächst ist das eine positive Entwicklung. Wir wissen aus mannigfaltigen Erfahrungen in zahlreichen Anwendungsgebieten über die Technikgeschichte hinweg, dass die stumpfe Nutzung eines neuen technischen Werkzeugs ohne jede Reflektion und Einordnung zumeist ins Abseits, wenn nicht in die Katastrophe führen kann. Daher ist die "verantwortliche Nutzung von KI" halt eben doch einen Artikel - und jenseits dessen ganz viele technische, juristische, ethische und anwendungsfachliche Gedanken und Entwicklungen - wert.

Die Begründungsmuster

Es ist nicht kontraproduktiv oder verwerflich, dass ethische Überlegungen - im weitesten Sinne - heutzutage Konjunktur haben. Dies ist einerseits einem gewandelten Verständnis des eigenen Handelns geschuldet, andererseits auch einem gewandelten Rechtsverständnis. Dazu steht ein "Buzzword" im Raum, das für westliche Gesellschaften sich zu einem "Elephant in the Room" entwickelt hat: "Compliance". Gewissen von außen oder von selbst gesetzten Regeln gegenüber compliant zu sein, lässt sich gut zu Werbezwecken nutzen und fördert den Umsatz. Daher ist es gut, sich für KI einen Regelsatz zu schaffen, und diesem nachgewiesen zu folgen. Dieses gilt nicht nur für einzelne Firmen oder Gesellschaften, sondern auch mehr und mehr für internationale Konzerne und Organisationen. So haben beispielsweise die NATO und die EU-Standards für den Umgang mit KI definiert. Herausfordernd wird es dabei immer dann, wenn unterschiedliche Wert- und zumeist auch Rechtsvorstellungen die Grenzen einer KI-Nutzung flexibel werden lassen. Konkret: für das Aufgreifen oder gar eine Tötung von Terroristen wird die Nutzung von KI im amerikanischen Umfeld weit flexibler betrachtet, als im europäischen, wo Letzteres ohne Weiteres als moralisch äußerst fragwürdig gilt. Eine ‚weltweite' Regelung hat also noch viel größere Herausforderungen, als sie bereits in der ‚westlichen Welt' sichtbar sind. Dies ist umso mehr der Fall, als große Teile der Welt, wie die BRICS plus-Mitgliedstaaten, die Transaktionalität in den Vordergrund ihres Handelns stellen und wertebezogene Ansätze nicht in höchster Priorität sehen.

Die Fachlichkeit

Ganz unabhängig von diesen generellen Erkenntnissen zu einer verantwortlichen Nutzung von KI spielt die Fachlichkeit der Anwendung eine entscheidende Rolle zur Beurteilung des KI-Einsatzes. Einerseits ist es einsehbar, dass die Schwere einer möglichen Folge eines verfehlten oder missbräuchlichen KI-Einsatzes für eventuelle begrenzende Regeln und Rahmenbedingungen unmittelbar entscheidend sein muss. Somit ist eine besondere Sorgfalt erforderlich, wo es um Leib und Leben, aber auch um die Bewertung und Einschätzung von Menschen geht, also in Bewerbungsverfahren oder bei Täterermittlungen. Für den Einsatz von KI in Waffensystemen hat man darüber hinaus zu berücksichtigen, dass gegnerisches Einwirken im Sinne einer Cyber-Beeinflussung möglichst nicht zu einer Fehlfunktion mit fatalen Folgen führen darf. Administrative Prozesse dagegen sollten zwar auch fehlerfrei sein, die Fehlerkultur kann jedoch wesentlich großzügiger sein. Bei all diesen Überlegungen zeigt sich, dass die Anwendungsfachlichkeit eine überaus große Rolle bei der Beurteilung einer KI-Nutzung darin spielt. Es ist deshalb unverhältnismäßig, KI beispielsweise in Waffensystemen pauschal abzulehnen, ohne ihre Funktion und Wirkung im systemischen Verbund zu verstehen. Daher bedarf es der Techniker und Operateure, die sich mit ethischen Fragen befassen, und mindestens in gleicher Weise der Ethiker, die sich tief in die Fachlichkeit einarbeiten, um ihre Ratschläge für ein "Ethical Design" zu geben - was, nebenbei, künftig ein wichtiges Ziel jeder Ingenieurleistung sein könnte und sollte.

Die Verantwortung in Recht und Ethik

Zugleich bedarf es der Analyse, wie ethisch-moralische Überlegungen zu einem "Ethical Design" führen können. Dabei nützt es wenig, generellen Regeln, wie den Asimovschen Gesetzen, zu folgen, infolge derer Roboter - und damit KI - keinem Menschen schaden oder ihn gar töten darf. KI im militärischen Bereich muss dazu beitragen, einen gezielten und präzisen, wirksamen Einsatz von Waffensystemen sicherzustellen, der lethale Wirkung hat. Ein verantwortlicher Einsatz von KI umfasst daher etwa, proportional und diskriminativ

vorzugehen, kurz: nur so viel Zerstörung anzurichten, wie militärisch unabdingbar notwendig, und Kollateralschäden, insbesondere in der Zivilbevölkerung, zu vermeiden. Diese Rahmenbedingungen sind - über die Jahrhunderte entwickelt - inzwischen in internationales Recht eingeflossen. Ein Ethical Design wird damit, in Umsetzung solcher Regeln, zu einem ‚Legal Design'. Ethik wäre damit die erklärende Wissenschaft, Recht die zu implementierende. Damit wäre keinerlei ethische Ausbildung in den Streitkräften für den verantwortlichen Einsatz von KI in Waffensystemen vonnöten, eine fundierte Rechtsausbildung schon. Warum steht Ethik dennoch im Vordergrund für KI-Anwendungen? Es gibt zwei Begründungen dazu: Erstens ist eine in Recht gegossene Übertragung von Regeln aus dem Mittelalter kaum 1:1 auf moderne Technologien und neue Operationsführung möglich. In einem ‚System der Systeme' mit horizontalen und vertikalen Mensch-KI-Verbindungen sind ganz neue Überlegungen für einen verantwortungsvollen Umgang mit digitalen Werkzeugen zu erarbeiten. Ethik muss sich angesichts neuer militärischer und technologischer Entwicklungen fortentwickeln. Es ist also keine weitere KI-Ethik wichtig, sondern eine neue Fachethik, die neue militärische Fähigkeiten begleitet, orientiert und auch begrenzt, ohne möglichst die Wirksamkeit und Nutzbarkeit des Waffeneinsatzes zu verringern. Und zweitens muss es ethische Überlegungen bei Soldatinnen und Soldaten – insbesondere auch in Führungsfunktionen und Hauptquartieren – geben, die zur Anwendung kommen können, selbst wenn allen rechtlichen Rahmenbedingungen genüge getan wird. Das Völkerrecht ermöglicht z.B. alle gegnerischen Kombattanten in einem kriegerischen Konflikt zur eigenen Verteidigung zu bekämpfen. Ob dieses alle Soldaten des Gegners - in jeglicher Funktion und zu jedem Zeitpunkt - umfassen ‚muss', ist eine militärische Frage; ob man es ohne militärische Notwendigkeit nicht tut, eine ethische. Ein verantwortlicher Umgang mit KI kann daher zunächst alle rechtlichen Rahmenbedingungen aufgreifen und abbilden, danach – quasi als add-on – ethische Rahmenbedingungen. Eine Ethikausbildung und ethische Regeln - auch mit Blick auf KI - sind also nur dann sinnvoll und praxisnah, wenn nicht immer das volle eigene militärische Potenzial in der Operationsführung in jeder Situation zur Anwendung kommen muss. Das ist auch eine grundlegende und strategische Entscheidung, insbesondere wenn der Gegner unethisch handelt. Letztlich geht es wohl auch nur dann, wenn zumindest ein gewisses Maß an eigener Überlegenheit vorhanden ist.

Die Konkretisierung

Alles Geschriebene bedarf der Konkretisierung in zweierlei Hinsicht: systemisch und ethisch, wobei es darüber hinaus erforderlich ist, beides aufeinander zu beziehen. Ein erster Versuch der Systematisierung sind die folgenden zehn Vorschläge. Sie versuchen die Leistungsfähigkeit von KI-Anwendungen zu nutzen und gleichzeitig ein ‚Legal Design' und ethische Überlegungen einzubeziehen. Sie wären ein erster Schritt hin zu einer verantwortungsvollen Anwendung von KI in militärischen Fähigkeiten der Zukunft:

1. Mache KI leistungsfähig; bestimme aber den Rahmen, in dem sie wirken darf.
2. Lege die notwendige Datenfülle für das Anlernen der KI fest.
3. Lege messbare Standards und Wahrscheinlichkeiten fest, in denen KI genutzt werden darf.
4. Die Verantwortung von Informatikern, Ingenieuren und Operateuren für den Einsatz von KI ist disjunkt und nicht übertragbar.
5. Definiere im Einzelnen die Verantwortung im Mensch-Mandanten-System. Sie kann situationsbedingt verschoben werden.
6. Bei weitestgehender Automatisierung setze Menschen dort ein, wo Verantwortung über ein "dennoch" oder ein "nein" zu tragen ist.
7. Beim Zusammenwirken verschiedener Systeme (Multi Domain) halte jedes System für sich funktionsfähig, rechtlich einwandfrei und ethisch akzeptabel.
8. Lege Fehlertoleranzen fest, die das Testen von KI-Systemen bestimmen.
9. Baue menschliche Entscheidung ein, wo ein Legal Design nicht möglich ist oder persönlicher Abschätzung bedarf (Proportionalität).
10. Ergänzend zur Rechtsbeachtung und zur Sicherstellung der Funktionsfähigkeit wende konkrete ethische Regeln ‚wo möglich' an.

Das Fazit

Eine verantwortliche Nutzung von KI ist damit von einer Vielzahl unterschiedlicher Parameter und Überlegungen abhängig. Sie wird von dem Verständnis geprägt, eine ethische Kriegführung tatsächlich zu wollen, und nicht nur unethisches oder illegales Handeln auszuschließen. Ferner führt ein Legal Design in gewissen Situationen zu Einschränkungen. Um eine rein emotionale Diskussion zu vermeiden, sind konkrete Rahmenbedingungen für die Nutzung von KI festzulegen, die sich aus einer künftigen Operationsführung mit modernen militärischen Systemen in allen militärischen Dimensionen ableiten. Wer nicht daran glaubt, dass "Ethik" so konkret gemacht und Verantwortung so technisch auch unterstützt werden kann, wird eine verantwortliche Anwendung von KI in militärischen Anwendungen pauschal ablehnen. Das würde militärisches Handeln in der Zukunft fragwürdig machen und wäre damit weder realistisch noch akzeptabel. KI verantwortungsvoll auszuformen und zu implementieren, ist damit unabdingbar.

Software Defined Defense
Potenziale und Blockaden für das neue Paradigma

Marc Akkermann, AFCEA Vorstand Industrie, Vice President Public Defense bei Capgemini Deutschland GmbH

Marc Akkermann *Foto: Privat*

Der Begriff „Software Defined Defense“ (SDD) ist heute innerhalb unserer Branche in aller Munde und wird ernst genommen. Das an sich kann schon als erster Erfolg gewertet werden. Wir sind über die Phase „yet another buzzword“ hinaus. Dennoch haben wir bei weitem noch nicht den Status erlangt, dass eine erfolgreiche Umsetzung dieses neuen Paradigmas zur Fähigkeitsentwicklung und -bereitstellung bereits eine sichere Sache ist.

Wir haben bereits viel erreicht.

In den letzten Jahren ist das Bewusstsein dafür, dass die herkömmlichen Ansätze zur Fähigkeitsentwicklung und -bereitstellung allein den Anforderungen an die heute Zeit nicht mehr gerecht werden können, stark gestiegen.

Zu Beginn war SDD ein Schlagwort, das aus einem kleinen Kreis heraus geprägt wurde. Es bestand das Risiko in der Schublade anderer Initiativen mit guten Ideen aber geringer Aussicht auf Umsetzung zu landen. Was also lief bei SDD anders?

1. **Breiter Dialog mit hoher Transparenz**
   Erstmals in der jüngeren Vergangenheit wurde ein Thema so umfassend transparent und unter Einbindung verschiedenster Stakeholder er- und bearbeitet. Im Rahmen des Strategischen Industriedialogs des BMVg mit der Sicherheits- und Verteidigungsindustrie wurde unter Beteiligung mehrerer Verbände ein Arbeitsformat geschaffen, in dem die Ausgestaltung von SDD umfassend betrachtet wurde. Beginnend mit einer kleinen Kerngruppe überzeugter SDD-Enthusiasten sind mittlerweile alle relevanten Bereiche in diese Diskussion eingebunden.
2. **Beharrliches Senden der Botschaft**
   Keine größere Veranstaltung mit Bezug auf unsere Verteidigungsbereitschaft und die Fähigkeiten unserer Streitkräfte ohne SDD! Das war das Motto der vergangenen zwei Jahre. Die „Kernspieler“ in Ministerium, Truppe und Industrie haben gemeinsam „vom gleichen Notenblatt gesungen“ und das immer wieder. Somit wurden SDD und dessen Notwendigkeit immer breiter gestreut.
3. **Größerer Veränderungsdruck von außen**
   Nicht außer Acht lassen dürfen wir aber auch die Veränderung der Sicherheitslage. Mit dem Angriff auf die Ukraine und der radikalen Veränderung der sicherheitspolitischen Lage und damit auch der benötigten Kernfähigkeiten unserer Streitkräfte wurde das Thema SDD auf einer Trägerwelle von Veränderungsnotwendigkeit getragen. „Weiter wie bisher“ war keine Option mehr.

In Summe haben wir aktuell eine Ausgangslage, die eine breites Bewusstsein für den Veränderungsdruck mit dem Potenzial Software-basierter Fähigkeitsentwicklung kombiniert.

Wenn wir es richtig machen, können wir viel Potenzial heben

SDD steht nicht allein. SDD hat keinen Selbstzweck. SDD ist ein Enabler für etwas, dass wir zur Verteidigungsfähigkeit und für unsere Chancen auf dem Gefechtsfeld dringend brauchen: Die Möglichkeit zur Durchführung echter Multi-Domain-Operations (MDO). Und genau darauf zielen alle Handlungsfelder und Potenziale von SDD ab.

1. **Aufbrechen von Systemgrenzen und Datensilos**
   Das bisherige Fähigkeitsmanagement hatte einen starken Fokus auf Plattformen oder Systeme, die zum Abdecken einer Fähigkeitslücke ganzheitlich entwickelt wurden – mit eigenen Kontrollsystemen, Sensoren, Effektoren und oftmals auch proprietärem Datenmanagement. Der Grundgedanke muss von verschiedenen Systemen auf dem Gefechtsfeld hin zu dem einen Systemverbund (system of systems) schwenken. Jedes Flugzeug, jedes Fahrzeug, jedes Schiff und Spezialsysteme sind potenzielle Sensoren und Effektoren, die im Zusammenwirken die maximale Effektivität und Effizienz zur Auftragserfüllung entfalten. Selbstverständlich müssen die Systeme auch autark handlungsfähig bleiben, wenn Kommunikationsverbindungen nicht zur Verfügung stehen – das Fähigkeitsportfolio darf aber nicht auf diesen Zustand beschränkt bleiben.
2. **Effektive und effiziente Entwicklung und Bereitstellung von Fähigkeiten und deren situationsgerechte Anpassung**
   SDD ersetzt nicht Rüstung der Truppe mit Kernfähigkeiten und Waffensystemen. Diese ist weiterhin nötig – muss aber zwingend um SDD ergänzt werden.
   Wenn die Grundprinzipien von SDD umgesetzt sind, können Software-basierte Fähigkeiten unter Nutzung verschiedener Systeme und Plattformen aus allen Dimensionen schnell entwickelt oder angepasst und ef-

fizient ausgerollt werden. Das ermöglicht eine zeitnahe Anpassung an geänderte Anforderungslagen.

3. **Maximale Nutzung aller Potenziale und Ressourcen zur gemeinsamen Fähigkeitsentwicklung**
   Die Umsetzung eines echten SDD-Ökosystems senkt die Hürden für „neue Spieler“ auf dem Feld. Innovative StartUps, hochspezialisierte Mittelstandsunternehmen, die Ihr Geschäftsmodell unter Umständen gar nicht primär im Verteidigungsumfeld sehen, Forschungsbereiche oder auch branchenfremde große Unternehmen sind derzeit kaum bis gar nicht in die Innovations- und Entwicklungsprozesse militärischer Fähigkeiten eingebunden. Wenn SDD wirklich gelebt wird, können auch solche Stakeholder wertvolle Beiträge zur Verbesserung der Fähigkeiten unserer Truppe leisten.

SDD ist es ein Beitrag zur Verbesserung des „Gesamtsystems Rüstung“. Einige alte Spielregeln müssen hierzu angefasst werden. Dabei gibt es Widerstände oder auch nur unterschiedliche Sichtweisen.

Die nächsten Herausforderungen stehen vor der Tür

„Wir müssen vom Dokumente schreiben ins Handeln kommen“ - Das fasst den nächsten Schritt zusammen. Das bringt einige Herausforderungen mit sich.

1. **Einheitliches Verständnis und Leitlinien**
   Wie immer, wenn ein Thema eine gewisse Breite erreicht, werden auch bei SDD unterschiedliche Ansichten zur Ausgestaltung präsenter. Handlungsfelder und Umsetzungsideen werden auf Basis der eigenen Sichtweise identifiziert und es entstehen unter Umständen auch konkurrierende Handlungsfelder. Hier ist es wichtig aus dem „Brainstorming-Modus“ in das klare Aufstellen und Kommunizieren von Leitlinien überzugehen. Dazu braucht es ein konsolidiertes Handeln von Ministerium, nachgeordneten Behörden und eine ganzheitliche Umsetzung der notwendigen Änderungen. Ggf. heißt das auch, das Verständnis für den Ansatz und dessen Notwendigkeit noch an Stakeholder zu transportieren, die bisher nicht überzeugt sind.
2. **Komplexität**
   Grundlegende Änderungen an Systemarchitekturen, Software- und Softwareentwicklungsstandards, gemeinsame Arbeitsumgebungen, technische Transparenz über System- und Anbietergrenzen hinweg, Veränderung von Geschäftsmodellen und Wertschöpfungsketten, Verlagerung von Verantwortung, gemeinsame Prozessmodelle, vertragliche Fragestellungen – und so weiter…
   SDD bringt eine enorme Komplexität mit sich, die es zu beherrschen gilt. Hierzu müssen Ansätze gefunden werden, die das Bearbeiten all dieser Handlungsfelder ermöglichen und sich gegenseitig ergänzen, statt zu behindern.
3. **Partikularinteressen**
   Nicht alle Motivationsfaktoren von Akteuren im SDD-Umfeld sind auf die bestmögliche, gesamtheitliche Umsetzung von SDD ausgerichtet. Das ist vollkommen normal und verständlich. Disruptive Änderungen bringen immer Veränderungen und ggf. auch Verluste von bisher gut funktionierenden Profitquellen oder „Machtpositionen“ mit sich. Es ist relevant, sich dieser Situation bewusst zu sein und diese auch aktiv zu adressieren.
4. **Veränderungsmanagement**
   Last but not least – wie bei jedem Veränderungsprozess ist eine aktive kommunikative Begleitung dessen notwendig. SDD richtig umgesetzt bringt Veränderungen in vielen Bereichen mit sich, die Widerstände und Ängste zutage fördern und fördern werden. Ein Veränderungsmanagement ausgerichtet an den Gesamtzielen ist hier erforderlich.

Wir arbeiten weiterhin sehr kollaborativ mit allen Beteiligten an der Umsetzung von SDD. Wenn dieser Artikel Ideen oder Vorschläge in Ihrem/Eurem Kopf entstehen lassen hat, dann sind diese immer herzlich willkommen. Der Autor dieses Artikels, aber auch alle anderen, die das Thema bearbeiten und gestalten, sind dafür immer ansprechbar – jeder Beitrag zum Erfolg von SDD ist willkommen!

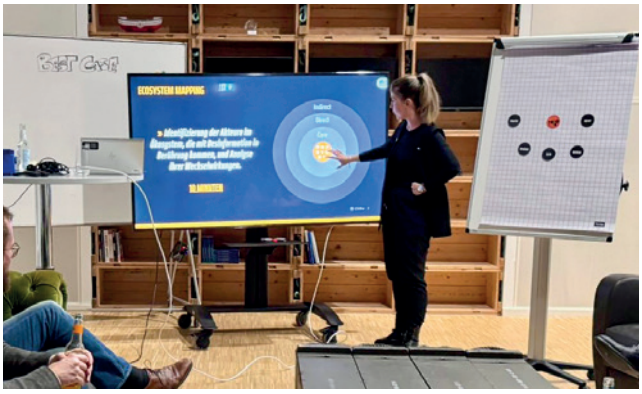
Mit Inhalten im Austausch Mehrwerte schaffen

Justus Groth, Emerging Leaders AFCEA, Vorstand AFCEA Bonn e.V., Matthias Klaus, Emerging Leaders AFCEA Bonn

Justus Groth

Foto: Emerging Leaders AFCEA Bonn

Die Umsetzung neuer Ideen benötigt Mut, Zeit und Kraft. Für die AFCEA Bonn e.V. werden neue Veranstaltungsformate und innovative Ergänzungen unter anderem von den Emerging Leaders des Vereins (ELA) entworfen und realisiert. Ein Beispiel aus dem vergangenen Jahr ist die ELA-Veranstaltung in Berlin. Erst durch den Einsatz der handelnden Personen werden gute Ideen zu wertvollen Ereignissen und Ergebnissen und aus Inhalten mit ihrer Ausgestaltung ein Mehrwert für alle Beteiligten.



Die AFCEA Fachveranstaltung der Emerging Leaders in Zusammenarbeit mit BITKOM und dem Cyber Innovation Hub der Bundeswehr (CIHBw) orientierte sich 2024 am Jahresthema „Zeitenwende in der nationalen Sicherheit – Resilienz durch disruptive digitale Lösungen“. Zentrales Element der Veranstaltungen waren vier interaktive Workshops mit unterschiedlichen thematischen und technologischen Schwerpunkten.

Der Workshop im CIHBw behandelte „KI gegen digitale Desinformationskampagnen, Auswertung von Messdaten und Datensuche in sozialen Medien.“

Desinformation ist Teil hybrider Kriegsführung. Gefälschte Videos, Texte und Fotos werden gezielt verbreitet, um Menschen und Diskurse zu manipulieren. Daher werden in Einsatzgebieten Desinformationen ausgewertet. Ähnlich wie zivile Medienorganisationen analysieren zuständige Teams Veröffentlichungen und Situationen in der Bevölkerung. Abgeleitet werden Lagebilder für die Operationsführung, die auf Basis öffentlich zugänglicher Daten Rückschlüsse auf das Debattenklima im Einsatzland zu lassen. Mit Hilfe von künstlicher Intelligenz können Bilddaten automatisch erfasst und ausgewertet werden.

Im Workshop mit der Prevency GmbH stand das Thema Krisenkommunikation im Vordergrund. Als Teil einer Krisensimulation schlüpften Teilnehmende in verschiedene Rollen und wurden durch das Szenario geführt. Die Teilnehmenden erlebten eine digital simulierte Krise beispielsweise als Krisenstabsleitung oder Presseverantwortliche und mussten sie bewältigten. Die kommunikativen Herausforderungen gegenüber der betroffenen Bevölkerung mussten gemeistert werden.

Matthias Klaus

Foto: Emerging Leaders AFCEA Bonn

Der interaktive Workshop zur Nutzung von innovativen Technologien für Frühwarnsysteme leitete die Traversals GmbH. Die Teilnehmenden erarbeiteten in kleinen Gruppen praxisnahe Lösungen und erprobten den Technologieeinsatz und die Integration von künstlicher Intelligenz, Satellitenüberwachung und Big Data in Frühwarnsystemen. Unterstützt von den Experten von Traversals entwickelten sie Strategien und identifizierten Herausforderungen im Katastrophenschutz.

Die Rasdaman GmbH führte in das Thema der automatisierten Verarbeitung von ISR (Intelligence, Surveillance and Reconnaissance) ein. Schlüsselfragen zur Vertrauenswürdigkeit von KI-Lösungen oder die Bereitstellung der notwendigen Big Data wurden diskutiert. Die Nutzung von Big Data zur Auswertung von Sensordaten, Bildern und Statistiken durch die schnelle und hochwertige Auslesung von Rasterdaten stand im Fokus.

Fotos: Emerging Leaders AFCEA Bonn

In Summe boten alle Workshops spannende Einblick in zukunftsweisende Ansätze und Technologien. Die interaktive Bearbeitung der unterschiedlichen Breakouts kreierte Lerneffekte und prägende Erlebnisse für die Teilnehmenden. Herzlichen Dank an den Cyber Innovation Hub der Bundeswehr für die Gastfreundschaft und die fachliche Leitung eines Workshops.

Der angeregte Austausch wurde beim Netzwerken fortgeführt. Die Mischung aus Themen, Vortragenden und Interaktion sind Bausteine für den Erfolg dieser Veranstaltung. Das bewährte Format wird im Jahr 2025 weiterentwickelt und fortgeführt.

Technologische Zeitenwende: Engpass Personal – Wie KI die Bundeswehr in die digitale Zukunft führen kann

Christopher Gaube, Vorstand Ausbildung AFCEA Bonn e.V., Head of Aerospace and Defense bei Capgemini Deutschland, Gero Wülfken, Experte Data & AI bei Capgemini Deutschland

Christopher Gaube *Foto: privat*

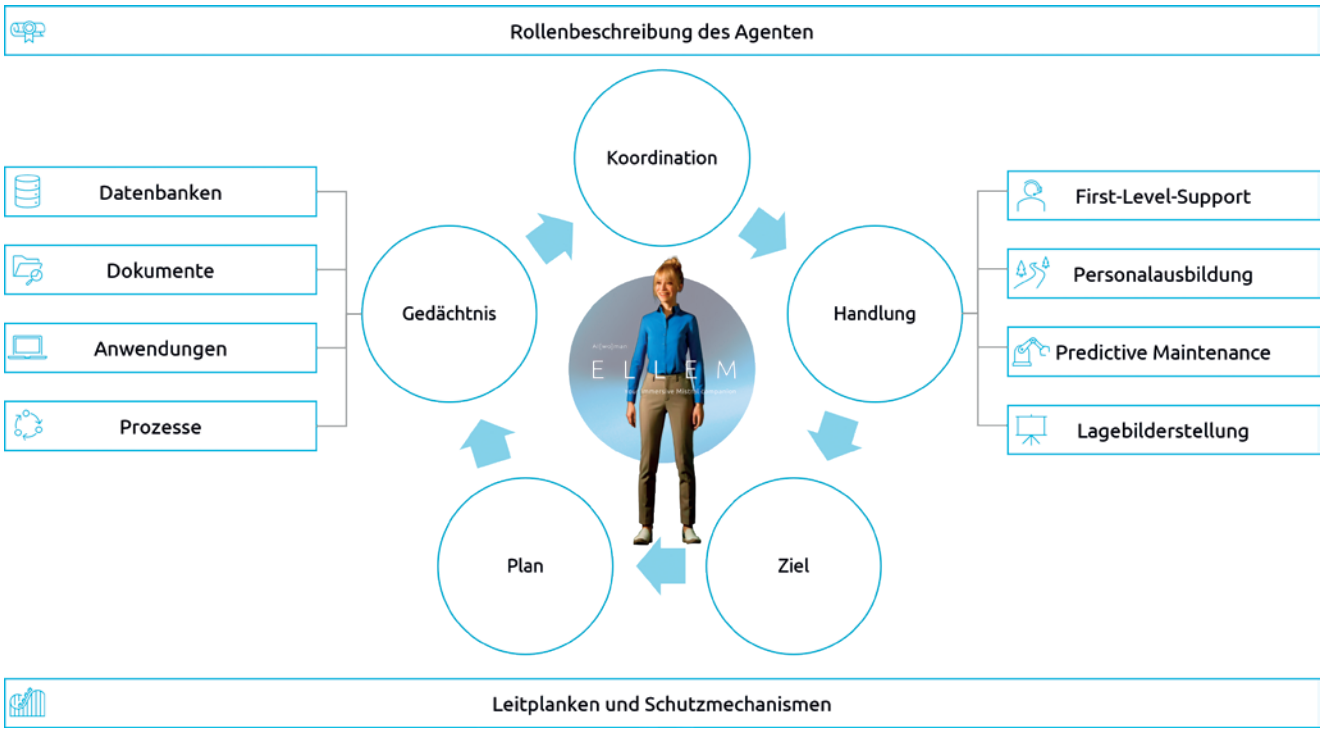
Die internationale sicherheitspolitische Lage wird zunehmend komplex. Geopolitische Spannungen, wirtschaftliche Stagnation und der demografische Wandel setzen Staaten, Streitkräfte und Industrien unter Druck. Verteidigungsressorts stehen vor multiplen Herausforderungen. Sie müssen ihre technologische Wettbewerbsfähigkeit mit den verfügbaren Mitteln sichern, um auf neue Bedrohungen schnell und flexibel reagieren zu können. Das vorhandene Personal sollte möglichst dem Kernauftrag dienen und weniger administrativen Aufgaben. Sie müssen um begehrte IT-Fachkräfte kämpfen, die auch in der Privatwirtschaft stark nachgefragt sind. Die Digitalisierung erhöht den Druck zusätzlich, da immer mehr Aufgaben technologischer Natur sind und spezialisierte Kompetenzen erfordern. Mit dem Konzept Software-Defined Defense wird deutlich, wie Verteidigungstechnologie heute gedacht werden muss. Ähnlich wie ein Smartphone, dessen Funktionen durch Software-Updates erweitert werden können, sollen militärische Systeme flexibler, anpassungsfähiger und effizienter werden und zunehmend Software-enabled arbeiten.

Gero Wülfken *Foto: privat*

Doch diese Transformation bringt auch Herausforderungen mit sich, insbesondere beim Personal. Der demografische Wandel verschärft die Situation zunehmend, da viele erfahrene Mitarbeitende aus den geburtenstarken Jahrgängen in den kommenden Jahren in den Ruhestand gehen. Gleichzeitig fehlt es an Nachwuchs, um die entstehenden IT- und technologiebezogenen Stellen ausreichend zu besetzen. Die Digitalisierung verändert die Anforderungen grundlegend und drückt auf eine Umverteilung der Aufgaben innerhalb der Bundeswehr. IT-gestützte Tätigkeiten wie Softwarepflege und -entwicklung, IT-Betrieb, Administration, IT-Support und viele weitere gewinnen an Bedeutung. Eine Pattsituation droht – ein signifikanter Personalzuwachs deutet sich nicht an, gleichzeitig setzen sich die Technologisierung und „Softwarisierung“ der Streitkräfte mit zunehmender Geschwindigkeit fort.

Holografischer KI-Agent ELLEM. *Foto: Capgemini*

Um diese Herausforderungen zu bewältigen, bedarf es eines stringenten Einsatzes verschiedener Technologien. Agentic AI bietet eine Lösung, um die Personalbedarf für solche Aufgaben zu mindern. Diese Technologie basiert auf generativer künstlicher Intelligenz (Gen AI), die es Systemen ermöglicht, Inhalte oder Lösungen eigenständig zu erzeugen und Aufgaben autonom zu übernehmen. Agentic AI geht jedoch einen Schritt weiter. Sie handelt als eigenständiger „Agent“, der wiederkehrende, routinemäßige Aufgaben wie den First-Level-Support, das IT-Problemmanagement oder die



Beispielhaftes Einsetzen eines KI-Agenten. *Foto: Capgemini*

Prozessoptimierung übernehmen kann. Durch die Fähigkeit, Probleme autonom zu identifizieren und zu lösen, reduziert Agentic AI die Abhängigkeit von menschlichen Ressourcen für einfache, aber zeitaufwändige Tätigkeiten und steigert gleichzeitig die Effizienz.

1. Agentic AI steigert die Effizienz, indem sie repetitive Prozesse automatisiert und Aufgaben schneller erledigt.
2. Sie reduziert Kosten, da weniger menschliche Ressourcen für einfache Tätigkeiten gebunden werden.
3. Sie verbessert die Qualität der Arbeit, indem sie Fehler minimiert und durchgehend verlässliche Ergebnisse liefert.

Durch den Einsatz von Agentic AI kann die Bundeswehr nicht nur dem Fachkräftemangel entgegenwirken, sondern auch ihre Innovationsgeschwindigkeit erhöhen. Das (IT) Personal kann sich mehr dem Kernauftrag widmen und auf die Weiterentwicklung von Technologien konzentrieren, was langfristig die digitale Transformation beschleunigt.

Die Zeitenwende erfordert ein Umdenken, und Agentic AI ist einer der Schlüssel, um Ressourcen effizienter zu nutzen und technologischen Anforderungen gerecht zu werden. Mit entschlossenem Handeln kann die Bundeswehr ihren Weg in die digitale Zukunft erfolgreich gestalten.

Verbände und Netzwerke wie die AFCEA Bonn e.V. spielen dabei eine Schlüsselrolle. Sie helfen, technologische Trends frühzeitig zu erkennen, Anwendungsfälle näher zu bringen und deren Integration voranzutreiben. Sie bauen Brücken zwischen Streitkräften, Forschung und Industrie.

Der Feind im Kopf – Wie Wahrnehmung Zeitenwende ermöglicht oder verhindert

Jochen Reinhardt, AFCEA Vorstand Presse & Medien, Leitung Communications & Marketing BWI GmbH

Jochen Reinhardt

Foto: BWI GmbH

Der 24. Februar 2022 markiert für die deutsche Verteidigungs- und Sicherheitspolitik eine Zeitenwende. An diesem Tag griff Russland in einer groß angelegten Militäroffensive die Ukraine an. Seither hat die Frage der Wehrhaftigkeit Deutschlands eine ganz neue Bedeutung bekommen. War die Verteidigungspolitik bis dahin vom „freundlichen Desinteresse“ gegenüber der Bundeswehr (Bundespräsident Horst Köhler 2005) geprägt, die in fernen Auslandseinsätzen begrenzt eingesetzt wird und Deutschland ansonsten von der Friedensdividende profitiert, stellte Bundesverteidigungsminister Boris Pistorius im Oktober 2023 die „Kriegstüchtigkeit“ von Bundeswehr und Gesellschaft in den Mittelpunkt. Das Ziel, zwei Prozent des Bruttoinlandsprodukts für Rüstung auszugeben, ist seither akzeptiertes Ziel. Einher geht auch eine digitale Zeitenwende in der Bundeswehr. Konflikte sind immer stärker digital und technologisch geprägt. Um in Konflikten die Informations-, Führungs- und Wirkungsüberlegenheit zu erhalten, muss die Bundeswehr mindestens technologisch Schritt halten.

Die Nationale Sicherheitsstrategie der Bundesregierung hat vor dem Hintergrund der Zeitenwende folgendes Ziel formuliert: „Unser Land muss wehrhaft sein, um sich und seine Verbündeten schützen und verteidigen zu können. Unsere Gesellschaft und Volkswirtschaft müssen resilient sein, um sich entfalten und behaupten zu können: widerstandsfähig, anpassungsfähig und im Inneren gefestigt.“

Auf das formulierte Ziel der wehrhaften Gesellschaft hinzuarbeiten, gehört mehr als nur Führungs- und Regierungsarbeit. Es ist ein gesellschaftliches Verständnis. Dies zu erreichen und zu begleiten ist ausdauernde Kommunikationsarbeit für Politik und Staat genauso wie für gesellschaftliche Gruppen von der sicherheits- und verteidigungspolitischen Community aus Verbänden, Unternehmen und Wissenschaft, um Akzeptanz, Verständnis und idealerweise Beteiligung zur Erreichung des Ziels einer resilienten Gesellschaft in einer veränderten Sicherheitslage.

Kommunikativ stehen die Akteure dabei vor vielfältigen Herausforderungen:

- **„Es war doch alles gut.“** Den notwendigen gesellschaftlichen, rechtlichen und wirtschaftlichen Veränderungen stehen enorme Beharrungskräfte entgegen. Der Status quo aus üppiger Friedensdividende, einer dreifachen Nulltarifpolitik (kostenlose Sicherheit durch die USA, günstige Energie aus Russland und günstige Technologieproduktion aus China) sowie das Fehlen einer unmittelbaren, kurzfristigen negativen Wirkung durch fortgesetztes tradiertes Verhalten wirken vielversprechender als eine oft nur vage gezeichnete neue sichere Zukunft. Bekannte, gelernte und eingeschliffene Verhaltensweisen und Abläufe wollen nicht für neue Geschäftsmodelle, Kooperationen oder agilere Methoden aufgegeben werden.
- **„Der Krieg ist weit weg.“** Es fehlt noch immer die Erkenntnis über die Bedrohungslage und damit die Handlungsnotwendigkeit. Unmittelbar hat die neue Situation keine Wirkung für das Individuum.
- **„Aber andere Dinge sind auch wichtig.“** In der Wahrnehmung konkurrieren verschieden Krisen. Hybride und Cyberangriffe, Energie, Inflation, Migration oder Gendern: Die Aufzählung zeigt: Was gesellschaftlich wichtig ist, spiegelt sich in der veröffentlichten Bedeutung wider. Wahrnehmung ist verzerrt oder steht nicht in größeren Zusammenhängen.
- **„Die nächste Sau kommt.“** In der Medienberichterstattung folgt der Krieg und die sicherheitspolitische Zeitenwende dem typischen Wahrnehmungszyklus. Zu Beginn ist das Thema durch hohes Interesse und intensive Berichterstattung geprägt, die über die Zeit abflacht. Das ist unabhängig davon, wie sich 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.
- **„Alternative Fakten“**: Immer stärker erodiert in der politischen Debatte der gemeinsame, akzeptierte Grund, was Tatsachenrealität ist. Meinung ersetzt Fakten, Wissenschaft ist ein Interpretationsangebot unter vielen. Was bleibt, ist ein reiner Kampf der Narrative.

Sowohl AFCEA Bonn e.V. als neutrale Dialogplattform als auch seine Mitglieder aus Industrie, Wissenschaft und Bundeswehr – und natürlich die Bundeswehr als solche, ebenso wie Verwaltung und Staatsführung haben eine Fülle von Lösungsansätzen, diese Herausforderungen zu adressieren und das Ziel gesellschaftlicher Resilienz nach der sicherheitspolitischen Zeitenwende zu verankern und erfolgreich zu begleiten.

1. **Klarer Purpose, klare Ziele:** Lange Veränderungszyklen benötigen eine klare Zielausrichtung und eine klare,

nachvollziehbare Begründung. Jegliche Kommunikation und Handlung sollte daher mit dem „Sense of Urgency“ aufgeladen werden, um sie immer mit dem gesellschaftlichen Ziel zu verknüpfen. Eine zusätzliche konkrete Ambition zum Ziel hilft dabei. Ähnlich wie das 2-Prozent-Ziel der NATO könnte das auch der Wertschöpfungsanteil der Branche, die nationale Unabhängigkeit oder ein Führungsanspruch in der EU sein.

2. **Klare Verbindung zum konkreten Handeln:** Das gesellschaftliche Ziel von Resilienz darf dabei kein abgehobenes Ziel sein, sondern benötigt klare Wirkungen und Vorteile sowohl für einzelne gesellschaftliche Akteure als auch für Individuen.
   Diese können beispielsweise der gesellschaftliche Beitrag zur Stärkung Deutschlands, zu seiner Sicherheit, Fortschritt oder Einigkeit sein. Genauso relevant kann und muss der individuelle Nutzen herausgearbeitet werden – etwa die Sicherheit vor Angriffen und die eigene Unversehrtheit. Wichtiger jedoch sind positive Auswirkungen wie etwa Wirtschaftswachstum und Transformation in Branchen wie Rüstung, Sicherheit und Technologie. Daraus ergeben sich positive Aspekte für den Einzelnen wie etwa die Aufwertung des eigenen Arbeitsplatzes, neue Arbeitsplätze und Entwicklungsmöglichkeiten.
3. **Mehr als nur Waffensysteme:** Die Bundeswehr spielt eine grundlegende Rolle bei der Wehrhaftigkeit Deutschlands. Doch zu einer gesellschaftlichen Resilienz gehört weit mehr. Ohne Digitalisierung ist heute kein Kampf mehr zu gewinnen. Ohne erneuerbare Energien beispielsweise ist in einem rohstoffarmen Deutschland die Reduktion von Abhängigkeiten nicht möglich. Ohne Bürokratieabbau sind schnellere Anpassungen an Entwicklungen nicht möglich. Solche Zusammenhänge sind deutlich zu machen, damit Verteidigung nicht auf Beschaffungsvorhaben und Zahlen von Waffensystemen reduziert wird.
4. **Fokus behalten:** IInsbesondere die Community kann einen entscheidenden Beitrag dazu leisten, dass die Wahrnehmung der Transformation zu einer resilienten Gesellschaft verbessert wird. Dazu ist der Fokus auf den eigenen Beitrag, das gemeinsam Geleistete und zu leistende klar in den Fokus zu stellen und auch gegen weniger relevante Debatten mit krisenhafter Wahrnehmung aber ohne tatsächliche Krise selbstbewusst zu positionieren.
5. **Standhaftigkeit:** Nicht alle Positionen, Aussagen und Botschaften werden einen gesellschaftlichen Konsens finden. Dies kann auch nicht das Ziel sein. Die aktuell bestehende Akzeptanz für die Bundeswehr, ihre Notwendigkeit zur weiteren Digitalisierung und Modernisierung sowie zu einer veränderten Sicherheitspolitik ist grundsätzlich und weitgehend gegeben. Daran aufzusetzen und das Thema voranzubringen, ist jetzt Führungs- und Kommunikationsaufgabe. Dabei dürfen Beiträge zur gesellschaftlichen Debatte weder politisch noch populistisch anbiedern. Dafür ist die Sicherheit des Landes zu bedeutend.

AFCEA – die zentrale IT-Messe für den Verteidigungs- und Sicherheitsbereich

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

Wolfgang Quirin

Foto: AFCEA Bonn e.V.

Der Krieg in der Ukraine tobt weiter, im Nahen Osten kehrt kein Friede ein, ein Machtwechsel in Syrien mit all den Ungewissheiten über die Zukunft des Landes, aber auch Spannungen in Fernost wie etwa die China-Taiwan Frage oder Nordkoreas Rüstungsprogramm, und nicht zu vergessen die Unruhen in verschiedenen Ländern Afrika – all das unterstreicht die Wichtigkeit der eigenen Wehrhaftigkeit und Krisenvorsorge in einer sich sehr schnell wandelnden Weltlage.

Dazu ist eine abgestimmte Zusammenarbeit zwischen Regierung, Industrie, Forschung und Bildungseinrichtungen unerlässlich, um die unterschiedlichen Themenfelder zusammenzubringen, Chancen zu identifizieren und Potenziale zu heben.

Dies erfordert erhebliche Investitionen in Forschung und Entwicklung, Bildung, Infrastruktur und vieles mehr, um die nationale Souveränität im Zeitalter neuer sicherheitspolitischer Herausforderungen und disruptiver IT-Technologien in allen Dimensionen, einschließlich des Weltraums zu stärken und gleichzeitig globale Herausforderungen anzugehen. Hierzu bringt die fünfte AFCEA Fachausstellung im World Conference Center Bonn (WCCB) wieder Bundeswehr, Sicherheitsbehörden, Verwaltung, Industrie, Wissenschaft und Bildungseinrichtungen zusammen.

AFCEA Fachausstellung

AFCEA Bonn e.V. als neutrales, nationales Netzwerk zum Austausch über Themen der Informations- und Kommunikationstechnik bietet mit der AFCEA Fachausstellung als Treffpunkt der IT-Community Bundeswehr und Firmen und Organisationen aus dem Bereich Sicherheit im WCCB weiterhin die gewohnt informative Plattform für ”IT zum Anfassen”.

Die diesjährige AFCEA Fachausstellung bietet ideale Möglichkeiten, Beratungs- und Verkaufsgespräche zu führen, Produkte und Dienstleistungen vorzustellen, innovative Ideen zu präsentieren, den Bekanntheitsgrad der eigenen Firma zu steigern, Business to Business Geschäftsbeziehungen auszubauen und neue Kontakte zu knüpfen bzw. bestehende Kontakte zu vertiefen.

Nirgendwo sonst trifft man auf eine so große Anzahl an Fachpublikum sowie Firmen und Organisationen aus dem Bereich der öffentlichen und privaten Sicherheitsaufgaben. Die vierte AFCEA Fachausstellung im Word Conference im Juni 2024 zeigte allein durch die Zahl der Aussteller (rund 250) und der über 4.500 Teilnehmer wieder das überwältigende Interesse an dieser Veranstaltung. Das lag unter anderem am neuen, erweiterten Format der AFCEA Fachausstellung, das aufgrund der guten Resonanz für die AFCEA Fachausstellung 2025 ausgebaut wird.

Bis auf den letzten Stand ausgebucht: Die AFCEA Fachausstellung im WCCB

Die AFCEA Fachausstellung 2025 enthält neue, traditionelle und bekannte Elemente:

- Ausstellung auf den acht Ausstellungsflächen
- Industrievorträge von Firmen und Fachvorträge von Organisationen zu verschiedenen BOS-relevanten Themen im Plenarsaal und im Saal Addis Abeba 3
- Ein Symposium zu aktuellen militärpolitischen Brennpunktthemen
- Ein Get-together am Dienstagabend von 18 bis 22 Uhr auf der Ausstellungsfläche Rheinebene
- Inhaltlich-methodischer Workshop mit Teilnehmenden aus dem Bundeswehrumfeld zu verschiedenen sicherheitsrelevanten Themen.
- Eine DigitalDefenceDebate, eine Podiumsdiskussion mit ranghohen Teilnehmern.
- Zwei parallele Panels von kurzen Industrievorträgen der Aussteller in 31 Vortragsslots, ferner auch die Präsentation von Startups (Pitch Session) durch die Emerging Leaders AFCEA Bonn e. V.
- Eine NEUE Sonderausstellungsfläche für Startups zu vergünstigten Ausstellungs-konditionen.
- Ergänzung der Fachausstellung durch ein Recruiting Element, organisiert in Kooperation mit dem Berufsförderungsdienst Köln

- Liveberichtserstattung von der AFCEA Fachausstellung
- Cateringbereich auf der Rheinebene
- Digitale Werbemöglichkeiten für Aussteller.

Mit der Schaffung der „DigitalDefenseDebate“ haben die Emerging Leaders AFCEA Bonn e.V. ein besonderes Veranstaltungsformat geschaffen. So werden auch Personen angesprochen, die bisher eher selten in der „Verteidigungsbubble“ anzutreffen waren, z.B. Vertreter und Vertreterinnen aus Startups, Venture Capital und junge Sicherheitspolitiker und Sicherheitspolitikerinnen. Dieses virtuelle Format setzt die richtigen Impulse und ist somit geeignet, auch dieses Jahr auf der Bühne der Fachausstellung seinen Platz einzunehmen.

Interessierte Zuhörer bei den Industrievorträgen

Industrievorträge

Die Industrievorträge werden wieder in zwei Räumlichkeiten des WCCB durchgeführt.

Im sehr prominenten Plenarsaal des WCCB werden 18 Speaker-Slots in neuem Format zur Auswahl stehen. Die zweite Vortragsräumlichkeit wird wieder im Raum Addis Abeba 3 mit insgesamt 17 Speaker-Slots stattfinden. Beide Vortragsräumlichkeiten sind ausschließlich über die Rheinebene erreichbar.

Für Aussteller, die einen Speaker-Slot gebucht haben, besteht die Möglichkeit, im Rahmen dieses Formats in einem Kurzvortrag von 20 bis 25 Minuten auf die Produkte und Dienstleistungen ihres Unternehmens hinzuweisen. Die ersten Abstracts zu den Vorträgen sind auf der AFCEA Homepage einzusehen.

Die gedruckte ”Broschüre Industrievorträge” finden die Besucher der AFCEA Fachausstellung 2025 am Eingang sowie am Eingang zu den beiden Vortragsräumlichkeiten. Selbstverständlich wird die Broschüre auch digital als PDF zum Downloaden bereitgestellt.

Startups

Damit junge Startups die Vernetzungsmöglichkeiten der AFCEA Fachausstellung ausschöpfen und ihre innovativen Produkte vorstellen können, haben wir, gemeinsam mit unseren Emerging Leader, eine „Sonderausstellungsfläche für Startups” neu eingerichtet.

Die ausgewählten jungen Unternehmen dürfen ihre innovativen Konzepte, Produkte und Dienstleistungen den Besuchern darstellen. Zudem wird eine Startup-Pitch Session im Plenarsaal durchgeführt. Gleichzeitig werden diese jungen Unternehmen in der eKompetenzmatrix mit Kompetenzen und Firmenprofil und im AFCEA Heft genauso beworben wie die anderen Aussteller.

Einer der größten Herausforderung der heutigen Zeit – dem Fachkräftemangel – nimmt sich die Fachausstellung ebenfalls wieder an. Gemeinsam mit dem Berufsförderungsdienst der Bundeswehr werden im Rahmen des neuen Recruitingelements, Mitgliedsfirmen von AFCEA und die Aussteller der Fachausstellung offene Stellen anbieten können. Darüber hinaus wird es Vorträge zur heutigen Marktsituation geben und Besuchern der AFCEA Fachausstellung (zum Beispiel ausscheidenden Zeit und Berufssoldaten) niedrigschwellige Möglichkeiten der Kontaktaufnahme mit potenziellen Arbeitgebern angeboten.

Gefüllte Ränge bei den Vorträgen *Alle Fotos: AFCEA Bonn e.V.*

eKompetenzmatrix

Die „eKompetenzmatrix“ (entwickelt von unserer Mitgliedsfirma CGI) wird auch bei der AFCEA Fachausstellung 2025 wieder zur Verfügung stehen. Sie dient der Orientierung der Besucher über die vielfältigen Angebote der Aussteller und wird auch dieses Jahr als datenbankbasierte, komfortable Webanwendung von unserer AFCEA-Mitgliedsfirma CGI zur Verfügung gestellt. Bei mehr als 200 Ausstellern erleichtert diese den Besuchern, die sich bei der AFCEA Fachausstellung zu einem spezifischen Thema informieren wollen, zielgenau diejenigen Aussteller zu finden, die am meisten zu dem jeweiligen Thema beitragen können.

Besucher können in der eKompetenzmatrix aus über 70 Kompetenzen diejenigen auswählen, die sie besonders interessieren, worauf die eKompetenzmatrix dann exakt diejenigen Aussteller anzeigt, bei denen die Besucher zu dem gewählten Thema/Kompetenz fündig werden.

Als weiteren messeunterstützenden Service wird auch die MesseApp wieder durch unsere Mitgliedsfirma Capgemini zur Verfügung gestellt, die ihnen alle wichtigen Informationen auf ihr Handy liefert.

Das Get-together am Dienstagabend von 18 bis 22 Uhr bietet bei Speisen und Getränken die Möglichkeit interessante Gespräche zu führen, Geschäftsbeziehungen zu festigen und ein erfolgreiches Networking zu betreiben.

Wir freuen uns, sie zur AFCEA Fachausstellung 2025 am 27. und 28. Mai 2025 im World Conference Center Bonn willkommen zu heißen.

Die Veranstaltungen von AFCEA Bonn e.V. im Überblick

Alle Veranstaltungen des Jahres

Foto: AFCEA Bonn e.V.

Flaggschiff-Veranstaltungen (einmal pro Jahr):
Die AFCEA Fachausstellung ist die größte Veranstaltung im Jahresprogramm des gemeinnützigen Vereins. Alljährlich trifft sich dort die IT-Community der Bundeswehr im Bereich Führungsunterstützung, Nachrichtengewinnung und Aufklärung, GIS, IT-Sicherheit, Simulation, Ausbildung, Logistik und SASPF im World Conference Center Bonn (WCCB). Auch immer mehr Unternehmen, Organisationen und Amtsvertreter aus dem Bereich der Inneren und Öffentlichen Sicherheit besuchen die Fachausstellung. Erstmalig 1986 durchgeführt gehört die AFCEA Fachausstellung mit rund 250 Ausstellern und über 4.000 Teilnehmern zu wichtigsten IT-Messen Deutschlands.

Koblenzer IT-Tagung und Bonner IT-Dialog im Wechsel mit dem BAAINBw und dem Kdo CIR
Die Koblenzer IT-Tagung im Herbst befasst sich mit der Unterstützung des Einsatzes von Streitkräften durch leistungsfähige Informations- und Kommunikationstechnik und blickt auf das Jahresthema aus verschiedenen Perspektiven mit dem Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAAINBw). konzentriert. Seit 2004 (damals noch unter dem Titel „Koblenzer Fachtagung IT“) steht die gemeinsame Veranstaltung von AFCEA Bonn e.V. im Wechsel mit dem Bonner IT-Dialog und dem Kdo CIR und im Folgejahr mit dem BAAINBw unter der Schirmherrschaft der Koblenzer Oberbürgermeister.

Parlamentarischer Abend (einmal pro Jahr):
Die Parlamentarischen Abende in Zusammenarbeit mit dem Branchenverband bitkom haben sich mittlerweile jährlich etabliert. Die Abende in der Parlamentarischen Gesellschaft in Berlin greifen mit hochrangigen Vortragenden aus der Politik, der Bundeswehr oder der NATO relevante Führungs- und IT-Themen auf, diskutieren sie mit IT-affinen Parlamentariern und tragen zur Meinungsbildung bei.

Partner-Events (zwei- bis viermal pro Jahr)
Als Austauschplattform tragen Partner-Events als gemeinsame Veranstaltungen mit Vereinen, Verbänden oder Organisationen zur thematischen Vertiefung bei. Mit dem BDSV (Bundesverband Deutschen Sicherheits- und Verteidigungsindustrie) findet jährlich der Konvent zur Digitalen Konvergenz in Berlin statt. Ebenfalls in Berlin und jährlich haben die Emerging Leaders AFCEA Bonn e.V. (ELA) mit dem bitkom im Cyber Innovation Hub der Bundeswehr eine Veranstaltungsreihe etabliert. Darüber hinaus ergänzen weitere gemeinsame Veranstaltungen mit unterschiedlichen Partnern (beispielsweise der BWI GmbH als Digitalisierungspartner der Bundeswehr) das Jahresprogramm.

Mittagsforum (bis zu zweimal pro Jahr)
Zweimal jährlich bietet AFCEA Bonn e.V. seinen Mitgliedsfirmen mit dem Mittagsforum die Möglichkeit, sich mit ihren Themen vorzustellen.

Zukunfts- und Technologieforum (einmal pro Jahr)

Zur technologischen Ergänzung des Spektrums der AFCEA-Veranstaltungen wurde diese Veranstaltungsreihe im Jahre 2010 mit Fraunhofer FKIE ins Leben gerufen. Sie richtet sich an Fachexpertinnen und -experten aus Technik, Wissenschaft und Weiter- und Konzeptentwicklung. Sachkundige Teilnehmer stellen neue und sich entwickelnde Technologien vor, die für den Bereich Sicherheit und Verteidigung relevant sind. Die Agenda lässt stets ausreichend Zeit, um technische Details zu hinterfragen und ausführlich zu diskutieren.

Fachveranstaltungen (vier- bis fünfmal pro Jahr)

Die Fachveranstaltungen von AFCEA Bonn e.V. greifen aktuelle Themen der Informations- und Kommunikationstechnik auf, die von einem besonderen Interesse für die Bundeswehr sowie für die Behörden und Organisationen mit Sicherheitsaufgaben sind. Einen Schwerpunkt bildet dabei die Verbesserung der Führungsfähigkeit im Einsatz. In der Ausgestaltung werden dabei nicht nur Fachveranstaltungen mit Schwerpunktthemen organisiert, sondern jeweils auch eine Fachveranstaltung gemeinsam mit einem Organisationsbereich der Bundeswehr und speziell für Behörden und Organisationen mit Sicherheitsaufgaben (BOS).

ELA-Veranstaltungen (zwei bis dreimal pro Jahr)

Die Emerging Leaders AFCEA Bonn e.V. als Vereinsteil für junge Fach- und Führungskräfte bis zum Alter von 40 Jahren, bringen sich mit verschiedenen Veranstaltungen und Formaten ins Jahresprogramm von AFCEA Bonn e.V. ein. Dazu gehört beispielsweise die gemeinsame Veranstaltung mit dem Branchenverband Bitkom im Cyber Innovation Hub (CIH) der Bundeswehr in Berlin. Seit 2023 veranstalten die ELAs das Format BONNF1RE – in Anlehnung des englischen Begriffs für Lagerfeuer – ein modernes Kaminabend-Event zum intensiven Austausch in Bonn sowie eine Digital Defence Debate (DDD) online oder bei der Fachausstellung mit interessanten Gästen aus Politik, Behörden, Wissenschaft oder Lehre.

Mitgliederversammlung (jährlich)

Einmal jährlich führt AFCEA die satzungsgemäße Mitgliederversammlung in Präsenz durch.

https://www.afcea.de/veranstaltungen/veranstaltungsformate-afcea-bonn-ev.html

Sicher.
Verbunden. Jederzeit.

AUFKLÄRUNG

KOMMUNIKATION

NAVIGATION

Ihr Systemhaus für die Dimension Raum.

Globale, zuverlässige, flexible, sichere und verteidigungsfördernde Vernetzung ist für unsere Streitkräfte unverzichtbar. Die mit dem Heinrich-Hertz-Satelliten wiedergewonnene Systemfähigkeit in Deutschland und die zukünftige Nutzung der vollelektrischen Small-GEO-Plattform zur Frequenz- und Fähigkeitssicherung im Rahmen von SatcomBW Level 3 leisten hierzu einen wichtigen Beitrag.

Die Entwicklung nicht-geostationärer Satellitensysteme in MEO und LEO mit dem Ziel, die Resilienz, Flexibilität, Verteidigungsfähigkeit und Funktionalität durch Software Defined Defence (SDD) mittels rollierender Beschaffung und schrittweisem Fähigkeitsaufbau deutlich zu erhöhen, wird die Kommunikationsfähigkeit der Streitkräfte für die Zukunft sichern. Langfristig kommen wir dadurch von der Systemfähigkeit in Deutschland zur Technologieführerschaft in der militärischen Weltraumnachrichtentechnik und zu Synergien für die zukünftige digitale Verkehrsinfrastruktur.

Angesichts der begrenzten verfügbaren militärischen Frequenzen und der damit verbundenen Nutzungsrechte, ist es von entscheidender Bedeutung, solche umlaufenden Satellitensysteme zeitnah zu realisieren und die Frequenzrechte im nationalen Interesse langfristig zu sichern.

We. Create. Space.

Bechtle AG:
Ihr starker IT-Partner im Public Sector

Das Thema Multi-Cloud zieht sich quer durch die zahlreichen Bereiche der Bundeswehr (digitale Lagebilder, Krisenfrüherkennung, Multi-Domain-Operation) und bringt eine Reihe von Herausforderungen mit sich. Bechtle hat nicht nur dafür die passenden Lösungen, die ebenso sicher wie innovativ sind. Auch beim Einsatz von KI-Anwendungen, No-Code-Lösungen und Open-Source-Produkten ist Bechtle führend.
Den entscheidenden Schritt voraus ist der, der die neusten Technologien und Entwicklungen kennt, versteht und zum Vorteil seiner Auftraggeber anwenden kann. Bechtle ist das zukunftsstarke Fundament dafür – mit langjähriger Erfahrung, weitreichender Kompetenz und einem leistungsfähigen Netzwerk.
Auf dieser Basis hat sich Bechtle auch in den Bereichen Sicherheit und Verteidigung als innovationsgetriebener, leistungsstarker, zuverlässiger und herstellerunabhängiger IT-Partner etabliert, der überzeugende Konzepte und passgenaue Lösungen aus einer Hand anbietet – in Deutschland und Europa, wie beispielsweise der Gewinn des Rahmenvertrags R1753 (IT-Plattform 2./3. Rechnerebene: Hardware, Integration, Projektmanagement, Services etc.) zeigt.
Das Produkt- und Dienstleistungsportfolio umfasst dabei die Bereiche Handelsware mit mobilen Endgeräten, PCs, Peripherie, Drucker, Server, Speichersysteme, USV-Anlagen sowie hardwarenahe Softwareprodukte. Neben der Lieferung von Informationstechnik plant, installiert und konfiguriert Bechtle auch gesamte IT-Umgebungen und Netzwerke. Dazu gehören IT-Sicherheitskonzepte (InfoSichK nach Vorgaben Z.Dv. A-960/1 in SAVe), Service- & Systemsteckbriefe, Enterprise Architecture nach NATO Architecture Framework (NAF) sowie Teilekennzeichnung (TKZ) von Geräten, Gütern und Behältern (TuLB/TuBB) mit grafischen Codierungen und Nummernkreisen.

Nutzer & Dienststellen profitieren zudem von der dezentralen Struktur von Bechtle: Mit den IT-Systemhäusern gibt es stets einen kompetenten Ansprechpartner in der Nähe, dem das Know-how des dedizierten Geschäftsbereichs Public Sector sowie die Leistungsstärke des gesamten Unternehmens zur Verfügung stehen.
Zu den öffentlichen Kunden von Bechtle zählen neben der Bundeswehr und Dataport auch zahlreiche Bundesministerien, Landesverwaltungen und Universitäten sowie das niederländische Innenministerium, die Europäische Kommission und die NATO.

Über Bechtle

Bechtle ist mit über 100 IT-Systemhäusern nah an den Standorten der Nutzer & Dienststellen und zählt mit IT-E-Commerce-Gesellschaften in 14 Ländern zu den führenden IT-Unternehmen in Europa. Das herstellerübergreifende Produkt- und Leistungsportfolio reicht von (Standard- und Individual-) Hard- und Software, Open Source Produkten, Hybrid- und Multi-Clouds, Managed Service hin bis zu disruptiven digitalen Lösungen. Bechtle begleitet bei KI-Lösungen, Quantentechnologien und Cybersicherheit. Damit bietet das IT-Unternehmen ein breites Spektrum an Produkten und Dienstleistungen rund um IT-Infrastruktur und Betrieb. Gegründet 1983, beschäftigt Bechtle Group derzeit über 15.800 Mitarbeitende. 2024 lag der Umsatz bei rund 6.305 Mio. €.

Kontakt:

Bechtle AG
Gabor Jeszenoei
Zentrales Team Bundeswehr
Telefon: 0228 6888 400
Email: zpls-r1753@bechtle.com
Web: www.bechtle.com

Die Digitalisierung der Streitkräfte vor dem Hintergrund der Zeitenwende aus industrieller Sicht

Dr. Hans Christoph Atzpodien, Hauptgeschäftsführer des Bundesverbands der Deutschen Sicherheits- und Verteidigungsindustrie (BDSV) e.V.

Dr. Hans C. Atzpodien

Foto: Illing&Vossbeck

Sehr geehrte Leserinnen und Leser dieses AFCEA-Sonderheftes, das wir wieder in Kooperation unserer beiden Verbände – AFCEA Bonn e.V. und BDSV e.V. – gestalten dürfen. Die Veröffentlichung dieser Publikation fällt in eine höchst spannende, um nicht zu sagen angespannte Zeit. Rund um die Münchner Sicherheitskonferenz im Februar 2025 gab es durch die Äußerungen der Trump-Administration eine gefühlte „Zeitenwende 2.0“. Ein weiterer, sehr wichtiger Einfluss geht von den Erfahrungen des Ukraine-Krieges aus. Hierbei geht es vor allem den Einsatz und die Bekämpfung von Drohnen, neue Entwicklungen rund um den elektronischen Kampf, um KI-gestützte Lagebild-Analyse sowie um die Vernetzung aller im Gefechtsfeld verfügbaren Datenquellen. Hierdurch werden komplett neue Rahmenbedingungen definiert, die durch höchste Agilität der technischen Entwicklung gekennzeichnet sind. Diese auf einen Rüstungsmodus zu übertragen, wie wir ihn aus „Friedenszeiten“ gewöhnt sind, stellt aktuell eine der großen Herausforderungen für die Bundeswehr-Beschaffung und für die industriellen Ausrüster dar. Wie die Industrie-Beiträge in diesem Heft deutlich machen sollen, sehen sich die BDSV-Mitgliedsunternehmen absolut in der Lage, diesen Herausforderungen mit ihren Produkten zu entsprechen, und zwar zeit- und anforderungsgerecht.

Softwarelösungen zur Digitalisierung der Streitkräfte sind dabei ein absolut querschnittliches Thema, das zum raschen Fähigkeitsaufwuchs in allen Dimensionen beiträgt. Digitalisierung ist „key“ zur Verbesserung der Führungs- und Kommunikationsmöglichkeiten, zur besseren Lagebilderstellung und -analyse und zur Bereitstellung innovativer Lösungen für die vielfältigen logistischen Herausforderungen zur Ermöglichung der „Drehscheibe Deutschland“. Digitalisierung leistet einen entscheidenden Beitrag zur Erlangung der „Kriegstüchtigkeit“, wie sie Minister Pistorius und Generalinspekteur Breuer zu Recht seit Herbst 2023 immer wieder gefordert haben. Diese Forderung bezog sich nicht alleine auf die Bundeswehr, sondern auch auf die gesamte Gesellschaft und unsere zivile Resilienz. Hier liegt ein weiteres Anwendungsfeld, für das Digitalisierung absolut unverzichtbar ist. Wir sehen dies derzeit im Bereich der Behördenvorgänge rund um Migration, aber auch in anderen Bereichen der öffentlichen Verwaltung, die uns als Bürger unmittelbar betreffen. Vom „Digitalen Staat“ sind wir in Teilen noch weit entfernt.

Es bleiben also noch zahlreiche Herausforderungen im Kontext von Digitalisierung und Sicherheit sowie Verteidigung, die unsere Mitgliedsunternehmen mit ihrer technologischen Spitzen-Kompetenz und entsprechenden Produktentwicklungen immer wieder proaktiv annehmen. Wichtig ist, dass die Unternehmen bei der Identifizierung neuer Technologien und deren rascher Integration und Skalierung nicht – wie es derzeit leider der Fall ist – durch allzu belastende bürokratische Verfahren behindert werden. Angesichts immer agilerer Methoden und Verfahren würde dies die Fähigkeit unserer Industrie, die Anforderungen ihrer Kunden bestmöglich zu bedienen, zunehmend einschränken. Zusammenfassend aber bleibt es dabei, dass wir als deutsche Sicherheits- und Verteidigungsindustrie auch in der „Zeitenwende 2.0“ liefern können, was unsere Kunden benötigen. Voraussetzung ist, dass die neue Bundesregierung möglichst schnell die haushalterischen Weichen dafür stellt, klare Aufträge erteilt werden und die Rahmenbedingungen für den schnellen Aufbau weiterer Kapazitäten verbessert werden. An Ideen und innovativen Produkten mangelt es nicht. Jetzt müssen die notwendigen Schritte unternommen werden, um das Potential von IT- und softwaregestützten Lösungen zu heben. Deutschland braucht es und die deutsche Sicherheits- und Verteidigungsindustrie hat es!

CAE: Decision Support, Missionsplanung & Ausbildung

Matthias Schrade, Dipl.-Ing., EMEA Region Chief Architect, CAE GmbH

Der digitale, interaktive Sandkasten *Foto: CAE*

Matthias Schrade *Foto: CAE*

Problemstellung

Digitalisierung und Digitale Konvergenz lassen nicht nur die Grenzen zwischen Plattformen und IT Equipment verschwimmen, auch die Nutzung von Ausrüstung wird neu gedacht. Bislang gab es häufig eine strikte Trennung zwischen operationeller Ausrüstung, Planungs- und Ausbildungsmitteln. Der in letzter Zeit regelmäßig auftauchende Begriff „Train as you fight“ weist bereits in die richtige Richtung, greift aber zu kurz. Benötigt werden integrierte Systeme, die Einsatz, Planung, Aus- und Weiterbildung vereinen. Die Handhabung dieser Systeme muss dabei für jeden Einsatzzweck konsistent, logisch und intuitiv sein. Weiterhin ist erforderlich, dass auch komplexe Vorgänge einfach zu bedienen und die Ergebnisse schnell zu erfassen sind, damit eine Auswertung quasi in Echtzeit stattfinden kann, um eine adäquate Reaktion zu planen und umzusetzen.

Darüber hinaus beschränkt sich dieses Weiterdenken nicht auf die Streitkräfte. Eine hochauflösende, umfassende und eindeutige Sicht auf die Lage (Situation Awareness) ist eine unbedingte Notwendigkeit auch für Sicherheitsorgane und zivile Rettungskräfte. Um wieviel einfacher wäre die Koordination aller Einsatzkräfte beim Hochwasser im Sommer 2021 gewesen, wenn damals entsprechende Hilfsmittel zur Verfügung gestanden hätten.

Visualisierung ist der Dreh- und Angelpunkt der Situation Awareness. Dabei kommt es darauf an, die vorhandenen Daten schnell und übersichtlich darzustellen, alle Informationen bei Bedarf verfügbar zu haben, aber andererseits kognitive Überlastung zu verhindern. Sensor Fusion einerseits und gezielte Informationsdarstellung (Decluttering) andererseits sind hier unabdingbar.

Zur Beurteilung eines Lagebildes ist es notwendig, sich nicht mehr auf statische Bilder oder Karten verlassen zu müssen. Eine dreidimensionale, interaktive Ansicht, die von mehreren Personen betrachtet werden kann, die nicht notwendigerweise an einem Ort versammelt sind, ist das Gebot der Stunde und technisch ohne weiteres möglich. Die Interaktion mit der Datenbasisdarstellung und den Einheiten, sowie das gezielte, kontextabhängige Ein- und Ausblenden von Informationen durch jeden der Teilnehmer, beispielsweise durch Auswertung der Blickrichtung (Gaze Tracking) muss gegeben sein. Ebenso benötigt man Optionen, um Vorgehensweisen interaktiv skizzieren zu können und neben der aktuellen Lagedarstellung auch Szenarien zu planen und durchzuspielen.

Digitalisierung direkt beim Endnutzer.
Ein „digitaler, interaktiver Sandkasten“, der über sichere Weitbereichsvernetzung Teilnehmer aus verschiedensten Hierarchieebenen und Waffengattungen zusammenschaltet, ermöglicht genau dies. Mit einem solchen frei skalierbarem System kann Aus- und Weiterbildung (z.B. unter Nutzung weiterer vorhandener Ausbildungssysteme wie SIRA) dislozierd durchgeführt werden. Man kann aber darüber hinaus in Echtzeit taktische Lagebeurteilung erstellen (beispielsweise unter Einbindung von SitaWare), simulationsgestützte Planung durchführen, bei der durch das Durchspielen verschiedener Optionen die Entscheidungsfindung unterstützt wird, und letztlich auch die Durchführung der Operation überwachen.
CAE hat das CAERidge™ System unabhängig von der dahinterliegenden Hardwareplattform entwickelt, um allen Notwendigkeiten gerecht werden zu können. Je nach Einsatzzweck kann also ein starker Backbone mit Echtzeitservern und PC Clients zur Anwendung gebracht werden, die Planung und Operation Support in Kommandozentralen unterstützen, oder ebenso Laptops, Tablets, Smartphones oder Lightweight Augmented Reality Brillen, die auch im Feld eine Übersicht über die aktuelle Lage ermöglichen. Die Einbindung von Echtzeitdaten, physikalischen Simulationsmodellen, Sichtweiten und -bereichen, Ausbreitungsmodellen von Radiowellen, Wetter- und Tageszeitdarstellung u.v.m. bei Nutzung von hochauflösenden Geländedatenbasen in offenen, standardisierten Formaten bringen den benötigen Mehrwert gegenüber konventionellen Methoden. Resilienz und Informationssicherheit runden das ganze System ab. Die gegenwärtige Nutzung des Systems im Zentrum Simulations- und Navigationsunterstützung Fliegende Waffensysteme der Bundeswehr ist nur ein Beispiel, wie flexibel und für welch unterschiedliche Zwecke CAERidge™ genutzt werden kann. Des Weiteren eröffnet die hardwareunabhängige Vorgehensweise die Möglichkeit, kontinuierliche Verbesserungen im Sinne von Software Defined Defence (SDD) durchzuführen.

Geschwindigkeit durch Software: Der Wandel der wehrtechnischen Industrie

John C. Eisenhauer, Partner / Head of Defence; Aida Stelter, Fachexpertin Defence; Torsten Stimmel, Fachexperte Defence; Dietmar Bernreuther, Fachexperte Software Excellence; Detecon International GmbH

Aida Stelter

Foto: Detecon

Die fortschreitende Digitalisierung macht auch vor dem Verteidigungssektor nicht halt. Ein zentraler Aspekt von Software Defined Defense (SDD) ist der kürzere Lebenszyklus von Software im Vergleich zu Hardware. Während Plattformen wie Fregatten oder Kampfjets 30 bis 50 Jahre im Einsatz sind und Hardware alle 10 bis 15 Jahre erneuert wird, erfolgt die Softwareaktualisierung regelmäßig in Zyklen von Wochen bis Monaten – bei sicherheitskritischen Updates unter Umständen sogar innerhalb weniger Tage bis Stunden.

Softwarebasierte Sicherheitssysteme können schnell an neue Bedrohungen angepasst werden, wodurch ein strategischer Vorteil entsteht. Ein aktuelles Beispiel zeigt, wie ein Hersteller eines Schutzsystems für Kampfpanzer (APS) ein bestehendes System durch „einige Software-Upgrades und geringfügige Änderungen an der Hardware“ in die Lage versetzte, Drohnen abzufangen. Diese Fähigkeit, durch Software-Updates schnell neue Funktionen zu integrieren, wird zunehmend entscheidend für Streitkräfte, die wehrtechnische Industrie und KRITIS-Organisationen.

Die Beherrschung des hochdynamischen Software-Lebenszyklus stellt Hersteller, Betreiber und Nutzer von softwaregetriebenen wehrtechnischen Produkten vor neue Herausforderungen. Wer SDD erfolgreich umsetzen will, benötigt:

- ein Software-gerechtes Produktdesign
- eine Software-unterstützende Organisation
- eine Software-orientierte Unternehmenskultur sowie
- eine Software-getriebene Strategie

Software-gerechtes Produktdesign: Die Produktarchitektur muss sowohl auf Gesamtsystem- als auch Hardware-Ebene darauf ausgelegt sein, schnelle Softwareanpassungen zu unterstützen. Dazu gehören:

- Standardisierung und Abstrahierung von Hardware-Komponenten durch einen Hardware Abstraction Layer (HAL), um Software vom Hardware-Lifecycle zu entkoppeln
- Verschiebung von Funktionalität in den Software-Layer (Softwareization), um Software-Anpassungen überhaupt zu ermöglichen

Software-Defined Defense sollte nicht nur rein technisch über die Produktdimension betrachtet werden, sondern betrifft auch organisatorische, kulturelle und strategische Aspekte.

Grafik: Detecon International GmbH

- Einplanung von Ressourcenpuffern bei Rechenleistung, Speicher und Bandbreiten für zukünftige Funktionsaufwüchse, insbesondere durch den absehbar steigenden Ressourcenbedarf durch KI
- Modularisierung und lose Kopplung von Diensten, z.B. durch Microservice-Architekturen und Containerisierung von Anwendungen, um die schnelle Anpassung und Verteilung einzelner Modulbausteine zu ermöglichen

Dietmar Bernreuther

Foto: Detecon

Software-unterstützende Organisation: Prozesse, Methoden und Werkzeuge, die bei der Entwicklung des Produktes zum Einsatz kommen, müssen schnelle Software-Entwicklungszyklen unterstützen. Wasserfallartige Projekt-Roadmaps, papierbasierte Dokumentation und Anforderungslisten im Excel-Format sind für software-orientierte Produktentwicklungen nicht geeignet. Vielmehr wird benötigt:

- Agile Entwicklungsmethoden wie SAFe, um Software-Änderungen kontinuierlich und iterativ in kurzen, getakteten Entwicklungszyklen umzusetzen
- DevOps, um Übergaben zwischen Entwicklung und Betrieb zu vermeiden
- Continuous Integration & Delivery (CI/CD) zur Automatisierung von Build, Test und Deployment in die Produktion

- Continuous Exploration, um Innovationen maximal zu fördern und zu beschleunigen
- Model-Based Systems Engineering (MBSE), um Software-Änderungen für Experimente und Tests unabhängig von physischer Hardware modellbasiert simulieren zu können
- Ansätze wie Product Line Engineering zur systematischen Wiederverwendung von Software-Ressourcen
- Software Update Management Systeme (SUMS) zum effizienten Managen und Nachverfolgen von Software-Updates
- Cyber Security Management System (CSMS) zur Gewährleistung der Informationssicherheit auf militärischem Niveau, auch im Rahmen kontinuierlicher Entwicklung (DevSecOps)
- Durchgängiges Konfigurationsmanagement, um Abhängigkeiten und Varianten effektiv zu managen und eine umfassende, maschinenlesbare Vernetzung aller Informationen vom NATO-Standard bis zur Codezeile zu gewährleisten

John Eisenhauer

Foto: Detecon

Software-orientierte Unternehmenskultur: Die Implementierung von SDD erfordert nicht nur technologische, sondern auch organisatorische, kulturelle Anpassungen und eine hohe Verzahnung der Kommunikation zwischen Hersteller, Betreiber und Nutzer. Dies beinhaltet:

- **Etablierung einer Lern- und Fehlerkultur,** die Fehlschläge zulässt und den sich daraus ergebenden Erkenntnisgewinn konstruktiv nutzt. Wenn Fehler gemacht werden, sollten diese schnell gemacht werden, um Leeraufwände zu minimieren („fail fast, fail early“). Rückschläge sind ein natürlicher Teil des Software-Entwicklungsprozesses, allerdings hat dieser Ansatz Grenzen, wenn es um funktionale Sicherheit und Informationssicherheit geht
- **Moderation zwischen Software-Agilisten und klassischen Ingenieuren:** Ein allzu missionarisches Erzwingen von agilen Methoden-Frameworks kann klassisches Systems Engineering (SE) schnell überfordern, besonders in hardwareaffinen oder sicherheitskritischen Bereichen. Dennoch müssen SE-Bereiche dazu beitragen, Software von den langen Hardware-Entwicklungszyklen zu emanzipieren. Auch Ingenieure, die selbst keine Software schreiben, müssen hierfür ihre Methoden anpassen, z.B. durch modellbasierte Systementwicklung von Hardware oder DevSecOps-Ansätzen im Bereich Cyber Security
- **Engere Verzahnung zwischen Hersteller, Betreiber und Nutzer:** Die Kommunikation zwischen Streitkräften / Ministerien, wehrtechnischer Industrie und Soldat:in muss sich von einem statischen Phasenprozess (Beschaffung, Lieferung, Übernahme, Change Request) hin zu einem kontinuierlichen Dialog zwischen Product Owner, Dienstleister und Nutzer weiterentwickeln
- **Veränderungsmanagement** wie z.B. die Etablierung von Change Agents, Stakeholder & Communication Management, Coaching oder die Einführung eines kontinuierlichen Verbesserungsprozesses, um die notwendige Transformation innerhalb der Organisation professionell zu managen

Software-getriebene Strategie: Die beste Software-Orientierung nutzt wenig, wenn die gewonnenen Vorteile nicht strategisch eingesetzt werden. Es gilt, den Mehrwert von Software schnell für die Truppe nutzbar zu machen. Wichtige Elemente sind:

Torsten Stimmel

Foto: Detecon

- **Innovationsmanagement:** Software-orientierte Unternehmen nutzen kontinuierlich Trend Scouting, Benchmarking, Wettbewerbsanalysen und Kreativitätsmethoden wie Design Thinking. Bei Defense-Anwendungen kommen spezifische militärische Quellen hinzu, wie Nachrichtendienste oder Feedback aus dem Einsatz. Entscheidend ist, dass Innovationsprozesse genauso agil wie die Softwareentwicklung sind, um kontinuierlich die Backlogs der Software-Produktteams mit Ideen zu versorgen
- **Soldier Centricity:** Angelehnt an „Customer Centricity“ geht es darum, Software an den Bedürfnissen der Truppe zu entwickeln. Soldat:innen sollten von der Idee bis in den laufenden Betrieb kontinuierlich in den Entwicklungsprozess eingebunden werden, um eine positive Nutzererfahrung (UX) zu gewährleisten
- **Steering und Portfolio Management:** Steuerstrukturen müssen agile Software-Prozesse ermöglichen. Moderne agile Management-Frameworks wie Objectives und Key Results (OKRs) unterstützen die Verfolgung von Zielen entlang von iterativ anpassbaren Zwischenergebnissen

Die Beherrschung des Software-Lifecycles im Rahmen von Software-Defined Defense wird auf den zunehmend digitalisierten Schlachtfeldern der Zukunft erfolgskritisch sein. Der Verteidigungssektor muss sich darauf einstellen, seine Produkte, Arbeitsorganisation, Kultur und Strategie entsprechend anzupassen. Die zunehmend unsichere geopolitischen Lage macht zügiges und entschlossenes Handeln erforderlich, damit Deutschland und Europa auch in Zukunft wehrfähig bleiben.

Exportkontrolle und KI

Roland Stein, BLOMSTEIN

Roland Stein *Foto: BLOMSTEIN*

Diese Broschüre zeigt eindrucksvoll das beträchtliche Potenzial von KI zur Erfüllung der durch die Zeitwende und die Digitalisierung geschaffenen Anforderungen an die Sicherheits- und Verteidigungsindustrie auf. Gleichzeitig machen die Entwicklung, Vermarktung und Anwendung von KI-Systemen nicht an Landesgrenzen Halt. Die für die Sicherheits- und Verteidigungsindustrie ohnehin sehr wichtigen Vorgaben der Exportkontrolle werden daher künftig eine besonders herausragende Rolle spielen.

Mit diesem Beitrag möchte ich auf zwei praktische Entwicklungen aufmerksam machen: zum einen die zunehmend wichtiger werdende Rolle von KI-Systemen als Werkzeug zur Umsetzung exportkontrollrechtlicher Vorgaben und zum anderen die zurzeit zu beobachtenden Bemühungen des Gesetzgebers, KI selbst zum Gegenstand der Exportkontrolle zu machen.

Potentiale von KI-Systemen für die Exportkontrolle

KI-Systeme versprechen die Anwendung exportkontrollrechtlicher Vorschriften zu erleichtern, indem sie Compliance-Abteilungen insbesondere beim „Wo“, „Wer“, und „Was“ Unterstützung bieten. Bei der Frage des „Wo“ können sie die Identifizierung von einschlägigen Exporteinschränkungen nach Jurisdiktionen leisten. Beim „Wer“ können KI-Systeme helfen, KYC-Prozesse risikoabhängig und weitgehend automatisiert zu gestalten. Auch die Frage des „Was“ – des Abgleichens von in Frage stehendem Produkt und Exportverbotslisten – kann vereinfacht werden. In Deutschland hat sich beispielsweise die SEIA auf die Einhaltung von Ein- und Ausvorschriften konzentriert und auch die AEB bietet Produkte an, die gezielt auf die Einhaltung von Handelsbeschränkungen ausgerichtet sind.

Für Exporteure bringt der Einsatz von KI-Systemen erhebliche Vorteile mit sich. Erstens wird wegen der Verbesserung des Compliance-Systems ihr Risiko zur Zahlung von Geldstrafen und Bußgeldern reduziert. Zweitens tragen KI-Systeme zur Verringerung von Kosten und Komplexität der Compliance bei. Drittens erhöhen sie die Geschwindigkeit bei der Überprüfung von Transaktionen und macht solche Exporteure agiler und kundenorientierter.

Bislang sind viele europäische Unternehmen jedoch noch zurückhaltend und beginnen erst langsam, KI-Modelle in ihre Überwachungs- und Screening-Prozesse zu integrieren. Auch wenn ein flächendeckender Einsatz von KI-Modellen bei der Einhaltung von Ausfuhrkontrollvorschriften mithin noch in Ferne steht und die menschliche Überwachung in den nächsten Jahren unverzichtbar bleiben wird, bewegt sich dennoch vieles. Innerhalb des nächsten Jahrzehnts dürften KI-Tools aller Voraussicht nach zum Industriestandard werden, und eine halbherzige oder unterlassene Nutzung KI-basierter Maßnahmen keine Option mehr sein. Früher oder später wird deren Einsatz – selbst wenn nicht explizit im Gesetz verankert – in den Compliance-Handbüchern und Richtlinien der Regulierungsbehörden auftauchen.

Gleichwohl ist es kein Geheimnis, dass dem Einsatz von KI-Systemen Grenzen gesetzt sind. Zu denken ist etwa an die teilweise noch immer auftretende KI-Halluzination, überzeugend formulierte, aber weitgehend KI-erfundene Ergebnisse. Daneben stehen auch einzelne Fragen bezüglich der Anreicherung von Sprachmodellen mit urheberrechtlich geschützten Daten im Raum. Zuletzt haben Gesellschaft, Gesetzgeber und Gerichte noch den gordischen Knoten zu lösen, wer die Verantwortung für Fehlverhalten von KI-Systemen trägt. So dürfte eine deutsche Strafverfolgungsbehörde die Prüfung und Gestattung einer rechtswidrigen Ausfuhr durch eine KI-Lösung zum derzeitigen Zeitpunkt dem handelnden Menschen zurechnen, als hätte dieser selbst fehlerhaft gehandelt.

KI als Gegenstand der Exportkontrolle

Mit der zunehmenden "Intelligenz" von Gütern jeglicher Art – sei es bei Marschflugkörpern, Thermostaten oder Panzern – ist die Exportkontrolle von KI-Komponenten (seien es KI-Modelle, Software oder Hardware) bald nicht mehr wegzudenken aus der effektiven Eindämmung unerwünschten Technologietransfers ins Ausland. Wie bei jedem anderen Exportgut muss auch bei nicht oder nicht genehmigungsfrei exportierbaren KI-Komponenten zwischen Dual-Use und militärischen Gütern unterschieden werden.

Auf europäischer Ebene besteht bisher auf Dual-Use-Ebene kein direktes Verbot speziell für KI-Systeme. Jedoch können sie bereits heute indirekt auf verschiedenen Dual-Use-Listen auftauchen und danach Beschränkungen unterliegen. So finden sich in der europäischen Dual-Use-Verordnung verschiedene Güter, die ihrerseits Software – worunter auch KI-Modelle fallen – benötigen, um produziert oder betrieben zu werden. Beispielsweise sind nach Anhang IV Nr. 7B103 Systeme/Anlagen für bestimmte Flugjustierungssysteme gelistet. Damit bestehen an verschiedenen Stellen auch Einfallstore für die Einschränkung der Ausfuhr von KI-Systemen. Anders verhält es sich in Hinblick auf KI-Modelle im Kontext militärischer Nutzung. KI und Rüstung können Hand in Hand gehen: verschiedene KI-Modelle wurden ausdrücklich für militärische Anwendungen konstruiert. Exemplarisch sei auf das Münchner KI-Rüstungsunternehmen Helsing, das nach seiner jüngsten Finanzierungsrunde zum wertvollsten

KI-Startup Europas aufgestiegen ist, oder das französische Start-up Preligens, das zum Ende des letzten Jahres von Safran aufgekauft wurde, hingewiesen. KI-Modelle unterliegen der Exportkontrolle, soweit sie insbesondere unter den Softwarebegriff des Teils I Abschnitt A der Ausfuhrliste fallen – also zum Beispiel besonders für die Modellierung, Simulation oder Auswertung militärischer Waffensysteme entwickelt wurden.

Daneben können aber auch augenscheinlich rein zivile KI-Systeme militärische Nutzung finden, die sich auch nicht in den Anhängen der Dual-Use-Verordnung oder sonstiger Ausfuhrlisten wiederfinden. In diesem Fall ist eine Ausfuhr grundsätzlich genehmigungsfrei möglich. Gerade weil KI-Tools so flexibel einsetzbar sind, werden allerdings „Catch-All"-Regelungen an Relevanz gewinnen. Solche, wie sie auch die europäische Dual-Use-Verordnung in ihrem Artikel 4 kennt, regulieren insbesondere die Ausfuhr von leicht oder nahezu uneingeschränkt erwerbbaren Gütern, die nichtsdestotrotz in militärischen oder sonstigen sensiblen Einsatzbereichen nutzbar gemacht werden können. Dann kann die Ausfuhr im Einzelfall doch einer Genehmigung bedürfen.

Darüber hinaus haben einzelne Staaten in der EU begonnen, im Alleingang nationale Exportkontrollen zu erlassen. Nach anderen Mitgliedstaaten ist auch Deutschland im letzten Jahr auf diesen Trend aufgesprungen und hat die nationale Listung von Dual-Use-Gütern erweitert, um den Export kritischer Technologien zu beschränken. Hintergrund der Novellierung ist vor allem die Bedeutsamkeit von Quantencomputern und „klassischen" Chips modernster Bauart für die Entwicklung von KI-Systemen. Konkret wurden unter anderem integrierte Tieftemperatur-CMOS Schaltkreise (Cryo-CMOS), bestimmte Quantencomputer, Quanten-Kontrollanordnungen und Quanten-Messeinheiten aufgenommen. Die Erweiterung der Ausfuhrliste kann durchaus kritisch betrachtet werden. So hat die Europäische Kommission bereits Anfang des letzten Jahres ihre Skepsis gegenüber Ergänzungen der nationalen Dual-Use-Kontrolllisten der Mitgliedstaaten deutlich gemacht, da solche Alleingänge mittelfristig dem Entstehen eines regulatorischen Flickenteppichs Vorschub leisten könnten.

Fazit

Wie auch andere Querschnittstechnologien ändert KI die Modalitäten menschlichen Arbeitens und wirtschaftlicher Realitäten im Sicherheits- und Verteidigungssektor fundamental. Für die Einhaltung bisheriger und neuer Exportbeschränkungen versprechen KI-Systeme eine sichere, schnelle und günstige Normumsetzung. Um diese technologischen Potentiale fruchtbar zu machen, müssen Compliance-Betraute zwar keine tiefen technologischen Fähigkeiten erwerben. Sie sollten sich jedoch frühzeitig einen Überblick über bestehende und in der Entwicklung befindliche Tools von etablierten Technunternehmen und RegTech-Startups verschaffen. Daneben müssen Exporteure sich mit den Tücken von KI-Modellen als direktem oder indirekten Gegenstand von Exportkontrollen vertraut machen.

Zeitenwende in der Cyber Security

Ramon Mörl, itWatch

Ramon Mörl

Foto: itWatch GmbH

Deutschlands Cyberbedrohungslage ist erhöht. Das stellen die nationalen Dienste, das BKA und das BSI im Kontext des russischen Angriffskrieges gegen die Ukraine fest. Bereits vor dem Überfall Russlands auf die Ukraine waren Angreifergruppen, die Russland zugeordnet werden, in Deutschland insbesondere mit Cyberspionage und finanziell motivierten Ransomware-Angriffen aktiv. Seit dem russischen Angriffskrieg auf die Ukraine hat sich das Spektrum der Bedrohungslage erweitert. Gleichzeitig versuchen verschiedene Nationen die Demokratien über Fake News, Deep Fakes und Angriffe auf die Lieferketten zu destabilisieren und anzugreifen.

Viele große Schäden durch Cyberangriffe belegen die Notwendigkeit eines verstärkten Schutzes im Cyberraum in den gesamten Lieferketten der militärischen Industrie. Cyberbedrohungen kennen keine nationalen Grenzen. Der Ausfall eines Windparks in Deutschland Anfang 2022 war die Folge eines Cyberangriffs, der eigentlich gegen die Ukraine gerichtet war. Ein Kollateralschaden.

Eine potenziell aus China stammende Hintertür in der Hardware einer Barracuda Sicherheitsappliance, Schwachstellen in vielfach genutzter Open Source Software wie Log4J, Heartbleed, ein Lieferkettenangriff auf Solarwinds - alle gefährden die Integrität, Produktivität Ihres Unternehmens und Ihrer Produkte. Acht Millionen BlueScreens durch Crowdstrike zeigen, wie weitreichend Konsequenzen in Qualitätsproblemen sein können. Schadsoftware kann sich leicht über die gesamte Lieferkette ausbreiten. Es zeigt sich: Die IT-Sicherheitslage mit all den Auswirkungen auf die interne IT und die hergestellten Produkte hängt immer mehr von der Qualität, Integrität und Sicherheit der genutzten Produkte ab. Eine qualitativ hochwertige Vertrauenskette stellt in Deutschland der Geheimschutz dar – insbesondere sind die qualitätssichernden Maßnahmen der Bundeswehr sehr verlässlich. Nachahmung der Architektur und des Bebauungsplans der Bundeswehr ist also empfehlenswert, um qualitativ hochwertigen Schutz zu erreichen.

itWatch ist einer der wenigen inhabergeführten Cyber Security Hersteller in Deutschland. itWatch stellt patentierte IT-Sicherheit in Deutschland her und bedient damit IT-Umgebungen der Inneren und Äußeren Sicherheit bis zu einem Schutzgrad von GEHEIM – inkl. Waffentragender Systeme.

Cloud-Datensicherheit-Datenwäsche

Bild: itWatch GmbH

Die Besonderheit der Produkte der itWatch liegt darin, dass der Zufluss aller Daten und Anwendungen identifiziert, isoliert und mit verschiedensten Verfahren nach vertrauenswürdigen und nicht vertrauenswürdigen Elementen getrennt und dann geeignet behandelt wird.

Die itWatch Enterprise Security Suite (itWESS) ist eine zentral gemanagte, manadantenfähige Endpoint Security mit EDR-Funktion. Sie schützt gegen Datendiebstahl (Data Loss Prevention - DLP), bietet technische Vertrauensketten von der Tastatur bis zu den Daten, die organisatorische Einbettung Ihrer Sicherheitsrichtlinie durch rechtsverbindliche Dialoge und integriert mit 14 Modulen alle Themen wie Device Control, Port- und Schnittstellenkontrolle, Application Control, Printkontrolle, Contentüberprüfung und -kontrolle, Verschlüsselung, Monitoring. Risikoüberwachung, benutzerverwendbare Sandboxen, Isolierung zur Härtung Ihrer Systeme.

Contents, die auf den Endpoints von nicht vertrauenswürdigen Quellen wie Browserdownload, Internet, Mail, mobilen Datenträgern, offenen Schnittstellen und kommunizierenden Anwendungen (ftp, s-ftp …) genutzt werden sollen, können mit itWash, einer netztrennenden Datenschleuse mit Datenwäsche (Data Sanitizing) und Workflow gewaschen werden, bevor das Betriebssystem auf diese Daten zugreifen kann. Nach der Wäsche stehen die Daten im Benutzerkontext zur Verfügung und können ohne Sicherheitsdefizite genutzt werden.

itWash (itWash.de) ist eine Datenwaschmaschine, die es ermöglicht, jede ausführbare Software – unabhängig von ihrer Einbettung – zu erkennen und zu entfernen. Dadurch können alle Dokumente direkt vom Anwender genutzt werden.

CodePurITy prüft Software, die zur Ausführung kommen soll. Nach positiver Prüfung kann das Modul Application-Watch diese direkt ohne weiteren Arbeitsschritt freigeben.

Diese Fähigkeit ist für Software Defined Defense (SDD) Umgebungen sehr hilfreich, weil neben der Codeprüfung auch

die SBOM (Software Bill of Material) ermittelt und angereichert, die CVE geprüft und alle Ergebnisse in den Metadaten für das automatisierte Life Cycle Management gesammelt werden.

Höchste Qualität des Schutzes

itWatch hat viele tausend Lizenzen im GEHEIM-Umfeld, wie 300.000 Lizenzen im militärischen Einsatz sowie weit über 100.000 Lizenzen in VS-NfD-Umgebungen. Dem Einsatz in GEHEIM Umgebungen gehen intensive Prüfungen voraus. Auf der Skala der Common Criteria Prüfungen sind diese höher als eine CC EAL 4+ Prüfung zu bewerten, da nicht gegen ein vom Hersteller definiertes Protection Profile geprüft wird, sondern alle Facetten der Produkte in realen vernetzten Einsatzumgebungen durch professionelle Pentester den verschiedensten Angriffsszenarien ausgesetzt werden.

Wo verstecken sich Angriffe?

Jeder Angriff braucht ein Stückchen Code, der sich in den Daten im Download, den E-Mails, den mobilen Datenträgern oder auch den Softwarepatches versteckt. Die Daten, die Sie jeden Tag bekommen, in der Personalabteilung als Bewerbung, als Informationen von Partnern im Vertrieb, im Marketing, in der Technik etc. haben nicht den Grad der Vertrauenswürdigkeit. Lassen Sie die Daten einfach waschen und Sie können sie gefahrlos nutzen.

Wo ist der Bedarf in Ihrem Haus?

Daten von unsicheren Umgebungen oder aus öffentlich zugänglichen IoT Geräten können leicht mit Schadcode oder Überwachungswerkzeugen infiltriert sein. Trotzdem sollen die Daten genutzt werden, wenn es sich z.B. um Bewerbungen handelt. Seit vielen Jahren ist itWash zur Übernahme von Daten aus unsicherer Umgebung bei Polizeien, Diensten, Energieversorgern, Justiz, Kommunen, der äußeren Sicherheit und vielen weiteren im Einsatz – nebenbei werden die Daten standardisiert und über die Wokflowkomponente bei Bedarf verschlüsselt den berechtigten Empfängern über deren gewünschten Informationskanal zugestellt:

- Personalabteilungen-Mailanhänge der Bewerber „waschen“
- Standardisieren von Kameradaten und IoT Devices
- Schadensmeldungen, Datenaustausch mit dem Maschinenpark, (Updates, Neukonfigurationen etc.)
- Darknet-Recherche
- Daten aus Fachverfahren
- Internetdownloads, USB und vieles mehr.

Welche Gefährdungen können in Daten enthalten sein? Ein Skript in einer pdf-Datei, das die Konfiguration Ihres remote Desktop Tools so verändert, so dass Unbefugte, die Rechte der Anwender übernehmen – schädlich aber eben kein bekannter Schadcode. So wie diesen Angriffsvektor gibt es viele, die von den Standardsystemen nicht erkannt werden. Verschlüsselte Daten in zip-Archiven oder pdf-Dateien können schädliche Objekte bis auf den Client tragen – itWESS und itWash erkennen das und verhindern auch diese Angriffe.

Jedes Unternehmen hat andere Vorstellungen, was saubere Daten sind und wie mit schmutzigen Daten verfahren werden soll. Makros, die von vertrauenswürdigen Partnern signiert sind, selbst erstellte Makros in Whitelists - bekannte Viren und Schadcode herausgewaschen oder das gewaschene Datenobjekt ohne den Virus oder Schadcode zustellen? Welche Metadaten sind bei welcher Datenquelle automatisiert zu ermitteln? Welche Drittprodukte sollen zusätzliche Metadaten einbringen – wie sollen diese für den Workflow genutzt werden?

Welches Waschmittel für welches Objekt?

Digitale Wäsche besteht aus Zerlegen, Inspizieren, Durchleuchten, Entfernen von Unerwünschtem und dann wieder nutzbar Zusammensetzen. Ein Teil dieser Verfahren wurde bekannt unter dem Begriff CDR – Content Disarm and Recover. Sinnbehaftete Datenwäsche enthält aber noch viel mehr Funktionalität. Sinnvoll sind hybride Verfahren, die es zum einen erlauben entlang der Herkunft und weiterer Metadaten der Objekte die richtige Behandlung – also das Waschmittel – zu bestimmen und gleichzeitig die Fähigkeit besitzen eine Standardisierung durchzusetzen und beliebige Sonderformate wie zum Beispiel medizinische Bildinformation kontextabhängig zu behandeln. So ist in vielen Unternehmen die Nutzung von Video und Voice auf mp4 beziehungsweise mp3 Formate standardisiert. Dieser Vorgang kann in der Datenwäsche untergebracht werden.

Datenwaesche-testen

Bild: itWatch GmbH

Weltraumbasierte Fähigkeiten as-a-Service: Beitrag zur souveränen Handlungs- und Einsatzfähigkeit der Bundeswehr und deren Partner

Sven Sünberg, Geschäftsführer, Media Broadcast Satellite GmbH;
Dr. Constantin Götze, Direktor Vertrieb Militär, Media Broadcast Satellite GmbH

Sven Sünberg

Foto: MBS

MBS (Media Broadcast Satellite) stellt mit eigener resilienter Infrastruktur in Deutschland und Europa von grundlegender Satellitenkommunikation (Satcom) bis hin zu anspruchsvollen Anwendungen als flexible Services bereit – weltweit und im Weltraum. Die weltweit verfügbaren Services sind einsatzerprobt, kriegstauglich und zuverlässig durch die stetige Weiterentwicklung mit den Kunden. Als unabhängiges inhabergeführtes Unternehmen verfügt MBS über Kompetenz und ausgewiesene Erfahrung in Konzeption, Realisierung und Betrieb von weltraumbasierten Fähigkeiten in as-a-Service. Satcom und Weltraum sind die DNA des Unternehmens. Auf dieser Basis stellt MBS Lösungen für unterschiedliche Kunden bereit. Für den Bedarf aller militärischen Dimensionen und Plattformen (konventionell, autonom) – stationär, verlegefähig und mobil in der Bewegung während der Übertragung nutzbar.

Dynamische Lagen und Herausforderungen an die Streitkräfte erfordern einen innovativen, verbindlichen und loyalen Partner bei der Leistungserbringung.

Um Kunden die für die jeweilige Auftragserfüllung benötigte Fähigkeit als flexible Leistung bereitstellen zu können,

Dr. Constantin Götze

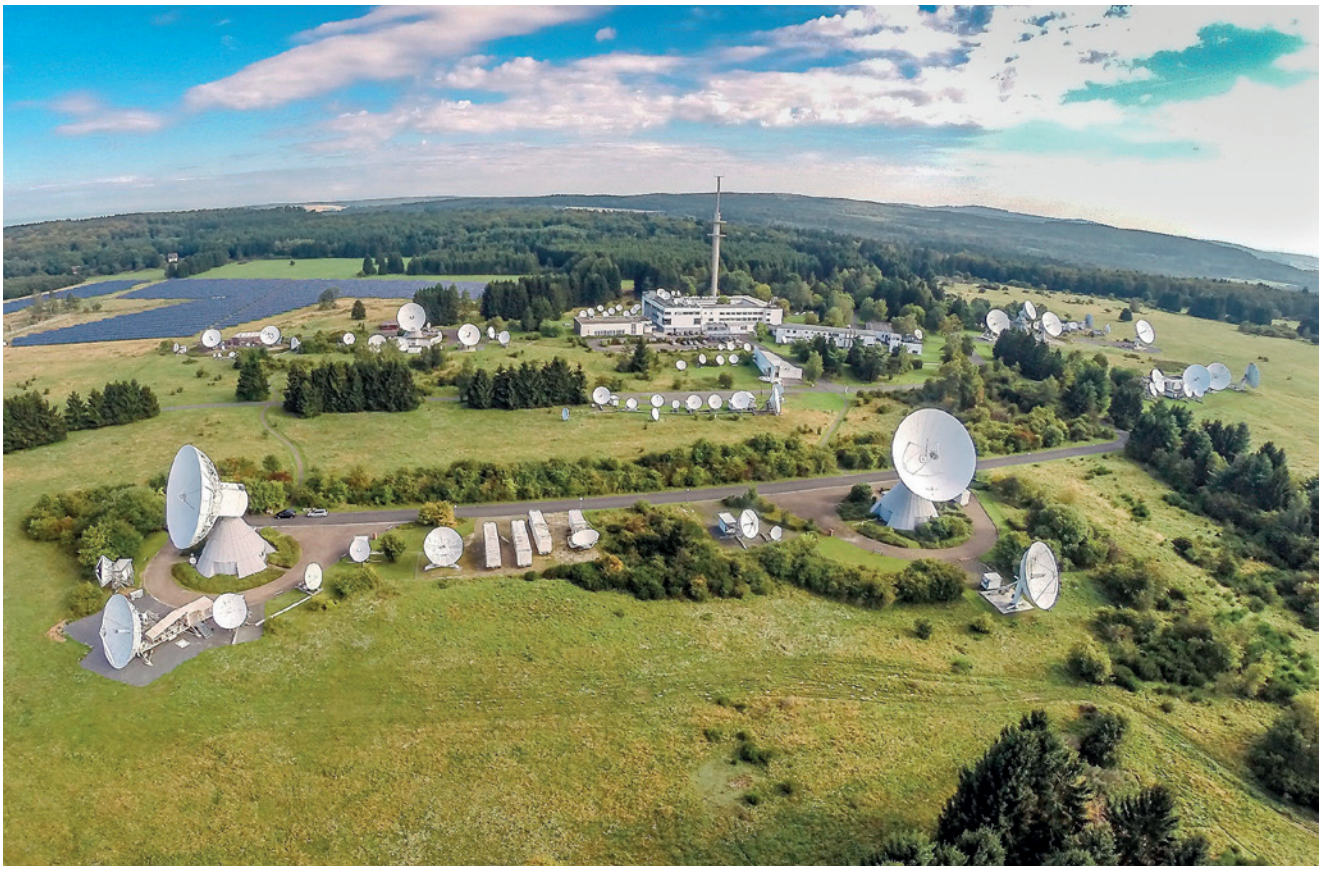
Foto: privat

integriert MBS bereits seit mehreren Jahren sogenannte Multi-Orbit und Multi-Frequenzband Fähigkeiten. Das bedeutet im Fall von Satcom die Bereitstellung der bestmöglichen Technologie, zugeschnitten auf den zu erfüllenden militärischen Auftrag. MBS integriert unterschiedliche Systeme und Technologien - wie z.B. Low Orbit Earth (LEO), Medium Earth Orbit (MEO) und Geostationary Orbit (GEO) mit den entsprechenden terrestrischen Anteilen. MBS realisiert so die für die Bedarfsträger passenden technologie-agnostischen Lösungen und entwickelt diese kontinuierlich weiter. Um dies zu gewährleisten, hält MBS entsprechende Rahmenverträge mit zahlreichen Dienstleistern. Dadurch ist eine schnelle und verbindliche Leistungserbringung garantiert. Mit einem Fokus auf souveräne europäische und deutsche Fähigkeiten nutzt MBS zur Leistungserbringung vier eigene miteinander vernetzte Bodenstationen (Teleports, in Europa - Deutschland, Polen, Frankreich) inklusive Network Operations Center (NOC). Die Infrastruktur und Leistungserbringung der MBS ist hochverfügbar und resilient ausgelegt, wird 24*7*365 durch Fachpersonal betreut und ist u.a. ISO27001 zertifiziert.

Die deutsche MBS-Erdfunkstelle in Usingen (bei Frankfurt a.M.) ist die größte ihrer Art in Europa und eingebunden in ein europaweites Netz von Bodenstationen. Der Teleport Usingen ist sowohl hochverfügbar und georedundant an das Kommunikationsnetz der Bundeswehr angebunden, als auch an relevante Hosting Center und internationale Kommunikationsnetzbetreiber in Frankfurt am Main und Europa.

Die MBS-Teleports sind direkt an die Infrastrukturen der

Abbildung: MBS Teleport Netzwerk



Media Broadcast Satellite Teleport Usingen

Foto: MBS GmbH

Satelliten-Konstellationen unserer Partner angebunden und können zeitnah skaliert und flexibel funktional erweitert werden. Dies ermöglicht die Gewährleistung hoher Sicherheitsstandards, Verfügbarkeit und Qualität in der Leistungserbringung für Kunden. MBS verfügt heute schon über die Fähigkeit, zukünftige Satelliten (-konstellationen) mit vorhandener Infrastruktur zu vernetzen. Diese bereits vorhandene Infrastruktur ermöglicht MBS „weltraumbasierte Fähigkeiten as-a-Service“ in herausfordernden und dynamischen Lagen verlässlich bereitstellen zu können.

Neben der Bereitstellung von Satcom-Leistungen für Endkunden im Bereich Militär, Behörden und Organisationen mit Sicherheitsaufgaben (BOS), sowie kritische Infrastrukturen (KRITIS), unterstützt MBS auch weltweit bei der Erschließung, Integration und dem Betrieb von weiteren Bodenstationen. So können bedarfsorientiert weitere souveräne Bodenstationen für den Betrieb von VLEO-, LEO-, MEO und GEO-Konstellationen produktiv genutzt werden. Diese können dann z.B. durch MBS, deren Partner, Bedarfsträger selbst oder im gemeinsamen Modell betrieben und genutzt werden. MBS-Leistungen haben sich vielfach im missionskritischen und militärisch-robusten Umfeld bewährt.

Beitrag zur Einsatzbereitschaft der Streitkräfte und Sicherheitsbehörden durch eigene resiliente Infrastruktur, souveräne Technologien und einsatzbewährte Dienstleistung – made in Germany, delivered globally

MBS entwickelt Lösungsvorschläge auf Basis marktgängiger Standards und stellt diese gemäß spezifischer Anforderungen der Nutzenden zur Verfügung. Von der schnell nutzbaren Anfangsbefähigung, über den Fähigkeitsaufwuchs, bis hin zur umfangreichen Zielbefähigung. Dafür hält MBS zertifiziertes und autorisiertes Personal bereit. Diese Art der Leistungserbringung hat sich für Kunden mit hohen Sicherheits- und Missionsanforderungen bewährt – in Deutschland, Europa und weltweit. Das Portfolio umfasst auch die Leistungserbringung in Umgebungen ohne zuverlässiges Global Positioning System (GPS) und zugehörige Zeitgeber. Eine globale Mission der Bundesmarine mit mehreren Einheiten (Fregatten) im Jahr 2024 wurde durch MBS mit Satcom versorgt. Dies umfasste die Unterstützung mit GEO-Kapazität unter Nutzung der Bundeswehr-eigenen Ku-Band Terminals SAILOR 900 und die Auswahl und Berechnungen für unterschiedlichen Ku-Band Satelliten entlang der weltweiten Fahrstrecke inkl. Reachback. Darüber hinaus auch die Bereitstellung von LEO-Kapazität unter Verwendung der OneWeb Konstellation entlang der Fahrstrecke inkl. Design der Anbauadapter/ Terminalhalterungen, Installation, Integration und Verwendungsüberprüfung der Terminals mit Reachback der Daten nach Deutschland.

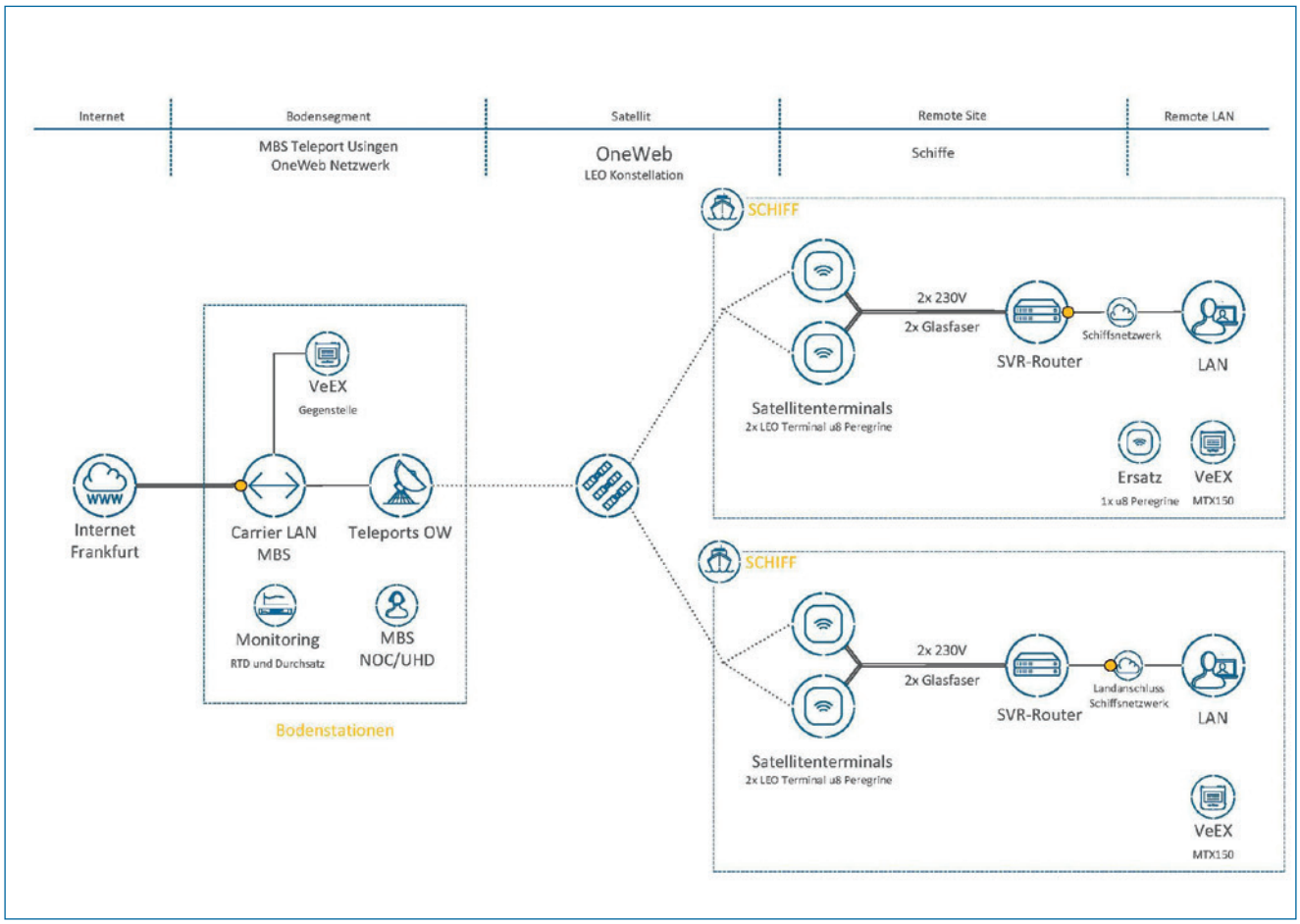


Abbildung: Beispiel 1

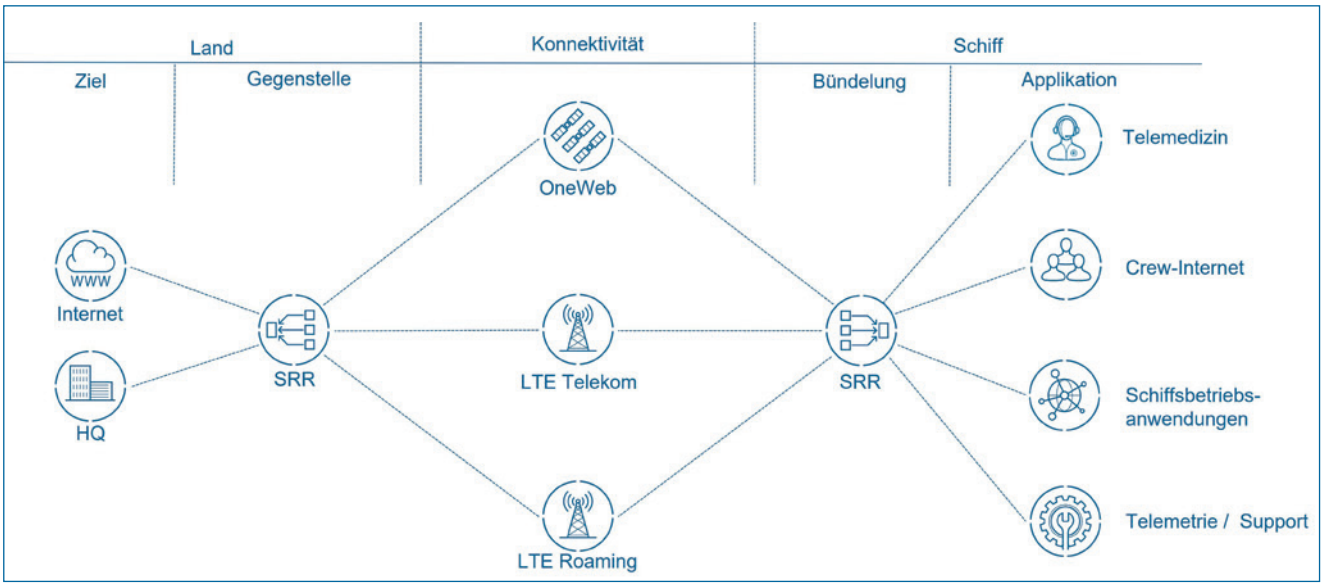


Abbildung: Beispiel 2

MBS hält u.a. verschiedene Rahmenverträge für öffentliche Auftraggeber, die eine Bereitstellung kommerzieller Satellitenverbindungen, weltweit ermöglicht. Für eine deutsche Nicht-Regierungsorganisation mit Aufgaben im Bereich der Personenrettung auf See hat MBS die einsatznahe Erprobung eines Long Range LTE-Antennensystem mit SD-WAN und LEO OneWeb Anbindung realisiert. Dies umfasste die Realisierung eines hybriden Kommunikationsnetzwerk mit Internet-Breakout für 3 seegehende Rettungseinheiten mit Long Range LTE-Systemen und OneWeb (Schiffs-)Terminals. Installation, Integration und Betrieb eines hybriden Netzwerks (2x LTE und 1xLEO mit SD-WAN) an Bord der

Schiffe erfolgte durch MBS. Die Schiffe waren über zwei LTE-Anbieter mit je einer LTE-Antenne mit Überreichweite und einem LEO OneWeb Terminal mit dem Internet verbunden. Die Umschaltung der drei Zugangswege erfolgte automatisch über ein SD-WAN-Netzwerk. Primär und küstennah wurden Daten z.B. für Telemedizin über beide LTE-Provider weitergeleitet. Ohne LTE-Abdeckung wurde die gesamte Internetverbindung über die OneWeb Konstellation bereitgestellt.
Mit OneWeb bietet MBS bereits heute eine robuste, leistungsstarke und wirtschaftlich attraktive Europäische Alternative zu Starlink. Mit OneWeb als auch im Verbund mit Starlink bietet MBS schon heute souveräne Optionen für Kunden. Anspruchsvolle Regierungs- und Geschäftskunden weltweit vertrauen auf die Integrität und Innovationskraft von MBS.

Investition in zukünftige souveräne Fähigkeiten – Software Defined Defense @ Space

MBS hat mit Partnern aktive Teilhabe an bedarfszentrischer Entwicklung von Schlüsselelementen zur Erbringung WR-basierter Fähigkeiten – von terrestrischen Terminals, über Satelittennutzlasten inkl. Verarbeitungskette am Boden bis hin zu spez. Hardware oder Softwarekomponenten als Teil der Verarbeitungsketten im Weltraum und auf dem Boden. Hierzu verfolgt MBS seit geraumer Zeit den Ansatz der „Software-ification“ und der dafür gezielt ausgelegten Entwicklung von Hardware. Dies ermöglicht eine schnellere Leistungssteigerung im Lebenszyklus der Systeme per Software. Bestandteil ist auch der Aufbau und die Aufrechterhaltung vertrauenswürdiger Lieferketten über den Lebenszyklus komplexer Systeme hinweg, um zukunftssicher und nachhaltig Spitzenleistungen erbringen zu können.

Karrierechancen

MBS wächst kontinuierlich und sucht hochmotivierte Personen zur Verstärkung des Teams, die Interesse haben, mit uns innovative, anspruchsvolle Projekte weiter voranzutreiben. Sehr gerne werden ehemalige Soldatinnen und Soldaten bzw. Mitarbeiterinnen und Mitarbeiter der Bundeswehr in vielfältigen Funktionen eingestellt. Aktuelle Stellenangebote mit ausgezeichneten Rahmenbedingungen in einem kollegialen, internationalen Umfeld sind auf https://career.mb-satellite.com/de/stellenangebote/ tagesaktuell abrufbar. Dort sind auch Kontaktdetails zur Vereinbarung eines persönlichen Gesprächs hinterlegt. Keine ad-hoc passende Stelle dabei? Kein Problem, auch Initiativbewerbungen sind jederzeit willkommen.

Echtzeit Geodatenanalyse zur Lösung Logistischer Herausforderungen in militärischen Landoperationen

Patrick Franz, Vice President Customer Success, Carmenta Geospatial Technologies

Patrick Franz *Foto: Carmenta*

Der russische Angriffskrieg in der Ukraine hat den hohen Stellenwert logistischer Fähigkeiten deutlich aufgezeigt. Gerade zu Beginn hatte die russische Seite aufgrund einer Vielzahl unterschiedlicher Faktoren erhebliche Probleme, Nachschub an die Front zu bringen. So gab es immer wieder Bilder von Konvois mit Versorgungsgütern, die sich stauten oder gar zurückgelassen wurden.

Die ukrainischen Streitkräfte haben ihre Bemühungen, russische Versorgungsfahrzeuge und Konvois zu bekämpfen, weiter verstärkt. Sowohl Munitionslager als auch Versorgungsfahrzeuge sind kritische Ziele, da sie die Versorgung der Kampftruppen mit überlebenswichtigen Ressourcen sicherstellen. NATO-Generalsekretär Jens Stoltenberg hat den Krieg in der Ukraine als „Kampf um Munition“ bezeichnet.

Neben der Herstellung großer Mengen an Verbrauchsgütern, stellt die effiziente Verteilung an die kämpfenden Truppen eine ganz andere kritische Herausforderung dar, um insbesondere der heutigen modularen Truppenstruktur und der hohen Mobilität von Kampftruppen Rechnung zu tragen. Ist die logistische Versorgung von Waffensystemen gefährdet, wird das System im Gefecht wirkungslos und verliert seinen Einsatzwert.

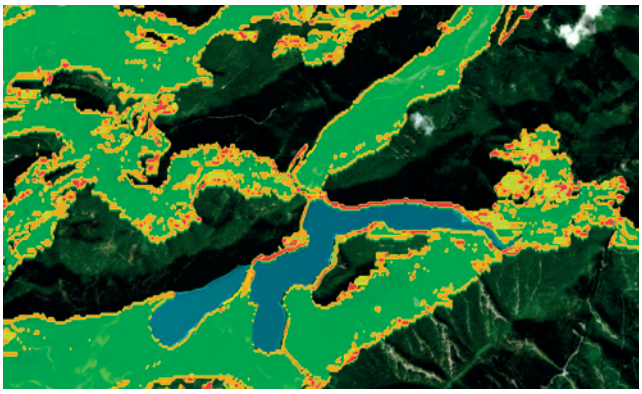
Softwarelösungen mit Echtzeit- Lage- und Geodatenanalysen können zur Bewältigung dieser Herausforderungen eingesetzt werden, um die Versorgung von Einheiten effizienter und robuster zu gestalten. Dabei können diese Lösungen aktuell schon bemannte und autonome Fahrzeuge unterstützen, um den Schritt in eine ganzheitlich automatisierte Logistik zu bestreiten.

Anhand des folgenden Beispiels soll anschaulich dargestellt werden, wie rein softwarebasierte Echtzeit-Geodatenanalysen zur Verbesserung der Systemversorgung beitragen können.

Robustheit des Gefechtsfeldes

Ein wesentlicher Bestandteil einer Operationsplanung, ist neben der Bewertung der Feindlage, insbesondere auch die Bewertung der Geofaktoren. Die Qualität einer geplanten Route hängt nicht nur von der möglichen Geschwindigkeit ab, sondern auch von der Fähigkeit, bei unerwarteten Ereignissen, wie Sperren, gangbare Alternativen zu bieten.

Mit Hilfe einer neu entwickelten Geoanalyse von Carmenta können aus den Geländedaten Räume und Wege berechnet werden, die robuster sind und somit die Gefahr von Missionen reduzieren. Im Allgemeinen ist die Robustheit ein Maß für den Verlust an Bewegungsfreiheit, wenn ein ungewolltes Ereignis oder Gefahr auftritt, die das Fahrzeug daran hindert, seine geplante Mission fortzusetzen.



Robust Battlefield *Foto: Carmenta Geospatial Technologies*

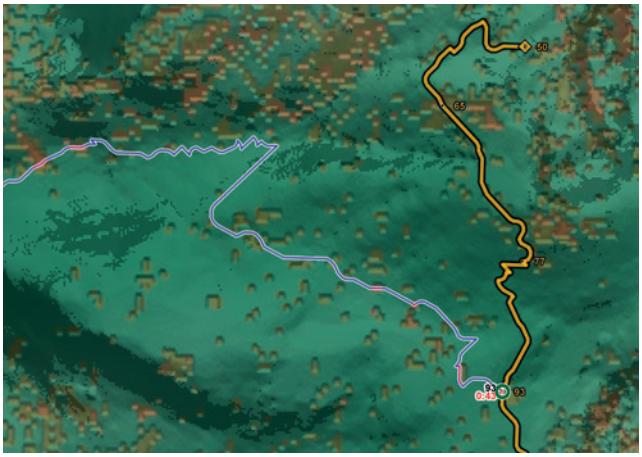
Im Bild sind die robusten Bereiche grün und die nicht robusten Bereiche orange/rot dargestellt. Hier ist deutlich zu erkennen, dass die Straße am See nicht robust ist. Wird hier beispielsweise eine Sperre aktiviert, kann die Mission mit hoher Wahrscheinlichkeit nicht fortgesetzt werden oder das Fahrzeug muss im schlimmsten Fall zurückgelassen werden. Die nicht robusten Bereiche können nun bei der Wegplanung dynamisch und automatisiert berücksichtigt bzw. gemieden werden. Dadurch kann die Gefechtsfeldversorgung robuster gestaltet und die Wahrscheinlichkeit einer erfolgreichen Versorgung deutlich erhöht werden.

Die Robustheit des Gefechtsfeldes ist aber nicht nur für die Wegeplanung von Interesse. Es können auch potenziell günstige Räume für Sperren identifiziert werden, um dem Gegner möglichst viel Bewegungsfreiheit zu nehmen.

Dynamische Berechnung von Versorgungspunkten

Moderne Waffensysteme zeichnen sich durch hohe Mobilität und Geschwindigkeit aus, wodurch die Planung von zeitlich und sicher erreichbaren Versorgungspunkten immer komplexer wird. Wartezeiten stellen für Plattformen und Waffensysteme ein erhebliches Risiko dar. Idealerweise sollte das Versorgungsfahrzeug zeitgleich mit dem Waffensystem am Versorgungspunkt eintreffen, um Wartezeiten möglichst zu vermeiden. Darüber hinaus können sich gerade auf dem Weg des Versorgungsfahrzeugs Gefahren und unpassierbare Stellen befinden, die die Ankunftszeit

des Versorgungsfahrzeugs verzögern und den zuvor geplanten Versorgungspunkt nicht mehr erreichbar machen. Diese komplexen und dynamischen Anforderungen stellen die manuelle Planung von Versorgungspunkten vor Herausforderungen.
Echtzeit-Geoanalysen in Verbindung mit Live-Positionsdaten können einen wesentlichen Beitrag zur dynamischen Berechnung von Versorgungspunkten zwischen Versorgungsfahrzeug und zu versorgenden Truppen leisten. Basierend auf Carmentas Terrainrouter wurde eine Echtzeitberechnung von zeitlich und sicher erreichbaren Versorgungspunkten entwickelt. Diese Berechnung erfolgt dynamisch und berücksichtigt taktische Informationen sowie Veränderungen in der Umgebung. Dadurch können neue zeitgenaue Versorgungspunkte kontinuierlich und präzise berechnet werden, um den aktuellen Anforderungen gerecht zu werden. Dies ermöglicht eine flexible und effiziente Versorgung der Kampftruppe, selbst unter sich schnell ändernden Bedingungen.



Rendez-vous der Systeme *Foto: Carmenta Geospatial Technologies*

In der Abbildung ist der Weg des Waffensystems gelb dargestellt. Entlang dieses Weges wurden mögliche Versorgungspunkte definiert. Die Zeit, die das Waffensystem benötigt, um die definierten Versorgungspunkte zu erreichen, ist ebenfalls gelb und in Minuten angegeben. Carmenta Engine berechnet nun den optimalen Versorgungspunkt sowie den zeitgenauen und sichersten Weg für das Versorgungsfahrzeug. Die Zeit, die das Versorgungsfahrzeug benötigt, um den Versorgungspunkt zu erreichen, wird schwarz dargestellt. Die Zeit, die das Versorgungsfahrzeug im offenen Gelände verbringt, wird rot dargestellt. Im dargestellten Beispiel erreicht das Versorgungsfahrzeug den Versorgungspunkt zeitgleich mit dem Waffensystem und verbringt nur 43 Sekunden im offenen Gelände.
Diese Berechnung ermöglicht eine schnelle und dynamische Reaktion auf Veränderungen im Gefechtsfeld. Durch die Berechnung von Versorgungswegen und -punkten in Echtzeit kann die Effizienz und Sicherheit der Versorgung erheblich gesteigert werden. Dies ist besonders wichtig in unvorhersehbaren und sich schnell verändernden Situationen, in denen Flexibilität und schnelle Entscheidungsfindung von Bedeutung sind.

Aktuelle und hochauflösende Geodaten

Die Genauigkeit von Geoanalysen hängt stark von der Aktualität und Auflösung der verfügbaren Geodaten ab. Satellitenbilder bieten oft nur eingeschränkte Aktualität, Blickwinkel und Auflösung. Heute können KI-Werkzeuge und Drohnen dabei helfen, aktuelle und hochauflösende Geodaten zu generieren. Carmenta und SE3 Labs arbeiten gemeinsam an der Erstellung von Geländeklassifikationen aus aktuellen Bilddaten mittels KI.
Echtzeit-UAV-Daten werden mit KI-unterstützter Computer Vision in hochauflösende, semantische 3D-Karten transformiert. SE3 Labs integriert 3D-Rekonstruktion, Objekterkennung und szenenbasierte Analysen über das lokale Sprachmodell „SpatialGPT“. Diese einzigartige Technologie dynamisiert die Geodatenanalyse, indem detaillierte Geländeklassifikationen erstellt und Geodaten kontinuierlich aktualisiert werden. Der Vorteil: robuste, nahezu „live“ Befahrbarkeitskarten und Geländeanalysen, die direkt in die Carmenta Engine eingebunden werden. Dies ermöglicht Echtzeit-Missionsplanung und -anpassung auf erkannte Änderungen, basierend auf minutenaktuellen Geodaten. Zusammen mit dem SpatialGPT Sprachinterface entsteht so eine intuitive, präzise und adaptive Grundlage für die Missionsplanung – besonders relevant für autonome und UGV-gestützte Operationen.

Fazit

Geodatenanalysen verbessern die Fähigkeiten der militärischen Logistik, indem sie genaue, zeitnahe und umsetzbare Informationen für die Entscheidungsfindung, Planung und Durchführung von logistischen Operationen in unterschiedlichem und oft schwierigem Gelände liefern. Sie spielen eine unverzichtbare Rolle bei der Verbesserung militärischer Logistik, insbesondere bei der Bewältigung der Komplexität. Da sich militärische Einsätze ständig weiterentwickeln, kann die Bedeutung der dynamischen Echtzeit- Geodatenanalyse für den Erfolg von Missionen und die Verbesserung des Situationsbewusstseins nicht hoch genug eingeschätzt werden.

DATAGROUP DefenseCloud

Der BSI zertifizierte VS-NfD-konforme Informationsverbund als Kollaborationsplattform „as-a-Service“ im Verbund OEM – Zulieferer – Bedarfsträger

Andreas Wiewel, Director DATAGROUP Defense IT Services

Andreas Wiewel

Foto: DATAGROUP

DATAGROUP betreut seit vielen Jahren behördliche und industrielle Kunden aus dem Verteidigungsbereich. Dies schließt auch Betriebe der wehrtechnischen Zulieferindustrie ein. Als Full-Managed-Service-Provider bietet DATAGROUP über flexible und hybride Liefermodelle 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.

Durch die jahrzehntelange Expertise als Rechenzentrumsbetreiber erfüllen alle Bereiche – Technologie, Housing, Hosting und Services – höchste Sicherheitsstandards. Die fortschreitende Digitalisierung stellt Unternehmen und Organisationen vor große Herausforderungen, insbesondere im Hinblick auf die Sicherheit sensibler Daten. Gerade unsere Kunden aus dem Bereich Aerospace & Defense benötigen speziell entwickelte Lösungen, um höchste Standards in puncto Datensicherheit und Datenschutz zu gewährleisten.

In vielen Unternehmen wird der Arbeitsalltag bereits heute von hybriden Arbeitsmodellen dominiert. Dabei nutzen Unternehmen vermehrt Shared Services oder Software-as-a-Service-Modelle, Applikationen aus der Public Cloud oder Hosting- und Platform-as-a-Service-Angebote. Laut der Bitkom-Studie „Cloud Report 2023“ setzen 9 von 10 deutschen Unternehmen bereits auf Cloud-Modelle, während jedes 9. Unternehmen in Deutschland eine Cloud-only-Strategie verfolgt. Die branchenübergreifenden Gründe hierfür sind in der Regel Flexibilität und Skalierbarkeit, eine hohe Verfügbarkeit, die Einbindung spezieller Applikationen, der Zugang zu KI und IoT, Environmental Social Governance (ESG) zur Reduktion der CO_2-Emissionen sowie Kostenoptimierung.

Für 81 % der befragten Unternehmen ist der Standort des Rechenzentrums sehr wichtig, wobei 93 % Deutschland als bevorzugten Standort angeben. Dies ist keinesfalls ein rein deutscher Trend – die Gartner-Studie 2022 „Enterprise IT Spending on Public Cloud Computing“ zeigt, dass sich die Cloud-Investitionen von Unternehmen zwischen 2019 und 2023 nahezu jährlich verdoppelt haben, während Investitionen in traditionelle IT stagnieren. Somit ist der hybride Weg kein kurzfristiger Trend oder eine reine Auslagerung von Servern, sondern bietet Unternehmen vielfältige strategische Chancen. Cloudbasierte Leistungen wie Hosting, Service-Auslagerung, Kollaboration, Skalierung von IT-Umgebungen und rechenintensive KI-Prozesse sind essenzielle Bausteine hybrider Zusammenarbeitsmodelle. Im wehrtechnischen Umfeld sind diese jedoch stets mit besonderen Anforderungen und Auflagen verbunden, die spezielle Cloud-Lösungen erforderlich machen.

Die Services der DATAGROUP DefenseCloud werden vollständig und georedundant aus Deutschland heraus erbracht. Hier kann DATAGROUP Defense IT Services auf jahrzehntelange Erfahrung als Rechenzentrumsbetreiber und Full-Managed-Service-Provider mit starker Reputation zurückgreifen. Die DATAGROUP Data Center bieten höchste Sicherheit, Georedundanz, Flexibilität und Skalierbarkeit – basierend auf den Standards C5, ISO 20000 und ISO 27001 auf der Basis IT-Grundschutz unter Berücksichtigung des Bausteins CON.11.1 sowie den Anforderungen der Schutzstufe „Verschlusssache – Nur für den Dienstgebrauch“ (VS-NfD).

So ist es uns möglich, Technologie, Housing, Hosting und Services mit höchsten Sicherheitsstandards aus einer Hand bereitzustellen. Dies stellt sicher, dass DATAGROUP nicht nur allgemeine Sicherheitsstandards für Informationssicherheits-Managementsysteme erfüllt, sondern auch spezifische Vorgaben für Kunden aus den Bereichen Aerospace, Defense und KRITIS im Rahmen einer vollständigen End-to-End Cloud VS-NfD Lösung. DATAGROUP setzt dabei auf standardisierte, sichere Datenaustauschlösungen für Auftraggeber und Auftragnehmer zur Kollaboration sowie BSI-konforme Lösungsansätze, die eine beschleunigte Freigabe des jeweiligen Modells für den Auftraggeber ermöglichen.

Der Serverbetrieb und das Servermanagement mit VS-Daten sind durch DATAGROUP auch für SAP-Systeme möglich. Darüber hinaus bietet DATAGROUP die Möglichkeit, BSI-konformes Mobile-Device-Management-as-a-Service (VS-NfD) bereitzustellen. VS-NfD-konforme Zugriffe für Outtasking-Modelle zum Management kundeneigener VS-Umgebungen sind ebenfalls anwendbar.

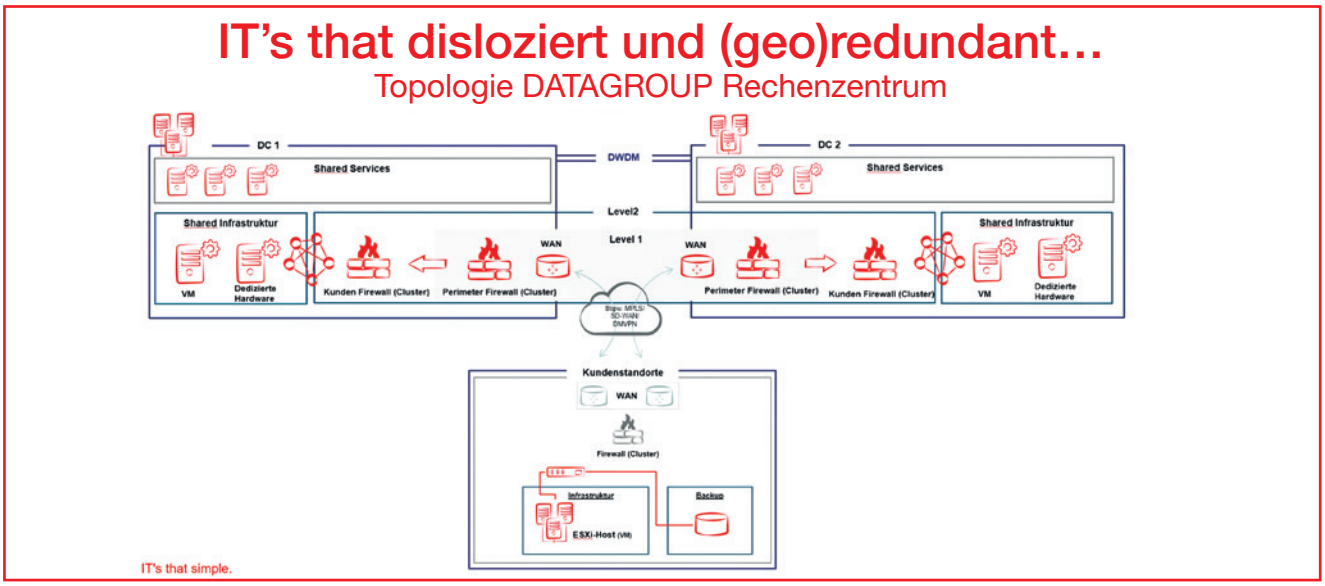
Als Rechenzentrumsbetreiber ist es unser tägliches Geschäft, uns bestmöglich gegen aktuelle und sich schnell verbreitende Bedrohungslagen zu schützen. Unsere umfassenden Security Services erkennen potenzielle Angriffe und Störfälle frühzeitig und ergreifen

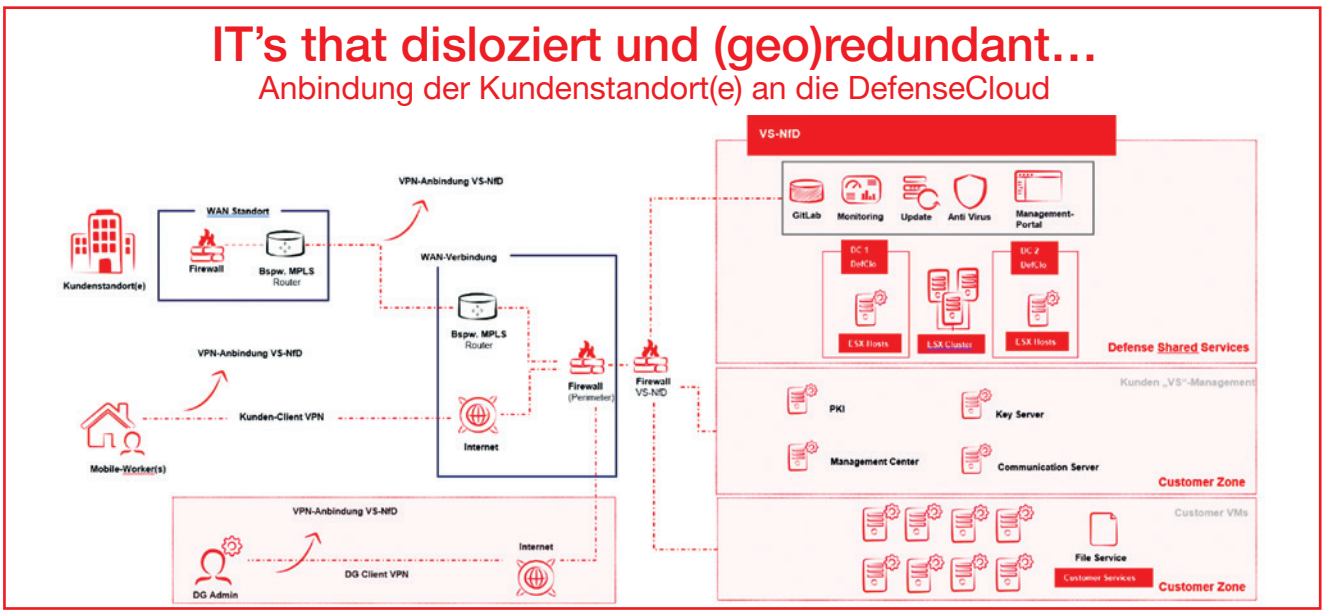
Gegenmaßnahmen. Die logische sowie physikalische Trennung der DefenseCloud-Services von anderen Dienstleistungen verhindert eine Kompromittierung von Daten durch verschiedene Angriffsszenarien. Damit leistet DATAGROUP einen entscheidenden Beitrag zur Resilienz der IT-Umgebungen unserer Kunden.

In der DATAGROUP DefenseCloud sind die Daten während des gesamten Verarbeitungsprozesses – von der Übertragung über die Speicherung bis zur Weiterverarbeitung – sicher und geschützt. Auch am Ende des Lebenszyklus werden die Daten nach zertifizierter Methodik sicher gelöscht oder physisch vernichtet. DSGVO- und VS-Konformität sind hierbei gelebter Standard. Die DATAGROUP DefenseCloud ist der erste und bis dato einzige BSI-zertifizierte Informationsverbund bis VS-NfD und ermöglicht die Bereitstellung einer IaaS-Umgebung sorgenfrei und unkompliziert „as-a-Service."

Unsere Lösungen – Managed. Secure. VS-NfD-konform:

- DefenseCloud
- Managed Firewall / Secure-VPN-Services
- Mobile Defense Management
- Mobile Device Management
- Field Service / On-Site Support
- VS-NfD Consulting





Panasonic CONNECT

TOUGHBOOK

TOUGH is

Jederzeit zuverlässig Datenzugriff zu haben

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

IP66

IP66

38999-connector

12 hours

intel CORE ULTRA 7

Intel® Core™ Ultra 7 Prozessor

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

www.toughbook.eu

Windows 11

Spionage und Sabotage: Die unterschätzte Zeitenwende in der nationalen Resilienz

Robert Friebe, Head of Communications & Public Policy, MONARCH

Robert Friebe *Foto: MONARCH*

Die sicherheitspolitische Zeitenwende, die Bundeskanzler Scholz im Februar 2022 ausrief, hat Deutschland in ein neues Zeitalter geführt. Neben der Neuausrichtung der Bundeswehr und ihrer Digitalisierung zeigt sich jedoch ein weiteres Element dieser Zeitenwende, das oft übersehen wird: die wachsende Bedrohung durch Industriespionage und Sabotage. Diese Angriffe gefährden nicht nur Unternehmen, sondern greifen tief in die nationale Resilienz ein. Die hybride Natur dieser Bedrohungen – das Zusammenspiel von physischen und digitalen Angriffen – verlangt nach einer grundlegenden Neubewertung, wie Staat und Wirtschaft aufgestellt sind, um gemeinsam Resilienz zu schaffen.

Hybride Bedrohungen im Kontext der Zeitenwende

Während die Digitalisierung und die Einführung disruptiver Technologien für die Bundeswehr zentrale Aufgaben sind, steht Deutschland zugleich vor der Herausforderung, hybride Bedrohungen besser zu erkennen und abzuwehren. Industriespionage, häufig orchestriert von staatlichen Akteuren, verfolgt das Ziel, wirtschaftliches Know-how zu stehlen, um geopolitische Vorteile zu erlangen. Ergänzt wird dies durch gezielte Sabotageakte, die kritische Infrastrukturen destabilisieren können – sei es durch Angriffe auf Energieversorgung, Logistikketten oder IT-Systeme.

Ein prägnantes Beispiel bietet der Vorfall im Sommer 2023, als Drohnen über LNG-Terminals in Schleswig-Holstein flogen, um Schwachstellen auszuspähen und Angriffsflüge zu simulieren. Solche Vorfälle verdeutlichen, dass hybride Bedrohungen zwar auf Unternehmen zielen mögen, aber eigentlich die strategischen Fähigkeiten der Bundeswehr und ihre Zusammenarbeit mit zivilen Partnern herausfordern sollen.

Kriegstüchtigkeit bedeutet mehr als Soldaten und Material

Verteidigungsminister Pistorius sprach davon, dass Deutschland kriegstüchtig werden müsse. Diese Forderung geht über die reine Erhöhung von Truppenstärke und Material hinaus. Es bedeutet auch, die Kapazitäten zur Absicherung kritischer Infrastrukturen erheblich auszubauen und die Resilienz der Bevölkerung zu stärken.

Tagtägliche Cyberangriffe auf Krankenhäuser, Energieversorger und Logistikketten verdeutlichen, wie schnell diese Einrichtungen „vom Netz gehen“ können. Eine kriegstüchtige Gesellschaft muss darauf vorbereitet sein, solche Störungen nicht nur zu überstehen, sondern ihre Funktionsfähigkeit schnell wiederherzustellen. Hier könnte Schweden mit seiner Agentur für psychologische Kriegsführung (MPF) ein Vorbild sein. Eine vergleichbare Institution könnte auch in Deutschland dazu beitragen, die Bevölkerung auf hybride Bedrohungen vorzubereiten und ihre psychologische Widerstandskraft zu stärken. Der Aufbau einer „dicken Haut“, die neben militärischer auch zivile Resilienz umfasst, ist ein ebenso zentraler Bestandteil der Zeitenwende wie die Modernisierung der Streitkräfte.

Spionage und Sabotage als Herausforderung für die nationale Resilienz

Die Bedrohung durch Spionage und Sabotage greift weit über den wirtschaftlichen Bereich hinaus. Angriffe auf die Lieferketten oder Produktionskapazitäten eines Rüstungsunternehmens haben potenziell direkte Auswirkungen auf die Einsatzfähigkeit der Streitkräfte. Ebenso gefährdet der Verlust von technologischen Innovationen in Schlüsselbereichen wie Künstliche Intelligenz, Sensorik oder Kommunikationstechnologie die strategische Souveränität Deutschlands.

Einfallstore für Spionage sind dabei vielfältig: Neben Cyberangriffen auf IT-Systeme nutzen Angreifer physische Schwachstellen wie schlecht gesicherte Büros oder manipulierte Hardware in Lieferketten. Ebenso rückt Social Engineering zunehmend in den Fokus, bei dem menschliche Schwächen gezielt ausgenutzt werden, um sensible Informationen zu erlangen.

Sabotageakte hingegen verfolgen das Ziel, physische und digitale Systeme zu destabilisieren. Beispiele reichen von gezielten Cyberangriffen auf Produktionslinien bis hin zu physischen Angriffen auf kritische Infrastruktur. Die hybride Natur dieser Angriffe erfordert eine enge Zusammenarbeit zwischen militärischen und zivilen Akteuren, um die nationale Resilienz zu stärken.

Strategische Handlungsfelder zur Abwehr hybrider Bedrohungen

1. Resilienz durch Integration: Die Zeiten, in denen militärische und zivile Sicherheitsmaßnahmen unabhängig voneinander betrachtet wurden, sind vorbei. Eine enge Verzahnung der Bundeswehr mit Wirtschaft und Behörden ist essenziell, um hybride Bedrohungen abzuwehren. Das Kommando Cyber- und Informationsraum der Bundeswehr kann hier eine Schlüsselrolle einnehmen, indem es die Schnittstelle zwischen militärischen und zivilen Sicherheitsstrategien stärkt.

2. Schutz kritischer Technologien: Disruptive Technologien wie KI, Quantencomputing und autonome Systeme sind nicht nur Innovationstreiber, sondern auch potenzielle Angriffspunkte. Die Bundeswehr und ihre zivilen Partner müssen gemeinsam Mechanismen entwickeln, um den Diebstahl und die Manipulation dieser Technologien zu verhindern.
3. Stärkung der Lieferketten: Die Sicherheit der Lieferketten ist ein zentraler Aspekt der Resilienz. Angriffe auf Zulieferer oder manipulierte Hardware können immense Schäden verursachen. Regelmäßige Audits und die Einführung von Sicherheitsstandards entlang der gesamten Lieferkette sind unerlässlich.
4. Schulungen und Sensibilisierung: Der Faktor Mensch bleibt die Achillesferse in der Abwehr hybrider Bedrohungen. Regelmäßige Schulungen, auch für militärische und zivile Führungskräfte, sowie simulierte Angriffe können dazu beitragen, das Bewusstsein für aktuelle Bedrohungen zu schärfen und Reaktionsfähigkeiten zu verbessern.
5. Technologische und organisatorische Innovation: Die Einführung disruptiver Technologien darf nicht auf technologische Innovation allein beschränkt bleiben. Organisationen – ob militärisch oder zivil – müssen auch ihre Strukturen und Prozesse anpassen, um flexibel auf Bedrohungen reagieren zu können.

Ausblick: Die Zeitenwende aktiv gestalten

Die hybride Bedrohung durch Spionage und Sabotage ist ein elementarer Bestandteil der sicherheitspolitischen Zeitenwende. Die Bundeswehr, die Wirtschaft und die Gesellschaft als Ganzes stehen vor der Aufgabe, die Resilienz durch eine enge Zusammenarbeit und die Einführung innovativer Ansätze zu stärken.

Die neue Bundesregierung ist gefordert, diese Herausforderungen aktiv anzugehen. Dazu gehört, erheblich mehr in Cyber Capacity Building zu investieren, aus den Erfahrungen des Ukraine-Krieges zu lernen und die aktuell fragmentierte Cybersicherheitsarchitektur Deutschlands zu zentralisieren und zu fokussieren. Nur durch eine klare Governance und abgestimmte Zuständigkeiten kann Deutschland eine kriegstüchtige Resilienz aufbauen, die sowohl militärische als auch zivile Bereiche umfasst.

Die neue Teilstreitkraft der Bundeswehr, das Kommando Cyber- und Informationsraum, bietet hier eine zentrale Plattform, um die Schnittstellen zwischen militärischen und zivilen Akteuren zu koordinieren und die nationale Resilienz zu fördern.

Die sicherheitspolitische Zeitenwende ist nicht nur eine Herausforderung, sondern auch eine Chance, die Grundlagen für eine widerstandsfähige und sichere Zukunft zu schaffen.

ADVERTORIAL

Software Defined Defence – zentrales Prinzip für die zukünftige Entwicklung der Streitkräfte

Marcel Karl, Senior Architekt Defense bei Materna.
OTL d.R. Stephan Ursuleac, Lead Business Development Safety & Defense bei Materna.

Das weltweite Datenaufkommen wird bis ins Jahr 2050 um das ca. zehntausendfache ansteigen. Für Streitkräfte bedeutet dies disruptive Veränderungen für die Art der vernetzten Kriegsführung. Digitalisierung sowie Vernetzung werden zum Erfolgsfaktor der Informations- und Führungsüberlegenheit. Gesteigerte Präzision und Schnelligkeit erreichen eine partielle Wirkungsüberlegenheit. Insgesamt werden Agilität und Geschwindigkeit bei Taktik und Logistik erhöht.

Software Defined Defence (SDD) ist ein zentrales Prinzip für wehrfähige Streitkräfte. Software dient der kontinuierlichen Verbesserung und Erweiterung von militärischen Fähigkeiten. Diese ermöglichen eine flexible Anpassung und Resilienz von Verteidigungssystemen, durch standardisierte und wiederverwendbare Module, wie durch Apps bei mobilen Endgeräten.
Für die Bundeswehr ergeben sich dabei vier zentrale Herausforderungen: Software muss aufgrund eines volatilen Gefechtsfeldes innerhalb weniger Stunden agil anpassbar sein. Dies erfordert leistungsfähige Software Factories nahe dem Gefechtsfeld und im rückwärtigen Raum. Dazu sind leistungsstarke Rechenverbünde, die Daten sicher und resistent vom Gefechtsfeld in den rückwärtigen Raum und umgekehrt übertragen, eine essenzielle Grundlage, z.B. für die Übermittlung von Sensordaten oder Software-Updates.
Dabei ist Cybersicherheit das zentrale Element, um die Geräteplattformen (z. B. Panzer) bzw. die von ihnen übermittelten Datenströme vor Ausspähung und Störung zu schützen. Gleichzeitig muss ihre digitale Signatur möglichst gering sein, um eine Detektion und somit Bekämpfung durch den Gegner zu vermeiden. Schließlich müssen die Geräteplattformen untereinander interoperabel sein.
Die heutigen Geräteplattformen der Bundeswehr verfügen noch nicht über diese Fähigkeiten. Sie bilden analoge, nicht vernetzte Systeme, die ggf. noch Jahrzehnte im Einsatz sind. Um die Geräteplattformen für SDD zu befähigen, bedarf es einer Analyse bestehender IT-Systeme, Schnittstellen und Sensoren sowie deren Funktion und Leistungsfähigkeit. Anschließend gilt es Lösungen zu entwerfen, die neue und alte Systeme miteinander integrieren. Das erfordert in der Praxis jedoch vielfältige Anstrengungen für Integration und Testung inkl. Sicherheitschecks. Dies muss in enger Abstimmung zwischen Bundeswehr und Industrie erfolgen.

Analoge Geräteplattformen können durch gängige Lösungen der IT-Branche neue Software integrieren. Dazu gehören zu installierende offene Betriebsplattformen für Cloud Open-Source-Container-Lösungen. Diese „Mini-Rechenzentren“ können die Form einer Streichholzschachtel haben. Das ermöglicht den Betrieb und die Integration diverser Software-Lösungen und Dienste, von unterschiedlichen Dienstleistern und verschieden Software-Formaten.
Die offenen Betriebsplattformen müssen ihre interne Kommunikation und externen Kommunikationswege, z.B. von Fahrzeug zu Fahrzeug, absichern. Dabei gelten die vier Grundprinzipien der Cybersicherheit:

- Vertraulichkeit (unbefugtes Auslesen von Daten verhindern, Verschlüsselung, einschließlich agiler kryptografischer Verfahren zzgl. Überlegungen zu einer Post-Quanten-Kryptografie, um heute bereits gesammelte Daten auch noch nachträglich vor Entschlüsselung zu schützen)
- Integrität (Schutz von Programmen und Daten vor unbemerkter Manipulation)
- Authentizität (der Benutzende stellt durch Programme, digitale Signaturen, Zertifikate etc. die Authentizität von Kommunikationspartnern sicher)
- Verfügbarkeit (die Systeme sind nutzbar, robust, resilient und anpassbar)

Dafür muss jedoch die Zusammenarbeit zwischen Rüstungs- und IT-Unternehmen sowie mit der Bundeswehr und Wissenschaft neu gedacht werden. Für gemeinsame Weiterentwicklungen gilt es den Zugang zu Geräteplattformen und geeigneten Testumgebungen sicherzustellen. Neue Kollaborationsnetzwerke bieten Zugang zu Know-how. Die IT-Branche verfügt z. B. über Erfahrungen aus der Automobilbranche und Best Practice für Kollaborationsplattformen, die sowohl den Austausch von Daten als auch gemeinsame Entwicklungsumgebungen sicherstellen. Das lässt sich durch die Etablierung von Reallaboren umsetzen, die Innovationen in einer befristeten Zeit, unter realen Bedingungen und unter der Einbeziehung von Nutzenden ermöglichen und somit die Nutzerfreundlichkeit von Lösungen steigern. Nur durch Kooperation lassen sich in Deutschland die Herausforderungen des Datenzeitalters bewältigen, um auf Augenhöhe mit Partnern und Antagonisten militärisch zu bestehen.

Warum eine leistungsstarke und sichere Netzwerkkarte in Zeiten vernetzter Operationen unverzichtbar ist

Dr. Bernd Götzelmann, Head of Products infodas

Dr. Bernd Götzelmann

Foto: infodas

Ein modernes militärisches Einsatzumfeld erfordert mehr als nur präzise Strategien und taktisch kluge Entscheidungen – es benötigt vor allem eine sichere, zuverlässige und resiliente digitale Infrastruktur. Die zunehmende Vernetzung in der modernen Kriegsführung ist kein vorübergehender Trend, sondern ein unverzichtbarer Bestandteil der Effektivität von Streitkräften. Im Zeitalter der Multi-Domain-Operations müssen Daten schneller und sicherer ausgetauscht werden; sei es im Heimatland, im Ausland oder in gemeinsamen Bündnissen. Über alle Führungsebenen hinweg, von Operationszentren bis hin zu mobilen Einsatzszenarien und verlegefähigen Systemen, wird die Fähigkeit zur sicheren Kommunikation zu einem entscheidenden Faktor für den Erfolg. Hier setzt die SDoT Secure Network Card, mit einer Zulassung bis zur Einstufung GEHEIM, EU SECRET und NATO SECRET, an. Die Netzwerkkarte von infodas, einem Airbus Tochterunternehmen spezialisiert auf Cyber und IT, stellt eine essenzielle Komponente zur Sicherung von IT-Infrastrukturen dar. Netzwerkkarten sind zentrale Komponenten jeder Kommunikationsstruktur, da sie die Verbindung zwischen den verbundenen Rechnern erlauben. Daher rücken sie zunehmend in den Fokus von Bedrohungsakteuren, denn ein Angriff hätte gravierende Auswirkungen auf die Funktionsfähigkeit der Systeme und der Kommunikation im Netzwerk. Der Schutz dieses sensiblen Bausteins wird daher zu einem entscheidenden Faktor im Kampf gegen die Cyberbedrohungen unserer Zeit.

Sicherheitsrisiko durch nicht dokumentierte Funktionen

Es ist kaum möglich, zu erkennen, welche Funktionen eine Netzwerkkarte von einem großen Hersteller zur Verfügung stellt. Dadurch können Produzenten, auch unter Druck von staatlichen Stellen, Funktionen in der Karte verbergen. Bedrohungsakteuren ermöglicht dies, effektive Angriffe auf das Kommunikationsnetz durchzuführen. Ein denkbares Szenario ist, dass eine versteckte Funktion aktiviert wird, die sensible Daten in Kopie an den Angreifer sendet. Neben den Daten, die unmittelbar über das Netzwerk fließen, sammelt die Netzwerkkarte auch Informationen, die im Rechner zwischen den Komponenten ausgetauscht werden, und leitet diese weiter. Es ist auch möglich, dass sich die Netzwerkkarte im Rechner als eine andere Komponente ausgibt, zum Beispiel als Bootmedium, und dadurch die Kontrolle übernimmt. Wir raten daher eindringlich dazu, ausschließlich Netzwerkkarten einzusetzen, deren Implementierung vollständig vorliegt und nur die Funktionen anbietet, die IEEE-Normen entsprechen. Diese Sicherheit bietet die SDoT Secure Network Card, die in Deutschland nach Security-by-Design-Prinzipien hergestellt und entworfen wird. Sie erfüllt das Anforderungsprofil BSI-VS-AP-0004-2016 und wurde nach einer eingehenden Prüfung für den Einsatz zum Schutz von Verschlusssachen bis GEHEIM freigegeben.

Hoher Schutz bei niedriger Latenz

Jede Komponente und die Software sind der Gefahr ausgesetzt, dass Angreifer Schwachstellen finden und diese für Ihre Zwecke ausnutzen. Die SDoT Secure Network Card zeichnet sich durch eine sehr kompakte Implementierung aus, die von externer Stelle umfassend geprüft wurde. Die Umsetzung führt nicht nur zu einem geringeren Angriffsvektor, sondern auch im Vergleich zu namhaften Herstellern, zu einer niedrigeren Latenz bei gleichem Durchsatz. Streitkräfte profitieren somit von einem Austausch ihrer Missionspläne, Lagebilder und Geodaten in nahezu Echtzeit. Im Ernstfall verschaffen sich Anwender dadurch einen taktischen Vorteil und bleiben in der Lage, schnelle Entscheidungen zu treffen und die Befehle sicher zu übermitteln.

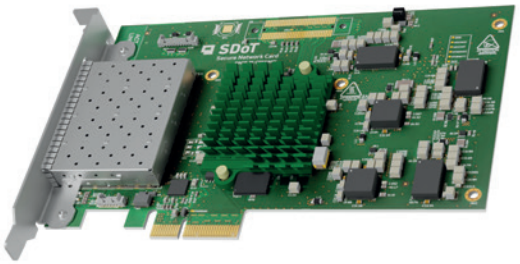
Konsequenter Schutz der militärischen IT-Infrastruktur

Mit der sich wandelnden geopolitischen Lage verändert sich auch die Bedrohungslandschaft. Cyberkriminelle nutzen verschiedene Techniken, um schadhafte Befehle in IT-Systeme einzuschleusen. Sie zielen nicht direkt auf die Netzwerkkarte ab, sondern auf andere Komponenten, die über den PCIe-Bus an den Rechner angeschlossen sind. Ein typisches Szenario ist die Übernahme der Management-Funktion. Gelingt es dem Angreifer, einen Befehl abzusetzen, hat das erhebliche Folgen bis hin zur Übernahme des Systems - unabhängig davon, ob es sich um einen Exploit, einen standardmäßigen Funktionsaufruf oder sogar um eine nicht dokumentierte Funktion handelt, die nur dem Hersteller des Bauteils bekannt ist. Angriffe dieser Art bieten ein hohes Gefahrenpotenzial, weil sie tief in die Systemarchitektur eingreifen. Gegen diese Angriffe schützt die Netzwerkkarte der infodas konsequent. Die SDoT Secure Network Card überprüft alle eingehenden Daten und verändert diese, sodass potenziell gefährliche oder unerwünschte Befehle aus dem feindlichen Netzwerk nicht durch die Zielkomponenten er-

kannt werden. In Kombination mit dem speziell entwickelten Treiber bleiben all diese Sicherheitsmaßnahmen für den Anwender transparent, während die sensiblen Systeme konsequent vor Angriffen geschützt sind.

Maximale Sicherheit durch geprüfte Technologie

Im Zeitalter der „Zeitenwende“ gewährleistet eine sichere Netzwerkkarte unseren Streitkräften die digitale Widerstandsfähigkeit gegen äußere Bedrohungen. Führungssysteme, Kommunikationseinrichtungen und sensibler Datenverkehr müssen gezielt vor Angriffen geschützt werden, um die Einsatzfähigkeit und die Sicherheit der Bundeswehr weiterhin aufrechtzuerhalten. C4I-Führungssysteme sind das Herzstück vernetzter Operationsführung, geraten in der modernen Kriegsführung jedoch verstärkt ins Visier von Bedrohungsakteuren. Deshalb ist es unerlässlich, Kommando- und Kommunikationsstrukturen mit einer robusten Netzwerkkarte konsequent vor Cyberattacken zu sichern.
Die infodas steht bereits seit über 50 Jahren einzelnen Nationen und Allianzen als vertrauenswürdiger Partner zur Seite. Mit effektiven und wirkungsvollen Cybersicherheits- und IT-Lösungen unterstützt das Systemhaus bei der digitalen Transformation und der Nutzung von gemeinsamen, missionskritischen Daten. Die höchsten Sicherheitsstandards durchlaufen militärische und geheimdienstliche Prüfungsprozesse. Seit Jahrzehnten genießen die zertifizierten Lösungen das Vertrauen der Bundeswehr, der NATO und mehrerer ihrer Mitgliedstaaten. Mit der NATO-konformen und kriegserprobten SDoT Produktfamilie wird die infodas den höchsten Anforderungen der Verteidigungsbranche gerecht. Ein kundenorientierter Ansatz und individuelle Beratung sorgen für eine schlagkräftige Unterstützung.



infodas connect more. be secure. SDoT Secure Network Card

Foto: infodas

Die Zukunft der militärischen Interoperabilität: Standards und digitale Transformation

Ralph Michel, Global Head of Sales, Defence & Space, secunet Security Networks AG

Ralph Michel

Foto: secunet

Die moderne Kriegsführung entwickelt sich in einem rasanten Tempo weiter. Während früher Einzellösungen für spezifische militärische Probleme entwickelt wurden, steht heute die Vernetzung im Mittelpunkt. Die zunehmende Digitalisierung, künstliche Intelligenz (KI) und Bedrohungen wie Hyperwar verändern die Art und Weise, wie Streitkräfte künftig operieren werden. Angesichts hybrider Bedrohungen, zunehmender Cyberangriffe und der wachsenden Rolle autonomer Systeme setzen die Bundeswehr und die NATO verstärkt auf das Thema Software Defined Defense (SDD). Diese Entwicklung markiert eine Zeitenwende: Software ist nicht mehr nur eine Unterstützung für militärische Abläufe, sondern zunehmend selbst ein strategischer Faktor. Doch diese Interoperabilität und Effizienz sind ohne gemeinsame Standards kaum zu realisieren.

Wo kommen wir her?

Es ist bekannt, dass Waffensysteme traditionell als eigenständige Lösungen konzipiert wurden, ohne deren Einbindung in ein gemeinsames System von Anfang an mitzudenken. Jedes Land und jede Teilstreitkraft entwickelten eigene Lösungen, oft ohne Berücksichtigung internationaler Kompatibilität. Das erschwert nicht nur die Zusammenarbeit in multinationalen Einsätzen, sondern führt auch zu kostspieligen Anpassungen und ineffizienten Strukturen. Interoperabilität ist der Schlüssel zu einer effektiven militärischen Zusammenarbeit im Rahmen von Joint & Combined Operations. Mit dem Ziel SDD zu realisieren, müssen Streitkräfte und Industrie, vernetzte und flexible Systeme zu schaffen.

Software Defined Defense: Vom Schachspiel zur Formel 1

Früher konnte ein erfahrener Kommandeur die Gesamtsituation analysieren, abwägen und seinen "Zug" planen – ähnlich wie ein Schachspieler. Doch die moderne Kriegsführung gleicht eher einem Formel-1-Rennen: Entscheidungen müssen in Sekundenbruchteilen getroffen werden, während sich die Lage kontinuierlich verändert.
Hier kommt KI ins Spiel. Sie fungiert als "Boxenfunk", analysiert riesige Datenmengen in Echtzeit und gibt Empfehlungen an den menschlichen Entscheidungsträger weiter. Ohne diese technologische Unterstützung sind moderne Konflikte kaum noch zu bewältigen. Streitkräfte setzen daher verstärkt auf KI im OODA-Loop (Observe, Orient, Decide, Act), um Reaktionszeiten zu verkürzen und Entscheidungsprozesse zu optimieren.
Die Bundeswehr betrachtet im Rahmen der SDD-Aktivitäten bereits MLOps (Machine Learning Operations) als Standard für den KI-gestützten Entwicklungsprozess. Eine robuste IT- und Dateninfrastruktur ist essenziell für das Training und die sichere Nutzung von KI-Modellen mit eingestuften Daten.

Die Notwendigkeit einheitlicher Standards

Doch all diese Fortschritte stehen und fallen mit der Standardisierung. Ohne einheitliche Protokolle für den Datenaustausch bleiben selbst die besten Technologien ineffektiv. Ein Beispiel für erfolgreiche Standardisierung der Schiffscontainer. Container sind standardisiert nach den ISO 668 Normen und haben weltweit einheitliche Abmessungen (z. B. 20-Fuß-Container, 40-Fuß-Container). Egal, ob ein Container auf einem Schiff, Zug oder LKW transportiert wird – er passt überall. Das hat die Logistik und den Welthandel revolutioniert. Erst die Einführung dieses Standards ermöglichte den reibungslosen Transport von Gütern über Landesgrenzen hinweg – ohne dabei die nationale Souveränität oder individuelle Innovationen einzuschränken. Was im Container drin ist, spielt eine untergeordnete Rolle.
Ein ähnlicher Ansatz ist heute für die militärische Interoperabilität erforderlich: Minimale gemeinsame Standards ermöglichen Kooperation, während sich jedes Land weiterhin eigene technologische Vorteile bewahren kann.
Als solche Standards etablieren sich derzeit beispielsweise Kubernetes als Container- und Orchestrierungsarchitektur sowie die umfassende Virtualisierung („Software-Defined Everything“) als Basis für skalierbare und interoperable Systeme.

Die Zukunft: Digitale Transformation und resiliente Systeme

SDD bildet die Basis für die nächste Generation militärischer Systeme. Diese müssen nicht nur nutzerfreundlicher und anpassungsfähiger werden, sondern sich auch in dynamischen Einsatzumgebungen bewähren. Resiliente System-of-Systems-Strukturen können durch KI und digitale Technologien unterstützt werden. Dies erfordert entschlossene politische und wirtschaftliche Weichenstellungen:

- Eine Standardisierung auf EU- und NATO-Ebene ist entscheidend, um Insellösungen zu vermeiden und eine reibungslose Zusammenarbeit in multinationalen Operationen sicherzustellen.

Der SINA Communicator H ist das erste Gerät aus dem SINA Portfolio mit einer modularisierten Architektur und bereits seit 2021 im Einsatz.

Foto: secunet

- Interoperabilität darf nicht auf Kosten technologischer Innovationskraft gehen. Die Herausforderung besteht darin, gemeinsame Standards zu etablieren, ohne die Entwicklung neuer, disruptiver Technologien zu bremsen.

Zur durchgängigen Umsetzung der notwendigen Standards wurde durch die gemeinsame Arbeitsgruppe von Industrie und Bundeswehr bereits eine Software Factory vorgeschlagen die nach DevSecOps-Prinzipien arbeitet und dabei automatisierte Softwareentwicklung mittels CI/CD (Continuous Integration/Deployment) nutzt, um den Entwicklungsprozess effizienter und sicherer zu gestalten.

Zukunftsperspektive: Sicherheit durch Modularität

Neben der Interoperabilität ist Cybersicherheit ein entscheidender Faktor für die Verteidigungsfähigkeit. Angriffe auf Netzwerke und Systeme können die Einsatzfähigkeit erheblich beeinträchtigen. Daher müssen moderne Verteidigungssysteme nicht nur vernetzt, sondern auch aktiv gegen Cyberbedrohungen gesichert werden.

Das erfordert die Weiterentwicklung vorhandener Konzepte. Traditionell wurden Sicherheitslösungen als monolithische Systeme, die fest in eine bestimmte Umgebung eingebunden sind, entwickelt. Dieser Ansatz erschwert eine agile Entwicklung und gleichzeitig die notwendigen Zulassungsprozesse. Eine zukunftsweisende Herangehensweise ist eine modularisierte Architektur wie sie bei SINA seit einigen Jahren bei der Entwicklung neuer Produkte und Releases genutzt wird. Dadurch können einzelne, bereits zugelassene Komponenten für sicherheitsrelevante Funktionen flexibel in verschiedenen Lösungen verwendet werden. Diese bleiben somit stabil und gut evaluierbar, was eine erneute Zulassung beschleunigt und den Entwicklungsprozess effizienter macht.

Ein Beispiel dafür ist die Entwicklung einer Cloud-Technologie, welche die Flexibilität moderner Cloud-Technologien mit den besonderen Anforderungen an den Geheimschutz verbindet. Die SINA Cloud wurde mit diesem modularen Ansatz speziell für hochsichere Einsatzszenarien konzipiert und bildet das Rückgrat des SINA Ökosystems.

Fazit

Die moderne Kriegsführung befindet sich in einem tiefgreifenden Wandel. Bundeswehr und NATO reagieren darauf mit der Forcierung der digitalen Transformation, dem Einsatz künstlicher Intelligenz und Software Defined Defense. Um in dieser dynamischen Umgebung handlungsfähig zu bleiben, müssen Streitkräfte und Industrie nicht nur technologisch aufrüsten, sondern vor allem ihre Systeme und Prozesse durch einheitliche Standards interoperabel und skalierbar gestalten.

Standardisierung ist kein Hemmnis für Innovation – im Gegenteil: Sie ermöglicht die Integration neuer Technologien, erleichtert die Zusammenarbeit zwischen internationalen Partnern und schafft eine belastbare Grundlage für resiliente, anpassungsfähige Systeme. Die Einführung von DevSecOps-Prinzipien, Cloud-Technologien und modularen Sicherheitsarchitekturen zeigt bereits, wie Effizienz und Sicherheit Hand in Hand gehen können.

Die Herausforderungen der Zukunft werden durch eine gemeinsame, flexible und vernetzte Verteidigungsstrategie bewältigt. Die Streitkräfte müssen nicht nur auf den letzten Krieg vorbereitet sein, sondern sich konsequent an den Erfordernissen der Zukunft orientieren. Wer heute die richtigen Standards setzt, bestimmt, wie effektiv und reaktionsschnell die Verteidigung morgen sein wird.

Verschlüsselungssysteme und Kryptografie im Wandel
Entwicklung der Kryptosysteme über die Zeit

Michael Kälber, Senior Manager Solutions, Thales Deutschland

Michael Kälber *Foto: THALES*

Kryptographie im ursprünglichen Wortsinn meint Geheimschrift, bzw. die Wissenschaft der Verschlüsselung von Informationen. Von Beginn an bis zum heutigen Tag wurden und werden hierfür so genannte symmetrische Verfahren verwendet. Dies bedeutet die Verwendung desselben Schlüssels zur Ver- und Entschlüsselung der zu schützenden Information. Bereits vor mehr als zweitausend Jahren übermittelten die Spartaner verschlüsselte Informationen in Form eines Lederstreifens. Der „Schlüssel“ zur Ver- und Entschlüsselung der Information bestand aus einem Stock (Scytale) eines definierten Umfangs. Bei der so genannten Cäsar-Chiffre wurden Verschiebungen von Buchstaben im Alphabet verwendet. Der symmetrische Schlüssel besteht hierbei in der Definition der Verschiebung.

In den nachfolgenden Jahrhunderten wurden verschiedenste Verschlüsselungsverfahren entwickelt und zur Anwendung gebracht. Wichtiges Merkmal der symmetrischen Verfahren ist, dass Sender und Empfänger über denselben Schlüssel verfügen müssen, der im Vorfeld der Nutzung bekannt gemacht werden muss.

Auch mit Einführung der Digitaltechnik waren und sind symmetrische Verfahren zentrales Mittel der Wahl. Im Rahmen dieses Technologiewechsels wurden neben den eigentlichen Verschlüsselungsgeräten auch digitale Systeme zur Verwaltung der Schlüssel eingeführt, so genannte Key-Managementsysteme, um u. a. komplexen Kommunikationsbeziehungen und großen räumlichen Entfernungen Rechnung zu tragen.

Die Skytale ist das älteste bekannte militärische Verschlüsselungsverfahren. Vor rund 2.500 Jahren verwendeten die Spartaner bereits eine Methode zur Übermittlung geheimer Nachrichten.

Foto: iStock / Bari Paramarta

Im Rahmen der Einführung asymmetrischer Kryptographie wurden mathematische Verfahren entwickelt, deren Anwendung die Verteilung operativer symmetrischer Schlüssel überflüssig machen. Dies trägt u. a. auch der Komplexität der Kommunikationsbeziehungen und den räumlichen Entfernungen der Anwender Rechnung. Die Key-Managementsysteme erweitern sich hierbei zu komplexen Key-Management-Infrastrukturen zur Verwaltung digitaler Schlüssel und Zertifikate.

Anwendung in Bereichen mit hohen/höchsten Sicherheitsanforderungen

Die Entwicklung der Kryptographie sowie auch die angewendeten Verfahren sind in Bereichen mit hohen und höchsten Sicherheitsanforderungen (z. B. Defence, Space, Transportation) prinzipiell vergleichbar zu rein zivilen Anwendungen. Allerdings werden in Hochsicherheitsbereichen naturgemäß höhere sicherheitstechnische Anforderungen an Anwendung und Schutz eingesetzter Standards, Verfahren und Algorithmen gestellt. Zudem werden Bestandsgeräte und -Systeme (Legacy) in der Regel parallel zu neueingeführten Systemen über einen längeren Zeitraum weiterhin genutzt. Dies hat den heterogenen Einsatz bisheriger und neuer Verfahren zur Folge. Die Bedrohung durch Quantencomputer erhöht die Sicherheitsanforderungen an die in Hochsicherheitsbereichen eingesetzten Verfahren und Algorithmen weiterhin. Dies stellt insbesondere auch spezifische Anforderungen an die Key-Management-Infrastrukturen.

Zusammengefasst führt dies zu zusätzlichen Herausforderungen in Konzeption und Umsetzung sowie zu einer, in der Regel zeitlich versetzten Einführung volldigitaler Systeme im Vergleich zum zivilen Sektor.

Evolution und Zeitenwende

Kryptografische Verfahren werden seit den Anfängen regelmäßig modernisiert im Sinne von Weiterentwicklung bestehender bzw. Einführung neuer Verfahren. Im Zeitalter der Digitalisierung findet diese Modernisierung jedoch unter veränderten Vorzeichen, komplexeren Rahmenbedingungen und kürzeren Evolutionszyklen statt. Neben grundlegendem konzeptionellem und technologischem Wandel führt dies zur Befähigung der Systeme zu kontinuierlicher Weiterentwicklung.

Die Bundeswehr nutzt im Kontext höchster Sicherheitsanforderungen und Einstufungsgrade Kryptosysteme für

hochsichere Kommunikation und Informationsaustausch. Für deren Versorgung mit Kryptomitteln ist aktuell ein leistungsfähiges Key-Management-System im Einsatz. Die operationellen Komponenten des Systems wurden von Thales Deutschland entwickelt und werden bedarfsgerecht regelmäßig bei Bedarf an neue Anforderungslagen angepasst.

Moderne Key-Management-Infrastrukturen berücksichtigen konzeptionell alle wesentlichen Anforderungen, um einen sicheren und resilienten Betrieb kryptografischer Systeme in komplexen Anwendungsszenarien – insbesondere in Hochsicherheitsbereichen – zu gewährleisten. *Foto: Shutterstock / Ranjith Ravindran*

Im Zuge der Berücksichtigung und Umsetzung der Anforderungen der Kryptomodernisierung konzipiert und realisiert Thales Deutschland eine moderne Key-Management-Infrastruktur. Die zugrundeliegende Konzeption berücksichtigt die wesentlichen Modernisierungsanforderungen, um einen sicheren und resilienten Betrieb kryptografischer Systeme in komplexen Anwendungsszenarien – insbesondere in Hochsicherheitsbereichen – zu gewährleisten. Dabei wird weiterhin ein breites Spektrum aktuell genutzter kryptografischer Endgeräte versorgt (Fähigkeitsbestand) sowie die Grundlage geschaffen, künftige moderne, teilweise online-fähige, Kryptosystemen zu unterstützen. Im Endausbau hat diese Key-Management-Infrastruktur potenziell die Fähigkeit, als „unsichtbarer“ Backend Service zu agieren. Unter Unterstützung automatisierter Betriebsabläufe und Workflows bietet die Lösung ein Höchstmaß an Sicherheit und Usability. Flexible Erweiterbarkeit und gesicherte Updatefähigkeit ermöglichen kontinuierliche Anpassung an sich ständig schneller verändernde Rahmenbedingungen.
Wesentliche Schwerpunktbereiche sind:

- Einsatz moderner Algorithmik und Kryptoagilität, Quantencomputer-Resistenz und aktuelle Sicherheitskonzeptionen.
- Konsequente Digitalisierung insbesondere in Bezug auf Prozesse zu Authentifikation und Autorisierung.
- Zeitgemäße System- und Softwarekonzeptionen, die flexible Deployment-Varianten der Systeme bis hin zum Einsatz in Secure-Cloud-Umgebungen zulassen.
- Modernste User Experience und Bedienergonomie für die Anwender.

Darüber hinaus findet der neue Key-Management-Interoperabilitäts-Standard der NATO durchgängige Berücksichtigung als wesentliche und notwendige Grundlage der Modernisierung im Key-Management. Der Standard definiert die Protokolle, Verfahren, Algorithmen und Workflows explizit für den NATO-Kontext.
Zusammengefasst ist dies eine zukunftsfähige Lösung, die einerseits die Interessen einer nationalen Lösung umsetzt und andererseits die überaus wichtige Interoperabilität zu internationalen Partnern sowie der NATO-Organisation selbst berücksichtigt.
Mit über zwanzigjähriger Erfahrung im Kontext Key-Management-Infrastrukturen für hochsichere Anwendungen und Expertise in den relevanten Themenbereichen der Modernisierung ist Thales Deutschland auch in Zukunft der ideale Partner der Bundeswehr für leistungsfähige, zeitgemäße und nachhaltige Lösungen.

Thales Deutschland

Mit langjähriger Erfahrung ist Thales Deutschland seit über 20 Jahren führender Anbieter im Bereich Key-Management für Anwendungen und Geräte höchster Sicherheitseinstufungen. Neben dem zentralen Anwendungsbereich Verteidigung agiert Thales Deutschland ebenso in den Segmenten Aerospace und Space. Das Unternehmen deckt mit spezialisierten Mitarbeiterinnen und Mitarbeiter die komplette Wertschöpfungskette in Deutschland ab, von der Entwicklung über Produktion bis hin zum Service. Besonders stolz ist Thales Deutschland darauf, die zentralen Komponenten der Schlüsselmittelversorgung für die Krypto-Systeme und Plattformen der Bundeswehr bereitzustellen.
Als Teil eines weltweit agierenden Hochtechnologie-Unternehmen konzentriert sich Thales Deutschland auf zukunftsorientierte und nachhaltige Systemlösungen, die neben der nationalen Souveränität stets die Interoperabilität mit internationalen Partnern im Blick haben. Modernste Standards für Schlüssel- und Zertifikatsmanagement werden auf internationaler Ebene mitgestaltet. Hierzu gehören unter anderem schon heute die zukunftssichere Entwicklung und Bereitstellung von quantencomputerresistenten Algorithmen „für morgen“ im Rahmen der Standardisierung des National Institute of Standards and Technology (NIST).

Schnelle Entwicklung – lange Serienverfügbarkeit: Embedded Vision Elektroniken für die Wehrtechnik

Oliver Helzle, Geschäftsführer hema electronic GmbH, Aalen

Oliver Helzle

Foto: hema electronic

Der Wunsch nach schneller Beschaffung und Integration neuester Technologien trifft in der Wehr- und Verteidigungsindustrie auf höchste Anforderungen an Zuverlässigkeit und Langzeitverfügbarkeit. Dass diese Anforderungen keinen Widerspruch darstellen müssen, zeigt hema electronic mit seiner hema Embedded Vision Plattform. Das Unternehmen aus Aalen 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.

Embedded Vision Elektroniken führen die Daten zahlreicher Kameras und weiterer Sensoren zusammen und sorgen dafür, dass jedem Nutzer zu jeder Zeit die richtigen Bilder und Daten zur Verfügung stehen. Für fahrende Anwendungen und die Aufklärung im Feldeinsatz müssen sie extrem niedrige Latenzzeiten erfüllen und komplexe Funktionalität unterstützen, von der Sensorfusion für 360°-Rundumsichten bis zur Überlagerung mit Grafiken und Informationen auf dem Bildschirm. Das hat die Entwicklung solcher Elektroniken in der Vergangenheit zeitaufwändig und teuer gemacht. Um das zu ändern, hat hema electronics ein Designkonzept entwickelt, das Entwicklungszeiten verkürzt, Kosten reduziert und Designrisiken minimiert. Als weiteren Vorteil ermöglicht das Design ein Höchstmaß an Skalierbarkeit für Upgrades und Produktvarianten.

Qualifiziert nach MIL-Standards

Das Unternehmen entwickelte kürzlich eine Video Distribution Unit für das Driver Vision System eines deutschen Wehrtechnik-Zulieferers, das in Raupen- und Radfahrzeugen eingesetzt wird. Dabei hat die Entwicklung von der Auftragserteilung bis zum Prototyp nur 24 Monate gedauert und die Zeit bis zur Serienreife der Gesamtlösung damit deutlich verkürzt. Das Driver Vision System integriert zahlreiche Kameras und Sensoren und kann als eigenständiges Vision System oder als Upgrade für bestehende DVS' verwendet werden. Es ermöglicht das Fahren unter Luke und kann herkömmliche Lösungen mit Winkelspiegeln ersetzen. Dank des robusten Designs der Elektronik und des Gesamtsystems widersteht es Stößen und Vibrationen sowie rauen Umweltbedingungen. Das System hat alle Zertifizierungen gemäß MIL-Standards bestanden und wird bereits in gepanzerten Fahrzeugen mehrerer internationaler Einheiten eingesetzt.

Baukasten für individuelle Vision-Elektroniken

Die Entwicklung der Elektronik basiert auf der hema Embedded Vision Plattform, die speziell für Embedded Vision Anwendungen konzipiert wurde. Basis der Designplattform sind über 45 Building-Blocks für Schnittstellen und Funktionalitäten, aus denen die Hardware frei konfiguriert werden kann. Entwickler wählen dazu einfach die benötigten Schnittstellen aus der hema Design Library aus. Standard-Interfaces wie Ethernet, USB, CAN und Wifi / Bluetooth sind dabei ebenso vorhanden wie die gängigen Videoschnittstellen. Das Platinenformat ist frei wählbar, sodass die Elektronik an bestehende Gehäuse angepasst werden kann. Auf Wunsch liefert hema auch Komplettlösungen inklusive kundenspezifischer Gehäuse.

Im Hardwaredesign gibt es für jeden der Building Blocks für die Elektronik entsprechende Vorlagen für Schaltplan und Layout. Vorteil für den Kunden: Innerhalb kürzester Zeit und zu überschaubaren Entwicklungskosten erhält er seine individuelle Elektronik. Entgegen einer kompletten Neuentwicklung kommen dabei vielfach bewährte Schaltungen zum Einsatz, die ideal für Wehrtechnik-Anwendungen geeignet sind. Kundenspezifische Schaltungen oder noch nicht in der hema-Bibliothek vorhandene Funktionen können unkompliziert integriert werden.

Skalierbare Rechenleistung durch austauschbare Module

Die Rechenleistung der Elektroniken liefern System on Modules (SoM) mit leistungsstarken ARM-Prozessoren und FPGAs. Die Module sind mit unterschiedlichen Leistungsklassen, Prozessoren und Speicherausbauten erhältlich und übernehmen das Management der Videodaten: Sie verarbeiten die Daten der multiplen Eingänge und verteilen sie an die Ausgänge. Dabei werden alle Funktionen mit geringsten Latenzzeiten von 30ms - 40ms umgesetzt, abhängig von den zusätzlichen Bildverarbeitungs-Aufgaben. Außerdem können mit den Prozessoren und FPGAs Videoströme zu Dual- und QuadView oder Picture-in-Picture-Daten zusammengefasst werden oder Overlays über die Videoausgänge ausgespielt werden. Je nach Ausstattung kann die Elekt-

Embedded Vision Elektroniken für die Wehrtechnik

Foto: hema electronic GmbH

ronik auch fertige Videodaten liefern, z.B. für Rundumsichten, die per Stitching zusammengefügt und entzerrt werden, oder mit zusammengeführten Bilddaten von Tag- und Nachtsicht-Kameras. Für diese Vorverarbeitung liefert hema zu seinen Elektroniken umfassende Software-Bibliotheken und Beispielanwendungen, auf die Kunden bei der eigenen Applikationsentwicklung aufbauen können.

Modulares Software-Design und agile Prozesse

Die Software für die FPGA-Elektroniken wird parallel zur Entwicklung der Hardware programmiert und basiert ebenfalls auf modularen Bausteinen, die kundenspezifisch und individuell an die Hardware angepasst werden. hema electronic stellt Code-Blöcke für bestimmte Bildverarbeitungsfunktionalitäten wie Split-Screen, Bild-im-Bild, Skalieren, Spiegeln, Drehen und Grafik-Overlays zur Verfügung. Das beschleunigt die Entwicklung und reduziert das Risiko von Programmierfehlern.

Der modulare Entwicklungsprozess ist vollständig in den digitalen Produktionsworkflow der hema Embedded Vision Plattform integriert. So erhalten Kunden innerhalb weniger Wochen maßgeschneiderte Prototypen, mit denen sie ihre eigenen Anwendungen schnell und einfach entwickeln, implementieren und testen können. Dank erprobter, industrietauglicher Schaltungen und Bauteile sind die Prototypen bereits sehr nah an der späteren Serienhardware. Serienoptimierung, Zertifizierungen und der Produktionsstart können in wenigen Wochen erfolgen.

Langzeitverfügbarkeit als Design-Feature

Neben der schnellen Entwicklung ist das Obsoleszenzmanagement von hema ein Garant, um eine langfristige und sichere Verfügbarkeit der Elektroniken zu ermöglichen – im besten Fall ohne Bauteil-Änderungen, die umfassende Tests und kostenintensive Re-Zertifizierungen erforderlich machen können. Bereits in der Design- und Prototypenphase prüft das Unternehmen dazu Lifecycle-Risiken von Bauteilen. Während der Serienqualifizierung einer Elektronik wird erneut eine umfassende Risikobewertung der Stückliste durchgeführt. Mit Beauftragung der Serienfertigung kann der Kunde für sein Produkte dann das jeweils passende Maß an Obsoleszenzmanagement vereinbaren – bis hin zu einem proaktiven Vorgehen, bei dem regelmäßig Lebenszyklus-Risiken evaluiert und bei Bedarf entsprechende Maßnahmen vereinbart werden. Das sorgt für ein Höchstmaß an Sicherheit und Vorlaufzeit, sollte die Elektronik doch einmal von Abkündigungen betroffen sein. In diesem Fall unterstützt hema mit geeigneten Maßnahmen – vom Last-time-buy und der Bevorratung bis zum Re-Design.

Modulares Design und Obsoleszenzmanagement für verlässliche Lieferbarkeit

Innerhalb der hema electronic sitzen Entwicklung, Produktion und Service unter einem Dach am Standort in Aalen. Das sorgt für kurze Wege und trägt ebenfalls zur Flexibilität und Zuverlässigkeit in der Belieferung bei – und das selbst für einen Produktlebenszyklus vieler Serienprodukte von 30 Jahren und mehr. Die hema Embedded Vision Plattform ist damit die ideale Basis für die schnelle und kostengünstige Entwicklung von Videoverarbeitungseinheiten und anderer Elektronik zur Sensordatenverarbeitung in zahlreichen militärischen und zivilen Anwendungen – und stellt im Zusammenspiel mit umfangreichen Maßnahmen sicher, dass Elektroniken auch in vielen Jahren noch höchsten Anforderungen an Zuverlässigkeit, Qualität und Lieferbarkeit gerecht werden.

Die Zukunft der Streitkräfte: Zeitenwende und Digitalisierung europäischer Lösungen

Andreas Reinecke, Head of Sales Defence Digital & Cyber

„Ukrainisches Drohnenboot Magura mit Lenkflugkörpern ausgestattet“

Es vergeht zurzeit keine Woche, ohne dass die Ukraine mit neuen oder angepassten militärischen Entwicklungen von sich hören lässt. Schwerpunktmäßig wird dabei über Entwicklungen rund um Drohnen oder allgemein um unbemannte Systeme berichtet.
Neben Reichweitenerhöhungen, welche überwiegend plattformabhängig sind, geht es aber um Fähigkeitserweiterungen, die sehr stark softwaregetrieben sind.

Sind wir Augenzeuge der Geschichte bei der Materialisierung von Software Defined Defence?

Fakt ist, dass die in der heutigen Nutzung befindlichen Systeme und Plattformen auf Grund ihrer physischen Merkmale in ihrem operationellen Wirken begrenzt sind und die Anpassung bzw. Neuentwicklung zeitlich aufwändiger ist als das Entwickeln von Softwarelösungen.
Softwarelösungen insbesondere bei Missionssoftware kann die Vorteile der Zeitenwende im Feld Digitalisierung zur Geltung bringen.
Eine mögliche Antwort auf den dynamischen Charakter digitaler Gefechtsfelder bietet der derzeit in den Streitkräften und der Verteidigungsindustrie viel diskutierte „Software-Defined-Defence-Ansatz“ (SDD).
Die Verbindung von SDD mit dem MDO-Ansatz der NATO kann zu einer Potenzierung der Entfaltung der militärischen Führungsfähigkeit führen. Die NATO definiert MDO als „Orchestration of military activities, across all domains and environments, synchronized with non-military activities, to enable the Alliance to create converging effects at the speed of relevance“. Die Entwicklung in diese Richtung und damit die Förderung gemeinschaftlicher Ansätze und die Überwindung von Silo-Denken erfordert allerdings ein Umdenken sowohl des öffentlichen Auftraggebers als auch der Industrie: Dazu gehören verzahnte und einheitlich formulierte Anforderungslagen seitens des öffentlichen Auftraggebers, das Neudenken der Beschaffungswege mit dem Fokus auf den Faktor Zeit sowie das Verfolgen von sowohl gemeinschaftlichen nationalen als auch europäischen Ansätzen durch die Industrie stets unter der Berücksichtigung offener Architekturen. Diese gehen dann über die jeweils projektspezifischen Forderungen und Umsetzungen hinaus.

Kontinuierliche Anpass- und Weiterentwicklung der Software als Schlüssel zur taktischen Dominanz

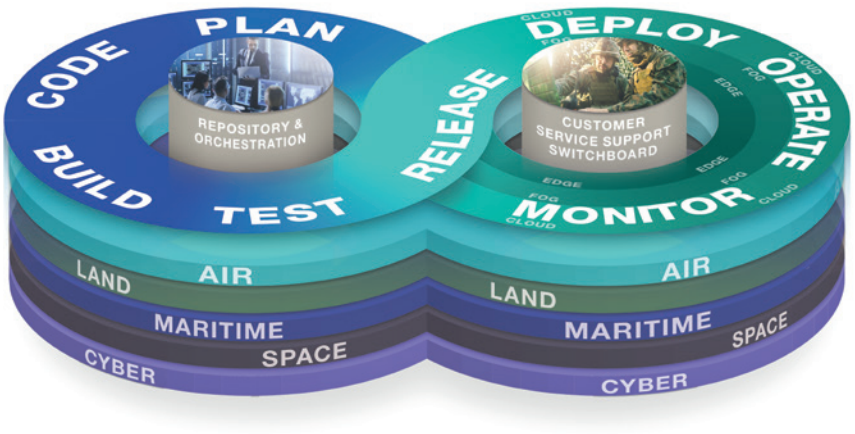
Insofern gilt es, die heutigen Bestandssysteme durch kluge Softwarelösungen zu ertüchtigen und ihren Kampfwert zu erhöhen. Ein Beispiel hierfür ist die Weiterentwicklung der Missionssoftware eines Eurofighters, um mit sogenannten Collaborative Combat Aircraft interagieren zu können.
Digitalisierung hat eine bisher unbekannte Dynamik und Beschleunigung von Gefechtshandlungen zur Folge. Beinahe jede technisch taktische aktuelle Entwicklung ist einer neuen oder angepassten Software geschuldet. Software bestimmt schon heute und insbesondere in der Zukunft die Leistungsfähigkeit von einzelnen Waffensystemen, aber insbesondere von System of Systems Lösungen.

Andreas Reinecke *Foto: Airbus*

Software ermöglicht es heute schon bisher voneinander getrennte Waffensysteme in einen interoperablen Verbund zu integrieren.
Auch wenn Software schnell unwiderlegbare zusätzliche taktische Vorteile für die Truppe bringt, gilt es anzuerkennen, dass der Grad der Komplexität zunehmen wird. Gilt es, ein isoliertes Waffensystem oder eine Plattform mittels Software in seiner Leistung zu steigern, bleibt der Komplexitätsgrad beherrschbar. Bei einer System of Systems Lösung, wie dem Future Combat Air System (FCAS), müssen die Interdependenzen schon per Design beherrschbar sein, um nicht in eine Komplexitätsfalle durch unerwünschte Nebeneffekte hineinzutappen. Die Fähigkeit zur stetigen Anpassung und Weiterentwicklung der Missionssoftware muss inhärent veranlagt sein, um „at the speed of relevance“ das Geschehen auf dem Gefechtsfeld bestimmen zu können. Hier wird die Software gepaart mit Künstlicher Intelligenz praktikable Lösungen für eine „Qualitätskontrolle“ bieten können.
Basis zur Umsetzung des SDD-Ansatzes kann die stringente Einbindung und Ausweitung von Erprobungslaboren sein – das Labor nicht als räumliche Einrichtung, sondern im Sinne der Sand-Box/Real-Labor-Definition.

Die Bedeutung des Faktors Mensch – Human Machine Interface als Schlüsselkompetenz

Bei all diesen Überlegungen und Ansätzen bleibt eines bestehen: Der Faktor Mensch. Es ist deutlich, dass die effektive Nutzung neuer Systeme und ihre Performanz vom Nutzer abhängt. Bei allen Planspielen und den daraus resultierenden neuen Ansätzen sollte das Human Machine Interface (HMI) im Zentrum stehen. Die kognitive Dimension gewinnt an Bedeutung.



Multi Domain Combat Cloud

Foto: Airbus

Die Gestaltung von Systemen sollte stets den Fokus auf die Bedienoberfläche und Bedienerunterstützung legen, anhand derer Szenarien erprobt werden können, und deren Ergebnisse in neue Ansätze, wie zum Beispiel agile Beschaffungsprozesse münden können. Benötigt werden offene Systeme, die aus Lessons-Learned oder roten Zwillingen (Feindsimulationen) heraus permanent erweiterbar und aufaddierbar sind.

Ein regelmäßiger Austausch zwischen Anwendern, Forschung und Industrie ist notwendig und sollte auch vertraglich so gestaltet werden können, dass er für innovative Beiträge aus der Industrie offen und interessant ist. Damit könnten völlig neue Innovationsprozesse initiiert und genutzt werden, um zukünftige Anforderungen der Führungsfähigkeit wesentlich besser zu bedienen als bisherige.

Die Zukunft der Kriegsführung liegt in der Befähigung zur kontinuierlichen Anpassung und Innovation. Die militärische Führung muss bereit sein, neue Wege zu gehen und sich kontinuierlich weiterzuentwickeln, um den sich ständig verändernden Bedingungen gerecht zu werden. Nur durch Flexibilität und Anpassungsfähigkeit können die Herausforderungen der modernen Kriegsführung unter Wahrung von Sicherheit und Stabilität erfolgreich bewältigt werden.

D-LBO: Fortschritte und aktuelle Entwicklungen aus Sicht der Industrie

Josef Stadler, Geschäftsführer und COO bei der blackned GmbH

Josef Stadler *Foto: blackned*

Die Digitalisierung landbasierter Operationen (D-LBO) nimmt weiter an Fahrt auf und entwickelt sich zunehmend zu einem zentralen Element der Bundeswehrtransformation. Seit dem Projektbeginn hat sich vieles getan – von strategischen Neuausrichtungen über technologische Meilensteine bis hin zu bedeutenden Vertragsabschlüssen. Die jüngsten Entwicklungen verdeutlichen, dass D-LBO nicht nur konzeptionell, sondern auch operativ in die entscheidende Phase übergeht.

Von der Konzeptphase zur Umsetzung – Eine Zwischenbilanz

Ursprünglich als Vorhaben mit Generalunternehmern mit zwei konkurrierenden Industriekonsortien geplant, wurde das Konzept 2019 zugunsten einer nationalen Umsetzung unter der Verantwortung des BAAINBw neu ausgerichtet. Die schrittweise Implementierung wurde auf acht sogenannte Kräftedispositive (KD1 bis KD8) angelegt und sollte bis 2038 abgeschlossen sein. Aufgrund finanzieller und operativer Anpassungen reduzierte sich der Fokus zunächst auf ein reduziertes KD 1.1, später auf die sogenannte Division 2025, die als Grundlage für die spätere Skalierung dient.

Mit der „Zeitenwende“ und dem gestiegenen Verteidigungsbudget nebst Sondervermögen wurden Ende 2024 die entscheidenden Weichen gestellt. Die Bundeswehr begann im Jahr 2021 mit der Ausschreibung der ersten Kernkomponenten, und mittlerweile sind nahezu alle relevanten Verträge aller Baugruppen für die Konfiguration D-LBO basic abgeschlossen. Insbesondere die Beauftragung der Arbeitsgemeinschaft IT-Systemintegration (ArGe D-LBO ISI), bestehend aus Rheinmetall und blackned, und die Beauftragung der Arbeitsgemeinschaft D-LBO HAI, bestehend aus den Firmen Rheinmetall Landsysteme und KNDS, markieren einen bedeutenden Schritt in der Umsetzung.

Technologische Säulen: Vernetzung, Plattformintegration und Führungsfähigkeit

D-LBO setzt auf eine durchgängige nahtlose und sichere Systemarchitektur, die alle Führungsebenen und Einsatzszenarien miteinander verbindet. Die Integration modernster IT-Systeme in die Fahrzeuge und Plattformen der Landstreitkräfte stellt dabei eine Kernherausforderung dar. Hier spielt der Tactical Platform Service (TPS), realisiert durch die Firma blackned mit Tactical Core, eine entscheidende Rolle. Dieser fungiert als zentrale Middleware und sorgt für die nahtlose Kommunikation zwischen verschiedenen Systemen und Netzwerken.

Die ersten Plattformintegrationen laufen bereits auf Hochtouren. Definiert als „Cluster 0“, umfasst dieser Abschnitt Musterintegrationen in 34 verschiedenen Plattformtypen, gefolgt von rund 540 Serienintegrationen. Damit werden wertvolle Erkenntnisse für die späteren Serienumrüstungen und den großflächigen Rollout der neuen Technologien gewonnen.

Tactical Core wird regelmäßig in Proofs of Concept und Nutzertests erprobt, um Verbesserungen basierend auf den gewonnenen Erkenntnissen umzusetzen. *Foto: blackned*

Neue Impulse durch Großaufträge und strategische Kooperationen

Mit der Auftragsvergabe von 1,2 Milliarden Euro an die ArGe D-LBO ISI wurde Ende 2024 ein entscheidender Schritt in Richtung flächendeckender Umsetzung getan. Diese Summe deckt insbesondere die IT-Integration aller relevanten Fahrzeuge und Systeme der Landstreitkräfte ab.

Ein weiteres bedeutendes Projekt innerhalb der D-LBO-Architektur ist TaWAN LBO, für dessen Realisierung Rheinmetall Anfang 2025 durch die Bundeswehr beauftragt wurde. Dieses System stellt eine hochleistungsfähige Kommunikationsinfrastruktur sicher, die die vordersten Einsatzkräfte mit den rückwärtigen Strukturen nahtlos verbindet.

Ausblick: Die nächsten Schritte zur digitalen Bundeswehr

Die kommenden Jahre werden entscheidend sein, um D-LBO in den flächendeckenden Einsatz zu überführen.

Die Division 2025 in der Konfiguration D-LBO basic dient hierbei als erster Prüfstein, in der die neuen Systeme unter realen Bedingungen genutzt und optimiert werden. Die gewonnenen Erkenntnisse werden die Grundlage für die weitere Skalierung der folgenden Kräftedispositive KD1 ff. bilden.

Die Bundeswehr hat mit der Umsetzung von D-LBO eine der größten digitalen Transformationen in der Geschichte der Streitkräfte eingeleitet. Entscheidend wird sein, dass die ambitionierten Zeitpläne eingehalten und technologische Innovationen kontinuierlich in das System integriert werden.

Die Digitalisierung landbasierter Operationen bleibt eine gewaltige Aufgabe, aber die aktuellen Entwicklungen zeigen: D-LBO ist nicht nur gesichert, sondern auf einem klaren Kurs in Richtung Zukunft.

Die blackned GmbH präsentierte 2024 zusammen mit ihren Partnern erstmals öffentlich die „D-LBO basic“ Führungsfunk-Ausstattung auf der AFCEA Fachausstellung in Bonn. *Foto: blackned*

HENSOLDT CERETRON: Software Defined Defence mit vernetzten landgebundenen Sensorlösungen

Thomas Koch, Produktmanager ISTAR Solutions, HENSOLDT

Thomas Koch

Foto: HENSOLDT

HENSOLDT, ein führender Anbieter in der Verteidigungs- und Sicherheitstechnologie, hat mit CERETRON eine innovative Softwarelösung entwickelt, die die FAWU-Prinzipien – Führung, Aufklärung, Wirkung und Unterstützung – neu definiert. Die Software verbindet Sensorik, Soldaten, Informationsverteilung und Wirkmittel in einer nahtlosen Kette und automatisiert Handlungsabläufe auf der Sensorplattform, um gewonnene Informationen optimal dem Gefechtsfeld verfügbar zu machen. Dabei ermöglicht CERETRON containerisierte Algorithmen und modulare Funktionen, die plattformunabhängig in verschiedenen Truppengattungen und für unterschiedliche Einsatzzwecke eingesetzt werden können.
Automatisierte Sensorlösungen kombiniert mit einem optimierten Backend-Workflow steigern die Effizienz in vielfältigen Einsatzszenarien. Dies umfasst den Selbstschutz, die Überwachung großer Räume, Nahbereichsabsicherung, Unterstützung im Marsch, den Infanterietransport, Zielfindung, Geschützausrichtung und „Joint Fire Support“. Kollaborative Tools vernetzen die Rollen innerhalb von Fahrzeugen und binden über Schnittstellen den Informationsfluss von- und zu Führungsständen ein – ein entscheidender Vorteil im modernen Gefecht.

Vernetzung, Automation und Software Defined Defence auf Landfahrzeugen

CERETRON integriert verschiedenste Sensoren – von bildgebender Technik in diversen Wellenlängen über Akustik, Radio und Radar bis hin zu 360°-Situational-Awareness-Systemen – in einem zentralen Core. Intelligente Assistenten übernehmen das aggregierte Health Monitoring der Sensorik, ermöglichen missionsspezifische Parametrisierung und sichern eine effiziente Datenerfassung inklusive smartem Reporting. Automatische Objekterkennung, Informationsanreicherung und die Eliminierung redundanter Daten garantieren, dass selbst bei niedrigen Bandbreiten nur relevante Informationen verteilt werden.
Im Fokus steht dabei das Prinzip der Software Defined Defence: Durch flexible, softwarebasierte Anpassungen können Systeme rasch aktualisiert und an veränderte Bedrohungslagen angepasst werden. So lassen sich nicht nur klassische Verteidigungsszenarien abbilden, sondern auch neue Bedrohungsbilder, wie Drohnen- oder Raketenangriffe, frühzeitig erkennen und wirksam abwehren. Moderne Cybersicherheitstechnologien schützen dabei das Datenmanagement und ermöglichen umfassende Auswertungen – auch im Nachgang.

CERETRON – Sensorintegration in Landfahrzeugen

Foto: Hensoldt

Drohnenerkennung, Performance und Nutzerzentrierung

Ein herausragendes Merkmal von CERETRON ist die frühzeitige Erkennung von Bedrohungen durch Drohnen ohne spezialisierte Selbstschutzsensorik. Vernetzte Auswertung multipler Sensoren und Fusion von Information aus Algorithmen identifizieren potenzielle Gefahren, was die Sicherheit der Einsatzkräfte deutlich erhöht. Optimierte Speicher- und Stromnutzung sowie eine verbesserte Softwareperformance sichern schnelle Informationsgewinnung und Datenübertragung. Rollenspezifische Datenaufbereitung und KI-gestützte Objekterkennung verbunden mit intuitiven Bedienkonzepten und Nutzerführung entlasten die Fahrzeugbesatzung, sodass sich Soldaten voll auf ihre Kernaufgaben konzentrieren können.
Der modulare Aufbau von CERETRON erlaubt flexible Anpassungen an diverse Missionsprofile – von Einzelalgorithmen bis zu kompletten Einsatzpaketen mit automatisierten Backends und Frontends gemäß militärischer Designstandards. Erweiterungen erfolgen bequem per Software-Update, ohne umfangreiche Hardwareanpassungen. Die Integration interner und externer Datenquellen, etwa von Drohnen oder CBRN-Sensoren, schafft eine verlässliche Informationsgrundlage für sichere Entscheidungen.

NATO-Standards, Shared Information Space und zukunftsweisende Transformation

CERETRON erfüllt strenge Militärstandards wie NGVA und GVA, was die Interoperabilität mit anderen NATO-Systemen sicherstellt und multinationale Einsätze erleichtert. Durch die Einbindung in den Shared Information Space und der nahtlose Datenaustausch mit Führungssystemen wie FüWES und BMS optimiert die Lösung die Digitale Gefechtsführung und Unterstützung (DGU).

Mit dem integrativen Ansatz der Software Defined Defence leitet HENSOLDT in seinem gesamten Software- und Hardwareportfolio eine digitale Transformation ein, bei der Sensorlösungen kontinuierlich an neue Bedrohungsszenarien angepasst werden. Diese Innovationskraft und Plattformunabhängigkeit sichern, dass Systeme stets auf dem neuesten Stand der Technik operieren. HENSOLDT, mit einem Umsatz von 1,85 Mrd. Euro (2023) und rund 8.000 Mitarbeitern, bleibt damit ein zentraler Akteur der europäischen Verteidigungsindustrie – bereit, den Herausforderungen der Zukunft mit intelligenter, vernetzter und adaptiver Technologie zu begegnen.

Computacenter

EINSATZFÄHIG. SOFORT.

Vertrauen Sie auf jahrzehntelange Erfahrung und Umsetzungsstärke für effiziente und sichere IT-Arbeitsplatzlösungen.

Computacenter:
Ihr Partner für IT-Services & Logistik.

AI Assurance: Vertrauen, Sicherheit und schnelle Einsatzfähigkeit für KI-Systeme in der Bundeswehr

Kim-Laura Wöhlk, IABG; Rafal Kaluga, IABG, Bastian Bernhardt, IABG

Kim-Laura Wöhlk

Foto: IABG

Mit der fortschreitenden Digitalisierung und der Einführung disruptiver Technologien steht die Bundeswehr vor einer doppelten Zeitenwende. Neue technologische Möglichkeiten revolutionieren militärische Operationen und Entscheidungsprozesse, während zugleich die wachsende Komplexität und Vernetzung dieser Systeme neue Anforderungen an deren Sicherheit und Verlässlichkeit stellen. Besonders die Integration von künstlicher Intelligenz (KI) in sicherheitskritische Anwendungen erfordert ein hohes Maß an Vertrauen. Um dies zu gewährleisten, rückt das Konzept der **AI Assurance**, der systematischen Absicherung von KI-Systemen, in den Mittelpunkt moderner Absicherungsstrategien.

Rafal Kulaga

Foto: IABG

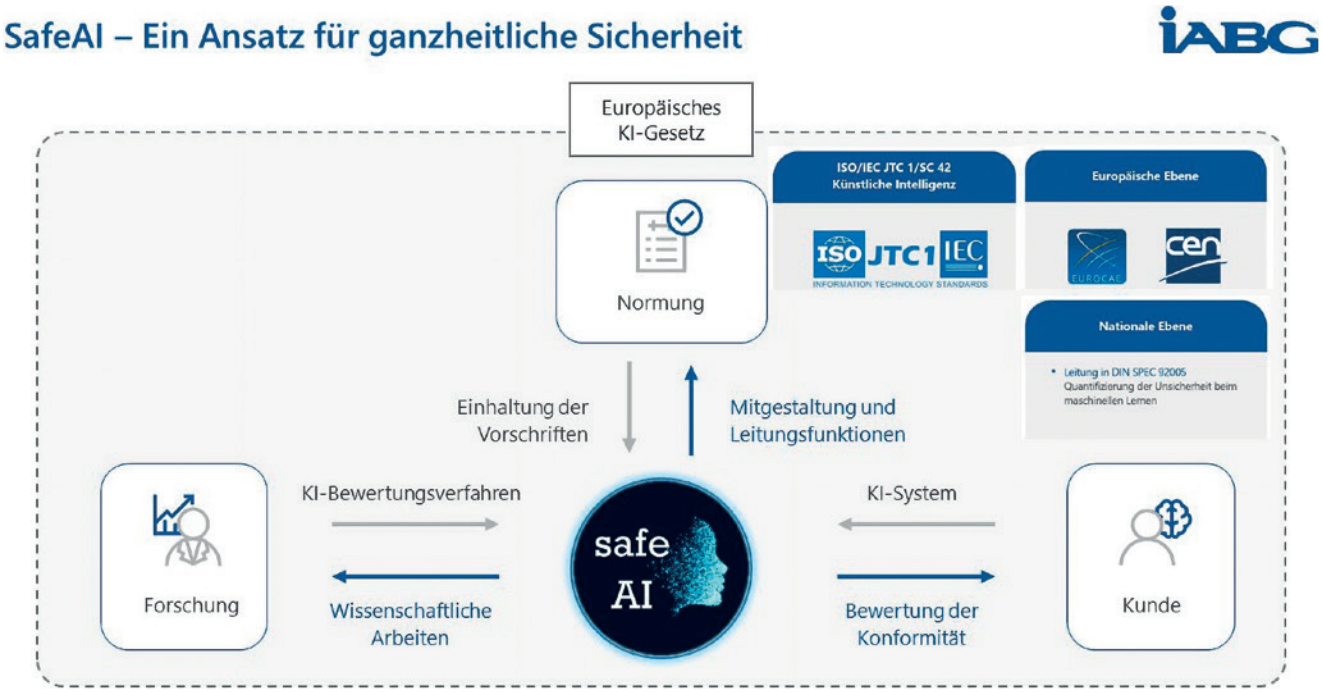
Die Einsatzmöglichkeiten von KI in der Bundeswehr sind vielfältig und reichen von der Automatisierung logistischer Abläufe über die Verarbeitung großer Datenmengen aus Sensor- und Aufklärungssystemen bis hin zur Entscheidungsunterstützung in dynamischen, sich schnell verändernden Szenarien. Die Vorteile liegen auf der Hand: KI setzt an, wo klassische Lösungen an ihre Grenzen kommen. Sie kann enorme Datenmengen analysieren, Muster erkennen und auf dieser Basis Handlungsempfehlungen ableiten, die weit über die Fähigkeiten traditioneller Systeme hinausgehen. Doch so beeindruckend diese Fortschritte auch sind, sie bringen Herausforderungen mit sich, die nicht ignoriert werden dürfen. KI-Systeme müssen nicht nur zuverlässig funktionieren („Konformitätserklärung“), sondern auch robust gegen Angriffe sein, nachvollziehbare Entscheidungen treffen und regulatorischen sowie ethischen Anforderungen genügen. Ein besonders kritischer Aspekt ist die Frage der Verlässlichkeit und Robustheit. KI-Systeme sind komplex und basieren oft auf maschinellen Lernverfahren, die große Mengen an Daten nutzen, um Modelle zu trainieren. Diese Modelle sind jedoch nicht immun gegen Manipulationen oder unvorhergesehene Einflüsse. Schon kleine Änderungen an den Eingangsdaten können die Funktionsweise von KI-Systemen erheblich beeinträchtigen und in sicherheitskritischen Anwendungen fatale Folgen haben. Dies macht es unabdingbar, dass KI nicht nur leistungsfähig, sondern auch resilient gegen äußere Eingriffe gestaltet wird.

safeAI: Ein Ansatz für ganzheitliche Sicherheit

Bastian Bernhardt

Foto: IABG

Moderne Absicherungskonzepte wie der safeAI-Ansatz der IABG greifen auf einen ganzheitlichen Ansatz zurück, um diese Herausforderungen zu bewältigen. Neben funktionaler Sicherheit legt safeAI den Fokus auf die Gestaltung von sicheren und vertrauenswürdigen KI-Systemen. Dies erfordert eine Kombination technischer und organisatorischer Maßnahmen, die auf gesamten Lebenszyklus eines KI-Systems wirken. safeAI setzt auf fortschrittliche Test- und Validierungsumgebungen, die realistische Einsatzszenarien nachbilden und Schwachstellen frühzeitig aufdecken. Dabei wird nicht nur die technische Leistung geprüft, sondern auch die Fähigkeit der KI, sich in unerwarteten oder dynamischen Situationen robust zu verhalten. Ergänzend integriert safeAI statistisch fundierte Sicherheitsmaßnahmen, wie die Bewertung der Unsicherheit oder der Robustheit gegenüber Angriffen. Diese Maßnahmen gewährleisten, dass die Systeme unter realen Bedingungen zuverlässig und sicher arbeiten. Ein weiterer Schwerpunkt von safeAI liegt auf der Erklärbarkeit und Transparenz. Gerade in sicherheitskritischen Kontexten müssen die Entscheidungen einer KI für die Nutzer nachvollziehbar sein. safeAI-Ansätze setzen hier auf Methoden der erklärbaren KI (Explainable AI, XAI), die Entscheidungswege offenlegen und so das Vertrauen der Anwender stärken. Für die Bundeswehr, die in hochkomplexen und oft unvorhersehbaren Szenarien agiert, ist diese Transparenz essenziell, um fundierte Entscheidungen treffen zu können.



safeAI – Ein Ansatz für ganzheitliche Sicherheit

Foto: IABG

Regulatorische und ethische Rahmenbedingungen

Neben der technischen Absicherung steht safeAI auch für die Einhaltung regulatorischer und ethischer Anforderungen. KI-Systeme müssen nicht nur zuverlässig funktionieren, sondern auch den strengen Vorgaben nationaler und internationaler Standards genügen. Mit safeAI unterstützt und entwickelt die IABG zertifizierbare Prozesse, begleitet Standardisierungsverfahren und passt das „Absicherungskonzept“ an. Darüber hinaus trägt die IABG mit safeAI aktiv führend zur Entwicklung von KI-Standards bei, etwa durch die Initiierung der DIN SPEC 92005 und die Mitwirkung an der ISO/IEC AWI TS 25223.

Die Bedeutung eines ganzheitlichen Ansatzes

Ein moderner Ansatz wie safeAI zeigt, dass AI Assurance nicht nur technische Innovation bedeutet, sondern auch ein ganzheitliches Denken erfordert. Die Kombination aus Sicherheitsanalysen, leistungsfähigen Simulationsumgebungen und einer systematischen Validierung trägt dazu bei, Vertrauen in KI-Systeme zu schaffen. safeAI betont dabei die Rolle einer nachhaltigen Sicherheitskultur, die technische Exzellenz mit organisatorischer Verantwortung verbindet.

Fazit: Vertrauen als Basis für Innovation

AI Assurance, gestützt durch innovative Ansätze wie safeAI, bildet die Grundlage, um Chancen für die Bundeswehr sicher und verantwortungsvoll zu erschließen. Dabei verbindet safeAI technische, regulatorische und ethische Aspekte und liefert somit einen entscheidenden Beitrag für die Einsatzfähigkeit und Resilienz moderner Streitkräfte.

SICHERHEIT IST DIE MUTTER ALLER NACHHALTIGKEIT

Die mehr als 300 Mitgliedsunternehmen des Bundesverbandes der Deutschen Sicherheits- und Verteidigungsindustrie e.V. (BDSV) sind hochqualifizierte Zulieferer und Partner der Bundeswehr und der Behörden und Organe mit Aufgaben der inneren Sicherheit.

Damit tragen unsere Mitglieder unmittelbar auch zu Frieden, Sicherheit und Nachhaltigkeit bei.

BDSV

AFCEA Bonn e.V.

38. AFCEA Fachausstellung 2025

Willkommen Welcome Bienvenu

38. AFCEA FACHAUSSTELLUNG

World Conference Center Bonn

Der Treffpunkt der IT-Community Bundeswehr und BOS

AFCEA Bonn e.V.

2025

Digitalisierung und Fähigkeitsentwicklung

Einen Überblick über die AFCEA-Symposien finden Sie auf Seite 71 sowie über den Link (QR-Code):

Einen Überblick über die Ausstellerliste finden Sie auf Seite 72-73 sowie über den Link (QR-Code):

Zwischen den Keynotes laden unsere Aussteller auch in diesem Jahr wieder zu spannenden Fachvorträgen parallel in den Saal Addis Abeba III oder in den historischen Plenarsaal. Über den Link (QR-Code) finden Sie die Vortragsthemen, die Redner und die Abstracts.

AFCEA Bonn e.V.

Symposium AFCEA FA 2025

„Digitalisierung und Fähigkeitsentwicklung“

27. / 28. Mai 2025 | World Conference Center Bonn

Dienstag 27. Mai 2025 | 09:00 Uhr – 18:00 Uhr | Ausstellung Vorträge der Key Notes und Symposien finden im ehemaligen Plenarsaal des Bundestages statt	
09:30 Uhr	**Begrüßung/Eröffnung der 38. AFCEA Fachausstellung**
	Generalmajor Armin Fleischmann, Kdo CIR, Vorstandsvorsitzender AFCEA Bonn e.V.
	Oberst a.D. Wolfgang Quirin, Leiter der AFCEA Fachausstellung Bonn
09:40 Uhr	**Key Note: Der Wirtschaftstandort NRW**
	Staatsminister Nathanael Liminski, Minister für Bundes- und Europaangelegenheiten, Internationales sowie Medien des Landes Nordrhein-Westfalen und Chef der Staatskanzlei
18:00 Uhr – 22:00 Uhr | Get-together AFCEA Fachausstellung 2025	

Mittwoch 28. Mai 2025 | 09:00 Uhr – 18:00 Uhr | Ausstellung	
10:00 Uhr bis 11:00 Uhr	**Digital Defence Debate** “Fit for the future? Notwendige Weichenstellungen für gelingende Gesamtverteidigung in Deutschland“ Organisiert und moderiert durch die Emerging Leaders der AFCEA Bonn e.V.
	Panelteilnehmer: Neben weiteren geladenen Experten und Expertinnen aus dem sicherheitspolitischen Umfeld werden **BrigGen Dr. Pötzsch** (UAL BMVg CIT I) und **Dr. Haas** (CDO Rheinmetall) teilnehmen.
	Moderation: Valerie Lünsmann (BwConsulting GmbH, Inhouse Beratung der Bundeswehr) und **Yuliya Maltseva** (Women in Defence Tech)
11:05 Uhr bis 12:00 Uhr	**Startup Pitch & Panel Session**
	Moderation: Anna Lena Hohmann und **Frank Dürrbeck**
	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.
	Jury: Prof. Eva-Maria Kern (UniBw M UC), sowie je ein Vertreter aus der Industrie, Venturecapital und Bundeswehr.
14:30 Uhr	**Key Note: Ausblick auf Digitalisierung in Deutschland/Bayern;** was ist zu tun in DEU; gute Beispiele; wie kommen wir wieder vor die Welle; Hochtechnologiestandort, KI, Big Data, Digitalisierung, neues Ministerium.
	Bayerischer Staatsminister Dr. Fabian Mehring
Abschluss des Symposiums und Schlusswort **Generalmajor Armin Fleischmann,** Kdo CIR, Vorstandsvorsitzender AFCEA Bonn e.V.	

Ausstellerliste AFCEA Fachausstellung 2025

Bedeutung der Standabkürzungen:
Ausstellungsfläche

F = FOYER EINGANGSBEREICH
N = SAAL NAIROBI
W = SAAL WIEN
G = FOYER GALERIE
S = SAAL NEW YORK/GENF
R = RHEINEBENE
B = SAAL BANGKOK
A = AUSSENBEREICH

Aussteller (Stand 03.04.2025)	Standnr.
]init[AG	B12
A. WEIDELT Systemtechnik GmbH & Co. KG	S60
Accenture	W07
adesso SE	G02
Adva Network Security GmbH	N04
AIRBUS	F03
Akkodis Edge Germany GmbH	N07
Alcatel-Lucent Enterprise	S17
Alfabet BD GmbH	S20
Amphenol Precision Optics GmbH	F30
Amphenol-Air LB GmbH	F30
Amphenol-Air LB GmbH	R12
ATDI Group	F14
AVS Systeme GmbH	S21
B&T Solutions GmbH	F14
B&W International GmbH	F14
BAKO Systemintegration GmbH & Co. KG	S84
BAPersBw/HRLab	R62
Barco	S21
BDSV e.V.	S41
Bechtle AG	S18
Bechtle Logistik & Service, Apple Authorised Enterprise Reseller	S18
Behörden Spiegel-Gruppe	F34
Bernd Richter GmbH	R12
Bertrandt AG	R71
best Systeme GmbH	R48
Bittium	F14
Black Box Deutschland GmbH	S05
blackned GmbH	S40
BlueBird Aero Systems	S86
Bren-Tronics International Solutions	S83
BRESSNER Technology GmbH	B05
Brodit GmbH	F14
Bundeswehr, Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAAINBw)	N05
BWI GmbH	F07
CAE GmbH	W05
Capgemini Deutschland GmbH	N02
Carl-Cranz-Gesellschaft e.V.	R24
Carmenta Germany GmbH	W11
Cellebrite GmbH	B01a
CENIT	R63
CEOTRONICS AG	F26
CGI Deutschland B.V. & Co.KG	F04
CGI Deutschland B.V. & Co.KG	A03
Chora GmbH	S76
Cisco Systems GmbH	F08
citema group GmbH	F11
Codan Communications	F14
Computacenter AG & Co. oHG	W02
Comrod Communication AS	F17
CONDOK GmbH	S01
CONET	S45
Conrad Electronic SE	F35
Constructor University Bremen gGmbH	F09
Cordsen Engineering GmbH	S75
CPI Vertex Antennentechnik GmbH	R27
CPM GmbH	N06
dainox GmbH	S33
Dassault Systemes Deutschland GmbH	R11
DATAGROUP Defense IT Services	S73
DATAGROUP Defense IT Services	A04
Dataminr Germany GmbH	R52
Data-Warehouse GmbH	F36
DCON GmbH	F32
deepset GmbH	R48
Dell GmbH	S18
Dell Technologies	R51
DESAPRO AG	R73
Deutsche Gesellschaft für Wehrtechnik e.V	R28
Deutsche Telekom Geschäftskunden GmbH	F06a1
Deutsche Telekom Geschäftskunden GmbH	F06a2
DIAMOND GmbH	R17
DIGITTRADE GmbH	F29
DriveLock SE	S61
dtec.bw - Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr (UniBw M)	N03
D-Trust GmbH	S25
Dynamit Nobel Defence	S31
EAL Leidel GmbH	S42
ECOS Technology GmbH	F27
EGL Elektronik Vertrieb GmbH	S57
EIZO Europe GmbH	S82
Elbit Systems Deutschland	F23
eleQtron GmbH	R48
Elma Electronic	R46
ELP GmbH European Logistic Partners	R72
Emerging Leaders AFCEA	AA01
Emerging Leaders AFCEA	AA02
Emerging Leaders AFCEA	AA03
Emerging Leaders AFCEA	AA04
Emerging Leaders AFCEA	AA05
Enercon Technologies Europe AG	S15
EPAK GmbH	S07
Epson Deutschland GmbH	R18
Esri Deutschland GmbH	F22
Eviden GmbH	F31
Extron	S66
FERCHAU GmbH	R56
FFG Flensburger Fahrzeugbau Gesellschaft mbH	F14
Forschungszentrum Space - UniBw München	S74
Fortinet GmbH	S04
Fraunhofer FKIE	F15
Fraunhofer IOSB	W01
Frequentis Deutschland GmbH	S28
Fujitsu Germany GmbH	F13
GAF AG	S22
GAF AG	A08
GBS TEMPEST & Service GmbH	S03
genua GmbH	S25
Gesellschaft für Sicherheitspolitik e.V.	R07
Getac Technology GmbH	W02
Glenair GmbH	S72
Global RadioData Communications Europe Ltd.	S16
GMC TASSTA GmbH	F14
Google Germany GmbH	G01
griffity defense GmbH	F14
Hagenuk Marinekommunkation GmbH	B07
HAT.tec GmbH	R14

Helsing GmbH	S71
hema electronic GmbH	B09c
HENSOLDT	F01
HENSOLDT	A05
Hexagon - HxGN Safety & Infrastructure GmbH	S14
Hirt Zerspanungstechnik GmbH	F24
Hitachi Vantara GmbH	F25
HPE Aruba Networking	S18
IABG mbH	W06
IABG Teleport GmbH	W06
IBM Deutschland GmbH	F02
iesy GmbH	S63
IGEL Technology GmbH	A01
Ihse GmbH	S81
Imtradex Hör- und Sprechsysteme GmbH	F14
Indra (Indra Avitech, Indra Sistemas, Indra Park Air & Indra Air Traffic)	S11
INFODAS GmbH	S46
INNOSYSTEC GmbH	S34
Intracom Defense S.A.	F14
IntraFind Software AG	R41
inxire GmbH	F37
ISEC7 GmbH	S51
itWatch GmbH	S10
Janes	R47
JK Defence & Security Products GmbH	S30
JOWO - Systemtechnik AG	W10
Kappa optronics GmbH	R19
Knapp Service Koblenz GmbH	W09
KNDS Deutschland GmbH & Co. KG	A11
KNDS Deutschland Mission Electronics GmbH	S48
Kommando Cyber- und Informationsraum	B03
Kommando Heer	S65
Kommando Luftwaffe	G03b
KPMG AG Wirtschaftsprüfungsgesellschaft	S26
L3Harris Technologies	S30
LEONARDO Germany GmbH	A06
LS telcom	B08
LWL-Sachsenkabel GmbH	F30
M4Com System GmbH	R43
Marinekommando	G03a
Materna Information & Communications SE	S52
Materna Virtual Solution GmbH	S56
Media Broadcast Satellite GmbH	S29
Micropol Fiberoptic GmbH	F33
Microsoft Deutschland GmbH	R57
Mittler Report Verlag GmbH	R13
ML Eingabesysteme GmbH	B01b
mmt gmbh I Meffert Microwave Technology	B06b
MÖNCH Verlag GmbH	R10
Motorola Solutions Germany GmbH	S32
Narda Safety Test Solutions GmbH	F14
ND SATCOM GmbH	S43
NEOSAT GmbH	S74
NetApp Deutschland GmbH	W02
NetApp Deutschland GmbH	S18
Newsletter Verteidigung / VDS Verlag	R08
nexus	S19
NI Network Innovations	B09b
NTT DATA	S17
NVIDIA GmbH	R48
NVIDIA GmbH	R51
NVIDIA GmbH	S18
ODM GmbH	F28
OHB SE	F20
Panasonic Connect Europe GmbH	F05
PEGA	F04
PELI PRODUCTS GERMANY GmbH	S02
Pexip Germany GmbH	R22
PHYSEC GmbH	F04
Planet Solutions GmbH	S18
Planungsamt der Bundeswehr	R61
PLATH GmbH & Co KG	F18
PNY Technologies Quadro GmbH	R48
ProCase GmbH	R23
promegis Gesellschaft für Geoinformationssysteme mbH	S13
ProSoft GmbH	S61
PROSTEP AG	R16
Pure Storage GmbH	B10
QGroup GmbH	R42
Quantum-Systems GmbH	A10a
Raptor Photonics	B09a
RHEINMETALL	N09
RHEINMETALL	N01
RHEINMETALL	R57
Rick Location Solutions GmbH	F22
Rocket.Chat Technologies Inc.	B04
roda computer GmbH	F05
Rohde & Schwarz GmbH & Co. KG	F10
rola Security Solutions GmbH	F06b
RUAG GmbH	S70
SailPoint Technologies GmbH	R15
SAP Deutschland SE & CoKG	F21
SAP Deutschland SE & CoKG	A20
Satcube AB	F16
Schönhofer Sales and Engineering GmbH	S54
SCOPE Engineering GmbH (ARBOR Gruppe GmbH)	R63
SCOTTY Group Austria GmbH	N08
SCOTTY Group Austria GmbH	A02
secunet Security Networks AG	F19
Secusmart GmbH	S51
SELECTRIC Nachrichten-Systeme GmbH	S35
Sepura Deutschland GmbH	S35
SES SPACE & DEFENCE	B11
Siemens Industry Software GmbH	G04
SINORA Cases	R23
Skyline Europe GmbH	S85
Skyline Europe GmbH	S86
Software AG	S20
Soldaten- und Veteranenstiftung	R09
Solifos Deutschland GmbH	S27
Sophos Technology GmbH	S62
Sopra Steria SE	S12
STACKIT GmbH & Co. KG	A07a
steep GmbH	S39
Stellar PCS	F14
SThree GmbH	S52
SVA System Vertrieb Alexander GmbH	S53
Systematic GmbH	S47
systerra computer GmbH	S64
tde - trans data elektronik GmbH	S06
TEKSAM GMBH	W03
Telespazio Germany GmbH	S22
Telespazio Germany GmbH	A08
Thales Deutschland	S23
Thinklogical LLC	F14
TQ Systems GmbH	B09d
Trend Micro Deutschland GmbH	S36
Treo - Labor für Umweltsimulation GmbH	S55
Unterstützungskommando der Bundeswehr	R64
USU GmbH	R54
Utimaco	S19
VDI TZ GmbH / NKS Europäischer Verteidigungsfonds	R29
VECTED GmbH	R55
Verband der Reservisten der Bundeswehr e.V.	B02
Viasat	A07c
Vitec GmbH	W04
Willert Software Tools GmbH	B06a
WORK Microwave GmbH	F12
Xecuro GmbH	S25
Zarges GmbH	W08
Zebra Technologies GmbH	S35

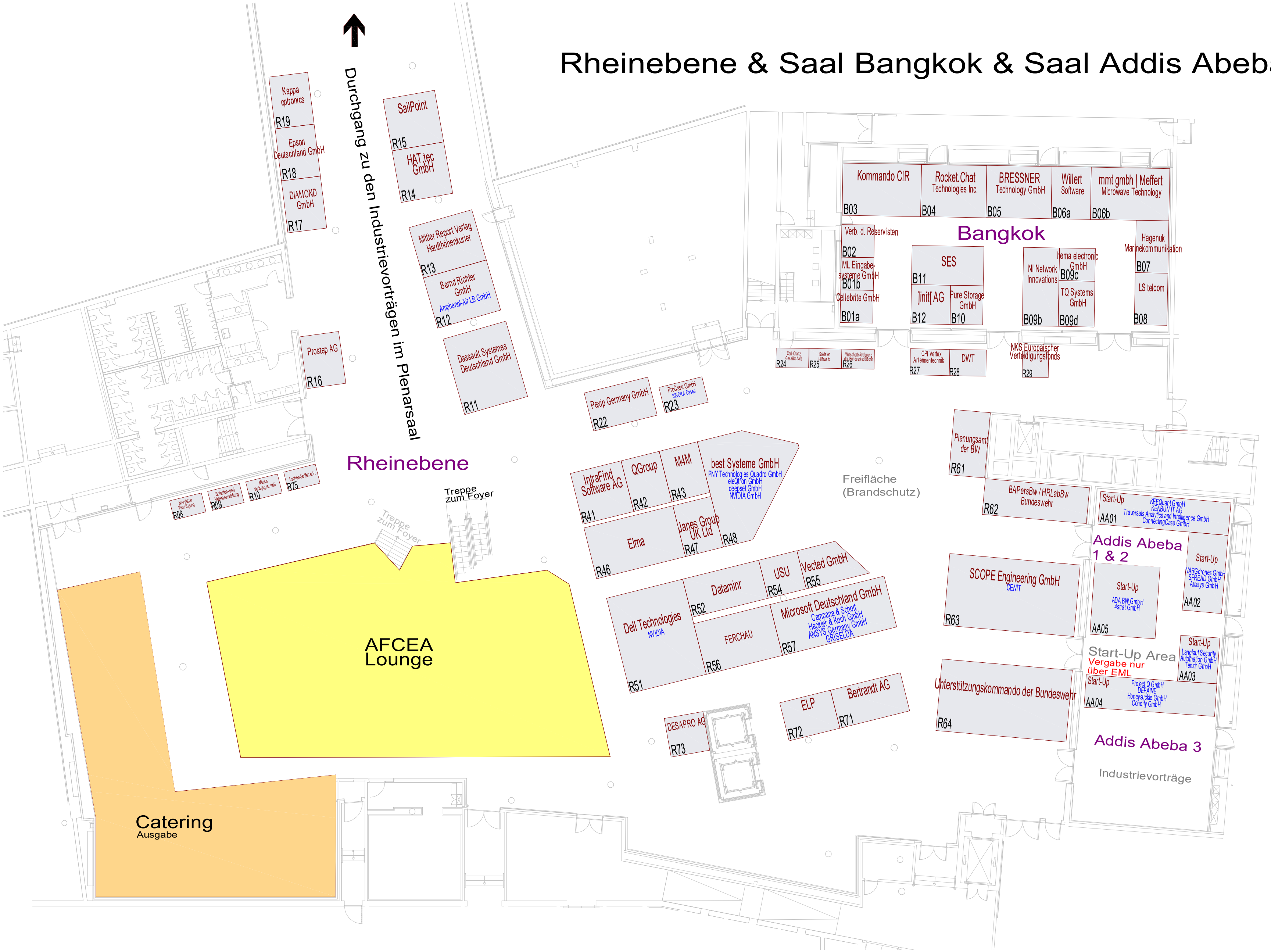
Standpläne im World Conference Center Bonn

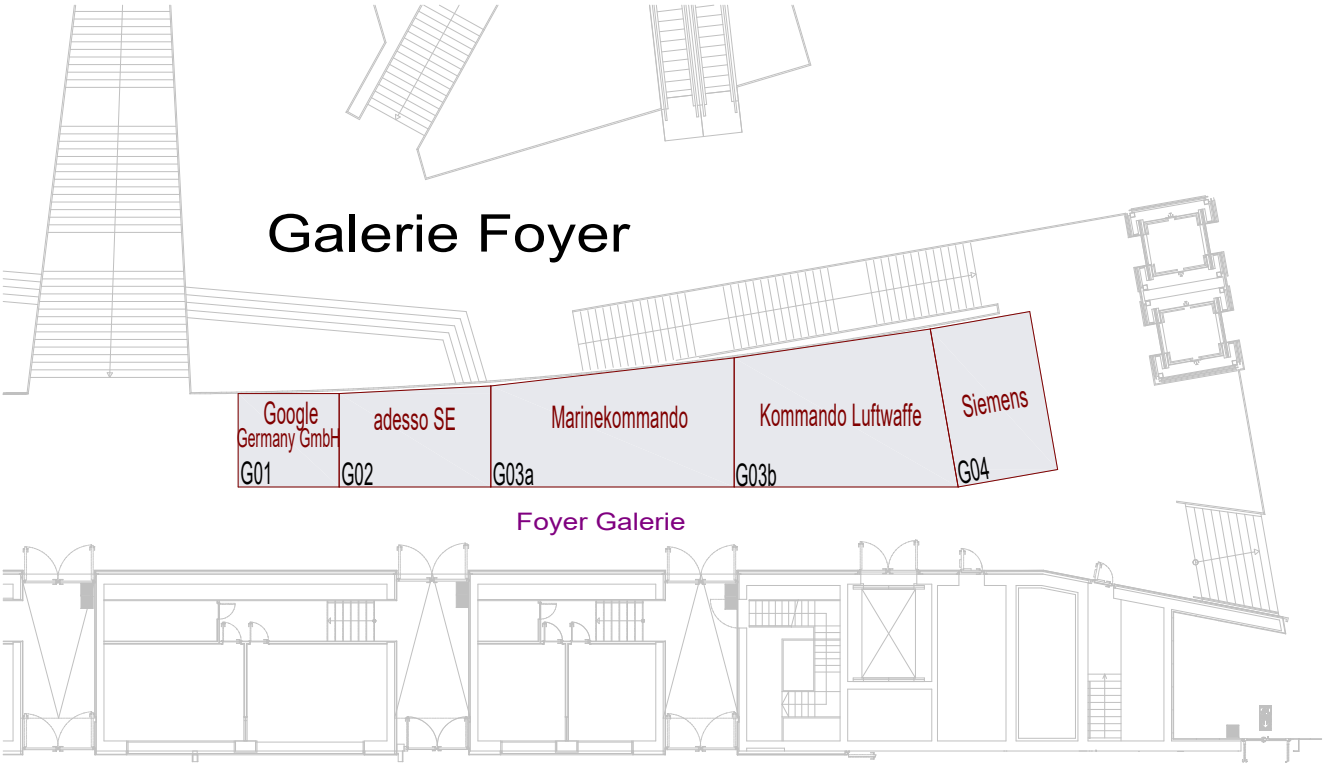
Saal New York / Genf

Übergänge ins Foyer Eingangsbereich

Saal Nairobi & Saal Wien

Rheinebene & Saal Bangkok & Saal Addis Abeba




Galerie Foyer
Google Germany GmbH
G01
adesso SE
G02
Marinekommando
G03a
Kommando Luftwaffe
G03b
Siemens
G04
Foyer Galerie

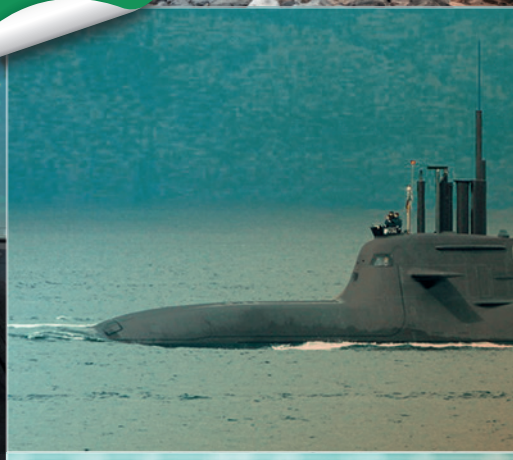

Außenbereich
Eingang Plenarsaal
Entrance Plenary
KNDS
A11
Pfleger Group Gmbh
A10b
Quantum-Systems GmbH
A10a
A09b
A09
Telespazio Germany GmbH
A08
STACKIT
A07a
Zscaler Germany GmbH
A07b
Viasat
A07c
SAP
A20
LEONARDO Germany GmbH
A06
HENSOLDT
A05
DATAGROUP Defense IT Services
A04
CGI
A03
IGEL Technology GmbH
A01
SCOTTY Group Austria GmbH
A02
Veteranenbüro der Bundeswehr
A100
Haupteingang
Main entrance

System integration — customer centric & independent

TO PROTECT & PREVENT

ONE STEP AHEAD WITH INNOVATIVE INTELLIGENCE SOLUTIONS

BESUCHEN SIE UNS AUF DER **AFCEA 2025: STAND F18**



Bessere Entscheidungen – mehr Handlungsspielraum

Datenbasierte Krisenfrüherkennung mit PLATH Systems & Integration:

- Spitzentechnologie für mehr Sicherheit
- Bewährte Systeme für Operationen an Land, auf See, in der Luft & im Cyberspace
- Global Player mit hoher Innovationskraft & jahrzehntelanger Branchenerfahrung

plath.de

PLATH

Systems & Integration

Symposium und Industrievorträge

Zeitplan für die Industrievorträge bei der FA 2025

AFCEA Fachausstellung 2025

27.05.2025	incl. Live-Aufzeichnung Plenarsaal Bundestag		Vortragssaal ADDIS ABEBA 3	
09:00				
09:30				
10:00	Eröffnung u. KeyNote 1			
10:30				
11:00				
11:05 - 11:30	1	QGroup	15	Dassault Systems
11:35 - 12:00	2	SCOTTY	16	Accenture
12:05 - 12:30	3	Materna Information	17	IntraFind Software
12:35 - 13:00	4	Secusmart	18	Uni Bw München
13:05 - 13:30	5	Rheinmetall	19	Adva Network
13:35 - 14:00	6	Motorola	20	best Systeme
14:05 - 14:30	7	SINORA Cases	21	Prostep AG
14:35 - 15:00	8	CONET	22	IBM
15:05 - 15:30	9	Sophos	23	Thales
15:35 - 16:00	10	Constructor Uni	24	Pure Storage
16:05 - 16:30	11	Google	25	AIRBUS
16:35 - 17:00	12	rola	38	Plath
17:05 - 17:30	13	Esri	39	Genua
17:35 - 18:00	14	Hensoldt	40	USU
18:00				
19:00				
20:00				
21:00				
22:00				

AFCEA Bonn e.V.
lädt
Aussteller
und
Besucher
ein zum
Get-Together
(RHEINEBENE)

AFCEA Fachausstellung 2025

28.05.2025	incl. Live-Aufzeichnung Plenarsaal Bundestag		Vortragssaal ADDIS ABEBA 3	
09:00				
09:30				
10:00	KeyNote 2 Defence-Debate			
10:05 - 10:30				
10:35 - 11:00				
11:05 - 11:30	26	ELA	32	Infodas
11:35 - 12:00	27	StartUp-Pitches	33	Narda
12:05 - 12:30	28	CGI	34	SThree
12:35 - 13:00	29	Deutsche Telekom	35	NVIDIA
13:05 - 13:30	30	Bechtle	36	Data Warehouse
13:35 - 14:00	31	Dainox	37	roda Computer
14:30	KeyNote 3			
15:00				
15:30				
16:00				
16:30				
17:00	Ende der Fachausstellung 2025			

Themen der Industrievorträge

Slot	Aussteller	Thema des Industrievortrages
1	QGroup GmbH	Abwehr staatlicher APT in eingestuften Bereichen: Modernstes Cyberimmunsystem mit voller Datensouveränität
2	SCOTTY Group Austria GmbH	Kommunikation, sicher und resilient
3	Materna Information & Communications SE	Gemeinsame Datenräume in Kollaborationsplattformen als zukünftige Basis von Software Defined Defence
4	Secusmart GmbH	Titel lag zum Redaktionsschluß noch nicht vor
5	RHEINMETALL	Rheinmetall Battlesuite: Die digitale Plattform für vernetzte Militärsysteme – Der Schlüssel zur Überwindung von Silos im Kampfraum
6	Motorola Solutions Germany GmbH	Militärische Führung durch hybride Kommunikation
7	SINORA Cases	Sicher. Mobil. Einsatzbereit. Transportlösungen für moderne Streitkräfte
8	CONET	Decision Intelligence - Fähigkeitsgewinn durch Reasoning-Modelle und Multi-Agenten-AI-Einsatz
9	Sophos Technology GmbH	Cybersecurity im Zeitalter des KI-Hypes
10	Constructor University Bremen gGmbH	Föderierte, interoperable AI-Cubes für GEOINT und FMN
11	Google Germany GmbH	Titel lag zum Redaktionsschluß noch nicht vor
12	rola Security Solutions GmbH	Entscheidungsstärke durch moderne KI-Technologien: Medizinische Lagebilder in Auslandseinsätzen
13	Esri Deutschland GmbH	Geoinformationen im Verteidigungsumfeld: Aktuelle Trends und ihre Bedeutung für die Bundeswehr
14	HENSOLDT	Software-Defined Defence (SDD) als ganzheitlicher Transformationstreiber für Streitkräfte und Industrie
15	Dassault Systemes Deutschland GmbH	„Sicherer Produktionsstart mit Absicherung der Qualität“ (Manufacturing Operations & DIOTA)
16	Accenture	Model-Based Procurement und Model-Based Sustainment: Erfolgreiche Implementierungen in der Verteidigungsindustrie
17	IntraFind Software AG	Titel lag zum Redaktionsschluß noch nicht vor
18	Uni Bw München	Titel lag zum Redaktionsschluß noch nicht vor
19	Adva Network Security GmbH	Schutz sensibler Daten im Zeitalter der Quantencomputer
20	best Systeme GmbH	best und PNY bilden die Lieferkette für Ihre Datenkette mit High Performance Edge Computing
21	PROSTEP AG	Integrated Development Environment für Joint Ventures und Merger - Erfahrungen aus internationalen Projekten, Optimierung der Entwicklungsprozesse, Systemintegration und IP Schutz, Aufbau digitaler Zwillinge, Digital Thread.
22	IBM Deutschland GmbH	Software Defined Defense - Gewappnet für die Verteidigung der Zunkunft
23	Thales Deutschland	Hybride KI für robuste taktische Netzwerke
24	Pure Storage GmbH	Der Schlüssel für mehr Cyberresilienz - Fit für NIS2 mit Pure Storage
25	AIRBUS	SDD = Software als Schlüssel zur taktischen Dominanz
26-27	Emergin Leaders AFCEA Bonn e.V.	Startup-Pitches
28	CGI Deutschland B.V. & Co.KG	OPLAN Deutschland: Führungsfähigkeit als Schlüssel zum Erfolg – Wie flexibler Zugang für alle Organisationen realisiert werden kann
29	Deutsche Telekom Geschäftskunden GmbH	Die Zukunft von Software-Souveränität in der Verteidigungsbranche
30	Bechtle AG	Von Visionen zu Lösungen: Innovationskraft mit der IT entfalten
31	dainox GmbH	IT-Resilienz und digitale Souveränität – Wer nicht flexibel und unabhängig ist, ist angreifbar!
32	INFODAS GmbH	Warum eine leistungsstarke und sichere Netzwerkkarte in Zeiten vernetzter Operationen unverzichtbar ist.
33	Narda Safety Test Solutions GmbH	Passive Drohnenerkennung mit semimobiler Funküberwachung und Funkpeilverfahren
34	SThree GmbH	Sicherheit durch Expertise – Strategisches Recruiting und spezialisierte Teams als Schlüssel zur Cyber-Resilienz
35	NVIDIA GmbH	Accelerate your Software Development with NVIDIA
36	Data-Warehouse GmbH	Q-day, aber sicher? Quantensichere Verschlüsselung: - Krypto-Agilität für die Bundeswehr
37	roda computer GmbH	Solider Connection Hub im Kontext D-LBO
38	PLATH GmbH & Co KG	Software-Defined Defense als Schlüsselstrategie für zukünftige Herausforderungen in autonomen und vernetzten Systemen
39	genua GmbH	„Digitale Festungen: Die Zukunft der Sicherheit mit Software Defined Defence und sicheren Infrastrukturen.“
40	USU GmbH	Von Risiko zu Resilienz: Servicemanagement für sicherheitsrelevante Bereiche

Aussteller AFCEA-Fachausstellung 2025

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

Bedeutung der Standabkürzungen:

F = Ausstellungsfläche FOYER EINGANGSBEREICH
N = Ausstellungsfläche SAAL NAIROBI
W = Ausstellungsfläche SAAL WIEN
G = Ausstellungsfläche FOYER GALERIE
S = Ausstellungsfläche SAAL NEW YORK/GENF
R = Ausstellungsfläche RHEINEBENE
B = Ausstellungsfläche SAAL BANGKOK
A = Ausstellungsfläche AUSSENBEREICH

]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 1050 Mitarbeitende. Zum Kundenkreis gehören das Presse- und Informationsamt der Bundesregierung sowie zahlreiche Bundes- und Landesministerien, die Continental AG und BSH Hausgeräte.

]init[bietet individuell zugeschnittene, praxisbewährte IT-Sicherheitslösungen für Verwaltungen, Organisationen und Sicherheitsbehörden. Unser modulares Portfolio gewährleistet umfassenden Schutz, effektive Risikominimierung und höchste Sicherheitsstandards. Vom CyberRisikoCheck über Penetrationstests bis hin zu ganzheitlicher Multi-Level-Security –]init[ist Ihr verlässlicher Partner für nachhaltige IT-Sicherheit.

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

Accenture — W07

Accenture ist ein global tätiges Beratungsunternehmen, das Unternehmen, Regierungen und Organisationen hilft, einen digitalen Geschäftskern zu entwickeln, ihre Effizienz zu steigern, Umsatzwachstum zu fördern und öffentliche Dienste zu verbessern. Wir schaffen Mehrwert für Kunden in über 120 Ländern. Technologie steht im Zentrum des Wandels, den wir durch starke Partnerschaften im Ökosystem vorantreiben. Unsere 800.000 Mitarbeitenden verfügen über technologische Kompetenz in Cloud, Data und KI sowie Branchen- und Funktionsexpertise. Sie bieten Lösungen in Strategy & Consulting, Technology, Operations, Industry X und Song. Weitere Infos unter www.accenture.de

adesso SE — G02

Kerngeschäftsprozesse optimieren durch den gezielten Einsatz moderner IT.

Erfolgreiches Geschäft entsteht durch innovative Ideen, zukunftsfähige Strategien und passgenaue IT-Lösungen, die Organisatio optimal bei ihren individuellen Herausforderungen unterstützen. Immer sind dabei Menschen beteiligt, die den richtigen Mix aus Technologieexpertise und fundiertem Verständnis für das jeweilige Geschäft der Kunden mitbringen. Mit einem Team von über 10.200 Mitarbeiterinnen und Miterbeiter arbeiten wir an mehr als 60 Standorten innerhalb der adesso Group als einer der führenden IT-Dienstleister im deutschsprachigen Raum täglich daran, die Vorhaben unserer Kunden erfolgreich ans Ziel zu bringen. Als adesso wollen wir auch für unsere nationale Sicherheit einen wesentlichen Beitrag leisten.

Adva Network Security GmbH — N04

Beschr Adva Network Security ist ein führendes deutsches Unternehmen im Bereich IT-Sicherheit. Wir bieten robuste optische und Ethernet-Netzwerklösungen sowie ein umfassendes Dienstleistungsangebot. Unsere ConnectGuard(TM)-Technologie gewährleistet eine quantensichere Verschlüsselung. Kunden in den Bereichen kritische Infrastruktur, Regierung, Verteidigung und Privatwirtschaft schätzen unsere technische Kompetenz sowohl in der Nettechnik als auch der Informationssicherheit. Unser professionelles Serviceteam unterstützt sie vom ersten Entwurf bis zum sicheren Betrieb und sorgt so für die Geschäftskontinuität – trotz zunehmender Cyber-Bedrohungen. Die Design- und Fertigungsprozesse sowie unsere cyberresilienten Lösungen sind von führenden staatlichen Sicherheitsbehörden zertifiziert. eibung

AIRBUS — 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.

Alcatel-Lucent Enterprise — S17

Digital Age Networks von Alcatel-Lucent Enterprise bietet Verteidigungslösungen, die durch Automatisierung, erweiterte Sicherheit und hohe Verfügbarkeit eine geschäftskritische, verschlüsselte Kommunikation für Teams im Büro und auch remote und mobil arbeitende Teams ermöglichen. Die digitale Zusammenarbeit vernetzt alle Nutzer und jedes Gerät, und auf die Verteidigung abgestimmte Funktionen und Geräte halten die Kommunikation auch unter schwierigsten Bedingungen aufrecht.

Amphenol Precision Optics GmbH — F30

Die Amphenol Precision Optics entwickelt Lösungen für faseroptische Kommunikationssysteme und ist Teil der Amphenol Corporation, einem der weltweit größten Anbieter von Hightech-Verbindungslösungen.

Die faseroptischen Steckverbinder von Amphenol Precision Optics, mit ihrer hochpräzisen Ausrichtungstechnologie und ihrer überlegenen verlustarmen optischen Leistung, entsprechen dem militärischen Standard MIL-DTL-83526-20/21.

Kontakt: Amphenol Precision Optics GmbH, Zur Dornheck 32-34, 35764 Sinn

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.

ATDI Group — F14

ATDI delivers spectrum management, frequency assignment, and electronic warfare solutions for defence, government, and security organisations. Its technology integrates communications links, EW sensors, jammers, and radars, ensuring secure operations and enhanced situational awareness.

HTZ Warfare: Tactical network planning tool for resilient networks across airborne, terrestrial, and maritime platforms. ICS Monitoring SDRN Control: A vendor-neutral RF monitoring solution for spectrum surveillance, data analysis, and EW operations.

HTZ Web API: Provides high-accuracy network planning, optimisation, and RF analysis, automating workflows. With 30+ years of expertise, ATDI enhances military spectrum operations worldwide.

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*

B&T Solutions GmbH — F14

B&T Solutions GmbH ist Teil der MOSOLF Group, Spezialist im Sonderfahrzeugbau in den Bereichen BOS, Verteidigung, Öffentlicher Sektor, Industrie und bietet Komplettlösungen aus einer Hand – seit mehr als 30 Jahren.

Ganz nach Kundenwunsch statten wir Fahrzeuge in unserem Produktionsnetzwerk aus oder liefern technische Ausrüstung. Mit unserem mobilen Serviceteam führen wir europaweit auch Sonderlösungen oder Nachrüstungen vor Ort aus.

Neben Fahrzeugumbauten bieten wir ganzheitliche Lösungen im Funk- und Komponentenbau, von mechanischen Bauteilen über Kabelbäume und kompletten Funkverkabelungen bis zu komplexen Informations- und Kommunikationssystemen.

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.

BAPersBw/HRLab 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. Der Aufwuchs der Bundeswehr stellt das Personalmanagement vor Herausforderungen, denen das BAPersBw unter anderem mit umfassenden Digitalisierungsmaßnahmen und innovativen Ansätzen in der Personalgewinnung begegnet.

Zentraler Bestandteil dieser Zukunftsstrategie ist das Human Resources Laboratory (HR Lab). Hier werden neue Methoden, Verfahren und Technologien erprobt und die Entwicklung von Innovationen bis zur Einsatzreife vorbereitet. Kontakt: BAPersBw HRLab, Militärringstraße 1000, 50737 Köln, Britta Sturm-Platz, Tel.: +49 221 9571 6574, Mail: BrittaSturmPlatz@bundeswehr.org

Barco Control Rooms GmbH S21

Barco has decades of expertise in the critical control room market. First as a pioneer in large visualization, later also as an innovator in control room workflow and workspace solutions.

This vast amount of experience makes us a trusted partner for public safety and security applications. Our goal is to enhance situational awareness and optimize operations, for better and faster decision-making. All our solutions are purpose-made for the critical control rooms market, with world-class cybersecurity measures integrated into our platforms. We are an established Belgian company, with a global reach. For more information, please contact us at controlrooms@barco.com or visit us at https://www.barco.com/en

BDSV e.V. S41

Der Bundesverband der Deutschen Sicherheits- und Verteidigungsindustrie vertritt rund 250 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

Bechtle AG S18

Bechtle: Der IT-Zukunftspartner im Public Sector

Bechtle ist mit über 100 IT-Systemhäusern nah an den Kunden und zählt mit IT-E-Commerce-Gesellschaften in 14 Ländern zu den führenden IT-Unternehmen in Europa.

Bechtle verfügt zudem über ein weltweites Netzwerk an Partnern, das die Anforderungen global agierender Kunden erfüllt. Gegründet 1983, beschäftigt die Bechtle Gruppe mit Hauptsitz in Neckarsulm derzeit über 15.000 Mitarbeitende. Die mehr als 70.000 Kunden aus Industrie und Handel, dem Public Sector sowie dem Finanzmarkt begleiten wir bei ihrer digitalen Transformation und bieten herstellerübergreifend ein lückenloses Angebot rund um IT-Infrastruktur und IT-Betrieb. Bechtle ist im MDAX und im TecDAX notiert. 2023 lag der Umsatz bei 6,42 Mrd. €. Mehr unter: bechtle.com

Behörden Spiegel-Gruppe F34

Der Behörden Spiegel begleitet die öffentliche Verwaltung sowie den Modernisierungsprozess bei Bund, Ländern und Kommunen. Er zeigt Monat für Monat in journalistisch kritischer und unabhängiger Berichterstattung Wege zu mehr Effizienz in der staatlichen Verwaltung auf. Der Behörden Spiegel führt zudem zahlreiche Veranstaltungen und Kongresse durch, wie z. B. den Europäischen Polizeikongress (EPK) und die Berliner Sicherheitskonferenz (BSC). Wöchentlich erscheinen mehrere Newsletter.

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 200 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.

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 14.000 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.

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.

Bittium F14

Bittium ist auf die Entwicklung zuverlässiger, sicherer Kommunikations- und Konnektivitätslösungen spezialisiert. Für den militärischen Bereich sind das softwarebasierte IP Backbone Struktur, SDR Funkgeräte und VoIP Lösungen. Ergänzend dazu bietet Bittium bewährte Informationssicherheitslösungen an mit eigenem Smartphone und möglicher Integration mobile Geräte und tragbare Computer, alles innerhalb eines sicheren Systems mit MDM, VPN sowie Applikationen. Alle Produkte werden in Finnland produziert.

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 und ruggedized 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.

Black Box Deutschland GmbH S05

Black Box ist seit 1976 ein vertrauenswürdiger Anbieter von IT-Lösungen. Wir unterstützen Sie bei der Erstellung effizienter, hochleistungsfähiger KVM-Lösungen, die Anwendern sicheren Fernzugriff auf ihre Netzwerkdomänen, klassifizierten und unklassifizierten Systemen geben. Nahtloses Umschalten, einfache Bedienung und pixelgenaue Visualisierung ermöglichen ein hohes Situationsbewusstsein und schnellere Reaktionen bei sinkenden Gesamtkosten.

Erleben Sie unsere Lösungen live am Stand #S 05. Sehen Sie sich das flexible Emerald® KVM-über-IP System mit sicherem Zugriff auf physikalische und virtuelle Maschinen an. Black Box Kontrollraum Lösungen sind entscheidend für die Überwachung, Verwaltung und Steuerung kritischer Systeme in Leitstellen und Kommandozentralen.

Bundeswehr, Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAAINBw) N05

Der Organisationsbereich Ausrüstung, Informationstechnik und Nutzung (Org-Ber 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.

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.

BWI GmbH F07

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 7.000 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

Bren-Tronics International Solutions S83

Bren-Tronics (ein Unternehmen der Enersys-Gruppe) ist ein weltweit tätiger Entwickler und Hersteller von für die US-Armee und die NATO qualifizierten NiMh- und Li-Ionen-Akkus (z. B. BB-390B/U, BB-2590/U etc.) und Ladegeräten. Bren-Tronics entwickelt und produziert fortschrittliche tragbare Stromversorgungssysteme für militärische Anwendungen, die von US, NATO und Streitkräften auf der ganzen Welt eingesetzt werden.

Wir stellen Lösungen für:

- Militärische und industrielle Primär- und wiederaufladbare Akkupacks
- Militärische Universal-Ladegeräte
- Energieversorgungssysteme für Soldatensysteme
- Eigenständige erneuerbare Energieversorgungssysteme
- Wiederaufladbare Lithium-Ionen-Großbatterien für Anwendungen in Fahrzeugen und Unterkünften zur Verfügung.

CAE GmbH W05

Der Geschäftsbereich „Defense & Security“ der CAE ist führend in der digitalen Innovation und bietet Schulungs- und Einsatzunterstützungslösungen für diverse, militärische Einsatzbereiche - 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 ist ein globaler Partner für Business- und Technologie-Transformationen, der Organisationen auf dem Weg zu einer digitaleren und nachhaltigeren Welt unterstützt. Mit Expertise in Strategie, Design und Ingenieurwesen bietet Capgemini umfassende Ende-zu-Ende-Lösungen und -Services und nutzt seine Kompetenz in KI, Cloud und Daten sowie seine Branchenexpertise. Als engagierter Partner für die souveräne Digitalisierung der Sicherheitsarchitektur in Deutschland und Europa entwickelt Capgemini innovative Lösungen für die Verteidigung. Auf der AFCEA 2025 präsentieren wir Software Defined & Connected Defense für vernetzte Plattformen, KI-gestützte Lagebildanalyse für präzisere Entscheidungen und smarte Prozessautomatisierung für eine effizientere Verwaltung.

Carl-Cranz-Gesellschaft e.V. R24

Carl-Cranz-Gesellschaft e.V. - Gesellschaft für technisch-wissenschaftliche Weiterbildung

Technisch-wissenschaftliche Weiterbildung für Ingenieure und Naturwissenschaftler auf höchstem Niveau seit 63 Jahren. Jährlich über 120 Seminare (1-5 Tage Dauer) in den Fachgebieten Informations- und Kommunikationstechnologie, Führungs- und Aufklärungssystemsysteme, Sensorik, Transport- und Verkehrssysteme, Verteidigungs- und Sicherheitstechnik, Werkstoffkunde und Werkstofftechnologie sowie fachgebietsübergreifende Querschnittsthemen (Seminarkreise der CCG: Wissen im Fokus). Details siehe www,ccg-ev.de.

Zertifikatslehrgang „Rüstung und Nutzung“, Details siehe https://www.ccg-ev.de/aktuelles/detailansicht/zertifikatslehrgang-ruestung-und-nutzung

Carmenta Germany GmbH W11

Unser Kernprodukt, Carmenta Engine, bietet als rein softwaredefinierte Lösung erheblichen Mehrwert für zahlreiche militärische Use Cases. Neben dem Einsatz als Grundlage klassischer Battle-Management- und Missionssysteme ermöglicht sie den autonomen Betrieb unbemannter Systeme in allen Dimensionen. Carmenta Geospatial Technologies liefert Software zur Visualisierung, Analyse und Verwaltung georeferenzierter Daten für missionskritische Anwendungen. Die Technologie lässt sich nahtlos integrieren oder als Kernstück für Geospatial Webservices nutzen. Seit fast 40 Jahren entwickelt Carmenta marktführende Software für militärische und zivile Sicherheit – in enger Zusammenarbeit mit führenden Systemhäusern der Sicherheits- und Verteidigungsindustrie.

Cellebrite GmbH B01a

Cellebrite hat es sich zur Aufgabe gemacht, seinen Kunden zu ermöglichen, Leben zu schützen und zu retten, Justizverfahren zu beschleunigen und den Datenschutz in Gemeinwesen rund um die Welt zu wahren. Wir sind ein weltweit führendes Unternehmen im Bereich von digitalen Ermittlungslösungen für den staatlichen und privaten Sektor und ermöglichen es Organisationen, die Komplexität rechtlich zulässiger digitaler Ermittlungen durch die Optimierung der dazu erforderlichen Prozesse zu bewältigen. Die digitale Ermittlungsplattform und die digitalen Ermittlungslösungen von Cellebrite, denen Tausende von führenden Behörden und Unternehmen in aller Welt vertrauen, verändern die Art und Weise, wie Kunden Daten bei rechtlichen Ermittlungen erfassen, prüfen, analysieren und verwalten.

CENIT R63

CENIT empowers sustainable digitalization. Our solutions are based on innovative technologies in product lifecycle management such as the digital twin for simulation and engineering, production planning and manufacturing, predictive maintenance and enterprise information management. CENIT consultants support their customers holistically. They ensure that the 3DEXPERIENCE solutions are integrated along the entire value chain, considering the specialist areas involved.

Based on a strategic approach and trusting partnerships, CENIT offers solutions that give its customers a competitive edge through technological consistency.

CENIT works with customers from the automotive, aerospace, architecture, industrial equipment, tool and mould making and consumer goods industries.

CEOTRONICS AG F26

Für Menschen, auf die es ankommt.

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 Verteidigungskräften sind solche komplexen Situationen Alltag. Eine störungsfreie Kommunikation sichert hier nicht nur reibungslose Abläufe, sondern rettet im Ernstfall Leben. Im Wissen darum wurde CEOTRONICS vor 40 Jahren gegründet.

Unsere Mission: Für diejenigen Menschen Kommunikationslösungen zu entwickeln, auf die es ankommt. Und für die Situationen, wenn es darauf ankommt. When it counts.

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 5.000 Mitarbeitenden in Deutschland – davon etwa 800 in Defence, Intelligence und Space – ergebnisorientierte Strategien für ihre digitale Transformation und unterstützen sie mit End-to-End-Services.

Mit Bundeswehr und NATO arbeiten wir seit über 48 Jahren im Grundbetrieb wie in Übungen und Einsätzen zusammen. Wir stärken die Führungsfähigkeit in der Gesamtverteidigung Deutschlands: Mit erfolgreichen IP-Lösungen wie DokMBw und KI oder Managed Services wie SINA Managed Service und Betrieb HIL ermöglichen wir Streitkräften und anderen Organisationen die sichere Bearbeitung ihrer Verschlusssachen.

Chora GmbH S76

Chora liefert einzigartige EW- und SIGINT-Lösungen, die speziell für Streitkräfte, Geheimdienste und Sicherheitsbehörden entwickelt wurden. Als anerkannte Experten auf dem Gebiet der Satellitenkommunikation und PNT konzentrieren wir uns auf Innovation, Performance 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 gefertigt und weltweit über unsere Tochtergesellschaft in Deutschland, ein Netz lokaler Vertriebshändler und eine begrenzte Anzahl enger Partner vermarktet.

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 geschützt weiterentwickeln kann.

Die Digitalisierung von Behörden, Ministerien und Verwaltungen ist ein Großprojekt. Cisco ist ein seit Jahrzehnten verlässlicher Partner der Bundeswehr auf allen Ebenen. Dazu entwickelt Cisco Produkte und Lösungen rund um das Netzwerk, Netzwerkinfrastrukturen, Cybersicherheit, Rechenzentrumsausrüstung, Videokommunikations- und Kollaborationslösungen, Cloud/Software und Services.

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.

Comrod Communication AS F17

The Comrod group of companies design and manufacture antennas, antenna systems, RF amplifiers, telescopic masts, sectional masts, and power supplies for the defence industry. Comrod's aim is to maximize the performance of our customers' critical communication and sensor systems through cutting-edge technology, high-quality ruggedized products, and exceptional engineering solutions.

CONET S45

„Erfolg. Unsere Leidenschaft." CONET ist der Digitalisierungspartner mit Fokus auf Consulting, Digital Experience, AI & Data Intelligence, Cloud & Managed Services, Business Applications und Software Development. Seit mehr als 35 Jahren begleitet CONET die Bundeswehr zuverlässig auf dem Weg einer sicheren digitalen Transformation. Durch partnerschaftliche Zusammenarbeit, Innovationsstärke, Prozess-Know-how und hohe Dienstleistungsqualität entstehen erfolgreiche Lösungen in SAP & Non-SAP, Individualsoftware, Architektur- und Datenmanagement, IT-Infrastruktur und IT-Sicherheit. Auf der AFCEA präsentiert CONET Lösungsansätze für das Cyberlagebild mittels KI sowie Data Analytics, Informationsmanagement und die Entwicklung leistungsstarker KI-Applikationen. Kontakt: www.conet.de | info@conet.de

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 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. Hersteller und Distributoren erreichen als Seller auf dem Conrad Marketplace schnell und unkompliziert neue Zielgruppen und Märkte.

Constructor University Bremen gGmbH F09

Big Datacube Analytics in Earth and Space, mit standorttransparenter Föderation, ist die Schlüsselinnovation, die von der Constructor University und ihrem Spin-off, der rasdaman GmbH, hervorgebracht wurde. Unsere rasdaman-Engine bietet erstklassige Leistung, nahtlose Skalierbarkeit von Nanosatelliten über die Cloud bis zu superskaligen Rechenzentren, Flexibilität und KI-Integration auf raum-zeitlichen Sensoren, Bildern, Bildzeitreihen, Wetter-/Klima-Zeitreihen usw.

Die rasdaman AI-Cube™-Technologie hat Pionierarbeit für Big Datacube Analytics für raum-zeitliche Erddaten und darüber hinaus geleistet. Die KI-fähige Engine ist für ihre Leistung und die Zusammenführung mehrdimensionaler Datenwürfel bekannt. Unsere Innovationspreise: NATO Defence Innovation Challenge, Tech Connect Award, ...

Cordsen Engineering GmbH S75

Mittelständisches Unternehmen und Teil der Bechtle Group. Die Kernkompetenz liegt in der Entwicklung, Herstellung und Zertifizierung von IT-Geräten, nach NATO-Standard SDIP-27 Level A. Neben den NATO-SDIP-27 Level A/B/C Aktivitäten bieten wir die Zonierung und Zertifizierung von IT-Geräten nach dem deutschen Zonenmodell an. Wir liefern unsere Produkte zum größten Teil innerhalb der NATO an entsprechende Dienststellen, sowie an Regierungsbehörden in Europa

CPI Vertex Antennentechnik GmbH R27

CPI Vertex Antennentechnik GmbH ist führender Hersteller von Antennen- und Bodenstationssystemen für die Satellitenkommunikation. Das Unternehmen bietet weltweit schlüsselfertige Lösungen aus dem Ruhrgebiet und ergänzt das Angebot mit Produkten der Muttergesellschaft CPI. Zu den Kunden zählen Telekommunikationsunternehmen, Rundfunkanstalten, Regierungsbehörden und Militärorganisationen. Innovation, Zuverlässigkeit und Qualität sichern CPI Vertex eine Spitzenposition in der Branche.

CPM GmbH N06

DEFENCE. SECURITY. MILITARY-MEDICINE. CPM verstärkt und verbessert!

Durch die Fusion mit der beta Verlag & Marketinggesellschaft mbH ist zusammengewachsen, was zusammengehört – Innere und äußere Sicherheit! Verstärkt durch die Fachsparte Wehrmedizin kommunizieren wir ab sofort in den Ihnen bestens bekannten Formaten Publications, Events und Digital. Diversifiziert in drei verschiedenen Communities.

Größere Reichweite – der Multiplikator für Ihre Kommunikationsstrategie!

Dataminr Germany GmbH R52

Unsere KI-Plattform verarbeitet täglich Milliarden von Daten aus öffentlich zugänglichen Informationsquellen um Warnungen und Alarme in Echtzeit bereitzustellen.

dainox GmbH S33

Wir sind ein etabliertes und innovatives Hightech IT-Unternehmen. Unsere Schwerpunkte sind IT-ARCHITEKTUREN: IP-Netzwerke & IT-Sicherheit, Collaboration, Digitalisierung | SOFTWARE-ENTWICKLUNG: Automation & Orchestrierung |IT-SYSTEME: Entwicklung & Fertigung. Wir unterstützen unsere Kunden im gesamten Workflow: Von der Machbarkeitsbetrachtung bis hin zur Realisierung und dem Betrieb. Dabei setzen wir auf langlebige 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®.

info@dainox.net | +49 (0) 8247 33609 0 | www.dainox.net

Data-Warehouse GmbH F36

Unsere KI-Plattform verarbeitet täglich Milliarden von Daten aus öffentlich zugänglichen Informationsquellen um Warnungen und Alarme in Echtzeit bereitzustellen.

Dassault Systemes Deutschland GmbH R11

Dassault Systèmes ist ein Katalysator für den menschlichen Fortschritt. Durch virtuelle Umgebungen ermögli-chen 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.

DATAGROUP Defense IT Services S73 & A04

Dassault Systèmes ist ein Katalysator für den menschlichen Fortschritt. Durch virtuelle Umgebungen ermögli-chen 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.

deepset GmbH R48

deepset provides the AI platform and expertise for Defense to build safe, mission-critical AI agents and applications under the strictest accuracy, security, and compliance standards. As creators of the deepset AI platform and open-source Haystack framework, we take an outcome-first approach to AI, solving high-value challenges with rapid time-to-value. Designed for on-prem and cloud deployments, our platform ensures flexibility and security. Trusted by ministries and partners like Airbus in the aerospace and combat defense spaces, deepset delivers AI for high-stakes, high-accuracy, real-time environments. Our platform integrates with NVIDIA AI Enterprise for scalable, high-performance AI and has been recognized by Gartner as a Cool Vendor in AI Engineering. Learn more: deepset.ai

Dell GmbH S18 & R51

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.

DESAPRO AG R73

DESAPRO ist führend in der Entwicklung und Produktion von Spezial-Gehäusen für die Rüstungsindustrie. Das Sortiment umfasst Aluminium- und Composite 19 Zoll-Gehäuse sowie Aluminium-Transportbehälter.

Die Gehäuse und Behälter schützen deren Inhalt vor mechanischen, klimatischen oder elektrischen Einwirkungen wie Schock, Vibration, Wasser, Staub, Korrosion und EMI. Die Firma hat eine breite Palette von Produkten bestehend aus MILEX & COMEX 19 Zoll Gehäusen, STANEX Transportbehälter, PORTEX Behälter für sensitive Messinstrumente sowie KOOLEX Kühlungselementen. DESAPRO verfügt über einzigartige Erfahrungswerte in der Entwicklung von kundenspezifischen massgeschneiderten Lösungen zum Schutz von kostbaren Gütern.

DESAPRO ist eine weltweit tätige Firma und ist AS9100 zertifiziert.

Deutsche Gesellschaft für Wehrtechnik e.V 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/

DIAMOND GmbH R17

Die DIAMOND als inhabergeführtes Unternehmen mit Stammsitz in der Schweiz ist ein weltweit wegweisender Entwickler und Hersteller von hochpräzisen, leistungsstarken Glasfaserkomponenten, welche die sehr hohen spezifischen Anforderungen unserer Kunden erfüllen. Seit über 40 Jahren sind wir ein verlässlicher Partner und erarbeiten gemeinsam mit unseren Kunden Lösungen für vielfältigste Projekte.

In die Märkte Industrie, Militär und Luft- und Raumfahrt liefert DIAMOND seit vielen Jahren hoch zuverlässige Glasfaserlösungen. Unsere Stecker für Anwendungen in rauer Umgebung verbinden Kompaktheit, Robustheit (IP Schutz bis zur IP-Klassifizierung 68), Zuverlässigkeit, Modularität (2 bis 12 Kanäle) und hervorragende optische Eigenschaften. Kontakt: DIAMOND GmbH, www.diamond.de, info@diamond.de

DriveLock SE S61

HYPERSECURE IT aus Deutschland: DriveLock ist der führende Spezialist für präventive IT-Sicherheitslösungen Made in Germany. Die HYPERSECURE Platform vereint hochspezialisierte Abwehrkräfte, die in ihrer jeweiligen Disziplin zu den besten zählen, und erfüllt auf diese Weise selbst die anspruchsvollsten Sicherheitsanforderungen digitaler Arbeitsplätze.

dtec.bw - Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr (UniBw M) N03

Das dtec.bw ist ein von beiden Universitäten der Bundeswehr gemeinsam getragenes wissenschaftliches Zentrum und Bestandteil des Konjunkturprogramms der Bundesregierung zur Überwindung der COVID-19-Krise. dtec.bw wird von der Europäischen Union – NextGenerationEU finanziert. Diese Mittel werden an beiden UniBw zur Finanzierung von Forschungsprojekten und zum Wissens- und Technologietransfer eingesetzt. Mit 66 Forschungsprojekten und einem einzigartigen Themenspektrum, das u.a. Raumfahrttechnik, 5G-/6G-Technologie, Quantentechnologie, Mobilität der Zukunft, Cybersicherheit, Sensorik und Künstliche Intelligenz bis hin zu Kompetenzen für die digitale Arbeitswelt abdeckt, ermöglicht dtec.bw die Förderung digitaler Schlüsseltechnologien und nachhaltiger Innovationen.

D-Trust GmbH S25

Die D-Trust GmbH ist ein Unternehmen der Bundesdruckerei-Gruppe mit Sitz im Herzen Berlins. Technologisch ausgereifte Lösungen machen uns zu einem Vorreiter für sichere digitale Geschäftsprozesse und Identitäten. So stärken wir das Vertrauen in die Digitalisierung. Neben VS-NfD Zertfikaten, die aus einer BSI-Root erstellt werden, entwickeln wir im Moment auch eine Filesharing Lösung, namens Bdrive, die es ermöglicht VS-NfD Dateien sicher abzulegen sowie mit externen Dritten sicher zu teilen. Eine entsprechende BSI-Zulassung wird im Rahmen der Produktentwicklung mit vorangetrieben.

Dynamit Nobel Defence S31

Die Dynamit Nobel Defence GmbH ist ein mittelständisches Systemhaus der wehrtechnischen Industrie mit Sitz in Burbach, Berlin und Leipzig. Unser Portfolio umfasst schultergestützte Mehrzweckwaffen, Reaktivschutztechnologien für Landplattformen, Sperrsysteme, Lösungen zur Digitalisierung von Landstreitkräften, Brandschutz für zivile und militärische Anwendungen, Testladungen, Umwelt- und Qualifikationsdienstleistungen sowie Forschung und Entwicklung im Grundlagen- und anwendungsnahen Bereich.

Elbit Systems Deutschland F23

Elbit Systems Deutschland, weltweites Kompetenzcenter der Elbit Systems für HF- und VHF-Funktechnologie, ist bei der AFCEA Fachausstellung 2025 mit verschiedenen modernen, einsatzbewährten und marktverfügbaren Systemen, u.a. aus den Bereichen C4I&Cyber, vor Ort.

Darunter ist z.B. das innovative SmarTrack, das exaktes Blue-Force-Tracking abgesessener Kräfte in Einsatzräumen ermöglicht, in denen GNSS nicht verfügbar sind oder gestört werden. Außerdem zeigt Elbit Systems Deutschland in Bonn Systeme zur wirksamen stationären, mobilen und abgesessenen Drohnenabwehr. Darüber hinaus sind an Stand F23 bewährte Kommunikationslösungen zu sehen, die teilweise bereits in der Bundeswehr oder bei befreundeten Partnernationen eingeführt sind.

Mehr Informationen unter www.elbitsystems-de.com

ECOS Technology GmbH F27

ECOS ist ein deutscher Softwarehersteller für IT-Security-Produkte, spezialisiert auf:

Homeoffice, mobiles Arbeiten, ext. Dienstleister, BYOD: Der ECOS SecureBootStick ermöglicht hochsicheren Zugriff auf VS-NfD eingestufte Daten und Anwendungen, von einem ungemanagten Endgerät aus.

Videokonferenzen, Fernausbildung, Fortbildung: Das ECOS SecureConferenceCenter bietet alle Funktionen einer modernen Videokonferenzlösung. Für den Zugriff außerhalb eines gesicherten Netzes erlaubt die Kombination mit dem Secure Boot Stick VS-NfD-konforme Videokonferenzen.

Identitäten, Signaturen, Schlüssel, Zertifikate: Die ECOS TrustManagement-Appliance ist eine skalierbare & einfach integrierbare PKI- und Key-Management-Lösung zur Absicherung von mobilen Geräten, PCs, Servern oder Prozessen.

eleQtron GmbH R48

eleQtron entwickelt und betreibt Quantencomputer. Unsere Rechenmaschinen werden Probleme lösen können, an denen auch die besten konventionellen Supercomputer scheitern. Dafür nutzen wir die Quantenzustände von Ionen, die mit etablierter und miniaturisierter Hochfrequenztechnik gesteuert werden – ein einzigartiges Konzept, das wir MAGIC (Magnetic Gradient Induced Coupling) nennen.

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

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.

EIZO Europe GmbH S82

EIZO ist ein weltweit führender Anbieter von visuellen Lösungen mit einer Reihe von exklusiven COTS- und MCOTS-Produkten für extreme Anwendungen. Wir beliefern die Bereiche Verteidigung, Avionik, Luft- und Raumfahrt, ISR, Marine, EW und SIGINT mit MIL STD-konformen Lösungen. Hierzu gehören rugged LCD-Monitore, Hochleistungsgrafikkarten, GPGPU-Verarbeitung und Videoerfassung, rugged Video-Encoder-Lösungen sowie Bildoptimierungstechnologien. EIZO, mit Hauptsitz in Japan und Niederlassungen u.a. in den USA und Europa, entwickelt Produkte im eigenen Haus und ist in der Lage selbst nach MIL-Standards zu testen. Spezifische Kundenanforderungen, erweiterter Lebenszyklus-Support und ein hohes Maß an Performance sowie Zuverlässigkeit durch strenge Kontrollprozesse können gewährleistet werden.

ELP GmbH European Logistic Partners R72

Die ELP GmbH European Logistic Partners befasst sich mit der technischen Ausstattung für den polizeilichen und militärischen Entschärfungsdienst. Das Produktsortiment besteht aus portabler Röntgentechnik, ballistischer Schutzvorrichtungen, Spreng- und Disruptortechnik, Drogen- und Sprengstoffdetektoren, Unbemannter Boden- und Luftfahrzeuge sowie einer leistungsstarken, sicheren Mobile-ad-hoc-Networking Funk-/Datenlösung für die intelligente taktische Vernetzung in extremen Umgebungen.

Enercon Technologies Europe AG S15

Enercon Technologies designs non-ITAR power conversion and networking solutions exclusively for military and aerospace applications. With over 40 years of experience, we design COTS, factory configurable, and tailor-made solutions to overcome the demanding requirements of today's MIL-Standards, austere environments and rugged military and defense applications.

Eviden GmbH F31

Wir sind ein weltweit führendes Unternehmen im Bereich der digitalen Transformation und Europas erste Wahl für Cybersicherheit und Cloud. Mit 95.000 talentierten Mitarbeiter:innen stellen wir weltweit maßgeschneiderte, sichere und nachhaltige digitale End-to-End-Lösungen bereit, die den Erfolg und die Wertschöpfung globaler Unternehmen für ihre Kunden und die Gesellschaft als Ganzes fördern. Wir sind in 70 Ländern mit zwei Geschäftsbereichen tätig: Tech Foundations und Eviden.

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.

Extron S66

Extron Electronics ist einer der führenden Hersteller professioneller AV-Systemprodukte, einschließlich AV-Mediensteuerungen, Computervideo-Interfaces, Umschalter, Kreuzschienen, Verteilverstärker, Audioverstärker und -signalprozessoren, Lautsprecher, Twisted Pair- und Glasfaser-Lösungen, Videowandprozessoren, Videosignalprozessoren, AV-Streaming- und Aufnahme-Produkte, Beschallungssysteme für Klassenräume und hochauflösende Kabel.

Epson Deutschland GmbH R18

Die Epson Deutschland GmbH ist ein führender Anbieter von Projektoren, Druckern und Scannern für Unternehmen, öffentliche Auftraggeber und Privatkunden. In eigenen Fabriken produziert EPSON nach höchsten Umweltstandards und verfügt u.a. über den RBA (Responsible Business Alliance) Platin Status. Die Epson Deutschland GmbH wurde 1979 als Tochter der japanischen SEIKO EPSON CORPORATION gegründet. Das in Düsseldorf (Nordrhein-Westfalen) ansässige Unternehmen beschäftigt rund 300 Mitarbeiter und verantwortet die Vertriebsgebiete Deutschland, Österreich und die Schweiz. Am Standort Meerbusch betreibt Epson zudem ein Industrial Solutions Center, in dem energieeffiziente Büro- und spezialisierte Industrieanwendungen im Einsatz präsentiert werden.

www.epson.de

FERCHAU GmbH R56

In der FERCHAU Aviation Group bündeln wir unsere Engineering- und Produktionskompetenzen für die Luft- und Raumfahrt sowie Verteidigungsindustrie. Das Ergebnis: ein leistungsstarkes End-to-End-Portfolio - mit zunehmender Beliebtheit auch in anderen Industriezweigen.

Der Geschäftsbereich Aviation der FERCHAU GmbH und die RST Rostock System-Technik GmbH bilden gemeinsam die FERCHAU Aviation Group. Als „Preferred Supplier for Engineering & Customer Services" der Airbus Group und als zuverlässiger Entwicklungspartner für die europäische Luft- und Raumfahrt sowie Verteidigungsindustrie bieten wir ganzheitliche Engineering-Dienstleistungen für komplexe Luft-, Raumfahrt- und Verteidigungssysteme.

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.

FFG Flensburger Fahrzeugbau Gesellschaft mbH F14

Die FFG Flensburger Fahrzeugbau Gesellschaft mbH (FFG) ist ein Unternehmen mit rund 900 Mitarbeitenden und einer über 150-jährigen Tradition.

Heute ist die FFG ein internationales Hightechunternehmen, welches mit Innovationen im wehrtechnischen Bereich neue Maßstäbe setzt und sich als Systemhaus etablieren konnte. Nicht umsonst vertrauen Auftraggeber aus über 40 Ländern seit vielen Jahren auf Fahrzeugtechnologie „Made in Flensburg".

Komplettlösungen von A bis Z – von Entwicklung und Konstruktion über Fertigung, Modernisierung und Instandhaltung vor Ort bis zur termingerechten, weltweiten Auslieferung und After-Sales-Service rund um die Uhr.

Die FFG stellt sich jeder Herausforderung!

Forschungszentrum Space - UniBw München S74

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.

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.

Fraunhofer FKIE F15

Das Fraunhofer FKIE entwickelt Technologien und Prozesse mit dem Ziel, existenzbedrohende Risiken frühzeitig zu erkennen, zu minimieren und beherrschbar zu machen. 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.

Zentrale Bedeutung hat der »Faktor Mensch«: Im Fokus der Forschung steht die Entwicklung effektiver und effizienter Mensch-Maschine-Systeme, bei denen der Mensch als Entscheider und verantwortlicher Akteur im Mittelpunkt steht.

Fraunhofer IOSB W01

Beratung und Technologie für die Verteidigung: In seinem Geschäftsfeld Verteidigung 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. Ein wichtiges Thema ist dabei auch der Einsatz unbemannter 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.

Frequentis Deutschland GmbH S28

Frequentis ist ein weltweit führender Anbieter für sichere Kommunikationssysteme mit über 75 Jahren Erfahrung. Das Unternehmen arbeitet mit großen Verteidigungsorganisationen wie der U.S. Air Force, der Bundeswehr und dem britischen Verteidigungsministerium zusammen.

Unsere Lösungen ermöglichen schnelle, sichere Kommunikation in kritischen Einsätzen – von militärischer Flugsicherung über Luftverteidigung bis hin zur Missionskontrolle. So können Streitkräfte sich auf ihre Hauptaufgabe konzentrieren: den Schutz von Menschen zu Land, in der Luft und auf See.

Frequentis unterstützt Verteidigungszentren in den USA, Österreich und Australien, mit Sicherheitsfreigaben für US-Verteidigungsprogramme.

Kontakt: Florian Kölders, florian.koelders@frequentis.com

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. Fujitsu unterstützt die Verteidigungsindustrie mit innovativen, maßgeschneiderten Lösungen für die digitale Transformation – stets unter Einhaltung höchster Sicherheitsstandards. Dabei erstreckt sich die Expertise auf die gesamte Wertschöpfungskette, von Beratung und Planung bis hin zu Implementierung und Support. Als global agierendes Unternehmen mit rund 126.000 Mitarbeitern in über 100 Ländern verfügt Fujitsu über die Ressourcen und das Know-how, um auch die komplexesten Herausforderungen der Verteidigung zu meistern.

https://global.fujitsu/de-de/industries/defence

GAF AG S22 & A08

Die GAF AG, ein e-GEOS (Telespazio/ASI) Unternehmen, ist seit 40 Jahren einer der führenden europäischen Anbieter von Geodaten und Informationsdiensten für Kunden aus Verteidigung, Nachrichtendienst und Sicherheit und bietet ein umfassendes Know-how in der angewandten Fernerkundung und im Vertrieb von Multi-Source-Satellitendaten. Das GAFportal bietet einen standardisierten und automatisierten Zugang zu Satellitendaten aller wichtigen Datenanbieter, auch 24/7/365. Softwarelösungen zur Archivierung, Produktion, Verteilung und Visualisierung von Geodaten sowie thematische Kartenprodukte erfüllen stets die entsprechenden Qualitätsanforderungen. Hochwertige 2D- und 3D-Produkte (z.B. GAF Elevation Suite, Bodenbewegungsdienste) ergänzen das auf jeden Kundenbedarf anpassbare Portfolio.

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).

Getac Technology GmbH W02

Die Getac Technology Corporation 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. Kürzlich wurde Getac von Newsweek als eines der „Verlässlichsten Unternehmen der Welt“ für 2024 ausgezeichnet.

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.

Global RadioData 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.

Google Germany GmbH G01

Google Cloud ist der neue Weg in die Cloud und bietet KI-, Infrastruktur-, Entwickler-, Daten-, Sicherheits- und Kollaborationstools, die für heute und die Zukunft entwickelt wurden. Google Cloud liefert einen leistungsstarken, vollständig integrierten und optimierten KI-Stack mit einer eigenen weltweiten Infrastruktur, maßgeschneiderten Chips, generativen KI-Modellen und einer Entwicklungsplattform sowie KI-gestützten Anwendungen, die Organisationen bei der Transformation unterstützen. Kunden in mehr als 200 Ländern und Regionen setzen auf Google Cloud als ihren Technologiepartner des Vertrauens

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 „Beiträge zur Führungsunterstützung für hochmobile, interoperable, resiliente Kommando- und Befehlsstellen““ zeigen wir mit unseren Partnern anhand von fiktiven Szenaren modulare Lösungen, die einen wesentlichen Beitrag zur Ausgestaltung von mobilen Führungs- und Gefechtsständen für die Digitalisierung der Landstreitkräfte in der taktischen Ebene leisten können.

Hagenuk Marinekommunkation GmbH B07

Die Hagenuk Marinekommunikation GmbH (HMK) ist eine Tochterge-sellschaft der ATLAS ELEKTRONIK und gehört zum thyssenkrupp-Konzern. Integrierte Fernmeldeanlagen kommen zum Einsatz auf U 212 A, den Korvetten K130, sowie den Einsatzgruppenversorgern (je-weils 1. + 2. Los). Weltweit nutzen 29 Nationen 590 Systeme. HMK’s bewährte HF Sender und Empfänger sind auf allen Schiffen/Booten der Deutschen Marine eingebaut:

- HF-Sender/Transceiver (3003er Serie bis 10 kW, 1,5 – 30 MHz)
- VLF/HF-Empfänger (10 kHz – 30 MHz)
- HF-Breitbandsysteme
- Antennensysteme
- IP Backbone für Kommunikationssysteme/Subsysteme der in-ternen/externen Kommunikation
- Message Handling und Steuerungssysteme

Hagenuk Marinekommunikation GmbH, 24220 Flintbek, www.hmk.atlas-elektronik.com, info@hmk.atlas-elektronik.com

Helsing GmbH S71

Helsing ist eine neue Art von Verteidigungsunternehmen. Wir verfolgen einen Software-First Ansatz und entwickeln KI-basierte Softwarelösungen für alle Teilstreitkräfte. Gemeinsam mit unseren Industriepartnern bringen wir neue Fähigkeiten auf bestehende und neue Hardware-Plattformen und liefern hochpräzise Wirkmittel an unsere militärischen Kunden. Verantwortungsvolles, auf ethischen Standards basierendes Handeln steht dabei im Mittelpunkt unseres unternehmerischen Engagements.

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.

HENSOLDT F01 & A05

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.

Hexagon - HxGN Safety & Infrastructure GmbH S14

Hexagon ist ein global führendes Unternehmen im Bereich der digitalen Realität und bietet Lösungen für die Erfassung, Verarbeitung und Analyse von Daten. Auf der AFCEA Fachausstellung in Bonn präsentiert Hexagon innovative Produkte und Technologien, die vor allem auf den Verteidigungs- und Sicherheitssektor abzielen. Zu den Highlights gehören hochpräzise Geoinformationssysteme, fortschrittliche Sensorlösungen und Software für die Echtzeit-Datenanalyse. Diese Technologien unterstützen die Entscheidungsfindung, verbessern die situative Wahrnehmung und optimieren die Planung und Durchführung von Einsätzen. Hexagon zeigt damit sein Engagement für die Bereitstellung modernster Lösungen zur Steigerung von Effizienz und Sicherheit.

Hirt Zerspanungstechnik GmbH F24

Die Firma Hirt Zerspanungstechnik 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.

Hitachi Vantara GmbH F25

Hitachi Vantara verändert die Art und Weise, wie Daten Innovationen vorantreiben. Als hundertprozentige Tochtergesellschaft der Hitachi Ltd. bietet Hitachi Vantara die Datengrundlage, auf die sich Innovationsführer weltweit verlassen. Mit Datenspeicher, Infrastruktursystemen, Cloud-Management und digitaler Expertise hilft das Unternehmen seinen Kunden, die Grundlage für nachhaltiges Unternehmenswachstum zu schaffen. Um mehr zu erfahren, besuchen Sie www.hitachivantara.com.

HPE Aruba Networking S18

HPE Aruba Networking, Teil der Hewlett Packard Enterprise, ist ein führender Anbieter von Next-Generation-Netzwerklösungen für Unternehmen jeder Größe weltweit. Das Unternehmen liefert sichere und intelligente Edge-to-Cloud-Netzwerklösungen, die mithilfe von KI das Netzwerk automatisieren und Daten nutzen, um bessere Geschäftsergebnisse zu erzielen. Mit Aruba ESP (Edge Services Platform) und As-a-Service-Optionen verfolgt Aruba cloud- sowie onPremise-basierte Ansätze, um Konnektivitäts-, Sicherheits- und Budgetanforderungen an Standorten, Zweigstellen, Rechenzentren und Remote-Arbeitsumgebungen zu erfüllen. Dabei deckt HPE Aruba Networking alle Bereiche von Funk-Netzen, wie WLAN und private 5G sowie kabelgebundenen Netzwerke bis hin zu softwaredefinierten Wide Area Networks (WAN) ab.

IABG mbH W06

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 weltweit führender Anbieter von IT-Lösungen. Das Portfolio reicht vom Quantencomputer und Software über Beratung und Diestleistungen bis hin zur Finanzierung. Kernziel von IBM ist, Unternehmen aller Größen bei der digitalen Transformation zu unterstützen. Als langjähriger Partner sind wir mit den Aufgaben der Bundeswehr vertraut und davon überzeugt, dass softwarebasierte Digitalisierung die Grundlage für eine effektive Verteidigung ist.

Mehr Information: www.software-defined-defense.de

iesy GmbH S63

Wir sichern und stärken digitale Souveränität

Die iesy GmbH aus Meinerzhagen (Deutschland) entwickelt und fertigt seit über 55 Jahren hochsichere Embedded Computer für unterschiedliche Defence-Anwendungen. Unsere maßgeschneiderten Lösungen erfüllen höchste Anforderungen an Robustheit, Cybersicherheit und Langzeitverfügbarkeit – für eine zukunftsfähige und verlässliche Sicherheit.

We secure and strengthen digital sovereignty

iesy GmbH from Meinerzhagen (Germany) has been developing and manufacturing highly secure embedded computers for various defense applications for over 55 years. Our customized solutions meet the highest requirements for robustness, cyber security and long-term availability - for future-proof and reliable defence.

IGEL Technology GmbH A01

IGEL, ein weltweit führender Anbieter im Bereich End-User-Computing, bietet mit IGEL OS ein sicheres Endpoint-Betriebssystem – ein schlankes, effizientes und zentral verwaltetes OS, das Endpoints vor Ransomware und anderen Cyberbedrohungen schützt, das Management und die Kontrolle von Endpoints erheblich vereinfacht und die Lebensdauer bestehender Hardware verlängert. So werden die Gesamtbetriebskosten gesenkt und die Nachhaltigkeit verbessert.

Das IGEL Preventative Security Model (PSM) bildet die vielschichtige Sicherheitsgrundlage von IGEL OS für einen sicheren und produktiven Endpoint-Betrieb.

Erfahren Sie, wie IGEL Unternehmen dabei unterstützt, ihre Mitarbeitenden und Endpoints vor Malware zu schützen, IT-Teams und Endanwender produktiver zu machen und Kosten zu sparen.

www.igel.de

Ihse GmbH S81

Die IHSE GmbH ist ein weltweit führender Entwickler und Hersteller hochsicherer, zertifizierter IT-Infrastrukturlösungen zum Verlängern und Schalten von Computersignalen.

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.

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.

Indra (Indra Avitech & Indra Sistemas) S11

Indra ist eine globale Technologiegruppe und ein führendes Unternehmen in den Bereichen Verteidigung, Luftverkehrsmanagement und Raumfahrt. Mit über 11.000 implementierten Luftverkehrslösungen unterstützt seine Technologie mehr als 85 % der Passagierflüge weltweit.

Indra Avitech, eine Tochtergesellschaft von Indra, ist auf luftfahrt- und verteidigungsbezogene Lösungen spezialisiert. Seit über 25 Jahren ist sie ein wichtiger Partner der Bundeswehr und bietet Lösungen für aeronautische Plattformen & Publikationen, Flugplanung und SWIM an. Ihre Produkte werden in der gesamten Bundeswehr sowie an Standorten alliierter Streitkräfte eingesetzt.

AFCEA 2025: wir präsentieren die Integration aeronautischer Daten auf EKBs. Indra Avitech GmbH Bahnhofpl.3, FDH. indra-avitech.aero , indra-company.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 20 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

Intracom Defense S.A. F14

INTRACOM DEFENSE (IDE) ist ein anerkanntes Unternehmen der Verteidigungsindustrie mit einer hohen Reputation in Griechenland und mit einer hohen Exportrate an internationale Kunden in Europa und den USA.

IDE nutzt High-End-Technologien für Design und Entwicklung moderner Systeme in den Bereichen taktische IP-Kommunikation, integrierte C4I-Systeme, Raketenelektronik, Überwachung, hybride elektrische Energiesysteme und unbemannte Systeme. Das Unternehmen ist international anerkannt durch die langjährige Teilnahme an europäischen und NATO-Programmen zur Entwicklung neuer Technologien. IDE nutzt fortschrittliche Produktionskapazitäten und umfangreiches Projektmanagement-Know-how und ist ein wichtiger Akteur im Hochtechnologiesektor der griechischen Verteidigungsindustrie.

IntraFind Software AG R41

Die IntraFind Software AG mit Hauptsitz in München ist ein etablierter deutscher Hersteller von KI-basierter Such- & Analyse-Software und intelligenten Chatbots mit langjähriger Projekterfahrung bei der Bundeswehr und weiteren Sicherheitsbehörden.

Als zuverlässiger Partner für Digitalisierung machen wir Informationen in großen Datenbeständen aller relevanten Datenquellen schnell, sicher und benutzerfreundlich auffindbar - für fundierte Entscheidungen.

Unsere Lösung steigert die Effizienz bei der Informationssuche, verbessert das Wissensmanagement und bietet höchste Sicherheit durch die Berücksichtigung von Zugriffsberechtigungen und Geheimhaltungsgraden sowie sicherheitsüberprüftes Personal.

Besuchen Sie uns für Software Live Demos an Stand R41: täglich um 11 Uhr, 14 Uhr und 15 Uhr.

inxire GmbH F37

inxire ist ein Produkt- und Serviceanbieter für Enterprise Digitalization. Mit unseren innovativen Produkten schaffen wir die Grundlage für neue digitale Lösungen und ermöglichen, dass Unternehmen und Organisationen ihr volles Digitalisierungspotenzial ausschöpfen.

Die Bundeswehr setzt mehrere inxire-Produktkomponenten u.a. als VS-Registratur in Führungsinformationssystemen sowie für die KI-basierte Datenanalyse im Kommando Cyber- und Informationsraum ein.

inxire entwickelt maßgeschneiderte Software zu Themen wie Intelligent Decision Support, Enterprise-Content-Management, Compliance, Instandhaltung und Analytics. Zahlreiche internationale Kunden beschleunigen mit inxire schon heute ihre digitale Transformation. Weitere Informationen finden Sie unter www.inxire.com.

ISEC7 GmbH S51

Sicherheitsbehörden, Streitkräfte und Betreiber kritischer Infrastrukturen brauchen sichere Kommunikation, zuverlässiges Krisenmanagement und resiliente IT. Die ISEC7 Group bietet speziell entwickelte Services und Softwarelösungen – von sicherer Telefonie und Messenger-Diensten bis zu Managed Mobility und Post-Quantum-Sicherheit. Jeder zweite Polizeibeamte in Deutschland nutzt ISEC7-Technologie, über 700 Organisationen weltweit vertrauen auf unsere Lösungen. Wir ermöglichen Behörden und Organisationen, flexibel und sicher zu agieren – unter Einhaltung strengster Vorgaben. Gegründet 2003 in Deutschland, sind wir heute global tätig.

itWatch GmbH S10

itWatch stellt patentierte IT-Sicherheit her. Der Fokus liegt auf Schutz gegen Datendiebstahl (Data Loss Prevention – DLP), technische Vertrauensketten von der Tatstatur bis zu Daten und deren organisatorischer Einbettung durch rechtsverbindliche Dialoge, Endgeräte-Sicherheit (Endpoint Detection & Response – EDR), der Lösung itWash, einer Datenschleuse mit Datenwäsche (Data Sanitizing) und Workfl ow, sowie Mobile Security und Verschlüsselung.

Erste Produkte wurden bereits 1997 entwickelt. Die Lösungen der itWatch zeichnen sich durch weltweite Alleinstellungsmerkmale aus. Hierbei stehen kosteneffiziente, sichere Lösungen mit hervorragendem ROI im Fokus.

Janes R47

Janes trusted defence, security, and geopolitical information delivered through seamless digital platforms and system integrations—turns overwhelming data into clear, actionable intelligence and insight. Enhance your own analysis of the strengths, dispositions, and capabilities of actual and potential adversaries and allies by adding essential context to your briefings with:

- Orders of battle for all the world's military forces
- Data on over 89,000 pieces of military equipment, associated platforms, weapons, and subsystems
- Details of over 29,000 geolocated military installations, including early warning, SAM, and ballistic missile sites, and nuclear facilities
- Over 900,000 events linked to key datasets support indicators and warnings and pattern of life analysis

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, 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

Kappa optronics GmbH R19

Advanced Cameras and Vision Systems | Kappa optronics

Auf der AFCEA zeigen wir skalierbare, hochperformante Driver Vision Enhancer (DVE) und Situational Awareness Systeme (SAS) für gepanzerte Fahrzeuge. Basierend auf verschiedenen Kamerakonfigurationen mit hochwertigen Sensoren für Tag- und Nachtsicht, einem leistungsstarken digitalen Videomanagementsystem und robusten Displays bieten diese Systeme eine Rundumsicht von bis zu 360° mit extrem niedriger Latenz°. Durch die Fusion von LWIR- und VIS-Bildern wird die DRI verbessert, PiP-Stitching ermöglicht eine umfassende Sicht. Erfolgreich im Einsatz auf verschiedenen Plattformen. Mit über 40 Jahren Erfahrung steht Kappa für robuste Vision-Lösungen für Verteidigung und Luftfahrt.

Knapp Service Koblenz GmbH W09

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 ging aus dem Zusammenschluss von Krauss-Maffei Wegmann und Nexter hervor, zwei der führenden europäischen Hersteller militärischer Landsysteme mit Sitz in Deutschland und Frankreich.

Das Produktspektrum der Gruppe umfasst Kampfpanzer, gepanzerte Fahrzeuge, Artilleriesysteme, Waffensysteme, Munition, Militärbrücken, Kundenservice, Battle-Management-Systeme, Ausbildungslösungen, Lösungen für Schutzsysteme sowie ein breites Sortiment an Ausrüstung.

Die Bildung von KNDS stellt den Beginn der Konsolidierung der Industrie für militärische Landsysteme in Europa dar. Der Zusammenschluss von KMW und Nexter stärkt die Wettbewerbsfähigkeit und die internationale Position beider Unternehmen sowie deren Fähigkeit, den Anforderungen der Armeen ihrer jeweiligen Länder gerecht zu werden.

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.

Kommando Heer S65

Das Kommando Heer ist das Planungs-, Führungs-, Lenkungs- und Kontrollinstrument des Inspekteurs des Heeres. Das Kommando ist der zentrale Ansprechpartner für das Bundesministerium der Verteidigung und andere Organisationsbereiche der Bundeswehr in Angelegenheiten der Landstreitkräfte und der Dimension Land.

Damit die Landstreitkräfte auf dem Gefechtsfeld der Zukunft bereits „heute“ ihre Aufträge von „morgen“ im Schulterschluss mit den anderen Dimensionen und im Zusammenwirken mit internationalen Partnern erfüllen können, ist die Informationsverarbeitung und -übertragung der Schlüssel zum Erfolg.

Kommando Cyber- und Informationsraum B03 & A07b

Die digitale Kriegstüchtigkeit Deutschlands liegt in der Verantwortung der Teilstreitkraft Cyber- und Informationsraum (TSK CIR). Sie ist wie ein digitales Schutzschild und zugleich „High-Tech-Werkzeugkasten“ für Bedrohungen der hybriden Kriegsführung. Die IT-Netze der Bundeswehr zu betreiben und zu schützen, technologische Innovationen zu erschließen sowie in fremden Systemen aufzuklären und zu wirken, gehört zu ihren Kernaufgaben. Als „zentrales Nervensystem“ stellt sie die Vernetzung der Streitkräfte sicher und ermöglicht dadurch moderne Multi Domain Operations. Im Kommando CIR in Bonn befindet sich der Dienstsitz des Inspekteurs CIR und seines Vertreters, der als Chief Information Security Officer die Gesamtverantwortung für die Informationssicherheit in der Bundeswehr trägt.

Kommando Luftwaffe G03b

Die Luftwaffe spielt eine zentrale Rolle bei der Sicherung des Luft- und Weltraums Deutschlands. Ihr Auftrag umfasst lufthoheitliche Aufgaben sowie die Unterstützung gemeinsamer Operationen mit anderen Teilstreitkräften und Verbündeten. Die Luftwaffe gewährleistet die Einsatzbereitschaft und Leistungsfähigkeit ihres Personals und Materials. Durch umfassende Ausbildung und Einsatzvorbereitung wird sichergestellt, dass die Kräfte schnell und effektiv in einem breiten Spektrum von Szenarien weltweit eingesetzt werden können, wie in Hilfs-, Rettungs- und Evakuierungseinsätzen. Mit der Verantwortung für den Luft- und Weltraum ist die Luftwaffe an der Spitze moderner Verteidigung und trägt zur nationalen und globalen Stabilität und Sicherheit bei.

KPMG AG Wirtschaftsprüfungsgesellschaft S26

KPMG ist eine Organisation unabhängiger Mitgliedsfirmen mit mehr als 273.000 Mitarbeitenden in 143 Ländern. In Deutschland gehört KPMG zu den führenden Wirtschaftsprüfungs- und Beratungsunternehmen und ist mit über 14.000 Mitarbeitenden an 27 Standorten präsent.

Der Bereich Public Sector Consulting befasst sich seit über 25 Jahren mit der Unterstützung des öffentlichen Sektors und hat eine Vielzahl von Projekten im Bereich der Organisationsentwicklung und -beratung durchgeführt. Dabei verbinden wir unsere fachliche Spezialisierung in der Organisationsberatung mit der Branchenexpertise des öffentlichen Sektors in einem lösungsorientierten Dienstleistungsangebot. Unsere besondere Stärke liegt in der Verbindung von betriebswirtschaftlicher, rechtlicher und IT-technischer Expertise.

L3Harris Technologies S30

In einer schnelllebigen und immer komplexeren Welt antizipiert L3Harris Herausforderungen und reagiert mit agilen Technologien - für eine sicherere Welt und eine sicherere Zukunft.

L3Harris gehört zu den weltweit führenden Anbietern von militärischen Kommunikationslösungen. Mit den kampferprobten und innovativen Lösungen sind Sie auf taktischer und strategischer Ebene zukunftssicher aufgestellt. Die Sicherheit der eigenen Kräfte im elektromagnetischen Raum wird durch das Angebot von etablierten ECM (Electronic Counter Measure) und EA (Electronic Attack) Lösungen abgerundet.

Weitere Infos unter: https://www.harris.com/solutions, JK Defence & Security Products GmbH, Industriering Ost 74, 47906 Kempen, milcom@jkdefence.de, www.jkdefence.de, 02152/1445-207

LEONARDO Germany GmbH 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 2025 zeigen wir unsere maßgeschneiderten Containerlösungen für den IKT-Bedarf.

LS telcom B08

VERWALTEN, ÜBERWACHEN und VERTEIDIGEN Sie Ihr Spektrum | Das elektromagnetische Spektrum ist zu einem wesentlichen und grundlegenden Faktor geworden. Ein verfügbares und sicheres elektromagnetisches Spektrum (EMS) ist der Schlüssel zum Erfolg einer Mission. Elektronische Kampfführung (Eloka) unterstützt die Dominanz der Streitkräfte und die Nutzung des EMS innerhalb der elektromagnetischen Umgebung und erleichtert den Einsatz von Fähigkeiten und Sensoren durch die Streitkräfte.

LS telcom ist ein führender Lösungsanbieter für elektromagnetische Spektrums-Operationen (EMSO):

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

LWL-Sachsenkabel GmbH F30

Seit 1991 ist Sachsenkabel ist führender Anbieter von glasfaserbasierten Infrastrukturlösungen, Verkabelungssystemen und Dienstleistungen. Ihre kundenindividuellen faseroptischen Lösungen kommen in Bereichen wie Telekommunikation, Rechenzentren, Industrie, Veranstaltungstechnik und Security zum Einsatz. Sachsenkabel entwickelt maßgeschneiderte Lösungen für sicherheitskritische Anwendungen, die optimal vor Staub, Wasser und extremen Temperaturen geschützt sind. Mit

VG 96927-2-zugelassener Entwicklungs- und Produktionsstätte in Deutschland garantiert Sachsenkabel höchste Qualität und kurze Lieferzeiten. Als Teil der Amphenol Corporation bietet Sachsenkabel weltweit Verlässlichkeit, Skalierbarkeit und ein breites Produktportfolio.

M4Com System GmbH R43

M4Com ist ein Systemhaus mit über 20 Jahren Erfahrung in der Bereitstellung von Verteidigungs- und Sicherheitslösungen für schlüsselfertige ISR-Prozessketten und ISR-Informationsmanagement und ist mit seinen Produkten sowohl bei Systemintegratoren als auch beim öffentlichen Auftraggeber anerkannt. M4Com bietet etablierte softwarebasierte Produkte, die als Komponenten oder als Gesamtlösung eingesetzt werden können.

M4Com bietet offene, interoperable leistungsstarke Software und Hardware-Technologie für Echtzeit Informationsmanagement und Datenverarbeitung in den Bereichen IMINT und SIGINT aus luftgestützte Aufklärungsplattformen.

Wir liefern NATO STANAG-kompatiblen Lösungen mit jeweils offenem Standard, generischen Schnittstellen und funktionsübergreifender Verbindung in eine netzwerkzent

Materna Information & Communications SE S52

Materna ist eine familiengeführte, deutsche Unternehmensgruppe, mit Hauptsitz in Dortmund. Seit 1980 gewährleisten wir die digitale Souveränität unserer Kunden. Wir stehen für Verlässlichkeit, verbunden mit einem langfristigen und kundenzentrierten Ansatz, u.a. in Fragen der Verfügbarkeit von Services und einer berechenbaren Preispolitik. Materna verfügt weltweit über 4.500 Mitarbeitende, u.a. über 1.000 Developer und über 300 Cloud-Spezialisten und erwirtschaftete 2024 einem Gruppenumsatz von ca. 710 Mio. Euro. Wir sind einer der größten (KI) Integrationsdienstleister Europas. Unser Fokus liegt auf der Realisierung von IT- und Digitalisierungsprojekten im Bereich Wirtschaft, Verwaltung und Sicherheitsbehörden.

Materna Virtual Solution GmbH S56

Materna ist eine familiengeführte, deutsche Unternehmensgruppe, mit Hauptsitz in Dortmund. Seit 1980 gewährleisten wir die digitale Souveränität unserer Kunden. Wir stehen für Verlässlichkeit, verbunden mit einem langfristigen und kundenzentrierten Ansatz, u.a. in Fragen der Verfügbarkeit von Services und einer berechenbaren Preispolitik. Materna verfügt weltweit über 4.500 Mitarbeitende, u.a. über 1.000 Developer und über 300 Cloud-Spezialisten und erwirtschaftete 2024 einem Gruppenumsatz von ca. 710 Mio. Euro. Wir sind einer der größten (KI) Integrationsdienstleister Europas. Unser Fokus liegt auf der Realisierung von IT- und Digitalisierungsprojekten im Bereich Wirtschaft, Verwaltung und Sicherheitsbehörden.

Media Broadcast Satellite GmbH S29

MBS is a trusted service integrator and managed gateway operator. We operate data and voice communications via satellite and data networks - globally and in space. Our expertise ranges from legacy satellite services to tailored new space applications.

Governmental and business customers worldwide rely on the integrity and innovation of MBS, with its own fail-safe infrastructure in Germany and a team of more than 90 specialists.

From efficient standardised, to tailored high-end, fully managed solutions - scalable and vendor independent with high availability and field-proven under the toughest conditions.

Contact: info@mb-satellite.com, +49 6081 100 00

Micropol Fiberoptic GmbH F33

Bei Micropol kombinieren wir einzigartige Design- und Produktionstechnologien, um komplexe und kompakte Lösungen für passive Glasfaseroptik anzubieten und somit ein absolutes Alleinstellungsmerkmal zu schaffen. Wir arbeiten mit extrem hoher Präzision und bieten kurze Lieferzeiten, hohe Qualität und kundenspezifische Anwendungen.

Unabhängig von der Anwendung verfügen wir über das Wissen und die Kapazität, das benötigte Produkt herzustellen – entweder nach Kundenspezifikation oder als maßgeschneiderte Lösung. Alle unsere Produkte werden in unserem eigenen Werk in Schweden hergestellt. Unsere Kunden sind in einer Vielzahl von Märkten zu finden, in denen fortschrittliche Glasfaserlösungen entscheidend sind.

Microsoft Deutschland GmbH R57

„Empowering Defense & Intelligence: Resilience, Security, and Innovation by Microsoft.“

Microsoft deckt den vielfältigen Technologiebedarf für Einsatz und Grundbetrieb von heute und morgen. Mit unseren Lösungen gewährleisten wir zuverlässige und sichere digitale Infrastrukturen und Services für Streitkräfte, Sicherheitsbehörden und die Verteidigungsindustrie.

Zusammen mit unseren Partnern stellen wir marktführende Angebote bereit. Damit ertüchtigen wir z.B. die NATO, gewährleisten Interoperabilität in Bündnissen und machen schnelle Innovation unter härtesten Einsatzbedingungen wie in der Ukraine möglich. Dies beinhaltet unter anderem Lösungen für Kollaboration, Künstliche Intelligenz, Cloud Computing, Cybersecurity, Digital Engineering, (Military) Internet of Things und Mixed Reality.

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

MÖNCH Verlag GmbH R10

MÖNCH ist einer der weltweit führenden Zeitschriftenfachverlage in den Bereichen Verteidigung und Sicherheit. Unsere Zeitschriften erscheinen auf Deutsch, Englisch und auf Italienisch - sowohl in Druck wie auch digital. Dazu gehören:

- WEHRTECHNIK (Deutsch):Erscheinungsweise acht (8) Ausgaben per annum, für Leser in Deutschland, Österreich und in der Schweiz.
- HANDBUCH der BUNDESWEHR -das who is who in German defence
- NAVAL FORCES (Englisch): Erscheinungsweise vierteljährlich
- MILITARY TECHNOLOGY (Englisch): erscheint 2025 in Form von Sonderausgaben zu den Themen OCCAR - UNMANNED SYSTEMS sowie THE WORLD DEFENCE ALMANAC 2025
- RIVISTA ITALIANA DIFESA (Italienisch): erscheint monatlich.

Darüber hinaus veröffentlicht MÖNCH ca. 250 Buchtitel im Segment Verteidigung, Politik und Geschichte

Motorola Solutions Germany GmbH S32

BESSERER SCHUTZ DURCH OPTIMALE KOMMUNIKATION

Unser integriertes Technologie-Ökosystem verbindet Sprache, Daten, Video und Analysen auf einer einzigen Plattform für die erfolgreiche Planung und Durchführung Ihrer Missionen.

Streitkräfte sehen sich einer Vielzahl feindlicher Situationen gegenüber. Von komplexen Missionen in anspruchsvollen Einsatzgebieten bis hin zum Schutz von Stützpunkten vor konventionellen Bedrohungen. Streitkräfte bleiben dank unserer maßgeschneiderten Kommunikationslösungen jederzeit verbunden und optimal geschützt.

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

Mit mehr als 30 Jahren Erfahrung im Bereich Satellitenkommunikation ist ND SATCOM der weltweit führende Lieferant von satellitenbasierten Kommunikationssystemen und Bodenstationen, um Kunden mit kritischen Operationen überall auf der Welt zu unterstützen.

Kunden in mehr als 130 Ländern haben sich für ND SATCOM als eine zuverlässige Quelle für qualitativ hochwertige und sichere Lösungen, die schlüsselfertige und maßgeschneiderte Systeme beinhalten, entschieden. Die innovativen Technologien des Unternehmens werden weltweit von Regierungen, dem Militär sowie in den Bereichen Fernseh- und Rundfunkübertragung, der Telekommunikation und von Unternehmen eingesetzt.

Das Kernprodukt SKYWAN ermöglicht Tausenden von Nutzern täglich, eine sichere, zuverlässige und schnelle Kommunikation.

NetApp Deutschland GmbH W02 & S18

NetApp ist Ihr Partner für intelligente Dateninfrastruktur – denn Informationsüberlegenheit ist entscheidend. Mit Unified Storage, integrierten Data Services bis hin zu möglichen CloudOps-Lösungen von NetApp minimieren Sie Inselösungen und nutzen den Wandel als Chance. Ergänzt um daten- und KI-basierte Analyse schaffen wir volle Transparenz über die gesamte Systemlandschaft und ermöglichen dadurch optimales Datenmanagement. Unsere Data Services liefern starke Cyber-Resilienz, umfassende Governance und agile Applikationen; unsere CloudOps Services optimieren fortlaufend die Performance und Ressourceneffizienz mit Hilfe künstlicher Intelligenz und telemetrischer Analyse. Egal welche Daten und Umgebungen – NetApp transformiert Dateninfrastrukturen.

Newsletter Verteidigung / VDS Verlag R08

Der Newsletter Verteidigung (NV) aus dem Verlag Deutsche Spezialmedien berichtet wöchentlich aus den Bereichen Sicherheits- und Verteidigungspolitik sowie Beschaffung, Bedarf, Ausbildung, Personal, Technologie, Forschung und Events von Seiten der Bedarfsträger und der Industrie.

Der NV ist meinungsbildend, unabhängig und objektiv. Er zielt darauf ab, als Argumentationshilfe Entscheidungsprozesse zu erleichtern und zu beschleunigen. Geopolitisch konzentriert sich der NV auf internationale Themenfelder, die einen direkten oder indirekten Bezug zu den deutschen Streitkräften, der Industrie oder der deutschen Innen- und Außenpolitik haben.

NI Network Innovations B09b

Wir von Network Innovations haben uns auf die Bereitstellung zuverlässiger Satellitenkommunikationslösungen für kritische Missionen spezialisiert.

Unsere Kompetenz liegt in der Entwicklung und Wartung resistenter Netzwerke, die auf Ihre spezifischen Bedürfnisse zugeschnitten sind. Von Konnektivitätsverbindungen, Bandbreite und Abdeckung bis hin zu Terminals, Management-Tools, Installation und laufendem Support sorgen wir für einen nahtlosen Service. Wir arbeiten mit führenden Anbietern wie OneWeb, Starlink, ViaSat und Iridium zusammen und bieten hochgradig mobile, autarke Falllösungen, um Ihre Kommunikation auch in anspruchsvollen Umgebungen zu sicherzustellen.

NVIDIA GmbH R48, R51, S18

NVIDIA accelerated computing has reached a tipping point and achieved a virtuous cycle. The significant CUDA® installed base attracts developers and applications, which attracts resellers reaching customers, which expands the installed base to attract more developers.

CUDA, our parallel computing model launched in 2006, offers developers an unparalleled toolkit with over 300 libraries, 600 AI models, numerous SDKs, and support for 3,700 GPU accelerated applications. It has more than 53 million downloads. The success of the CUDA model has led to the creation of a thriving ecosystem that now includes over 5 million developers, 40,000 companies, and thousands of generative AI companies— all building on the NVIDIA platform.

ODM GmbH F28

Die ODM GmbH bietet ein breites Spektrum an Lösungen an, die genau auf die dynamischen Anforderungen des Militärs, der Spezialeinheiten, der Polizei und der Rettungsdienste weltweit zugeschnitten sind. Als Anbieter von Kommunikations- und Aufklärungstechnik haben wir uns darauf spezialisiert, Produkte zu entwickeln, die den individuellen Anforderungen unserer Kunden gerecht werden. Made in Germany.

OHB SE F20

Die OHB SE ist einer der führenden Anbieter von Raumfahrtsystemen in Europa. Mit der Expertise von über 3.000 hochqualifizierten Mitarbeiterinnen und Mitarbeitern in Europa und Übersee ist der Konzern hervorragend für den internationalen Wettbewerb aufgestellt und hat sich einen Namen als zuverlässiger Partner von staatlichen Institutionen und privaten Unternehmen gemacht.

Mit seinen drei Geschäftsfeldern Space Systems, Aerospace und Digital bietet der OHB-Konzern Raumfahrt von A bis Z. Die Aktivitäten erstrecken sich von der Realisierung von Satellitensystemen und Raumfahrtmissionen über die Fertigung von Bauteilen für Flugzeuge und Raketen bis hin zur Entwicklung von neuen Anwendungen für Satellitendaten. We.Create.Space.

Panasonic Connect Europe GmbH F05

Panasonic TOUGHBOOK bietet einsatzbereite Full-Ruggedized Laptops und Tablets, die nach Militärstandards (MIL-STD 810G) und gemäß IP65 / IP66 auf Zuverlässigkeit und Langlebigkeit getestet wurden.

Unsere COTS-basierten Geräte sind das ideale Tool für jede Mission im Verteidigungssektor. Dank leuchtstarker Outdoor-Displays mit Handschuhmodus, äußerst langer Akklaufzeiten und Hot-Swap Funktionen garantieren sie unterbrechungsfreien 24-Stunden-Einsatz.

Durch modulare Anpassungsoptionen wie integrierte maßgeschneiderte militärische Anschlüsse und Schnittstellen, verschlüsselte SSDs sowie eine breite Palette an Zubehör, Fahrzeug-Docking- und Tragelösungen machen sie zum perfekten Begleiter. TOUGHBOOK Geräte sind mit Windows erhältlich, aber auch für Red Hat Enterprise Linux zertifiziert.

PEGA F04

Mit der leistungsstarken Low-Code-Plattform von Pega sind weltweit führende Organisationen bestens für die Zukunft gerüstet, ganz nach unserem Motto Build for Change®. Durch KI-gestützte Entscheidungen und Workflow-Automatisierung meistern unsere Kunden ihre größten Herausforderungen – sie personalisieren Interaktionen, automatisieren ihren Service oder optimieren Geschäftsprozesse. Wir entwickeln unsere skalierbare und flexible Architektur seit 1983 stetig weiter, damit Unternehmen und der öffentliche Dienst heutige Kunden- und Bürgeranforderungen erfüllen und auch mit zukünftigen Entwicklungen Schritt halten.

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

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, Director Public Sector Business DACH, contact-dach@pexip.com

Planet Solutions GmbH S18

Die Planet-Gruppe (kurz “PLANET”) mit den Firmen PLANET Solutions & PLANET AI ist eine Firmengruppe, die sich seit 1992 der Entwicklung von Software mit kognitiven Fähigkeiten widmet.

Mit der KI-basierten IDP-Lösung (Intelligent Document Processing) “IDA” für intelligente Dokumentenanalyse bietet man umfassende Möglichkeiten zur Erfassung, Klassifikation und Extraktion von jeder Art von Dokumenten auch iVm. Large Language Modellen (LLM). Damit können dokumenten-basierte Prozesse stark automatisiert und effizienter agieren. Kombiniert mit agenten-basierten RAG-Systemen können auch komplexe KI-Chatbot-Systeme umgesetzt werden, die eine enorme Entscheidungsunterstützung für Fachanwender ermöglichen und auch ganz neue Möglichkeiten zur Informationsfindung eröffnen.

Planungsamt der Bundeswehr R61

Als zentraler Bedarfsträger für alle Organisationsbereiche der Bw gewährleistet das Planungsamt Bw-gemeinsame Planung aus einer Hand. Das Planungsamt erarbeitet die Grundlagen für die zukünftige Ausrichtung der Bw und trägt maßgeblich zur Weiterentwicklung der Fähigkeiten bei.

Das Innovationsmanagement des Planungsamtes ist Teil des Innovationsökosystems der Bw. Neben der Erschließung und Operationalisierung von Themen der Zukunftsentwicklung, sucht das Innovationsmanagement auch konkrete Ideen zur Verbesserung des Handlungs- und Leistungsvermögens der Bw mit dem Ziel, diese in Innovationsvorhaben zu überführen. Das Planungsamt hat dabei eine zentrale Rolle und bringt Ideengeber, potenziellen Nutzer der Organisationsbereiche, sowie weitere zentrale Akteure der Bw an einen Tisch.

PLATH GmbH & Co KG F18

Die PLATH GmbH & Co. KG ist ein international tätiger Anbieter von integrierten Systemen zur datenbasierten Krisenfrüherkennung. Unser innovatives Portfolio deckt den gesamten Aufklärungszyklus ab und hat sich weltweit in strategischen und taktischen Operationen bewährt. Als familiengeführtes Unternehmen mit 70 Jahren Branchen-Erfahrung unterstützen wir unsere Kunden bei der Erfüllung ihres Sicherheitsauftrags – mit dem Ziel, die Welt zu einem sicheren Ort zu machen.

Die PLATH GmbH & Co KG operiert als vollständig neutraler Systemintegrator unter dem Dach der PLATH Group eigenständig am Markt. Die PLATH Group ist in fünf Geschäftsbereiche unterteilt und umfasst 11 Unternehmen. Sie beschäftigt über 600 Mitarbeiter in Europa und weltweit. Weitere Informationen unter plath.de.

PNY Technologies Quadro GmbH R48

PNY Professional Solutions bieten leistungsstarke Lösungen für anspruchsvolle Workloads, insbesondere für Künstliche Intelligenz (AI), Data Science und High-Performance Computing. Das Portfolio umfasst NVIDIA Professional- und Data-Center-GPUs, Netzwerklösungen sowie PNY Speicher-Upgrades und SSDs.

Speziell für Systemintegratoren und Unternehmen entwickelt, ermöglichen PNY Produkte maximale Leistung, Produktivität und Energieeffizienz für AI, Deep Learning und datenintensive Workflows.

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 gleichzeitig zukunftssichere Lösungen und steht Ihnen mit langjähriger Erfahrung bei der Realisierung komplexer, integrationsfähiger Systemlösungen zur Seite.

ProSoft GmbH S61

ProSoft stellt an Stand S61 (Saal New York/Genf) leistungsstarke, wegweisende Lösungen vor, für den Schutz sensibler Netzwerke in Militär, Rüstungsindustrie und öffentlicher Sicherheit.

Während Datenschleusen mobile Datenträger isoliert und sicher überprüfen und so Netzwerke vor Schadsoftware „zu Fuß“ sichern, setzt unser Mitaussteller DriveLock mit seiner Lösung am Endpoint-Schutz an. Auf der AFCEA FA erfahren Sie mehr über beide Lösungen für lückenlosen Schutz vor Cyberangriffen, Spionage und Insider-Bedrohungen.

Seit über 35 Jahren steht ProSoft für kompetente Beratung, exzellenten Support und hochsichere Lösungen für den Schutz sensibler Daten und Netzwerke. Sprechen Sie unverbindlich mit uns an Stand S61. Sie erreichen uns auch unter 08171/405-200 oder info@prosoft.de.

PROSTEP AG R16

Die PROSTEP Gruppe ist der führende, unabhängige Anbieter für Beratung und Software rund um das Product Lifecycle Management (PLM) und das Application Lifecycle Management (ALM).

Wir unterstützen unsere Kunden bei der Schaffung der digitalen Durchgängigkeit, der Entwicklung Ihrer PLM-Strategie oder der Einführung eines digitalen Zwillings und stärken dadurch ihre Innovationskraft und Wettbewerbsfähigkeit und befähigen sie hochkomplexe Produkte und Systeme zu entwickeln, zu fertigen und zu betreiben.

Internationale Konsortien beraten wir bei der Erarbeitung Ihrer PLM-Strategie im Rahmen von Joint-Ventures. Wir haben über 30 Jahre Erfahrung in der PLM-Strategieberatung sowie der Systemauswahl bis zur Beratung rund um die Prozess-, Methoden- und IT-Systemgestaltung.

Pure Storage GmbH B10

Pure Storage (NYSE: PSTG) bietet die branchenweit beste Plattform, um Daten zu speichern, zu verwalten und zu schützen. Mit einem Cloud-Erlebnis in einer einheitlichen Speicherumgebung gibt Pure jedem Unternehmen die Flexibilität, die sich ändernden Anforderungen an die Nutzung und den Umgang mit Daten schnell und skalierbar zu erfüllen sowie gleichzeitig die Gesamtbetriebskosten zu senken. Pure ist davon überzeugt, einen erheblichen Beitrag zur weltweiten Reduzierung der Emissionen von Rechenzentren leisten zu können, indem es eine Speicherplattform anbietet, die es Kunden ermöglicht, ihren CO2-Fussabdruck und den Energieverbrauch deutlich zu reduzieren. Pure ist stolz darauf, ein kundenorientiertes Unternehmen zu sein, was durch den höchsten Net Promoter Score der Branche belegt wird.

QGroup GmbH R42

Die QGroup als IT-Security Hersteller und Dienstleister überträgt mit ihren Produkten und Dienstleistungen die Grundsätze der militärischen IT-Sicherheit auf ihre Auftraggeber. Unsere QTrust-Plattform erfüllt die Voraussetzungen für Security-by-Design. Sie ermöglicht den separationsfähigen Sicherheitsaufbau und integriert Sicherheitslösungen Dritter. QTrust steht u.a. für Resilienz, Interaktions- und Kooperationsfähigkeit.

Wir bieten ein Portfolio von Sicherheitsanwendungen: eigenentwickelte Penetrationstests, Passwortaudits und Schwachstellenanalysen, Implementierung unterschiedlicher Instrumente zum Endgeräteschutz, Netzwerküberwachung und Sicherstellung der Systemintegrität. www.qgroup.de

RHEINMETALL N01 & N09

Die börsennotierte Rheinmetall AG ist ein integrierter Technologiekonzern. Das substanzstarke und international erfolgreiche Unternehmen ist mit innovativen Produkten und Leistungen auf unterschiedlichen Märkten aktiv. Rheinmetall ist ein führendes internationales Systemhaus der Verteidigungsindustrie und zugleich Treiber zukunftsweisender technologischer und industrieller Innovationen auf den zivilen Märkten. 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, 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 über 35 Jahren ist roda strategischer Partner für die Entwicklung, Modifikation und Lieferung von militärischen mobilen Endgeräten, Displays, Servern, Netzwerktechnik und Stromversorgungen. roda Produkte zeichnen sich durch hohe Zuverlässigkeit, Langlebigkeit, sowie ein hohes Maß an kundenindividuellen Anpassungen aus, um den aktuellen und zukünftigen IT-Architekturen und Digitalisierungsvorhaben der europäischen Streitkräfte gerecht zu werden.

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; Funksysteme für die NATO-VJTF (Land) 2023; die Beteiligung im transeuropäischen Interoperabilitätsprojekt ESSOR; der wesentlicher „Combat Cloud“ und „Military IoT“ Enabler zu sein bei FCAS; und die Ausstattung von mehr als 40 Marinen weltweit.

rola Security Solutions GmbH F06b

ZUSAMMENARBEIT STÄRKEN, SICHERHEIT SCHAFFEN

Die Lagebearbeitung und Lagebilderstellung in militärischen Organisationen erfordert das Verdichten großer Informationsmengen aus unterschiedlichsten Quellen. Angesichts der steigenden Datenflut sind moderne Analyse- und Informationssysteme unverzichtbar. www.rola.com

Unsere Lösungen für das militärische Nachrichtenwesen bieten:

- Dynamische, bedarfsträgerorientierte Lagebilder
- Datenfusion und KI-gestützte Erkennung von Zusammenhängen
- OSINT-Recherchen und Objekterkennung
- Biometrische Analysen
- Praxiserprobten Datenschutz und nachvollziehbare Datenhaltung

RUAG GmbH 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

SAP Deutschland SE & CoKG F21 & A20

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 Schönhofer Sales and Engineering GmbH (SSE) ist ein deutsches Unternehmen, das seit 2022 zur Rohde & Schwarz Gruppe gehört. Die SSE entwickelt innovative Lösungen für den Sicherheits- und Verteidigungssektor. Die KI-unterstützte Datenanalyseplattform wandelt Sensordaten in Lösungen zur Entscheidungsunterstützung und Cybersicherheit um. Als zertifiziertes Unternehmen nach ISO 9001, ISO/IEC 20000-1 und ISO/IEC 27001 bietet die SSE maßgeschneiderte Lösungen mit Beratung und Unterstützung an.

SCOPE Engineering GmbH (ARBOR Gruppe GmbH) R63

Drei starke Unternehmen. Eine Starke Gruppe. ARBOR.

Die ARBOR-Gruppe vereint die Kompetenzen von OSW, TECO und SCOPE und bietet maßgeschneiderte Lösungen entlang des gesamten Entwicklungsprozesses von Produkten und Systemen. OSW Technische Dokumentation Verlag GmbH ist Ihr Partner für technische Dokumentation – von Anleitungen über Ersatzteilkataloge bis hin zu interaktiven Online-Dokumentationen.

Technical Concept GmbH ist spezialisiert auf Betriebsanleitungen, Risikobeurteilungen und Konformitätserklärungen für Maschinen und Anlagen nach EU-Recht. SCOPE Engineering GmbH bietet innovative Lösungen in den Bereichen System-, Software-, Hardware- und Mechanik-Engineering sowie technische Dokumentation. Gemeinsam stehen wir für Qualität, Präzision und Innovation.

SCOTTY Group Austria GmbH N08 & A02

SCOTTY ist ein Unternehmen, welches landmobile, maritime als auch aeronautische Kommunikationslösungen für sicherheitskritische Anwendungen realisiert.

Das Unternehmen ist darauf spezialisiert, in den Bereichen Software, Hardware und Netzwerktechnologie Kommunikationsinfrastrukturen für komplexe Einsatzbereich zu realisieren und zu optimieren.

Diese Lösungen unterstützen das gemeinsame Situationsbewusstsein durch den hochzuverlässigen, nativen und multimedialen Informationsaustausch, basierend auf resilienten Funk- und Satellitennetzen. Weltweit vertrauen zivile und militärische Organisationen auf Technologien von SCOTTY, um jederzeit, überall und unter allen Umständen kommunizieren zu können.

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. Cloud, IIoT, eGovernment und eHealth. Mit den Sicherheitslösungen von secunet können 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.

Secusmart GmbH S51

Secusmart ist führender Anbieter für sichere, ultramobile Kommunikationslösungen, speziell entwickelt für die Prozesse in Behörden.

Die Lösungen SecuSUITE for Samsung Knox und SecuSUITE for iOS ermöglichen mobiles Arbeiten auf Smartphones und Tablets bis hin zum Sicherheitsstandard VS-NfD. Apps mit der Einsatzerlaubnis des BSI für VS-NfD wie SecuFOX, SecuWORK und SecuOFFICE und SecuVOICE sichern die gesamte Kommunikation sowohl im Homeoffice als auch auf Dienstreisen und bei Einsätzen. Zudem setzt die Anwendung SecuVOICE neue Maßstäbe in der abhörsicheren Mobiltelefonie – zum Beispiel mit dem neuen Feature Group-Calling – und steht in Zusammenarbeit mit ISEC7 auch Landesbehörden und KRITIS-Unternehmen zur Verfügung. Sie finden uns: Saal New York/ Genf, S51

SELECTRIC Nachrichten-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 & DEFENCE B11

SES hat die Vision, durch die Verbreitung von Videoinhalten in höchster Qualität und die Bereitstellung nahtloser Datenkonnektivitätsleistungen beeindruckende Erlebnisse rund um den Erdball zu ermöglichen. Als Anbieter globaler Lösungen für Inhalte und Konnektivität besitzt und betreibt SES eine Satellitenflotte in der geosynchronen (GEO) und eine Konstellation in der mittleren (MEO) Erdumlaufbahn, die für eine weltweite Abdeckung und äußerst leistungsstarke Dienste sorgen. Mithilfe des intelligenten cloudfähigen Netzwerks kann SES an jedem Ort zu Land, zu Wasser und in der Luft hochwertige Konnektivitätslösungen bereitstellen und ist ein verlässlicher Partner für Telekommunikationsunternehmen, Mobilfunkbetreiber, staatliche Regierungsbehörden, Konnektivitäts- und Cloud-Dienstleister, Rund

Siemens Industry Software GmbH G04

Digitale Überlegenheit für Verteidigung und Sicherheit

Das Siemens Xcelerator Portfolio ermöglicht führenden Unternehmen der Verteidigungs- und Sicherheitsindustrie, digitale Zwillinge komplexer Systeme von der Anforderungsphase bis zum Einsatz zu entwickeln und zu nutzen. Diese hochpräzisen digitalen Repräsentationen verbessern Entscheidungsfindung, Zusammenarbeit und Automatisierung – für mehr Innovationskraft und operative Effizienz im gesamten Partner-Ökosystem.

Mit bewährter Interoperabilität, durchgängiger Systemintegration und breiter industrieller sowie behördlicher Akzeptanz ist Siemens Xcelerator der Schlüssel zur erfolgreichen digitalen Transformation in der Verteidigung. Vertrauen Sie auf Siemens – den digitalen Wegbereiter für Streitkräfte, Behörden und Industrie.

SINORA Cases 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.

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).

Software AG 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

Solifos Deutschland GmbH S27

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

Sophos Technology GmbH S62

Sophos schützt Unternehmen mit innovativen, anpassungsfähigen Schutzmaßnahmen und fundierter Expertise vor unvermeidbaren Cyberangriffen. Dank kontinuierlicher Innovationen bleibt Sophos Cyberbedrohungen immer einen Schritt voraus. Endpoint Security, Firewall Security, MDR und viele weitere Sicherheitskomponenten sind in die zentrale Management-Konsole Sophos Central integriert und das gesamte Cybersecurity-Ökosystem wird mit umfassender Threat Intelligence von Sophos X-Ops stetig optimiert.

Sopra Steria SE S12

Sopra Steria ist ein führender europäischer Tech-Player mit anerkannter Expertise in den Geschäftsfeldern Consulting, Digital Services und Solutions. Mit 52.000 Mitarbeitenden in rund 30 Ländern unterstützt der Konzern seine Kunden dabei, die digitale Transformation voranzutreiben und konkrete und nachhaltige Ergebnisse zu erzielen. Sopra Steria 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. Das Unternehmen 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.

STACKIT GmbH & Co. KG A07a

STACKIT ist der Cloud- und Colocation-Provider der Schwarz Gruppe. Auch externe Partner und Kunden in der DACH-Region können sich bei ihrer digitalen Transformation auf die Cloud-Services verlassen, von denen die Unternehmen der Schwarz Gruppe seit Jahren profitieren. Mit einer weit über den Marktstandard hinausgehenden Datensouveränität sowie individuellen Ansätzen zur Implementierung und zum Betrieb von Cloud-Lösungen begleitet STACKIT Digitalisierungsvorhaben ganzheitlich. Das im schwäbischen Neckarsulm beheimatete Team ebnet so den Weg in ein unabhängiges Europa – digital, führend. Als Teil von Schwarz Digits gehört die STACKIT GmbH und Co. KG zur IT- und Digitalsparte der Schwarz Gruppe. www.stackit.de

SVA System Vertrieb Alexander GmbH S53

Die SVA System Vertrieb Alexander GmbH zählt mit mehr als 3.300 Mitarbeitenden an 28 Standorten zu den führenden Systemintegratoren Deutschlands. Mit modernen, hochwertigen Lösungen und einschlägiger Projekterfahrung ist SVA der optimale Partner für Mittelständler, Großkonzerne und Behörden. Die Geschäftsstelle für den Öffentlichen Dienst ist spezialisiert auf den Verkauf von Hard- und Software etablierter Hersteller sowie den Vertrieb entsprechender IT-Dienstleistungen für öffentliche Auftraggeber. Über 440 Mitarbeitende widmen sich ausschließlich den besonderen Bedürfnissen von Verwaltungen: Ihre Kernkompetenz reicht von der Konzeption über die Planung und Beratung bis hin zur Integration und zu dem Betrieb von Systemlösungen und Fachanwendungen für öffentliche Auftraggeber. www.sva.de

steep GmbH S39

Zur 38. 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

Systematic GmbH S47

Mit 50+ Nutzernationen ist SitaWare von Systematic die global meistgenutzte C4ISR-Applikation und Wegbereiter der militärischen Interoperabilität. Die Commercial-off-the-Shelf (COTS) Produkte der SitaWare und IRIS Produktsuiten sind in multinationalen Einsätzen bewährt und werden kontinuierlich weiterentwickelt. Einsetzbar in stationären, verlegefähigen, mobilen und seegehenden Systemumgebungen, bietet SitaWare einen direkten operationellen Mehrwert. Intelligente Datenkommunikationsdienste ermöglichen die Nutzung vorhandener militärischer Kommunikationsmittel. Interoperabilität mit nationalen-, internationalen- und NATO-Systemen steht im Fokus. In der Bundeswehr ist SitaWare zentraler Bestandteil des Mission Enabling Service Bundeswehr (MESBw) und des National Maritime C2 Service (NMC2S).

Stellar PCS 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.

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, Mercury Systems, Moxa, RTD, Trenton Systems und Acromag, Kontakt: systerra computer GmbH, Kreuzberger Ring 22, 65205 Wiesbaden, Tel. 0611 / 44 88 9 – 400, E-Mail: info@systerra.de

SThree GmbH S52

SThree ist die globale STEM-Workforce-Beratung – angetrieben von Ambition, Expertise und Technologie.

Wir beraten Unternehmen, bauen Expertenteams auf und liefern maßgeschneiderte Projektlösungen, um gemeinsam der Zeit voraus zu sein.

Wir sind die Game Changer in STEM. Seit 38 Jahren konzentrieren wir uns ausschließlich auf STEM – mit einem globalen Team von über 2.700 Fachkräften und lokaler Expertise in 11 Ländern. Wir besetzen hochgefragte Kompetenzfelder wie Engineering, Life Sciences und Technologie.

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 38. 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.

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.

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.

Telespazio Germany GmbH — S22 & A08

Telespazio Germany GmbH, eine Tochtergesellschaft von Telespazio – einem Joint Venture von Leonardo und Thales (67:33) – ist ein führendes Unternehmen der Luft- und Raumfahrt, das Beratungs-, Technologie- und Ingenieurdienstleistungen anbietet.

Mit über zwei Jahrzehnten Erfahrung ist Telespazio Germany ein anerkannter Experte für Trainingslösungen und bietet maßgeschneiderte Trainingssysteme für Piloten- und Operator-Training, virtuelle Wartungstrainer und VR-basierte Lösungen für Wartungstechniker.

Durch Partnerschaften mit führenden Satellitenanbietern liefert Telespazio Germany zuverlässige Kommunikationslösungen mit unabhängigen, maßgeschneiderten Netzwerken über LEO-, MEO- und GEO-Satelliten und gewährleistet krisenfeste Konnektivität für Unternehmen, Regierungen und Industrie.

Trend Micro Deutschland GmbH — S36

Trend Micro, einer der weltweit führenden Anbieter von Cybersicherheit, hilft dabei, eine sichere Welt für den digitalen Datenaustausch zu schaffen. Basierend auf jahrzehntelanger Expertise in IT-Sicherheit und Künstlicher Intelligenz, globaler Bedrohungsforschung und beständigen Innovationen schützt unsere KI-gestützte Cybersecurity-Plattform hunderttausende Unternehmen und Millionen von Menschen über Clouds, Netzwerke, Geräte und Endpunkte hinweg.

Trend Micros Plattform ist führend in Cloud- und Enterprise-Cybersecurity und bietet fortschrittliche Verteidigungstechnologien für Umgebungen wie AWS, Microsoft und Google. Zentrale Sichtbarkeit ermöglicht es Unternehmen, Angriffe schneller zu erkennen und besser darauf zu reagieren.

https://www.trendmicro.com/de_de/business.html

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, elektrische Sicherheit 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.

Unterstützungskommando der Bundeswehr R64

Zentraler Dienstleister der Bundeswehr

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, Sanitätswesen, ABC-Abwehr, Feldjägerwesen und Zivil Militärische Zusammenarbeit unterstützt. Die im Unterstützungsbereich gebündelten Kräfte und Fähigkeiten stehen nur begrenzt zur Verfügung, sind aber kriegsentscheidend. Sie stärken die Einsatzfähigkeit der Bundeswehr und gewährleisten flexible Unterstützung in Frieden, Krise und Krieg. Die Führung obliegt dem Unterstützungskommando der Bundeswehr in Bonn mit rund 750 Soldatinnen und Soldaten sowie zivilen Mitarbeiterinnen und Mitarbeitern.

USU GmbH R54

USU ist führender Anbieter von Software und Services für IT- und Enterprise Service Management. Unsere KI-gestützten, ITIL®-konformen Lösungen helfen Unternehmen weltweit, smartere Services, effizientere Workflows und bessere Zusammenarbeit zu realisieren. Damit digitalisieren und automatisieren Kunden Prozesse für Planung, Design, Betrieb, Steuerung, Nutzung und Verrechnung von Services – in IT, technischem Kundendienst, HR und Facility Management. Für den öffentlichen Bereich bieten wir Sicherheitsfunktionen wie On-Premises-Betrieb, die Unterstützung des Federal Mission Network Standards (FMN) und die Möglichkeit, in isolierten Netzen zu arbeiten (Air-Gap).

Mehr Infos: www.usu.com

Utimaco S19

Utimaco ist ein global führender Anbieter von Hochsicherheitstechnologien für Cybersecurity und Compliance-Lösungen und Services mit Hauptsitz in Aachen, Deutschland und Campbell (CA), USA. Utimaco entwickelt und produziert On-Premise und Cloud-basierte Hardware-Sicherheitsmodule, Lösungen für Schlüsselmanagement, Datenschutz und Identitätsmanagement sowie Data Intelligence-Lösungen für regulierte kritische Infrastrukturen und öffentliche Warnsysteme. In seinen Kernbereichen nimmt Utimaco eine führende Marktposition ein.

Veteranenbüro der Bundeswehr A100

Das Veteranenbüro der Bundeswehr in Berlin ist die zentrale Anlaufstelle für alle Veteraninnen und Veteranen. Es bietet Beratung, Information und Unterstützung in allen Fragen der Betreuung und Fürsorge – für aktive Soldaten wie ehrenhaft Entlassene der Bundeswehr. Unsere Aufgaben: Wir beraten individuell, vermitteln Unterstützungsangebote, informieren die Öffentlichkeit, stärken Netzwerke und unterstützen Vereine und Verbände sowie den Beauftragten für Veteranenangelegenheiten. Mit einem engagierten Team arbeiten wir sichtbar in der Mitte der Gesellschaft. Das öffentliche Büro befindet sich nahe dem Berliner Hauptbahnhof in einem zivilen Gebäude und steht auch zivilen und militärischen Organisationen offen. https://www.bundeswehr.de/de/betreuung-fuersorge/veteranenbuero.

VDI TZ GmbH / NKS Europäischer Verteidigungsfonds R29

Die Nationale Kontaktstelle für den Europäischen Verteidigungsfonds (NKS EVF) informiert und berät deutsche Unternehmen und Institutionen, die sich im europäischen Förderprogramm für die Verteidigungsforschung beteiligen möchten oder bereits mit Projekten aktiv sind.

Der Europäische Verteidigungsfonds ist ein Industrieförderprogramm der Europäischen Kommission und hat zum Ziel, die europäische Verteidigungsindustrie durch Anreize zur gezielten Kooperation wettbewerbs - und innovationsfähiger zu machen. Unternehmen können sich im europäischen Verbund auf Fördermittel für Forschung und Entwicklung bewerben.

Die NKS EVF ist bei der VDI Technologiezentrum GmbH angesiedelt und arbeitet im Auftrag des Bundesministeriums der Verteidigung. Weitere Informationen unter bundeswehr.de/nksevf.

VECTED GmbH R55

Als Spezialist für Wärmebildtechnologie mit integrierter Künstlicher Intelligenz (KI) entwickeln wir individuelle optoelektronische High-End Lösungen für unsere Kunden. Aktuelle Schwerpunkte im Bereich KI liegen bei der Objekterkennung und Klassifizierung sowie der emissionslosen Entfernungsmessung. Das Spektrum der möglichen Anwendungen für die KI reicht von Beobachtungsgeräten über Waffenvisierungen, optischen Systemen aller Art in Fahrzeugen bis hin zu Guidance Systemen in Flugkörpern.

In der Rüstung bieten wir von der Entwicklung hauseigener Hard- und Software über das Design, Training und die Evaluierung der integrierten KI, den Prototypenbau und die Qualifikation bis hin zur Produktion ITAR-frei alles aus einer Hand an.

Kontakt: Pascal Stammer, info@vected.de, +49 911 960 687 0

Verband der Reservisten der Bundeswehr e.V. B02

Der Verband der Reservisten der Deutschen Bundeswehr (VdRBw) hat mehr als 110.000 Mitglieder. Wir vertreten die Reservisten in allen militärischen Angelegenheiten. Sie sind: Reservisten der Bundeswehr (ordentliche Mitglieder), aktive Soldaten (außerordentliche Mitglieder), Personen ohne Wehrdienst (fördernde Mitglieder).

Wir sind für Sie da!

Beim Verband haben alle Reservisten der Bundeswehr die Möglichkeit, eine militärische Heimat zu finden. Die Vielfalt der Informations- und Veranstaltungsangebote aller Gliederungen deckt so gut wie alle Einzelinteressen ab, Kameradschaft und Betreuung ergänzen das Angebot.

www.reservistenverband.de

Viasat A07c

Viasat (ehemals Inmarsat) stellt sich der Aufgabe die Art und Weise, wie Kunden, Regierungen und Militär kommunizieren, sicher und zuverlässig zu gestalten.

Viasat wird von über 90 Regierungen weltweit für alle operativen Anforderungen und kritischen Missionen eingesetzt.
Wir verfügen über langjährige Erfahrung in der Bereitstellung von aktuellen Lagebildern und der Steigerung von kritischen Fähigkeiten unsere Kunden überall und jederzeit. Neben globaler nahtloser Satellitenkommunikation über die verschiedensten Bänder und Orbits, bieten wir auch die Werkzeuge für die sichere Kommunikation von Behörden. Das umfasst die sichere Übertragung und Speicherung von Daten.

Ebenso wie Terminals und Dienste für alle Domänen: Land, Luft, See, Cyber und Weltraum.

Vitec GmbH W04

Seit 1988 ist VITEC weltweit führend als Anbieter von innovativen IP-Video Produkten und Systemen im Bereich von professionellen “End to End”-Video Streaming Lösungen für Behörden und Organisationen mit Sicherheitsaufgaben (BOS), das Militär und die Industrie.

Mit weit mehr als dreihundert Entwicklungsingenieuren realisiert VITEC innovative und kosteneffektive Hard- und Software-Lösungen, Advanced Technology Research und Custom Design Projekte für ein internationales Kundennetzwerk.

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.

WORK Microwave GmbH F12

Seit über 35 Jahren ist WORK Microwave ein führender Anbieter von Verteidigungselektronik und Governmental-Lösungen. Zu den allesamt selbst entwickelten und produzierten Produkten gehören Komponenten, Module und Systeme

sowie viele weitere innovative HF- und Digital-Produkte. WORK Microwave ist für seine Qualität, kundenspezifischen Lösungen, Zuverlässigkeit und seinen erstklassigen Kundenservice bekannt. Das Unternehmen setzt Maßstäbe für Innovationen im Bereich der HF-Technologie und in der digitalen Signalverarbeitung. Mit ca. 150 Mitarbeitern am Hauptsitz in Holzkirchen bedient WORK Microwave weltweit ansässige Kunden. Seit 2015 gibt es Niederlassungen in den USA, Frankreich und Singapur.

Weitere Informationen zum Unternehmen finden Sie auf www.work-microwave.com

Xecuro GmbH S25

Mit Sicherheit geheim.

Xecuro ist Ihr Partner für Verschlusssachen-Kommunikation. Das Unternehmen bietet darüber hinaus Services im Rahmen von VS-Infrastruktur & Betrieb, von VS-NfD bis GEHEIM, sowie VS-Dienstleistungen an.

Xecuro wurde im November 2021 gegründet und ist eine Tochtergesellschaft der Bundesdruckerei Gruppe.

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.

Zebra Technologies 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

Advertorials

Anzeigen

BSC Berlin Security Conference

SAVE THE DATE

18–19 NOV 2025

24th Congress on European Security and Defence

Vienna House Andel's

#BSC25

SIGN UP NOW

www.euro-defence.eu

Vorankündigung:

39. AFCEA-Fachausstellung

12. – 13. 05. 2026

World Conference Center Bonn

www.afcea.de