



AFCEA 2024

BWI – Digitalisierungspartner der Bundeswehr

ISBN 978-3-934401-81-5

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

SecuSUITE for iOS oder SecuSUITE for Samsung Knox?

**„Sagen
Sie es uns!“**



Neugierig?

Besuchen Sie uns:
Messestand: Saal New York / Genf
Stand S 51



Highlight:

Give users a choice.

Ab sofort haben Sie die Wahl.

Vortrag von Dr. Christoph Erdmann,
Geschäftsführer Secusmart GmbH
26. Juni 2024, 15:45 Uhr
Plenarsaal Bundestag

**Mit den Lösungen von Secusmart
können Sie Ihr Betriebssystem
für Smartphone & Tablet frei wählen.**

Spitzen-Sicherheit
für mobile Kommunikation
und mobiles Arbeiten.

So komfortabel, wie
Sie es von der privaten
Nutzung kennen.

So kompatibel und
verlässlich, wie Sie es von
Secusmart gewohnt sind.



Frank Leidenberger

Foto: BWI GmbH/Xandra Herdieckerhoff

Die 2020er-Jahre stellen uns vor immense sicherheitspolitische Herausforderungen. Das gilt für die Situation in Europa genauso wie für die Lage im Nahen Osten und im pazifischen Raum. Daraus ergeben sich Konsequenzen für Deutschland, die mittlerweile immer deutlicher zu spüren sind: Freiheit und Sicherheit sind auch hierzulande bedroht. Und um sie zu verteidigen, brauchen wir einsatzbereite, kriegstüchtige – siegfähige – Streitkräfte.

Aber was heißt das in Zeiten der Digitalisierung? Die Geschwindigkeit, mit der Innovationen entwickelt werden, hat immens zugenommen. Das hat signifikante Auswirkungen auf die Fähigkeitsentwicklung auch im Militärischen, wie wir täglich auf den Gefechtsfeldern in der Ukraine beobachten können. Klassische Modernisierungsprozesse für militärische Hardware werden den Anforderungen an das Veränderungstempo nicht mehr gerecht. Gleichzeitig hat der Einsatz von vielfältigen Sensoren, digitalen Kommunikationsmitteln bis hin zu „intelligenten“ Wirkmitteln die Entscheidungszyklen auf dem Gefechtsfeld nachhaltig beschleunigt. Der Einsatz von Software in allen Elementen der militärischen Systeme revolutioniert derzeit die Kriegsführung.

Die umfassende Antwort auf dieses Phänomen ist das Konzept von Software Defined Defence, also des „Internet of Military Things“. Dahinter steckt die Idee, militärische Fähigkeiten nicht mehr nur über die Hardware zu definieren, sondern sie als Gesamtsystem zu interpretieren, dessen Intelligenz in der Software liegt. Dabei bietet die Software neue Optionen, Systemfähigkeiten schnell zu adaptieren. Kampfwertsteigerungen können über Software-Updates erzielt werden, die auf konkrete Herausforderungen angepasst sind. Innovationszyklen werden verkürzt und agiles Problemlösen ermöglicht.

Entscheidend für eine performante Softwareentwicklung ist eine leistungsfähige, resiliente IT-Infrastruktur, in der große Datenmengen sicher verarbeitet und Applikation sowie deren Updates verzuglos verteilt werden können. Der Ausbau einer solchen Technologie ist eine der Kernaufgaben, um die Bundeswehr für die Herausforderungen der Zukunft zu wappnen. Die Ankündigung des Bundesverteidigungsministers, im April den Organisationsbereich CIR als vierte Teilstreitkraft aufzustellen, hat die Relevanz des Cyber- und Informationsraums noch einmal sehr deutlich gemacht. Damit wird der Tatsache Rechnung getragen, dass Kriege der Gegenwart in allen Dimensionen geführt werden. Zudem zeigt es deutlich die Relevanz der Digitalisierung und des digitalen Raums für die Streitkräfte. Die AFCEA wird in diesem Jahr einen guten Rahmen bieten, um darüber ins Gespräch zu kommen.

Frank Leidenberger

Chief Executive Officer, BWI GmbH

Impressum Sonderheft Behörden Spiegel „AFCEA 2024“ **Redaktionelle Leitung** Reimar Scherz, Behörden Spiegel, Telefon: 0228/970970 **Herausgeber** (presserechtlich verantwortlich) Dr. Eva-Charlotte Proll, Behörden Spiegel-Gruppe **Verlegt** von der ProPress Verlagsgesellschaft mbH, Friedrich-Ebert-Allee 57, 53113 Bonn, 0228/970970; Berlin, Kaskelstraße 41, 10317 Berlin, 030/5574120; **Anzeigen** Jennifer Großblotekamp **Herstellung** Spree Service- und Beratungsgesellschaft mbH, Berlin **Satz und Layout** Maximilian Spuling, Spree Service- und Beratungsgesellschaft mbH, Berlin **Fotos** Autoren, AFCEA Bonn e.V., BWI, Behörden Spiegel-Archiv **Druck** Köllen Druck + Verlag GmbH, Bonn **Heftpreis** 7,50 Euro ©Alle Beiträge (Wort und Bild) in diesem Heft sind urheberrechtlich geschützt. Eine Weitergabe – auch digital – bedarf der Einwilligung des Verlages. www.behoerdenspiegel.de

Vorwort	3
Frank Leidenberger, Chief Executive Officer, BWI GmbH	
Unser Beitrag verpflichtet!	6
Brigadegeneral Armin Fleischmann, Vorsitzender AFCEA Bonn e.V., Unterabteilungsleiter BMVg CIT I	
AFCEA Vorstand und Aufgaben	8
Geschäftsstelle AFCEA Bonn	9
Generative KI – Neue Chancen und Risiken im Bereich Verteidigung und Sicherheit	11
Dr. Michael Gerz, Vorstand AFCEA Bonn e.V. Wissenschaft und Forschung, Informationstechnik für Führungssysteme, Fraunhofer FKIE	
Und was hat Mentoring mit Resilienz und der Zeitenwende zu tun?	13
Marianna Schwarz, AFCEA Vorstand Mentoring & Innovation, Account Direktor BWI GmbH, mit dem Autoren- und Organisationsteam AFCEA Mentoring Programm Annika Harpening, Airbus Defence and Space GmbH, Key Account Manager Information Systems and Cybersecurity, Florian Mahlmeister, Lead Business Architect BWI GmbH	
Mehr gemeinsame Wertschöpfung wagen und eine schnellere Fähigkeitsentwicklung ermöglichen	15
Christopher Gaube, AFCEA Bonn e.V. Vorstand Ausbildung, Head of Defense Business & Technology Solutions, Capgemini Deutschland GmbH	
Digitalisierung als Faktor der Resilienz oder umgekehrt? – Eine gegenseitige Betrachtung	18
Generalleutnant a.D. Dr. Ansgar Rieks, AFCEA Vorstand Schulförderung	
Vertrauenswürdige Künstliche Intelligenz	20
Justus Groth, AFCEA Vorstand Emerging Leaders AFCEA Bonn e.V., IBM, mit Autorenteam: Paul Bauer, Matthias Klaus, Moritz Diederichsen, Andreas de Jonge	
Kriegsführung im Wandel – Auswirkung disruptiver Innovationen auf die Führungsunterstützung in der Dimension Land	22
Oberst i. G. Rainer Beeck, AFCEA Vorstand Bundeswehr, CDO Heer	
Sicherheitsarchitektur im Wandel – Die Bedeutung fortschrittlicher Beschaffungsstrategien	25
Christian Rösch, Schriftführer AFCEA Bonn e.V., Senior Sales Manager Eviden	
AFCEA Fachausstellung 2024 am 26./27. Juni 2024 – Die IT-Fachmesse der Sicherheitsorganisationen und -firmen	27
Oberst a.D. Wolfgang Quirin, Leiter AFCEA Fachausstellung	
Antworten auf die Zeitenwende – Die BWI und das Zielbild 2028	32
Dr. Christian Marwitz, Chief Digital Officer, Mitglied der Geschäftsführung, BWI GmbH	
Durch Informations- und Führungsüberlegenheit zur Wirkungsüberlegenheit – Anforderungen moderner Streitkräfte	35
Vizeadmiral Dr. Thomas Daum, Inspekteur Cyber- und Informationsraum	
Die Komplexität hinter „einfach funktionieren!“	37
Julian Klein, Leiter Shared Service Operations, BWI GmbH	
Informationsüberlegenheit – Data Analysis als Game Changer	41
Christian Bartels, Head of & SVP Owner Software Data Solutions & Analytics	
Mit digitaler Vernetzung zur militärischen Überlegenheit	44
Dr. Martin Deeg, Leiter BWI Customer Solutions	
Agiler und robuster – Cloud und die Fähigkeitsentwicklung der Bundeswehr	48
Dr. Götz Reinhäkel, Programmleiter pCloudBw, BWI GmbH	
BWI International, Mission & Training: IT-Unterstützung für Einsätze und Übungen	51
Alexander Behrends, Leiter Military IT bei BWI International, Mission & Training	
Der Cyber-Schutz-Schild der Bw – Datenintegrität und Informationsüberlegenheit durch ein ganzheitliches Sicherheitskonzept	55
Oliver Frommherz, Leiter Competence Center IT-Security, BWI GmbH	
BWI Technology Center ebnen Weg für die Bundeswehr-IT von morgen	58
Matthias Görtz, Chief Technology Officer, BWI GmbH	
BWI – Resiliente Leistungserbringung in Frieden, Krise und Krieg	62
Andreas Bänsch, Account-Direktor einsatznahe IT und Themengebiet LV/BV, BWI GmbH	
„Wir brauchen IT-Services, die uns bei Resilienz und Robustheit unterstützen“	63
Generalleutnant André Bodemann im Interview	
Resilienz durch gute Partnerschaften	65
Katrin Hahn, Chief Resources Officer, Mitglied der Geschäftsführung, BWI GmbH	

Symposium AFCEA FA 2024	69
Ausstellerliste AFCEA Fachausstellung 2024	70
Standpläne im World Conference Center Bonn	72
Symposium und Industrievorträge	76
Aussteller AFCEA-Fachausstellung 2024	78
Inserentenverzeichnis	114

MATERNA
VirtualSolution

Ultramobiles Arbeiten für Einsatz- und Streitkräfte

**Bis zum Geheimhaltungsgrad »VS-NfD« und
»NATO RESTRICTED«**

Per Smartphone und Tablet:

- + sicher mobil arbeiten und kommunizieren (geräte- und plattformunabhängig)
- + jederzeit und von jedem Ort auf interne Fachanwendungen zugreifen
- + Koordinaten, Lagedaten und Informationen sicher austauschen

**Zertifiziert vom BSI mit einer Zulassung (iOS) und einer
Freigabeempfehlung (Android)**

Erfahren Sie mehr über unsere Container-Lösung SecurePIM:

Tel.: +49 89 30 90 57-0 · E-Mail: sales@virtual-solution.com
www.materna-virtual-solution.com



VS-NfD
ZULASSUNG FÜR IOS
FREIGABE FÜR ANDROID
BUNDESAMT FÜR SICHERHEIT
IN DER INFORMATIONSTECHNIK



NATO RESTRICTED
FÜR IOS
SICHERHEIT MADE IN GERMANY

Unser Beitrag verpflichtet!

Brigadegeneral Armin Fleischmann, Vorsitzender AFCEA Bonn e.V., Unterabteilungsleiter BMVg CIT I



Armin Fleischmann
Brigadegeneral

Foto: privat

Als AFCEA Bonn e.V. widmen wir uns in diesem Jahr dem Motto „Zeitenwende in der nationalen Sicherheit – Resilienz durch disruptive digitale Lösungen“. Der russische Angriff auf die Ukraine, die Konflikte um Berg-Karabach, die Krisenregion Naher Osten und viele weitere Konflikte und Spannungen rund um den Globus führten zum berühmten Ausspruch der „Zeitenwende“ im Deut-

schen Bundestag. Dies soll auch für die Bundeswehr eine „Zeitenwende“ darstellen: mehr Geld, bessere Ausrüstung, schnellere Einsatzbereitschaft. Das entsprechende angekündigte Sondervermögen umfasst formal 100 Milliarden Euro für den Bereich Verteidigung.

Die Zeitenwende in der nationalen Sicherheit, die sowohl durch die neue sicherheitspolitische Lage als auch durch disruptive und digitale Lösungen vorangetrieben wird, setzt neue politische und vor allem operative Notwendigkeiten. Dies eröffnet technisch – und insbesondere von der Digitalisierung her – neue Möglichkeiten und Herausforderungen. Diese Ansätze machen es – richtig implementiert – möglich, die notwendige Resilienz der Bundesrepublik Deutschland gegenüber verschiedenen Bedrohungen zu erhöhen und die nationale Souveränität zu stärken sowie eine führende Rolle in verschiedenen Bereichen zu spielen. Wichtig ist, alle Maßnahmen an den operativen und politischen Notwendigkeiten auszurichten.

Zeitenwende in der nationalen Sicherheit – Resilienz durch disruptive digitale Lösungen

Das bedeutet auch eine Zeitenwende in der Digitalisierung und für uns als IT-Community der Verteidigung und Sicherheit. Neun Felder lassen sich dabei konkret benennen, in denen die Zeitenwende für unseren Tätigkeitsbereich Wirkung entfalten wird, wenn wir das Ziel Resilienz und nationale Sicherheit auch in der IT ernstnehmen:

1. Frühwarnsysteme:

Durch den Einsatz von fortschrittlichen Analysemethoden und KI können Frühwarnsysteme verbessert werden, um Bedrohungen schneller zu erkennen.

2. Cybersicherheit:

Die Stärkung der Cybersicherheit durch z. B. Security by Design und Zero Trust-Ansätze ist von entscheidender Bedeutung, um sich gegen Cyberangriffe zu verteidigen, die heute eine ernsthafte Bedrohung darstellen.

3. Krisenkommunikation:

Digitale Lösungen ermöglichen eine schnellere und effektivere Kommunikation während Krisen, was die Reaktionsfähigkeit erhöht.

4. Datenmanagement:

Durch Datenschutz und verantwortungsvolle Datennutzung kann Deutschland die nationale Datensouveränität stärken und gleichzeitig datenbasierte Innovationen vorantreiben.

5. Künstliche Intelligenz (KI):

Deutschland kann KI nutzen, um z.B. seine Industrie, Gesundheitsversorgung und Bildung zu transformieren, die Fähigkeiten der Streitkräfte zu optimieren und in die Lage zu versetzen, einen potenten Gegner erfolgreich zu bekämpfen, und gleichzeitig KI-Systeme mit hohen ethischen Standards zu entwickeln.

6. Quantentechnologien:

Als Vorreiter in Quantencomputing kann Deutschland komplexe wissenschaftliche Probleme lösen und fortschrittliche Verschlüsselungstechnologien entwickeln und Lagebilder optimieren.

7. Software Defined Defence:

Fortschrittliche Verteidigungssysteme ermöglichen eine bessere Anpassungsfähigkeit und Sicherheit gegenüber Cyberbedrohungen. Sie ist aber auch eine notwendige Voraussetzung, um Fähigkeiten adäquat und einsatzbereit den Herausforderungen anzupassen.

8. Weltraumtechnologien:

Deutschland kann seine Präsenz im Weltraumsektor ausbauen und die nationale Souveränität in der Weltraumforschung und -technologie stärken.



Stetig gewachsen und gut besucht: Die AFCEA Fachausstellung ist seit Jahrzehnten ein zentraler Ort zum Austausch.

Foto: AFCEA Bonn e.V.

9. Innovationsförderung:

Die Zusammenarbeit mit der privaten Industrie, den inneren und äußeren Sicherheitsorganen, sowie der Forschung kann die Entwicklung neuer Technologien und Lösungen beschleunigen. Die Förderung von Innovationen und Start-ups im IT-Sektor, aber auch eine Konvergenz digitaler Lösungen der etablierten IT-Firmen, kann Deutschland helfen, Technologieführerschaft zu erlangen und neue Geschäftsfelder zu erschließen.



Inhaltlich begleitet das Symposium mit hochrangigen Rednern und Experten die Fachausstellung.

Foto: AFCEA Bonn e.V.

Die koordinierte Zusammenarbeit zwischen Regierung, Industrie, Forschung und Bildungseinrichtungen ist unerlässlich, um die unterschiedlichen Themenfelder zusammenzubringen, Chancen zu identifizieren und Potenziale zu heben. Dies erfordert erhebliche Investitionen in Forschung und Entwicklung, Bildung, Infrastruktur im Bereich der inneren und äußeren Sicherheit, 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.

Sind wir hier bereits am Ziel? Sicher nicht! Ich bin überzeugt, dass gerade unsere Community mit engagierten Mitgliedern aus Ämterseite, der Industrie und der Wissenschaft zusammen Lösungen entwickeln und umsetzen kann. Wir als Community sind diejenigen, die von dieser neuen Technologie in höchstem Maße profitieren können – wenn man es denn richtig organisiert!

AFCEA Bonn e.V. möchte als gemeinnütziger Verein mit seinem Jahresprogramm 2024 die Austauschplattform bieten, auf der sich Bedarfsträger, Bedarfsdecker, Industrie und die Wissenschaft austauschen können. So wird AFCEA dazu beitragen, dass durch sachlichen Dialog und frühzeitige Information der Bedarfsträger seine Interessen darstellen, der Bedarfsdecker Lösungsräume identifizieren und die Industrie den Sachstand und das Entwicklungspotential darstellen kann. Aber auch die Wissenschaft sollte die neuesten Erkenntnisse in Konzeptionen einfließen lassen.

Die AFCEA Fachausstellung ist dafür in besonderem Maße geeignet. Zum vierten Mal öffnet sie am 26. und 27. Juni

2024 im World Conference Center Bonn ihre Tore. Wir erwarten wieder mehrere tausend Teilnehmer aus Besuchern und Standpersonal. Weit über 200 Aussteller werden auf sieben Ausstellungsflächen dabei sein. Unser Symposium beschäftigt sich in Vorträgen und Podiumsdiskussionen mit aktuellen militärpolitischen Brennpunkthemen. Fachliche Firmenvorträge gibt es in der Speaker's Corner zu hören. Natürlich wird auch der gesellige Austausch mit dem traditionellen Get-together am ersten Messeabend wieder stattfinden.

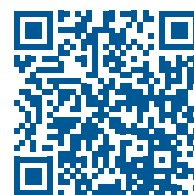
AFCEA Bonn e.V. hat sich der Zielsetzung verschrieben, seinen Mitgliedern und der interessierten Öffentlichkeit ein Spezialforum moderner Informations- und Kommunikationstechnologie zu bieten. Das Anwenderforum für Fernmeldetechnik, Computer, Elektronik und Automatisierung (AFCEA) Bonn e.V. umfasst als gemeinnützig anerkannter Verein ohne kommerzielle Interessen über 1.000 persönliche und mehr als 100 Firmenmitglieder. Die AFCEA Fachausstellung stellt als unsere Flaggschiff-Veranstaltung so etwas wie ein lebendes Kondensat unseres Vereins dar.

In diesem Jahr wollen wir die Fachausstellung als aktiven Beitrag zur Zeitenwende anbieten. Uns ist die Bedeutung und die Notwendigkeit des Handelns und der schnellen Umsetzung von Veränderungen bewusst. Wir dürfen die Bedeutung des Informationsraumes nicht unterschätzen: Desinformationskampagnen und Extremismus destabilisieren unsere Gesellschaft und setzen tagtäglich unsere freiheitliche demokratische Grundordnung unter Druck. Über Jahrzehnte haben wir die Friedensdividende eingestrichen. Doch die zunehmende militärische Bedrohung erfordert ebenfalls die Investition in Verteidigungsfähigkeit – oder wie es der Bundesverteidigungsminister nennt: Kriegstüchtigkeit.

Die Antwort darauf ist ein „Mehr“: Mehr Engagement für die digitale Zeitenwende, mehr Investitionen in diese Lösungen, mehr Resilienz für den Wandel durch diese Zeiten! Selten konnte unsere Community mit ihren Lösungen und Erfahrungen so einen wertvollen Beitrag für die nationale Sicherheit und für mehr Resilienz durch disruptive digitale Lösungen leisten. Dieser Beitrag sollte uns eine Verpflichtung für die Gesellschaft sein.

Auch dafür steht unser Jahresmotto 2024. Und für diesen Austausch laden wir Sie zur AFCEA Fachausstellung ein!

AFCEA-Jahresprogramm



AFCEA Vorstand und Aufgaben

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

Vertretungsberechtigter Vorstand nach §26 BGB



Brigadegeneral 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



Oberst i. G. Rainer Beeck, Bundeswehr

Fotos: Homepage AFCEA Bonn e.V.

Geschäftsstelle AFCEA Bonn

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



Damit aus sicherheitsrelevant nicht allgemein bekannt wird.

SINA schützt Daten und IT der Streitkräfte bis GEHEIM und NATO SECRET. Hochskalierbar, resilient, flexibel.

Wo die nationale Sicherheit geschützt werden muss, steht secunet bereit.

Als IT-Sicherheitspartner der Bundesrepublik Deutschland sind wir Lösungslieferant für Multi-Level-Security und hochsichere Verschlüsselungstechnik.

secunet.com protecting digital infrastructures

secunet

KI bei HENSOLDT

Von Daten zur Entscheidung

- Jahrzehntelange Erfahrung im operationellen Einsatz maschineller Lernverfahren.
- Modernste KI-Verfahren für Detektion, Tracking und Klassifikation.
- Sensornahe, vollintegrierte Datenverarbeitung bei minimaler Latenz.
- Kompetenz in der Analyse und Nutzbarmachung großer Datenmengen.
- Fusion von Daten aus Radaren, Kameras, SIGINT und OSINT.

Besuchen Sie uns auf der AFCEA 2024 am Stand W07 und A07.

Generative KI – Neue Chancen und Risiken im Bereich Verteidigung und Sicherheit

Dr. Michael Gerz, Vorstand AFCEA Bonn e.V. Wissenschaft und Forschung, Informationstechnik für Führungssysteme, Fraunhofer FKIE



Dr. Michael Gerz

Foto: privat

Als Ende 2022 OpenAI das Werkzeug ChatGPT einer breiten Öffentlichkeit vorstellte, löste dies einen wahren Hype aus. Erstmals war eine auf künstlicher Intelligenz (KI) beruhende Anwendung in der Lage, natürlichsprachliche Dialoge zu führen. ChatGPT konnte dabei auch Aufgaben bearbeiten, für die es nicht spezifisch trainiert war, was manche als Vorzeichen einer Künstlichen Allgemeinen Intelligenz

(engl.: artificial general intelligence) deuteten. Auch wenn es bis dahin noch ein sehr langer Weg ist, so sind bereits jetzt zahlreiche Anwendungen möglich oder zumindest perspektivisch absehbar.

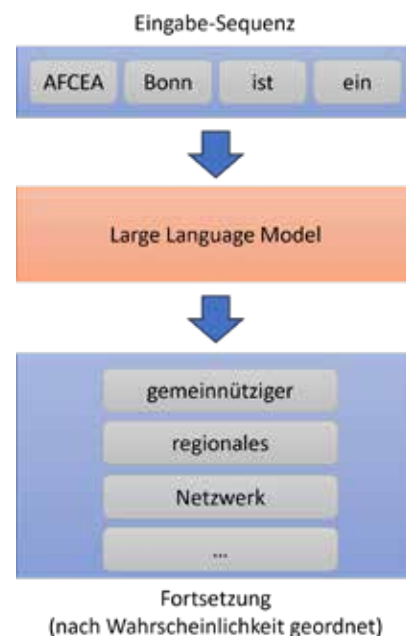
Anwendungen wie ChatGPT lassen sich der sogenannten generativen KI zuordnen. Sie ermöglicht es, Muster und Strukturen in Trainingsdaten zu erkennen und daraus neue Daten mit ähnlichen Eigenschaften zu erzeugen. Im Fall von ChatGPT läuft es darauf hinaus, dass auf Basis des bisherigen Chatverlaufs und der bisher generierten (Teil-)Antwort die jeweils wahrscheinlichsten nächsten Wörter (bzw. Tokens) ermittelt werden und dann eine Wahl getroffen wird. Die generative KI grenzt sich von der diskriminierenden KI ab, die Eingaben in vordefinierte Kategorien einteilt, z. B. ob ein Social-Media-Beitrag „Hate Speech“ enthält (Kategorien: ja/nein) oder welche Typen von Objekten in einem Bild enthalten sind. Die generative KI beruht für die Verarbeitung von geschriebenen Texten auf sogenannten Large Language Models, deren Entwicklung aktuell von einigen wenigen großen Playern vorangetrieben wird.

Die Methoden der generativen KI eröffnen ein breites Spektrum von Fähigkeiten, u. a. die Erzeugung und Vervollständigung von natürlichsprachlichen Texten, die Erstellung von Programmcode für die Softwareentwicklung, die Generierung von Bildern und Videos auf Basis von textuellen Beschreibungen, die Übersetzung, Zusammenfassung und Sentiment-Analyse von Texten sowie Frage-/Antwort-Systeme. Die generative KI hat das Potential, weite Bereiche des gesellschaftlichen Lebens zu verändern. Die Bandbreite reicht dabei von der Unterstützung bei kreativen Tätigkeiten, über Kundeninteraktion und Vertragsprüfungen, bis hin zur

Betreuung einsamer Menschen. Mit Bezug auf Verteidigung und Sicherheit eröffnet die generative KI ebenfalls zahlreiche Möglichkeiten, birgt aber auch neue Bedrohungsrisiken. Eine naheliegende Anwendung generativer KI ist zunächst die automatische Übersetzung von natürlicher Sprache. Hiermit ist es möglich, verfügbare Informationen schneller zu erfassen und auszuwerten. Ein aktueller Forschungsgegenstand sind dabei insbesondere Sprachen, für die nur eingeschränkte Trainingsdaten zur Verfügung stehen. Dieses Problem kann z. B. dadurch adressiert werden, indem man in einem ersten Schritt Trainingsdaten einer verbreiteteren Sprache aus derselben Sprachfamilie nutzt.

Generative KI wird zukünftig im Bereich der Open Source Intelligence (OSINT) dabei unterstützen, Social Media-Beiträge automatisiert auszuwerten. So wird es möglich sein, dass eine Anwendung aus einer Menge vorhandener Posts einen kurzen Report erstellt, der z. B. die Themen und unterschiedlichen Sichtweisen der Nutzer zusammenfasst. Eine ähnliche Vorgehensweise ist perspektivisch auch für die Erstellung von Lageberichten denkbar.

Mit Hilfe von generativer KI wird es gegnerischen Kräften andererseits erheblich erleichtert, Desinformationskampfa-



Funktionsweise von Generativer KI

Foto: Gerz/privat

gnen durchzuführen. Texte, die mit großen Sprachmodellen erstellt werden, lassen sich bereits jetzt nicht mehr von denen eines Menschen unterscheiden. Anstatt die sozialen Medien über Botnetze mit den immer gleichen Texten zu fluten, können Gegner mit generativer KI vollautomatisch individuelle Texte erstellen, die auf die jeweilige Zielgruppe zugeschnitten sind. Man stelle sich beispielsweise eine Anwendung vor, die systematisch Nutzerforen scannt und – mittels eines entsprechend antrainierten Narrativs – in laufende Diskussionen eingreift und diese gezielt in die gewünschte Richtung steuert. Aufgrund der neuen Möglichkeiten, die öffentliche Meinung zu beeinflussen, ist es umso wichtiger, Strategien zu entwickeln, um derartige Desinformationskampagnen frühzeitig zu erkennen und entsprechend entgegenzuwirken.

Eine inhärente Eigenschaft aktueller KI-Systeme ist es, dass sie keine deterministischen Ergebnisse liefern und gelegentlich auch „halluzinieren“, d.h. überzeugend formulierte Ergebnisse liefern, die sich bei genauerer Betrachtung jedoch als objektiv falsch erweisen. Für viele Anwendungen stellt dies aktuell noch eine große Herausforderung dar, insbesondere bei Frage-/Antwort-Systemen. Insofern ist es bei der Integration von KI-Services in militärische Systeme von zentraler Bedeutung, dass diese in einem gesicherten Rahmen genutzt werden können und die Nutzer sich der Grenzen generativer KI stets bewusst sind.

Andererseits ist der Nichtdeterminismus von generativer KI bei kreativen Aufgaben von Vorteil. So ist es denkbar, dass sie bei der Erstellung von operationellen Szenarien unterstützt. In einem mehrstufigen Prozess kann beispielsweise mit Hilfe von KI anhand einiger weniger Stichworte zunächst der grobe Rahmen entwickelt und anschließend das vorhandene Szenario durch einzelne Ereignisse angereichert wer-

den. Ebenso kann generative KI genutzt werden, um vermeintliche Beiträge (Audio, Video, Text) in öffentlichen und sozialen Medien zu simulieren. Bereits heute ist es möglich, Avatare als Nachrichtensprecher einzusetzen.

Es ist zu erwarten, dass auch beim Wargaming und für das Training generative KI einen wichtigen Beitrag leisten kann. Durch die Fähigkeit, menschliches Verhalten zu simulieren, können menschliche Agenten in einer virtuellen Simulationsumgebung noch natürlicher interagieren.

Darüber hinaus gibt es zahlreiche weitere Anwendungsfälle: Für die Wartung von Ausrüstung erleichtern Sprachassistenten die Interaktion mit dem Nutzer; bei juristischen Fragestellungen können große Sprachmodelle aufgrund vorheriger Trainingsdaten Empfehlungen geben – mit der gebotenen Vorsicht!

Aufgrund der sehr hohen Ressourcenanforderungen liegt die Erstellung großer Sprachmodelle derzeit in den Händen einiger weniger Firmen. Viele Entwicklungen finden derzeit im Ausland statt. Die entwickelten Sprachmodelle stellen eine Blackbox dar. Eine versehentliche oder vorsätzliche Beeinflussung bzw. ein Bias kann nicht ausgeschlossen werden. Daher sind neue Verfahren zu entwickeln, mit denen große Sprachmodelle im Kontext spezifischer Anwendungen bewertet werden können. Es gilt, die nationale Souveränität auf diesem wichtigen KI-Gebiet sicherzustellen und Modelle zu schaffen, die auch in eingestufteten Umgebungen nutzbar sind.

Bereits im vergangenen Jahr wurde das Thema generative KI in verschiedenen AFCEA-Veranstaltungen aufgegriffen. Aufgrund der hohen Relevanz wird ihm im November 2024 mit dem AFCEA Zukunfts- und Technologieforum eine ganztägige Veranstaltung gewidmet.



steep GmbH
Service. Technik. Sicherheit.



**Besuchen Sie uns auf der AFCEA 2024
an unserem Stand S39 im Saal New York/Genf**

Und was hat Mentoring mit Resilienz und der Zeitenwende zu tun?

Marianna Schwarz, AFCEA Vorstand Mentoring & Innovation, Account Direktor BWI GmbH, mit dem Autoren- und Organisationsteam AFCEA Mentoring Programm Annika Harpening, Airbus Defence and Space GmbH, Key Account Manager Information Systems and Cybersecurity, Florian Mahlmeister, Lead Business Architect BWI GmbH



Marianna Schwarz

Foto: BWI GmbH

Das diesjährige Leitthema von AFCEA Bonn lautet: „Zeitenwende in der nationalen Sicherheit – Resilienz durch disruptive digitale Lösungen“. Entsprechend ranken sich alle Veranstaltungen und Programme rund um dieses Themengebiet. Zu erwarten sind Beiträge zu Multi Domain Operations, Software Defined Defence oder Sensor-to-Effector Wirkketten. Wie aber passt das Mentoring-Programm zu diesem Jahresthema?

Eines sei vorweggenommen

Ja, Mentoring passt zum Jahresthema, und zwar sogar ziemlich gut. Nicht umsonst führt AFCEA nun schon zum dritten Mal in Folge das jeweils auf ein Jahr angelegte AFCEA Mentoring Programm durch. Ein Zusammenhang zwischen Mentoring und Jahresthema lässt sich immer sehr gut herstellen. Schließlich bietet gerade ein Mentoring-Programm einen Nutzen und Wert für die inhaltliche Betrachtung!

Im Jahr 2021 haben wir das Mentoring Programm erstmals ins Leben gerufen, damals noch als Testballon. Als gemeinnützig agierender und anerkannter Verein hat sich AFCEA



Annika Harpening

Foto: privat

Bonn e.V. mit seiner Satzung selbst auferlegt, junge Talente zu fördern und Nachwuchskräfte zu entwickeln. Daneben hat AFCEA sich zum Ziel gesetzt, Bundeswehr und öffentliche Verwaltung, Industrie und Forschung ins Gespräch miteinander zu bringen und in diesem Rahmen Meinungen und Lösungen auszutauschen. Aus diesem Gedanken heraus ist das cross-organisationale Mentoring

geboren, das auf beide Ziele einzahlt. Das Programm trägt dazu bei, die nächste Generation von Führungskräften und Fachleuten auf die mit der Zeitenwende verbundenen Herausforderungen vorzubereiten. Durch die Zusammenarbeit mit MentorInnen außerhalb der eigenen Organisation, also dem cross-organisationalen Ansatz, erhalten die Mentees frische Perspektiven und Einblicke in unterschiedliche Arbeitsweisen, Branchen und Organisationen. Dies kann zu innovativen Ideen und neuartigen Ansätzen führen. Über das Jahr hinweg sind die Mentees angehalten, über eine strukturierte 360-Grad-Selbstreflexion sich selbst und ihre Werte zu reflektieren und sich ihrer eigenen Wirkung auf andere bewusst zu werden. Dabei werden sie durch ihre Mentorinnen und Mentoren unterstützt und begleitet, um ihre ganz persönlichen Ziele zu erreichen.



Florian Mahlmeister

Foto: privat

Aber zurück zum (Jahres-)Thema

Beginnen wir mit der Definition der Begrifflichkeiten „Zeitenwende“ und „Resilienz“. Resilienz bezieht sich auf die Fähigkeit eines Systems, Störungen zu überstehen und sich anzupassen. Dieses System kann technischer, organisatorischer, prozessualer oder auch menschlicher Natur sein. Eine Zeitenwende bezieht sich auf einen Zeitpunkt, an dem grundlegende Veränderungen in verschiedenen Aspekten der Gesellschaft, Wirtschaft und Technologie auftreten.

Bringen wir Resilienz und Zeitenwende in den Kontext des Mentorings

Ein qualifiziertes Mentoring-Verhältnis kann dazu beitragen, die Fähigkeit einer Person zur Bewältigung von Herausforderungen und zur Anpassung an Veränderungen zu stärken – also die Resilienz einer Person auszuprägen. Mentoring kann darüber hinaus in Zeiten des Wandels und der Zeitenwende einen wichtigen Beitrag zur Bewältigung von Veränderungen und Herausforderungen in unserer sich ständig verändernden Welt leisten und vielfältige Auswir-

kungen auf individueller, organisatorischer und gesellschaftlicher Ebene mitbringen.

Und was heißt das nun genau?

Resiliente Menschen sind dadurch gekennzeichnet, dass sie Impulse kontrollieren und Emotionen steuern können, über eine optimistische Einstellung verfügen und situativ fokussieren. Sie sind in der Lage zu bewerten, wann sie ein Vorhaben aufgeben oder adaptieren müssen und passen ihre Ziele entsprechend an.



Verabschiedung des ersten Mentoring-Jahrgangs und Begrüßung des zweiten Jahrgangs im Rahmen der AFCEA Fachausstellung 2023

Foto: privat

„Die Kunst ist, einmal mehr aufzustehen, als man umgeworfen wird.“ (Winston Churchill)

Aufbauend auf diesem Verständnis können MentorInnen eine wichtige Rolle bei der Ausprägung von Resilienz von Mentees in Zeiten der Veränderung spielen. Sie haben dabei die Aufgabe, ihren Mentees das Handwerkzeug und Erfahrungswissen im Umgang mit schnellen Veränderungen, bei Unsicherheit und zur Krisenbewältigung mitzugeben –

ihnen also bei der Steigerung ihrer Resilienz in einem dynamischen Umfeld zur Seite zu stehen.

Im Rahmen des Programms soll basierend auf der Selbstreflexion ein besseres Verständnis für die eigenen Stärken und Schwächen geschaffen werden. Dieser Ansatz stellt ein wertvolles Instrument dar, um eine umfassende und ausgewogene Perspektive auf die individuelle Entwicklung zu gewinnen und weiter persönlich zu wachsen. Da die Mentees im cross-organisationalen Mentoring-Ansatz außerhalb ihrer eigenen Institution agieren, sind sie oft eher bereit, sich zu öffnen, kritisch zu reflektieren und ihre Fähigkeiten und Herangehensweisen zu überdenken. Für beide Seiten, Mentorin oder Mentor und Mentee, kann der intensive Austausch mit einer „anderen Welt“ zu wertvollen Einsichten, neuen Ideen und Gedankenanstößen führen.

Und wie werde ich Mentorin, Mentor oder Mentee?

MentorInnen werden entweder auf Basis bestehender Kontakte angesprochen. Alternativ können sich alle, die eine Mentoring-Rolle übernehmen wollen, an das OrgTeam bei AFCEA Bonn e.V. wenden. Mentees hingegen müssen einen Bewerbungsprozess durchlaufen, der jeweils zum Jahresbeginn startet. Hierbei sind sie angehalten, ihr persönliches Ziel und Motivation zu definieren, das sie im Rahmen des Mentorings erreichen und worauf sie in einem Jahr hinarbeiten möchten. Die Mentorinnen und Mentoren wählen daraufhin sorgfältig die/den Mentee aus, die/der am besten zu ihnen passt. Das Programm-Kickoff findet während der AFCEA Fachausstellung statt.

An dieser Stelle bedanken wir uns ganz herzlich bei den bisherigen Teilnehmerinnen und Teilnehmern, unseren zehn Mentees und zehn Mentorinnen und Mentoren der ersten beiden Durchläufe. Wir freuen uns auf weitere erfolgreiche Mentoring-Beziehungen, die im Geiste der AFCEA junge Talente fördern, Nachwuchskräfte entwickeln und den Austausch zwischen Bundeswehr, öffentlicher Verwaltung, Industrie und Forschung verstärken.

VITEC

Any Asset | Anywhere | Any Network
Der Spezialist für taktische Videos

Bereitstellung von IP-Video und Informationsdaten für Situational Awareness und ISR-Video-streaming

Zuverlässiges Live-Video-Streaming für kritische Entscheidungsprozesse

Robustes IP-Streaming mit ultraniedriger Latenz und Stream Protection



Besuchen Sie uns auf der AFCEA 2024
Messestand W04 / Ausstellungsfläche SAAL WIEN

www.vitec.com

Mehr gemeinsame Wertschöpfung wagen und eine schnellere Fähigkeitsentwicklung ermöglichen

Christopher Gaube, AFCEA Bonn e.V. Vorstand Ausbildung, Head of Defense Business & Technology Solutions, Capgemini Deutschland GmbH



Christopher Gaube Foto: privat

Der Begriff Zeitenwende steht für den Beginn einer neuen Ära. Die aktuelle Zeitenwende ist vor allem durch die sich dynamisch entwickelnde globale sicherheitspolitische Rahmenlage geprägt. Flankierend wirken der rasante technologische Wandel und eine kommerziell getriebene Verfügbarkeit und Nutzung, was zugleich die Reifung der Technologie beschleunigt.

Um relevant zu bleiben, muss sich ein System ständig an veränderte Rahmenbedingungen anpassen können. In der Marktwirtschaft lässt sich das exemplarisch an der Ablösung alter Branchenführer wie beispielsweise Nokia und im militärischen Kontext an den Teilerfolgen und dem Überleben der ukrainischen Streitkräfte erkennen.

Zur Steigerung der agilen Adaptionfähigkeit in Verfügbarkeit und Nutzung von technologischen Fähigkeitspotentialen hat die Bundeswehr erste Schritte unternommen. Das Narrativ von Software Defined Defense folgt dem Aspekt von schneller Adaption entlang der Linien des Möglichen. Schnelligkeit aufbauen insbesondere durch das Vorsehen einer zeitweisen Entkopplung von Hardware und Software und Nutzung der Entwicklungsgeschwindigkeit von Software. Im Ergebnis wird eine Steigerung der Anpassungsgeschwindigkeit von (Waffen-) Systemen und Plattformen sowie zugleich eine effektivere Fähigkeitsentwicklung erreicht. Dieser Betrachtung folgend bildet die Fähigkeitsentwicklung eine Konvergenz aus Hardware und Software für militärische Funktionsketten ab und bricht mit dem alleinigen Fokussieren auf Hardware als Fähigkeitstreiber.

Medien und Politiker beschreiben die aktuelle Situation als Polykrise. Die sich verändernden sicherheitspolitischen Rahmenbedingungen stellen eine ständige Herausforderung dar, die eine Flexibilität und kontinuierliche Anpassung

erfordert – auch eine Frage von Kultur und Mindset. In einer dynamischen und komplexen Welt, geprägt von technologischem Fortschritt, geopolitischen Veränderungen und neuen Herausforderungen, ist es unerlässlich, dass Methoden und Vorgehensweisen überdacht werden und anpassungsfähig gestaltet sind. Flexibilität und Agilität werden zu entscheidenden Elementen, um auf unvorhergesehene Ereignisse und Herausforderungen reagieren zu können.

Das Ökosystem aus Streitkräften, Industrie und Wissenschaft ist Kern der Fähigkeitsentwicklung. Die Grenzen zwischen den Akteuren gilt es zu minimieren, damit jede Seite essenzielle und integrierte Beiträge für die Fähigkeitsentwicklung leisten kann. Dabei muss das Rad nicht neu erfunden, sondern die Bandbreite an Formaten ausgeschöpft werden.

Auf der einen Seite lassen sich Aspekte wie Architektur, Schnittstellen und Standards aufführen, die eine eher technologische Perspektive unterstützen. Architektur, die von Grund auf Modularität, Skalierbarkeit und offene Schnittstellen ausgelegt ist, ermöglicht neue Technologien schnell zu integrieren und erhöht nicht nur die Effizienz, sondern stärkt zugleich die gemeinsame Wertschöpfung im Ökosystem. Ein Ökosystem, das auf etablierten Standards basiert, bildet die Grundlage für eine moderne und zukunftsorientierte Verteidigungsfähigkeit. Auf der anderen Seite befinden sich grundsätzliche Zusammenarbeitsmodelle innerhalb des Ökosystems, welche eine methodische Perspektive verfolgen. Zentral hierbei ist die Frage: Wie kann sichergestellt werden, dass der Nutzer seine Bedürfnisse klar, transparent und möglichst permanent artikulieren kann, sodass diejenigen, die Lösungen entwickeln und bereitstellen, ein präzises



Grafik: privat

Verständnis der Anforderungen des Nutzers erlangen?

In diesem Fall muss die gemeinsame Wertschöpfung von Streitkräften, Wissenschaft und Industrie auf mehreren Ebenen überdacht und weiterentwickelt werden. Einerseits muss die Intensität der Formate zunehmen und andererseits muss die Bandbreite an Formaten genutzt werden. Die Intensivierung und Stärkung der Tiefe der vertrauensvollen Zusammenarbeit an gemeinsamen Missionen steht im Zentrum, die nicht nur punktuell, sondern kontinuierlich und intensiv erfolgen muss – eine Zielsetzung, die im Einklang mit dem Narrativ der AFCEA steht.



Vertrauensvolle Zusammenarbeit für gemeinsame Missionen steht im Zentrum – auch bei der AFCEA Fachausstellung.

Foto: AFCEA Bonn e.V.

Die Bundeswehr als Nutzer verfügt über ein präzises Verständnis der operativen Herausforderungen. Auf der anderen Seite stehen die Lösungsentwickler und -anbieter – Industrie und Wissenschaft – mit dem Wissen um Technologien und deren Machbarkeit. Die Einbindung der Nutzer und Integration des aktiven Feedbacks ist essenziell, um Use Cases präziser darstellen und weiterentwickeln zu können. Die bislang bestehenden Widerstände bzw. Hindernisse einer tiefen gemeinsamen Wertschöpfung sind zu überwinden, um die digitale, technologische Transformation erfolgreich zu gestalten. Der Fokus auf herkömmliche Ansätze ist oft nicht mehr ausreichend.

Aktuell geschehen wesentliche Anteile des Wissensaustauschs auf Messen, Konferenzen und in gemeinsamen Arbeitsgruppen. Der initiale Austausch und die konzeptionelle Erarbeitung eines gemeinsamen Verständnisses als Katalysator können dabei nur der Anfang sein. Der nächste Schritt ist dann oft Einzelpersonalunterstützung durch Industrie und Wirtschaft in (Rüstungs-)Vorhaben. Auch erreichen den Markt oftmals komplexe, schwer nachvollziehbare Leistungsbeschreibungen, um die eigenen Anforderungen zu kommunizieren. Die gemeinsame Wertschöpfung ist dabei nur punktuell oder nur auf Personenbasis, nicht auf Systemebene. Doch die Bandbreite der gemeinsamen Wertschöpfung lässt sich darauf nicht limitieren. Dabei ist es entscheidend zu verstehen, dass es in diesem Kontext keine starren Schwarz-Weiß-Kategorien gibt; jedes Projekt ist einzigartig

und erfordert eine individuelle Herangehensweise. Die gemeinsame Wertschöpfung lässt sich in den im Weiteren angerissenen Formaten intensivieren.

Produktzentrierte Ausschreibungen bieten über punktuelle Formate – wie etwa Leistungsbeschreibung oder Einsatzprüfung – ein niedriges Maß an gemeinsamer Wertschöpfung. Steigern ließe sich dies, wenn das Produkt im Rahmen eines (Managed) Services die Partner näher zusammenbringt. Die Zusammenarbeit wäre hier nicht punktuell, sondern integriert. Der Reifegrad der Zusammenarbeit wird über die Zeit dieses transformatorischen Ansatzes gesteigert. Hier gestalten die Nutzerorganisation und Industrie zusammen die Transformation und tragen ein gemeinsames Risiko. In dieser tiefen Integration verschwimmen die Grenzen zwischen öffentlichem Auftraggeber, Industrie und Wissenschaft. Es entsteht eine gemeinsame Vision, in der beide Seiten gemeinsam an Problemstellungen arbeiten und den Weg für zukünftige Innovationen ebnen. Es entsteht gemeinsames Wissen und Expertise.

Ein hohes Maß an Wertschöpfung kann durch die Gründung einer gemeinsamen Unternehmung realisiert werden. Hier erreicht die Integration eine noch tiefere Ebene, begleitet von einem höheren Investitions- und Risikoniveau, das jedoch gemeinsam getragen wird. Durch die Schaffung einer gemeinsamen Unternehmung werden nicht nur Wissen und Ressourcen effektiv geteilt, sondern auch das Engagement für die gemeinsame Lösungsfindung intensiviert. Dieser Ansatz zeichnet sich besonders durch einen offenen Lösungsraum aus, der Raum für Kreativität und Innovation bietet, anstatt ihn zu begrenzen. Auf diese Weise wird nicht nur die Zusammenarbeit auf ein neues Level gehoben, sondern es entsteht auch ein gemeinsames unternehmerisches Ökosystem, das den Grundstein für wegweisende Entwicklungen legt.

Inmitten der dynamischen und umfassenden Transformation des Ökosystems bestehend aus Bundeswehr, Industrie und Wissenschaft gibt es eine unumgängliche Erkenntnis: Die gemeinsame Wertschöpfung muss intensiviert werden, um den Herausforderungen gerecht zu werden. Die softwaregetriebene Transformation verändert nicht nur militärische Funktionsketten, sondern prägt neue Geschäftsmodelle in der Zusammenarbeit mit der Wirtschaft. Diese Veränderungen verlangen von den Akteuren im Ökosystem eine Anpassung an neue Realitäten und Vertrauen. Es liegt an allen Beteiligten, diese Chancen zu nutzen, um eine sicherere und erfolgreichere Zukunft zu gestalten. Die Leitplanken erlauben es die dargestellten Möglichkeiten stärker zu nutzen. Der persönliche Austausch auf Veranstaltungen von AFCEA Bonn e.V. ist dabei meist der Anfang einer gemeinsamen Wertschöpfung. Im Kern bleibt die Feststellung: Einfach mal machen!



WIR STELLEN UNS DEN HERAUSFORDERUNGEN EINER DIGITALEN WELT

Erfahren Sie mehr über vernetzte Systemlösungen der Zukunft

- Infanterist der Zukunft – Integration von Drohnen und Loitering Munition
- Smart und small UAS – Aufklärung und Situational Awareness
- Mobile Smart Factory – Der mobile 3D-Druck
- Innovative Softwarelösungen – Digitalisierung von Instandhaltungsprozessen

auf unserem Stand N01 + N09 im Saal NAIROBI auf der AFCEA in Bonn am 26. und 27. Juni 2024.

Digitalisierung als Faktor der Resilienz oder umgekehrt? – Eine gegenseitige Betrachtung

Generalleutnant a.D. Dr. Ansgar Rieks, AFCEA Vorstand Schulförderung



Dr. Ansgar Rieks
Generalleutnant a.D. Foto: privat

Wählen wir als Startpunkt für die Diskussion „Resilienz“, dann wissen wir intuitiv, dass Digitalisierung darin eine große Rolle spielt. Jenseits der notwendigen Sicherheit gegen Angriffe auf unsere IT können wir danach fragen, wie funktionsfähig in Krisen die zunehmende Digitalisierung ist. Wir verbinden mit Resilienz also eine Art Schutz, Durchhaltbarkeit oder Stabilität in herausfordernden Lagen.

Das verlangen wir auch für unsere IT.

Wählen wir als Startpunkt die „Digitalisierung“, dann ist konkret zu ermitteln, wie sie in ihrer Anwendung Resilienz schafft. Zweifellos müssen auch alle digitalen Entwicklungen Resilienz erzeugen oder unterstützen. Manchmal zweifeln wir etwas daran, dass dieses gelingt. Hat also weiterhin nur das Einfache im Krieg Erfolg, oder wird es angesichts der notwendigen Digitalisierung künftig anders sein?

Es bedarf einer gegenseitigen Betrachtung zwischen Resilienz und Digitalisierung. Das gilt umso mehr im Konkreten: Resilienz und Digitalisierung bedingen einander.

Informationstechnik ist ein wichtiger Faktor der Resilienzförderung. Zugleich schafft sie neue Angriffsmöglichkeiten und Verwundbarkeiten, die einer Resilienz entgegenstehen. Unabhängig davon, wohin sich die Waage neigt, sind Digitalisierung und Informationstechnik nicht mehr aus unserer

Welt wegzudenken. Digitalisierung ist „unabdingbar“ geworden. Um sie resilienter aufzustellen, gibt es allerlei Ansätze und Forschungen. Dabei spielen Energie-, Rohstoff-, Emissions- und Liefereffizienz eine Rolle. Es gilt dabei: Technologie fördert Effizienz, und Effizienz fördert Resilienz.



Gehärtete Hardware: Digitalisierung, die bei Einflussnahme von außen nicht mehr funktioniert, ist nicht einsatztauglich.

Foto: AFCEA Bonn e.V.

In der militärischen Anwendung kommt die Frage hinzu, wie ein Waffensystem durch Digitalisierung auch gegen einen unsachgemäßen, ungewollten oder widerrechtlichen und unethischen Gebrauch resilient gemacht werden kann. Für digitale Resilienz gilt konkret:

- Digitalisierung, die zwar Präzision und Durchsetzungskraft erhöht, aber bei Einflussnahme von außen nicht mehr funktioniert, ist nicht einsatztauglich.
- Lagebilder sind nur dann hilfreich, wenn die Daten auch bei einer Cyber-Bedrohung unverfälscht vorliegen.

Multi-Domain-Warfighting – als operativer Ansatz gegenüber einem militärisch modern aufgestellten Gegner – ist notwendig. Hinreichend ist es nur, wenn die eingesetzte IT auch im Krieg ausreichend ‚standhaft‘ ist. Vom ‚Infanteristen der Zukunft‘ bis zum Kampfflugzeug ist von dieser Diskussion keine Ebene ausgenommen.

Für die Datenhaltung gilt im Speziellen: Angesichts der immer größeren Menge von Daten ist eine proprietäre Datenhaltung nur begrenzt sinnvoll. Bei allen Ansätzen einer



Kampfpanzer Leopard 2 und Tablet: Digitalisierung ist „unabdingbar“ geworden. Foto: AFCEA Bonn e.V.



Multi-Domain-Warfighting ist notwendig. Hinreichend ist es nur, wenn die eingesetzte IT auch im Krieg ausreichend ‚standhaft‘ ist. Keine Ebene ist ausgenommen.

Foto: AFCEA Bonn e.V.

Cloud-basierten Datenverarbeitung mit zentralen Ansätzen für Datenfusion und -verteilung, ist allerdings die Rückfallposition bei einer Unterbrechung oder Störung der Datenversorgung einzubeziehen. Hierzu sind vorgesehene und programmierte Automatismen eine Lösung – beispielsweise die klassische Auftragstaktik.

Wechseln wir nochmal die Perspektive: Militärische Resilienz braucht Digitalisierung. Generalinspekteur Carsten Breuer betont: „Die alte Formel ‚Kämpfen können, um nicht

kämpfen zu müssen‘ reicht nicht mehr. ... Das Ziel muss sein: ‚Gewinnen wollen, weil wir gewinnen müssen‘.“ Dazu gehört, definierte operative Notwendigkeiten durch moderne Technologien leistungsfähig zu realisieren. Digitalisierung spielt hierbei „die“ prägende Rolle. Ihre schnellen, innovativen Entwicklungen sind ebenso einzubeziehen, wie die Interoperabilität mit unseren Partnern. Operateure müssen sich mit Digitalisierung befassen und Forschung und Entwicklung mit Operationsführung.

Das Ganze klingt durchaus komplex. Wenn aber Optimismus, Cleverness, praktische Intelligenz, Vertrauen und innere Stärke Eigenschaften des Menschen sind, gibt es die Chance, sowohl die notwendige Resilienz als auch die Digitalisierung voranzutreiben. Zukunft war schon immer etwas für die Aktiven, Informierten und Mutigen.



IT-ARCHITEKTUR
IP NETZWERKE & IT-SICHERHEIT
COLLABORATION
DIGITALISIERUNG

SOFTWARE-ENTWICKLUNG
AUTOMATION & ORCHESTRIERUNG

IT-SYSTEME
ENTWICKLUNG & FERTIGUNG



www.dainox.net

SDMN®
SOFTWARE DEFINED
MISSION NETWORKING



AutOr®
AUTOMATION AND
ORCHESTRATION



dainBox®
MODULAR SERVICE
PLATFORM



Vertrauenswürdige Künstliche Intelligenz

Resümee zur Veranstaltung der Emerging Leaders AFCEA Bonn e.V. mit dem Cyber Innovation Hub der Bundeswehr und BITKOM am 12. Oktober 2023

Justus Groth, AFCEA Vorstand Emerging Leaders AFCEA Bonn e.V., IBM, mit Autorenteam: Paul Bauer, Matthias Klaus, Moritz Diederichsen, Andreas de Jonge



Justus Groth

Foto: privat

Was einst nach ferner Zukunft klang, ist heute aus unserem Alltag nicht mehr wegzudenken. Künstliche Intelligenz (KI) ruft neben Bewunderung auch Skepsis hervor, insbesondere im militärischen Anwendungsbereich. Dabei sind die Chancen und Möglichkeiten, die KI mit sich bringt, unverzichtbar, um unsere Sicherheit auch in Zukunft gewährleisten zu können. Um Licht ins Dunkel

zu bringen, haben sich daher die Emerging Leaders AFCEA Bonn e.V. gemeinsam mit Bitkom e. V. und dem Cyber Innovation Hub der Bundeswehr (CIHBW) im Rahmen eines Workshops unter dem Titel „Vertrauenswürdige Künstliche Intelligenz“ mit der Thematik der militärischen Anwendungsbereiche von KI auseinandergesetzt.

Wer entscheidet in Zukunft?

Es waren immer die Menschen, die die Entscheidungen getroffen haben. Dieser Umstand bedarf der Diskussion aufgrund neuer Möglichkeiten und Notwendigkeiten bezüglich des Zusammenspiels von „Mensch und Maschine“. Disruptive Technologien erfordern und ermöglichen zudem immer schnellere Reaktionszeiten. Auch der demografische Wandel trägt dazu bei, dass KI im militärischen Bereich zunehmend berücksichtigt werden muss. Grundvoraussetzung dabei ist das Vertrauen in diese Technologie. Anhand von drei Teilaspekten wurde das Konzept der vertrauenswürdigen KI vorgestellt und diskutiert.

Erklärbare KI

Im militärischen Kontext müssen Entscheidungen auf der Basis von immer mehr verfügbaren Informationen schnell und präzise getroffen werden. Hier liegen die Stärken der künstlichen Intelligenz, die in der Lage ist, große Datenmengen in kurzer Zeit zu verarbeiten und die relevanten Fakten darzustellen. Die KI kann hierbei deutlich schneller als menschliche Bearbeiter sein. Im militärischen Kontext sollen kritische Entscheidungen in Zukunft von Menschen getroffen werden. Die Frage ist jedoch, wie KI den Menschen dabei unterstützen kann und welche Entscheidungen aus-

gelagert werden können. Erklärbarkeit ist dabei eine wichtige Entscheidungsgrundlage.

Unsere Experten Torsten Fiolka, Florian Oßwald und Jan Roman Bartolosch vom Fraunhofer Institut für Kommunikation, Informationsverarbeitung und Ergonomie haben im Workshop dieses Konzept anhand eines Anwendungsbeispiels aus dem FCAS Ethical AI Demonstrator nähergebracht. Hier werden anhand von sogenannten Heatmaps, relevante Gegenstände oder Merkmale auf einem Bild hervorgehoben. So kann der Bearbeiter nachvollziehen, warum beispielsweise ein Objekt durch eine Bilderkennungssoftware als ein militärisches Ziel identifiziert wird. Erklärbarkeit ermöglicht zudem die Nachbesserung fehlerhafter Algorithmen und die Attribution von Verantwortung für die Folgen der KI-Nutzung. Ein besonderes Augenmerk lag während der Veranstaltung auf der ebenengerechten Erklärbarkeit. Ein Soldat im Spähfahrzeug benötigt eine andere Art der Erklärbarkeit als ein Auditor im Normalbetrieb.

Faire KI

Der in der deutschen Öffentlichkeit vorherrschende Eindruck von KI im Bereich militärischer Anwendungen besteht allzu oft aus Bildern von Killer-Robotern à la Terminator und könnte damit nicht weiter von der Realität entfernt sein. Umso wichtiger ist es, die öffentliche Debatte zu versachlichen. Mit Otto Obert von den Main DigitalEthikern haben wir in diesem Rahmen über die ethische Komponente von KI-Anwendungen gesprochen. Dabei wurde deutlich, dass die Anforderungen und Erwartungen



Paul Bauer

Foto: privat



Matthias Klaus

Foto: privat



Moritz Diederichsen Foto: privat

an KI deutlich höher sind als an menschliche Akteure. Werte wie Fairness und soziales Wohlergehen müssen daher bei der Entwicklung solcher Anwendungen berücksichtigt werden. Die Herausforderung besteht darin, diese Werte zu operationalisieren.

Die Leitlinien der NATO zum Umgang mit KI im militärischen Bereich können hierfür eine Grundlage bieten.

Auch wenn die Einbeziehung von Werten zunächst hinderlich erscheinen mag, ist eine langfristige Regulierung ein klarer Wettbewerbsvorteil auch für das Vertrauen in solche Anwendungen.

Robuste KI

Die Ukraine zeigt aktuell, welchen Einfluss KI auf die Kriegsführung von Streitkräften haben kann. Es zeigt sich, dass die Stärke der ukrainischen Streitkräfte im Informationsraum maßgeblich zu den Erfolgen der ukrainischen Truppen gegen die russischen Invasoren beiträgt. Der Erfolg von militärischem Handeln wird in Zukunft also auch in der Verlässlichkeit von KI-Anwendungen liegen, wie wir im dritten Themenkomplex beleuchteten.



Andreas de Jonge Foto: privat

Mit Oberstleutnant i.G Holger Prüßing vom Center for Intelligence and Security Studies (CISS) an der Universität der Bundeswehr in München haben wir daher über die notwendige Robustheit solcher Systeme gesprochen und diese anhand eines KI-gestützten sicherheitspolitischen Analyseprozesses diskutiert. Es entstand ein reger Austausch rund um die Frage, wie KI im militärischen Rahmen auch unter

widrigen Umständen zuverlässig und sicher funktionieren kann. Dazu gehören neben technischen auch prozessuale und rechtliche Aspekte, die in der Debatte zu berücksichtigen sind. Wie viele Daten werden benötigt für valide Informationen und welchen Einfluss hat das auf die Belastbarkeit der Ergebnisse? Welchen Grad an Fehler und Ungenauigkeit ist man bereit zu akzeptieren? Es wurde ersichtlich, dass es keine einfachen Antworten gibt und diverse Fragestellungen und Entwicklungen dazu beitragen können.



Veranstaltung der Emerging Leaders AFCEA Bonn e.V. am 12. Oktober 2023 / Die Veranstaltung fand gemeinsam mit dem CIHBW und BITKOM statt. Foto: Emerging Leaders AFCEA Bonn e.V.

Fazit

Das große Interesse an der Veranstaltung hat die Bedeutung des Themas unterstrichen. Wer in Zukunft einen Konflikt gewinnen will, wird auf den Einsatz von KI im militärischen Kontext angewiesen sein. Dafür müssen zunächst Irrtümer ausgeräumt und die Diskussion in der Öffentlichkeit versachlicht werden. Die Chancen und Möglichkeiten von KI-Anwendungen werden oft schlicht unterschätzt. Es liegt an den Beteiligten aus Bundeswehr, Industrie und Forschung, Wege zu finden, Werte zu operationalisieren und Vertrauen in künstliche Intelligenz durch erklärbare, faire und robuste Nutzung zu schaffen.



Großes Interesse an der ELA-Veranstaltung zu vertrauenswürdiger Künstlicher Intelligenz. Foto: Emerging Leaders AFCEA Bonn e.V.

Kriegsführung im Wandel – Auswirkung disruptiver Innovationen auf die Führungsunterstützung in der Dimension Land

Oberst i. G. Rainer Beeck, AFCEA Vorstand Bundeswehr, CDO Heer



Oberst i. G. Rainer Beeck

Foto: privat

„Die militärische Landschaft erfährt eine Zeitenwende durch den Einsatz disruptiver digitaler Lösungen, die die Resilienz gegenüber neuen Bedrohungen stärken. Die transformative Rolle dieser Technologien im militärischen Kontext darf nicht ignoriert werden. Der Schwerpunkt muss daher auf der Schaffung widerstandsfähiger Streitkräfte liegen, die flexibel auf sich entwickelnde Gefahren reagieren können.“

Als Chief Digital Officer Heer und Verantwortlicher für die Führungsunterstützung der Division 2025 bereitet mir dies schlaflose Nächte.

Warum? Weil dieser thematische Einstieg mit ChatGPT im Dezember 2023 innerhalb von ein paar Sekunden verfasst worden ist. Seit seiner Einführung im November 2022 stellt der Chatbot von OpenAI das Verständnis zur Automatisierbarkeit von Aufgaben, die vorher als nicht automatisierbar galten, in Frage. Bei ChatGPT liegen „Large Language Models“ zugrunde. Sie sind hier jedoch nur als ein kleiner Teil der disruptiven digitalen Lösungen zu sehen, die bestehende Strukturen zu einem Wandel herausfordern.

Der Begriff „Disruption“ beschreibt eine Veränderung, die relativ schnell oder in drastischer Weise eintritt. Disruption impliziert, dass der Wandel nicht von innen, sondern durch einen äußeren Stimulus hervorgerufen wird. Wir müssen uns daher nicht nur Gedanken um die zukünftige Rolle dieser Technologien machen, sondern zwangsläufig auch das eigene militärische Handeln an Disruption anpassen.

Das aktuelle Kriegsgeschehen in der Ukraine und in Israel/Gaza wird aus Sicht der NATO die Art der militärischen Operationsführung durch disruptive Technologien deutlich verändern. Diese technologischen Innovationen werden alle Aspekte des militärischen Handelns durchdringen und haben bereits jetzt schon einen großen Einfluss darauf.

Nachfolgend wird auf ausgewählte Aspekte näher eingegangen.

Künstliche Intelligenz

Die Entwicklung militärischer Strategien und Doktrinen erfährt zunehmende Disruption durch KI-gestützte Technologien. Bereits jetzt werden intelligente Systeme eingesetzt, um Strategen durch langfristige Vorhersagen und schnelle Analysen zu unterstützen.

Aktuelle Konfliktbilder und erkennbare Trends globaler Rüstung weisen darauf hin, dass sich die Operationsführung zukünftig stärker auf unbemannte Systeme und Automatisierung von Prozessen wird abstützen – von der KI-gestützten Bilderkennung über intelligente Feuerleitsysteme bis hin zur Etablierung kurzer Wirkketten. Das Gefechtsfeld der Zukunft ist absehbar (digital) gläsern, wodurch Einsatzumgebungen dynamischer werden und kritische Entscheidungen innerhalb von Sekunden getroffen werden müssen. Das allein wird durch analoge Methoden zur Lageführung nahezu unmöglich sein. Um eine künftige Entscheidungsfindung technisch zu unterstützen, werden von einem unübersichtlichen Schlachtfeld Live-Sensordaten, Bildübertragungen und eine enorm große Anzahl an Meldungen automatisiert zu aggregieren sein.



Panzergranadiere präsentieren das Zusammenwirken mit dem Roboterhund Wolfgang 001 beim Stab Test- und Versuchsverband Digitalisierung Landbasierter Operationen in Munster, am 05.07.2022.

Foto: Bundeswehr/Carl Schulze

Beispielsweise wird die enorme Datenmenge, darunter Millionen von Stunden an Drohnenaufnahmen, schneller erfasst, als menschliche Analysten sie auswerten können. Soldaten werden in zunehmendem Maße intelligente KI-fä-

hige Analyseinstrumente bei der Verarbeitung dieser Daten beaufsichtigen, überprüfen und unterstützen müssen. Mit der Unterstützung von Simulationstechniken können dann bestenfalls in einer Course of Action Analyse Handlungsvorschläge generiert werden.

Auch das Beherrschen des elektromagnetischen Spektrums bringt ähnliche Herausforderungen mit sich. Es gilt, große Frequenzbereiche effizient zu überwachen und mel-



Soldaten vom Jägerbataillon 413 nehmen an der Übung Griffin Lightning 2023 auf dem Truppenübungsplatz Pabrade/Litauen teil, am 02.03.2023.

Foto: Bundeswehr/Jana Neumann

dungsrelevante Nachrichten vor dem Hintergrund zahlreicher irrelevanter Signale mit hoher Zuverlässigkeit zu detektieren. Die automatisierte Verarbeitung von generierten Massendaten mittels moderner Methoden der KI ermöglicht eine schnelle und umfassende Auswertung. Gleichzeitig kann Fachpersonal gezielt und punktgenau für die Analyse eingesetzt werden.

Die Vorteile dieser Disruption liegen auf der Hand, sind jedoch mit Risiken verbunden, insbesondere aufgrund ihrer Anfälligkeit für Hackerangriffe oder für eine Störung der Kommunikationssysteme.

Quantencomputing

Quantentechnologien gelten in der NATO als eine „emerging disruptive technology“, sie sind also aufstrebend und gleichzeitig disruptiv. Die NATO stuft die Bedeutung der Quantencomputer bis 2050 als revolutionär ein.

Der Quantencomputer kommt und wird jede heute gängige und performante Verschlüsselung flächendeckend brechen. Die Frage lautet hier: Wann sind Quantencomputer leistungsfähig genug, sodass einfache Maßnahmen wie das Vergrößern von Schlüsseln nicht mehr greifen? Bis zu diesem Zeitpunkt müssen Maßnahmen zur Quantenresistenz ergriffen werden.

Quantentechnologie hat hierbei ein noch nicht zu ahnendes Fähigkeitspotential, was sich daraus entwickeln kann, ist heute noch nicht absehbar. Bereits heute werden daher zum Beispiel in großem Stil verschlüsselte Daten gesammelt, um sie bei Vorhandensein der Technologie entschlüsseln zu können.

Daraus folgt, dass Daten im Zeitalter performanter Quantencomputer noch mehr als heute das wichtigste Gut werden. Da konventionelle Verschlüsselungsalgorithmen absehbar nicht mehr das Mittel der Wahl sein können, wird es auf neue Ansätze wie z. B. zufälliger und dezentraler aber nachvollziehbarer und verfügbarer Daten ankommen. Neben der Kryptographie sind es die schnelleren Analyse- und Simulationsfähigkeiten und der damit entstehende Entscheidungsvorsprung, die sich disruptiv auf militärische Operationen auswirken können.

Train while you fight

Moderne Ausbildungstechniken sind im Kriegsfall extrem wichtig, da Ausbildung weiter stattfinden muss. Im Sinne eines „Train while you fight“ – trainiere während du kämpfst – bieten disruptive Technologien Möglichkeiten zur Fortsetzung der Ausbildung im Kriegsfall.

Neue Anwendungen und Formate können maßgeschneiderte Lernerfahrungen bieten, in denen die Unterrichtsinhalte an den Fortschritt des Lernenden automatisch angepasst werden. Die Zeit- und Ortsunabhängigkeit beim Zugriff auf die Lerninhalte ist hier ein wichtiger Faktor, um Ausbildung modern zu gestalten.

Nicht nur die Ausbildung, sondern auch die Ausbildungsfähigkeit muss betrachtet werden. Voraussetzungen hierfür sind eine abgesicherte Lerninfrastruktur, einfacher Zugang zu den Lernmaterialien und die ernsthafte Klärung, welche Daten im Kriegsfall tatsächlich schützenswert sind.

Was lernen wir aus der Ukraine?

Seit Beginn des Konflikts hat Russland entlang der über 1.000 km verlaufenden Frontlinie Stellungssysteme ausgehoben und errichtet. Der Stellungskrieg ähnelt den Kampfhandlungen des Ersten Weltkriegs. Gleichzeitig kommt es zum massiven Einsatz von Drohnen.

Mit ihnen besteht die Möglichkeit der Echtzeitaufklärung ohne eigene Kräfte zu gefährden, grundlegende Lageinformationen zu gewinnen, Zieldaten zu generieren und zu übermitteln sowie Wirkmittel in kurzer zeitlicher Abfolge einsetzen zu können. Die „Dritte Dimension“ wird durch Drohrentechnologie für immer mehr Akteure einfach zugänglich. Dies wird sich disruptiv auf die Gefechts-handlungen aus. Was im Krieg Erfolg hat, ändert sich beständig. Ganz dem „Train while you fight“ Paradigma entsprechend setzen die ukrainischen Streitkräfte moderne Ausbildungstechniken ein, um schnell und wirksam Ausbildungsinhalte zu vermitteln.

Hier existieren gleichzeitig archaische Kriegsbilder des letzten Jahrhunderts neben den hochdigitalen und insbesondere auf ukrainischer Seite sehr schnell adaptionsfähigen Aufklärungs- und Wirkungsmöglichkeiten. Gleichwohl unterscheiden sich die Herausforderungen des täglichen Lebens an den einzelnen Soldaten (Hygiene, Kälte, Wasser, Ratten und Ungeziefer, Tod) kaum von denen Ihrer Großväter und Urgroßväter, sie finden allerdings unter erweiterten Bedrohungen statt und können in Echtzeit in Sozialen Medien gepostet werden.

Was bedeutet das für uns?

Zusammenfassend ist festzustellen, dass den Aspekten Anpassungsgeschwindigkeit und Agilität wie auch Mut zur Innovation bei der erfolgreichen Bewältigung disruptiver digitaler Entwicklungen die zentrale Bedeutung zukommt. Regelprozesse werden im Gefecht nicht erfolgversprechend, da zu langsam, sein. Die Verschränkung von Rüstungsindustrie mit Start Ups genauso wie Forschung mit den Streitkräften in gegenseitigem Vertrauen und mit dem gleichen Ziel ist aus meiner Sicht ein wichtiger Ansatz zur Lösung der vor uns liegenden Herausforderungen. Wenn ich mir also als einen ersten Schritt etwas wünschen dürfte, wäre mein Wunsch, dass es möglich wäre, in der Domäne IT Beschaffungsvorhaben außerhalb des Customer Product Management novelliert (CPM nov.) zu beschaffen. In Erweiterung des Zitats von Generalleutnant Michael Vetter, dem Abteilungsleiter BMVG CiT „Wer nicht digitalisiert – verliert“ gilt: „Wer bei disruptiven digitalen Veränderungen nicht in der Lage ist, schnell zu digitalisieren, verliert schnell“ und wir in Deutschland müssen schneller werden.

Quellen:

„Disruption durch Technologien – Auswirkungen auf Politik, Wirtschaft und Gesellschaft“, Wissenschaftlicher Dienst des Europäischen Parlaments, September 2020

„Aus dem Einsatz lernen“, KdoH G7 AuswEval, 2023

„Smart & Digital Bundeswehr“, Konferenzbroschüre IT-Konferenz 2022, Oktober 2022

„Quantum Jahresbericht 2020/2021“, Fraunhofer IAF, 2021

„Kryptografie quantensicher gestalten“, Bundesamt für Sicherheit in der Informationstechnik, Oktober 2021

„Thema der Zukunftsentwicklung: Quantentechnologie – Erste Lagefeststellung und Bewertung der Potenziale für das Handlungs- und Leistungsvermögen sowie die Fähigkeitsentwicklung der Bundeswehr“, PlgABw Abt I, März 2022

„FKIE Forschungsbericht 2022/23“, Fraunhofer FKIE, 2023

Robuste Lösungen für einsatzkritische Anwendungen



High-Density Server



Lüfterlos



Mobil



Missionscomputer



Embedded PC mit Touchscreen

Sicherheitsarchitektur im Wandel – Die Bedeutung fortschrittlicher Beschaffungsstrategien

Christian Rösch, Schriftführer AFCEA Bonn e.V., Senior Sales Manager Eviden



Christian Rösch

Foto: privat

Bestehende und neue Technologien entwickeln sich in zunehmendem Tempo. Die Beschaffungsprozesse auf Seiten der „Guten“ müssen Schritt halten, da wir uns keine Lücken in unserer Sicherheitsarchitektur leisten können.

Wir erleben derzeit eine neue Realität, die eine schnellere Reaktion auf Veränderungen erfordert als in der Vergangenheit.

Die Bewältigung kurzfristiger Krisen erfordert rasche, qualitativ hochwertige Entscheidungen sowie neue Fähigkeiten für Gegenmaßnahmen. Eine entscheidende Rolle dabei spielt Software. Die digitale Befähigung und Vernetzung von Systemen sind für die Steigerung der Leistungsfähigkeit der Bundeswehr von entscheidender Bedeutung. Es gilt durch disruptive digitale Lösungen eine höhere Resilienz zu erlangen.

Betrachten wir die Digitalisierung in der Kriegsführung. Kampfwertsteigerungen erfolgen zunehmend innerhalb der Kill-Chain oder des Kill-Webs in einem transparenten Gefechtsfeld. Unterschiedliche automatisierte Sensoren und Effektoren sowie KI-basierte Analytik mit widerstandsfähiger Kommunikation sind unerlässlich. Aktuelle Konflikte, nicht nur auf dem europäischen Kontinent, zeigen die enorme Beschleunigung von Entwicklungs- und Innovationszyklen vom Bedarf bis zur Umsetzung im Einsatz. Sind die

Prozesse einer historisch hardwarezentrierten Beschaffung für eine softwareorientierte Beschaffung geeignet?

Beschaffung bedeutet „in time, in quality und in budget“, also die zeitgerechte Verfügbarkeit angemessener Mittel weit über „State of the Art“ hinaus. Technologiezyklen vorhersehen und die Zukunftstechnik heute schon nutzen, sind entscheidend. Nur so können Konflikte gewonnen werden. Mit nichts Geringerem als diesem Anspruch an uns und unser Gesellschaftssystem können wir unsere Soldaten in Einsätze schicken.



Auch Startups sollten stärker in der Beschaffung betrachtet werden.

Foto: AFCEA Bonn e.V.



Beschaffung bedeutet „in time, in quality und in budget“ und dabei auch Zukunftstechnik zu nutzen. Nur so können Konflikte gewonnen werden.

Foto: getty Image

Die Beschaffung rückt weiter ins strategische Zentrum der Verteidigung. Sie ist ein elementarer Bestandteil bei der Schaffung von Wirkungsüberlegenheit und somit bei der Verteidigungsbereitschaft für unser Land und unser Bündnis.

Deutschland kann sich heute keine Kompromisse bei der Versorgung seiner Sicherheitsorganisationen erlauben. Die behördlichen Anforderungen und Prozesse in der Beschaffung müssen in Bezug auf Beschaffungszeit und -volumen Kongruenz aufweisen. Dies bezieht sich sowohl auf allgemeine Technologie- und Innovationszyklen als auch auf die Geschwindigkeit und das Volumen, das aggressive Regime und kriminelle Organisationen vorlegen. Hier dürfen wir keine Abweichungen mehr akzeptieren.

Wenn wir unser Sicherheitspersonal ernst nehmen, benötigen wir die besten Ideen, erstklassige Strategen, technische und operative Konzeptarbeiter sowie ambitionierte und mutige Umsetzer aus Behörden, Industrie und Nutzerkreisen. Das kann nur eine Beschaffung leisten, die schon in Friedenszeiten effektiv im Sinne von Landes- und Bündnisverteidigung agiert.

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 neuesten 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 15.000 Mitarbeitende. 2023 lag der Umsatz bei rund 6,4 Mrd. €.

Kontakt:

Bechtle AG

Gabor Jeszenoei

Zentrales Team Bundeswehr

Telefon: 0228 6888 400

Email: zpls-r1753@bechtle.com

Web: www.bechtle.com



AFCEA Fachausstellung 2024 am 26./27. Juni 2024 – Die IT-Fachmesse der Sicherheitsorganisationen und -firmen

Oberst a.D. Wolfgang Quirin, Leiter AFCEA Fachausstellung



Wolfgang Quirin, Oberst a.D.

Foto: privat

Mit dem Thema „Zeitenwende in der nationalen Sicherheit – Resilienz durch disruptive digitale Lösungen“ greift die diesjährige AFCEA Fachausstellung die Erfordernisse einer sich sehr schnell wandelnden Weltlage und die damit verbundenen geänderten Sicherheitsstrategien mit neuen operativen Notwendigkeiten auf.

Eine abgestimmte Zusammenarbeit zwischen Regierung, Industrie, For-

schung und Bildungseinrichtungen ist 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 vierte AFCEA Fachausstellung im World Conference Center Bonn (WCCB) wieder die öffentliche Hand mit ihren Behörden- und Organisationen mit Sicherheitsaufgaben, Industrie, Forschung und Bildungseinrichtungen zusammen.

Die Teilnahme an der 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 und 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 dritte AFCEA Fachausstellung im World Conference Center im Mai 2023 zeigte allein durch die Zahl der Aussteller (ca. 250) und der über 4.500 Teilnehmer wieder das überwältigende Interesse an dieser Veranstaltung. Das lag sicher auch am neuen, erweiterten Format der dritten AFCEA Fachausstellung, das aufgrund der guten Resonanz

bei der AFCEA Fachausstellung 2024 beibehalten wird.

Die AFCEA Fachausstellung 2024 enthält neue, traditionelle und bekannte Elemente:

- Ausstellung auf den sieben Ausstellungsflächen:
 1. FOYER EINGANGSEBENE
 2. FOYER Galerie
 3. SAAL WIEN
 4. SAAL NEW YORK/GENF
 5. RHEINEBENE
 6. SAAL BANGKOK
 7. AUSSENBEREICH
- Ein Symposium zu aktuellen militärpolitischen Brennpunktt Themen
- Ein Get-together am Mittwohabend von 18.00h – 22.00h auf der Ausstellungsfläche RHEINEBENE
- Inhaltlich-methodischer Workshop am Tag vor der Fachausstellung, bei dem mit Teilnehmenden aus dem Bundeswehrumfeld zu Themen wie der Innovation von Beschaffung diskutiert wird
- DigitalDefenceDebate/Podiumsdiskussion mit ranghohen Teilnehmern (im Rahmen des Symposiums am Donnerstagvormittag)
- 2 parallele Panels von kurzen Industrievorträgen der Aussteller (Speaker Corner) in 31 Vortragsslots, ferner auch die Präsentation von Startups (Pitch Session) durch die Emerging Leaders AFCEA Bonn e.V.
- Eine 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

Als „Pre-Opening“ der Fachausstellung wird am 25. Juni 2024 ein Innovationsworkshop stattfinden, in dem Vertreter der Emerging Leaders Bonn mit Teilnehmenden aus dem Bundeswehrumfeld aktuelle Herausforderungen diskutieren werden.

Mit der Schaffung der #DigitalDefenseDebate haben die Emerging Leaders AFCEA Bonn eine besondere Chance für den Verein AFCEA Bonn e.V. gesehen. So werden auch Personen angesprochen, die bisher eher selten in der „Verteidigungsbubble“ anzutreffen sind, beispielsweise Vertreter*innen aus Startups, VCs und junge Sicherheitspolitiker*innen. Dieses virtuelle Format setzt die richtigen Impulse und ist

somit geeignet, auch dieses Jahr auf der Bühne der Fachausstellung seinen Platz einzunehmen.

Mit der Einführung der Industrievorträge ging ein langgehegter Wunsch der Aussteller in Erfüllung. Erstmals in diesem Jahr wird ein Speakers' Corner im Plenarsaal des WCCB eingerichtet. In diesem sehr prominenten Raum werden 18 Speakerslots zur Auswahl stehen. Die 2. Speakers' Corner wird wieder im Raum Addis Abeba 3 mit insgesamt 13 Speakerslots sein.



Das World Conference Center Bonn in Eigendarstellung

Foto: WCCB

Beide Speakers' Corners sind ausschließlich über die Rheinebene erreichbar.

Für Aussteller, die einen Speakerslot gebucht haben, besteht die Möglichkeit, im Rahmen dieses Formats in einem Kurzvortrag von 20 bis 25 min auf die Produkte oder Dienstleistungen ihres Unternehmens hinzuweisen. Die Abstracts zu den Vorträgen sind außerdem auf der AFCEA Homepage einzusehen.

Die gedruckte „Broschüre Industrievorträge“ finden die Besucher AFCEA Fachausstellung 2024 am Eingang sowie am Eingang zu den beiden Speakers' Corners. Selbstverständlich wird die Broschüre auch digital als pdf zum Download bereitgestellt.

Damit junge Startups für kleines Geld „AFCEA-Fachausstel-

lungs-Luft“ schnuppern, die Vernetzungsmöglichkeiten der AFCEA Fachausstellung ausschöpfen und ihre innovativen Produkte vorstellen können, haben unsere Emerging Leader eine „Sonderausstellungsfläche für Startups“ eingerichtet. Die ausgewählten jungen Unternehmen dürfen ihre innovativen Konzepte, Produkte und Dienstleistungen den Besuchern darstellen. Zudem wird eine Startup-Pitch Session durchgeführt. Gleichzeitig werden diese jungen Unternehmen in der eKompetenzmatrix mit Kompetenzen und Firmenprofil und im AFCEA Heft genauso beworben wie die anderen Aussteller.

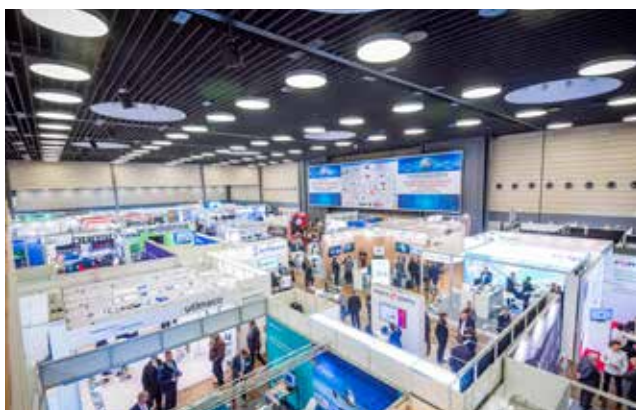
Auch einer der größten Herausforderung der heutigen Zeit – dem Fachkräftemangel – nimmt sich die Fachausstellung wieder an. Gemeinsam mit dem Berufsförderungsdienst der Bundeswehr werden im Rahmen des neuen Recruiting-Elements, AFCEA-Mitgliedsfirmen und die Aussteller der Fachausstellung offene Stellen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

Auch bei der AFCEA Fachausstellung 2024 steht zur besseren Orientierung der Besucher über die vielfältigen Angebote der Aussteller wieder die datenbankbasierte, komfortable Webanwendung „eKompetenzmatrix“ von unserer AFCEA-Mitgliedsfirma CGI zur Verfügung. Bei mehr als 200



Verabschiedet: Mit der Fachausstellung 2023 hat der langjährige Ausstellungsleiter Friedrich W. Benz (im Bild) die Leitung an Wolfgang Quirin übergeben.

Foto: AFCEA Bonn e.V.



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

Foto: AFCEA Bonn e.V.

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, in 15 „Oberkategorien“ gruppierten, Kompetenzen diejenigen auswählen, die sie besonders interessieren, worauf die eKompetenzmatrix dann exakt diejenigen Aussteller anzeigt, bei denen die Besucher zu dem gewählten Thema und Kompetenz fündig werden.

Bei der vergangenen AFCEA Fachausstellung – insbesondere beim Get-together am Mittwochabend – war bei allen Beteiligten – Ausstellern und Besuchern – mehr als deutlich

erkennbar, dass sie es wohltuend empfanden, endlich wieder an einer Ausstellung und an einem Get-together teilnehmen zu können. Der Gesprächsbedarf war so groß, sodass wir das Get-together von 18 bis 22 Uhr einplanen.

AFCEA Bonn e. V. – als neutrale Plattform zwischen Industrie, Streitkräften und BOS – bietet mit der AFCEA Fachausstellung als Treffpunkt der IT-Community Bundeswehr und BOS im WCCB weiterhin die gewohnt informative Plattform für „IT zum Anfassen“.

Wir freuen uns, sie zur AFCEA Fachausstellung 2024 am 26. und 27. Juni 2024 im World Conference Center Bonn willkommen zu heißen.

Software Defined Defense Gewappnet für die Verteidigung der Zukunft



Interoperabilität

Vernetzung von Bestandssystemen und Neuentwicklungen durch gemeinsame Architektur als Fundament.



Automation

Effiziente Ressourcennutzung durch intelligente Verteilung und Automatisierung wiederkehrender Sicherheitsaufgaben.



Wirkungsüberlegenheit

Offene Architekturen und vertrauensvolle KI-Integration ermöglichen eine proaktive Vorbereitung und dynamische Reaktionen auf Angriffe.



Besuchen Sie uns an unserem Stand F 02 (im Foyer)
oder erleben Sie die Verteidigung der Zukunft auf

software-defined-defense.de





Bundesamt für Ausrüstung, Informationstechnik
und Nutzung der Bundeswehr



Einladung zur Koblenzer IT-Tagung 2024 am 24. Oktober 2024

„Zeitenwende in der nationalen Sicherheit – Resilienz durch disruptive digitale Lösungen“

Als Jahresthema 2023 hat AFCEA Bonn e.V. "(Künstliche) Intelligenz und Innovation – Konkrete Nutzungsmöglichkeiten" gewählt und auch im Rahmen der Koblenzer IT-Tagung 2023 diskutiert, welchen Einfluss KI auf das IT-System der Bundeswehr sowie auf andere Behörden hat. Zukunftstechnologien, wie KI, wirken in immer schnelleren Schritten auf unseren Staat, unsere Arbeitswelt und insgesamt unser ganzes Leben. Mit Hilfe der Digitalisierungsplattform hat die Bundeswehr eine Struktur geschaffen, die ihr hilft, technologische Innovationen zu „organisieren und realisieren“, um für die Bereiche Verteidigung und Sicherheit deren Möglichkeiten und Chancen zu identifizieren, gleichzeitig aber auch Risiken und Gefahren zu minimieren.

Die Koblenzer IT-Tagung 2024 wird sich dem AFCEA Jahresthema „Zeitenwende in der nationalen Sicherheit – Resilienz durch disruptive digitale Lösungen“ widmen. In drei Blöcken werden ein Zwischenfazit zur Digitalisierungsplattform gezogen, das Thema Cyber Security im Kontext Resilienz beleuchtet und in Fortsetzung des 2023 erstmals durchgeführten Innovationsraums neue Technologien durch Amtsseite, Wissenschaft, Forschung und Industrie in diversen Stationen mit kurzen Workshops, Vorführungen oder Produktdemos (an-)fassbar gemacht. Bei allen drei Blöcken soll dabei der Schwerpunkt auf disruptiven digitalen Lösungen liegen, so dass am Ende ein Beitrag zur Beantwortung der Fragen:

„Können wir disruptive digitale Lösungen?“ – „Welche Bedeutung haben sie gerade im Bereich der Cyber Security und Resilienz?“ – „Was gibt es schon bzw. was dürfen wir absehbar erwarten?“

geleistet wird.

Vor der Mittagspause wollen wir die Gelegenheit nutzen, die Gewinner des Studienpreises AFCEA Bonn e.V. 2024 auszuzeichnen. Den Abschluss der Tagung bildet dann in alter Tradition ein Vortrag „Out of the Box“.

Organisatorische Hinweise

Ort: Rhein-Mosel-Halle, Julius-Wegeler-Straße 4, 56068 Koblenz

Datum/Zeit: Donnerstag, 24.10.2024 08:45 – 18:15 (Einlass 08:00 Uhr)
Get-Together „Koblenzer Abend“ 18:30 – 21:00

Teilnehmer:

Bundesministerien, Kommandobehörden, Ämter, Dienststellen und Truppenteile der Bundeswehr, Behörden und Organisationen mit Sicherheitsaufgaben (BOS), Institute, Verbände, Universitäten und Hochschulen, Industrie mit Schwerpunkt Informations- und Kommunikationstechnik, internationale Gäste.

Fachliche Leitung: Brigadegeneral Dr. Volker Pötzsch, Abteilungsleiter Informationstechnik BAAINBW
Brigadegeneral Armin Fleischmann, Vorsitzender AFCEA Bonn e.V.

Moderation: Nils Merkle, AFCEA Bonn e.V.

Programm: Das Programm wird zeitnah unter www.afcea.de und www.baainbw.de veröffentlicht.

Kostenbeiträge: + Tagungspauschale: 90,- €
+ Tagungspauschale für Öffentlichen Dienst und AFCEA-Mitglieder: 40,-€
+ Teilnahme am Koblenzer Abend: 35,-€ zusätzlich

REALISE MORE TO PREVENT THREATS AHEAD OF TIME

BESUCHEN
SIE UNS AUF DER
AFCEA 2024:
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

Antworten auf die Zeitenwende – Die BWI und das Zielbild 2028

Dr. Christian Marwitz, Chief Digital Officer, Mitglied der Geschäftsführung, BWI GmbH



Dr. Christian Marwitz

Foto: BWI GmbH/Xandra Herdieckerhoff

Der russische Angriffskrieg auf die Ukraine veränderte nicht nur die sicherheitspolitische Lage in Europa, er markiert auch einen historischen Einschnitt in unser eigenes Sicherheitsdenken. Bundeskanzler Olaf Scholz sprach von einer „Zeitenwende“, nach der die Welt „nicht mehr dieselbe“ sein würde wie zuvor. Das Sondervermögen Bundeswehr in Höhe von 100 Milliarden Euro zeugt ebenfalls von einer tiefgreifenden

Veränderung der europäischen Sicherheitsordnung. Die neue Sicherheitslage gibt den Takt vor, an dem wir uns heute orientieren und auf das wir künftig unser Handeln ausrichten werden und müssen. Und natürlich haben die Zeitenwende und das damit einhergehende Sondervermögen auch Auswirkungen auf die Leistungserbringung der BWI GmbH. Die vergangenen drei Jahrzehnte nach dem Ende der Ost-West-Konfrontation waren lange Zeit von dem Glauben geprägt, dass es in Europa keine größeren landgestützten Kriege mehr geben würde. Die Landes- und Bündnisverteidigung rückte aus dem Fokus. Stattdessen lag er auf der Terrorismusbekämpfung und zeitlich und personell begrenzten Auslandseinsätzen. Dieses Bild bekam 2014 mit dem Krieg in der Ostukraine erste Risse. Die russische Invasion im Jahr 2022 hat schließlich gezeigt, dass wir uns im Rahmen der künftigen Herausforderungen auch intensiv auf die Landes- und Bündnisverteidigung (LV/BV) vorbereiten müssen. Dafür brauchen wir eine einsatzbereite und kriegstüchtige Bundeswehr. Und das bedeutet auch wegweisende Veränderungen für die strategischen Partner, die der Truppe dabei zur Seite stehen.

Landes- und Bündnisverteidigung rückt in den Fokus

Für uns als BWI haben sich die Anforderungen seitens der Bundeswehr in den vergangenen zwei Jahren verändert. Die BWI und unsere Leistungserbringung müssen noch resilienter aufgestellt werden. Praktisch heißt dies, dass wir auftretenden Belastungen von außen widerstandsfähiger entgegentreten können, ohne dabei unseren Fokus zu verlieren. Das betrifft sowohl die Organisation selbst als auch jeden einzelnen. Die Landes- und Bündnisverteidigung rückt dabei wieder in den Mittelpunkt unserer Arbeit. Und damit verbunden sind eine ganze Reihe von Handlungsfeldern, die wir identifiziert

haben. In unserem Integrationsprojekt LV/BV wurden diese Felder bereits auf die neuen Herausforderungen angepasst und in den erneuerten strategischen Ansatz implementiert. Ferner bedeutet die Zeitenwende für uns auch, dass wir uns auf den Kunden Bundeswehr konzentrieren. Die BWI ist und bleibt der primäre Digitalisierungspartner der Bundeswehr! Durch den Ukraine-Krieg und den Fokus auf die Landes- und Bündnisverteidigung haben sich deren Bedürfnisse natürlich verändert. Für uns bedeutet das, dass es einen größeren Bedarf an IT-Lösungen gibt – und diese in kürzeren Intervallen bereitgestellt und aktualisiert werden müssen.

Resilienz durch Software-gestützte Lösungen

Generell hat die Bedeutung von IT-Lösungen im militärischen Bereich zugenommen. Auch das hat uns nicht zuletzt der Verlauf des Krieges in der Ukraine gezeigt. Der schnelle Aufbau einer belastbaren IT-Infrastruktur hat der ukrainischen Armee in den ersten Kriegswochen entscheidend dabei geholfen, den Vormarsch der russischen Armee zu stoppen. Die Übermittlung militärischer Daten mittels Satellitenverbindungen oder die Nutzung des vorhandenen Expertenwissens in der Drohnentechnologie haben außerdem dafür gesorgt, dass die ukrainischen Streitkräfte wichtige Fähigkeiten hinzugewonnen haben und vorhandene Nachteile ausgleichen konnten.

Zudem haben Software-gestützte Lösungen dazu beigetragen, die Verteidigung des Landes resilienter zu gestalten. Den sich ständig verändernden Herausforderungen auf dem Gefechtsfeld tritt die ukrainische Armee mit innovativen Lösungen entgegen. So ist es einem Land, das selbst über keine nennenswerten Seestreitkräfte verfügt, binnen zwei Jahren gelungen, die russische Schwarzmeerflotte aus dem Kriegsgeschehen zurückzudrängen und entscheidend zu schwächen.

Unter der Dringlichkeit eines erlittenen Angriffskrieges arbeiten die Akteure im ukrainischen Verteidigungssektor agil und flexibel. Sie denken und handeln in Innovationsrhythmen, die jenen aus der Start-up-Welt nicht unähnlich sind und die es dem Militär ermöglichen, die Geschwindigkeit, mit denen digitale Innovationen erschaffen werden, für das Gefechtsfeld nutzbar zu machen. Auch wir können als Gesellschaft, als Bundeswehr aber auch als BWI davon lernen. Die ausgerufenen Zeitenwende und das Sondervermögen werden uns nicht zum Erfolg führen, wenn wir unser Denken nicht verändern. Die Ukraine hat gezeigt, wie man mit 80-Prozent-Lösungen oder am Markt verfügbaren Produkten schnell produktiv werden kann. Die Zeiten von Goldrandlösungen sind vorbei.

Das Zielbild 2028

Wir als Gesellschaft können aus dem Ukraine-Krieg Vieles lernen. Für uns in Deutschland heißt das vor allem erst einmal, dass wir den „Sense of Urgency“ erkennen, der diesem Moment innewohnt. Wir als BWI haben diesen Gedanken in unserem „Zielbild 2028“ ausdefiniert. Das Zielbild 2028 beschreibt den Anspruch an uns selbst, den wir aufgrund der veränderten sicherheitspolitischen Lage neu definiert haben. Unsere Leitlinie ist dabei klar: Die BWI ist der primäre Digitalisierungspartner der Bundeswehr in Frieden, Krise und Krieg. Wir stehen an der Seite der Bundeswehr und sorgen dafür, dass die Truppe in jedweder Situation die nötigen Fähigkeiten bekommt, um den Herausforderungen dieser Zeit entgegen zu können. Wir tragen auf diese Weise zur kontinuierlichen Erhöhung der Führungs- und Einsatzfähigkeit der Streitkräfte bei.

Services und Leistungen immer und zu jeder Zeit

Unser Anspruch ist es dabei, die benötigten Services und Leistungen immer und zu jeder Zeit zu erbringen. Die Sicherheitslage garantiert keine Pausen und Ruhephasen. Und so wie die Bundeswehr stets bereit sein muss, die Landes- und Bündnisverteidigung zu garantieren, so müssen wir auch stets bereit dafür sein, der Bundeswehr dabei zur Seite zu stehen.

Um unser Ziel zu erreichen, stellen wir einen stabilen, sicheren und effizienten Betrieb der beauftragten, insbesondere auch einsatznahen IT Services, im In- und Ausland, sicher und gewährleisten die umfassende IT- und Datensicherheit des IT-Systems der Bundeswehr.

Wir sind innovativ, beraten kompetent und stellen mit unseren clusterorientierten Programm- und Projektleistungen die zügige Bereitstellung neuer IT- Lösungen für die Streitkräfte auch unter Nutzung agiler, nutzerorientierter Methoden sicher. Nicht zuletzt optimieren wir unsere Leistungserbringung durch einen Mix von eigenem und Markt-Know-how. Wir pflegen ein auf Resilienz ausgerichtetes Partner-Ökosystem. Und wir sind berufliche Heimat für Menschen, die unseren Purpose verinnerlicht haben und ihren Teil dazu beitragen wollen, die Führungs- und Einsatzfähigkeit der Bundeswehr zu erhöhen.

Umsetzung in der Praxis

Grundlegend setzen wir dies natürlich bereits um: Etwa durch den Aufbau und Betrieb der pCloudBw, mit der die qualitätsgesicherte Bereitstellung von IT-Lösungen gewährleistet wird. Oder durch das German Mission Network zur Harmonisierung und serviceorientierten Ausrichtung der Führungsinformationssysteme in der Bundeswehr. Auch die Erhebung und Auswertung von Daten spielt in Zukunft eine immer stärkere Rolle – hier sind wir mit einer Vielzahl von Projekten engagiert. Das gilt auch für die Vernetzung militärischer Kräfte und Systeme. Und unsere Partner-Ökosysteme helfen uns dabei, resilient für die Herausforderungen der Zukunft zu werden. Mehr dazu und zu vielen anderen Themen können Sie in den Geschichten erfahren, die wir für dieses Heft vorbereitet haben.

Im Februar 2022 war die „Zeitenwende“ vor allem etwas, das mit einem Prozess des sicherheitspolitischen Umdenkens zu tun hatte. Heute, mehr als zwei Jahre später, geht es vor allem um das Handeln. Mit dem Zielbild 2028 leistet die BWI ihren Beitrag dazu, dass die Zeitenwende Gestalt bekommt.



Software Defined & Connected Defense

Softwarebasierte und agile Fähigkeitsprofile

Digital Continuity

Effizientere Beschaffung und Nutzung durch digitale Zwillinge und mehr

Smart Administration

Nutzer- und zielorientierte Verwaltungsprozesse durch Ende-zu-Ende-Digitalisierung

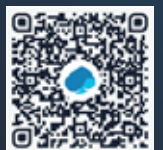
Cloud Transformation

Skalierbare und resiliente Infrastrukturen durch souveräne Multi-Cloud-Orchestrierung

Wir freuen uns auf den Austausch!

AFCEA 2024
Stand N02 | Saal Nairobi

Mehr erfahren:



Capgemini

Verteidigung braucht *Resilienzwirtschaft.*

Wir müssen im Rahmen der politischen *Zeitenwende* zur Vermeidung eines Verteidigungsfalles einen Grad an gesamtgesellschaftlicher und wirtschaftlicher Resilienz erreichen, der gegenüber jedem möglichen Aggressor eine umfassende Abschreckung glaubhaft vermittelt.

Durch Informations- und Führungsüberlegenheit zur Wirkungsüberlegenheit – Anforderungen moderner Streitkräfte

Vizeadmiral Dr. Thomas Daum, Inspekteur Cyber- und Informationsraum



Vizeadmiral Dr. Thomas Daum

Foto: PIZ CIR/IJ

„Wer nicht digitalisiert, verliert“, pflegt Generalleutnant Michael Vetter, Abteilungsleiter CIT im BMVg regelmäßig zu sagen. Claudia Plattner, Präsidentin des Bundesamtes für Sicherheit in der Informationstechnik (BSI), fordert: „Wir müssen Deutschland zur Cybernation machen.“ Die beiden Aussagen unterstreichen die Bedeutung der digitalen Revolution für unsere Gesellschaft.

Dies gilt auch für uns als Streitkräfte. Sie sind ein Teil der staatlichen Verwaltung. Und der digitale Wandel birgt neue Gefahren und Angriffsmöglichkeiten gegen unsere Sicherheit und Freiheit. Neben die traditionellen Gefechtsfelder ist ein digitales Gefechtsfeld getreten. Ich formuliere das regelmäßig so: „Wenn der Panzer – bei aller Kampfkraft – nicht auch zum Netzwerknoten auf dem digitalisierten Gefechtsfeld wird, wird er in der Gefechtssituation kaum überleben können.“ Der aktuelle Konflikt in der Ukraine findet auch und insbesondere im Cyber- und im Informationsraum statt.

Die Bedeutung von Informationen in der militärischen Wirkkette

Es war zu beobachten, wie Russland bereits in Vorbereitung des Angriffskrieges gegen die Ukraine im Februar 2022 mit Cyberangriffen und Desinformationskampagnen die Unsicherheit, Unzufriedenheit und auch die Angst der ukrainischen Bevölkerung zu schüren suchte. Solche Aktivitäten zeigen sich nach Ausbruch der Kriegshandlung in unterschiedlicher Intensität auf beiden Seiten.

Informationen sind in diesem Krieg auch für die militärische „Wirkkette“, die „Kill Chain“, von entscheidender Bedeutung. Informationen über den Gegner sind das wesentliche Ziel der Aufklärung auf beiden Seiten. Ziel- und Lagedaten müssen in großem Umfang ermittelt und für das Gefecht aufbereitet werden, der Faktor Zeit spielt dabei eine erhebliche Rolle. „Wer schneller schießt und besser trifft, bleibt Sieger im Gefecht“. Dieser Satz bestätigt sich auch in der Ukraine.

Schlüsselfaktor Geoinformationen

Elektronische Kampfführung (EloKA) wird auf beiden Seiten genutzt. Auf russischer Seite, die offenbar mit starken Störern die Aufklärung des Gegners behindert, können so Vorteile erreicht werden. Geoinformationen sind ein Schlüsselfaktor. Das Nutzen veralteter Landkarten soll vielen russischen Fallschirmjägern das Leben gekostet haben, die nachts über Waldgebieten abgesprungen sind.

Auch beim Konflikt im Nahen Osten ist das Ringen um die Deutungshoheit und die Narrative erkennbar, Desinformation spielt eine Rolle bei beiden Konfliktparteien.

Drei Faktoren für die Kriegsführung im 21. Jahrhundert

Für die Ausrichtung der deutschen Streitkräfte ist die aufgezeigte militärische Relevanz des CIR zu berücksichtigen, auch die gestiegene Bedeutung des Drohnenkrieges ist zu beachten. Drei Faktoren für die Kriegsführung im 21. Jahrhundert will ich hier ableiten:

Faktor Zeit: Durch moderne Aufklärungs- und Kommunikationstechnik lassen sich Daten in gesteigertem Umfang erheben, auswerten und verteilen. Das gläserne Gefechtsfeld ist Realität. Mehr Aufklärungssensoren verfügbar zu haben und deren gewaltige Datenmengen schneller und akkurater zu operativ nutzbaren Lagebildern aggregieren zu können als der Gegner führt zur Informationsüberlegenheit. Auf Grundlage dieses umfassenden, gemeinsamen und aktuellen Lagebildes Entscheidungen zur Durchführung militärischer Operationen schneller zu treffen als der Gegner führt zur Führungsüberlegenheit. Die eigene Operations- und Gefechtsführung sodann gesichert und geschützt gegen fremden Zugriff und Manipulation an die eigene Truppe – die Effektoren – zu übermitteln und damit am „scharfen Ende“ der Wirkungskette auf Grundlage von Informations- und Führungsüberlegenheit schneller Effekte zu erzielen führt zur Wirkungsüberlegenheit. Nur die Digitalisierung dieser Schritte wird den notwendigen Zeitvorteil ermöglichen.

„Software Defined Defence“ denken

Faktor Software: Beim Angriffskrieg gegen die Ukraine sehen wir einen gleichzeitigen Einsatz moderner Hightech-Systeme sowie veralteter Technik. Die Parallelität von Kampfhandlungen in Schützengräben wie im Ersten Weltkrieg und der Einsatz modernster Innovationen – insbesondere von Drohnen – mögen befremdlich anmuten, sind aber auch zukünftig zu erwarten. Ermöglicht wird diese Parallelität und

das koordinierte Zusammenwirken von Legacy-Systemen und Hightech durch die Einbindung in einen gemeinsamen Führungssystemverbund. So erleben Altsysteme durch den Anschluss an ein umfassendes Battle-Management-System eine signifikante Steigerung ihres Einsatzwertes. Aber auch für vergleichsweise moderne Waffensysteme sind der Datenanschluss und die Software des Systems immer mehr ein bestimmender Parameter für deren Einsatzwert – wir müssen „Software Defined Defence“ entsprechend denken und die Systeme danach ausrichten.

Faktor *Verbundene Dimensionen*: Die Einbindung einer möglichst breiten Vielfalt unterschiedlicher Sensoren sowie des ganzen Spektrums verfügbarer Effektoren in die militärische Wirkkette – die „Kill Chain“ – erfordert eine leistungsfähige, resiliente Netzwerkarchitektur und den Einsatz einer „Multi Domain Combat Cloud“. Truppenteile in dieser Cloud verfügen dann über gleiche Lageinformationen und können schnell und effektiv gemeinsam wirken, im Sinne von „Multi-Domain Operations“.

Verlässliche Service-Levels

Die Bundeswehr ist auf die enge Zusammenarbeit mit der zivilen Industrie und vor allem auf die Leistungen unseres strategischen Partners BWI als Servicedienstleister angewiesen. Die BWI muss die redundanten und gesicherten Leitungen für die Übertragung großer Datenmengen bereitstellen. Wir benötigen diese in hoher Verfügbarkeit mit geringem Ausfallrisiko. Dazu zählen eine Netzwerk-, Server- und Cloudinfrastruktur, die georedundant und ausfallsicher alle für unseren Auftrag relevanten Daten in der Bundeswehr jederzeit verfügbar hält. Der Anwender benötigt dabei moderne, nutzerfreundliche, intuitive Softwaretools für die digitale Umsetzung unserer „militärischen Geschäftsprozesse“. Und es bedarf eines vereinbarten „Service-Levels“, auf das sich die Bundeswehr jederzeit verlassen kann, denn im Falle des Falles müssen wir als Bundeswehr unseren Auftrag unverzüglich, zuverlässig und robust – bei Gefahr für Leib

und Leben – erfüllen können. Dazu benötigen wir die Unterstützung und Dienstleistungen aus Wirtschaft, Industrie und Gesellschaft – auch und insbesondere im Cyber- und Informationsraum.

Enge Einbindung aller Akteure

In diesem Themenheft wird vor dem Hintergrund der skizzierten Entwicklungen der Beitrag ausgewählter Vorhaben dargestellt, die zur „digitalen Kriegstüchtigkeit“ beitragen, wie dies unser Verteidigungsminister Boris Pistorius nennt. Sie werden die ganze militärische Wirkungskette vom Sensor bis zum Effektor wiederfinden: Datenerhebung, -aufbereitung und -auswertung, die Vernetzung von Manöverelementen und die gesicherte Datenübertragung zwischen diesen, der Einsatz von Cloud-Computing bis hin zum „scharfen Ende“ auf dem Gefechtsfeld.

Für die BWI gilt, den Blick in die Zukunft zu richten und auf die Handlungsfelder, die zu deren Gestaltung notwendig sind: Neue Technologien und deren Nutzbarmachung für die Bundeswehr, die erforderlichen Anpassungen von Prozessen, um unter den geänderten sicherheitspolitischen Rahmenbedingungen den Auftrag als Serviceprovider der Streitkräfte zu erfüllen und das Umgehen mit dem demografischen Wandel, der vor allem in der IT-Branche zu einem enormen Fachkräftemangel führt.

Es wird auch die enge Einbindung aller Akteure in die Digitalisierungsplattform der Bundeswehr betrachtet. Denn nur im koordinierten Zusammenwirken von politisch-strategischer Steuerung aus dem BMVg, den Nutzerforderungen aus den Teilstreitkräften Heer, Luftwaffe und Marine, der fachlichen Expertise aus der Teilstreitkraft CIR, sowie den Beschaffenden und Beschaffern im BAAINBw und unserem zivilen strategischen IT-Partner, der BWI GmbH, wird es gelingen, das Großvorhaben der Digitalisierung der Streitkräfte umzusetzen.

Ich wünsche Ihnen gute Einblicke in die fachlichen Themen sowie viel Vergnügen bei der Lektüre.

ON THE OCCASION OF THE BERLIN SECURITY CONFERENCE

The new Pre-BSC Magazine

- » Contributions from high-ranking political and military representatives
- » Detailed presentation of the partner country
- » Introduction to the key topics of the congress
- » Increased awareness among readers through target group-specific postal and digital distribution

Benefit from improved market visibility and place your advertisement now. Please contact our Sales Team:



BSC Berlin
Security Conference
23rd Congress on European Security and Defence

For further information: www.euro-defence.eu





Damit die IT-Systeme der Bundeswehr reibungslos funktionieren, kümmert sich die BWI im Hintergrund um den IT-Grundbetrieb.

Foto: BWI GmbH/Frank Löschke

Die Komplexität hinter „einfach funktionieren!“

Julian Klein, Leiter Shared Service Operations, BWI GmbH



Julian Klein

Foto: BWI GmbH/ Xandra Herdieckerhoff

Seit 2007 steht die BWI dafür, die Digitalisierung der Bundeswehr voranzutreiben und den IT-Grundbetrieb sicherzustellen. Die Bandbreite reicht dabei von Innovationsexperimenten zu neuen Formen der KI-gestützten Aufklärung über die Einführung von Cloud-Computing und digitaler Zugangskontrollen an den Liegenschaften bis hin zu digitalen Bahnfahrkarten für Reservisten.

Aber was genau ist eigentlich der IT-Grundbetrieb? Eine allgemeingültige Definition gibt es dazu nicht. Man könnte sagen, im Grundbetrieb stellt die BWI sicher, dass die IT der Bundeswehr funktio-

niert. Was einfach klingt, ist in der Realität ein gut abgestimmtes Zusammenspiel verschiedenster Einheiten, sowie vieler Fachexpertinnen und Fachexperten. Was das Team dabei leistet, sollen folgende Einblicke vermitteln.

Dienstbeginn in einer deutschen Kaserne. Für viele Angehörige der Bundeswehr ist das Einschalten des Arbeitsplatz-PCs (APC) Morgenroutine. Äußerlich unterscheidet sich der APC nicht von marktüblichen Geräten, aber auf die inneren Werte kommt es an. Mit dem APC erhalten die Soldatinnen und Soldaten nicht nur sicheren Zugriff auf IT-Services, die von BWI und Bundeswehr bereitgestellt werden. Er ist auch einer der meistverteilten Services der BWI. Der größte Teil der 182.000 uniformierten und 80.000 zivilen Angehörigen der Bundeswehr arbeitet mit einem der von der BWI bereitgestellten APCs. Diese sind voll gemanaged und in ihrer Soft- und Hardwareausstattung auf die Bedarfe der jeweiligen Dienstposten ausgerichtet. Updates für Software, Betriebssysteme und Sicherheitseinstellungen werden zentral und automatisiert von der BWI ausgebracht und die Nutzen-

den können sich stets auf einen aktuellen und abgesicherten APC verlassen.

Ein APC alleine macht den Nutzer noch nicht arbeitsfähig. Im Vordergrund steht auch bei den Arbeitsabläufen der Bundeswehr die reibungslose und digitale Kommunikation miteinander. Im letzten Jahr hat die BWI erfolgreich den Rollout von „Groupware“ abgeschlossen. Damit bezeichnen wir die Lösung zur E-Mail-, Telefonie-, Video- und Chat-Kommunikation, sowie Content- und Dokumenten-Management-Systeme. Mit dem Rollout von „Groupware“ wurde den Nutzenden ein Toolset zur Verfügung gestellt, das aus verschiedenen Softwarekomponenten besteht, die auch in der Industrie weitläufig genutzt werden. Das erleichtert die Kommunikation intern, mit der Industrie und auch mit den Bündnispartnern. E-Mails und Termine werden mit Outlook ausgetauscht, wahlweise mit entsprechender Verschlüsselung. Und in Konferenzen wählt man sich per VoIP Telefon, oder über eine Software wie Jabber ein. Dokumente, Inhalte und Workflows können kollaborativ in Echtzeit bearbeitet werden. Mit der Bereitstellung der „Groupware“-Funktionalitäten für über 230.000 Bundeswehrangehörige betreibt die BWI eine der größten Umgebungen in diesem Sicherheitskontext.

Sichere Sprach- und Datenkommunikation über das Glasfasernetz

Die besten IT-Services zur Kommunikation und APCs nutzen nichts, ohne eine schnelle, stabile und sichere Verbindung vom Endgerät über die Liegenschaften bis in die Rechenzentren. Egal wo die Nutzenden arbeiten – im Büro, von unterwegs oder zu Hause.

Als Basis dafür dient das Weitverkehrsnetz (WAN). Mit 13.000 Kilometern, redundant ausgelegten Glasfaserleitungen und rund 850 angebundenen Liegenschaften, sowie den Rechenzentren, gewährleistet es die sichere Sprach- und Datenkommunikation der Bundeswehr. Seit Ende 2023 ist der WAN-Backbone von Grund auf modernisiert und technologisch mit quantensicherer Verschlüsselungstechnologie ausgestattet. Mit derzeitigen Übertragungsgeschwindigkeiten bis zu 100 GBit/s sind wir für die aktuellen Herausforderungen gerüstet und können auch für die Zukunft weiter skalieren.

Eine genauso zentrale Rolle spielen die lokalen Netzwerkverbindungen innerhalb der Liegenschaften (LAN und WLAN), die jeweils mit einem Liegenschaftszugangsknoten (LZK) an das WAN angebunden sind. Mit fast 360.000 LAN-Anschlüssen an knapp 24.000 LAN-Komponenten und 42.000 WLAN-Accesspoints ist die Anbindung bei der Arbeit aus den Liegenschaften flächendeckend gewährleistet.

Das Arbeiten von zu Hause und unterwegs ist nicht mehr aus dem Arbeitsalltag vieler Bundeswehrangehöriger wegzudenken. Um auch über Mobilfunk oder den heimischen Internetzugang gesicherten Zugriff auf das Bundeswehrnetz zu erhalten, gibt es die Möglichkeit des Remote-Zugangs auf den APCs. Zum Ersatz der bisherigen hardwarebasierten Lösung, wird derzeit eine zugelassene Software-Lösung pilotiert, die den Zugang der Anwendenden unterwegs erleichtern soll.

APC, Kommunikationslösungen und gesicherte Verbindungen – check

Die BWI betreibt zum sicheren Hosting der skizzierten Services und Lösungen mehrere Rechenzentren (RZ). Diese bestehen aus beigestellten Rechenzentren der Bundeswehr, sowie extern angemieteten, besonders gesicherten RZ-Flächen. Die Rechenzentren verfügen über Geo-Redundanzen, um für besonders kritische Services komplette RZ-Ausfälle kompensieren zu können. In diesen RZs betreibt die BWI knapp 14.000 Server, ca. 9.000 Datenbanken und stellt Speicherkapazitäten von in Summe 240 Petabyte, was rund 240.000 Terabyte entspricht, zur Verfügung. Der Einsatz moderner Virtualisierungslösungen und Cloud-Technologien verdichtet die Rechen- und Speicherkapazität auf weniger, dafür aber leistungsstärkere Hardware. Damit können die Kapazitäten dynamisch und flexibel für den jeweiligen Bedarf genutzt werden.



Für die Einsatzfähigkeit der Bundeswehr sind funktionierende IT-Systeme unverzichtbar.

Foto: BWI GmbH/Frank Löschke

IT-Betrieb läuft hinter den Kulissen. Und man bemerkt ihn meistens erst, wenn etwas nicht wie gewohnt funktioniert. Daher ist die Königsdisziplin des IT-Betriebs, speziell in einer so groß dimensionierten und erfolgskritischen Umgebung, die frühzeitige Erkennung und der Umgang mit Störungen, sowie die zeitnahe Entstörung. Über unseren 24/7 erreichbaren Service-Desk können die Bundeswehrangehörigen eine Störung melden. Mit hoher Eigen-Kompetenz kann eine Vielzahl der Störungen direkt im Service-Desk, beim ersten Kundenkontakt gelöst werden. Eine Sprachführung mit Natural-Language-Understanding sorgt dafür, dass der Anwender sein Problem in gebräuchlicher Sprache schildern kann und automatisch den Service-Desk Mitarbeitenden mit entsprechenden Kenntnissen erreicht. Bei komplizierteren oder größeren Störungen, widmen sich die Fachexperten des Second- und Third-Level-Supports der Lösung.

Prüfung der Verbindungen, Backendsysteme und gegebenenfalls tiefgehende Protokoll- und Logdaten-Analysen führen fast immer zu einer zeitnahen Lösung. Sollte die Lösung nur vor Ort möglich sein, ist ein Service-Techniker des Field-Service, aus einem der 17 Service-Center in Deutschland

schnell und direkt zur Stelle und tauscht, wenn nötig defekte Hardware vor Ort aus oder grenzt das Problem weiter ein. Eine transparente Information für die Problemmeldenden mit aktuellen Informationen, während des gesamten Lösungs-Prozesses versteht sich von selbst. Über ein Wissens-Management werden die Erkenntnisse aus vorherigen Störungen wiederum allen Beteiligten zugänglich gemacht, um zukünftige, ähnliche Störungen wie oben erwähnt direkt beim Erstkontakt lösen zu können.



Nur einen Anruf entfernt – der Service-Desk der BWI. Für die Bundeswehr 24/7 im Einsatz.

Foto: BWI GmbH/Frank Löschke

Wichtig wie nie – Sicherheit der Daten

Die besonderen Sicherheitsanforderungen in unserem Umfeld verstehen sich von selbst. Vertrauliche Daten und Vorgänge, die auf IT-Systemen verarbeitet werden, sind eine potentielle Zielscheibe für Cyberangriffe. Aus diesem Grund hat Cybersicherheit eine herausragende Bedeutung bei allen strategischen Überlegungen und Entwicklungen und ist von Beginn an fester Bestandteil der bereitgestellten Lösungen. Um auch zukünftig ein sicheres, resilientes IT-System zur Verfügung zu stellen, das Gefahren effizient abwehrt und nach einem Angriff schnell wieder verfügbar ist, müssen wir das Themenfeld der Cybersicherheit ganzheitlich betrachten. Die Weiterbildung und Sensibilisierung unseres Personals, gehört ebenso dazu, wie die technische Aufrüstung und aktives Management erkannter Risiken.

Auch im Ausland ist auf die BWI Verlass

Soldatinnen und Soldaten der Bundeswehr sind nicht nur in Deutschland im Einsatz, sondern in vielen Ländern weltweit. Auch im Auslandseinsatz müssen die IT-Services und digitalen Lösungen verlässlich funktionieren. Als Beispiel für den IT-Betrieb der BWI im Ausland dient das Bundeswehr-Kontingent der Kosovo Force (KFOR) in Pristina. Dies stellt nur einen der Standorte dar, den die BWI im Ausland betreut. Mit der Einheit „International Mission & Training“ (IM&T) unterstützt die BWI militärische Übungen, Missionen und wir führen gemeinsam mit der Bundeswehr Schulungen für IT-Personal durch. Für Pristina überwacht und steuert IM&T seit 2018 den gesamten IT-Betrieb aus Deutschland. Alles im Zusammenspiel mit den militärischen IT-Experten

der Bundeswehr vor Ort. Teamwork also nicht nur innerhalb der BWI, sondern gemeinsam mit der Bundeswehr, unabhängig vom Einsatzort.

Im Auslandseinsatz oder im Tagesgeschäft in Deutschland ist die Logistik ein zentraler und einsatzkritischer Baustein. Ob Munitionsnachschub, Treibstofflieferungen oder Ersatzteile, alles muss zur richtigen Zeit am richtigen Ort sein. Hinter dem Begriff „Standard-Anwendungs-Software-Produkt-Familien“ – kurz SASPF – verbergen sich unter anderem von der BWI betriebene SAP-Systeme der Bundeswehr mit rund 80.000 Nutzenden und damit eine der größten SAP-Installationen Europas. Über den reinen Betrieb hinaus, leistet die BWI grundsätzlichen Support, unterstützt bei den Projekten und schult Nutzende auf den Systemen. Aktuell bereitet die Bundeswehr den Umstieg auf das Nachfolgeprodukt S/4 HANA vor, natürlich mit tatkräftiger Unterstützung der BWI.

Wir stellen uns den Herausforderungen der Zukunft

Besonders die aktuelle sicherheitspolitische Lage in Europa trägt dazu bei, dass wir uns neuen und unbequemen Fragen stellen. Wie erbringen wir unsere Leistungen im Fall einer Landes- oder Bündnisverteidigung? Welche Maßnahmen ergreifen wir, um in jeder Situation handlungs- und leistungsfähig zu bleiben? Mit dem Projekt „Landes- und Bündnisverteidigung“, setzen wir uns gemeinsam mit der Bundeswehr intensiv mit diesen und vielen weiteren Fragestellungen auseinander und leiten Maßnahmen zur Umsetzung ab. Genau wie die Bundeswehr, stellt sich die BWI diesen neuen Herausforderungen.

IT-Betrieb muss einfach funktionieren und das geht nur mit Blick nach vorne und einem starken Team! Unsere Soldatinnen und Soldaten, Nutzerinnen und Nutzer bei ihrer Arbeit mit „IT für Deutschland“ – unseren gemeinsamen, digitalen Services und Lösungen – zu unterstützen, ist unsere Aufgabe! Darauf sind wir stolz und dafür geben wir jeden Tag unser Bestes. Im Einsatz, in Deutschland, im Ausland, im Büro, zu Hause oder unterwegs, das große Team der BWI, das weit über den IT-Betrieb hinaus geht, ist bereit.

Panasonic CONNECT

TOUGHBOOK

TOUGH is

in erfolgskritischen
Momenten stark zu bleiben



Das ultimative C4I-Werkzeug für Verteidigungskräfte

Die Merkmale und das einzigartige Design des TOUGHBOOK 40 machen es zum perfekten Gerät für taktische Kommunikation – maßgeschneidert für Militäranwendungen, einschließlich Lageerfassung, militärischem Transport und Wartung.



Wasser- &
staubgeschützt



IP66 MIL-STD-810H
& MIL-STD-461F



Wetterfest



180 cm sturzfest



Intel® Core™ i7 vPro® Prozessor



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

www.toughbook.eu



Windows 11



Zusammenarbeit von BWI und Bundeswehr auf dem 5. BWI Data Analytics Hackathon 2023

Foto: BWI GmbH/Xandra Herdieckerhoff

Informationsüberlegenheit – Data Analysis als Game Changer

Christian Bartels, Head of & SVP Owner Software Data Solutions & Analytics



Christian Bartels Foto: BWI GmbH

Ob zu Lande, in der Luft, unter Wasser oder im Cyber- und Informationsraum – die BWI, als primärer Digitalisierungspartner der Bundeswehr, entwickelt in Zusammenarbeit mit ihren Expert*innen und einem starken Partnernetzwerk vielseitige Lösungen. Ziel ist es, die Führungs- und Handlungsfähigkeit der Streitkräfte durch gezielte Informationsverarbeitung weiter zu stärken. Dies gilt

für Friedenszeiten ebenso wie in Krisen- und Kriegssituationen, indem eine ganzheitliche Unterstützung über alle Dimensionen hinweg gewährleistet ist.

Das Team „Software Data Solution & Analytics“ der BWI, ein zentraler Bestandteil des „Center of Excellence Software En-

gineering“, fördert diese Bemühungen mit wissenschaftlicher Expertise in der Datenerhebung und -analyse. Wir halten Schritt mit den neuesten Entwicklungen in den sich rasant weiterentwickelnden Feldern der Künstlichen Intelligenz, des maschinellen Lernens sowie der Virtual und Extended Reality. Durch Beobachtung, Evaluation und Anpassung dieser Technologien streben wir danach, den hohen Ansprüchen unserer Arbeit gerecht zu werden und die Ziele unseres Kunden zu erfüllen. Der Einsatz dieser fortschrittlichen Technologien hat das Potenzial, militärische Prozesse von der Ausbildung über die Einsatzplanung bis hin zur Analyse entscheidend zu verändern.

Übergreifende Zusammenarbeit im Krisenfall: Krisenvorsorgeinformationssystem Bund

Die grundlegende Verantwortung eines jeden Staates besteht darin, im Notfall Bundesbürger aus Gefahr für Leib und Leben zu retten. Im Krisenfall entscheiden mitunter Minuten über Leben und Tod. Geleitet durch diese Vision entwickelt die BWI eine digitale Lösung in Form des Krisenvorsorge-

informationssystem Bund (KVInfoSysBund), um in Zukunft die Bundeswehr zur Krisenbewältigung zu befähigen. Mit dem KVInfoSysBund kann ein schnellerer Informations-transfer zwischen verschiedenen Bundesressorts, wie dem BMVg, dem Bundeskanzleramt, dem Auswärtiges Amt sowie dem BMI ermöglicht werden.

Das System soll eine Vielzahl von unterschiedlichen Komponenten innerhalb einer Microservice-Architektur beinhalten. Diese dienen dann der Darstellung und Analyse der Lageentwicklung durch die Verarbeitung von nachrichtendienstlichen und öffentlichen Dokumenten und Daten aus sozialen Netzwerken. Aussagen über Konflikte oder Krisen könnten so mithilfe von Methoden des maschinellen Lernens getroffen werden. Darüber hinaus soll das System im Krisenfall mobil und autark, also ohne Datenverbindung, einsatzfähig sein und die Handlungsfähigkeit der beteiligten Bundesressorts sicherstellen. Gleichzeitig gilt es, die hohen Anforderungen von Bundesbehörden und der Bundeswehr hinsichtlich Datenschutz und Informationssicherheit zu beachten. Die bisherigen Tests zeigen, dass Synergien zwischen den Fachbereichen erschlossen werden können. Unter anderem konnte das Zentrum für Geoinformationswesen der Bundeswehr (ZGeoBw) Geodaten und -dienste auf der von der pCloudBw betriebenen Geoinformationssystem-Plattform erfolgreich erproben. Die private Cloud der Bundeswehr unterliegt wiederum höchsten Anforderungen an Sicherheit, Resilienz und Autarkie.



Blick in den Laderaum eines Evakuierungsfliegers der Bundeswehr
Foto: Bundeswehr/Marc Tessensohn

Die bisherige Entwicklung des Projektes offenbart bereits ein enormes Potential für das System, welches durch sein Datenintegrationskonzept zukünftig bereit sein wird, KI-Technologie zu nutzen. So könnte neben der intelligenten und raumbezogenen Suche auch die Auto-Summarization dazu beitragen, schlagartig Lagebilder durch das Zusammenfassen vieler Dokumente zu erstellen. Das KVInfoSysBund zeigt bereits in der Entwicklungsphase seinen Nutzen und verspricht durch die Darlegung relevanter Informationen einen bedeutenden Vorteil in Krisensituationen.

KALMAR optimiert militärische Aufklärung Unterwasser

Während der Einsatz von KI zu Lande, in der Luft und auch im Cyber- und Informationsraum schon zur gängigen Praxis gehört, gestaltete sich die militärische Aufklärung unter Wasser aufgrund physikalischer Gegebenheiten und technischen Einschränkungen als zeitaufwändig und schwierig. Üblicherweise suchen autonome Unterwasserfahrzeuge über mehrere Stunden automatisiert vorher festgelegte Planbereiche ab. Bei ihren Aufklärungsfahrten bleiben sie für den gesamten Zeitraum unter Wasser und kommunizieren nicht mit der Operationszentrale. Aufgrund dessen können die erfassten Daten erst nach dem Auftauchen ausgelesen und durch einen Operateur aufwändig manuell gesichtet werden. Der Prozess soll nun digitalisiert und zeitig effizienter gestaltet werden. Wie dies mithilfe von KI funktionieren kann, zeigt das Innovationsexperiment KALMAR.



Innovationsexperiment KALMAR bei einem Tauchgang in Eckernförde
Foto: Marcus Mohr

Gemeinsam mit dem Marinekommando, der marinom GmbH, der Hochschule Bremen und wesentlicher Unterstützung durch die Wehrtechnische Dienststelle WTD71, entwickelte die BWI das Experiment. Bei KALMAR werden autonome Unterwasserfahrzeuge der Bundeswehr mit einem Edge Device – einem Minicomputer, der seine Arbeit am Rand, also dezentral von einem Netzwerk, durchführt – und einer darauf installierten, speziell trainierten KI ausgestattet. Diese ist in der Lage, Sonardaten unter Wasser in Echtzeit auszuwerten und vorab definierte Objekte zu erkennen. Bei der Sichtung eines vorab definierten Objektes – beispielsweise einer Mine – bringt die KI das Unterwasserfahrzeug unmittelbar zum Auftauchen. Diese sendet dann die Daten des erkannten Objekts, wie zum Beispiel Tiefe, Maße oder Objektwahrscheinlichkeiten, zur Einbindung in das Lagebild direkt an den Operateur weiter. Anschließend kann das Fahrzeug seine Suche im Planbereich fortsetzen oder neue Befehle durch den Operateur erhalten. Damit wird der Prozess der Datengewinnung und –Auswertung enorm beschleunigt und Sichtungen unter Wasser nahezu in Echtzeit ermöglicht. Mit der beschleunigten Auswertung kann eine Lücke in der militärischen Aufklärung geschlossen werden. Das Potential des Experiments ist groß. Durch das Training mit neuen Objektgeometrien kann KALMAR Seeminen detektieren und sowohl im Küstenschutz, in Auslandshäfen als auch bei Kritischen Infrastrukturen eingesetzt werden. Eine mög-

liche zeitgleiche Aussendung mehrerer AUVs deutet zudem auf einen entscheidenden Vorteil bei einer zeitintensiven Aufklärung hin.

Neuronale 3D-Visualisierung für präzise Lagebilder aus der Luft

Abseits der kontextuellen Datenerhebung von KI bergen die Entwicklungen in der Virtual Reality (VR) und Extended Reality (XR) im militärischen Kontext großes Potential. Während beide im zivilen Bereich bereits eine breitere Anwendung finden, kann XR die Art und Weise des Trainings und die Arbeitsabläufe von Streitkräften auf dem Gefechtsfeld grundlegend verändern. Dies betrifft insbesondere die Lagebilderstellung und -erfassung.

Präzise und verlässliche 3D-Lagebilder werden im Alltag der Bundeswehr in den unterschiedlichsten Situationen benötigt. Häufig wird dabei auf Satellitenbilder zugegriffen, die nur einen geringen Detailgrad besitzen. Dies macht beispielsweise eine zuverlässige Auswertung von Waldbereichen oder der Befahrbarkeit von Wegen schwierig und eine zuverlässige Lageübersicht kaum möglich.

Gleichzeitig erweist sich die Erfassung großer Landschaften in 3D durch die enorme Datenmenge als schwierig. Neural Radiance Fields bietet hier einen Ansatz, der der Problematik entgegenwirkt: Unterstützt durch neuronale Netze können 3D-Darstellungen aus Bildern erlernt und diese sehr realistisch und kompakt dargestellt werden. Fängt eine Drohne beispielsweise Bilder eines dichten Waldes ein, in dem ein verdeckter Panzer steht, können mithilfe von KI einzelne Elemente entfernt und darunter liegende Objekte sichtbar gemacht werden. Das Projekt hat seine Erstuntersuchung durchlaufen und seine Funktionsfähigkeit bewiesen. Derzeit arbeitet die BWI daran, mithilfe mehrerer Fluggeräte größere Gebiete zu erfassen.

Data Analytics: Advantage through technological adaptation

Die BWI setzt sich zum Ziel, neue Technologien proaktiv zu identifizieren, zu evaluieren und für die Bundeswehr nutzbar zu machen. Das Team „Software Data Solutions & Analytics“, in enger Zusammenarbeit mit dem Bereich Innovation & Technology (I&T), spielt eine Schlüsselrolle bei der Realisierung datenzentrierter Projekte für die BWI und die Bundeswehr. Dieser Prozess umfasst alles – von der Erprobung neuester wissenschaftlicher Erkenntnisse in den Bereichen Künstliche Intelligenz und Data Science bis hin zur Entwicklung von Softwarelösungen, die in Krisensituationen entscheidend sein können. Sobald ein Projekt den hohen Anforderungen unseres Qualitätsauswahlprozesses genügt, wird es für eine praktische Anwendung innerhalb der Streit-



Bei dem BWI Data Analytics Hackathon entwickeln BWI und Bundeswehr gemeinsam innovative KI-Lösungen.

Foto: BWI GmbH / Xandra Herdieckerhoff

kräfte weiterentwickelt. Diese sorgfältige Auswahl und Implementierung sichert nicht nur den technologischen Vorsprung der Bundeswehr, sondern gewährleistet auch, dass jede neue Lösung einen direkten Beitrag zur Effizienz und Effektivität der Streitkräfte leistet.

Der immense Fortschritt in der Informationstechnologie unterstreicht die Notwendigkeit, kontinuierlich mit dem technologischen Wandel

Schritt zu halten. Um die aktuellsten Trends und Technologien auf ihre Eignung für die Bundeswehr zu testen, richtet die BWI seit 2019 den jährlichen BWI Data Analytics Hackathon aus. Dieses Ereignis hat sich als feste Institution etabliert, bei dem Expert*innen aus der Bundeswehr und der BWI für eine Woche zusammenkommen, um innovative Ideen in den Bereichen der Künstliche Intelligenz (KI) und Datenanalyse prototypisch zu entwickeln.

Die aus diesem Kontext entstandenen Prototypen unterziehen sich anschließend weiteren Experimenten oder fließen direkt in Projekte ein, die in enger Zusammenarbeit mit den Innovationseinheiten der BWI vorangetrieben werden.

In den vergangenen Jahren wurden bereits etwaige Lösungen praxisorientiert umgesetzt. Unter anderem ermöglicht die „Signal Intelligence“, mit KI durch Wände zu schauen. Zudem wurde unter Verwendung von Machine Learning Methoden ein Innovationsexperiment zur Vorhersage des Weltraumwetters kreiert. Abseits dessen wird aktuell Doctagging für den SharePoint implementiert. Auch der sogenannte „Propaganda Compass“ wurde im Rahmen des Hackathons erarbeitet und weiterentwickelt. Der Compass stellt eine IT-Lösung dar, die unter anderem Propagandakampagnen auf Social-Media-Plattformen erkennt und Hilfe bei der Recherche und Analyse von Onlinemedien zur Lagebilderstellung bietet.

Fazit: Data Analytics als entscheidender Faktor für die digitale Handlungsfähigkeit der Bundeswehr

Die ganzheitliche und zuverlässige Erhebung und Auswertung von Daten ist für eine digitale Bundeswehr unerlässlich. Die BWI steht der Bundeswehr durch die gezielte Einbindung modernster Technologien fortwährend zur Verfügung. Mittels der Anpassung an den technologischen Fortschritt befähigt die BWI die Bundeswehr mit leistungsstarker, zuverlässiger und sicherer IT dazu, ihre Aufgaben bestmöglich zu bewältigen und für den Einsatz digital vorbereitet zu sein.



Der Erfolg militärischer Operationen hängt immer stärker von der Qualität der Digitalisierung ab.

Foto: Bundeswehr/Maximilian Schulz

Mit digitaler Vernetzung zur militärischen Überlegenheit

Dr. Martin Deeg, Leiter BWI Customer Solutions



Dr. Martin Deeg Foto: BWI GmbH

Das digitale Gefechtsfeld von heute und morgen stellt immer neue Anforderungen an die Bundeswehr. Standen früher vor allem örtlich gebundene Kampfhandlungen im Fokus, finden militärische Auseinandersetzungen inzwischen nicht nur über mehrere Domänen wie Land, Luft und See statt, sondern umfassen zunehmend auch den Cyber- und Informationsraum. Daher ist es auch Ziel mi-

litärischer Operationen, Überlegenheit über einen Gegner durch das orchestrierte Zusammenwirken von Effekten über mehrere Dimensionen zu erlangen.

Das (vernetzte) Gefechtsfeld der Zukunft

Dieser Multi-Domain-Operations-Ansatz unterscheidet sich von den bisherigen operativen militärischen Ansätzen durch den Anspruch, von allen Dimension in alle Dimensionen zu wirken. Eines der entscheidenden Erfolgskriterien ist die Realisierung einer digitalisierten Führungsorganisation, die nahtlos von der taktischen zur strategischen Ebene zusammenarbeiten kann. Basis ist hier die Vernetzung, die Interoperabilität von Daten und Anwendungen, das Informationsmanagement sowie die nötige Resilienz, um auch bei gravierenden Störungen die Funktionalitäten nutzen zu können. So werden Daten für die Führungs- und Informationssysteme über alle Domänen und Hierarchieebenen verfügbar. Darüber hinaus werden auf dem Gefechtsfeld der Zukunft intelligente Systeme Daten erheben, im Verbund auswerten und den militärischen Entscheidern Möglichkeiten für angemessenes Handeln bereitstellen („Sensor to Decider“) sowie das Zusammenspiel zwischen Aufklärung und militärischem Vorgehen weiter automatisieren („Sensor to Shooter“).

Erfolgskriterien für eine dimensionsübergreifende Vernetzung

Die Implementierung derart anspruchsvoller Anforderungen über unterschiedliche Dimensionen der Bundeswehr, Streitkräfte von Partnerstaaten sowie ziviler Partner ist ein komplexes Vorhaben, das nur über eine klare Governance umsetzbar ist. Auch wenn die Realisierung der einzelnen Digitalisierungsvorhaben in unterschiedlicher Verantwortung erfolgt, müssen einheitliche Architekturvorgaben berücksichtigt werden. Vorgaben aus dem „Federated Mission Networking“ und der „Multi Security Domain Architecture“ stellen die Interoperabilität sicher. In der technischen Implementierung bleiben gewisse Freiheitsgrade erhalten, da Standardisierung nicht zur Abhängigkeit von einzelnen Produkten führen soll. Ein weiterer Aspekt ist die Bereitschaft und eine positive Haltung aller Beteiligten, Digitalisierung wirklich einzusetzen und sich auf Daten und Informationen zu verlassen. Ziel ist die effektive und effiziente gemeinsame Einsatzbereitschaft, Verkürzung von Vorlaufzeiten, Führungsfähigkeit und nahtlose Zusammenarbeit intern und mit den Bündnispartnern zu erreichen.

Die Digitalisierung landbasierter Operationen

Im Programm „Digitalisierung landbasierter Operationen“ (D-LBO) geht die Bundeswehr diese dimensionsübergreifende Vernetzung zunächst für die mobile Ebene an. Die BWI unterstützt die vielfältigen Teilprojekte im D-LBO-Umfeld in diversen Disziplinen mit ihrer Expertise in der Integration und im Betrieb in der mobilen taktischen Ebene sowie im Customer Product Management. Darüber hinaus ist sie in die Einführung der durch D-LBO bereitgestellten IT-Lösungen eingebunden und trägt somit dazu bei, dass die Truppe neue Fähigkeiten zur Umsetzung ihrer Aufgaben erhält.

Datennutzung, schnell und sicher

Im Bereich der einsatznahen IT steht die Bundeswehr vor der Mammutaufgabe, sich so zu digitalisieren, dass auf dem Gefechtsfeld die entscheidenden Daten gefiltert, ausgewertet und so aufbereitet zur Verfügung gestellt werden, dass militärische Entscheider präziser und schneller als der



Die BWI unterstützt die Bundeswehr bei den Teilprojekten im D-LBO-Umfeld.
Foto: BWI GmbH



Das Ziel einer vernetzten Operationsführung besteht darin, durch eine effiziente Vernetzung von Informationstechnologien militärische Vorteile zu erlangen.
Foto: BWI GmbH/Peter Clemens

Gegner handeln können. Hierbei ist es entscheidend, dass im Zielbild einer datenzentrierten IT-Architektur durchgehend von der mobilen Ebene bis ins Heimatland gedacht wird. Zunächst sind IT-Systeme und Transmission wichtige Bausteine, Daten schnell zu übertragen, um an der richtigen Stelle Handlungsoptionen abzuleiten. Zudem sind eine dezentrale Datenhaltung und ein durchgehendes Datenmodell erforderlich, damit alle notwendigen Ressourcen ohne Zeitverlust und große Anpassungen an Schnittstellen interagieren können. Schließlich muss sichergestellt werden, dass die Datenhoheit nicht an Dritte weitergegeben wird, um beim zunehmenden Einsatz von automatisierten und (teil-)autonomen Systemen die Integrität der Daten sicherzustellen.

Vernetzte Kräfte, präzise Lagebilder

Das Erzeugen und Teilen aktueller und präziser Lagebilder auf Grundlage sicherer Daten ist eine wesentliche Voraussetzung, um militärische Überlegenheit zu erzielen. Die ist beispielsweise mit dem „Battle Management System“ (BMS) möglich. Dieses digitale Führungsinformationssystem bindet Sensoren und Effektoren in den Führungsprozess ein und stellt einen durchgängigen Systemverbund her. Damit kann die Bundeswehr ihre Einsätze digital planen, deren aktuelle Lage in Echtzeit darstellen sowie Gefechtsstände und Einheiten im Feld interoperabel vernetzen und dies auch im internationalen Verbund.

Auf dem BMS ist auch der „Mission Enabling Service“ (MESBw) enthalten, den die Bundeswehr-Einheiten sowohl in Fahrzeugen als auch Gefechtsständen nutzen können. Die von der BWI vorkonfigurierten und ausgerollten Software-Pakete mit umfassendem Datenmaterial und umfangreichen Funktionalitäten können dabei über verschiedene Kommunikationsmittel übertragen werden. Hierbei unterstützt die BWI beim Aufbau der IT-Infrastruktur, der Vernetzung mit den bestehenden Systemen der Bundeswehr sowie bei der Ausbildung der Soldatinnen und Soldaten für die Bedienung des BMS und der IT in Fahrzeugen und Gefechtsständen.

Weiterentwicklung der Vernetzung

Die Lösung zur Vernetzung der militärischen Kräfte wird schrittweise ausgerollt. Dabei werden auch neue Systeme wie etwa digitale Funkgeräte in Nutzung für die Bundeswehr gebracht. Aber auch das BMS für die Fahrzeugebene wird von der BWI auf dem dafür eigens entwickelten Tactical Client integriert und stetig weiterentwickelt. Die Gefechtsstände erhalten damit ein leicht zu installierendes Serversystem und periphere IT-Systeme, die eine einfache Nutzung des BMS ermöglichen. Auch zivil genutzte Verfahren und Applikationen werden für die autarke Nutzung in Fahrzeugen und Gefechtsständen übertragen. Das reduziert den Entwicklungsaufwand und beschleunigt die Bereitstellung in Form von regelmäßigen Releases.

Jedes durch die BWI erstellte MESBw-Release für die Fahrzeug- und Gefechtsstandebene durchläuft einen intensiven Testzyklus, sowohl in der BWI als auch in der Bundeswehr. Dies erfolgt in Form von Hands-On Erprobungen, da derartige Tests oftmals bereits der realen Nutzung entsprechen und in kurzer Zeit wichtige Erkenntnisse liefern, um die Produkte stetig zu verbessern. Technische oder organisatorische Änderungswünsche an Releases werden durch die Bundeswehr kontinuierlich erfasst und in die Serviceentwicklung der BWI zur Bewertung gegeben. Die Anpassungen erfolgen zeitnah in den anstehenden Releases, die durch die umfangreichen Testzyklen bei BWI und Bundeswehr direkt auf Tauglichkeit überprüft werden.

sungen erfolgen zeitnah in den anstehenden Releases, die durch die umfangreichen Testzyklen bei BWI und Bundeswehr direkt auf Tauglichkeit überprüft werden.

Herausforderungen auf dem vernetzten Gefechtsfeld

Trotz schneller technologischer Entwicklungen bestehen aber nach wie vor große Herausforderungen bei der Vernetzung der militärischen Einheiten. Dazu zählen etwa die zur Verfügung stehende Bandbreite, die Störfestigkeit des Signals und die Nicht-Detektion durch die feindliche Aufklärung. Zwar kann eine zunehmende Digitalisierung einige dieser Herausforderungen verringern, aber nicht gänzlich beseitigen. So ist die Umrüstung auf neue Geräte ein mehrstufiger Prozess, bei dem die Besonderheiten einzelner Fahrzeugplattformen berücksichtigt werden müssen. Für die Truppe bedeutet dies, sich bei den jeweils eingesetzten Technologien immer wieder auf den aktuellen Wissenstand zu bringen. Eine weitere Herausforderung stellt die IT-Sicherheit dar: Damit sichere Übergänge zwischen einzelnen Dimensionen und Domänen erfolgen können, unterstützt die BWI die Bundeswehr auch bei der Erstellung von Informationssicherheitskonzepten, die eine Balance zwischen der praktischen Bedienbarkeit im Einsatz und der Sicherheit der Daten und Systeme herstellen sollen.

Rahmenbedingungen für Übertragungstechnologien im militärischen Kontext

Im militärischen Umfeld, insbesondere auf der mobilen taktischen Ebene existieren besondere Herausforderungen im Hinblick auf die Informationsübertragung. Hier sind unter anderem die mit verschiedenen Missions- und Operationsarten einhergehenden, teils sehr unterschiedlichen Anforderungsprofile an Übertragungsinfrastrukturen, variable und mitunter extreme Umweltbedingungen sowie die außerordentliche Einsatzdynamik zu nennen. Gleichzeitig versuchen gegnerische Kräfte durch Maßnahmen des elektronischen Kampfs gegen die Nutzung des elektromagnetischen Spektrums zu wirken.

Im Zuge von Potenzialanalysen werden Übertragungstechnologien meist entlang der Ausprägung von Fähigkeitsmerkmalen gegeneinander bewertet. Feststehende physikalische Gesetzmäßigkeiten bedingen Wechselwirkungen zwischen Fähigkeitsmerkmalen – eine starke Ausprägung eines Fähigkeitsmerkmals hat häufig eine verminderte Ausprägung eines oder mehrerer anderer Merkmale zur Folge. Beispielsweise ist ein hoher Datendurchsatz in der Regel gepaart mit geringerer Reichweite. Und eine gesteigerte Resilienz geht zumeist mit geringer Bandbreiteneffizienz einher. Konsequenz ist, dass die über alle Bedarfsprofile kumulierten Leistungsmerkmale unabhängig von künftigen technologischen Fortschritten nicht gleichzeitig durch eine einzige Übertragungstechnologie beziehungsweise ein einziges Übertragungssystem abgedeckt werden können.

Neben den rein übertragungstechnischen Gesichtspunkten spielen ebenfalls betriebliche Aspekte, Benutzerfreundlichkeit, Formfaktoren und Entwicklungszyklen eine zentrale Rolle. Im Hinblick auf den ex-

ponentiellen Charakter technologischer Neuerungen bietet der „Dual-Use“ Ansatz, bei dem kommerzielle Technologien in die militärische Domäne transferiert werden, großes Potential, die enormen Entwicklungsressourcen des zivilen Markts wertschöpfend zu nutzen. Zwei Übertragungstechnologien stehen hier derzeit besonders im Fokus und werden auch in Zukunft zunehmend an Bedeutung gewinnen: Satellitenkommunikationssysteme und 3GPP Mobilfunknetze. Erstere existieren bereits seit einigen Jahrzehnten und bieten viele Vorteile, denen aufgrund geostationärer Umlaufbahnen bis dato jedoch häufig geringe Datendurchsätze und sehr hohe Laufzeiten gegenüberstehen. Dieser Malus wird durch den Low-Earth-Orbit-Ansatz substantiell reduziert, ohne die Vorzüge wie große Gebietsabdeckung insbesondere auch in unzugänglichen Regionen einzubüßen.

Kommerzielle Mobilfunktechnologien sind durch extrem hohe Datenraten, ausgezeichnete Bandbreiteneffizienz, kurze Entwicklungszyklen und Benutzerfreundlichkeit gekennzeichnet. Darüber hinaus bieten eingeführte Service-orientierte Architekturansätze in Verbindung mit der Möglichkeit Netzwerkfunktionen zu virtualisieren großes Potential im Hinblick auf Software-Defined-Defence-Konzepte. Häufigster Kritikpunkt ziviler Lösungen war bislang die geringe Resilienz gegenüber Störeinflüssen. Diesem Defizit wird in der fünften Generation des 3GPP-Standards und folgenden, mit zunehmend ausgefeilten Richtwirkungsmechanismen (Beamforming) sowie Verfahren zur Direktkommunikation zwischen Endgeräten begegnet.

SitaWare: Die Software-Suite für militärische Führungsinformationssysteme

Systematic ist weltweit führend in der Entwicklung und Bereitstellung hochmoderner C4I-Software für militärische Führungsinformationssysteme. Mit unserer SitaWare-Suite setzen wir weltweite Standards für Effizienz, Zuverlässigkeit und Interoperabilität.

Warum SitaWare?

SitaWare ist eine interoperable Commercial-off-the-Shelf (COTS) Software-Suite und basiert auf einer offenen Architektur, welche individuelle Erweiterungen und die Integration mit Drittsystemen ermöglicht. Im Bereich der Interoperabilität gilt SitaWare als Benchmark für die Entwicklungen anderer Nationen und setzt damit Standards für den Datenaustausch in multinationalen Operationen. Durch die offene Architektur, die inhärente Interoperabilität sowie die Skalierbarkeit bietet SitaWare eine passende Grundlage für eine multidimensionale Operationsführung. SitaWare unterstützt neben Landoperationen im gleichen Maße die Operationen in den Dimensionen Luft, See, Cyber sowie Space. Systematic ist Marktführer für Battle Management Applikationen, Führungsinformationssysteme und Lösungen für die militärische Interoperabilität. Mit 50+ Nutzernationen inklusive 18 NATO-Staaten ist SitaWare die meistgenutzte C4I-Software Suite weltweit.

SitaWare im Einsatz

Unser Software-Ökosystem wird bereits von Streitkräften auf der ganzen Welt eingesetzt und hat sich in den anspruchsvollsten Einsatzumgebungen bewährt. Von NATO-Mitgliedern bis hin zu Partnerländern in anderen Teilen der Welt vertrauen Militärs auf die Leistungsfähigkeit und Zuverlässigkeit von SitaWare. Unsere langjährige Erfahrung und kontinuierliche Innovation haben uns zu einem vertrauenswürdigen Partner für Streitkräfte auf der ganzen Welt gemacht. Von kleinen taktischen Einsätzen bis hin zu groß angelegten Multi-Domain-Operations im Verbund mit Bündnispartnern, bietet die SitaWare Suite die Flexibilität, die unsere Nutzer benötigen. Mit SitaWare haben militärische Führer aller Ebenen Zugriff auf Echtzeitinformationen, die es ihnen ermöglichen, schnellere und fundiertere Entscheidungen zu treffen. Durch die Einbindung in den Führungsprozess sowie den Austausch aller Daten, geht die Integration weit über die reine Darstellung von Eigenpositionsdaten hinaus. Ob mit unseren Produkten SitaWare Headquarters für stationäre und verlegfähige Gefechtsstände, SitaWare Frontline für Gefechtsfahrzeuge oder SitaWare Edge für den abgesessenen Einsatz - SitaWare ist für die Einsatzbereiche konzipiert, in denen Mobilität und Geschwindigkeit die Schlüsselfaktoren sind.



Abbildung – SitaWare Edge ist eine Android-Applikation für den abgesessenen Einsatz und steht für mobile Endgeräte zur Verfügung.
Foto: Systematic GmbH

Unser Engagement für Sicherheit und Zuverlässigkeit

Wir investieren kontinuierlich in Forschung und Entwicklung um sicherzustellen, dass unsere Produkte stets an der Spitze der Technologie bleiben. Unsere Nutzer können sich darauf verlassen, dass sie mit SitaWare stets Zugang zu den neuesten Funktionalitäten und Innovationen haben. Systematic ist stolz darauf, mit einem globalen Netzwerk von Partnern zusammenzuarbeiten, um unsere Produkte weltweit anzubieten. Von der Beratung und Schulung vor Ort bis hin zum technischen Support bieten wir unseren Nutzern weltweit erstklassigen Service und Unterstützung. Mit Systematic und der SitaWare Suite sind Sie für die Herausforderungen der modernen Einsatzszenarien bestens gerüstet.

Besuchen Sie uns auf der AFCEA am Stand S47

Erleben Sie die Zukunft der militärischen Führungsinformationssysteme hautnah und besuchen Sie unseren Stand. Unsere Experten stehen Ihnen gerne zur Verfügung, um Ihnen einen Einblick in die Leistungsstärke von SitaWare zu geben und Ihre Fragen zu beantworten. Um mehr über unsere Produkte zu erfahren, besuchen Sie unsere AFCEA Event Page.

SYSTEMATIC

Systematic GmbH
Im Zollhafen 14
50678 Köln

Tel + 49 221 29294319
more.info.de@systematic.com
www.systematic.com





Mitarbeiter der BWI vor einem Serrack in einem Rechenzentrum

Foto: BWI GmbH/Frank Lösche

Agiler und robuster – Cloud und die Fähigkeitsentwicklung der Bundeswehr

Dr. Götz Reinhäkel, Programmleiter pCloudBw, BWI GmbH



Dr. Götz Reinhäkel Foto: privat

Cloud-Computing gehört zu den wichtigsten Technologien der Digitalisierung. Auch und gerade für die Bundeswehr. Anwendungen, Plattformen und Infrastrukturen lassen sich mithilfe von Cloud schneller, bedarfsgerechter und effizienter bereit- und im Zweifel wiederherstellen. Deshalb ist eine eigene, private Cloud für die Bundeswehr ein Kernelement ihrer künftigen IT-Architektur. Und sie bietet einige wesentliche Vorteile. Dazu

ein Beispiel: Kubernetes ist ein von Google entwickeltes Open-Source-System, mit dem auf Cloud-Infrastrukturen sogenannte Container-Anwendungen verwaltet werden können. Bei Containern handelt es sich um Pakete, die alle Elemente enthalten, um eine Software in einer beliebigen Umgebung auszuführen. Das heißt: Sie enthalten den Code, Bibliotheken und alle sonstigen Abhängigkeiten. Anstatt nun Rechenleistung für eine Anwendung auf einem physischen oder virtuellen Server auf Vorrat vorzuhalten, sucht Kubernetes nach Servern, die freie Kapazitäten haben, startet Softwarepakete automatisiert und gibt die Rechenleistung nach Beendigung ebenso automatisiert wieder frei – je nach Bedarf und Auslastung. Mehr Agilität, Effizienz und Skalierbarkeit – das wird durch die Cloud möglich.

Die Technologie bietet die Chance, Speicher- und Rechenkapazitäten kurzfristig dem jeweiligen Bedarf anzupassen, was ressourcenschonender und kostengünstiger ist. Cloud-

basierte Anwendungen können zentral und damit schneller ausgerollt werden, da sie nicht lokal auf einem Rechner installiert werden müssen. Im Umkehrschluss können Nutzer auf Cloud-Anwendungen praktisch von jedem angebandenen Gerät aus zugreifen. Und auch Innovationen lassen sich beschleunigen, da beispielsweise Instanzen für die Entwicklung in einer Cloud mit wenigen Klicks eingerichtet werden können.

Digitalisierung als Schlüssel

Kurzum: Über eine Cloud lassen sich Anwendungen, Plattformen und Infrastrukturen als skalierbare Services schneller, flexibler und effizienter zur Verfügung stellen. Das macht die Technologie so relevant für die digitale Transformation der Bundeswehr. Und die wiederum eröffnet der Bundeswehr viele Möglichkeiten. Digitalisierung hilft ihr dabei, Prozesse zu vereinfachen, den Wissenstransfer zu beschleunigen, die Zusammenarbeit zu verbessern und so das eigene Personal zu entlasten. Im Einsatz ermöglicht sie der Bundeswehr, grundlegende militärische Ziele zu erreichen: Informations-, Führungs- und damit Wirkungsüberlegenheit. Ob militärische Operationen erfolgreich sind, hängt nämlich zunehmend auch davon ab, wie gut die eigenen Streitkräfte digitalisiert sind. Damit eigene und verbündete Einheiten im Gefecht präzise, angemessen und vor allem schneller als der Gegner handeln können, benötigen sie Informationen und müssen miteinander vernetzt sein. Aber nicht nur in den klassischen militärischen Dimensionen Land, Luft und See werden digitale Fähigkeiten immer wichtiger, auch im Cyber- und Informationsraum selbst. Militärische Konflikte sind heute zunehmend auch durch Cyberangriffe, Störungen von Übertragungswegen sowie hybriden Einschränkungen der eigenen Operationsplanung und -führung geprägt. Das heißt, Einsätze finden zunehmend unter erschwerten Bedingungen statt und werden zunehmend über mehrere Dimensionen hinweg geführt. Daher benötigt die Bundeswehr in allen Dimensionen handlungsfähige Kräfte und militärische Fähigkeiten.

Hinzu kommt der rasante technologische Fortschritt, allen voran in Form der Digitalisierung selbst, von der die Bundeswehr durch ihre Größe und als Nutzerin komplexer Tech-

nologien besonders betroffen ist: immer größere Datenmengen, die beherrscht werden müssen, und in der Folge immer leistungsfähigere Hardware und eine immer schnellere Entwicklung von Software. Und schließlich funktioniert heute kaum ein Waffensystem noch ohne Informationstechnik.

Die Cloud auf dem Gefechtsfeld

Cloud ist aber nicht nur ein wesentlicher Treiber der Digitalisierung. Sie gehört neben Künstlicher Intelligenz oder modernen Übertragungswegen auch zu jenen Kerntechnologien, die den kombinierten Einsatz von Kräften und Fähigkeiten in mehreren Dimensionen möglich machen. „Multi Domain Operations“ heißt diese neue Art der Einsatzführung. Cloud kann hierbei als IT-Plattform nicht nur die nötige Speicher- und Rechenkapazität liefern. Sie bietet auch Agilität und Resilienz. Im Einsatz müssen Einheiten schnell den Standort wechseln können und umgehend wieder einsatzbereit sein. Über eine Cloud lassen sich Anwendungen, Plattformen und Infrastrukturen bei Operationen nicht nur schneller bereitstellen. In Folge von Angriffen oder Störungen etwa lassen sich cloudbasierte Systeme auch schneller wiederherstellen.

Auch im Kontext von „Software Defined Defence“ offenbart Cloud-Computing seine Stärken. Im Kern geht es bei dem Konzept darum, sich bei Weiterentwicklungen von Waffensystemen mehr auf die Software, als wie bisher auf die Hardware zu konzentrieren, da der technologische Fortschritt dort schneller ist. Das ermöglicht zum einen bessere Anpassungen an die Anforderungen der modernen Operationsführung. Zum anderen erlaubt der softwaredefinierte Ansatz die Vernetzung und damit die verbesserte Zusammenarbeit der Systeme mit- und untereinander. Die Cloud ist dabei die integrierende IT-Plattform, über die die verschiedenen Systeme im Einsatz miteinander verbunden werden. Zudem können darüber als sogenannte „Provisioning Plattform“ beispielsweise Updates für Plattformen im Backend vorbereitet und bis in die einzelnen Waffensysteme bei Verfügbarkeit einer Anbindung ausgerollt werden. Die Nutzbarmachung von Cloud für das einsatznahe Umfeld ist also eine wesentliche Grundlage, um IT-Anwendungen zu flexibilisieren. Damit kann die Technologie einen wichtigen Beitrag zur Reaktionsgeschwindigkeit und damit Wirkungsüberlegenheit der deutschen Streitkräfte leisten.

Von Sicherheit bis Autarkiefähigkeit

Das Potenzial von Cloud-Computing ist groß, die Anforderungen der Bundeswehr ebenso, insbesondere in puncto Informationssicherheit und Datenschutz. Vor allem, wenn die Cloud den Schutz von vertraulichen oder gar geheimen Informationen sicherstellen muss. Hinzu kommen Interoperabilität, Verlege- und Autarkiefähigkeit: Eine Cloud-Lösung der Bundeswehr muss interoperabel sein. Das heißt, sie muss mit anderen Systemen zusammenarbeiten können. Dafür muss sie Standards von nationalen und internationalen Cloud-Initiativen erfüllen, wie zum Beispiel der „Deutschen Verwaltungscloud-Strategie“, um die Integrationsfähigkeit von externen Anwendungen oder Infrastrukturen



Geschützführer in einer Panzerhaubitze 2000

Foto: Bundeswehr/Marco Dorow

im Bereich des Bundes, der Europäischen Union oder der NATO, sicherstellen zu können. Darüber hinaus gilt die Informations- und Kommunikationstechnik der Bundeswehr als Kritische Infrastruktur, die im Krisenfall über Monate weiter betrieben werden muss – unabhängig von Interessen oder wirtschaftlicher Lage kommerzieller Anbieter.

Zu Sicherheit, Interoperabilität und Souveränität kommen als Anforderungen Verfügbarkeit, Durchhaltefähigkeit und Ausfallsicherheit dazu, insbesondere im Einsatz. Cloud-Plattformen müssen auch dann unterbrechungsfrei funktionieren, wenn ein Arbeitsplatz nicht permanent mit dem Internet verbunden ist, wie beispielsweise an Bord eines Schiffes oder in Einsatzgebieten mit eingeschränkter Konnektivität. Und schließlich muss die Bundeswehr in der Cloud unterschiedliche Sicherheitsdomänen abbilden: von „OFFEN“ bis „GEHEIM“ beziehungsweise deren multinationale Pendanten, wie beispielsweise „NATO SECRET“. Das erfordert eine Multi-Security-Domain-Architektur, mit der Daten unterschiedlicher Schutzklassen in unterschiedlichen Sicherheitsdomänen getrennt voneinander verarbeitet werden können, ohne für jede Domäne eigene Hardware mit Strom- und Klimaversorgung bereithalten zu müssen.

Die private Cloud der Bundeswehr

Kein kommerzieller Anbieter bietet bis dato eine Lösung an, die die Anforderungen der Bundeswehr erfüllt und zugleich die technologische Souveränität und erforderliche Hoheit über die eigenen Daten vollumfänglich sicherstellt. Daher hat die Bundeswehr die BWI GmbH mit der Entwicklung und dem Aufbau einer privaten Cloud beauftragt: der pCloudBw. Seit Juli letzten Jahres erprobt die BWI die Plattform als betriebsbereites „Minimum Viable Product“. Die erste Anwendung, die sie für die pCloudBw entwickelt und darüber bereitstellen wird, ist das „Krisenvorsorgeinformationssystem Bund“. Mit ihm wird es möglich sein, Lagebilder zu erstellen und ressortübergreifend Maßnahmen zu planen, um deutschen Staatsangehörigen bei Krisen im In- und Ausland zu helfen und sie gegebenenfalls evakuieren zu können.

Die pCloudBw wird das Herzstück der „Multi Cloud der Bundeswehr“ bilden, die darauf abzielt, die Abhängigkeit von einem einzelnen Cloud-Anbieter zu vermindern, die Interoperabilität zu strategischen Partnern sicherzustellen und, auf den jeweiligen Anwendungsfall bezogen, unter Berücksichtigung der operativen Anforderungen, die wirtschaftlichste Lösung zu nutzen. Anwendungen sollen dabei aufwandsarm und unverändert zwischen Laufzeitumgebungen verschoben werden können. In einer ersten Ausbau-



BWI-Logo der pCloudBw

Grafik: BWI GmbH/Xandra Herdieckerhoff

stufe wird die pCloudBw als stationäre Plattform im Inland stehen, mit der Daten verarbeitet werden können, die als VS-NfD („Verschlusssachen – nur für den Dienstgebrauch“) eingestuft sind.

Damit wird die Entwicklung aber noch nicht abgeschlossen sein. Die zukünftige Funktionalität „Verlegefähigkeit“ wird die Bundeswehr in die Lage versetzen, Teile ihrer privaten Cloud vor Ort in Einsatzgebieten zu betreiben. Auch die Verarbeitung von Daten, die einen höheren Geheimhaltungsgrad als VS-NfD haben, ist bereits geplant. Neben Entwicklung und Betrieb der pCloudBw wird die BWI Aufgaben eines sogenannten „Cloud-Brokers“ übernehmen. Als solcher wird es ihre Aufgabe sein, die Bundeswehr bei Anforderungen an externe Anbieter von Cloudservices zu unterstützen, Vorgaben zu formulieren und deren Einhaltung zu überwachen sowie als zentraler Eingangskanal zu fungieren.

Mehr als nur eine Plattform

Die pCloudBw wird einen wesentlichen Beitrag dazu leisten, das IT-System der Bundeswehr leistungsfähiger, sicherer, adaptiver und somit resilienter und widerstandsfähiger zu machen. Mit ihrer Cloud-First-Strategie verpflichtet sich die BWI daher, neue Anwendungen so zu entwickeln, dass sie sich für die Cloud eignen. Für die BWI ist Cloud damit mehr als nur eine Technologie. Sie ist Teil ihrer strategischen Weiterentwicklung und ihres Leistungsversprechens als primärer Digitalisierungspartner der Bundeswehr in Frieden, Krise und Krieg.



Teamwork in der Sahelzone: Angehörige von Bundeswehr und BWI verladen Arbeitsmaterial am militärischen Teil des Flughafens Niamey (Niger).

Foto: BWI GmbH/Dirk Beckert

BWI International, Mission & Training: IT-Unterstützung für Einsätze und Übungen

Alexander Behrends, Leiter Military IT bei BWI International, Mission & Training



Alexander Behrends

Foto: BWI GmbH/Roland Seifert

Murnau, im März 2024: Bei 2 Grad Celsius beginnt an diesem Morgen um 7 Uhr der Dienst für etwa 150 Angehörige der Bundeswehr. Im Rahmen des Vorhabens GELBER MERKUR 2024 – einer jährlichen Schwerpunktübung des Kommando Cyber- und Informationsraum (Kdo CIR) und der IT-Bataillone der Bundeswehr – trainieren sie die Einsatztauglichkeit von IT-Systemen und -Verfahren. An der Seite der

Soldatinnen und Soldaten: vier Mitarbeiter von BWI IM&T. Da bei der Übung GELBER MERKUR insbesondere auch die Betriebsführung geprobt wird, unterstützen die IM&T-Mitarbeitenden vor Ort im Service Desk und im Security Operations Center sowie bei der Auswertung der Betriebsführungsanteile. Mit eigener Ausrüstung begleiten sie die Soldaten zudem beim Üben des regelmäßigen Verlegens von Gefechtsständen. Im Ernstfall muss dies schnell und reibungslos ablaufen, weshalb es die Bundeswehr im Rahmen von GELBER MERKUR intensiv übt – zu jeder Tages- und Nachtzeit. Wann immer BWI-Mitarbeitende Gelegenheit haben, die Bundeswehr bei ihren Übungen zu begleiten, und dabei – mit Ausnahme vom Waffeneinsatz – auch direkt eingebunden sind, erfahren sie aus erster Hand, wie sie als primärer Digitalisierungspartner die Bundeswehr am besten unterstützen können. Viele der rund 50 Mitarbeitenden bei IM&T kennen

die Bedarfe der Bundeswehr auch daher so gut, weil sie über einen eigenen Bundeswehrhintergrund verfügen – beispielsweise als ehemalige Zeitsoldaten. Für ihre Arbeit bei der BWI bringen sie daher oft auch Erfahrungen und Expertise aus früheren Verwendungen im Ausland mit. Ein Glücksfall für die BWI, die mit IM&T IT-Unterstützung bei Einsätzen und Übungen für die Bundeswehr leistet, die seit mehreren Jahren über das Inland hinausgeht.

Pristina 2018+: Der erste Schritt der BWI in die Welt der Auslandseinsätze

Im Projekt ‚Pristina 2018+‘ hat die BWI vor über fünf Jahren den IT-Betrieb für das deutsche Kontingent der Kosovo Force (KFOR) übernommen und damit ihr Engagement um die Unterstützung von Auslands- und Einsatzliegenschaften der Bundeswehr erweitert. Die Betriebsleistung in Pristina basiert auf einer einzigartigen Kooperation: Von Deutschland aus verantwortet, überwacht und steuert die BWI unter Koordination von IM&T den Betrieb, während die Umsetzung vor Ort durch die im Kosovo stationierten IT-Kräfte der Bundeswehr erfolgt. Lediglich für umfangreichere Maßnahmen vor Ort reisen Mitarbeiter von IM&T temporär an. Die Leistung der BWI umfasst die Netzwerkanbindung – von der Telefonie über Arbeitsplatzendgeräte bis zur Bereitstellung von Verschlüsselungskomponenten. Bis heute hat sich daraus eine stabile Betriebsleistung etabliert, in deren Zentrum die BWI alle notwendigen IT-Komponenten für die Anbindung der Liegenschaft Pristina an das IT-System der Bundeswehr in Deutschland bereitstellt.

Personelle Entlastung – mitten im Einsatzgebiet

Bei Verpflichtungen der Bundeswehr im multinationalen Verbund zählt ein stabiles IT-System zu den zentralen Voraussetzungen für ein erfolgreiches Bestehen im Einsatz. Seit März 2022 hat IM&T mit seinem Team MISSION den Auftrag, das militärische IT-Fachpersonal des Kdo CIR in Niamey (Niger) personell zu entlasten. Mitten im Einsatzgebiet – am militärischen Teil des Flughafens von Niamey – betreibt das deutsche Einsatzkontingent im Rahmen des EUMPM-Einsatzes der Europäischen Union einen Lufttransportstützpunkt. Zur Entlastung des MINUSMA-Einsatzes im benachbarten Mali fungierte er als Drehkreuz zum Verwundeten-, Personen- und Materialtransport sowie darüber hinaus zur Zwischenlagerung beziehungsweise zum Weitertransport von Material im Zuge der Rückverlegung nach Deutschland.

Bei in der Sahelzone herrschenden Außentemperaturen von durchschnittlich über 40 Grad Celsius und einer Luftfeuchtigkeit von über 40 Prozent sind die IM&T-Mitarbeiter in einem Feldlager von der Größe eines Fußballfelds untergebracht. Zusätzlich halten die wochenlange Trennung von Familie und Freunden sowie die Unterbringung im kargen Wohncontainer besondere Herausforderungen für sie bereit. Um den stabilen Betrieb, die reibungslos laufende Anbindung von IT, Telefonie und Satellitenkommunikation sowie darüber hinaus die Gesundheit ihrer Mitarbeitenden sicherzustellen, investiert die BWI viel in ihre Vorbereitung auf fordernde Missionen fernab von ‚Büro-IT‘.



An der Seite der Bundeswehr: Bei der Begleitung von Bundeswehrübungen – hier auf dem Truppenübungsplatz Wildflecken (Bayern) – erfahren IM&T Mitarbeitende aus Erster Hand, womit sie als IT-Dienstleister die Bundeswehr am besten unterstützen können.

Foto: BWI GmbH/Peter Clemens

IT-Training sowie mentales und interkulturelles Know-how zur Vorbereitung

Bevor sie in Niamey das IT-Personal der Bundeswehr entlasten konnten, haben die Mitarbeiter von IM&T MISSION eine mehrwöchige Ausbildung in der Administration von einsatznaher IT durchlaufen. Die Inhalte dieser IT-Trainings wurden in bewährtem Team Play mit dem Ausbildungszentrum CIR speziell für die Mitarbeiter der BWI konfiguriert. Während des Einsatzes in einem Konfliktgebiet muss nicht nur das technische Know-how stimmen: Infolge des Militärputsches Anfang August 2023 in Niger und aufgrund der sich rapide verschlechternden Sicherheitslage mussten IM&T-Mitarbeiter zusammen mit zahlreichen weiteren Zivilisten schnellstmöglich das Land verlassen. Ihre Evakuierung gelang dank der professionellen Zusammenarbeit von Frankreich und Deutschland reibungslos. Wie alle Mitarbeitenden der BWI, die in Risikoländern eingesetzt werden, hatten auch diese Kollegen zuvor das Hostile Environment Awareness Training (HEAT) absolviert. Während dieses Kurses trainieren die Teilnehmenden den ‚Ernstfall‘, üben Maßnahmen der Evakuierung und das optimale Verhalten unter Kampfmittelbedrohung, Geiselnahme oder Beschuss anhand simulierter Szenarien. Mit einem Basisrüstzeug an interkulturellen Kompetenzen wappnet darüber hinaus die einsatzlandspezifische Ausbildung (ELSA) der Bundeswehr militärisches wie ziviles Personal für ihre internationalen Einsätze.

Im Gegenzug bietet auch die BWI im Auftrag der Bundeswehr IT-Schulungen für Einsätze und Übungen. Seit 2020 betreibt IM&T das IT-Trainingscenter der Bundeswehr (IT-TCBw) im niedersächsischen Bergen-Lohheide. In unmittelbarer Nähe zu großen Bundeswehr-Standorten wie Munster, Bergen und Faßberg können Truppenteile der Bundeswehr fähigkeitsübergreifend beim Zusammenstellen und Testen von IT-Services für Einsätze und Übungen unterstützt werden. Zusätzlich können in derzeit sechs Hörsälen sowie im Außenbereich des IT-TCBw durch die BWI bis zu 90 Personen zeitgleich beispielsweise in IT-Betriebsführung oder der

einsatz- und übungsspezifischen Zusammenstellung von IT-Servicepackages teambasiert unterrichtet werden.

Logistik und IT-Infrastruktur für die Übung Air Defender 2023

Ihre Expertise im logistischen Bereich konnte die BWI bei der internationalen Großübung Air Defender 2023 unter Beweis stellen: Rund 10.000 Soldatinnen und Soldaten aus 25 Nationen nahmen mit 250 Flugzeugen daran teil und trainierten bei der bislang größten Luftkampfübung seit Bestehen der NATO unter Führung der Luftwaffe verschiedene Übungsszenarien. Die erforderliche temporäre IT-Infrastruktur hatte die BWI unter der Koordination von IM&T bereitgestellt, dazu über Monate eng mit der Luftwaffe zusammengearbeitet und unter anderem in Kropp (Schleswig-Holstein) ein komplettes Containerdorf mit IT ausgestattet.

Mit dem Bereitstellen von etwa

500 Endgeräten sowie 30 aktiven Komponenten aus dem IM&T-Hardware-Pool, dem Inbetriebnehmen von Kommunikationsnetzen sowie Einbinden und Beteiligen zahlreicher BWI-Services beim Aufbau konnte IM&T für den Air Defender 2023 ein Support-Paket schnüren und darüber hinaus dem Dauerthema ‚Materialknappheit bei der Bundeswehr‘ beispielhaft mit einem eigenen liefer- und leistungsfähigen Pool an Hardware begegnen.

Gemeinsames NATO-Ausbildungsprojekt von Bundeswehr und BWI

Seit Ende 2017 wird im Joint Logistic Support Group Coordination and Training Center (JCTC) an der Logistikschiele der Bundeswehr in Osterholz-Scharmbeck (bei Bremen) logistisches Personal der NATO geschult. Bundeswehr und

BWI haben dafür in einem gemeinschaftlichen Projekt ein lokales Übungsnetzwerk aufgebaut, das die Verbindung von 150 IT-Arbeitsplätzen vor Ort sowie variable Zuschaltungen von bis zu weiteren 30 IT-Arbeitsplätzen von externen Standorten ermöglicht. Im Mittelpunkt der Einrichtung steht die Ausbildung von Logistikabläufen an den IT-Produkten der NATO.

Die Einrichtung wurde von Beginn an in Zusammenarbeit von Bundeswehr und BWI aufgebaut. Nach seiner Fertigstellung übergab die BWI das Übungsnetzwerk an die Bundeswehr, die den Betrieb verantwortet. Auch dabei steht

die BWI der Bundeswehr in einem föderalen Modell unterstützend zur Seite. Die Aufgaben für den Betrieb von IT-Komponenten sowie die Beiträge zur Vorbereitung einer Übung sind dafür klar zwischen der Bundeswehr und der BWI aufgeteilt.

Derzeit wird die IT-Infrastruktur des JCTC ertüchtigt, um künftig Übungen bis



Das Handlungs-Portfolio der BWI-Einheit International, Mission & Training (IM&T)

Grafik: BWI GmbH/Markus Albring

zu einer Sicherheitsdomäne NATO-Secret unterstützen zu können. Der Aufbau und die Inbetriebnahme wird durch das Programm ‚German Mission Network‘ begleitet und durch Mitarbeitende von IM&T vor Ort ausgeführt. Durch ihre Beteiligung und die gemeinsame Arbeit an diesem Projekt zieht die BWI bereits heute wertvolle Parallelen zu einem künftigen Bedarf an verlegefähigen Rechenzentren.

Auch wenn dies noch Zukunftsmusik ist – das Engagement in Einsätzen und Übungen kann die BWI einmal mehr dazu nutzen, ihren Erfahrungsschatz zu erweitern. Dabei gilt es gleichzeitig, für eine Förderung der Kriegstüchtigkeit der Bundeswehr dieses neu hinzugewonnene Know-how in geeigneter Weise auch wieder an die Soldatinnen und Soldaten weiterzugeben.

Wege zur IT-Instandhaltung im Felde

Auf der AFCEA-Messe zeigen Branchengrößen ihre aktuellen, rüstungsnahen Informationstechnologien und stellen Trends und Innovationen vor. Bei all der Abhängigkeit der modernen Gefechtsführung von IT möchte die infodas auf das präsente Risiko des IT-Ausfalls eingehen. Verfügbarkeit ist nicht nur ein Thema der IT-Sicherheit, sondern auch für die Instandsetzung im Feld. Und sie betrifft nicht nur Führungsinformationssysteme, sondern auch weitere elektronische Komponenten in landgebundenen Waffensystemen. Ein IT-bzw. Elektronik-Ausfall stellt die strategisch-taktischen Axiome der vernetzten Operationsführung infrage und gefährdet das Erreichen militärischer Ziele. Aber noch mehr kann es zum Verlust von Material und – viel tragischer – zum Verlust von Menschenleben führen.

Im Rahmen von Outsourcing durch finanzielle Anreize und der Knappheit von hoch qualifiziertem Fachpersonal wird die Instandhaltung verstärkt in die Hände der Industrie oder Inhouse-Gesellschaften verlagert. Doch eine vertragliche Verpflichtung, dass sich Industriepersonal den aktiven Kriegsrisiken aussetzt, gestaltet sich juristisch schwierig. Wie kann man nun Soldaten als Systembedienende oder Instandsetzende dazu befähigen, bei IT-Ausfällen Abhilfe zu verschaffen? Die Antwort liegt in der IT selbst: Intelligente und vernetzte Diagnosesysteme helfen bei der frühzeitigen Erkennung, Eingrenzung und Behebung von Fehlern innerhalb des Waffensystems. Eine systeminterne Vernetzung bietet bei sorgfältiger Architekturplanung mehr Chancen als Risiken – und schafft eine interne Prüfmöglichkeit. An Bord von Waffensystemen können gemäß der Fehlerbilder automatisierte Rückfallsysteme aktiv werden und Soldaten Handlungshinweise erhalten. Parallel dazu sollten für Instandsetzungspersonal IT-Systeme bereitstehen, die idealerweise nicht an Schadensereignissen teilgenommen haben und über externe Schnittstellen Prüfungen an komplexen IT-Systemen ermöglichen. Ein Vorbild dafür ist die international etablierte On-Board-Diagnose (OBD) im zivilen Kraftfahrzeugbereich oder die in Heeresverbänden bzw. der Zentrallogistik eingesetzte Offline-Systemprüfung für das Führungsinformationssystem des Heeres.

Für die Vernetzung der elektronischen Komponenten gibt es Vordenker für landgebundene Waffensysteme: Mit dem NATO-Standard AEP-4754 „NATO Generic Vehicle Architecture (NGAV) for Land Systems“ gibt es einen umfangreichen Ansatz, wie elektronische Komponenten untereinander kommunizieren können und gemeinsame Ressourcen verwenden. Mit dem „Watchdog Pattern“ – einem Datenmuster zur Überwachung von Systemzuständen – ist es möglich, dass die Diagnosedaten der Eigendiagnose von IT-Geräten über den Data Distribution Service (DDS) auf dem internen Monitoring-System NGAV-HUMS



(NGVA Health and Usage Monitoring System) dargestellt werden. Im feldmäßigen Instandsetzungspunkt benötigt die Truppe den Zugriff auf diese Daten über ein fahrzeug-unabhängiges Prüfsystem. Nicht immer ist gewährleistet, dass das fahrzeugspezifische Monitoring-System einen Einsatz schadlos überstanden hat. Ein weiterer Vorteil ist, dass ein Diagnosesystem unterschiedliche Fahrzeugtypen bedienen kann, wie es z. B. bei OBD oder der heeres-eigenen Offline-Systemprüfung der Fall ist. Doch was ist, wenn nicht das hochwertige IT-Gerät, sondern nur ein Kabel kaputt ist? Hier unterstützt die externe Systemprüfung mit geeigneten Prüfhilfsmitteln bei der Fehlerlokalisierung. Diese Art der Systemprüfung bietet in Verbindung mit NGAV für die IT-Instandhaltung weitere spannende Ansätze:

- Interne und externe Systemprüfung nähern sich durch Nutzung der NGAV-Schnittstellen einander an, wodurch automatisierte und manuelle Prüfschritte Hand in Hand gehen. Das spart Zeit und Ressourcen, die Einsatzbereitschaft von landgebundenen Waffensystemen wird erhöht.
- Gerätediagnosen können zentral abgerufen werden, Instand setzende müssen nicht direkt am Gerät den Fehler ablesen.
- Die Prüfung der Energieversorgung, Fahrzeugmechanik, Sensoren und Effektoren können in die Diagnose einbezogen werden.
- Bereits ab Werk oder im Truppenverband können Rüstsätze geprüft werden, selbst wenn nicht alle einzurüstenden Geräte vorhanden sind.
- KI wird durch Diagnosedaten befähigt, als Helfer in der Instandsetzung zu fungieren.

Lesen Sie den gesamten Artikel im infodas Blog unter www.infodas.de und informieren Sie sich über das umfassende Produkt- und Beratungsangebot der infodas im Bereich der IT- und Cybersicherheit.

Verfasser: Matti Friedrich, IT Consultant INFODAS GmbH



Security Operations Center der BWI, das „zentrale Nervensystem“ unseres Netzwerks

Foto: Dominik Kraus/BWI GmbH

Der Cyber-Schutz-Schild der Bw – Datenintegrität und Informationsüberlegenheit durch ein ganzheitliches Sicherheitskonzept

Oliver Frommherz, Leiter Competence Center IT-Security, BWI GmbH



Oliver Frommherz

Foto: BWI GmbH/Xandra Herdieckerhoff

Wir befinden uns in einem Informationskrieg mit Russland. Für Auseinandersetzungen im Cyberraum sind detaillierte, umfassende und aktuelle Lagebilder notwendig. Deren zugrundeliegende Daten und Informationen sind essenziell für die Wirkfähigkeit der Bundeswehr im Rahmen der Landes- und Bündnisverteidigung (LV/BV). In der aktuellen Bedrohungslage geraten diese Daten immer stärker ins

Fadenkreuz hybrider Angriffe.

Im Kontext eines datenzentrierten Konflikts (Data Centric Warfare) haben Daten das Potential, Leben zu retten oder zu gefährden, Krisen auszulösen und den Ausgang von Konflikten zu bestimmen. Die daraus resultierenden Folgen umfassen die Destabilisierung demokratischer Strukturen durch Desinformation und gezielte Angriffe auf die Bundeswehr, Bündnispartner und Kritische Infrastrukturen. Dank moderner Schlüsseltechnologien, welche die Massenerfassung, Vernetzung und Übertragung von Daten ermöglichen, kann das Militär von Echtzeit-Lagebildern stark profitieren. Interoperable Schnittstellen und Standards erhöhen hierbei die Geschwindigkeit – ein Ziel, dass die NATO mit dem Federated Mission Network (FMN) weiter ausbaut.

Unsere Zusammenarbeit mit den Partnernationen, sowie durch die BWI-Einheit „International Mission & Training“

und das „Operative Steuerungsgremium (OSG)“, stärkt die Verteidigungsfähigkeit der Ukraine. Diese Kooperationen liefern wertvolle Erkenntnisse für die Cybersicherheit. Ein bedeutendes Beispiel dafür ist die ukrainische Regierung, die kurz vor dem völkerrechtswidrigen Angriff Russlands ihre Systeme und Daten in die Cloud migrierte. Diese Entscheidung erwies sich als kritisch für die Aufrechterhaltung der Handlungsfähigkeit der ukrainischen Streitkräfte, selbst bei Ausfällen in der physischen Infrastruktur. Ein weiterer wichtiger Punkt betrifft die Bedeutung der Informationsüberlegenheit. Das wird auch in Zukunft für die Bundeswehr ein entscheidender Faktor sein. Als Partner in Frieden, Krise und Krieg unterstützen wir die Bundeswehr dabei, Daten, Informationen und Infrastrukturen jederzeit sicherzustellen und bereitzustellen. Eine vollständige und sphärenübergreifende Datenintegrität ist unser bester Schutzschild.

Gemeinsam sicher zur Informationsüberlegenheit

Resiliente Systeme und zukunftssichere Technologien, zusammen mit der Effizienz und Expertise der BWI, spielen im interdisziplinären Zusammenspiel eine entscheidende Rolle. Wir gewährleisten die Sicherheit sämtlicher Liegenschaften sowie der „Network Operations Center“ im In- und Ausland (NOC B.I./B.A.) durch kontinuierliche Systemhärtung sowie durch den Schutz der Daten und Informationen, physischer Systeme und Personen. Dazu zählen auch die Absicherung mobiler Kommunikationssysteme, verlegefähige IT-Netze und robuste Krypto- und Hardshell-Systeme, die extremen Einsatz- und Klimabedingungen standhalten. Diese Systeme und Daten, welche unter anderem für Echtzeit-Lagebilder essenziell sind, erfordern besonders hohen Schutz. ITSysBw dient der einheitlichen Bereitstellung von IT-Strukturen und IT-Service-Management (ITSM). Dabei setzen wir im Sinne der Autarkie auf ein besonders diverses Partner-Ökosystem sowie on-premise-Lösungen wie pCloudBw. Darüber hinaus bietet ITSysBw eine technisch-betriebliche sowie informationssicherheitsrelevante Netzwerküberwachung in Echtzeit und personelle Entlastung der Truppe durch Reachback-Lösungen.

Zentrale Kernaufträge wie German Mission Network (GMN), Digitalisierung Landbasierter Operationen (D-LBO), Federated Mission Network (FMN) sowie angestrebte Multi-Domain-Operations (MDO) erfordern schnelle, verlässliche und akkurate Entscheidungsunterstützung. Diese basiert wiederum auf Analyse komplexer Daten unter Einsatz hochvernetzter KI-Systeme, Smarter Technologie (Internet of Military Things) und Software Defined Defence in einer Cloud-Umgebung, interoperabel in Echtzeit.

Disruptive Technologien und das Defender's Dilemma

Die Einführung innovativer Technologien bringt nicht nur Vorteile, sondern konfrontiert uns auch mit neuen Herausforderungen beim Schutz unserer Systeme. Kriminelle und staatliche Akteure, die mit umfangreichen Ressourcen operieren, nutzen ausgefeilte Methoden wie Phishing und Social Engineering, um unsere Systeme zu kompromittieren.



Mit dem Schutz von Daten und Informationen tragen wir erheblich zur Datenintegrität und Informationsüberlegenheit der Bundeswehr bei.

Foto: Bundeswehr/Jana Neumann

Besonders anfällig in dieser Dynamik ist der menschliche Faktor, der oft als Einfallstor für Cyberangriffe dient. Um dieses Szenario zu unseren Gunsten zu wenden, setzen wir auf umfassende Sensibilisierungsmaßnahmen. Durch zielgerichtete und kreative Aufklärungskampagnen stärken wir das Sicherheitsbewusstsein unserer Nutzerinnen und Nutzer, die somit zu einer ersten Verteidigungslinie gegen Cyberbedrohungen werden.

Digitale Identitäten und datenzentrische Sicherheit

Für stabilen und sicheren Transport von Bundeswehr-Daten zwischen Einsatzorten, Rechenzentren und sonstigen Liegenschaften sorgen SINA-Systeme im Ende-zu-Ende-verschlüsselten und georedundanten WAN23+ Netz. Alle Server-Standorte befinden sich unter deutscher Jurisdiktion und bieten die erforderliche Kapazität für Big Data. Die angemessene Zertifizierung von Hard- und Software gewährleistet zudem den Schutz gespeicherter Daten.

Im Rahmen unserer Data Centric Security (DCS) Strategie legen wir einen besonderen Fokus auf die Datensicherheit während ihrer Verarbeitung. Ein umfangreiches Identity Access Management (IAM) und die dedizierte Vergabe von Zugriffsrechten bilden das Fundament für ein wirksames Monitoring. Unsere Sicherheitsteams in den Security Operations Centern (SOC) und dem Cyber Emergency Response Team (CERT) überwachen Systeme auf potenzielle Bedrohungen und reagieren unverzüglich auf Sicherheitsvorfälle.

Mehr Sicherheit, Zero Trust

Um unbefugten Zugriff auf Daten zu verhindern, setzen wir auf das Zero-Trust-Modell, das von einer konsequenten Überprüfung aller digitaler Identitäten ausgeht. Jeder Zugriffsversuch wird streng kontrolliert, indem die Identität des Anfragenden authentifiziert und die Zugriffsrechte sorgfältig abgewogen werden. Ein solches Vorgehen ermöglicht es uns, die Sicherheit unserer Daten auch vor internen Bedrohungen zu verbessern.

Die Implementierung des Zero-Trust-Modells basiert auf drei Kernprinzipien: die Annahme einer potenziellen Kompromittierung, die Verweigerung impliziten Vertrauens und

die Anwendung des Prinzips der minimalen Rechtevergabe. Diese Herangehensweise erlaubt uns eine effektive und flexible Reaktion auf die dynamische Bedrohungslandschaft im Cyberraum.

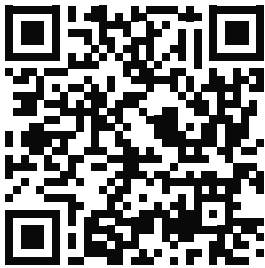
Der „Zero Trust“-Ansatz ist eine Sicherheitsstrategie, die darauf basiert, grundsätzlich keinem Gerät, Benutzer oder Dienst innerhalb oder außerhalb des eigenen Netzwerks zu vertrauen, ohne dass diese eine strenge Verifizierung durchlaufen haben. Anders als traditionelle Sicherheitskonzepte, die alles innerhalb des Netzwerkperimeters als sicher ansehen, geht Zero Trust davon aus, dass Bedrohungen überall existieren können – sowohl innerhalb als auch außerhalb des Netzwerks. Daher erfordert jeder Zugriffsversuch auf Netzwerkressourcen eine Authentifizierung, Autorisierung und kontinuierliche Überprüfung, unabhängig vom Standort des Zugriffs. Der Ansatz zielt darauf ab, die Sicherheit zu erhöhen, indem er die Bewegungsfreiheit eines potenziellen Angreifers innerhalb eines Netzwerks einschränkt und sicherstellt, dass Zugriffsrechte streng nach dem Prinzip der geringsten Berechtigung vergeben werden. Dies reduziert das Risiko von Datenverletzungen und anderen Sicherheitsvorfällen, indem es die Angriffsfläche auf das Netzwerk minimiert und eine detaillierte Überwachung und Kontrolle des Datenverkehrs ermöglicht.

Autark, souverän & interoperabel vernetzt – Softwareentwicklung im Zeichen von Open Source

In der Entwicklung und Gestaltung unserer IT-Architektur setzen wir von Beginn an auf hohe Sicherheitsstandards. Das originäre BWI Softwareentwicklungs-Framework (SWE) wird fortlaufend auf Stand gehalten um den hohen Sicherheitsvorgaben zu genügen. Ein

wesentlicher Bestandteil unserer Softwareentwicklungsstrategie ist hierbei die bevorzugte Nutzung von Open Source Software (OSS).

Bei der Umsetzung dieser Strategie setzen wir ausdrücklich auf die Mitwirkung der Coding Community. Wie verstehen uns als aktiven Teil dieser Gemeinschaft, die auf dem Prinzip des gegenseitigen Gebens und Nehmens basiert und von Austausch mit den Anwendern lebt.



*Wir setzen auf Open Source
Software nach dem Prinzip
„Geben und Nehmen“.*

Code: BWI GmbH

Um unseren Beitrag zum langfristigen Erfolg des Open-Source-Ökosystems zu leisten, engagieren wir uns aktiv in der Szene und teilen unsere Erfahrungen und Erkenntnisse. Ein Beispiel hierfür ist die Bereitstellung des Source Codes des „Bw Messenger“ auf GitLab. Perspektivisch soll unsere GitLab-Datenbank weiter ausgebaut werden.

Security als Teamleistung

Der Spagat zwischen maximaler Informationssicherheit und gleichzeitig konstanter Performance wird in der Softwareentwicklung durch einen DevSecOps-Ansatz erreicht. Durch den Einsatz von Open-Source-Tools wie CNAPP sowie Kubernetes zur Skalierung und Verwaltung von containerisierten Anwendungen ermöglichen wir die flexible Handhabung von Containern und deren Applikationen. Diese Technologien steigern die operative Resilienz durch Ausfallsicherheit und Skalierbarkeit, sowohl für stationäre als auch für mobile Lösungen – unterstützt durch die bevorzugte Nutzung von „Rugged Devices“.

DevSecOps setzt außerdem auf Agilität im Dreiklang von Entwicklung, Sicherheit und Betrieb. Dessen konsequente und automatisierte Implementierung über alle Projekte hinweg soll zusätzliche Awareness, gelebte Sicherheitsstandards und eine Ende-zu-Ende-Verantwortung in den interdisziplinären Teams etablieren.

Ansätze wie DCS, Zero Trust und DevSecOps bedeuten neben großem organisatorischen Aufwand auch kulturellen Wandel. Für die BWI ergibt sich daraus die Intention einer modernen und kooperativen Firmenkultur im Sinne eines „Team of Teams“ als Fundament eines sicheren agilen Betriebs. Soft Skills fördern auch Security-relevantes Networking, etwa Mitgliedschaften in renommierten Insider-Netzwerken wie der AFCEA oder Teilnahme an hochrangigen NATO-Übungen wie TIDE Sprint und Locked Shields.

Sicherheit ist eine übergreifende Aufgabe, die nur gemeinschaftlich funktioniert und in einer Sicherheitskultur verankert wird. Indem wir als BWI-Team resiliente IT-Systeme zur Verfügung stellen, die auf das zentrale Schutzbedürfnis jeglicher Daten und Informationen im Eigenbetrieb sowie im Bundeswehrnetz ausgerichtet sind, gewährleisten wir Korrektheit, Vollständigkeit und Konsistenz – für unsere Informationsüberlegenheit.



BWI Technologie Center prüfen mit Weitblick die Einsatzmöglichkeiten neuer Technologien für die Bundeswehr.

Foto: BWI GmbH/Montage Oliver Kunkel

BWI Technologie Center ebnen Weg für die Bundeswehr-IT von morgen

Matthias Görtz, Chief Technology Officer, BWI GmbH

Der sich immer schneller vollziehende technologische Wandel stellt Unternehmen vor die Herausforderung einer kontinuierlichen Anpassung – technisch, menschlich und organisatorisch. Auch die BWI ist gezwungen, frühzeitig und zielgerichtet auf die nie gekannte Veränderungsgeschwindigkeit zu reagieren. Sie prüft ganzheitlich, welche neuen Technologien sich für die Bundeswehr einsetzen lassen. Einen wesentlichen Beitrag hierzu leisten die neu geschaffenen BWI Technology Centers.



Matthias Görtz

Foto: BWI GmbH/Roland Seifert

BWI Technology Centers steuern technologische Innovationen

Seit August 2023 hat die BWI vier Technology Cen-

ters etabliert, die sich in unterschiedlichen Kompetenzfeldern mit der Technologie-Früherkennung und Technologie-Vorausschau befassen. Die Spanne reicht von Extended Reality über Artificial Intelligence und Cloud, Communications bis hin zu Quantum-Enabled Technologies. Damit wirken die Technology Centers genau in den Feldern, deren neue technologische Lösungen eine Vielzahl von Innovationen in sämtlichen Geschäftsfeldern der BWI prägen werden. Die Centers arbeiten in engem Austausch, mit einem gemeinsamen Ziel: Die Bundeswehr und die BWI zu befähigen, frühzeitig auf bevorstehende technologische Entwicklungen reagieren zu können.

Einsatz von Extended und Virtual Reality von der Ausbildung bis zum Gefechtsfeld

Mit der technologischen Vorausschau sollen die Tech Centers frühzeitig aufkommende Technologien im Bereich Extended und Virtual Reality erkennen und sie auf ihre Eignung für die BWI und Bundeswehr prüfen. Nicht nur im zivilen Bereich finden die fortschreitenden Entwicklungen in der Extended Reality (XR) eine immer breitere Anwendung. Auch

im militärischen Kontext bieten sie großes Potential, die Art und Weise von Training und Arbeitsabläufen der Streitkräfte grundlegend zu verändern.



Der „Virtuelle Mensch“ schafft neue Möglichkeiten in der Bundeswehrausbildung.

Foto: BWI GmbH/Frank Wefers

Eine innovative Trainingsmöglichkeit bietet beispielsweise der „Virtuelle Mensch“, der bereits dieses Jahr zum Einsatz kommen soll. Während bei der Darstellung des Menschlichen in der virtuellen Realität bislang zwischenmenschliche, emotionale, verbale und nonverbale sowie psychologische Aspekte kaum berücksichtigt werden konnten, soll das Projekt eine neue Kommunikation zwischen Menschen und virtuellen Menschen ermöglichen. Damit ergeben sich gänzlich neue Ansätze in der Bundeswehrausbildung, beispielsweise beim Wachdiensttraining. Hier wird bereits ein Prototyp entwickelt, der realistische Animationen, Sprache, Mimik und Gestik besitzt und damit eine realistische und verständliche Interaktion zulässt. So können Soldat*innen beispielsweise den korrekten Umgang mit schwierigen Verhaltensweisen lernen. Auf diese Weise wird das Training wiederholbar und ressourcenschonender. Gleichzeitig werden vollautomatisch messbare Daten zum Blick- und Sprachverhalten gesammelt und zur Verbesserung der Ausbildungsqualität genutzt, die für die spätere Auswertung des Trainings hilfreich sein können.

Mit mehr Einsatznähe setzt die Fernunterstützung im Bereich Telemedizin auf Mixed Reality. Muss beispielsweise eine Sanitätskraft einen nicht-alltäglichen schwierigen Eingriff durchführen, kann per Mixed Reality Brille erfahrenes Medizinpersonal hinzugezogen werden. Durch die Bildübertragung der Brille kann die live zugeschaltete Fachperson von überall auf der Welt Anweisungen geben und sogar 3D-Anmerkungen am Patienten anbringen – für die Handlungsfähigkeit in kritischen Situationen ein enormer Gewinn. Die BWI arbeitet innerhalb der Tech Centers intensiv daran, vielseitige Lösungen weiter voranzutreiben und zu verstetigen. Auch die Künstliche Intelligenz (KI) ist dabei eine Schlüsseltechnologie für Streitkräfte.

Mit Lösungen zur Artificial Intelligence & Cloud am Puls der Zeit

Künstliche Intelligenz beeinflusst schon heute militärische Konflikte. Der Erfolg militärischer Operationen hängt zunehmend auch von den Einsatzmöglichkeiten von KI ab. Auch abseits dessen ist sie ein wichtiges technologisches Innovationsfeld innerhalb der BWI. Daher erforscht die BWI Möglichkeiten intelligenter Systeme für die Bundeswehr, von denen viele bereits im Praxiseinsatz sind, um die digitale Transformation der Bundeswehr voranzutreiben und KI auch in militärische Operationen zu integrieren. Seit dem ersten Quartal 2024 nutzt das Tech Center AI & Cloud dafür sogar ein eigenes KI-Labor.

Das Labor ist unter anderem mit neuartigen, speziell für den KI-Einsatz entwickelten Systemen ausgestattet, mit denen neue Ansätze in der Entwicklung von KI-Architekturen oder -Anwendungen verfolgt werden können, die mit den heute noch üblichen Systemen nur schwer realisierbar sind. Kurz gesagt: Mit einem eigenen KI-Labor ist die BWI in der Lage, auch mit großen und komplexen KI-Modellen eigenständig und souverän zu arbeiten. Für die Zukunft ist die Anschaffung weiterer spezialisierter KI-Systeme geplant, die ganz neue Möglichkeiten für die Evaluierung und Entwicklung von KI-Modellen schaffen sollen. Mit neuer Hardware, dem Aufbau neuer Kompetenzen und der Zusammenarbeit mit KI-Spezialisten macht die BWI in Sachen KI einen großen Schritt nach vorne.

In der Praxis ist Künstliche Intelligenz immer auch auf eine funktionierende Cloud angewiesen. Aus diesem Grund laufen im Technology Center AI & Cloud beide Bereiche sinnvoll zusammen. Im Cloud Computing beschäftigt sich das Technology Center vor allem mit Zero-Trust-Strategien und den damit verbundenen Techniken, wie dem Confidential Computing. Hierbei werden sensible Daten während der Verarbeitung in einer sicheren hardwarebasierten Umgebung geschützt, die eine Verschlüsselung auch in der laufenden Anwendung ermöglicht. Die Daten sind damit nur für autorisierte Personen oder Einheiten zugänglich. Denn um eine KI sicher trainieren und anwenden zu können, muss die komplette Datenkette verschlüsselt werden.



BWI erforscht Einsatzmöglichkeiten von KI für die Bundeswehr.

Foto: Adobe Stock 473509904

Dank der engen Zusammenarbeit auch mit den anderen Tech Centers können Kompetenzen gebündelt und ein breites Wissensspektrum eingebracht werden. Diese Zu-

sammenarbeit als übergreifendes Team macht es möglich, gemeinsam zukunftsfähige Technologie zu identifizieren, zu prüfen und für die Bundeswehr nutzbar zu machen. Was dabei als Grundvoraussetzung alle cyber-physischen Systeme verbindet, ist die Fähigkeit, Daten in großen Mengen sicher und möglichst verzugsfrei zu übertragen. Dazu ist eine funktionierende Netzwerkstruktur unerlässlich.

Keine Kommunikation ohne vernetzte Systeme: Tech Center Communications

Auf dem Gefechtsfeld der Zukunft sind alle militärischen Einheiten und die von ihnen genutzten Waffen- und Einsatzsysteme miteinander vernetzt. Eine große Anzahl von Sensoren, die im Einsatzraum verteilt werden, sammeln vielfältige Informationen und geben diese automatisiert an unterschiedliche verarbeitende Anwendungen weiter. Im nächsten Schritt werden die verarbeiteten Daten dann beispielsweise zur Lagedarstellung verwendet. Eine funktionierende Netzwerk- und Übertragungsinfrastruktur ist dafür essentiell, denn diese ermöglicht erst den Informationsaustausch der Systeme und Akteure untereinander. Doch nicht nur dort, sondern in nahezu allen militärischen Bereichen bilden Kommunikationslösungen die Basis für IT-Services. Das BWI Tech Center Communications befasst sich mit technologischen Neuerungen im Bereich der Kommunikationssysteme. Ziel ist es, sowohl die BWI als auch die Bundeswehr zu befähigen, frühzeitig auf Entwicklungen reagieren zu können. Daher werden aufkommende Übertragungs- und Netzwerktechnologien identifiziert, erschlossen und auf ihre Eignung für den Nutzen im Kontext Bundeswehr bewertet. Damit stellt das Tech Center das unverzichtbare Fundament für Tätigkeiten in allen Technologiegebieten, in denen die BWI für die Bundeswehr tätig ist.

Einen besonderen Fokus legt das Tech Center dabei auf einsatznahe Systeme und prüft, inwieweit kommerzielle Technologien und Lösungen im militärischen Umfeld mit Mehrwert eingesetzt werden und somit zu einer robusten und resilienten Führungsfähigkeit beitragen können.

Hierfür werden innerhalb vorab definierter Suchfelder kontinuierlich neue technologische Entwicklungen im Forschungs- und Entwicklungsumfeld der BWI gesichtet und bei vielversprechenden Themen Nutzungsmöglichkeiten zur Bewältigung künftiger Herausforderungen herausgearbeitet. Innerhalb dieser Innovationspfade bewertet das Team

Einsatzmöglichkeiten, baut Technologiekompetenzen auf und führt initiale experimentelle Erprobungen durch. Bei der Bereitstellung von Kommunikationsinfrastruktur ist es von großer Bedeutung, auch Aspekte wie beispielsweise die Auswirkungen technologischer Neuerungen in der Netzwerk- und Übertragungstechnologie im Blick zu behalten. Hier ist eine enge Zusammenarbeit mit den anderen Technology Centers der BWI unerlässlich, um gemeinsam technologieübergreifende Demonstratoren zu entwickeln und die Bundeswehr ganzheitlich und bestmöglich zu unterstützen.

Mit Quantum Enabled Technologies bereit für den Quantensprung

Ein letztes wichtiges Feld, das angesichts seiner rasanten Entwicklung enorme Auswirkungen auf das BWI- und Bundeswehrumfeld haben wird, sind die Quantentechnologien. Sie revolutionieren die Technologiewelt: Superschnelle Computer, abhörsichere Kommunikation, extrem präzise Sensoren – die Möglichkeiten scheinen grenzenlos. Bereits im Jahr 2030 könnte der erste kryptografisch relevante Quantencomputer einsatzbereit sein. Durch die Verhaltensweisen der Quantenphysik ergeben sich ganz neue Fähigkeiten in der Sensorik und der sicheren Kommunikation: Mit den Quantentechnologien der Generation 2.0 ließen sich beispielsweise U-Boote detektieren oder asymmetrische Verschlüsselungen knacken, die mit heutigen Kryptosystemen noch gesichert sind. In Kampfhandlungen könnten Quantentechnologien so detaillierte Lagebilder liefern, wie es sie bislang noch nicht gab. Um die Verteidigungsfähigkeit des Landes zu erhalten, ist eine frühzeitige und intensivere Vorbereitung unerlässlich. Aus diesem Grund hat die BWI das Technology Center Quantum-Enabled Technologies gegründet, in dem sich Experten auf dem Gebiet intensiv mit Zukunftstechnologien und deren Auswirkungen auf die BWI befassen.

Der Fokus liegt auf den drei Schwerpunkten Quantencomputing, Quantensensorik und quantensichere Kommunikation. Quantencomputer werden zukünftig komplexe, heute noch nicht lösbare Rechenoperationen leisten können. Die Quantensensorik erlaubt zudem extrem genaue Messsysteme, die für Lagebilder genutzt oder in Quantensichtgeräte verbaut werden, mit denen sich gegnerische Kräfte präzise identifizieren lassen. Die quantensichere Kommunikation kümmert sich darüber hinaus um abhörsicheres Kommunizieren und Verschlüsselungsalgorithmen, die nicht von Quantencomputern gehackt werden können.

Unter anderem investiert die BWI schon jetzt in Post-Quanten-Kryptographie (PQC), um die Netze der BWI gegen Angriffe mit Quantencomputern abzusichern. Das gesamte optische Netz, inklusive der wichtigsten Standorte der Bundeswehr, ist bereits auf PQC-Verschlüsselung umgestellt. Parallel zur Einführung der PQC in den Liegenschaften überprüft die BWI die komplette IT-Infrastruktur auf Quantensicherheit. Darauf aufbauend entwickelt sie eine Roadmap ihrer zukünftigen Aktivitäten rund um das Thema Quantentechnologien. Sie steht im Dialog mit Herstellern quantensicherer Produkte und vernetzt sich mit For-



Die BWI bereitet sich schon heute auf künftige Quantentechnologien vor.
Foto: Adobe Stock/Production Perig

schungseinrichtungen. Sollten 2030 tatsächlich die ersten Quantencomputer marktreif sein, ist die BWI vorbereitet – und die IT-Infrastruktur der Bundeswehr ist das auch.

Zwischen State-of-the-Art und Zukunftsszenarien: gewappnet für das technologische Morgen

Mit den Tech Centers stellt die BWI schon heute die Weichen für die Technologie von morgen. Dabei arbeitet sie fachbereichs- und themenübergreifend von KI bis Quantentechnologie und bewahrt den Weitblick für langfristige technologische Perspektiven. Die BWI Tech Centers ebnen potentiellen künftigen Leistungsangeboten für die Bundes-

wehr den Weg. Damit hilft die BWI der Bundeswehr frühzeitig und gezielt dabei, dem rasanten technologischen Wandel standzuhalten, anpassungsfähig zu bleiben und handlungsfähig zu werden.

ADVERTORIAL

Intelligent Network Analyzer (INA) sorgt für gut geölte Beschaffung

Die MRO-Prozesse (Maintenance, Repair and Operations) der Streitkräfte gleichen weitverzweigten Netzwerken. Sie zu optimieren, funktioniert nur mithilfe von Technologie, je intelligenter und rechenstärker, desto besser. Eine Digital-Twin-Lösung von Sopra Steria nutzt Quantentechnologie für Optimierungsaufgaben.

Der Intelligent Network Analyzer (INA) basiert auf Azure-Quantum-Technologie und hilft derzeit, die Zuverlässigkeit und Energieeffizienz eines großen Mobilfunknetzes zu steigern. Für klassische Computer ist die Abbildung des Netzes eine große Herausforderung und erfordert viel Rechenzeit. Quantencomputing ermöglicht die parallele Durchführung mehrerer Berechnungen und damit eine Echtzeitanalyse zur Optimierung des Datenverkehrs.

INA eignet sich auch für die hyperkomplexen MRO-Prozesse der Bundeswehr. Die Lieferketten sind stark diversifiziert. Entstanden sind vielschichtige Versorgungsnetzwerke. Die aktuelle geopolitische Lage, aber auch Pandemien wirken sich massiv auf die Zuverlässigkeit der Lieferkette aus. Die Lösung entpuppt sich hier als wertvolle Gehilfin, denn sie ermöglicht eine schnelle Analyse von Abhängigkeiten im Netzwerk. Ausfallsicherheit, Zuverlässigkeit der Beschaffung lassen sich so deutlich verbessern.

Profitieren Sie von intelligenter Netzwerkoptimierung mit eingebauter Quantentechnologie

Sopra Steria begleitet die Streitkräfte der Bundeswehr sowie die Industrie beim Einsatz modernster Technologien. Wir unterstützen mit gezielter Beratung in allen Projektphasen sowie mit eigenen Produkten und Services. Sprechen Sie uns an!



Kontakt:
Thomas Gilles
 Telefon: +49 40 22703-0
 E-Mail: defence.de@soprasteria.com

BWI – Resiliente Leistungserbringung in Frieden, Krise und Krieg

Andreas Bänsch, Account-Direktor einsatznahe IT und Themengebiet LV/BV, BWI GmbH



Andreas Bänsch

Foto: BWI GmbH/Xandra Herdieckerhoff

Seit dem russischen Angriffskrieg auf die Ukraine und der damit verbundenen „Zeitenwende“ hat sich nicht nur in der Bundeswehr der Fokus auf die Landes- und Bündnisverteidigung (LV/BV) verschoben. Auch die BWI wappnet sich, um der Bundeswehr als primärer Digitalisierungspartner nicht nur in Friedenszeiten, sondern auch in Krise und Krieg stabile und sichere IT-Leistungen zur Verfügung zu stellen.

Bei der Erbringung ihrer sicherheitspolitischen Aufgaben ist die Bundeswehr nicht nur auf funktionsfähige militärische Infrastrukturen und geeignetes Personal angewiesen. Für die digitale Transformation zur Erhöhung von Effizienz und Kampfkraft bedarf die Truppe beispielsweise auch der Unterstützung durch externe IT-Dienstleister. Seit ihrer Gründung 2006 stellt die BWI verlässlich einen sicheren und stabilen Betrieb der beauftragten IT-Services 24/7 bereit. Damit leistet sie einen wichtigen Beitrag für die Einsatz- und Führungsfähigkeit der Bundeswehr.

Seit dem 24.2.2022 hat sich der sicherheitspolitische Rahmen in Europa verschoben: Der Beginn des russischen Angriffskriegs auf die Ukraine hat das Thema LV/BV nicht nur wieder bei Politik und Bundeswehr stärker in den Fokus gerückt: Die damit verbundene „Zeitenwende“ hat auch den Rahmen für die Leistungserbringung durch die BWI ausgeweitet. Denn mit Blick auf Quantität und Qualität werden wesentliche Anteile des IT-Systems der Bundeswehr inzwischen durch die BWI bereitgestellt. Unter der veränderten sicherheitspolitischen Großwetterlage leiten sich neue Ansprüche an eine resiliente IT-Leistungserbringung ab: Auch im Kontext hybrider Bedrohungen sowie der LV/BV muss die BWI als primärer Digitalisierungspartner der Bundeswehr den stabilen und sicheren IT-Grundbetrieb durchgängig aufrechterhalten.

Die Aufgaben der BWI im Bündnis- und Verteidigungsfall

Bereits im Grundbetrieb und im Szenario „DrehSchreibe Deutschland“ stellt die BWI die Vernetzung von militärischen Liegenschaften und den Betrieb von Rechenzentren

sicher. Tritt der Fall einer LV/BV ein, errichtet die Bundeswehr mit ihren eigenen IT-Kräften im Operationsgebiet Kernnetze, an welche die verlegefähigen nationalen und multinationalen Führungseinrichtungen angebunden werden. Für ihre Auftragserfüllung ist sie dabei weiterhin auf eine dauerhafte, stabile und sichere IT-Basis im Inland angewiesen. Planungsleitend ist die Aufrechterhaltung aller bestehenden Leistungen. Mit Blick auf eine notwendige Kaltstart- und Aufwuchsfähigkeit verschwimmen dabei die Grenzen zwischen Grundbetrieb und Einsatzbetrieb bei gleichzeitig steigenden Anforderungen an die Resilienz der Leistungserbringung.

„LV/BV by Design“ – So macht sich die BWI für den Ernstfall bereit

Die Herausforderungen, die eine Leistungserbringung insbesondere im Hinblick auf LV/BV mit sich bringen, sind zu umfangreich und komplex, um sich ihnen erst bei tatsächlichem Eintritt zu stellen. Dementsprechend gilt es auch für die BWI, ihre Leistungserbringung möglichst frühzeitig, explizit und integral auch auf derartige Szenarien auszurichten. Mit dem Ansatz „LV/BV by Design“ stellt sie den Wert der Leistungserbringung sowohl in Friedenszeiten als auch in Krise und Krieg und die zugehörige Wertschöpfungskette in den Mittelpunkt der Betrachtung. Hierbei geht es unter anderem darum, den Gedanken der Resilienz bei bestehenden wie künftigen Leistungen stets zu berücksichtigen. Die BWI verfolgt dabei das Ziel, die Resilienz zu erhöhen und gleichzeitig Fähigkeiten aufzubauen, um zusätzliche Anforderungen und Aufgaben in Krise und Krieg erfüllen sowie mit der Aufrechterhaltung und Wiederherstellung aller erforderlicher Leistungen im Kontext von LV/BV nachhaltig bestehen zu können.

Mit einem organisationsweiten Ansatz stellt die BWI sicher, dass sie mit allen IT-Services in ihrer Leistungserbringung auch im Krisen- und Kriegsfall noch resilienter wird. Ausgangspunkt stellt ein stabiler und sicherer Betrieb dar, welcher ständig weiterentwickelt und dessen Resilienz kontinuierlich gesteigert wird.

Leistungserweiterung im Kontext LV/BV

Bereits vor Beginn des Kriegs in der Ukraine hat die BWI mit der kontinuierlichen Erweiterung ihrer Leistungserbringungen für die Bundeswehr begonnen. Mit Blick auf die konkreten Anforderungen aus LV/BV erbringt die BWI bereits heute im Rahmen von Einsätzen und Übungen IT-Leistungen für die Bundeswehr im In- und Ausland mit militärischem Bezug. Für alle diese Leistungen wird die wesentliche Ziel-

setzung verfolgt, die Einsatz- und Führungsfähigkeit und damit auch die Kampfkraft der Truppe kontinuierlich zu verbessern. Trotz der Stellung als Inhouse-Gesellschaft gibt es hier Hürden bei der Leistungserbringung aufgrund der bestehenden Vorschriftenlage im Vergleich mit der Bundeswehr. Mit einfachen Änderungen von Berechtigungen und

Verfahrensweisen könnte hier eine noch bessere und einfachere Unterstützung für die Bundeswehr erfolgen. Insbesondere vor dem Hintergrund, dass die BWI ihre Präsenz im Ausland auch im Zuge der dauerhaften Stationierung einer Brigade in Litauen selbst deutlich verstärken wird.

„Wir brauchen IT-Services, die uns bei Resilienz und Robustheit unterstützen“

Generalleutnant André Bodemann im Interview

Am 31. März hat das Territoriale Führungskommando einen ersten Entwurf des Operationsplans Deutschland vorgelegt. Warum drängt die Zeit dafür?

Spätestens seit dem 24. Februar 2022 ist klar, was der russische Präsident Wladimir Putin beabsichtigt. Wir haben wieder Krieg in Europa, eigentlich schon seit 2014. Deutschland wird bereits heute und jetzt bedroht. Es ist nicht mehr auszuschließen, dass auch wir eines Tages den Ernstfall erleben. Und darauf müssen wir uns so rasch wie möglich vorbereiten. Am Ende müssen wir einen Plan haben, der funktioniert und dabei so glaubwürdig ist, dass er auch abschreckt.

Worum geht es im OPLAN Deutschland?

Deutschland kommt aufgrund seiner geostrategischen Lage eine besondere Rolle bei den Verteidigungsplänen der NATO zu. Wir liegen mitten im Herzen Europas. Die Aufmarschbewegungen der alliierten Kräfte werden größtenteils durch Deutschland erfolgen. Dabei kommt es natürlich auf die verschiedenen Verkehrswege an. Zudem sind die kritischen bzw. verteidigungswichtigen Infrastrukturen von großer Bedeutung. Und außerdem müssen wir als Gastnation die Unterstützung der Truppe selbst im sogenannten Host Nation Support sicherstellen, zum Beispiel während der Rast in den Convoy Support Centern: Da geht es um die Verpflegung, um Frischwasser, die Verfügbarkeit von Kraftstoffen, um Ersatzteile oder auch, wenn nötig, um die sanitätsdienstliche Versorgung. Das alles müssen wir für die alliierten Kräfte sicherstellen.

Kann man dabei auf ältere Pläne zurückgreifen?

Im Kalten Krieg gab es ähnliche Überlegungen. Wir haben aber verschiedene neue Herausforderungen – zum Beispiel die Digitalisierung. Da hat sich die Technologie derartig weiterentwickelt, dass wir hier ganz neue Rahmenbedingungen

und Herausforderungen haben. Auch die Cyberthematik hat es in den 1980er-Jahren so nicht gegeben. Und dann ist Deutschland auch kein Frontstaat mehr. Wir sind auf andere Weise bedroht. Dies sind bereits heute vor allem hybride Bedrohungen. Die Gegenseite wird zum Beispiel alles tun, um diese Bewegung zu hemmen und möglicherweise auch zu verhindern.

Sind wir in Deutschland schon so weit, dass wir Verteidigung als gesamtgesellschaftliche Aufgabe erkannt haben?

Man muss es zweigeteilt sehen. Die Bundesressorts und die Länder arbeiten eng mit uns zusammen. Die Blaulichtorganisationen sind sehr aktiv, weil sie wissen wollen, welche Aufgaben sie übernehmen können oder auch müssen. Auch zivilwirtschaftliche Unternehmen bereiten sich vor und arbeiten eng mit uns zusammen. Wo ich mir noch mehr erhoffe, das ist in der Erkenntnis der Bürgerinnen und Bürger selbst, dass Freiheit und Demokratie nicht zum Nulltarif zu haben sind. Das alles hat seinen Preis, auch im Alltag. Insgesamt glaube ich aber, dass in Deutschland angekommen ist, in welcher Lage wir uns derzeit befinden.

Was kann die BWI tun, um die Bundeswehr bei der Umsetzung des OPLAN Deutschland zu unterstützen?

Gerade bei der Landes- und Bündnisverteidigung ist die BWI als IT-Systemhaus der Bundeswehr ein wichtiger Partner für uns. Wir brauchen IT-Services, die uns bei der Resilienz und der Robustheit unterstützen. Das heißt für mich vor allem, dass es eine Redundanz an Möglichkeiten gibt. Praktisch gesagt: Wenn ein System ausfällt, muss ich andere Möglichkeiten haben, um z. B. die eigene Führungsfähigkeit zu sichern. Die BWI steht uns hier zuverlässig zur Seite.

Generalleutnant André Bodemann ist Befehlshaber des Territorialen Führungskommandos der Bundeswehr und Nationaler Territorialer Befehlshaber.

Cyberresilienz im Teamwork für das digitale Zeitalter

Der Übergang in eine hybride Arbeitswelt mit immer mehr verbundenen Geräten und mobilen Mitarbeitern stellt IT-Abteilungen jeglicher Größenordnung vor beträchtliche Herausforderungen. Das gilt vor allem für das Thema IT-Sicherheit. Doch es gibt flexible Lösungen.

Die Problematik wird in der Studie „State of Cybersecurity 2023“ von Sophos bestätigt. Immerhin glauben 52 Prozent der 3.000 befragten Teilnehmer aus 14 Ländern, dass die Cybergefahren zu fortgeschritten sind, um sie allein bewältigen zu können. Der Bedarf an Cybersecurity as a Service mit skalierbaren, zentral fernverwalteten und agilen Lösungen ist daher enorm, zusätzlich angefeuert durch den eklatanten Fachkräftemangel.

Obwohl der Zugriff auf Daten außerhalb des Büros schon immer mit Risiken verbunden war, hat die Häufigkeit dieser Praxis durch die Digitalisierungs- und Home-Office-Welle die Wahrscheinlichkeit eines erfolgreichen Angriffs und damit die monetären Anreize für Cyberkriminelle enorm erhöht. Zu diesem Ergebnis kommt auch das Bundeskriminalamt, das in seinem „Bundeslagebild Cybercrime“ im August 2023 Ransomware weiterhin als primäre Bedrohung für Unternehmen und öffentliche Einrichtungen definiert.

Es geht darum, Cyberangriffe so früh wie möglich zu entdecken

Als Antwort auf diese Entwicklung starten viele Organisationen aus dem öffentlichen Bereich konzertierte Anstrengungen, um ihre Abwehrmaßnahmen als Reaktion auf die hybride Arbeitswelt zu erweitern und zu synchronisieren. Dabei entsteht aktuell eine Verlagerung des grundsätzlichen Ziels beim Erstellen einer Cybersecurity-Strategie: Es geht nicht mehr primär darum, Bedrohungen nach dem Entdecken unschädlich zu machen. Das neue Hauptziel ist, Bedrohungen so früh wie möglich in der Angriffskette zu stoppen, idealerweise bevor der Angreifer überhaupt umfänglich in Systeme eindringt. Die Schwierigkeit besteht darin, die Signale eines potenziellen Angriffs zu erkennen – laut der State-of-Cybersecurity-Studie sehen 59 Prozent der in Deutschland Befragten genau darin ein Problem. Doch es kann geholfen werden. Mittlerweile können speziell ausgebildete und international vernetzte Experten durch gezielte Bedrohungssuche mit Hilfe von Künstlicher Intelligenz Lücken oder Schwachstellen frühzeitig identifizieren und schließen, bevor ein Angreifer sie ausnutzen kann – kurz Managed Detection and Response.

So bekannt das Problem, so aufwändig und schwierig ist allerdings die Lösung, da die Implementierung eines umfassenden Cybersecurity-Ökosystems zwei maßgeb-

liche Komponenten benötigt: die vernetzte und intelligente Kontrolle aller Endgeräte, Server und Netzwerke eines Unternehmens sowie die Unterstützung durch erfahrene Cybersecurity-Experten, die aus Kosten und Verfügbarkeitsgründen nur die wenigsten Einrichtungen intern vorhalten können.

Dass diese Grundpfeiler für eine moderne Cybersecurity-Strategie oftmals noch Fehlanzeige sind, ist besonders besorgniserregend, wenn man bedenkt, dass 93 Prozent der Organisationen laut der Sophos-Umfrage „State of Cybersecurity“ die Durchführung wesentlicher Sicherheitsmaßnahmen bereits als Herausforderung empfinden. Darüber hinaus sagen über die Hälfte der befragten IT-Verantwortlichen, dass Cyberbedrohungen mittlerweile zu weit fortgeschritten sind, um sie allein bewältigen zu können – eine ernüchternde Wahrheit.

Wie Unternehmen von Cybersecurity as a Service profitieren können

Die Lösung bietet sich in Form eines Cybersecurity-as-a-Service-Modells (CSaaS) in Kombination mit einem intelligenten Cybersecurity-Ökosystem an. In diesem Ökosystem kommunizieren alle relevanten Elemente, vom Endpoint bis zur Firewall, wodurch sowohl Prozesse automatisiert werden als auch ein großer Data Lake entsteht. Die Größe und der Umfang dieses Data Lake ist entscheidend, denn durch ihn ist die Analyse der Telemetriedaten nicht nur erheblich vereinfacht, sondern im Prinzip überhaupt erst möglich. So haben Organisationen mit einem adaptiven Cybersecurity-Ökosystem in Kombination mit einem MDR-Service (Managed Detection and Response) eine flexible Möglichkeit, ihre Sicherheitsabläufe zukunftssicher zu gestalten und gleichzeitig eine starke Cyberresilienz aufzubauen.

Sophos, das mit seinem MDR-Service unter anderem vom BSI als qualifizierter Dienstleister im Bereich APT geführt wird, bietet genau diesen Lösungsansatz an. Lernen Sie das komplette Cybersecurity-Ökosystem mit Schutzfunktion vom Endpoint über Server bis zum Netzwerk aus einer Hand im **Saal New York/Genf an unserem Stand S 62** kennen.

SOPHOS

Resilienz durch gute Partnerschaften

Katrin Hahn, Chief Resources Officer, Mitglied der Geschäftsführung, BWI GmbH



Katrin Hahn

Foto: BWI GmbH/Xandra Herdieckerhoff

Durch die Digitalisierung ist die Welt nicht nur schneller, sondern auch komplexer geworden. Wir spüren das selbst jeden Tag – der Rhythmus, in dem wir mit neuen Informationen konfrontiert werden, hat seit der Erfindung des Smartphones drastisch zugenommen. Gleichzeitig müssen wir in immer kürzerer Zeit immer mehr Entscheidungen treffen. Auch solche, die künftig für uns eine große

Bedeutung haben werden. Im militärischen Bereich ist das nicht viel anders: Digitale Technologien haben nicht nur das Gefechtsfeld gläsern gemacht. Die Menge an Daten, die heute verfügbar ist, hat auch dazu geführt, Entscheidungsprozesse zu beschleunigen. Die Anforderungen für die IT-Dienstleistungen, die von der BWI für die Bundeswehr erbracht werden, hat sich dadurch erhöht.

Umso wichtiger ist es, dass die BWI als primärer Digitalisierungspartner der Bundeswehr in Frieden, Krise und Krieg auch über ein gut aufgestelltes Partner-Ökosystem verfügt, das uns bei dieser Aufgabe unterstützt. Uns stehen dabei zahlreiche Modelle der Kooperation zur Verfügung, die unterschiedlich eng ausfallen können – vom inhaltlichen Austausch bis hin zur institutionellen Zusammenarbeit. Das Spektrum ist also weit gefasst, und damit auch die Möglichkeiten, die sich daraus ergeben. Für Kooperationen ist uns generell wichtig, dass ein Nutzen für alle beteiligten Partner entsteht, eine verbindliche und belastbare Zusammenarbeit etabliert wird und eine hohe Umsetzungsorientierung und gemeinsame Perspektiven sichergestellt werden.

Kooperationen als zentrales Instrument

Für alle Formen von Kooperationen gilt: Sie sind für uns ein zentrales Instrument, um die Anforderungen unserer Kunden zu erfüllen und damit ihre digitale Transformation zu unterstützen. Um Mehrwerte für unsere Kunden zu schaffen und die Integration von Markt-Know-How sicherzustellen, sucht die BWI starke Partner für Teile ihrer Leistungserbringung im partnerschaftlichen Dreiklang aus Bundeswehr, BWI und Industrie.

Der russische Überfall auf die Ukraine im Februar 2022 und die Zeitenwende in der deutschen Sicherheitspolitik haben darüber hinaus den Fokus auf einen anderen Aspekt erweitert, den ein gut aufgestelltes Partner-Ökosystem bietet: den der Resilienz gegenüber den immer komplexeren

Aufgaben der Gegenwart. Nur mit den passenden Partnern wird es der BWI gelingen, die Ansprüche an die Lieferung von Services auch zu erfüllen.

Zugang zu Innovationswissen

Resiliente Partner helfen uns, den sich immer schneller verändernden Herausforderungen zeitnah zu begegnen. Sie machen uns damit selbst auch widerstandsfähiger gegenüber den Aufgaben, mit denen wir uns beschäftigen. In einer Zeit, die in Deutschland durch Fachkräftemangel geprägt ist, verschaffen sie uns auch dringend benötigte Ressourcen.

Die Frage, welchen Nutzen man von einem Partner-Ökosystem hat, reicht jedoch viel weiter. Es geht nicht nur um materielle Ressourcen oder moderne Technologien, von denen man direkt profitieren kann – sondern auch um den Zugang zu Innovationswissen. Die Art und Weise, wie neue Ideen in Unternehmen entwickelt werden, hat sich in den vergangenen Jahren radikal verändert. Resilienz misst sich daher auch darin, welchen Zugang man zu den sich ständig erneuernden Innovationsströmen hat.



Die BWI kann sich auf ein gut aufgestelltes Partner-Ökosystem bei der Arbeit als primärer Digitalisierungspartner der Bundeswehr verlassen.

Foto: BWI GmbH/Frank Löschke

Schnellere Lernprozesse durch Digitalisierung

Denn die Digitalisierung hat nicht nur das Tempo erhöht, mit der Innovationen auf den Markt kommen. Sie hat auch die Art und Weise verändert, wie an Innovationen gearbeitet wird. Während Hardware-basierte Innovationen früher über einen langen Zeitraum erforscht und erprobt werden mussten, wird Software in agilen Lernprozessen fortentwickelt. Die Fähigkeit, im virtuellen Raum schnell aus den eigenen Erfahrungen lernen zu können, sorgt für kürzer werdende Intervalle, in denen Innovationen verfügbar sind. Gleichzeitig

sind dafür auch weniger Ressourcen nötig, als dies früher der Fall war. Bahnbrechende technologische Neuerungen können heute auch von Start-ups generiert werden.

Diese Entwicklung hat natürlich auch Auswirkungen auf das Militär. Noch vor einigen Jahrzehnten sorgte die staatlich geförderte Forschung an militärischen Projekten für technologische Impulse, die später von der zivilen Welt aufgenommen wurden. Das von der US Air Force im Jahr 1968 initiierte Advanced Research Projects Agency Network (ARPA) war das erste dezentrale Rechnernetzwerk und gilt heute als der Vorläufer des modernen Internets. Mittlerweile hat sich die Richtung geändert, in der Innovationen fließen: Technologien der Künstlichen Intelligenz, Instrumente zur Datenverarbeitung oder Cloud-basierte Anwendungen werden heute zuerst von privaten Unternehmen entwickelt und später für die Bedürfnisse des Militärs angepasst.

Digitale Souveränität

Diese Entwicklungen möglichst frühzeitig zu erkennen und aufnehmen zu können, ist deshalb auch für uns von immenser Bedeutung. Um der Truppe wirkungsvoll zur Seite stehen zu können, brauchen wir ein Partner-Ökosystem, das diesen Technologietransfer leisten kann.

Ein weiterer Aspekt ist die digitale Souveränität. Um in einer digitalen Welt unseren Auftrag selbstständig, selbstbestimmt und sicher ausüben zu können, müssen wir uns unabhängig(er) von einzelnen Anbietern und Produkten ma-

chen und unsere Resilienz durch die Austauschbarkeit von Komponenten zu erhöhen.

Digitale Souveränität ist vor dem Hintergrund multipler Krisensituationen mehr denn je ein zentraler Maßstab für staatliche Organisationen. Ihre Umsetzung funktioniert nur im Zusammenspiel verschiedener Akteure, dem Austausch von Wissen und der gemeinsamen Entwicklung von neuen Lösungswegen. Das BWI Partner-Ökosystem ist daher zentral, um die Schlüsselkompetenz der BWI für robuste und sichere IT-Systeme sicherzustellen und weiter auszuprägen.

Beide Seiten profitieren

Nur so erreichen wir Aufbau und Erhalt der notwendigen Fähigkeiten, zum Beispiel zur Beurteilung und Anwendung von Schlüsseltechnologien wie KI, Quantencomputing, IT-Sicherheit, Blockchain/DLT und Digitale Identitäten.

Bleibt die Frage: Was haben die Partner selbst davon? Zum einen leisten sie einen Beitrag dafür, die Bundeswehr in einer sicherheitspolitisch herausfordernden Situation fit für die Zukunft zu machen. Resiliente Streitkräfte, davon sind wir überzeugt, sind für die Zukunft dieses Landes ein Wert für sich. Die gestiegene Bedeutung der Landes- und Bündnisverteidigung eröffnet jedoch auch wirtschaftliche Chancen: Denn in Zusammenarbeit mit der BWI bietet sich die Möglichkeit, am wachsenden Markt Öffentlicher Sektor/Defense teilzuhaben. Am Ende profitieren beide Seiten. Und letztlich auch die gesamte Gesellschaft.

EVERYTHING UNDER CONTROL
WITH OUR JOYSTICK CONTROLLER
AND RUGGED TABLET DEVICES

VISIT US AT AFCEA

BOOTH F05 / FOYER

roda
RUGGED IT & ELECTRONICS



WWW.RODA-COMPUTER.COM
INFO@RODA-COMPUTER.COM



KI in der Wärmebildtechnologie für den militärischen Einsatz

Der Einsatz Künstlicher Intelligenz (KI) im militärischen Bereich birgt großes Potential. Einerseits kann die Zieldetektion und -erkennung in erheblichem Maße beschleunigt werden. Andererseits stehen mit KI Techniken zur Verfügung, die einen klaren taktischen Vorteil bieten. Die VECTED GmbH hat dieses Potential erkannt und beschäftigt sich schon viele Jahre mit den Möglichkeiten von KI und der verantwortungsvollen Integration von KI in ihre Wärmebildsysteme. Verlässlichkeit, Transparenz und Robustheit sind die Leitmotive, anhand derer VECTED Künstliche Intelligenz zur bestmöglichen Unterstützung des Anwenders zur Verfügung stellt.

Bisher sind plattformungebundene Wärmebildgeräte im militärischen Bereich nicht sehr verbreitet, dabei bieten sie bei Tag und Nacht eine wertvolle Sichtunterstützung. Den Grundsatz „Sehen, ohne gesehen zu werden“ erfüllen Wärmebildgeräte auf große Distanzen optimal, weitgehend unabhängig von Sicht- und Witterungsverhältnissen. Alles, was eine Wärmesignatur besitzt, lässt sich mit dem Wärmebildgerät praktisch sofort aufspüren, von feindlichen Gefechtsständen bis zu getarnten Fahrzeugen, deren Motorwärmesignatur detektierbar ist. Schwierige Sichtverhältnisse wie Regen oder Nebel stellen im Wärmebild meist kein Problem dar. Für eine kontrastreiche Bilddarstellung mit hoher Detailtiefe kommt es auf die Leistungsfähigkeit des Sensors, der Optik und der Bildverarbeitung an. VECTED erzielt hier sehr gute Ergebnisse, da das Unternehmen die komplette Bildverarbeitung selbst entwickelt.

KI im Wärmebild: Entwicklung eigener, kundenspezifischer Modelle

Um den Nutzer noch besser bei der Erkennung von Objekten zu unterstützen, arbeitet VECTED daran, Künstliche Intelligenz als festen Bestandteil in die Wärmebildsysteme zu integrieren. Worauf das Unternehmen dabei Wert legt, sind die Zuverlässigkeit und Transparenz der eingesetzten KI. Damit der Soldat im Einsatz bestmögliche Entscheidungen treffen kann, wird der zugrunde liegende Algorithmus nur mit kontextspezifischen Daten trainiert. Kontextspezifisch bedeutet, dass diese auf die jeweiligen Einsatzbereiche angepasst werden können.

Mittels KI-Unterstützung kann zum Beispiel ein vorgeschobener Beobachter oder eine Drohne schnell ein potenzielles Ziel detektieren und identifizieren. Der größte Vorteil der KI-Unterstützung offenbart sich, wenn sich mehrere potenzielle Ziele im Bildfeld der Kamera befinden. Diese werden simultan detektiert und identifiziert, was es dem Beobachter ermöglicht, Hochwertziele sofort ausfindig zu machen. Durchqueren potenzielle Ziele das Sichtfeld der Kamera, werden diese sofort detektiert und identifiziert. Mittels einer sicheren Verbindung kann der Beobachter

die Daten der Kamera in Echtzeit verfolgen, ohne seine Stellung verlassen zu müssen. Um diese Flexibilität zu gewährleisten, entwickeln die KI-Spezialisten von VECTED alle KI-Anwendungen selbst. Genau wie menschliche Spezialisten kleinste Details in ihrem Wissensbereich einüben, wird auch die KI von VECTED mit passenden Daten für den jeweiligen Anwendungsfall optimal trainiert.

Synthetische Trainingsdaten

Die Bereitstellung dieser Daten ist nicht trivial; qualitativ hochwertige, kontextspezifische Daten, z.B. von feindlichen Militärfahrzeugen, sind schwierig zu bekommen und wenn dann oft fehlerbehaftet. Das Problem: Viele KI-Anwendungen benötigen zum Anlernen vorher gelabelte (markierte) Trainingsdaten, d.h., dass das Objekt von Interesse (z.B. ein Panzer, oder Gefechtsstand) in dem jeweiligen Trainingsbild markiert sein muss. Synthetische Daten sind in dieser Hinsicht immer zu 100 Prozent korrekt. VECTED ist in der Lage, die KI auf Basis dieser synthetischen Daten so zu trainieren, dass die Algorithmen später ohne Probleme reale Daten verarbeiten können. Worauf es VECTED bei der Erkennungsunterstützung ankommt, ist durch eine hohe Verlässlichkeit Vertrauen in die KI zu schaffen. Aus diesem Grund hat das Unternehmen Plausibilitätschecks in die Verarbeitungsketten eingebaut. Bereits während der Verarbeitung wird regelmäßig überprüft, ob der Ergebnisprozess noch in einem sinnvollen Rahmen stattfindet.

Emissionslose Entfernungsmessung per Wärmebildgerät

Auf der diesjährigen AFCEA Fachausstellung präsentiert VECTED ein Novum in der Wärmebildtechnologie: die emissionslose Entfernungsmessung, also eine Messung „ohne sichtbare Spuren“. Üblicherweise werden Entfernungsmessungen auch im militärischen Bereich mit Lasertechnik durchgeführt. Die Messung mittels ausgesendetem Laser lässt sich jedoch sehr leicht vom Gegner detektieren, womit die eigene Stellung aufgeklärt ist und feindliches Feuer auf sich zieht. Bei der emissionslosen Entfernungsmessung von VECTED kann die integrierte KI bei der visuellen Erfassung des Objekts die Entfernung bestimmen und im Display angeben – ohne jede Sichtbarkeit für den Gegner und mit dem Vorteil auch bei schwierigen Witterungsverhältnissen zu funktionieren.

Im Anwendungsfall der Artillerie oder der Panzerabwehr können somit mehrere potenzielle Ziele erfasst, identifiziert und deren Entfernung ermittelt werden. Der Anwender kann, unter Zuhilfenahme seines Standorts und der Blickrichtung der Kamera, sofort die Koordinaten des strategisch wichtigsten Ziels übermitteln, gegen dieses dann umgehend gewirkt werden kann.



37. AFCEA Fachausstellung 2024

Informations- und Kommunikationstechnik

„Zeitenwende in der nationalen Sicherheit –
Resilienz durch disruptive digitale Lösungen“

am 26./27. Juni 2024

World Conference Center Bonn

Unsere Aussteller bei der AFCEA Fachausstellung 2024





Symposium AFCEA FA 2024

Die 37. AFCEA Fachausstellung wird an beiden Tagen ein Symposium mit der Thematik des Jahresthemas 2024 beinhalten:

„Zeitenwende in der nationalen Sicherheit – Resilienz durch disruptive digitale Lösungen“

Mittwoch, 26. Juni 2024

09:00 h - 18:00 h Ausstellung (Eintritt frei)

Vorträge Symposium im ehemaligen Plenarsaal des Bundestages

10:00 Uhr

Begrüßung/Eröffnung der 37. AFCEA Fachausstellung

Brigadegeneral Armin G. Fleischmann, BMVg, Abteilungsleiter CIT I und Vorstandsvorsitzender AFCEA Bonn e.V.

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

10:15 Uhr

Key Note: „Militär- und Sicherheitspolitische Konsequenzen der aktuellen Konflikte“

LTG US A (ret) Ben Hodges, ehemaliger Befehlshaber USAREUR

18:00 Uhr – 22:00
Uhr

Get-together AFCEA Fachausstellung 2024

AFCEA Bonn e.V. lädt Besucher und Aussteller ein zu Kölsch mit Snacks auf der RHEINEBENE des World Conference Center Bonn

Donnerstag, 26. Juni 2024

09:00 h - 18:00 h Ausstellung (Eintritt frei)

Vorträge Symposium im ehemaligen Plenarsaal des Bundestages

10.00 Uhr

#DigitalDefenceDebate: „Vom Datenmeer zur Datenmacht: Chancen und Herausforderungen struktureller Datennutzung in Politik und Verwaltung.“

organisiert/moderiert durch die **Emerging Leaders Bonn e.V.**

Panelteilnehmer:

Oberst i.G. Frank Endler, AL Steuerung II, Zentrum Digitalisierung der Bw (ZDigBw)

Faruk Tuncer, Co-Founder Polyteia

Nicola Jentzsch, AL Innovation, Deutsche Bundesbank

Dr. Christina Schmidt-Holtmann, RL Datenverfügbarkeit, Digitale Souveränität, SPRIND, Bundesministerium für Wirtschaft und Klimaschutz

Moderation:

Teresa Ritter & Antonia Leonie Schmidt, Emerging Leaders AFCEA Bonn e.V.

14.00 Uhr

Key Note: „Lessons Learned aus der Ausbildung UKR Soldaten“

Generalleutnant Andreas Marlow, StvInspH und Kdr Militärische Grundorganisation

danach

Abschluss des Symposiums

Brigadegeneral Armin G. Fleischmann, BMVg, Abteilungsleiter CIT I und Vorstandsvorsitzender AFCEA Bonn e.V.

Ausstellerliste AFCEA Fachausstellung 2024

Bedeutung der Standabkürzungen:

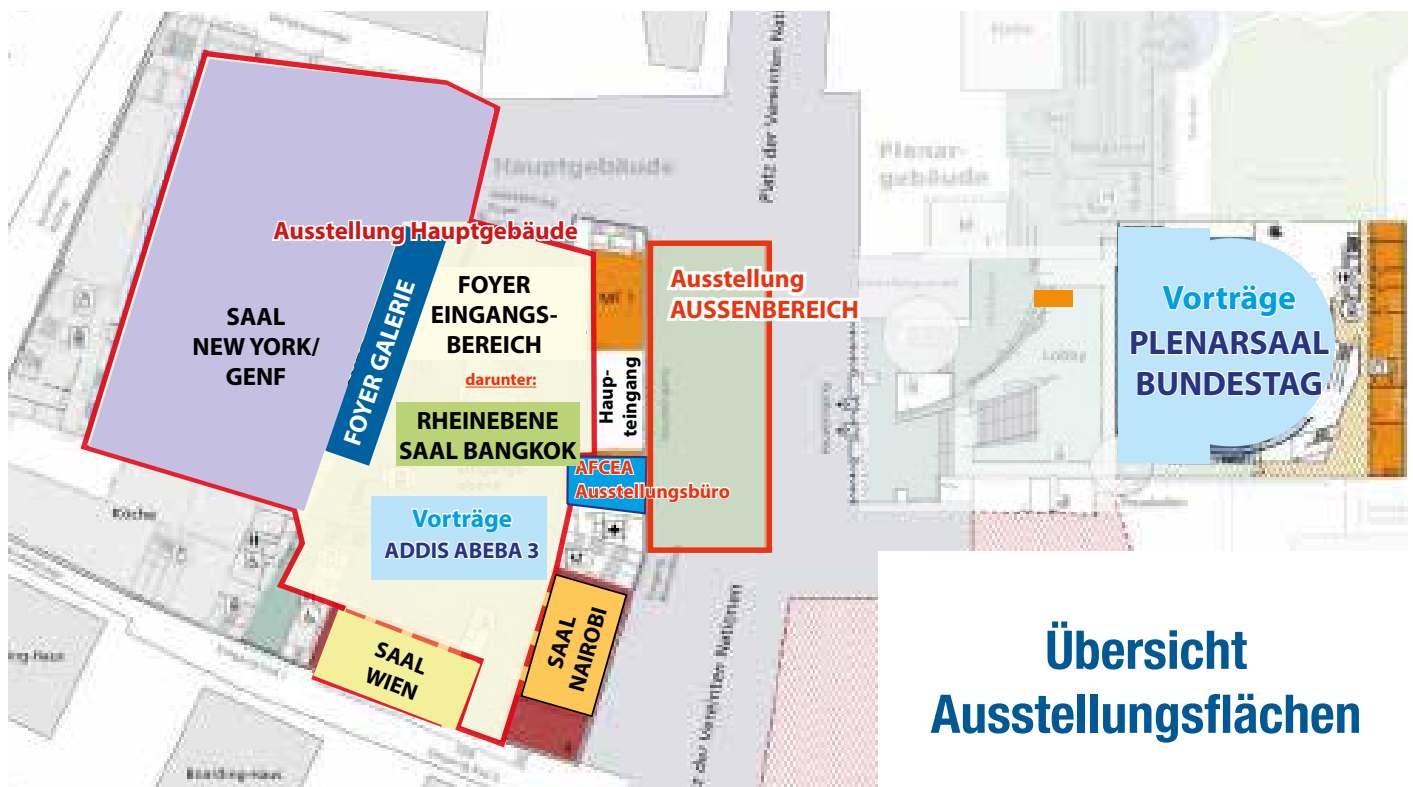
F = Ausstellungsfläche FOYER EINGANGSBEREICH
N = Ausstellungsfläche SAAL NAIROBI
W = Ausstellungsfläche SAAL WIEN
G = Ausstellungsfläche FOYER GALERIE

S = Ausstellungsfläche SAAL NEW YORK/GENF
R = Ausstellungsfläche RHEINEBENE
B = Ausstellungsfläche SAAL BANGKOK
A = Ausstellungsfläche AUSSENBEREICH

Nr.	Aussteller	Stand	
1	A. WEIDELT Systemtechnik GmbH & Co. KG	S 60	59 CyberArk Software (DACH) GmbH R 47
2	Accenture	S 32	60 dainox GmbH S 33
3	Adva Network Security	N 04	61 Dassault Systèmes Deutschland GmbH R 11
4	AFCEA International + AFCEA Europe	R 73	62 Data Respons Solutions GmbH N 07
5	Airbus Defence and Space	F 03 + A 06	63 Data-Warehouse GmbH F 36
6	AIUI GmbH	R 63 + S 18	64 DATAGROUP Defense IT Services S 16 + A 04
7	Alcatel-Lucent Enterprise	S 17	65 Dataminr Germany GmbH B 12
8	Amphenol-Air LB GmbH	R 13	66 DCON GmbH F 32
9	ASDRO GmbH	R 63	67 Dell Technologies R 51 + S 18
10	AVS Systeme GmbH	S 22	68 Deloitte Consulting GmbH B 09 b
11	B&W International	F 14	69 Detecon International GmbH S 73
12	BAKO Systemintegration GmbH & Co. KG	S 84	70 Deutsche Telekom F 06 a + A 11
13	BDSV e.V.	S 41	71 DIAMOND GmbH R 17
14	Bechtle AG	S 18	72 DIGITRADE GmbH F 29
15	Behörden Spiegel / ProPress Verlag GmbH	F 34	73 Dreger Group GmbH G 02
16	Belkin International Ltd	R 56	74 dttec.bw - Zentrum für Digitalisierungs- und N 03
17	Bernd Richter GmbH	R 13	Technologieforschung der Bundeswehr
18	best Systeme GmbH	R 48	75 DWT R 55
19	BFE Studio und Medien Systeme GmbH	B 08	76 Dynamit Nobel Defence (DND) S 31
20	Bittium	F 14	77 EAL Leidel GmbH S 42
21	Black Box Deutschland GmbH	B 05	78 ECOS Technology GmbH F 27
22	blackned GmbH	S 40	79 Edgeless Systems S 85
23	Bren-Tronics International Solutions	S 83	80 EGL Elektronik Vertrieb GmbH S 57
24	Broadcast Solutions GmbH	F 14	81 EIZO Europe GmbH S 82
25	Brodit	F 14	82 Elbit Systems Deutschland GmbH & Co. KG F 23
26	Bundeswehr BAPersBw/HLab	R 62	83 eleQtron GmbH R 63
27	Bundeswehr Kdo Cyber- und Informationsraum	R 46	84 Elma Electronic S 15
28	Bundeswehr Kdo Heer	S 66	85 ELP GmbH European Logistic Partners B 01
29	Bundeswehr Kdo Sanitätsdienst (Kdo SanDstBw)	S 65	86 ELT Group Deutschland S 34
30	Bundeswehr Kdo Streitkräftebasis	R 58	87 Endace R 48
31	Bundeswehr Kommando Luftwaffe	G 03	88 ESG Elektroniksystem- und Logistik-GmbH F 01
32	Bundeswehr Marinekommando	G 03	89 Esri Deutschland GmbH F 22
33	Bundeswehr Organisationsbereich Ausrüstung/BAAINBw	N 05	90 Eviden (an Atos company) F 31
34	Bundeswehr Planungsamt	R 61	91 Extron S 05
35	BWI GmbH	F 07	92 FERCHAU Aviation Group B 04
36	CAE GmbH	W 05	93 FFG Flensburger Fahrzeugbau Gesellschaft mbH F 14
37	Capgemini Deutschland GmbH	N 02	94 Forschungszentrum Space - UniBw München S 74
38	Carl-Cranz-Gesellschaft	R 24	95 FORTINET, inc. S 04
39	Carmenta Germany GmbH	W 11	96 Fraunhofer FKIE F 15
40	CeoTronics AG	F 26	97 Fraunhofer IOSB W 01 + F 14
41	CGI	F 04 + A 03	98 Frequentis Deutschland GmbH S 28
42	Check Point	W 02	99 Fujitsu Germany GmbH F 13
43	CHIFFRY GmbH	F 29	100 GAF AG F 09 + A 10
44	Chora A/S	S 76	101 Galvion S 30
45	Cisco Systems GmbH	F 08	102 GBS TEMPEST & Service GmbH S 03
46	citema group GmbH	R 54	103 genua GmbH S 25
47	Codan Communications/Domo Tactical Communications (DTC)/DTC	F 14	104 Gesellschaft für Sicherheitspolitik e.V. R 07
48	Computacenter AG & Co. oHG	W 02	105 Getac Technology GmbH B 09 a
49	Comrod Communication AS	F 17	106 Glenair GmbH S 72
50	Comtech Systems	S 30	107 Google Germany GmbH G 01
51	CONDOK GmbH	S 01	108 GovRadar GmbH R 63
52	CONET	S 45	109 griffity Defense F 14
53	Conrad Electronic SE	F 35	110 H&G Hansen & Gieraths IT Solutions GmbH F 25
54	Constructor University Bremen gGmbH (rasdaman)	R 18	111 Hagenuk Marinekommunikation GmbH B 07
55	Cordsen Engineering GmbH	S 75	112 HAT.tec GmbH R 14
56	CPI Vertex Antennentechnik GmbH	R 27	113 Heinen ICS S 57
57	cpm GmbH	N 06	114 Helsing S 71
58	Crisis Prevention (CP) - Beta Verlag	R 09	115 HENSOLDT W 07 + A 07
			116 Hexagon - HxGN Safety & Infrastructure GmbH S 14

Ausstellerliste AFCEA Fachausstellung 2024

Nr.	Aussteller	Stand	
117	Hirt Zerspanungstechnik GmbH	F 24	180 PROSTEP AG R 16
118	Hitachi Vantara GmbH	F 25	181 QGroup GmbH A 02
119	HP Deutschland GmbH	S 18	182 Quantum Systems R 57
120	IABG	W 06	183 RAM Mounts Germany GmbH R 15
121	IABG Teleport GmbH	W 06	184 Red Hat F 02
122	IBM	F 02	185 RHEINMETALL N 01 + N 09
123	iesy GmbH	S 63	186 Rick Location Solutions GmbH F 22
124	IGEL Technology GmbH	F 11	187 Rivada Space Networks GmbH R 63
125	IHSE GmbH	S 81	188 roda computer GmbH F 05
126	Imtradex GmbH	F 14	189 Rohde & Schwarz F 10
127	Indra Avitech GmbH	S 11	190 rola Security Solutions GmbH F 06 b
128	Indra Sistemas S.A.	S 11	191 Rolatube S 30
129	INFODAS GmbH	S 46	192 Rosenberger Hochfrequenztechnik GmbH & Co. KG R 12
130	INNOSYSTEC GmbH	S 06	193 RUAG S 70
131	INTRACOM DEFENSE (IDE)	F 14	194 SAP Deutschland SE & CoKG F 21
132	IntraFind Software AG	R 41	195 Satcube F 16 + A 09
133	inxire GmbH	F 37	196 Schönhofer Sales and Engineering GmbH S 54
134	itWatch GmbH	S 10	197 SCOTTY Group Austria GmbH N 08 + A 12
135	JK Defence & Security Products GmbH	S 30	198 secunet Security Networks AG F 19
136	JOWO - Systemtechnik AG	W 10	199 Secusmart GmbH S 51
137	Kappa optronics	R 19	200 SELECTRIC Nachrichten-Systeme GmbH S 35
138	KEEQuant GmbH	R 72	201 SentinelOne GmbH R 45
139	KENBUN IT AG	R 63	202 SES B 11
140	Knapp Service Koblenz GmbH	W 09	203 Siemens Digital Industry Software GmbH G 04
141	KNDS Deutschland GmbH & Co. KG (bisher: Krauss-Maffei-Wegmann GmbH & Co. KG)	A 01	204 SMS System-Management Stiewi GmbH S 56
142	KNDS Deutschland Mission Electronics GmbH (bisher: ATM ComputerSysteme GmbH)	S 48	205 Software AG S 20
143	KPMG AG Wirtschaftsprüfungsgesellschaft	S 26	206 Soldaten- und Veteranenstiftung R 26
144	L3Harris	S 30	207 Soldatenhilfswerk R 25
145	Lachen Helfen	R 75	208 Solifos Deutschland GmbH S 27
146	Langlauf Security Automation GmbH	R 63	209 SOPHIST GmbH R 53
147	Leonardo SpA	A 05	210 Sophos Technology GmbH S 62
148	LocateRisk GmbH	R 63	211 Sopra Steria SE S 12
149	Lumbird	F 14	212 Spleenlab GmbH R 57
150	M4Com System GmbH	R 52	213 Splunk W 02
151	Materna Information & Communications SE	S 52	214 steep GmbH S 39
152	Materna Virtual Solution GmbH	S 56	215 Stellar DBS GmbH F 14
153	Matrox Video GmbH	F 30	216 SThree GmbH S 52
154	MBS - Media Broadcast Satellite GmbH	S 29	217 SVA System Vertrieb Alexander GmbH S 53
155	Micropol Fiberoptic AB	F 33	218 Systematic GmbH S 47
156	Mittler Report Verlag GmbH	R 23	219 systerra computer GmbH S 64
157	Mönch Verlagsgesellschaft m.b.H.	R 10	220 TASSTA F 14
158	Mosolf	F 14	221 tde – trans data elektronik GmbH, Vertriebsbüro Dortmund R 71
159	Motorola Solutions Germany GmbH	S 21	222 TEHTRIS S 61
160	NanTenna	S 30	223 TEKSAM GMBH W 03
161	Narda Safety Test Solutions GmbH	F 14	224 Telespazio Germany GmbH F 09 + A 10
162	ND SatCom GmbH	S 43	225 Tenzir GmbH R 63
163	NEOSAT GmbH	S 74	226 Thales Deutschland S 23
164	NetApp	F 14 + S 18	227 ThermoAnalytics GmbH B 10
165	Newsletter Verteidigung - VDS	R 08	228 Traversals GmbH R 63
166	NVIDIA	R 48	229 Trend Micro Deutschland GmbH S 36
167	ODM GmbH	F 28	230 Treo - Labor für Umweltsimulation GmbH S 55
168	OHB System AG	F 20	231 Ultralife Corporation S 30
169	Panasonic Connect Europe GmbH	F 05	232 utimaco GmbH S 19
170	Pegasystems GmbH	F 04	233 VECTED GmbH R 43
171	Peli	S 02	234 Verband der Reservisten der Bundeswehr B 02
172	Pexip	R 74	235 Viasat S 30
173	PHYSEC GmbH	R 63	236 Vitec GmbH W 04
174	PLATH GmbH & Co. KG	F 18	237 VITES GmbH W 06
175	Precision Technic Defence	A 08	238 Willert Software Tools GmbH B 06 a
176	PREVENCY GmbH	R 63	239 WORK Microwave GmbH F 12
177	ProductionToGo	R 42	240 Xecuro GmbH S 25
178	promegis Gesellschaft für Geoinformationssysteme mbH	S 13	241 ZARGES GmbH W 08
179	ProSoft GmbH	S 61	242 Zebra Technologies Germany GmbH S 35

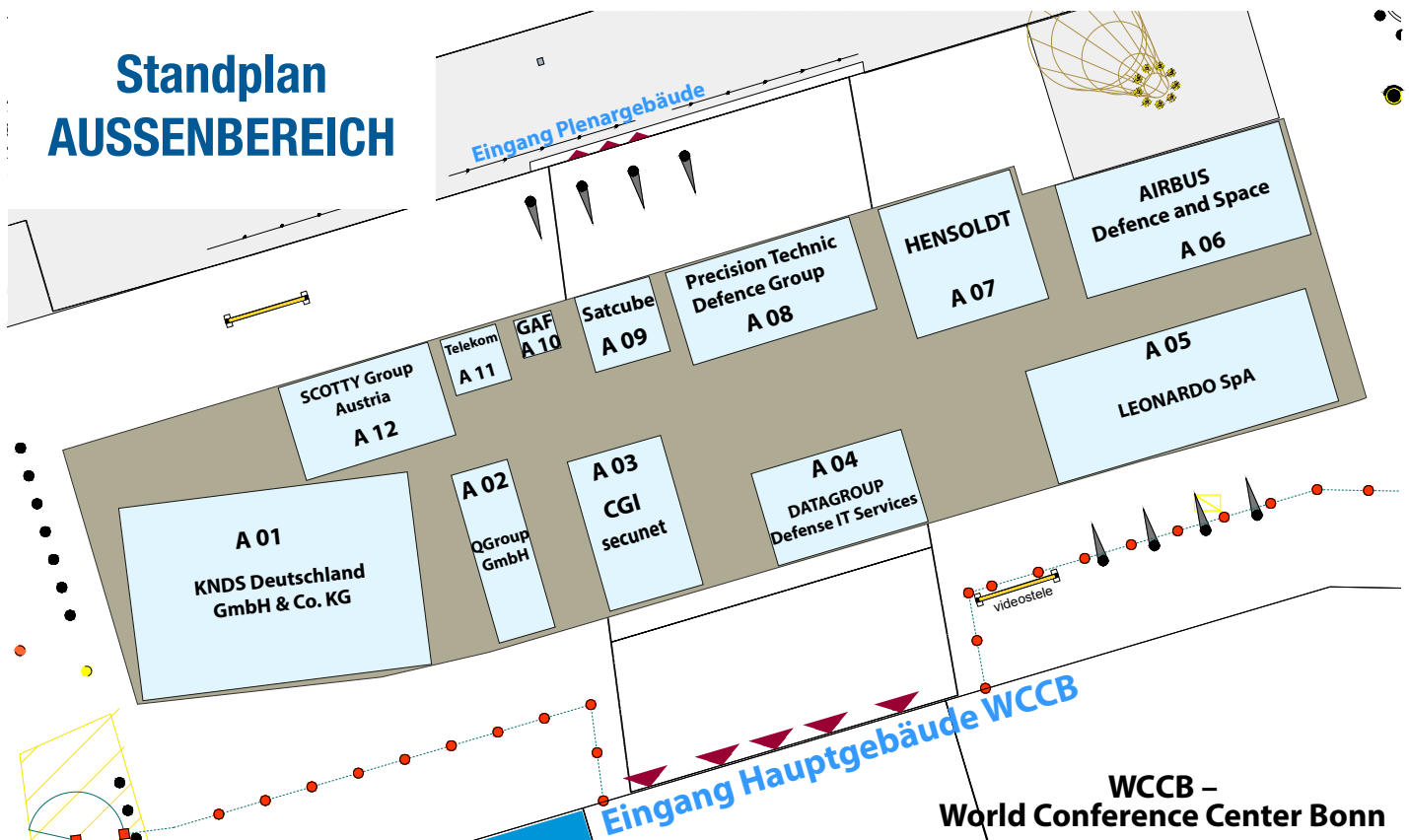


Übersicht Ausstellungsflächen

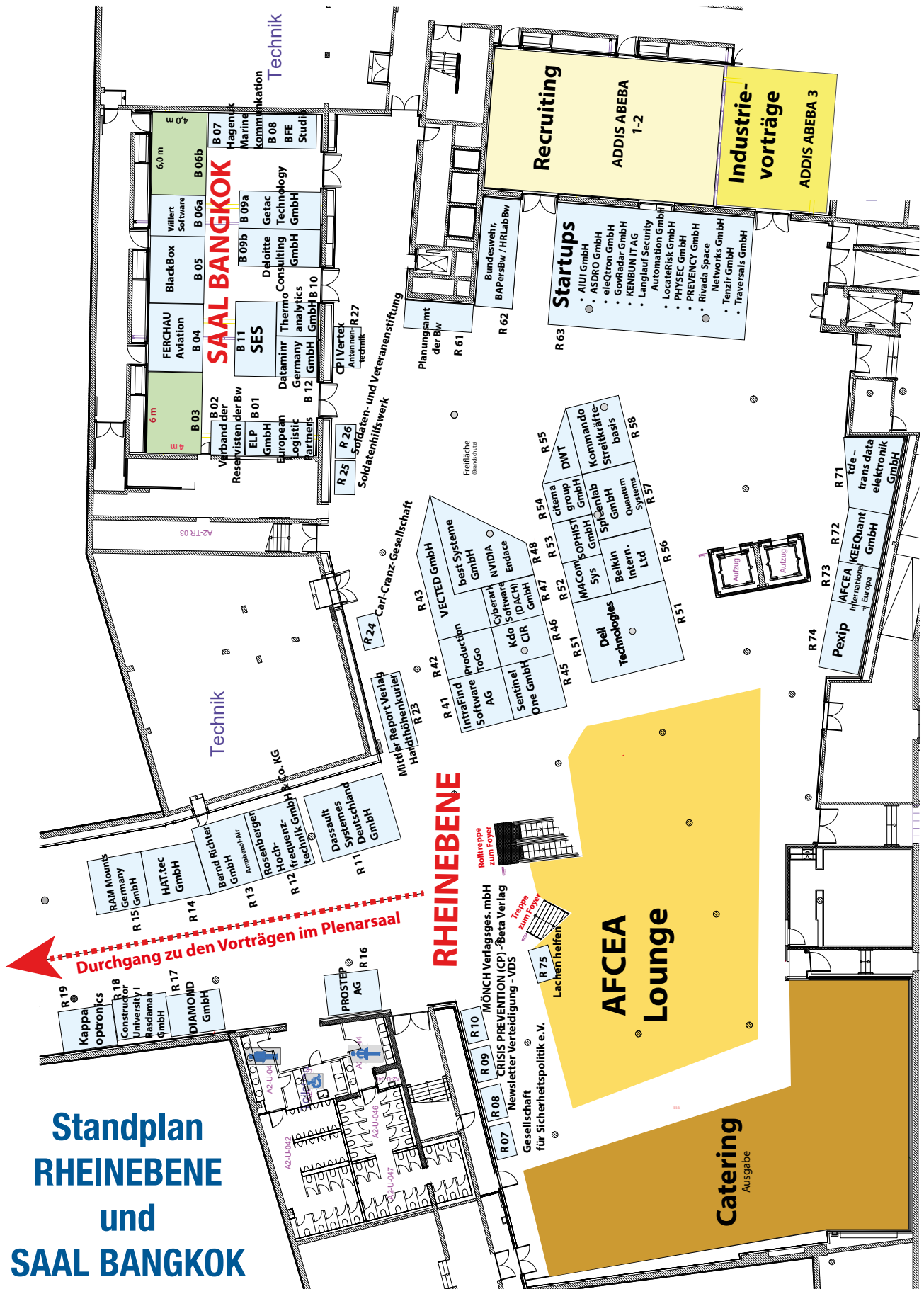
Unsere Ausstellungsflächen

- * AUSSENBEREICH
- * RHEINEBENE mit SAAL BANGKOK
- * FOYER EINGANGSBEREICH mit SAAL NAIROBI und SAAL WIEN
- * FOYER GALERIE

Standplan AUSSENBEREICH



Standplan RHEINEBENE und SAAL BANGKOK

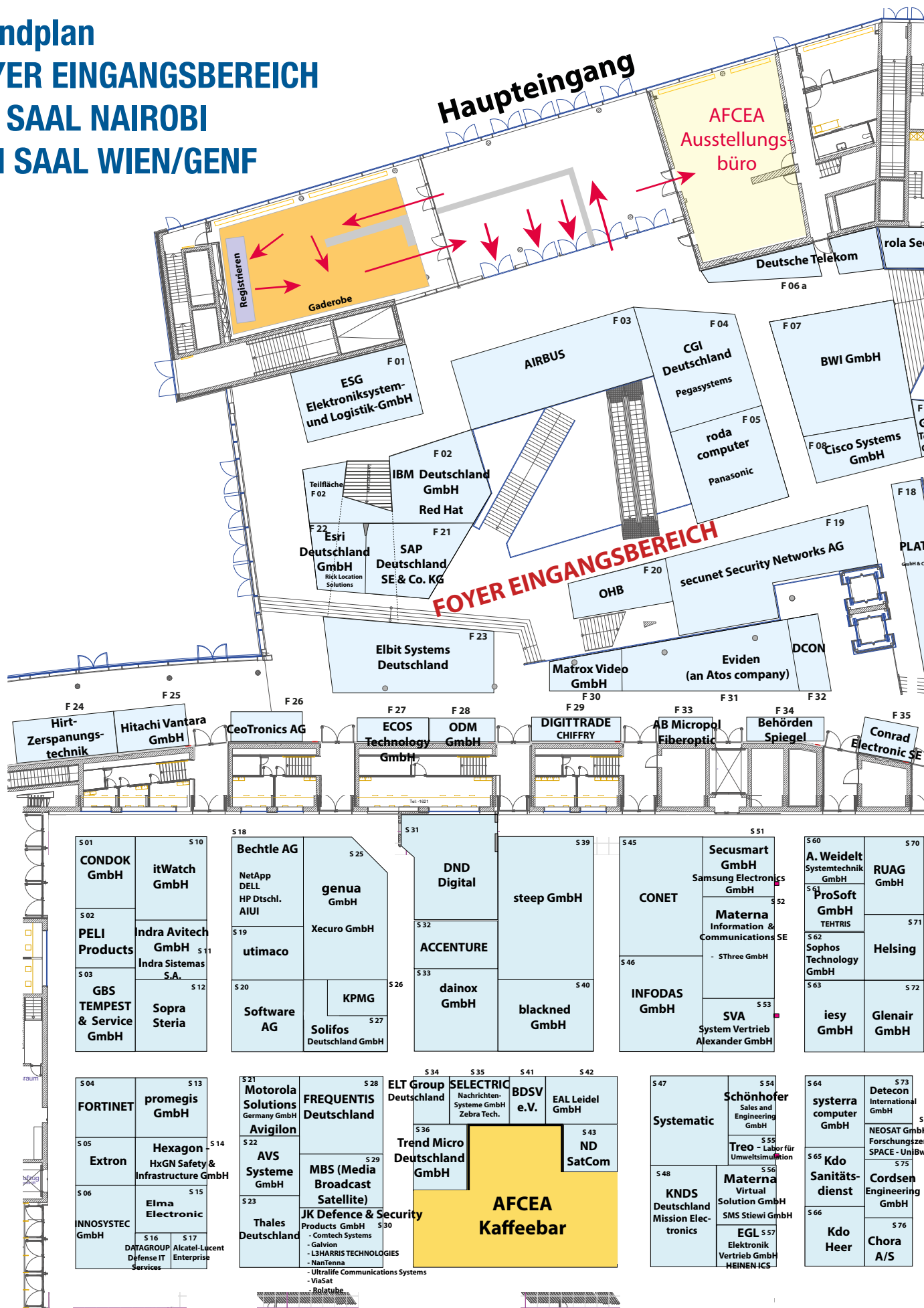


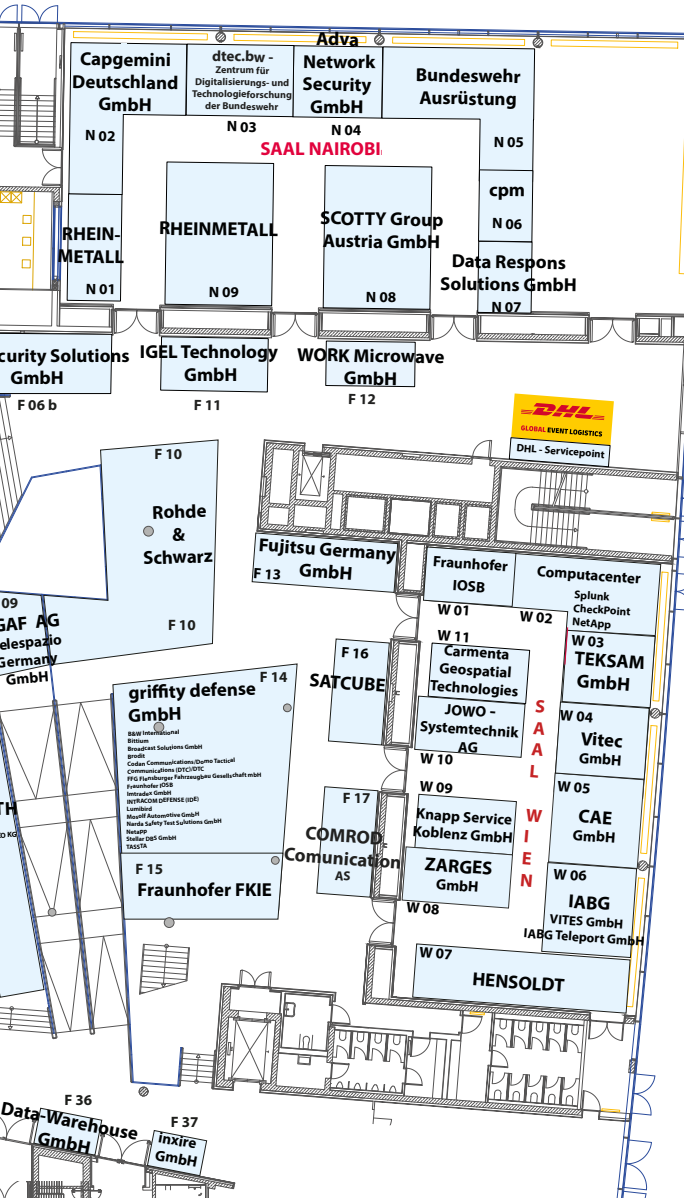
Standplan

FOYER EINGANGSBEREICH

mit SAAL NAIROBI

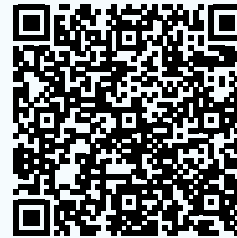
und SAAL WIEN/GENF





Die aktuellen Saal- und Standpläne

finden Sie unter

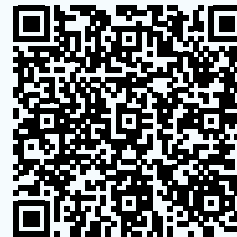


Die aktuelle Ausstellerliste

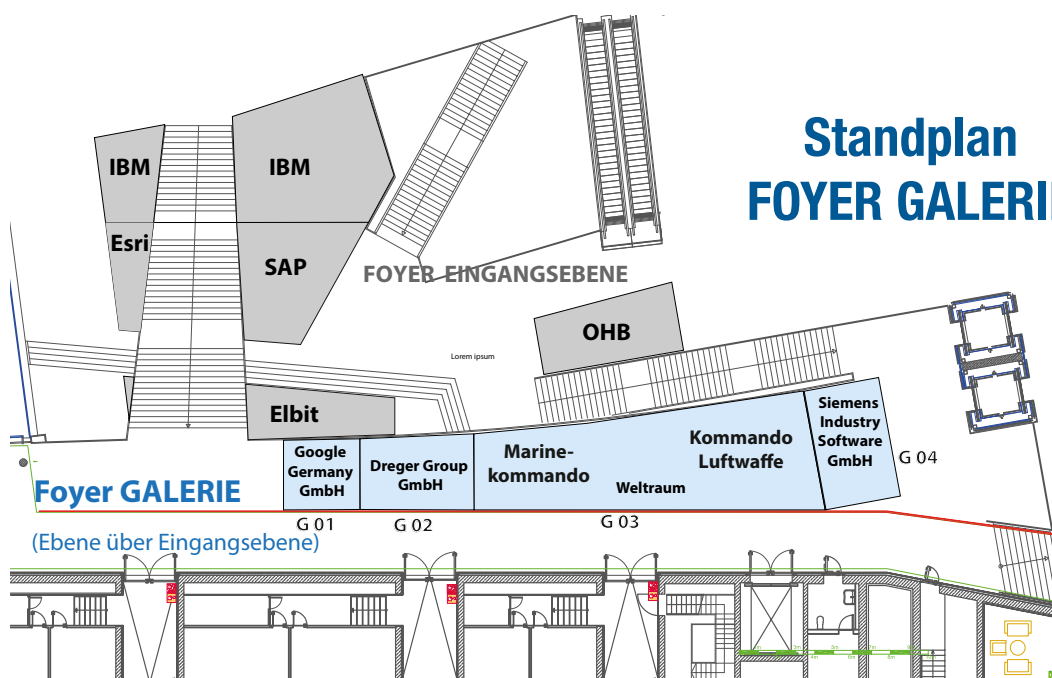
mit

Kompetenzen und Firmenprofilen

finden Sie unter:



Standplan FOYER GALERIE



Symposium und Industrievorträge

Zeitplan für die Industrievorträge bei der FA 2024

		26.06.2024		27.06.2024	
		Speaker-corner 1	Speaker-corner 2	Speaker-corner 1	Speaker-corner 2
		Plenarsaal Bundestag	Raum ADDIS ABEBA 3	Plenarsaal Bundestag	Raum ADDIS ABEBA 3
AFCEA Fachausstellung 2024	09:00				
	09:30				
	10:00	Eröffnung Symposiums-vortrag 1		Symposium 2 #Digital Defence Debate	
	10:30				
	11:00				
	11:15 - 11:40	1 Materna SE	14 Rohde & Schwarz	24 genua	29 Telespacio Germany
	11:45 - 12:10	2 CGI Deutschland	15 RUAG	25 HENSOLDT	30 Carmenta
	12:15 - 12:40	3 IBM Deutschland	16 Materna Virtual Solution	26 Deutsche Telekom	31 Adva Network Security
	12:45 - 13:10	4 dainox	17 Eviden	27 Airbus Defence and Space	32 NVIDIA
	13:15 - 13:40	5 RHEINMETALL	18 roda computer	28 SOPHIST	33 best Systeme
	13:45 - 14:10	6 SThree	19 Detecon International		
	14:15 - 14:40	7 ESG	20 Accenture		
	14:45 - 15:10	8 CONET	21 Thales Deutschland		
15:15 - 15:40	9 rola Security	22 Dataminr			
15:45 - 16:10	10 Secusmart	23 Pegasystems			
16:15 - 16:40	11 Sophos Technology				
16:45 - 17:10	12 Constructor Uni Bremen				
17:15 - 17:40	13 Bechtle				
		ab 16:15: Emerging Leaders AFCEA Bonn präsentieren: Startup Pitch und Panel Session ADDIS ABEBA 1 - 2			
	18:00	AFCEA Bonn e.V. lädt Aussteller und Besucher ein zum Get-Together (RHEINEBENE)			
	19:00				
	20:00				
	21:00				
	bis 22:00 h				

INDUSTRIEVORTRÄGE:

Auf vielfachen Wunsch der Aussteller richten wir auch bei der AFCEA Fachausstellung 2024 zwei **Speakercorner für Industrievorträge** ein: im ehemaligen **Plenarsaal des Deutschen Bundestages** und im **Raum ADDIS ABEBA 3**. Dort können Aussteller in den Zeiten - in denen keine Vorträge des Symposiums im Plenarsaal stattfinden - zu einem Thema ihrer Wahl vortragen (Vortrag 20 Min, 5 Min Fragen/Diskussion).

Auf dieser Seite sehen Sie die Vorträge der Aussteller im zeitlichen Ablauf. Der QR-Code oben rechts bietet den Link zu den Vortragsthemen und den Abstracts sowie zur „Broschüre Industrievorträge 2024“.

Wie bei der FA 2023 haben wir wieder ein **Symposium mit 3 Vorträgen** als Teil der AFCEA Fachausstellung 2024.

SYMPOSIUM:





Themen der Industrievorträge

Nr.	Aussteller	Thema des Industrievortrages
1	Materna Information & Communications SE	MEDEVAC-KI Assistent: In Echtzeit mit KI und Sensorik unterstützen
2	CGI Deutschland B.V. & Co. KG	AI Felix – Drei Erkenntnisse für KI-Projekte mit den Streitkräften
3	IBM Deutschland	Bundeswehr: Digital und innovativ
4	dainox GmbH	Software Defined die Zukunft gestalten: Die Symbiose von flexibler Software und robuster Hardware
5	RHEINMETALL	Welche Rolle übernimmt die „alte“ Rüstungsindustrie im digitalen Zeitalter?
6	SThree GmbH	Megatrends managen – und trotz fehlender Fachkräfte den Anschluss nicht verlieren
7	ESG Elektroniksystem- und Logistik-GmbH	Multi-Domain Operations End2End – Vom Sensor über den Shooter bis in die Munition
8	CONET	Mit Lagebildern und technischen Dokumenten sprechen
9	rola Security Solutions GmbH	Tiefenanalyse im Dienst der Sicherheit: Moderne IT-Lösungen für Militäroperationen
10	Secusmart GmbH	SecuSUITE Cross-Platform – Give Users a Choice
11	Sophos Technology GmbH	Zukunftssichere IT-Sicherheit – und welche Rolle spielen Mensch und KI?
12	ConstrConstructor University rasdaman GmbH	Mehr Nutzen aus Geo-Standards für das FMN?
13	Bechtle AG	Skalierbar, standardisiert, agil: beschleunigte Softwareentwicklung über verschiedene Clouds hinweg
14	Rohde & Schwarz	ESSOR – European Secure Software Defined Radio. Mit welchen Schritten wird die Funk-interoperabilität europäischer Streitkräfte endlich konkret ermöglicht?
15	RUAG	Krisenkommunikation - und wie kommunizieren Sie und Ihre Organisation in Zukunft?
16	Materna Virtual Solution GmbH	Der sichere ultramobile Arbeitsplatz: Per Smartphone und Tablet auf wichtige Fachanwendungen zugreifen. Schnell. Einfach. VS-NfD-konform.
17	Eviden Germany GmbH	Souveräne Digitalisierung und Ermöglichung von Multi Domain Operations: Erzeugung digitaler Wirkketten und durchgängiger Informationsräume als Element der Multi Domain Combat Cloud
18	roda computer GmbH	Vernetzte Visualisierung
19	Detecon International GmbH	Quantentechnologien und ihr Potenzial, Wirtschaft, Verwaltung und Gesellschaft stark zu verändern
20	Accenture	Adoption, Anpassung und Risiko: Generative KI und nationale Sicherheit
21	Thales Deutschland	Möglichkeiten zur Erhöhung von Effizienz und Usability bei der Absicherung von Daten und Sprache im High Security Bereich
22	Dataminr	KI und der Open-Source Datenvorteil: Ein Muss für aktuelle und zukünftige Kriege und
23	Pegasystems	Entwicklung mit Low Code: Vorsprung durch Geschwindigkeit & Anpassungsfähigkeit
24	genua GmbH	Souveräne Cloud: Eine geostrategisch-technische Analyse zu Cybersicherheit
25	HENSOLDT	HENSOLDT FCAS Accelerator – ein Paradigmenwechsel für das Innovationsmanagement in der Verteidigung
26	Deutsche Telekom Geschäftskunden GmbH	Fokussierung auf Kernaufgaben durch Digitalisierung von Verwaltungsprozessen
27	Airbus Defence and Space	Weltraumgestützte Kommunikation für militärische Anwender
28	SOPHIST GmbH	KI oder Mensch – Wer ist besser im Systems Engineering?
29	Telespazio Germany GmbH	Informationssicherheitskonzepte: Grundlagen und Notwendigkeit
30	Carmenta Germany GmbH	Echtzeit Geodaten als Game-changer auf dem Gefechtsfeld
31	Adva Network Security	Geschützte Glasfasernetze als Fundament einer hochsicheren Kommunikations-Infrastruktur: überwacht, resilient, quantensicher
32	NVIDIA GmbH	Sensorfusion, Metadatenextraktion und Datenreduktion in isolierten Edge-Systemen mit Nvidia Jetson
33	best Systeme GmbH	COTS-Ketten sprengen - Moderne IT für Militärische Anwendungen oder -> wie kann Ihr Unternehmen durch den Einsatz von MOTs profitieren? Ein Beispiel einer High-Performance-Switch-Modifikation (>100GBs) für die Luftfahrt

Aussteller AFCEA-Fachausstellung 2024

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

A. Weidelt Systemtechnik

Die A. Weidelt Systemtechnik ist ein seit Jahrzehnten führender Systemintegrator und unverzichtbarer zuverlässiger Partner der Bundeswehr und ziviler Kunden.

Durch langjährige Erfahrung in der

Realisierung mobiler und stationärer Systeme, sowie

- ein hohes Maß an Kompetenz und Erfahrung spezialisierter Mitarbeiter,
- fachkompetente Projektleitung, Konstruktion und Integration,
- Systemschulung und Dokumentation,
- ständige Weiterentwicklung von Systemen und Neukonzipierungen,
- einen bundesweiten Vor-Ort-Service,
- umfangreiche Erfahrungen in der Durchführung von militärischen Beschaffungsvorhaben und Projekten, liefern wir Lösungen zugeschnitten auf die individuellen Problemstellungen des Kunden.

A. WEIDELT
Systemtechnik



S 60

AFCEA International und AFCEA Europe

R 73

AFCEA International is a non-profit, member-based association that promotes global security by providing a forum for the ethical exchange of information. AFCEA Europe was founded in 1984 as the European office (in Brussels) of AFCEA International with the main purpose of helping individuals and industry get in contact with NATO, EU, and national governments while promoting the vision, mission and core values of AFCEA. AFCEA Europe organises events in Europe bringing together the government, industry, and academia - all with the purpose of equipping its individual and corporate members to meet the challenges of governments and to further their careers.



Accenture

Accenture ist ein weltweit tätiges Beratungsunternehmen, das führende Unternehmen, Regierungen und weitere Organisationen unterstützt. Durch den Aufbau eines digitalen Geschäftskerns, Prozess-

optimierung, Beschleunigung des Umsatzwachstums und die Verbesserung öffentlicher Dienstleistungen schaffen wir für unsere Kunden in mehr als 120 Ländern Mehrwert. Technologie steht dabei im Mittelpunkt des Wandels, den wir mit starken Partnerschaften in unserem Ökosystem vorantreiben. Unsere rund 742.000 Mitarbeitenden verfügen über umfassende technologische Kompetenz sowie über tiefgehende Branchenkenntnis und funktionale Expertise. Damit setzen sie ein breites Spektrum an Dienstleistungen und Lösungen in den Bereichen Strategy & Consulting, Technology, Operations, Industry X sowie Song um. Besuchen Sie uns unter www.accenture.de



S 32

Airbus

F 03 + A 06

Airbus ist Pionier einer nachhaltigen Luft- und Raumfahrt für eine sichere und vereinte Welt. Das Unternehmen arbeitet ständig an Innovationen für effiziente und technologisch fortschrittliche Lösungen in den Bereichen Luft- und Raumfahrt, Verteidigung sowie vernetzte Dienstleistungen. Airbus bietet moderne und treibstoffeffiziente Verkehrsflugzeuge sowie dazugehörige Dienstleistungen an. Airbus ist auch führend in Europa im Bereich Verteidigung und Sicherheit und eines der größten Raumfahrtunternehmen der Welt. Im Bereich Hubschrauber stellt Airbus die weltweit effizientesten Lösungen und Dienstleistungen für zivile und militärische Hubschrauber bereit.

AIRBUS

AIUI

R 63 + S 18

AIUI – Ihre Experten für künstliche Intelligenz im Unternehmen mit extremer Datensicherheit. Individualisierte KI-Lösungen für optimierte Geschäftsprozesse – von internen Wissensdatenbanken und Coding, über Dokumentenautomatisierung bis zum Kundenservice. Zeit sparen, Qualität erhöhen – alles DSGVO-konform!



Adva Network Security

N 04

Adva Network Security hat sich auf den Schutz von Datennetzen mit hohem Sicherheitsbedarf spezialisiert. Mit unserer ConnectGuardTM Sicherheitstechnik sind Unternehmen, Behörden und kritische Infrastrukturen schon heute in der Lage, zukünftige Cyber-Angriffe durch Quantencomputer abzuwehren. Unsere Verschlüsselungslösungen zeichnen sich durch eine sehr geringe Latenzzeit aus und bieten Glasfasernetzen einen umfassenden Schutz auf mehreren Netzebenen. Anerkannte Sicherheitsexperten haben unser Unternehmen in Deutschland gegründet, um Organisationen und Behörden beim Schutz ihrer Netze zu unterstützen und damit Cyber-Bedrohungen ihrer kritischen Anwendungen abzuwenden. Unsere Entwicklungs- und Fertigungsprozesse sowie unsere Verschlüsselungslösungen wurden von führenden staatlichen Sicherheitsbehörden zertifiziert und zugelassen. Erfahren Sie mehr unter www.advasecurity.com



Alcatel Lucent Enterprise

S 17

Alcatel-Lucent Enterprise bietet vernetzte Verteidigungslösungen für intelligente Basen, Feldoperationen und Krisenmanagement. Diese umfassen robuste Kommunikation und sichere Netzwerke, die den extremen Bedingungen standhalten. Für Krisenmanagement ermöglichen IoT-Geräte und Multimedia-Kommunikation schnelle und kontextbezogene Reaktionen. ALE implementiert darüber hinaus in seine Produkte und Lösungen strenge Cybersicherheitsstandards. In Frankreich betreibt ALE dazu ein spezielles Service-Center für sichere Kommunikation und Netzwerkinfrastruktur. Mehr als 100 Jahre Engagement für Innovation und den Erfolg der Kunden haben Alcatel-Lucent Enterprise zu einem führenden Anbieter gemacht, der heute mehr als eine Million Kunden in aller Welt betreut.

Alcatel-Lucent
Enterprise



Amphenol Air LB GmbH**R 13**

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

Amphenol-Air LB**ASDRO GmbH****R 63**

Die Fa. ASDRO ist ein Drohnen-Technologie Unternehmen, welches geophysikalische Sensorik und speziell konstruierte Drohnen nutzt, um Kampfmittel aus der Luft sicher zu detektieren. Das System kann automatisiert und auf jedem Untergrund eingesetzt werden um Minen, Granaten und Bomben auf belasteten Flächen zu identifizieren. Die eigens entwickelte Software macht es möglich, die Daten effizient zu visualisieren und zu interpretieren.

**AVS Systeme GmbH****S 22**

Die AVS Systeme GmbH hat sich auf die Planung und Realisierung von hoch technisierten audiovisuellen Visualisierungssystemen und Systemanlagen in Leitstellen und Führungsräumen spezialisiert – deutschlandweit, europaweit und über zahlreiche Märkte und Branchen hin-



weg. 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 Marktführer entwickelt.

B&W International**F 14**

Schnelle Einsätze, gesicherte Kommandokommunikation, effiziente Logistik: Einsatzkräfte in aller Welt vertrauen auf die mobilen Defenseschutzkofferlösungen von B&W International. Ob autarke Energieversorgung aus dem Koffer, unkomplizierter Lufttransport von Lithium-Ionen-Akkus, griffbereite, hochsensible Instrumente oder adhoc Drohen-Aufklärung: die modernen Schutzkoffer bieten optimierte Logistik, Kostenreduktion, Schnelligkeit und Effizienz, vor allem aber Sicherheit und Einsatzbereitschaft. B&W International ist Entwickler und Produzent von Kofferlösungen für den mobilen Schutz hochwertiger, empfindlicher und sicherheitsrelevanter Instrumente, Waffen und Munition. Und punktet darüber hinaus mit umfangreichen Zertifizierungen und Zulassungen sowie durchdachter Full-Service-Begleitung. Damit ist B&W strategisch aufgestellt für eine schnelle Individualisierung bei besonderen Herausforderungen. Plug & Protect mit B&W International.

**BAKO Systemintegration GmbH & Co. KG****S 84**

Seit der Firmengründung im Jahr 1994 vertrauen Kunden aus Medizin, Industrie und Militär auf die BAKO Leistungsfähigkeit und Flexibilität. Firmensitz und Fertigung des



MATERNA
Information & Communications

Treffen Sie **Materna** und **SThree** am **Stand S52**.

Materna Virtual Solution
am **Stand S56**.

IT-DIENSTLEISTER IM EINSATZ

Materna ist einer der führenden deutschen IT-Dienstleister mit über 40 Jahren Erfahrung im Bereich Systemintegration und beim Einsatz moderner IT-Lösungen für die öffentliche Verwaltung. Wir sind Teil der digitalen Transformation in der Bundeswehr.

Bereit für die digitale Transformation in der Bundeswehr?

Weitere Infos: www.materna.de/bw

inhabergeführten Familienunternehmens liegen in Eisenberg in der Metropolregion Rhein-Neckar. Die BAKO Gruppe unterteilt sich in zwei Geschäftsfelder:

- **Systems:** Schwerpunkt ist die Erstellung von mobilen und stationären Systemen im Allgemeinen und darüber hinaus die Berücksichtigung schwieriger Umwelt- und Operationsbedingungen.
- **Logistik:** Konstruktion und Erstellung von Mehrwegtransportverpackungen. Das Aufgabenfeld erstreckt sich vom einfachen Kunststoffkoffer mit Inlay bis hin zu intelligenten und hochbelastbaren Mehrwegverpackungen innerhalb der Logistikkette. www.bako.de

BDSV e.V.

S 41

Der BDSV vertritt die gebündelten Interessen der deutschen Sicherheits- und Verteidigungsindustrie (SVI). Damit unterstützt er die Unternehmen im nationalen und internationalen Wettbewerb. Er versteht sich dabei als Ansprechpartner für Unternehmen aller Größenordnungen eines sich stark wandelnden Wirtschaftssektors.

Er verfügt über ein weit verzweigtes Netzwerk in Deutschland und Europa, auf allen wichtigen Märkten und in internationalen Organisationen und bietet Informationen über die Themen der deutschen SVI.

Der BDSV fungiert als Point of Contact der deutschen SVI und als Scharnier zwischen Unternehmen, Politik, Gesellschaft, Institutionen und Medien. Übergeordnete Ziele sind der Erhalt und der Ausbau der Wettbewerbs- und Zukunftsfähigkeit der deutschen SVI und des Technologie- und Wirtschaftsstandorts Deutschland.



Bundesverband der Deutschen Sicherheits- und Verteidigungsindustrie e.V.

Bechtle AG

S 18

Bechtle: Der IT-Zukunftspartner im Public Sector

Bechtle ist mit über 100 IT-Systemhäusern nah an den Standorten der Kunden 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-) Hardware 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 derzeit über 15.000 Mitarbeitende. 2023 lag der Umsatz nach vorläufigen Zahlen bei rund 6,4 Mrd. €.



Behörden Spiegel / ProPress Verlag GmbH

F 34

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, u.a. der Newsletter „Verteidigung. Streitkräfte. Wehrtechnik“.

Behörden Spiegel

Belkin International Ltd

R 56

Belkin is an accessories market leader delivering power, protection, productivity, connectivity, audio, security and home automation solutions for a broad range of consumer electronics and enterprise environments. Belkin creates products that empower people through technology whether at home, at work or on a new adventure. Belkin is also the market leader in Secure KVM. Belkin's Secure KVM series combines cutting-edge cybersecurity provisions, video performance and user experience to deliver

belkin. Cybersecurity

a nocompromise solution for the most demanding applications. Designed and built for government and military agencies around the world to safeguard critical data and computer systems.

Bernd Richter GmbH

R 13

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 300 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 vom Designentwurf bis zur Prototypenfertigung technischen Support.



best Systeme GmbH

R 48

Der Fokus der best Systeme GmbH liegt immer auf einer kundenge-rechten IT-Lösung. Seit fast 30 Jahren erfüllt ein engagiertes Team von Fachexperten unter Einsatz von branchenführenden IT-Produkten diese Intention. Der fortwährende Wandel in der IT-Industrie und auch der wachsende technologische Anspruch unserer Kunden definiert unsere IT-Dienstleistung. Für spezielle Bedürfnisse in rauen Umgebungen (rugged), unter extremen Umwelteinflüssen wie Temperatur, Vibration, Schmutz oder Stöße setzen wir auch Minimalchargen und Einzelanfertigungen für den Einsatz zu Land, zu Wasser und in der Luft um. Neue Technologien wie Digital Twins unter Anwendung von Artificial Intelligence verkürzen dabei den Zeitrahmen für die Entwicklung signifikant.



BFE Studio und Medien Systeme GmbH

B 08

Als international tätiger Systemintegrator entwickelt BFE innovative Lösungen in den Bereichen Broadcast- und Medientechnik sowie im KRITIS Leitstellenbereich. Wir sind auf die Entwicklung herstellerunabhängiger Lösungen zur Steuerung von Audio- und Videoinhalten sowie KVM-Integrationen und IT-System-Implementierungen spezialisiert. Hierzu passend bietet BFE Serviceverträge auf allen SLA-Ebenen an. Alle Mitarbeiter in Planung und Service haben die Sicherheitsstufe 1 und sind somit befähigt, in den höchsten Sicherheitsbereichen tätig zu sein. Zu unseren Kunden zählen Polizeien, Innenministerium, Militär sowie weitere öffentliche und private Auftraggeber.

Ergänzt wird das Angebot durch maßgeschneiderte Möbel für Kontrollrauminstallationen aus eigener Herstellung sowie ein intuitives Leitstellen-Managementsystem zur Steuerung von Visualisierungssystemen.



Bittium

F 14

Bittium is a trusted Finnish company with over 35 years of experience in advanced radio communication technologies. For Defense & Security market Bittium provides the most modern products and solutions for tactical & secure communications. The products and solutions for tactical communications bring broadband data and voice to all troops across the battlefield. For secure communications Bittium offers proven mobile devices and cybersecurity solutions certified up to CONFIDENTIAL level. Bittium is listed on the Nasdaq Helsinki Exchange. www.bittium.com
Contact: Dominik Pöttinger, Sales Manager, Bittium Germany GmbH
tel. +49 (0)171 8336956, dominik.poetzing@bittium.com



Black Box Deutschland GmbH**B 05**

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 #B05. Sehen Sie sich das flexible Emerald® KVM-über-IP System mit sicherem Zugriff auf physikalische und virtuelle Maschinen an. MCX AV-über-IP zeigt neue Möglichkeiten für Simulationsanwendungen ohne Kompression und Latenz.

BLACK BOX**blackned GmbH****S 40**

Die Firma blackned GmbH hat sich seit ihrer Gründung im Jahr 2009 auf die Entwicklung von softwarebasierten Verteidigungslösungen spezialisiert. Besonders mit der taktischen Middleware RIDUX und dem Management-System XONITOR bildet das Unternehmen das Herzstück einer fortschrittlichen Architektur zur Digitalisierung von Landstreitkräften. Das digitale Ökosystem TACTICAL CORE, das von blackned entwickelt wurde, stellt einen zukunftssicheren und offenen Rahmen für die Umsetzung von Digitalisierungsprojekten innerhalb der NATO-Streitkräfte dar. Mit einem klaren Schwerpunkt auf modernen Technologien und kundenorientierten Lösungen strebt blackned danach, innovative Produkte und Dienstleistungen anzubieten, um die Anforderungen im Bereich der digitalen Transformation der Streitkräfte effektiv zu erfüllen. Ansprechpartner:

Thomas Hesse, Managing Director Sales, sales@blackned.de

blackned**Bren-Tronics International Solutions****S 83**

Bren-Tronics Inc. is a global designer and manufacturer of US Army qualified NiMH and Li-ion rechargeable batteries such as BB-390B/U and BB-2590/U. Bren-Tronics also designs and produces advanced portable power systems for military applications. With more than 150,000 military batteries produced per year, BTI is the largest global military manufacturer. We are servicing more than 35 different countries including NATO forces.

Our main business lines are:

- Military and industrial primary and rechargeable battery packs
- Military universal chargers
- Stand-alone renewable power stations
- Soldier Modernization Power platform
- Large scale rechargeable lithium-ion battery for vehicular and shelter applications

Bren-Tronics**Broadcast Solutions GmbH****F 14**

Broadcast Solutions ist einer der größten Systemintegratoren Europas und plant und realisiert in Europa, Asien und dem Mittleren Osten Projekte für Sicherheitseinrichtungen, First Responder, Einsatzkräfte und BOS. Wir bieten mobile oder fest-installierte Lösungen, die von körpergetragenen bis hin zu taktischen drahtlosen Kommunikationslösungen reichen, sowie eine Reihe ergänzender Technologien und Tools, die kundenorientierte, schlüsselfertige Implementierungen ermöglichen.

Wir sind Spezialisten für feste oder mobile Installationen und können die unterschiedlichsten Technologien in mobile und festinstallierte Einheiten integrieren. Diese können für Situational Awareness, verdeckte Ermittlungen oder vernetzte Operationsführung eingesetzt werden.

BroadcastSolutionsGmbH, Tel: +496721 40080, info@broadcast-solutions.de, <https://broadcast-solutions.de/de/behoerdenkommunikation/>

**broadcast
SOLUTIONS**
GOVERNMENTAL COMMUNICATION

WIR LASSEN WORTEN DATEN FOLGEN

IT-Plattformen einsatzfähig zur Verfügung stellen?
Als Integrationspartner der Bundeswehr haben wir Lösungen dieser Art längst für Sie gepackt.

Besuchen Sie uns auf **Stand W02**

**Computacenter**

Brodit

„Made in Sweden“ – Brodit entwickelt, designt und fertigt geräte- und fahrzeugspezifische Integrations- und Montagelösungen für Tablets, Drucker, Smartphones, Funkgeräte, sowie GPS-Geräte aus Kunststoff sowie Aluminium. Brodit-Halterungen und -Ladestationen sind maßgeschneidert, um den alltäglichen Anforderungen gerecht zu werden.

Brodit ist einer der weltweit führenden Lösungs-Anbieter für Montage und Integration von mobilen Geräten in Fahrzeugen und in fordernden Umgebungen entwickelt. Brodit-Halterungen für Geräte-Hersteller wie Samsung, Apple, Bittium, Ecom, und viele andere sorgen dafür, dass Ihre Geräte jederzeit sicher verstaut, aufgeladen, griffbereit und einsatzbereit sind.

Das 1983 gegründete inhabergeführte Unternehmen beschäftigt 220 Mitarbeiter und exportiert in mehr als 100 Länder seine Produkte.



F 14

Bundeswehr BAPersBw/HRLab

Das Bundesamt für das Personalmanagement der Bundeswehr (BAPersBw) gewährleistet das Personalmanagement und die Personalführung des überwiegenden Anteils der militärischen und zivilen Angehörigen der Bundeswehr. Wesentliche Aufgabe ist es, die Einsatzfähigkeit der Streitkräfte sicherzustellen.

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



R 62

Bundeswehr Kdo Cyber- und Informationsraum R 46

Die Digitalisierung hat unsere Welt maßgeblich verändert: Neben Chancen birgt sie auch Risiken. Die IT-Netze der Bundeswehr zu betreiben und zu schützen sowie in fremden Systemen aufzuklären und zu wirken, gehört zu den Aufgaben der Teilstreitkraft Cyber- und Informationsraum. Als „zentrales Nervensystem“ stellt sie die Vernetzung der Streitkräfte sicher und erschließt technologische Innovationen. Damit leistet diese TSK einen wichtigen Beitrag zur digitalen Kriegstüchtigkeit der Bundeswehr – denn Führungsfähigkeit geht mit Informationsüberlegenheit einher. Im Kommando CIR in Bonn befindet sich der Dienstsitz des Inspektors CIR und seines Vertreters, der als Chief Information Security Officer die Gesamtverantwortung für die Informationssicherheit der Bundeswehr trägt.



Bundeswehr Kommando Heer

Das Kommando Heer ist das Planungs-, Führungs-, Lenkungs- und Kontrollinstrument des Inspektors des Heeres. Das Kommando ist der zentrale Ansprechpartner für das Bundesministerium der Verteidigung und andere Organisationsbereiche der Bundeswehr in Angelegenheiten der Landstreitkräfte und für die 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. Dazu wurden unter einheitlicher Führung des „Chief Digital Officer Heer/Landbasierte Operationen“ die Führungsfähigkeit (G6), Operations Research, Modellbildung und Simulation, Concept Development und Experimentation und die „Digitalisierung Dimension Land“ zusammengefasst.



S 66

Bundeswehr Kdo Sanitätsdienst (Kdo SanDstBw) S 65

Das Kommando Sanitätsdienst der Bundeswehr führt den Zentralen Sanitätsdienst und ist fachlich für die Gesundheitsversorgung der gesamten Bundeswehr verantwortlich. Darüber hinaus nimmt das Kommando im Rahmen der Eigenvollzugskompetenz, soweit diese der Bundeswehr durch Rechtsvorschriften übertragen wurde, bestimmte Aufgaben auf dem Gebiet der öffentlich-rechtlichen Aufsicht wahr. Das Kommando Sanitätsdienst der Bundeswehr gestaltet im Zusammenwirken mit seinen Fähigkeitskommandos Verfahren und Abläufe so, dass die sanitätsdienstliche Versorgung der Soldatinnen und Soldaten sowohl im Inland als auch im Einsatz jederzeit gewährleistet ist.



Bundeswehr Kdo Streitkräftebasis

Die Streitkräftebasis (SKB) ist der zentrale Dienstleister für Heer, Luftwaffe, Marine, Sanitätsdienst sowie Cyber- und Informationsraum. Insbesondere in den Bereichen Logistik, ABC-Abwehr und Feldjäger liegen die besonderen Fähigkeiten dieses Organisationsbereiches als „Möglichmacher“ für die Auftrags Erfüllung der Bundeswehr. Die SKB bündelt die genannten Fähigkeiten schnell, flexibel und stellt diese auf den Punkt für alle Kräfte der Bundeswehr dort bereit, wo sie gebraucht werden. Die SKB leistet darüber hinaus wesentliche Beiträge für die Aus- und Fortbildung der gesamten Streitkräfte in der Bundeswehr. In der Summe: Der Beitrag der SKB ist essentiell für eine funktionierende Landes- und Bündnisverteidigung.



R 58

Bundeswehr Kdo Luftwaffe

Die Luftwaffe nimmt jederzeit lufthoheitliche Aufgaben wahr. Dazu überwacht sie den Luftraum Deutschlands mit Radarflug- und Leitzentralen und hält für die Sicherstellung der Lufthoheit reaktionsfähige Jagdflugzeugverbände bereit. Hinzu kommt das Herstellen und Erhalten ihrer personellen und materiellen Einsatzbereitschaft und die Teilnahme an Hilfs-, Rettungs- oder Evakuierungseinsätzen weltweit. Die Luftwaffe passt in Krisen ihre Einsatzbereitschaft flexibel an die Lageentwicklung an und leistet in internationalen Konflikten zusammen mit anderen Teilstreitkräften und verbündeten Streitkräften ihren Beitrag. Im Vordergrund steht dabei der Schutz der Bevölkerung und der lebenswichtigen Infrastruktur, die Wahrung der Integrität des Hoheitsgebietes und die Gewährleistung der politischen Handlungsfreiheit Deutschlands.



G 03

Bundeswehr Marinekommando

Wir leben in einem maritim geprägten Jahrhundert. Die Bedeutung der Meere für die Menschheit und Europa nimmt immer mehr zu. Dies wird angesichts der aktuellen geopolitischen Entwicklungen und durch die Entsendung einer Fregatte der Deutschen Marine in das Rote Meer unterstrichen.

Das Marinekommando nimmt als dem Bundesministerium der Verteidigung unmittelbar nachgeordnete höhere Kommandobehörde maritime Aufgaben auf allen militärfachlichen und zentralen Gebieten der Bundeswehr wahr. Dem Marinekommando sind mit der Einsatzflottille1 in Kiel, der Einsatzflottille2 in Wilhelmshaven und dem Marinefliegerkommando in Nordholz, drei maritime Großverbände unterstellt, darüber hinaus das Marineunterstützungskommando in Wilhelmshaven, die Ausbildungseinrichtungen sowie das Schiffahrtsmedizinische Institut der Marine.



G 03

Bundeswehr Organisationsbereich Ausrüstung/ BAAINBw

Der Organisationsbereich Ausrüstung, Informationstechnik und Nutzung (OrgBer AIN) gliedert sich in das Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAAINBw) und seinen Geschäftsbereich; sechs Wehrtechnische Dienststellen, zwei Wehrwis-



N 05

senschaftliche Institute, das Marinearsenal und die Deutsche Verbindungsstelle des Rüstungsbereichs in Reston, USA. Hauptaufgabe ist die bedarfs- und forderungsgerechte Ausstattung der Bundeswehr mit leistungsfähigen 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.

Bundeswehr Planungsamt

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

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



R 61

BWI GmbH

Die BWI GmbH ist primärer Digitalisierungspartner der Bundeswehr. In Frieden, Krise und Krieg erbringt sie für die Bundeswehr stabile, sichere und effiziente IT-Services im In- und Ausland, vom Grundbetrieb bis in den einsatznahen Bereich. Als attraktiver Arbeitgeber gewinnt und bindet sie hochqualifizierte Kräfte, welche die Bundeswehr-IT aus Überzeugung voranbringen. So trägt sie zur kontinuierlichen Erhöhung der Führungs- und Einsatzfähigkeit sowie Kampfkraft der Streitkräfte bei. www.bwi.de



F 07

CAE GmbH

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.



W 05

.INNO
NOW YOU KNOW

HERR VON DATEN UND LAGE

**Aktuell und präzise. Das Lagebild jederzeit beherrschen:
mit SCOPE, der Analysesoftware Made in Germany.**

Bleiben Sie Herr der Lage und treffen Sie schnelle und effiziente Entscheidungen zum Schutz eigener Kräfte und zur Unterstützung militärischer Operationen.

Jetzt informieren: info@innosystec.de

WWW.INNOSYTEC.DE

Capgemini Deutschland GmbH

N 02

Capgemini ist einer der weltweit führenden Partner für Unternehmen bei der Steuerung und Transformation ihres Geschäfts durch den Einsatz von Technologie. Die Gruppe ist jeden Tag durch ihren Purpose angetrieben, die Entfaltung des menschlichen Potenzials durch Technologie zu fördern – für eine integrative und nachhaltige Zukunft. Das Unternehmen wurde 1967 in Grenoble, Frankreich, gegründet und bietet heute ein umfassendes Dienstleistungsspektrum – von Strategieentwicklung und Design bis hin zum Geschäftsbetrieb. Dabei setzt Capgemini auf die sich schnell weiterentwickelnden Innovationen in den Bereichen Cloud, Data, KI, Konnektivität, Software, Digital Engineering und Plattformen.

Kontakt: Marc Akkermann Email: marc.akkermann@capgemini.com



A 03 + F 04



CGI

CGI Deutschland B.V. & Co. KG ist die unabhängige deutsche Tochter von CGI Inc., einem auf Nachhaltigkeit ausgerichteten globalen Dienstleister für IT- und Geschäftsprozesse. In Deutschland bieten wir unseren Kunden mit über 5.000 Mitarbeitenden – davon etwa 700 im Bereich Defence, Intelligence und Space – strategische IT- und Business-Beratung, Systemintegration, Managed IT und Intellectual Property auf Topniveau. Die Bundeswehr unterstützen wir seit über 47 Jahren im Grundbetrieb wie in Übungen und Einsätzen. Von dieser Erfahrung profitiert die NATO besonders in unseren Projekten mit KI-basierter Verarbeitung von Vorgängen. Unser Produkt CGI eGov360 bildet die Basis für DokMBw und die entsprechenden Services in GMN.

Carl-Cranz-Gesellschaft

R 24

Gesellschaft für technisch-wissenschaftliche Weiterbildung

Technisch-wissenschaftliche Weiterbildung für Ingenieure und Naturwissenschaftler auf höchstem Niveau – dieser Aufgabe widmet sich die Carl-Cranz-Gesellschaft e.V. (CCG) als gemeinnützige Einrichtung seit über 60 Jahren. Mit führenden Experten aus Forschung & Entwicklung sowie Industrie erarbeiten wir das Potenzial zukunftssträchtiger Technologien und stellen bedarfsgerechte, praxisorientierte Fort- und Weiterbildungen als offene Seminare sowie bei Bedarf auch Inhouse zur Verfügung. Kleine Lerngruppen und renommierte Dozenten aus Hochschule, Forschung und Industrie garantieren den Lernerfolg. Zu unseren Kernkompetenzen zählen die Fachgebiete Informations- und Kommunikationstechnologie, Führungs- und Aufklärungssysteme, Sensorik, Transport- und Verkehrssysteme, Verteidigungs- und Sicherheitstechnik, Werkstoffkunde und Werkstofftechnologie sowie fachgebietsübergreifende Querschnittsthemen.



Carmenta Germany GmbH

W 11

Carmenta liefert Softwarewerkzeuge zur Visualisierung, Analyse und Verwaltung georeferenzierter Daten für ortsbezogene Situationsanalysen innerhalb missionskritischer Anwendungen. Die Technologie ist für die vollständige Integration in Kundenanwendungen konzipiert, kann alternativ aber auch als Kernstück für jegliche Geospatial Webservice-Umgebung eingesetzt werden. Carmenta liefert seit 1985 hochwertige Software an militärische Endkunden, Systemhäuser und Unternehmen für Zivile Sicherheit. In enger Zusammenarbeit mit ihrer globalen Kundenbasis, investiert Carmenta kontinuierlich in die Weiterentwicklung ihrer Technologie. Mehr als 30 Jahre Erfahrung machen Carmenta's Technologien zur kompletten, marktführenden Lösung für situative Entscheidungsfindung. Kontakt: Carmenta Germany GmbH, www.carmenta.com, Andreas Stiebner, Pacellistraße 8, 80333 München, Tel: +49 162 2718891, andreas.stiebner@carmenta.com



CeoTronics AG

F 26

CeoTronics ist ein führender Hersteller von professionellen Kommunikationslösungen, die in den schwierigsten Umgebungsbedingungen zum Einsatz kommen. Feuerwehren, industrielle Anwender, Airlines, Airports sowie Polizei- und Militäreinheiten vertrauen unseren Produkten – national wie international. Die CeoTronics-Gruppe beschäftigt rund 130 Mitarbeiterinnen und Mitarbeiter, die meisten davon am Standort Rödermark vor den Toren von Frankfurt am Main. Der Konzern umfasst die CeoTronics AG und drei Tochterunternehmen, Außendienstmitarbeiter im In- und Ausland sowie Partner, die die Produkte weltweit in ausgewählten Ländern vertreiben. Die Verwendung neuester Technologien, Beratungskompetenz, Kundennähe und ausgezeichnete Produktqualität machen den Erfolg von CeoTronics seit der Gründung 1985 bis heute aus.

https://www.ceotronics.com, E-Mail: sales@ceotronics.com



Check Point

W 02

Check Point Software Technologies Ltd. (<https://www.checkpoint.com/de/>) ist ein führender Anbieter einer KI-gestützten, in der Cloud bereitgestellten Cybersicherheitsplattform, die über 100.000 Organisationen weltweit schützt. Check Point nutzt die Kraft der KI überall, um die Effizienz und Genauigkeit der Cybersicherheit durch seine Infinity-Plattform zu verbessern, mit branchenführenden Erkennungsraten, die eine proaktive Antizipation von Bedrohungen und intelligenteren, schnelleren Reaktionszeiten ermöglichen. Die umfassende Plattform umfasst Cloud-Technologien, bestehend aus Check Point Harmony zur Absicherung des Arbeitsplatzes, Check Point CloudGuard zur Absicherung der Cloud, Check Point Quantum zur Absicherung des Netzwerks und Check Point Infinity Core Services für kollaborative Sicherheitsabläufe und -dienste.



CHIFFRY GmbH

F 29

Chiffry Unterstützungssystem für sichere Einsatzkommunikation

Chiffry ist eine Kommunikationsplattform für Smartphones zum Unterstützen von Einsatzeinheiten durch verschlüsselte Text-, Sprach-, Bild-, Video- und Standort-Nachrichten sowie abhörsichere Telefonate und Telefon-Konferenzen. Bei der Verschlüsselung orientiert sich Chiffry an den BSI-Richtlinien und setzt auf modernste Ende-zu-Ende Verschlüsselung mit 256-Bit AES. Die Business Version des Messengers ist im besonderen Maße an die Bedürfnisse von Behörden und Organisationen mit Sicherheitsaufgaben (BOS) angepasst und beinhaltet die Installation des Servers in die IT-Infrastruktur des Auftraggebers. Zudem besteht die Möglichkeit zur Integration der Kommunikationsplattform in abgehardete Betriebssysteme, Container-Lösungen wie beispielsweise MobileIron und Samsung Knox sowie in VPN-Infrastrukturen. www.chiffry.de



Chora A/S

S 76

Chora liefert einzigartige, fortschrittliche Lösungen für kritische Herausforderungen und schafft effektive und benutzerfreundliche Systeme.

Wir bieten EW-Lösungen und -Produkte zur Überwachung und Lokalisierung, die für eine Vielzahl von use cases geeignet sind. Unsere Lösungen umfassen fortschrittliche Antennen, SDR-basierte Sensoren, integrierte Datenbanken und intuitive Benutzeroberflächen einschließlich GIS-Ansichten. Chora verfügt über ein umfassendes Wissen über die Branche, was eine wesentliche Voraussetzung dafür ist, dass wir unsere Forschungs- und Entwicklungsanstrengungen und -ausgaben auf die Konzeption von Produkten konzentrieren können, die den sich wandelnden Anforderungen der Kunden entsprechen.



Cisco Systems GmbH

F 08

Cisco macht das Internet möglich. Wir vernetzen Menschen, Daten, Prozesse und Dinge sicher miteinander – so treiben wir Innovationen, von der Wirtschaft und Gesellschaft profitieren.

Wir spannen die Brücke zum Möglichen.

Alles, was wir tun – jede Innovation, die wir vorantreiben – dient unserem Ziel: die Zukunft für alle inklusiver zu gestalten. Cisco bietet ein branchenführendes Portfolio an technologischen Innovationen. Mit Netzwerkinfrastrukturen, Cybersicherheit, Rechenzentrumsausrüstung, Videokommunikations- und Kollaborationslösungen, Cloud, Software und Services tragen wir zur sicheren Vernetzung von Unternehmen, Behörden, Organisation und dem deutschen Staat als strategischer Partner bei.



citema group GmbH

R 54

Driving Digital Technologies.

Die citema group GmbH ist Ihr Innovations-, Technologie- und Entwicklungspartner für Ihre Projektvorhaben, insbesondere im sicherheitskritischen Bereich. Gemeinsam mit unseren Kunden entwickeln wir mit unseren Tochterunternehmen citema consulting, citema experts und citema systems Softwareprodukte und -Services, Sicherheits- und Systemarchitekturen sowie Cyber Security und KI-Vorhaben. Unsere festangestellten Experten besitzen langjährige Projekterfahrungen mit fundiertem technischem und organisatorischem Know-how. Diese Expertise können wir basierend auf Werkverträgen, Dienstverträgen und Arbeitneh-



merüberlassungsverträgen bereitstellen. Die citema group und ihre Töchter gewährleisten Ihnen als inhabergeführte und deutsche Unternehmen ein Höchstmaß an Stabilität, Vertraulichkeit und Sicherheit.

Codan Communications/Domo Tactical Communications (DTC)/DTC

F 14

Codan Communications/Domo

Tactical Communications (DTC)

is a global technology company that develops robust technology solutions to solve customers' communications, safety, security and productivity problems in some of the harshest environments around the world.

The mission critical solutions secure, share and communicate real-time video, voice and data to enable Shared Situational Awareness (SSA) on land, on sea, in the water and in the air. DTC's Cutting-edge Mobile Adhoc Network (MANET) Mesh radio solutions deliver ultra-low latency, end-to-end encryption and are used globally on-board USV, UAV and UGV platforms to support mobile, long range semi-autonomous and autonomous operations.

www.codancomms.com/www.domotactical.com,
boris.seiter@codancomms.com



Computacenter AG & Co. oHG

W 02

Computacenter ist ein führender, unabhängiger Technologie- und Servicedienstleister, dem öffentliche Auftraggeber und große Unternehmen vertrauen. Wir helfen unseren Kunden bei der Beschaffung,



infodas SDoT Cross Domain Solutions.

Marktverfügbar / Zugelassen / Kriegserprobt

Mit infodas Cybersecurity zu mehr Resilienz und nachhaltiger Sicherheit im Zuge der Zeitenwende.

NATO-konforme Lösungen zur Sicherung komplexer Multi Domain Operationen.

infodas
connect more. be secure.



der Weiterentwicklung und dem Betrieb ihrer IT-Infrastruktur, um eine digitale Transformation zu ermöglichen, die Menschen und deren Geschäft erfolgreich macht.

In Deutschland sind wir mit rund 7.000 Mitarbeiter:innen einer der führenden ICT-Anbieter. An unserem Hauptsitz in Kerpen betreiben wir eines der modernsten Integration Center. Weltweit beschäftigt Computacenter über 20.000 Menschen. Wir arbeiten weltweit mit den führenden Technologiepartnern zusammen, um unseren Kunden jederzeit die sichersten und besten Lösungen, maßgeschneidert auf ihre Anforderungen, zur Verfügung zu stellen.

Comrod Communication AS

F 17

Comrod Communications AS have their corporate headquarters in Stavanger, Norway with manufacturing facilities in Norway, France, Hungary and the USA. Comrod designs and manufactures manpack, vehicle, remote and shipboard antennas in the HF/VHF/UHF/SHF frequency bands. Sophisticated multiband versions are available to overcome co-site or space constraints. Support masts are available to elevate top loads at heights ranging from 5 to 34 metres (16 to 110 ft). Aluminium telescopic, composite telescopic, sectional tripod and manpack sectional models are available. Comrod ComPack series power supplies and battery chargers provide the best power to size density available on the market today.



Comtech Systems

S 30

Comtech Systems ist auf Troposcatter-Kommunikation spezialisiert. Diese Art der Kommunikation ermöglicht Datenverbindungen mit hohen Datenraten und einer niedrigen Latenz für Entfernungen bis über den Horizont hinaus. Bei diesen Verbindungen ist man weder auf Satelliten noch auf quasi-optische Sichtverbindungen angewiesen. Troposcatter-Kommunikationen bieten ein höheres Maß an Vertraulichkeit und Integrität der Daten sowie einen höheren Schutz vor Aufklärung als die meisten Mikrowellen- und Satellitenkommunikationsverbindungen. Comtech ist mit seinen Troposcatter-Modems, die in über 90% der weltweit eingesetzten, modernen Troposcatter-Systemen verbaut sind, unangefochtener Marktführer in der fortschrittlichen Troposcatter-Technologie.

Kontakt: JK Defence & Security Products GmbH, Industriering Ost 74 47906 Kempen
milcom@jkdefence.de, www.jkdefence.de, 02152/1445-207



CONDOK GmbH

S 01

Das Systemhaus für technische Dienstleistungen, Technik und Logistik

Das Leistungsspektrum der CON-DOK umfasst die Bereiche Systementwicklung und Dienstleistungen im Rahmen des Integrated-Logistics-Support. Dazu gehören u.a. die Technische Dokumentation, die Produkt- und Betriebssicherheit, die logistische Betreuung von Produkten und Systemen sowie die Software-Entwicklung für das logistische Datenmanagement. Als Systemhaus entwickelt und realisiert CONDOK Einrüstungs- und Umrüstungsmaßnahmen in Kabinen und Fahrzeugen und führt Instandsetzungsleistungen durch. Die CONDOK GmbH beschäftigt an den Standorten Kiel, Hamburg und Koblenz mehr als 280 Mitarbeiter. Kontakt: www.condok.de



CONET

S 45

„Erfolg. Unsere Leidenschaft.“ CONET ist der Digitalisierungspartner mit Fokus auf Consulting, Customer Experience, Data Intelligence, Managed Services, SAP und Software Development. Seit mehr als 30 Jahren begleitet CONET die Bundeswehr zuverlässig auf dem Weg einer sicheren digitalen Transformation. Durch partnerschaftliche Zusammenarbeit, Innovationsfähigkeit, Prozess-Know-how und hohe Dienstleistungsqualität entstehen erfolgreiche Lösungen in den Bereichen von SAP und Non-SAP, Individualsoftware, Architekturmanagement, Doku-



mentenmanagement, Datenmanagement, IT-Infrastruktur und IT-Sicherheit. Auf der AFCEA 2024 präsentiert CONET im Schwerpunkt Lösungsansätze für Decision Intelligence zur schnellen Echtzeit-Lagefeststellung, Location Intelligence im KI-gestützten Dialog mit Lagebildern, Assistance Intelligence im Dialog mit technischen Dokumenten und intelligentes Asset Management mit Digitalen Zwillingen.

Kontakt: www.conet.de | info@conet.de

Conrad Elektronik SE

F 35

Conrad Electronic steht als zuverlässiger Partner seit 1923 für Technik und Elektronik und bietet heute als Sourcing Plattform 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 Sortiment mit Millionen von 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, Zeit und Kosten zu sparen. Hersteller und Distributoren erreichen als Seller auf dem Conrad Marketplace neue Zielgruppen und Märkte. Das Familienunternehmen ist in 17 Ländern Europas am Markt vertreten.



Constructor University | rasdaman GmbH

R 18

Big Datacube Analytics in Earth and Space, with location-transparent federation, is the key innovation brought by Constructor University and its spin-off, rasdaman GmbH.

Our rasdaman engine offers best-of-breed performance, seamless scalability from nanosats to cloud to super-scale data centers, flexibility and AI integration on spatio-temporal sensors, images, image timeseries, weather/climate timeseries, etc. The rasdaman AI-Cube™ technology has pioneered AI-enabled Big Datacube Analytics for spatio-temporal Earth data and beyond. The integration of AI analytics with datacube scalability is renowned for its performance, and federation of multi-dimensional datacubes. Awards: NATO Defence Innovation Challenge Award, Tech Connect World Innovation Award, and others.



Cordsen Engineering GmbH

S 75

CORSDEN Engineering GmbH entwickelt und fertigt eine breite Palette an militärisch gehärteter (Rugged) IT-Hardware nach MIL-STD-810F / MIL-STD-461E für mobilen und stationären Einsatz; sowie abstrahlsichere (TEMPEST) und individuell konfigurierbare Produkte nach SDIP

27 Level A. Beispielsweise Workstations, Notebooks, Server, Displays bis 70", FO-Hubs, Drucker und Scanner.

Wir verfügen über zwei TEMPEST/EMV-Labore: Für Zulassungsmessungen nach SDIP 27 Level A/B/C, sowie für Zulassungsmessungen und Kurzmesungen nach dem deutschen Zonenmodell (Zone 1/2/3). Kontakt: Cordsen Engineering GmbH, Am Klinggraben 1A, D-63500 Seligenstadt Tel. 06182-9294-0, Fax 06182-9294-45, www.cordsen.com



CPI Vertex Antennentechnik GmbH

R 27

CPI Vertex Antennentechnik GmbH zählt zu den führenden Herstellern von Antennen- und Bodenstationssystemen für die Satellitenkommunikation. Mit einer breiten Palette an Systemlösungen bedient Vertex Kunden weltweit mit hochwertigen Produkten und Dienstleistungen, die schlüsselfertig aus dem Ruhrgebiet geliefert werden. Ergänzt werden kann das Rundum-Sorglos-Paket mit allen Produkten der amerikanischen Muttergesellschaft CPI, einem weltweit agierenden Hersteller von elektronischen Komponenten und Subsystemen. Zu den Kunden zählen Telekommunikationsunternehmen, Rundfunkanstalten, Regierungsbehörden und Militärorganisationen. Vertex zeichnet sich durch



Innovationskraft, Zuverlässigkeit und hohe Qualität aus. Kontinuierliche Forschung und Entwicklung halten das Unternehmen an der Spitze der Branche und tragen zur Verbesserung der globalen Kommunikation bei.

cpm GmbH

vertrauensvoll, kompetent, zuverlässig
Seit 35 Jahren können Sie auf uns zählen. Informationen für Bundeswehr, Politik, wehrtechnische Industrie und Forschung. Das Verlags- und Veranstaltungshaus, die Kommunikationsprofis der Community! Wir sind etablierter Kommunikator und Multiplikator zwischen Streitkräften, Politik, Verteidigungsindustrie und Forschung. Dank weitreichender und langjähriger Erfahrungen umfasst unser Angebot eine hohe Expertise in Redaktion und Marketing sowie der Organisation von Veranstaltungen der wehrtechnischen Community. Aushängeschild unseres Verlages ist unser Fachmagazin cpmFORUM - das Magazin für Entscheider und Garant für Informationen aus erster Hand. In Kombination unserer Produktlinien cpmPUBLICATIONS, cpmEVENTS und cpmDIGITAL schaffen wir durch unseren einzigartigen Multichannel-Ansatz ein engmaschiges 360° Informationsnetzwerk.



N 06

Crisis Prevention (CP) – Beta Verlag

CRISIS PREVENTION (CP) ist das behördliche Fachmagazin für Gefahrenabwehr, Innere Sicherheit und Katastrophenhilfe. Der Leserkreis sind Dienststellenleiter und Multiplikatoren aus den Behörden und Organisationen mit Sicherheitsaufgaben (BOS), Hilfsorganisationen, Betreiber Kritischer Infrastrukturen, der Bundeswehr sowie Bundesämtern und Verbänden, Ministerien und Verwaltungen. Dieser Leserkreis erhält die CP quartalsweise (personalisiert) deutschlandweit direkt in die jeweilige Dienststelle. Der Verteiler wird in Zu-



R 09

sammenarbeit mit den Institutionen ständig erweitert und aktualisiert. Der Bezug an die Dienststelle ist für hauptberuflich Beschäftigte in dem o. g. Leserkreis kostenfrei. Nähere Infos finden Sie unter: www.crisis-prevention.de

CyberArk Software (DACH) GmbH

R 47

CyberArk ist das weltweit führende Unternehmen für Identity Security. Basierend auf intelligenten Berechtigungskontrollen bietet CyberArk die umfassendste Sicherheitslösung für jede menschliche oder nicht-menschliche Identität über Business-Anwendungen, verteilte Arbeitsumgebungen, hybride Cloud-Umgebungen und den gesamten DevOps-Lifecycle hinweg. Weltweit führende Unternehmen vertrauen beim Schutz ihrer kritischsten Assets auf CyberArk.



dainox GmbH

S 33

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®. Nehmen Sie Kontakt zu uns auf: dainox GmbH | info@dainox.net | +49 (0) 8247 33609 0 | www.dainox.net.



ADVERTORIAL

Cyberresiliente Glasfasernetze

Optische Netze bilden die Grundlage der Kommunikationsinfrastruktur in vielen kritischen Einrichtungen. Die hohe strategische Bedeutung von Glasfaserinfrastrukturen impliziert eine hohe Schutzwürdigkeit. Dies gilt besonders wegen einer zunehmenden Bedrohungslage durch geopolitische Verwerfungen oder Naturkatastrophen. Eine **robuste Verschlüsselung** in Kombination mit einer **starken Authentifizierung** sind eine bewährte Methode, um Daten auf der Übertragungsstrecke vor Diebstahl, Missbrauch und Manipulation zu schützen. Für eine langfristige, kompromisslose Sicherheit ist der Einsatz von quantensicherer Verschlüsselung mit Post-Quanten-Kryptografie oder Quantum Key Distribution (QKD) unerlässlich. Betreiber von Glasfaserinfrastrukturen müssen in der Lage sein, feindliche Ak-

tionen an jedem Punkt ihres großflächigen Netzes schnell zu detektieren, zu identifizieren und zu lokalisieren. **Faser-Monitoring** liefert mittels OTDR-Technik in Echtzeit Informationen, um Unterbrechungen zu orten aber auch andere Störungen zu erkennen.

Für die **schnelle Wiederherstellung** von Verbindungen im Fehlerfall müssen bei Planung und Installation des Netzes zusätzlich Ressourcen für die Ersatzschaltung vorgehalten werden. Die Wiederherstellung der gestörten Strecken auf dem optischen Layer schützt eine hohe

Anzahl von Verbindungen auf höheren Netzsichten und stellt einen wesentlichen Beitrag zur **Resilienz eines Netzes** dar.



Adva Network Security bietet Kompetenz, Lösungen und Dienstleistungen für resiliente Fasernetze im Hochsicherheitsbereich.

Dassault Systèmes Deutschland GmbH

R 11

Dassault Systèmes, the 3DEXPERIENCE Company, is a catalyst for human progress. We provide business and people with collaborative virtual environments to imagine sustainable innovations. By creating 'virtual twin experiences' of the real world with our 3DEXPERIENCE platform and applications, our customers push the boundaries of innovation, learning and production. Dassault Systèmes' 20,000 employees are bringing value to more than 300,000 customers of all sizes, in all industries, in more than 140 countries. www.3ds.com



Data Respons Solutions GmbH

N 07

Everything Digitalized, Secured, Connected & Automated.

Als Experte für die Entwicklung von Hardware im Militärbereich rüstet Data Respons Solutions bereits seit 1986 Streitkräfte in der Europäischen Union (oder EU) mit modernsten Embedded Technologielösungen aus. Unser Fokus liegt auf der Konzeption von Systemen und Lösungen für Marineeinsätze, 4G & 5G Militärkommunikation und robusten In-Vehicle-Technologien für militärische Fahrzeuge. Unser Verständnis für die spezifischen Anforderungen und Herausforderungen in diesem Bereich, einschließlich militärischer Normen, Umweltbelastungsfaktoren, Sicherheits- und Regierungsanforderungen, ermöglicht es uns, Lösungen zu entwickeln, die hohe Zuverlässigkeit und Schutz für kritische Funktionen unter extremen Umweltbedingungen bieten.



Data-Warehouse GmbH

F 36

Die Data-Warehouse GmbH (www.dwh.info) ist als inhabergeführtes, Münchner Mittelstandsunternehmen seit 1987 am Markt aktiv. Unser Firmenmotto „Use Your Information“ setzen wir erfolgreich mit Produkten in den Bereichen Datenmanagement (1995), Cybersecurity (1981), Softwareentwicklung (1987) und Datenschutz (1994) für unsere Kunden aus Verteidigung (Luftwaffe, Armee, Marine), Banken, Logistik und Transport, Luftfahrt, Sozialwesen, Automobilbau und erneuerbare Energien ein. Unsere Mission zielt auf die Verbesserung von Effizienz, Qualität und Transparenz in komplexen IT-basierten Umgebungen, für die wir in den Bereichen IT-Strategie, Digitalisierung, Compliance, Cryptoassets (z. B. PKI), Datenmanagement, Supply Chains, Produktlebenszyklen, Betrieb und Cyber Security Lösungen bieten.



Datagroup Defense IT Services

A 04 + S 16

Die DATAGROUP Defense IT Services betreut und unterstützt behördliche und industrielle Kunden aus dem Bereich Aerospace & Defense. Als Teil der DATAGROUP bieten wir als Full-Managed Service Provider über flexible und hybride Liefermodelle einen modular skalierbaren IT-Betrieb „as-a-Service“ an. Unsere Services werden vollständig aus Deutschland heraus erbracht und decken sowohl VS-NfD Umgebungen wie auch Mischsysteme aus regulären Netzen und VS-NfD Umgebungen ab.

Unsere zusätzlichen branchenspezifischen Lösungen und Services in den Bereichen DefenseCloud, Service Desk, Field Service, Mobile Device Management, VPN/Netzwerk, und Mobile Micro Datacenter haben eines gemeinsam: Sie sind immer managed, secure und VS-NfD konform.



DATAGROUP

Dataminr Germany GmbH

B 12

First Alert, die Software von Dataminr für den öffentlichen Sektor, bietet die früheste Übermittlung von aktuellen Nachrichten und ermöglicht die schnellstmögliche Reaktion auf kritische Ereignisse. First Alert verwendet künstliche Intelligenz,



um hochwirksame Ereignisse aus über 1.000.000 öffentlich verfügbaren Informationsquellen (Open Source Information) zu erkennen und liefert Echtzeit-Benachrichtigungen zu aktuellen Nachrichten an Organisationen weltweit.

DCON GmbH

F 32

Wir sind DCON. Wir denken das Service Management öffentlicher Organisationen weiter.

Wie wir das machen? Wir sehen die Themen Automatisierung und Digitalisierung durch die Augen unserer Public-Kunden. Und mit Servity – unserer Enterprise Service Management Software, die Organisationen genau in diesen Vorhaben unterstützt. Dafür bringt Servity wertvolle Features mit, wie bspw. mehrstufige Genehmigungen, Verlegefähigkeit, Mandantenfähigkeit uvm. und ein umfassendes Best Practice Framework zum Start ins automatisierte und digitalisierte Service Management. Wer sich im Public-Sektor 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.



Dell Technologies

R 51 + S 18

Dell Technologies unterstützt als global agierender Technologieanbieter Unternehmen und Organisationen dabei, ihre digitale Zukunft zu gestalten, ihre IT umfassend zu transformieren und ihr wichtigstes Gut – ihre Daten – wirksam zu schützen. Das Portfolio des Konzerns, der mit seinen über 130.000 Mitarbeitern in 180 Ländern der Welt tätig ist, reicht dabei von Clients über Server- und Speichersysteme bis hin zu umfassenden Software- und IT-Security-Lösungen sowie professionellen Dienstleistungen.



Deloitte Consulting GmbH

B 09 b

Deloitte ist ein weltweit führender Dienstleister in den Bereichen Audit und Assurance, Risk Advisory, Steuerberatung, Financial Advisory und Consulting und damit verbundenen Dienstleistungen; Rechtsberatung wird in Deutschland von Deloitte Legal erbracht. Unser weltweites Netzwerk von Mitgliedsgesellschaften und verbundenen Unternehmen in mehr als 150 Ländern (zusammen die „Deloitte-Organisation“) erbringt Leistungen für vier von fünf Fortune Global 500®-Unternehmen. Erfahren Sie mehr darüber, wie rund 330.000 Mitarbeiter von Deloitte das Leitbild „making an impact that matters“ täglich leben: www.deloitte.com/de.



Detecon International GmbH

S 73

Detecon ist eine führende, weltweit agierende Managementberatung mit Hauptsitz in Deutschland, die seit über 40 Jahren klassisches Management Consulting mit hoher Technologiekompetenz vereint. Ihr Leistungsschwerpunkt liegt im Bereich der digitalen Transformation: Detecon hilft Unternehmen aus allen Wirtschaftsbereichen, ihre Geschäftsmodelle und operativen Prozesse mit modernster Kommunikations- und Informationstechnologie an die Wettbewerbsbedingungen und Kundenanforderungen der digitalisierten, globalisierten Ökonomie anzupassen. Das Know-how der Detecon bündelt das Wissen aus erfolgreich abgeschlossenen Management- und ICT-Beratungsprojekten in über 160 Ländern. Detecon ist ein Tochterunternehmen der T-Systems International, dem herstellerübergreifenden Digitaldienstleister der Deutschen Telekom.



Deutsche Telekom

Die Deutsche Telekom gehört mit rund 252 Millionen Mobilfunk-Kundinnen und Kunden, 25 Millionen Festnetz- und 22 Millionen Breitband-Anschlüssen zu den führenden integrierten Telekommunikations-Unternehmen weltweit. Wir bieten Produkte und Dienstleistungen aus den Bereichen Festnetz/Breitband, Mobilfunk, Internet und Internet-TV für Privatkundinnen und -kunden sowie Lösungen der Informations- und Kommunikationstechnik für Groß- und Geschäftskundinnen und -kunden. Die Deutsche Telekom ist in mehr als 50 Ländern vertreten. Im Geschäftsjahr 2023 haben wir mit weltweit 199.652 Mitarbeitenden (31.12.2023) einen Umsatz von 112 Milliarden Euro erwirtschaftet.

A 11 + F 06 a



DIAMOND GmbH

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



DIAMOND
the fiber meeting

R 17

DIGITTRADE GmbH

KOBRA VS Datenträger – externe verschlüsselte Festplatten und USB-Sticks mit BSI-Zulassung bis VS-NfD, NATO- und EU-RESTRICTED
Der KOBRA Stick VS und das KOBRA Drive VS sind vorwiegend für Behörden und Unternehmen mit Geheimschutzbetreuung entwickelt und hergestellt. Die Vertraulichkeit der Daten wird durch die AES-Verschlüsselung mittels Verwendung zweier 256-Bit-Kryptoschlüssel, die Zwei-Faktor-Authentifizierung mittels Smartcard und PIN sowie die Verwaltung der Krypto-Schlüssel gewährleistet.
Verwaltungssoftware Kobra Client VS
Diese Software unterstützt Administratoren bei der Einrichtung und Verwaltung von KOBRA VS Datenträger. KOBRA Client VS steht kostenfrei zur Verfügung und ermöglicht die Nutzung zusätzlicher Funktionen dieser Datenträger. DIGITTRADE GmbH, Tel.: +49/345/2317353, E-Mail: kundendienst@digittrade.de, Webseite: www.kobra-infosec.de



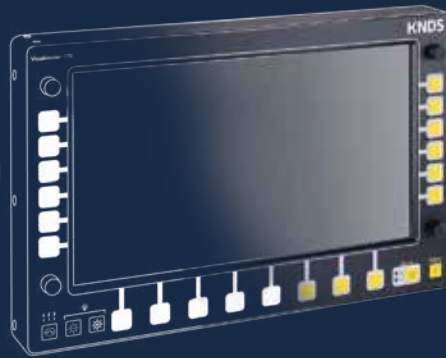
F 29

Dreger Group GmbH

Unser Schwerpunkt: Wir sind spezialisiert auf den Aufbau und den Betrieb von kompakten Führungseinrichtungen / Gefechtsständen mit Online und Offline Betrieb der Lageführung, gehärteter Informations- und Kommunikationstechnologien, OSINT Aufklärung, Lokalisierung In- und Outdoor sowie Nutzung und Abwehr Unbemannter Systeme im Rahmen von Cyber / Hybrider Kriegsführung, auch unter CBRNE Schutz.



G 02



Neuer Name – immer noch 100% Tec-Knowledge

Aus ATM ComputerSysteme GmbH wird KNDS Deutschland Mission Electronics GmbH KNDS, ein führender europäischer Hersteller militärischer Landsysteme mit Sitz in Amsterdam, hat mit Wirkung vom 08. April 2024 seine Konzerngesellschaften Nexter Systems S. A. und Krauss-Maffei Wegmann GmbH & Co. KG formal umbenannt. Krauss-Maffei Wegmann GmbH & Co. KG firmiert nunmehr als KNDS Deutschland GmbH & Co. KG, Nexter Systems S. A. als KNDS France S. A. Im Zuge dieser Umbenennungen wurde der Name der Tochtergesellschaft ATM ComputerSysteme GmbH in KNDS Deutschland Mission Electronics GmbH umfirmiert.

KNDS Deutschland
Mission Electronics GmbH
www.knds-electronics.de

Besuchen Sie uns auf der
AFCEA Fachausstellung 2024
26. – 27. Juni 2024
World Conference Center Bonn
Saal New York/Genf · Stand S48

KNDS

Dazu trainieren wir Einsatzkräfte, KRITIS Betreiber, Behörden in den jeweiligen Tätigkeitsfeldern, um die Handlungsfähigkeit bei vielfältigen Bedrohungen sicherzustellen. Dabei nutzen wir modernste, verfügbare und handhabbare Technologien.

Ganzheitliche Sicherheit – strategische Beratung bis operative Unterstützung. MISSION READY – ONLINE AND OFFLINE...

dtec.bw – Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr

N 03

Das dtec.bw ist ein von beiden Universitäten der Bundeswehr (UniBw) gemeinsam getragenes wissenschaftliches Zentrum und Bestandteil des Konjunkturprogramms der Bundesregierung zur Überwindung der COVID-19-Krise. Mit der Aufnahme in den Deutschen Aufbau- und Resilienzplan (DARF) wird dtec.bw von der Europäischen Union – NextGenerationEU finanziert. Diese Mittel werden an beiden UniBw zur Finanzierung von Forschungsprojekten und zum Wissen- und Technologietransfer eingesetzt. Mit 68 laufenden Projekten zu digitalen Schlüsseltechnologien und einem einzigartigen Themenspektrum, das u.a. Raumfahrttechnik, 5G-/6G-Technologie, quantengesicherte Kommunikation, Mobilität der Zukunft, Sensorik und Künstliche Intelligenz bis hin zu Kompetenzen für die digitale Arbeitswelt abdeckt, ermöglicht dtec.bw Forschung mit Mehrwert für alle Dimensionen.



DWT - Deutsche Gesellschaft für Wehrtechnik e.V. R 55

Die DEUTSCHE GESELLSCHAFT FÜR WEHRTECHNIK e.V. 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 / Bundeswehrverwaltung, anderen Behörden / Organisationen mit Sicherheitsaufgaben (BOS) 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.



Dynamit Nobel Defence GmbH (DND)

S 31

Die Dynamit Nobel Defence GmbH (DND) ist ein mittelständisches Systemhaus der wehrtechnischen Industrie. Unser Werksgelände umfasst mehr als einen Quadratkilometer und beherbergt 260 Gebäude und Fertigungskomplexe zur Entwicklung, Fertigung und Erprobung unserer Hochtechnologieprodukte. Weitere Standorte der DND sind Berlin und Leipzig. Mehr als 400 Mitarbeiterinnen und Mitarbeiter sind bestrebt, unseren Kunden und Partnern die zuverlässigsten und leistungsfähigsten Produkte und Dienstleistungen in unseren Geschäftsfeldern zu bieten. Unser Portfolio umfasst heute 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. www.dn-defence.com



EAL Leidel GmbH

S 42

Die EAL Leidel GmbH steht seit 1902 für Präzision und Zuverlässigkeit im Bereich der elektrischen und datentechnischen Steckverbindungen und Geräte. Mit seewasserbeständigen CEE-Steckvorrichtungen sorgen wir auf deutschen Marine Schiffen seit über 50 Jahren für eine verlässliche Verbindung. Unsere robusten LWL-Steckvorrichtungen werden neben Kabelverlegesystemen im Militär eingesetzt. Mit hoher Zuverlässigkeit beliefern wir



weltweit eine Vielzahl von Kranherstellern mit unseren Steckvorrichtungen für raue Umgebungen und das bereits seit 1958! Unsere hochwasserdichten smarten Landstromlösungen versorgen die Schiffe im größten Binnenhafen Europas.

Unser innovationsstarkes und familiegeprägtes Team sorgt mit seiner langjährigen Erfahrung stets für die beste Lösung. Wir haben auch die Lösung für ihre Aufgabenstellung! www.leidel-gmbh.de

ECOS Technology GmbH

F 27

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. Das ECOS SecureConferenceCenter bietet alle Funktionen einer modernen Videokonferenzlösung. Für den Zugriff außerhalb eines gesicherten Netzes erlaubt die Kombination mit dem ECOS SecureBootStick VS-NfD-konforme Videokonferenzen. Die ECOS TrustManagementAppliance ist eine skalierbare und einfach integrierbare PKI- und Key-Management-Lösung zur Absicherung von mobilen Geräten, PCs, Servern oder Prozessen. Sie dient zum Ausstellen, Validieren, Ausrollen und Verwalten von Zertifikaten und Schlüsseln.

ECOS Technology GmbH, 55276 Oppenheim, +49 6133 939-200, info@ecos.de, www.ecos.de



Edgeless Systems

S 85

Edgeless Systems entwickelt in Deutschland weltweit führende Open-Source-Lösungen für Confidential Computing. Mit der Software von Edgeless Systems sind Daten immer – auch zur Laufzeit – verschlüsselt und Anwendungen können vollständig von der Compute-Infrastruktur isoliert werden. Mittels kryptographischer Nachweise kann sichergestellt werden, dass beispielsweise Cloud-Admins, fremde Regierungen und Hacker/Co-Tenants an keine Daten kommen. Die Public Cloud wird so zur eigenen Private Cloud. Weitere Anwendungsfälle sind KI-Anwendungen für geheime und personenbezogene Daten, sowie mobile Rechenzentren bei denen Daten nicht physisch ausgelesen werden können. Software von Edgeless Systems wird bereits bei der BWI und in der deutschlandweiten ePatientenakte eingesetzt.



EGL Elektronik Vertrieb GmbH

S 57

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 Informationen führen.

Mit geeigneten Abschirmmaßnahmen kann diese kompromittierende Abstrahlung auf ein nicht auswertbares Maß reduziert werden. Auf diese Abschirmung und Entstörung hat sich die Firma EGL Elektronik Vertrieb GmbH spezialisiert. Gerne stehen wir Ihnen für Fragen zur Verfügung.

Tel.: 06051-71838, E-Mail: info@eglgmbh.de



EIZO Europe GmbH

S 82

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 Video-erfassung, 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.

Elbit Systems Deutschland GmbH & Co. KG

F 23

Zur 37. Auflage der AFCEA Fachausstellung mit dem Rahmenthema „Zeitenwende in der nationalen Sicherheit – Resilienz durch disruptive digitale Lösungen“ wird Elbit Systems Deutschland mit modernsten Systemen aus dem Bereich C4I&Cyber vor Ort sein. Neben echten Innovationen hat das Ulmer Systemhaus darüber hinaus bewährte Produkte im Gepäck, z. B. D-LBO-Lösungen der Serie E-LynX für Soldaten- und Führungsfunk, Kurzwellenfunk sowie SATCOM on the Move. Auch bereits eingeführte Geräte, wie das PNR1000 oder das HRM9000, die bei den Streitkräften vieler NATO-Partner sowie bei der Bundeswehr in der Nutzung sind, werden an Stand F23 im WCC Bonn zu sehen sein. Mehr Informationen unter www.elbitsystems-de.com



eleQtron GmbH

R 63

eleQtron ist der erste deutsche Hersteller von Quantencomputern. Um zum führenden Anbieter von Quantencomputerrechenzeit in Deutschland zu werden, werden derzeit sukzessiv leistungsstärkere, bahnbrechende Quantencomputer aufgebaut und an die Cloud angebunden. Dafür setzt das junge Unternehmen



Elma Electronic

S 15

Elma Electronic ist ein weltweit führender Anbieter von Embedded-Computing-Lösungen, darunter integrierte Chassis-Plattformen, Board-Produkte, Backplanes, modulare Gehäuse, Elektronik-schränke und Präzisionshardware-Komponenten sowohl für Standard- wie auch für kundenspezifische Konfigurationen. Als globale Organisation bleiben wir mit unseren eigenen Vertriebs-, Design- und Fabrikationsstandorten auf drei Kontinenten weltweit nah an unseren Kunden und Partnern.

Unsere Produkte sind bekannt für größte Widerstandskraft und exzellente Kühlkonzepte. Hardware-Spezifikationen wie OpenVPX, die Sensor Open Systems Architecture (SOSA) oder auch CompactPCI Serial wurden von uns maßgeblich mitgestaltet.

Zuverlässigkeit und langfristige Unterstützung mit tiefgreifender technischer Kompetenz und hochpräzisiertem Engineering – Das ist Elma Electronic.



ELP GmbH European Logistic Partners

B 01

Seit ihrer Gründung im Jahr 1989 befasst sich die ELP GmbH European Logistic Partners mit der technischen Ausstattung für den polizeilichen und militärischen Entschärfungsdienst. Die Spezialisierung des Unternehmens liegt da-



DRIVING THE FUTURE OF DEFENCE & SECURITY

Die ESG ist herstellerunabhängiger System-integrator und der nationale Technologie- und Innovationspartner für Verteidigung und öffentliche Sicherheit. Wir treiben mit unseren Lösungen und Services die sichere Digitalisierung und Vernetzung in allen Dimensionen voran. Dabei übernehmen wir die Entwicklung, Realisierung, Betreuung und den Betrieb einzelner Plattformen und komplexer Gesamtsysteme: innovativ, umsetzungsstark, leidenschaftlich.

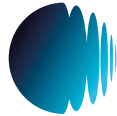
bei auf erklärungsbedürftigen und anspruchsvollen Technologien. Zunächst ausschließlich auf den Bereich der Fernhandhabung (z.B. mit Haken- und Leinensätzen) konzentriert, wurde das Produktsortiment um portable Röntgentechnik, ballistische Schutzvorrichtungen, Spreng- und Disruptortechnik sowie Drogen- und Sprengstoffdetektoren ergänzt. Ab dem Jahr 2003 erweiterte die ELP GmbH European Logistic Partners ihr Vertriebsprogramm um Fernlenkmanipulatoren. 2016 hielt damit verbunden die leistungsstarke, sichere Mobile-ad-hoc-Networking (MANET) Funk-/Datenlösung für taktische Einsätze Einzug.

ELT Group Deutschland

S 34

Als Unternehmen der deutschen Sicherheits- und Verteidigungsindustrie seit 1978 in der Elektronischen Kampfführung (EloKa) tätig, bieten wir seit knapp zwanzig Jahren mobile Lösungen für die Öffentliche Sicherheit. Das Unternehmen dient der Bundeswehr sowie Behörden und Organisationen mit Sicherheitsaufgaben (BOS) als Ausstatter mit nationalen Schlüsseltechnologien. Zu den Kernkompetenzen und Geschäftsfeldern zählen:

- die Integration und Instandsetzung von EloKa Sensoren in Trägerplattformen für den taktischen, operativen und strategischen Einsatz
- die Entwicklung von RF-basierten Systemen für den Test, Verifikation, Evaluierung und Ausbildung von Radar, COM und EloKa Anlagen
- die Entwicklung und Integration von mobilen Überwachungs- und Abhörsystemen in mobilen Anwendungen für die öffentliche Sicherheit



**ELTGROUP
DEUTSCHLAND**

Endace

R 48

EndaceProbe's scalable, always-on packet capture provides unified visibility of activity across your entire hybrid cloud network -- delivering the evidence needed to detect and respond to incidents quickly and accurately. Rapid, centralized search and datamining can be integrated into all your security and performance tools, putting accurate forensic evidence at your fingertips when you need it. Packet data can be replayed to analytics tools, for powerful back-in-time investigative capability. Find out more at www.endace.com



ESG Elektroniksystem- und Logistik-GmbH

F01

Die ESG ist herstellerunabhängiger Systemintegrator und der nationale Technologie- und Innovationspartner für Verteidigung und öffentliche Sicherheit. Wir treiben mit unseren Lösungen und Services die sichere Digitalisierung und Vernetzung in allen Dimensionen voran. Dabei übernehmen wir die Entwicklung, Realisierung, Betreuung und den Betrieb einzelner Plattformen und komplexer Gesamtsysteme: umsetzungsstark, leidenschaftlich, innovativ. Auf der Fachausstellung präsentieren wir Digitalisierungslösungen für Multi-Domain Operations: das Joint Fire Support Team abgesehen zur Anforderung und Lenkung des Close Air Supports sowie des Indirekten Feuers, das Innovationsvorhaben Augmented Common Operational Picture zur interaktiven 3D-Visualisierung des Gefechtsfelds, sowie das neue NATO-Standard CESMO zum systemübergreifenden Austausch von Bedrohungen im elektromagnetischen Spektrum.



Esri Deutschland GmbH

F 22

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



Esri unterstützt die Anwender mit einem breit gefächerten Schulungs-, Support- und Consultingangebot und dem gesamten Erfahrungsreichtum von mehr als 250 Mitarbeitern.

Eviden (an Atos company)

F 31

Eviden ist ein Technologieführer im Bereich datengesteuerter, vertrauenswürdiger und nachhaltiger digitaler Transformation. Mit einem starken Portfolio an Technologien in den Bereichen Advanced Computing, Sicherheit, KI, Cloud und digitale Plattformen bietet Eviden Fachwissen in mehr als 47 Ländern. Eviden vereint 53.000 Weltklasse-Talente und erweitert die Möglichkeiten von Daten und Technologie über das gesamte digitale Kontinuum hinweg. Eviden ist ein Unternehmen der Atos-Gruppe mit einem Jahresumsatz von über 5 Milliarden Euro. Eviden präsentiert auf der AFCEA seine Lösungskompetenz von der stationären bis zur mobilen Führungsfähigkeit.

EVIDEN Germany GmbH, Von-der-Wettern-Str. 27, 51149 Köln
Klaus Schindler (Vertriebsleiter Defense), Tel: +49 (151) 6782 1789
klaus.schindler@eviden.com



Extron

S 05

Extron Electronics ist einer der führenden Hersteller professioneller AV-Systemprodukte, einschließlich AV-Mediensteuerungen, Computer-Video-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.



FERCHAU Aviation Group

B 04

Der Geschäftsbereich Aviation der FERCHAU GmbH und die RST Rosstock 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.



FFG Flensburger Fahrzeugbau Gesellschaft mbH

F 14

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. Nicht umsonst vertrauen Auftraggeber aus über 40 Ländern seit vielen Jahren auf Fahrzeugtechnologie „Made in Flensburg“.

Ob Instandsetzung und Wartung, Modifikation, Rüstsatzintegration, Modernisierung oder eigenständige Neuentwicklung von Rad- und Kettenfahrzeugen: Die FFG stellt sich jeder Herausforderung!



Forschungszentrum Space – UniBw München

S 74

Das Forschungszentrum SPACE der Universität der Bundeswehr München, integriert fakultätsübergreifend Experten aus den verschiedenen wissenschaftlichen Disziplinen. Hierdurch ergibt sich ein weitreichendes Kompetenzprofil, welches es erlaubt, raumfahrtbezogene Problemstellungen unter verschiedenen Gesichtspunkten aller relevanten Disziplinen zu untersuchen. Es können einerseits neue Technologien und Entwicklungstrends umfassend identifiziert sowie strategische Handlungsempfehlungen daraus abgeleitet werden. Andererseits resultiert aus



der hochkarätigen Forschung der einzelnen Mitglieder in ihren spezifischen wissenschaftlichen Domänen und deren Koordination über das Forschungszentrum SPACE die aktive Gestaltung, Entwicklung und Implementierung innovativer Technologien und Methoden. Dabei werden sowohl Kerngebiete der Raumfahrt wie die Satellitentechnologie abgedeckt als auch terrestrische Anwendungen wie Kommunikation, Navigation und Erdbeobachtung.

FORTINET, Inc.

S 04

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. Zu den Kunden von Fortinet gehören große Unternehmen, Behörden und Service Provider aus allen Branchen, darunter Fertigung, Gesundheitswesen, Finanzdienstleistungen und Bildung.

FORTINET

Fraunhofer FKIE

F 15

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
FKIE

Fraunhofer IOSB

F 14 + W 01

Beratung und Technologie für die Verteidigung: In seinem größten Geschäftsfeld betreibt das Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung IOSB grundlagenorientierte wehrtechni-

Fraunhofer
IOSB

ADVERTORIAL



DIAMOND - HOCHLEISTUNGSLÖSUNGEN

www.diamond.de

DIAMOND ist ein weltweit führender Lieferant von hochpräzisen Glasfaser-Lösungen und beliefert seit über 40 Jahren erfolgreich verschiedene Märkte.

UNSER UNTERNEHMEN

DIAMOND ist ein internationales Unternehmen mit Hauptsitz in der Schweiz, welches sich auf die Entwicklung, Fertigung und Montage von hochpräzisen faseroptischen Komponenten und Baugruppen spezialisiert hat. Durch die Verwendung einer Zwei-Komponenten Ferrule, kombiniert mit dem patentierten Active Core Alignment-Prozess, erreichen die DIAMOND Steckverbinder beste Einfügedämpfungen. Durch dieses spezielle Verfahren ist es DIAMOND möglich, in allen Produkten höchste Leistungen zu erzielen. Darüber hinaus ist DIAMOND stolz darauf, der Erfinder des weltberühmten E-2000®-Steckers und weltweit der einzige Anbieter eines ESA-zertifizierten (ESCC) Einkanal-Weltraumverbinders zu sein.

UNSERE QUALITÄT

Als vertikal integriertes Unternehmen mit Produktion in der Schweiz ist DIAMOND einer der wenigen Hersteller mit vollständiger Kontrolle über ihre Herstellungsprozesse. DIAMOND ist in der Lage, hochwertige Keramik, Metalle und Kunststoffkomponenten, ausgehend vom Rohmaterial direkt bis hin zum fertigen Produkt, zu verarbeiten. Dadurch ist es möglich, die verschiedenen Herstellungsprozesse strengen Kontrollen zu unterziehen und zu garantieren, dass jede einzelne Komponente die hohen Qualitäts-, Zuverlässigkeits- und Leistungsstandards der DIAMOND erfüllt.



UNSERE KOMPETENZ

Mit über 40 Jahren Erfahrung ist DIAMOND ein Spezialist in Glasfaser-Verbindungs-Lösungen. Ursprünglich aus dem Telekommunikationsmarkt, entwickelt sich DIAMOND immer mehr zu einem Anbieter von Speziallösungen für raue Umgebungen (Weltraum, Avionik, Verteidigung) und Industrieanwendungen (Messinstrumente, Lidar/Laser). Die DIAMOND Harsh Environment-Stecker überzeugen

mit ihren herausragenden Eigenschaften für raue Umgebungsbedingungen wie hohe IP-Schutzklassen, Schock-, Schwingungs- und Vibrationsbeständigkeiten sowie starke mechanische Beanspruchungsresistenzen. Sie sind neben der Standardausführung auch als Linsen- und High Power Stecker zur Übertragung hoher optischer Leistungen ausführbar. Diamond verfügt auch über spezielle Hochtemperaturstecker.

sche Forschung und entwickelt daraus Machbarkeitsstudien und Verfahren. Es bewertet Trends und Technologien, prüft und entwickelt Demonstratoren, unterstützt die Industrie und stellt innovative Ausrüstung her. Kernkompetenzen sind die Erzeugung von Bildern und verwandten Sensor-signalen, ihre algorithmische Verarbeitung und Auswertung sowie die Nutzbarmachung in benutzerfreundlichen Systemen. Dabei konzentrieren wir uns auf die Bereiche Aufklärung, Navigation, Simulation, Satellitentechnik, land-, luft- und seegestützte Plattformen, Zielannäherung, Wirkung und Schutz, die Ausrüstung des Soldaten sowie Informationstechnologie. www.iosb.fraunhofer.de/verteidigung

Frequentis Deutschland GmbH

S 28

Frequentis ist ein internationaler Marktführer von Kommunikations- und Informationssystemen für militärische Gefechtsstände und Leitstände mit sicherheitskritischen Aufgaben. Frequentis entwickelt und liefert Produkte und Systemlösungen für die militärische Flugsicherung und die Luftverteidigung, einschließlich Luftraummanagement für unbemannte Systeme (UAV) und Counter UAV.



Fujitsu Germany GmbH

F 13

Fujitsu ist ein globaler Partner für die Digitale Transformation und hat sich zum Ziel gesetzt, die Welt nachhaltiger zu gestalten und mit Innovationen das Vertrauen in die Gesellschaft zu fördern. Mit rund 124.000 Mitarbeitern unterstützt Fujitsu seine Kunden in über 100 Ländern, einige der größten Herausforderungen der Menschheit zu lösen. Das Dienstleistungs- und Lösungsportfolio für nachhaltige Transformation basiert auf fünf Schlüsseltechnologien: Computing, Networks, AI, Data & Security und Converging Technologies.



GAF AG

A 10 + F 09

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



Galvion

S 30

Galvion hat es sich zur Aufgabe gemacht, militärische und taktische Missionen auf der ganzen Welt zu unterstützen. Unsere Abteilung Active Power & Data Systems konzipiert, entwickelt und liefert integrierte Lösungen, die die Leistungsfähigkeit und Überlebensfähigkeit moderner Soldatensystemen verbessern. Das Nerv Centr® vernetzt dabei alle Komponenten datenseitig und versorgt sie flexibel mit Energie. Leistungsstarke, kompakte Batterien mit bis zu 140 Wh ergänzen das einsatzerprobte System darüber hinaus. JK Defence & Security ist Partner von Galvion für Deutschland und Schweiz. Kontakt: JK Defence & Security Products GmbH, Industriering Ost 74, 47906 Kempen, milcom@jkdefence.de, www.jkdefence.de, 02152/1445-207



GBS TEMPEST & Service GmbH

S 03

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). Adresse: von-Braun-Straße 6 D-49356 Diepholz, Tel: +49 5441 9758-100, Fax: +49 5441 9758-129, Homepage: <http://www.gbs-tempest.de>, E-Mail: info@gbs-tempest.de



genua GmbH

S 25

Excellence in Digital Security

Die genua GmbH ist Enabler der digitalen Transformation. Wir schützen sensitive IT-Netzwerke im Public- und im Enterprise-Sektor, bei KRITIS-Organisationen und in der geheimschutzbetreuten Industrie. Als Tochter der Bundesdruckerei-Gruppe entwickeln und produzieren wir unsere IT-Security-Lösungen ausschließlich in Deutschland. Laut regelmäßiger Zulassungen und Zertifizierungen des BSI erfüllen diese die höchsten Sicherheitsstandards.

Kontakt: tel +49 89 991950-902 | vertrieb@genua.de | www.genua.de



Gesellschaft für Sicherheitspolitik e.V.

R 07

Wir sind die am 5. Januar 1952 gegründete Gesellschaft für Sicherheitspolitik e.V., die älteste sicherheitspolitische Bildungsinstitution der Bundesrepublik Deutschland.

Wir leisten mit unseren Sektionen, geführt von ehrenamtlich tätigen Sektionsleitern jährlich bis zu 1.000 öffentliche Veranstaltungen.

Wir vermitteln in unserer Informationsarbeit mit glaubwürdigem Engagement, überzeugender Kompetenz und nachvollziehbarer Argumentation die tiefgreifenden Veränderungen des internationalen Sicherheitsumfeldes.

Wir kommunizieren den im Grundgesetz verankerten Gedanken einer wehrhaften und streitbaren Demokratie als Voraussetzung für Frieden, Freiheit und Sicherheit.

Wir fördern die öffentliche sicherheitspolitische Debatte in Deutschland wider das Desinteresse in Fragen der Außen-, Sicherheits- und Verteidigungspolitik.



Getac Technology GmbH

B 09 a

Getac ist ein weltweit führender Anbieter robuster mobiler Technologie und intelligenter Videolösungen, darunter Notebooks, Tablets, Software, Bodycams, Kfz-Video-systeme, digitales Beweismanagement sowie Videoanalyselösungen für Unternehmen. Die Dienstleistungen und Lösungen von Getac sind so konzipiert, dass sie allen Arbeitenden an vorderster Front und in fordernder Umgebung erstklassige Erfahrungswerte bieten. In über 100 Ländern versorgt Getac Kunden in den Bereichen Verteidigung, öffentliche Sicherheit, Feuerwehr, Sanitäts- und Rettungsdienst sowie Versorgung, Automobilbau, Rohstoffe, Fertigung, Transport & Logistik. Weitere Informationen unter: <http://www.getac.com>



Glenair GmbH

S 72

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.

Google Germany GmbH

G 01

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 der Transformation unterstützen. Kunden in mehr als 200 Ländern und Regionen setzen auf Google Cloud als ihren Technologiepartner des Vertrauens.



GovRadar GmbH

R 63

Die GovRadar GmbH wurde im Jahr 2020 gegründet und hat sich seitdem erfolgreich entwickelt. Im Jahr 2022 erfolgte die Markteinführung ihrer innovativen Softwareplattform. Mit stetigem Wachstum verzeichnet die Plattform bereits über 1.000 aktive Nutzer im Jahr 2023. GovRadar bietet eine benutzerfreundliche Lösung für öffentliche Auftraggeber, um Ausschreibungsunterlagen einfach, schnell mit Hilfe von künstlicher Intelligenz zu erstellen. Unsere Plattform erleichtert den gesamten Erstellungsprozess der Unterlagen und optimiert die Effizienz bei der Beschaffung öffentlicher Aufträge, indem bis zu 94 % der Vorbereitungszeit eingespart werden.



griffity defense GmbH

F 14

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 klaren, 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, überlebensfähige Kommando- und Befehlsstellen“ zeigen wir auf der AFCEA 2024 mit unseren Partnern anhand von fiktiven Szenarien modulare Lösungen, die einen wesentlichen Beitrag zur Ausgestaltung von mobilen Führungs- und Gefechtsständen für die Digitalisierung der Landstreitkräfte in der taktischen Ebene leisten können. (info@griffity-defense.de)



H&G Hansen & Gieraths IT Solutions GmbH

F 25

H&G Hansen & Gieraths ist ein bundesweit tätiges IT-Systemhaus mit Hauptsitz in Bonn und weiteren Präsenzen an sechs Standorten in Deutschland. Seit über 35 Jahren betreuen wir unsere Kunden der öffentlichen Hand ganzheitlich von der Desktop-Bereitstellung bis zur Planung, Implementierung und Betreuung komplexer Server- und Storage-Systeme sowie kritischer Infrastrukturen ganz nach ihren individuellen Anforderungen. Unser Systemhaus bietet zudem umfassende Cyberresilienz-Lösungen, um sensible Daten vor aktuellen und zukünftigen Bedrohungen zu schützen und gewährleistet eine robuste IT-Infrastruktur für den reibungslosen Betrieb in sicherheitskritischen Bereichen. Mehr erfahren Sie auf <http://www.hug.de>, oder folgen Sie uns auf LinkedIn.



Sicher. Verbunden. Jederzeit.



AUFKLÄRUNG



KOMMUNIKATION



NAVIGATION

Sichere, schnelle und zuverlässige Kommunikationswege sind für die Einsatzfähigkeit unserer Streitkräfte essentiell und für eine erfolgreiche vernetzte Operationsführung unabdingbar. Fortschrittliche Satellitensysteme gewährleisten diese souveräne Handlungsfähigkeit. Mit der Entwicklung der agilen und robusten SmallGEO-Plattform haben wir die Systemfähigkeit für geostationäre Satellitenkommunikation zurück nach Deutschland gebracht. Sie ist zur Deckung des hoheitlichen Bedarfs optimal konzipiert und wird der Bundeswehr im Rahmen der Heinrich-Hertz-Satellitenmission zusätzliche, unabhängige Kommunikationskapazitäten und Datenverbindungen zur Verfügung stellen: **Sicher. Verbunden. Jederzeit.** Mehr über Deutschlands führendes Raumfahrtssystemhaus erfahren Sie unter: www.ohb-system.de

Hagenuk Marinekommunikation GmbH

B 07

Die Hagenuk Marinekommunikation GmbH (HMK) ist eine Tochtergesellschaft der ATLAS ELEKTRONIK und gehört zum thyssenkrupp-Konzern. Integrierte Fernmeldeanlagen kommen zum Einsatz auf U 212 A, den Korvetten K130, sowie den Einsatzgruppenversorgern (jeweils 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. Portfolio:

- HF-Sender/Transceiver (3003er Serie bis 10 kW, 1,5 – 30 MHz)
 - VLF/HF-Empfänger (10 kHz – 30 MHz)
 - HF-Verstärker mit Antennenanpassgeräten für SVFuA
 - HF-Breitbandsysteme
 - Antennensysteme
 - IP Backbone für Kommunikationssysteme/Subsysteme der internen/externen Kommunikation
 - Message Handling und Steuerungssysteme
- Hagenuk Marinekommunikation GmbH, 24220 Flintbek, +49 (0) 4347-714-101, www.hmk.atlas-elektronik.com, info@hmk.atlas-elektronik.com



HAT.tec GmbH

R 14

Die HAT.tec GmbH ist ein Unternehmen für Softwareentwicklung, Forschung und Beratung, das sich auf die Entwicklung von disruptiver Missionsoftware für „Human Autonomy/Human-AI“ und „Manned-Unmanned Teaming“, dem gemeinsamen koordinierten Einsatz von bemannten und unbemannten Systemen, spezialisiert hat. Zielsetzung ist, menschliche und maschinelle Stärken gewinnbringend zu kombinieren, um die Missionsleistung in hochkomplexen Umgebungen durch solche „Human Autonomy Teams“ zu maximieren.

HAT.tec's Kernkompetenzen umfassen die Nutzung modernster Technologien der Künstlichen Intelligenz, automatisiertes Denken, Planen und Entscheiden sowie die Verarbeitung und Analyse von Sensordaten, um Softwarelösungen zu schaffen, die den Output von Missionsplanungsaufgaben, Flugleistung und allgemeine menschliche Fähigkeiten in der modernen Avionik dramatisch verbessern.



Heinen ICS

S 57

Der Unternehmensbereich Heinen ICS aus dem Haaner Unternehmen Heinen Elektronik GmbH hat sich im Markt für militärisch genutzte IT-Komponenten und IT-Sicherheit positioniert und das Produktspektrum stetig erweitert. Auf der Basis von kommerzieller am Markt verfügbarer Computer-Hardware werden von Heinen ICS neben projektspezifischen, gehärteten und militärischen IT-Produkten ergänzende Hardware-Komponenten entwickelt, die ein Höchstmaß an Hardware-Sicherheit für den zukünftigen Computer-Arbeitsplatz garantieren. Wir bieten Lösungen vom kleinen MIL-Gigabit-Switch bis zu komplexen, vernetzten Systemkomponenten für ComSec Zone 1 und zugeschnittene kunden- bzw. projektspezifische Sonderlösungen für den Einsatz unter extremen Umweltbedingungen.

Gehärtete Geräte- und Systemlösungen:

- Hochleistungs-MIL-Server
- Switches
- Display-Lösungen
- Arbeitsplatz-Computer
- integrierbare Kontroll- und Überwachungssysteme (BITE)



HENSOLDT

A 07 + W 07

HENSOLDT ist ein führendes Unternehmen der europäischen Verteidigungsindustrie mit globaler Reichweite. Das Unternehmen mit Sitz in Taufkirchen bei München entwickelt Sensor-Komplettlösungen für Verteidigungs- und Sicherheitsanwendungen. Als Technologieführer treibt HENSOLDT die Entwicklung der Verteidigungselektronik und Optronik voran und baut sein Portfolio auf der Grundlage innovativer Ansätze für Datenfusion, Künstliche Intelligenz und



Cybersicherheit kontinuierlich aus. Mit ca. 7000 Mitarbeitern erzielte HENSOLDT 2023 einen Umsatz von 1,85 Milliarden Euro. HENSOLDT ist an der Frankfurter Wertpapierbörse im MDAX notiert.

Hexagon – HxGN Safety & Infrastructure GmbH S 14

Hexagon unterstützt nationale Verteidigungsstrategien mit zukunfts-sicheren Technologielösungen, die verbündeten Nationen einen dauerhaften Vorteil verschaffen. Unsere fortschrittlichen Lösungen umfassen Sensorik, Positionierung, Command & Control, Lagebild, Geospatial Intelligence, Mapping- und photogrammetrische Systeme. Wir liefern Informationen zur Entscheidungsfindung und verbessern die militärische Effektivität in der Luft-, an Land und zur See. Die heutige Dynamik von Daten, Informationen und Kommunikation sowie die Konfliktauflösung selbst stellen besondere Herausforderungen. Digitale Überlegenheit ist entscheidend für den Aufbau flexibler, effektiver und agiler Streitkräfte und ihrer systemtechnischen Ausrüstung, damit die Verteidigung auf jede Art von Bedrohung und Konfrontation vorbereitet ist. <https://hexagon.com/de/industries/defence>



HEXAGON

Hirt Zerspanungstechnik GmbH

F 24

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 Konstruktion und Fertigung über die Montage bis zur Auslieferung erhalten unsere Kunden eine maßgeschneiderte Komplettlösung aus einer Hand.

Die Montage von Baugruppen und komplexen Geräten nach höchsten Qualitätsstandards ist neben der Fertigung anspruchsvoller Präzisionsteile eine unserer Kernkompetenzen. Unsere qualifizierten Mitarbeiter erfüllen höchste Anforderungen bei der Montage von mechanischen und elektronischen Baugruppen bis hin zu hochkomplexen Geräten.

Die Konfektionierung von Kabeln und Leitungen nach VG 96927-2 Grundtypen A/B/C/D und M/N/P runden unsere Kompetenzen ab.



Hitachi Vantara

F 25

Hitachi Vantara, eine hundertprozentige Tochtergesellschaft von Hitachi, Ltd., unterstützt Unternehmen bei der Digitalen Transformation von dem, was jetzt ist, zu dem, was als nächstes kommt. In Zusammenarbeit mit jedem einzelnen Kunden setzen wir unsere industriellen und digitalen Fähigkeiten ein, um das Beste aus Daten und Anwendungen herauszuholen. Dies kommt sowohl dem einzelnen Unternehmen als auch der Gesellschaft zugute. Mehr als 80 Prozent der Fortune 100-Unternehmen vertrauen Hitachi Vantara bei der Erschließung neuer Einnahmequellen, der Generierung von Wettbewerbsvorteilen, der Senkung von Kosten, der Verbesserung des Kundenerlebnisses und der Schaffung von sozialem und ökologischem Mehrwert. Besuchen Sie uns unter www.hitachivantara.com.



HP Deutschland GmbH

S 18

HP ist ein weltweit führendes Technologieunternehmen, das Lösungen entwickelt, die es den Menschen ermöglichen, ihre Ideen zum Leben zu erwecken und sich mit den Dingen zu verbinden, die am wichtigsten sind. Mit einer Präsenz in mehr als 170 Ländern bietet HP ein umfassendes Portfolio innovativer und nachhaltiger Hardware, Services und Abonnements in den Bereichen Personal Computing, Drucker, 3D-Drucklösungen, Hybrid Work, Gaming und mehr.

Als Technologieunternehmen ist HP aus der Überzeugung heraus entstanden, nicht nur Gewinne zu erzielen, sondern die Welt zu einem besseren Ort zu machen. Die jahrzehntelangen Bemühungen in den Bereichen Klimaschutz, Menschenrechte und digitale Gerechtigkeit unterstreichen dies. <http://www.hp.com>



IABG

Die IABG bietet ganzheitliche Lösungen rund um sichere Digitalisierung, IT-Unterstützung, sichere Cloud-Lösungen für den Einsatz von VS-IT bzw. 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 Architectures und 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. Wir betrachten dabei nicht nur Lösungen für den Cyber- und Informationsraum, sondern berücksichtigen auch alle Anknüpfungspunkte zu den Dimensionen Land, Luft, See und Weltraum. info@iabg.de

**W 06****IBM**

IBM ist ein führender Anbieter in den Bereichen globale Hybrid-Cloud und KI sowie Consulting. Wir helfen Kunden in mehr als 175 Ländern, Erkenntnisse aus ihren Daten zu vermarkten, Geschäftsprozesse zu optimieren, Kosten zu senken und in ihrer Branche führend zu bleiben. Mehr als 4.000 Behörden und Unternehmen in Bereichen der kritischen Infrastruktur, wie Finanzdienstleistungen, Telekommunikation und Gesundheitswesen vertrauen bei der schnellen, effizienten und sicheren digitalen Transformation auf die Hybrid-Cloud-Plattform von IBM und Red Hat OpenShift. Die bahnbrechenden Innovationen von IBM in den Bereichen KI, Quantencomputing, branchenspezifische Cloudlösungen und Consulting eröffnen offene und flexible Optionen für unseren Kunden. Gestützt wird das Ganze durch das langjährige Bekenntnis von IBM zu Vertrauen, Transparenz, Verantwortung, Inklusion und Service. Weitere Informationen finden Sie unter: www.ibm.com/de

**F 02****IABG Teleport GmbH**

Seit 1999 betreibt der IABG Teleport in Ottobrunn, südlich von München eine Satellitenbodenstation. Über diese bieten wir Kunden weltweit effiziente und hoch verfügbare Kommunikations- und Datenverbindungen und ermöglichen zuverlässige Konnektivität auch in unterversorgten und abgelegenen Regionen sowie für maritime, luftgestützte oder mobile Landanwendungen. Von unserem Standort aus erreichen wir Satelliten mit Geoposition von 55° West bis 75° Ost und decken so ein Versorgungsgebiet von Südamerika bis Ostasien ab. Unser regionaler Fokus liegt dabei auf Afrika sowie dem Nahen und mittleren Osten. Für diese Regionen betreiben wir mehrere Dienste im C- und KU-Band mit modernster Hub-Technologie.

**W 06****iesy GmbH**

Bei der iesy GmbH handelt es sich um einen Anbieter für komplexe kundenspezifische Embedded Systemlösungen. Mit Leidenschaft für Technik und einem eingespielten Team in den Bereichen Hardware- & Softwareentwicklung, Materialbeschaffung, Fertigung und Geräteprüfung ist man seit 1966 der ideale OEM- und Outsourcing-Partner zur Entwicklung und Produktion individueller Embedded Produkte. Das Unternehmen mit Sitz im Nordrhein-Westfälischen Meinerzhagen orientiert sich stets an den Bedürfnissen seiner Kunden unter-

**S 63****AFCEA 2024, Stand F23**

TRUPPE IN VERBINDUNG

HF/VHF-Kommunikation

Mit hochmodernen Funksystemen stellen wir die zuverlässige Sprech- und Datenverbindung zwischen Befehlsständen, Fahrzeugen und abgessenen Einheiten sicher – weltweit und über große Entfernungen.

www.elbitsystems-de.com



schiedlichster Märkte. Im Bereich Verteidigung bietet man sichere und robuste Computerlösungen, welche sich an den rauen Umgebungen als auch an den hohen Sicherheitsanforderungen orientieren.

iesy GmbH, Darmcher Grund 22, 58540 Meinerzhagen, www.iesy.com, info@iesy.com

IGEL Technology GmbH

F 11

IGEL ist ein revolutionäres, sicheres Endpunkt-Betriebssystem für SaaS, DaaS, VDI und sichere Browser-Umgebungen. Das IGEL Preventative Security Model™ reduziert die Angriffsfläche für Endgeräte um bis zu 95 % und senkt die TCO für Endgeräte um bis zu 75 %. IGEL OS lässt sich nahtlos verwalten und hilft Unternehmen, ihre Nachhaltigkeitsziele zu erreichen.



IHSE GmbH

S 81

Die IHSE GmbH ist ein weltweit führender Entwickler und Hersteller hochentwickelter KVM-Produkte. KVM steht für Keyboard, Video, Mouse. Mit der KVM-Technologie wird die Distanz zwischen dem Computer und den Peripheriegeräten (Tastatur, Bildschirm, Maus) verlängert. So können komfortablere und effizientere Arbeitsumgebungen und optimierte Arbeitsabläufe geschaffen werden. Unsere zertifizierten und mehrfach ausgezeichneten Produkte bestehen durch herausragende Fertigungsqualität für den Dauerbetrieb und großen Bedienkomfort. Sie stehen für höchste Sicherheit, verhindern den unbefugten Zugriff oder das Einschleusen von Malware und gewährleisten die absolute Datensicherheit. Konfigurieren Sie Ihr individuelles KVM-System aus hunderten von flexiblen Modulen für jedes Budget. Bestehende Installationen können einfach und kosteneffizient mit den neuesten Funktionen aufgerüstet werden.



Intradex GmbH

F 14

Seit über 30 Jahren kümmern wir uns um die Bedürfnisse von Behörden und Organisationen mit Sicherheitsaufgaben, sowie militärischen Anwendern. Unser Portfolio umfasst Hör-Sprechgarnituren (Headsets) und Sprech Tasten (PTT-Tasten) für Anwendungsbereiche in der Leitstelle, im Feld oder in Fahrzeugen. Made in Germany. Wir vertreten seit 2017 auch exklusiv die führenden taktischen Gehörschutzheadsets und Sprech Tasten von INVISIO und seit der Akquise von Racal Acoustics auch die führenden CVC Headsets aus England. 2024 dürfen wir Ihnen einen neuen Maßstab aktiver, taktischer, In-Ear Gehörschützer präsentieren. Das INVISIO X7 erlaubt eine einfache Nutzung bei hohem Gehörschutzniveau und eine bahnbrechende Sprachübertragungstechnologie.



Indra Avitech GmbH

S 11

Indra Avitech, eine Tochtergesellschaft der Indra Sistemas S.A., ist seit über 25 Jahren kompetenter und verlässlicher Systempartner der Bundeswehr für das FSInfo-SysBw und InfoDADBw. Unsere Kompetenzen liegen im Bereich der Aeronautischen und Hindernis Datenbanken, Luftfahrtkarten sowie Flugplan- und Pilotenbriefingssysteme inklusive Schnittstelle zur zivilen Flugsicherung und zu Eurocontrol. Darüber hinaus sind Meldungsvermittlungs- und Kommunikationssysteme wie SWIM-Lösungen bei der Bw im Einsatz. Indra Avitech Produkte werden bundeswehrweit und von den in Deutschland stationierten Bündnispartnern an ca. 100 Standorten genutzt. Auf der AFCEA 2024 ist die Bereitstellung von (aeronautischen) Daten auf EKBs (Electronic Kneeboards) unser Schwerpunkt. Kontakt: Thomas Mattick, Sen. Key Acc. Manager Bundeswehr, Bahnhofplatz 3, 88045 Friedrichshafen, Telefon: +49 7541-282-0, www.indra-avitech.aero



Indra Sistemas S.A.

S 11

Indra ist ein börsennotierter Technologie-Konzern, der als „Global Player“ Lösungen in den Bereichen Informationstechnologie für Unternehmen und Behörden, Flugsicherung & Transportwesen und Verteidigung, Raumfahrt und Sicherheit anbietet.

Das Technologieportfolio Verteidigung, Raumfahrt und Sicherheit umfasst:

- Bemannte und unbemannte Fahrzeuge,
- Simulation & Training,
- Radar-Technologie inkl. Air Defence und Military Air Traffic Management,
- Digital Defence inklusive FüInfoSys und Cyberdefence,
- Elektronische Kampfführung (EloKa) inkl. Selbstschutz,
- Schutz kritischer Infrastruktur,
- Raumfahrt inkl. Space Surveillance & Tracking und Ballistic Missile Defence (BMD) Early Warning,
- In-Service Support.
- Satellitenkommunikation,

Kontakt: Gerd Hunno Philipps, Head of Business Development Indra DE-AT-CH, Indra Avitech GmbH, Bahnhofplatz 3, 88045 Friedrichshafen, www.indracompany.com



INFODAS GmbH

S 46

INFODAS GmbH zählt zu den führenden Unternehmen für Cybersicherheit und Digitalisierung in Deutschland. Das Unternehmen entwickelt Hochsicherheitsprodukte und begleitet seit 1974 insbesondere Militär, Behörden und Organisationen mit Sicherheitsaufgaben (BOS) aber auch Unternehmen im Bereich Kritische Infrastrukturen mit einem ganzheitlichen Dienstleistungsangebot zur Initiierung, Umsetzung, Aufrechterhaltung und Prüfung der organisatorischen und technischen Informationssicherheit und zum sicheren Einsatz neuer Technologien. Die Secure Domain Transition (SDoT)-Produktfamilie gehört zu den umfassendsten Cross Domain Solutions (CDS) für unidirektionale und bidirektionale Anwendungsfälle mit strukturierten oder unstrukturierten Daten und Protokollen. Die Produkte sind für DEU GEHEIM, EU SECRET und NATO SECRET zugelassen und zum Teil CC EAL4+ zertifiziert.



INNOSYSTECH GmbH

S 06

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. Wandeln Sie Ihre Informationen in Wissen – mit SCOPE. INNO: NOW YOU KNOW.



INTRACOM DEFENSE (IDE)

F 14

INTRACOM DEFENSE (IDE) ist ein High-Tech Unternehmen der Verteidigungsindustrie in Griechenland. IDE beliefert die griechische Armee und exportiert einen großen Teil seiner Produktion an internationale Kunden wie Finnland, Frankreich, Deutschland, Israel, Großbritannien und die USA.

IDE nutzt High-End-Technologien für Design und Entwicklung moderner Systeme in den Bereichen taktische IP-Kommunikation, integrierte C4I-Systeme, Raketen Elektronik, Obervierungssysteme, hybride elektrische Energieversorgung und unbemannte Systeme. Das Unternehmen ist international anerkannt durch die langjährige Beteiligung an europäischen und NATO-Programmen zur Entwicklung neuer Technologien. IDE nutzt fortschrittliche



Produktionsmethoden und besitzt umfangreiches Projektmanagement-Know-how und ist somit ein wichtiger Akteur im Hochtechnologiesektor der griechischen Verteidigungsindustrie.

IntraFind Software AG

R 41

Die IntraFind Software AG mit Hauptsitz in München ist ein etablierter deutscher Hersteller von intelligenter Such- und Analyse-Software.

Die KI-basierte Lösung iFinder ermöglicht es Organisationen, über alle ihre verfügbaren Datenquellen hinweg, relevante Informationen zu finden, zu vernetzen und zu analysieren.

So können Anwender auch aus sehr großen Mengen strukturierter und unstrukturierter Daten schnell wichtige Informationen herausfiltern und Zusammenhänge erkennen.

Als langjähriger Partner für die Bundeswehr, Polizei- und andere Sicherheitsbehörden präsentiert IntraFind Live Demos und Anwendungsbeispiele seiner Analyse-Software iFinder.

Kontakt: Franz Kögl, franz.koegl@intrafind.com | Manuel Brunner, manuel.brunner@intrafind.com | www.intrafind.com/de, Besuchen Sie uns auf der AFCEA Fachausstellung 2024 an Stand R 41.

INTRAFIND

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 Digitalisierungs-

INXIRE

potenzial 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.

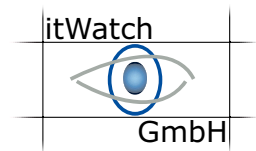
itWatch GmbH

S 10

itWatch stellt patentierte IT-Sicherheit in Deutschland her.

Der Fokus der itWatch Enterprise Security Suite (itWESS) liegt auf dem Schutz gegen Datendiebstahl (Data Loss Prevention - DLP), technischer Vertrauensketten von der

Tastatur bis zu den Daten, deren organisatorische Einbettung durch rechtsverbindliche Dialoge, Endgeräte-Sicherheit (Endpoint Detection & Response - EDR), der Lösung itWash, einer Datenschleuse mit Datenwäsche (Data Sanitizing) und Workflow, 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.



JK Defence & Security Products GmbH

S 30

Seit über 30 Jahren liefert JK Defence & Security Products GmbH als zuverlässiger Partner der Bundeswehr robuste und sichere Funk-



JK DEFENCE & SECURITY

Das Systemhaus für Technik und Logistik

<CONDOK>



CONDOK leistet umfassende Unterstützung in den Bereichen Systementwicklung und Dienstleistungen im Rahmen des Integrated Logistic Support.

Besuchen sie uns auf der AFCEA 2024, Stand S01, 26.-27. Juni 2024

Kiel - Koblenz - Hamburg

www.condok.de

kommunikationssysteme der Spitzenklasse. Marktverfügbare Lösungen bieten dem Anwender robuste und sichere Vernetzung in anspruchsvollen Szenarien.

Mit unseren Partnern L3Harris, Galvion, Ultralife, ViaSat, Comtech Systems und RolaTube 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, Regelstandsetzungen und Reparaturen durch. So steht unseren Kunden ein kompetenter, zuverlässiger und schnell agierender Partner in Deutschland zur Verfügung.

JK Defence & Security Products GmbH, milcom@jkdefence.de, www.jkdefence.de, 02152/1445-207

JOWO - Systemtechnik AG

W 10

Die JOWO - Systemtechnik AG ist Hersteller und Vertrieber von elektrischen- und optischen Steckverbindern, LWL- und elektrischen Verkabelungen, sowie kundenspezifischen Lösungen seit 1995. In Zusammenarbeit mit namenhaften

Herstellern erstellen wir für Sie die besten Lösungen:

- für Militär, Industrie, Luft- u. Raumfahrt
- Marine, Öl und Gas (Ex-Lösungen)
- Endgehäuse, Schutzkappen, Werkzeuge
- LWL-Steckverbinder Multimode/Singlemode
- Reinigungs- und Testkoffer
- Kabelbäume militärisch/zivil in LWL, Signal, Leistung, HF, Hybrid
- kundenspezifischer Lösungen
- Drucktests bis 1000 Bar

- Schnellfertigungslinie Marinebronzestecker MIL/VG

• Zugelassen nach EN9120, NATO C6689 und VG9692 Typen C, D und E
Kontakt: JOWO - Systemtechnik AG, Lange Wand 12, 27753 Delmenhorst, P: +49 4221 916 495-0, www.jowo.ag, info@jowo.ag



Kappa optronics

R 19

DVE & SAS Lösungen und Rohrinspektionssysteme: Skalierbare Driver Vision Enhancer (DVE) und Situational Awareness Systeme (SAS) für verschiedene Fahrzeugtypen und Einsätze. Das modulare Portfolio bietet hochwertige Sensoren, VIS / LWIR Image Fusion für Tag- und Nachsicht sowie Multi-Sensoransichten / Stitching.

RIB 4D: Das Inspektionssystem zur Verschleißprüfung großkalibriger Rohre kombiniert Laserscan- undameratechnik für schnelle, automatisierte Rohrdigitalisierung glatter und gezogener Rohre (120 mm und 155 mm). Bewertung des Rohrzustandes in einer nutzerfreundlichen Spezialsoftware, Reporting in Excel oder TDv18.

Über 40 Jahre Erfahrung in Vision Systemen z. B. bis SIL 2/ASIL-B/DAL-B, ISO 26262, MIL STD 810/461/1275. Unsere Lösungen sind direkt marktfähig!



KENBUN IT AG

R 63

Wir, die KENBUN IT AG, sind ein 2018 gegründetes KI-Startup aus Karlsruhe. Als Experten für Large Language Models, digitale Sprachsysteme und Künstliche Intelligenz unterstützen wir Unternehmen bei der digitalen Transformation. Wir entwickeln sprachgesteuerte Systeme, um Arbeitsprozesse zu beschleunigen und zu vereinfachen. Unser selbstentwickelter Sprachbaukasten KIDOU, der eine Vielzahl von KI-Komponenten für Sprach- und Textverarbeitung beinhaltet, meistert Herausforderungen, wie präzise Spracherkennung bei regionalen Dialekten sowie bei Lärm- und Hintergrundgeräuschen, verstehen und verarbeiten spezielle Fachbegriffe und können mit langen Zahlenkolonnen umgehen. Unsere Expertise liegt in der Entwicklung von individuellen und passgenauen KI-Sprachsystemen, die auch im Haus des Kunden On-Prem laufen können.



Knapp Service Koblenz GmbH

W 09

Die Knapp Service Koblenz GmbH ist mit ihrer über 60-jährigen Erfahrungskompetenz im Bereich Einrüstungs- und Instandsetzungsprojekten von Fahrzeugen, Kabinen und Baugruppen ein verlässlicher Partner der Bundeswehr (BAAINBw, HIL, BwFPS), sowie von Systemhäusern. Der Geschäftsbereich „Integration von militärischen Rüstsätzen“, speziell im Bereich Funk- und Führungssysteme wurde und wird dabei fortlaufend weiterentwickelt, um dem heutigen und zukünftigen Bedarf (D-LBO) des militärischen Kunden gerecht zu werden. Die Integration und Verkabelung nach VG-Normen von komplexen militärischen Rüstsätzen mit speziellen Geräteanteilen (z. B. Funkgeräte, BV-Anlagen, Sat-Com-Anlagen, Führungsausrüstung, BMS, mil. GPS) ist hierbei eine Kernkompetenz der Knapp Service Koblenz GmbH. Die hierfür benötigten Kabel werden ebenfalls im eigenen Hause gefertigt. Durch den Ausbau dieser Kernkompetenzen gepaart mit einer reibungslosen, schlanken und verlässlichen Mittelstandsstruktur erhalten wir kontinuierlich herausragende Ergebnisse in der Kundenzufriedenheit. Kontakt: info@knapp-service.de web: www.knapp-service.de



KNDS Deutschland GmbH & Co. KG

A 01

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. Die strategische Allianz zwischen 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 hat seinen Sitz in Amsterdam.

KNDS

KNDS Deutschland Mission Electronics GmbH

S 48

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-Switches, mobile und stationäre Kommunikationsanwendungen sowie Kommunikations- und Life-Cycle-Software. Kontakt: KNDS Deutschland Mission Electronics GmbH, Max-Stromeyer-Str. 116, 78467 Konstanz, info-kdme@knds.de, www.knds-electronics.de

KNDS

KPMG AG Wirtschaftsprüfungsgesellschaft

S 26

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 für Organisationen der öffentlichen Verwaltung durchgeführt. Dabei verbinden wir unsere fachliche Spezialisierung in der Organisationsberatung mit Branchenexpertise des



öffentlichen Sektors in einem lösungsorientierten Dienstleistungsangebot. Unsere besondere Stärke liegt in der Verbindung von betriebswirtschaftlicher, rechtlicher und IT-technischer Expertise.

L3Harris

S 30

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



Lachen Helfen e.V.

R 75

Seit 26 Jahren unterstützen wir von „Lachen Helfen e.V. – Initiative deutscher Soldaten und Polizisten für Kinder in Kriegs- und Krisengebieten“ in den Einsatzgebieten der deutschen Streitkräfte und Polizeibeamten erfolgreich in Not geratene Kinder vor Ort, mittlerweile in 17 verschiedenen Ländern auf 4 Kontinenten (Berichte stets aktuell auf unserer Website: www.lachen-helfen.de).

Die Projekte und den Bedarf an Hilfsmitteln ermitteln Soldaten und Polizisten, die bei der Erfüllung ihrer dienstlichen Aufgaben und Aufträge durch gezielte Erkundung auf besondere Not und gravierende Missstände aufmerksam werden. Dabei engagiert sich Lachen Helfen e.V. vor allem bei der Unterstützung, der Renovierung und dem Neubau von Schulen, Waisenhäusern, Kindergärten und Krankenhäusern.



Langlauf Security Automation GmbH

R 63

Die Langlauf Security Automation GmbH ist Spezialist für die Erstellung und Validierung von Softwarestücklisten (Software-Bill-of-Materials, kurz SBOMs). Unsere Analysetechnologie benötigt keinen Quellcode und eignet sich dadurch auch für zugelieferte Komponenten und Legacy Software, z. B. Embedded Images, Firmware, Container sowie Linux- und Windows-Applikationen. Die Lösung wird als Self-Service bereitgestellt und kann nahtlos in existierende Prozesse und Pipelines integriert werden. Unsere Kompetenz konnte in zahlreichen Projekten mit (M)DAX-Konzernen, der Cyberagentur (Gesellschafter BMVG) sowie durch die Auswahl für die hochdotierte BMBF-Initiative „Start-UpSecure“ unter Beweis gestellt werden. Langlauf ist unabhängig, inhabergeführt und beschäftigt derzeit 9 Mitarbeiter, darunter Experten mit Industrieerfahrung bei Siemens, Rohde & Schwarz und CGI.



Leonardo SpA

A 05

We are one of the world's major players in Aerospace, Defence and Security, a global solutions provider and a trusted long-term partner of choice for governments, institutions and business customers. We deliver cutting-edge and dual-use technologies, meeting both military and civil requirements. In partnership with our customers, we work to strengthen global security, protect people, territories, cyber networks and infrastructure. We guarantee the safe management of air, sea and urban spaces, as well as largescale events. We have a solid industrial legacy, strengthened by the expertise of our people and the conti-



nuous pursuit of innovation in our core technologies. Underpinned by a sustainable business model, we are pursuing a path of long-term growth that will create value for all our stakeholders.

LocateRisk GmbH

R 63

LocateRisk sorgt für Automatisierung, Transparenz und Kontrolle im Cybersicherheitsprozess von Unternehmen weltweit. Die nicht-invasive Lösung – Made in Germany – überwacht den Schutz von IT-Infrastrukturen, beschleunigt die Absicherung und erleichtert mit automatisierten IT- und DSGVO-Compliance-Prüfungen von Geschäftspartnern das Cyber Risk Management in der Lieferkette. Als Technologiepartner von Systemhäusern, Beratungsgesellschaften und Versicherungen unterstützt LocateRisk eine effiziente, kontinuierliche Cyberhygiene und hilft, die Risiken für Cybervorfälle präventiv und nachweisbar zu reduzieren.

External Attack Surface Management (EASM):

- Müheloser Nachweis für Zertifizierungen und Audits (bspw. NIS2)
- Einfache Kommunikation der IT-Sicherheitslage ans Management
- Interaktives Schwachstellenmanagement zur Angriffsflächenminimierung
- Security-Monitoring von Dritten/Geschäftspartner-Risikomanagement
- Konzernweite IT-Risiko-Analysen
- Schaffen von digitalen Lagebildern



Lumibird

F 14

Lumibird is one of Europe's leading specialists within laser technologies for advanced Defence, Scientific and Medical applications. Within defence we are specialized in laser range finders, laser designators, C-UAS and LIDAR for Naval, Land, Airborne and Space applications.

Since 1962, we have been providing the defence market with our multi-domain laser range finders. Lumibird Photonics Sweden is specialised in defence applications with customers in more than 40 countries, in 2022 we moved to a completely new R&D and production site in Gothenburg, Sweden.

For further information, please visit www.lumibird.com or contact Micael Malmberg mmalmberg@lumibird.com



M4Com System GmbH

R 52

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-kompatible Lösungen mit jeweils offenem Standard, generischen Schnittstellen und funktionsübergreifender Verbindung in eine netzwerkzentrierte Umgebung.



Materna Information & Communications SE

S 52

Die Materna-Gruppe beschäftigt über 4.000 Mitarbeitende an weltweit über 40 Standorten. Wir realisieren innovative und nachhaltige IT- und Digitalisierungsprojekte für Kunden aus Wirtschaft und öffentlicher Verwaltung. Zur IT-Unternehmensgruppe gehören mehrere Tochtergesellschaften. Materna begleitet Behörden bei der strategischen und IT-technischen Umsetzung staatlicher Aufgaben auf dem Weg zur digitalen Verwaltung. Wir betreuen alle Phasen der Wertschöpfungskette: von der Beratung bis zum Betrieb mithilfe standardisierter und skalierbarer Lösungen. Materna bietet ein spezialisiertes Lösungsportfolio für verschiedene Ressorts und Domänen der Verwaltung. Dazu gehören die



Themen EVA, E-Government, Registermodernisierung, Verfahrensentwicklung, digitale und mobile Szenarien, föderales Datenmanagement, Analytics und KI, Cyber Security und Management von Infrastrukturen.

Materna Virtual Solution GmbH

S 56

Materna Virtual Solution ist ein marktführender Softwarehersteller mit Mobile Security Expertise, der sich auf Produkte und Beratungsleistungen im Bereich des sicheren ultramobilen Arbeitens spezialisiert hat. Mit der zugelassenen Applikation SecurePIM können Behörden und Unternehmen mobil auf der Geheimhaltungsstufe Verschlusssachen – Nur für den Dienstgebrauch (VS-NfD) sowie auf der Sicherheitsstufe NATO RESTRICTED kommunizieren und arbeiten. Neben der Container-Lösung SecurePIM entwickelt Materna Virtual Solution auch Anwendungen für die neuen behörden-spezifische Lösungen „Apple indigo“ und „Samsung Knox Native Solution“.

Mit der Vision eines sicheren ultramobilen Arbeitsplatzes bietet Materna Virtual Solution mit seiner umfassenden Expertise Beratungsleistungen entlang der gesamten Wertschöpfungskette an – plattform- und geräteunabhängig.



Matrox Video GmbH

F 30

Matrox Video is a leading manufacturer of video products and components for the broadcast and media, live entertainment, and AV/IT markets. Our mission is to create innovative products and provide superior support, enabling our customers to harness the power of video to entertain, communicate and make critical decisions.

Matrox hardware and software products are deployed across a diverse range of industries, including broadcast and media, education, enterprise, government, houses of worship, medical, military and defense, process control and utilities, security, and transportation.



MBS – Media Broadcast Satellite GmbH

S 29

MBS ist ein zuverlässiger Service-integrator und Betreiber von Managed Gateways. Wir betreiben Daten- und Sprachkommunikation über Satelliten- und Datennetzwerke – weltweit und im Weltraum. Unser Know-how reicht von klassischen Satellite Services bis hin zu maßgeschneiderten Applikationen aus dem Anwendungsfeld New Space.

Regierungs- und Geschäftskunden weltweit vertrauen auf die Integrität und Innovationskraft von MBS. Auch weil wir über unsere eigene ausfallsichere Infrastruktur in Deutschland verfügen und mit unserem Team von mehr als 80 Spezialisten aufwarten.

Vom effizienten Standard bis hin zu maßgeschneiderten High-End-Lösungen mit vollständigem Management. Skalierbar und herstellerunabhängig. Hochverfügbar und unter härtesten Bedingungen praxiserprobt.



Micropol Fiberoptic AB

F 33

Micropol Fiberoptic AB hat seinen Sitz in Halmstad an der schwedischen Westküste. Wir sind eines der ältesten und erfahrensten Unternehmen Schwedens auf dem Gebiet der passiven Glasfaseroptik. Unsere Kunden sind in einer Vielzahl von Märkten zu finden, in denen fortschrittliche Glasfaserlösungen entscheidend sind. Unsere Produkte werden in einer ganzen Reihe von Technologien eingesetzt, von komplexen Glasfasernetzen für die Tele- und Datenkommunikation. Micropol wächst schnell und verfügt heute über Niederlassungen in Deutschland, Großbritannien und den USA.

Unsere erstklassige Produktionsstätte umfasst eine Reinraumproduktion, Laboreinrichtungen und Engineering Kapazitäten.



Mittler Report Verlag GmbH

R 23

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 internationalen Fachzeitschriften „European Security & Defence“ und „The European - Security and Defence Union“, die Fachzeitschrift „MarineForum“, die Broschürenreihe „Wehrtechnischer Report“, der Newsletter „Wehrwirtschaft“ und die Online-Plattformen „soldat-und-technik.de“. Die jährlich vom Verlag ausgerichtete Sicherheitspolitische und Wehrtechnische Tagung in Bonn und die NATO LCM Conference in Brüssel sind etablierte Foren für den Informationsaustausch unter Experten und Entscheidungsträgern.

MITTLER REPORT

Mönch Verlagsgesellschaft mbH

R 10

Die MÖNCH Gruppe ist einer der weltweit führenden Zeitschriften-fachverlage in den Bereichen Verteidigung und Sicherheit. Darüber hinaus werden ca. 250 Buchtitel im Segment Verteidigung, Technologie, Politik und Geschichte seit vielen Jahren durch BERNARD & GRAEFE verlegt. Unsere Zeitschriften erscheinen auf deutsch, englisch und italienisch. Dazu gehören:



- WEHRTECHNIK (Deutsch): Erscheinungsweise zweimonatlich für Leser in Deutschland, Österreich und in der Schweiz.
 - MILITARY TECHNOLOGY (Englisch): erscheint alle zwei Monate.
 - NAVAL FORCES (Englisch): Erscheinungsweise zweimonatlich
 - HANDBUCH DER BUNDESWEHR (Deutsch)
- KONTAKT: Herr Volker SCHWICHTENBERG, MÖNCH Verlagsges.mBH, Christine-Demmer-Str.7, 53474 Bad Neuenahr Ahrweiler (Tel.: 02641 3703 0, e mail: info@moench-group.com, https://monch.com)

Mosolf

F 14

Die MOSOLF Gruppe deckt mit 130 Mitarbeitern an europaweit 41 Technik- und Logistikzentren die gesamte Wertschöpfungskette der Automobillogistik ab.



Die Business Unit MOSOLF Special Vehicles ist zuverlässiger Partner der OEM bei der Integration von Rüstsatzlösungen für Informations- / Kommunikationstechnik, Komponentenkonstruktion und -Bau, Produktion von Kabelbäumen und Funkverkabelung bis hin zu komplexen fahrzeug- oder container-gebundenen Systemen. Mit unserem Team aus qualifizierten Ingenieuren und Experten, einer Werkstattfläche von 15.000 qm mit Kapazität für bis zu 5.000 Fahrzeugausbauten pro Jahr und der Fähigkeiten zur flexiblen Durchführung von Arbeiten an Standorten von OEM-Partnern und Endkunden entlasten wir Defence OEMs mit Engineering- und Produktionsdienstleistungen.

Motorola Solutions Germany GmbH

S 21

Motorola Solutions is solving for safer. We build and connect technologies to help protect people, property and places. Our solutions enable the collaboration between public safety agencies and enterprises that's critical for a proactive approach to safety and security. Learn more about how we're solving for safer communities, safer schools, safer hospitals, safer businesses – safer everywhere – at www.motorolasolutions.com.



NanTenna

S 30

Im Jahr 2020 begab sich NanTenna auf eine visionäre Reise - das Ziel: die Revolutionierung traditioneller militärischer Satellitenkommuni-



kationsantennen. Das Produkt, eine UHF-Antenne mit niedrigem Profil und hoher Verstärkung, zeigte das Engagement des Unternehmens, die Grenzen des Erreichbaren im Bereich der Satellitenkommunikationstechnologie zu verschieben. Das Unternehmen steht jetzt an der Spitze der Innovation und entwickelt kontinuierlich Antennen mit hoher Verstärkung und geringem SWaP-Faktor für verschiedene Anwendungen. NanTenna ist stolz auf seine Fähigkeit, die Nutzer zu überzeugen, und hat bereits mehrere NATO Nationen erfolgreich bei der Aktualisierung ihrer Kommunikationshardware unterstützt. Kontakt: JK Defence & Security Products GmbH, Industriering Ost 74, 47906 Kempen, milcom@jkdefence.de, www.jkdefence.de, 02152/1445-207

Narda Safety Test Solutions GmbH

F 14

Für die taktische Funküberwachung und -aufklärung oder der eigenen Emissionskontrolle auf dem Schlachtfeld, in Grenzkontrollszenarien und bei nachrichtendienstlichen Anwendungen sind leichte und tragbare Funkpeilgeräte erforderlich. Dies ermöglicht auch verdeckte Operationen, falls erforderlich. NARDA ist ein Marktführer im Bereich der elektromagnetischen Spektralanalyse. NARDA entwickelt handgeführte, tragbare und in Fahrzeuge integrierte Peilgeräte. Unsere AOA / TDOA-Hybridtechnologien verwenden „Made in Germany“ High Dynamic Range (HDR) SignalShark-Empfänger und NARDAs einzigartige Automatic Direction Finding Antenna (ADFA). NARDA-Geräte sind von zeitaufwändigen Exportkontrollverfahren befreit und können hoch-effektiv auch in autonomen Outdoor-Fernüberwachungsstationen eingesetzt werden.



ND SatCom GmbH

S 43

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.



NEOSAT GmbH

S 74

NEOSAT GmbH ist ein Spin-Off der Universität der Bundeswehr in München. Wir entwickeln neue wegweisende Übertragungstechnologien im Bereich der Satellitenkommunikation. NEOSAT hat mit UCSS eine Wellenform entwickelt, die beim Thema Military Internet-of-Things (IoT) neue Standards setzt. Damit ermöglichen wir eine jederzeit verfügbare, weltweite Verbindung mit batteriebetriebenen Kleinstsendern über Satelliten. Durch die Nutzung vorhandener geostationärer Satelliten erlaubt UCSS hoheitlichen Bedarfsträgern den autarken Betrieb eigener IoT Lösungen. Neben der Hard- und Software für SATCOM IoT, bietet NEOSAT auch Lösungen für die Vernetzung von Kleinsatelliten.



NetApp

F 14 + S 18

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 Inselfösungen 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 – sowohl für zivile als auch militärische Anwendungsfälle. Mehr unter www.netapp.com/de

Newsletter Verteidigung - VDS

R 08

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



Der NV ist meinungsbildend, unabhängig und objektiv. Er zielt darauf ab, als Argumentationshilfe Entscheidungsprozesse zu erleichtern und zu beschleunigen. Die bedarfsgerechte Ausstattung der Deutschen Bundeswehr mit Material und Personal steht bei diesen Bemühungen grundsätzlich im Mittelpunkt des Interesses.

Geopolitisch konzentriert sich der NV auf internationale Themenfelder, die einen direkten oder indirekten Bezug zu den deutschen Streitkräften, der Wehrtechnischen Industrie oder der deutschen Innen- und Außenpolitik haben. www.newsletter-verteidigung.de

NVIDIA

R 48

NVIDIA ist ein weltweit führendes Technologieunternehmen, das für seine innovativen Grafikprozessoren und leistungsstarken Computerplattformen bekannt ist. Mit Schwerpunkt auf künstlicher Intelligenz, Gaming, autonomen Fahrzeugen, Data Center und Edge Computing treibt NVIDIA die Entwicklung wegweisender Technologien voran, die die Grenzen des Möglichen neu definieren. Seit der Gründung im Jahr 1993 hat das Unternehmen kontinuierlich Lösungen entwickelt, die in verschiedenen Branchen und Anwendungen zum Einsatz kommen. NVIDIA strebt danach, die Zukunft der Computing-Technologie zu gestalten und das volle Potenzial von KI-basierten Innovationen auszuschöpfen.



ODM GmbH

F 28

ODM bietet durchdachte Sicherheit und nahtlose Kommunikation für jede Mission. Moderne BST und C4I Komponenten für den Infanteristen der Zukunft, regionale Produktion, nachhaltig gefertigt, zertifiziert und flexibel einsetzbar nach Bundeswehr Anforderungen. ODM hat sich nicht nur als zuverlässiger Partner für High-Tech-Headsets, robuste Handapparate, individuelle Verbindungskabel sowie für persönliche Schutzausrüstung etabliert, sondern bietet auch in Deutschland gefertigte Drohnen für Aufklärung und Transport, sowie einzigartige Garne und Klimatextilien mit hoher Belastbarkeit an. Weiterhin ist ODM für schnelles Prototyping, effiziente Entwicklung, schnelle Lieferung, sorgfältige Wartung und Instandsetzung sowie durch Obsoleszenz-Management aller Produkte bekannt. Kundenorientierte Lösungen aus einer vollumfänglichen Wertschöpfungskette bieten Zukunfts- und Wehrfähigkeit.



OHB System AG

F 20

Die OHB System AG gehört zu den führenden Raumfahrtunternehmen Europas und ist das größte Tochterunternehmen des börsennotierten Hochtchtechnologiekonzerns OHB SE. Mit Hauptsitz in Bremen und einem weiteren starken Standort in Oberpfaffenhofen bei München hat die OHB System AG mehr als 40 Jahre Erfahrung mit der Entwicklung von High-Tech-Lösungen für die Raumfahrt und weitere Anwendungsfelder. Das Portfolio an Produkten und Dienstleistungen reicht dabei von der Realisierung von Satellitensystemen für Erdbeobachtung, Navigation, Telekommunikation



und Aufklärung über die Ausarbeitung und Umsetzung von Missionen zur Erforschung des Weltalls bis hin zur Entwicklung von Systemen für die astronautische Raumfahrt. We.Create.Space.

Panasonic Connect Europe GmbH

F 05

Als Branchenführer im Bereich Rugged Mobile Computing bietet Panasonic TOUGHBOOK einsatzbereite „Full-Ruggedized“ Laptops und Tablets, die nach Militärstandards (MIL-STD 810G) und gemäß IP65 und teils IP66 auf Zuverlässigkeit und Langlebigkeit getestet wurden.

Unsere COTS-basierten Geräte sind ideal als C4I Tool, da sie für jede Mission im Verteidigungssektor ausgelegt sind. Dank leuchtstarker Outdoor-Displays mit Handschuhmodus, äußerst langer Akkulaufzeiten 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. Kontakt: www.toughbook.de



Pegasystems GmbH

F 04

Mit der leistungsstarken Low-Code-Plattform von Pega sind weltweit führende Unternehmen 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 heutige Kundenanforderungen erfüllen und auch mit zukünftigen Entwicklungen Schritt halten. Gemeinsam mit CGI helfen wir den Mehrwert dieser Anwender getriebenen Low-Code-Plattform, welche über die BWI ab sofort abrufbar ist, ganzumfänglich zu nutzen. Zudem profitieren unsere Kunden von der langjährigen Branchenkenntnis von CGI im Verteidigungsumfeld, welche auf Basis der etablierten BWI-Services und geschlossener Verträge zielgenaue, agile Implementierungsunterstützung und schnelle Projekt- und Prozessumsetzung gewährleistet.



Peli Products Germany GmbH

S 02

Peli-Hardigg™, der weltweit größte Hersteller von wiederverwendbaren Versand- und Lagerbehältern aus Kunststoff, mit Zulassung für die Verwendung in den Bereichen Militär und Luftfahrt, präsentiert auf der AFCEA das extrem widerstandsfähige 19-Zoll Rack-Gehäuse für einsatzkritische IT- & Kommunikationslösungen. Es bietet kompakte Mobilität für Ihr Equipment und erfüllt dabei die Anforderungen und Standards des Militärs.

Die PELI-Hardigg Militärbehälter sind nicht nur nahezu unverwundlich, luftdicht, wasserdicht und dekontaminierbar – sie sind auch wiederverwendbar. Einsatz für Einsatz kann man sich auch unter den härtesten Bedingungen auf sie verlassen, um überlebenswichtige Ausrüstung zu schützen, zu transportieren und zu verteidigen. www.peli.com



Pexip

R 74

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: Höchstmaß an 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

PHYSEC GmbH

R 63

PHYSEC ist Experte für IoT-Konnektivität und IoT-Sicherheit. Den Schwerpunkt bilden innovative Sicherheitsprodukte und -lösungen für Hersteller und Betreiber von vernetzten Geräten, insb. KRITIS-Anlagen. Das Produktportfolio von PHYSEC löst die IoT-Herausforderungen von morgen durch die Konvergenz von Cyber Security und physischer Sicherheit. Hierfür bietet PHYSEC innovative Lösungen wie das Anti Tamper Radio (ATR) an. Die Services und Produkte von PHYSEC helfen strategische Entscheidungen zu treffen sowie schnelle und sichere Implementierungen und Integrationen durchzuführen.



PHYSEC
SECURITY FOR THINGS

PLATH GmbH & Co. KG

F 18

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 fast 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 beschäftigt über 600 Mitarbeiter in Europa und weltweit. Weitere Informationen unter plathgroup.com.



Precision Technic Defence

A 08

Precision Technic Defence Group is a global leader in advanced defence solutions aimed at ensuring safe and stable societies and safeguarding people and communities from military threats, natural disasters, accidents, or acts of terrorism. We offer a unique range of solutions from a vast number of distinct partners worldwide and have extensive experience in matching technologies and interoperability requirements for a full range of integrated solutions.

Our solutions include:

- Soldier Systems
- Platform and Sensor Systems
- Unmanned Systems
- C4ISR Systems
- Service & Support

We are a trusted, long-term supplier and partner of choice for nations, governments, armed forces, national security agencies, and law enforcement around the globe.



PRECISION TECHNIC DEFENCE
PROTECTING PEOPLE AND SOCIETY

PREVENCY GmbH

R 63

PREVENCY - Information Environment Simulator (Synthetic Internet)
PREVENCY ist auf die immersive Simulation des digitalen Informationsraums zu Trainingszwecken spezialisiert. Unsere Trainings- und Simulationssoftware bietet vielfältige Möglichkeiten für simulationsbasiertes Training in den Bereichen StratCom, OSINT, Cyber Defence, Krisenmanagement und Öffentlichkeitsarbeit. Die



PREVENCY®

PREVENCY-Software wurde in Kooperation mit dem NATO Strategic Communications Centre of Excellence entwickelt und konnte bereits das Vertrauen namhafter internationaler Institutionen gewinnen. PREVENCY war Finalist der NATO Innovation Challenge 2021 „The Invisible Threat: Countering Cognitive Warfare“ und ist Teil der NATO-Übung „Locked Shields 2024“.

Production ToGo

R 42

ProductionToGo ist ein führender Anbieter von industriellen 3D-Drucklösungen in Europa. Mit umfangreicher Erfahrung und Expertise bieten wir über unsere fünf Geschäftseinheiten - ProductionToGo GmbH, PartsToGo GmbH, Additive Automation GmbH, Earn A Label GmbH und 3Dprinters-store.com - eine Vielzahl von Dienstleistungen an. Als zertifizierter 3D-Druck-Spezialist bedienen wir Deutschland, Österreich, die Schweiz, Belgien, die Niederlande und Luxemburg und bieten eine umfangreiche Palette von Hardware, Software und umfassender Unterstützung. Unsere Mission ist es, hochwertige 3D-Druckprodukte und -dienstleistungen mit Fokus auf Pünktlichkeit und Wettbewerbsfähigkeit zu liefern und dabei langfristige Partnerschaften aufzubauen. Unsere Vision ist es, der führende Anbieter von 3D-Drucklösungen in Europa zu werden, um Innovationen für eine nachhaltige Zukunft voranzutreiben. Unsere Kernwerte umfassen Integrität, Kundenorientierung, Hingabe und Innovationskraft.



promegis Gesellschaft für Geoinformationssysteme mbH

S 13

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

Weitere Informationen finden Sie unter www.promegis.de.

Kontakt: Klaus Scholle, Tel. +49 (0) 541 600196-0, E-Mail: sales@promegis.de.

promegis

Gesellschaft für
Geoinformationssysteme mbH

ProSoft GmbH

S 61

Secure, Manage, Optimise IT
Cyber-Angriffe können über Monate unentdeckt IT-Systeme infiltrieren – um dann innerhalb kürzester Zeit komplette Netzwerklanschaften zum Stillstand zu bringen. Für Militär, Rüstungsunternehmen, Bundes- und Landesbehörden sowie KRITIS-Organisationen ist es daher entscheidend, sich mit effektiver IT-Security und reibungslosem IT-Management zu schützen.

Seit 35 Jahren steht ProSoft für effiziente und sichere Lösungen für IT-Security & IT-Management. ProSoft bietet nur Lösungen mit überzeugendem Mehrwert an und unterstützt beim Implementieren. Über 5.000 Kunden vertrauen auf ProSoft. Am ProSoft-Stand S 61 (Saal New York/Genf) erfahren Sie, wie Sie Ihre IT effizient schützen können.

Kontakt: www.prosoft.de oder telefonisch 08171-405-200

ProSoft
SECURE | MANAGE | OPTIMISE IT

PROSTEP AG

R 16

PROSTEP ist der führende Experte für PLM und ALM. Wir unterstützen Fertigungsunternehmen unterschiedlicher Branchen, wie Defense, Luft- und Raumfahrt, Maschinenbau und Schiffbau, bei der Schaffung der digitalen Durchgängigkeit,

PROSTEP
integrate the future

um ihre Innovationskraft und Wettbewerbsfähigkeit nachhaltig zu stärken. Wir ermöglichen den Aufbau eines digitalen Zwillings, auch um Beschaffungs- und Logistikprozesse zu optimieren.

Wir kombinieren jahrelange Beratungskompetenz und eigene Software-Lösungen. Wir befähigen unsere Kunden, komplexe, software-intensive Produkte und Systeme zu entwickeln, zu fertigen und zu betreiben. Mit unserer Erfahrung unterstützen wir unsere Kunden, die digitale Transformation zu meistern. Unsere Software-Lösungen befähigen Unternehmen, sensible Daten in internationalen Lieferketten und der Ersatzteilversorgung sicher auszutauschen. www.prostep.com

QGroup GmbH

A 02

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. Unser Security Operations Team überwacht permanent Kundennetze. Bei einem Incident setzen wir ein 24/7 Incident Response Team ein. Absicherung, Beweissicherung, Netzwerkforensik und Schadensbeseitigung werden auf Grundlage neuester IT-Security-Erkenntnisse und eigener Threat Intelligence durchgeführt. www.qgroup.de

QGROUP
GMBH

Quantum Systems

R 57

Quantum Systems ist auf die Entwicklung, Konstruktion und Produktion kleiner unbemannter Flugsysteme (sUAS) spezialisiert. Die elektrischen senkrechtstart- und landefähigen (eVTOL) Fluggeräte des Unternehmens sind auf maximale Flugdauer und Vielseitigkeit ausgelegt und bieten den Anwendern eine nahtlose Nutzererfahrung. Durch die Integration modernster Softwarefunktionen wie Edge Computing und KI-gestützter Datenverarbeitung in Echtzeit baut Quantum Systems UAS der nächsten Generation für Kunden aus den Bereichen Sicherheit, Verteidigung, öffentliche Sicherheit, kommerzielle und geografische Operationen in ganz Europa.

**QUANTUM
SYSTEMS**

RAM Mounts Germany GmbH

R 15

RAM™ Mounts ist der weltweit führende Anbieter eines universellen 3-Komponenten-Befestigungssystems, gegründet 1992 in den USA.

Das System besteht aus 6.000 robusten Modulen, die bequem und flexibel mit anderen RAM® Mounts Komponenten erweitert werden können. Durch dieses ausgeklügelte Konzept entstehen stabile und flexible Verbindungen dank Kugelgelenksystem mit drei Größen je nach Anwendung und Gewicht der montierten Geräte. Die Elastomerbeschichtung der Kugeln schafft Stoß- und Vibrationsdämpfung bei allen Anwendungen und Temperaturen.

Die umfangreiche RAM™ Mounts Produktpalette erfüllt höchste Industriestandards, ausgewählte Produkte mit UN/ECE/Luftfahrt Zertifizierung. Man unterscheidet zwischen dem Basis-System mit passiven Haltern und aktiven Halterungen sowie drahtlose Lademöglichkeiten.

**RAM
MOUNTS**
GERMANY

SOLUTIONS
MADE
FOR
PROFESSIONALS

Red Hat

F 02

Red Hat, der weltweit führende Anbieter von Open-Source-Lösungen, folgt einem von der Community angetriebenen Ansatz bei der Entwicklung hochperformanter Cloud-, Linux-, Middleware-, Storage- und Virtualisierungstechnologien. Ferner bietet Red Hat einen vielfach ausgezeichneten Support, Schulungen sowie Consulting-Services. Als eine zentrale Vermittlungsinstanz

Red Hat

in einem weltweiten Netzwerk von Unternehmen, Partnern und der Open-Source-Community fördert Red Hat den Aufbau bedeutender, innovativer Technologien, die Wachstumskräfte freisetzen und Kunden fit machen für die künftige IT. Weitere Informationen: www.redhat.de.

RHEINMETALL

N 01 + N 09

Taking responsibility in a changing world

Die börsennotierte Rheinmetall AG mit Sitz in Düsseldorf 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

F 22

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.



Rivada Space Networks GmbH

R 63

Rivada Space Networks entwickelt das OuterNET – eine Konstellation aus insgesamt 600 Satelliten, die hoch verfügbare Konnektivität für sichere Anwendungen mit hohem Durchsatz ausschließlich für Unternehmen und Behörden gewährleistet. Die Konstellation wird lizenzierte Ka-Band-Frequenzen für die Kommunikation zwischen Weltraum- und Bodensegment nutzen. Ein vollständig vernetztes orbitales Netz wird wie ein zweites separates Internet-Backbone im All operieren, das den Datenverkehr mit Gigabit-Geschwindigkeit von einem Satelliten zum anderen weiterleiten kann, ohne dass Gateways auf der Erde erforderlich sind.



roda computer GmbH

F 05

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. Strategische Partnerschaften erweitern das Produktportfolio um robuste Netzwerk- und Kommunikationstechnik wie auch Hochleistungsserver und unterbrechungsfreie Stromversorgungen und bieten somit ein umfassendes Systemkonzept aus einer Hand.



Rohde & Schwarz

F 10

Rohde & Schwarz ist ein weltweit führender Konzern für drahtlose, vertrauenswürdige, störste und sichere Kommunikation, Verschlüsselung und digitale Protokolle. Das Unternehmen begleitet die Ausstattung moderner Streitkräfte mit sicheren und innovativen Lösungen zur robusten Vernetzung für die Führungsfähigkeit im Einsatz durch softwaredefinierte Funkgeräte inklusive netzwerkfähiger interoperabler Wellenformen. Auch Funkaufklärungssysteme (EloUM), Lösungen für die Fernmeldeaufklärung (FmAufkl) und Radaraufklärung (EloAufkl) sind Fokusthemen.

Kontakt: Rohde & Schwarz Vertriebs-GmbH, Sicherheit und Verteidigung, Ernst-Reuter-Platz 10, 10587 Berlin, Rohde & Schwarz Vertriebs-GmbH, Sicherheit und Verteidigung, Frankfurter Straße 720-726 51145, Köln, www.rohde-schwarz.com, Ansprechpartner: Britta Holdmann, E-Mail: Vertrieb-SV@rohde-schwarz.com, Telefon: 02203 8077-12



rola Security Solutions GmbH

F 06 b

ZUSAMMENARBEIT STÄRKEN, SICHERHEIT SCHAFFEN

Daten sammeln und Informationen verdichten sind wesentliche Herausforderungen bei der Lagebearbeitung und Lagebilderstellung in militärischen Organisationsbereichen. Insbesondere das steigende Informationsaufkommen und die Recherche in unterschiedlichsten Quellen fordern hohe Konzentration und Organisationsgeschick bei der Zusammenführung der relevanten Informationen. Ohne moderne Analyse- und Informationssysteme sind diese Aufgaben kaum beherrschbar.

Unsere Softwarelösungen für das militärische Nachrichtenwesen bieten:

- Bedarfsträgerorientierte und dynamische Lagebilderstellungen
- Datenfusionierung: Zusammenführung relevanter Informationen und Vorwertung großer Datenmengen
- Erkennung von Zusammenhängen und Beschleunigung von Abläufen mittels moderner KI-gestützter Funktionen
- Recherchen in offenen Quellen (OSINT und Objekterkennung)
- Biometrische Analysen
- Praxiserprobter Datenschutz
- Quellenorientierte Datenhaltung zur Nachvollziehbarkeit aller gespeicherten Informationen

www.rola.com



Rolatube

S 30

Rolatube Technology Ltd. ist es gelungen, einen einzigartigen und patentierten rollbaren Verbundwerkstoff zu entwickeln, der es ermöglicht, die leichtesten

Mastsysteme der Welt zu produzieren. Aufgrund der ebenfalls einzigartigen Integrationsmöglichkeiten von Antennen in den Verbundwerkstoff bieten die Rolatube Antennenmasten eine konkurrenzlose Mobilität, schnelle Herstellung der Einsatzbereitschaft sowie Funk Performance.

Rolatube bietet eine aufregende, dynamische und innovative Produktpalette, die dem Nutzer leichte- und kompakte Mastsysteme in Verbindung mit einem hohen Maß an Zuverlässigkeit und Robustheit bieten.

Kontakt: JK Defence & Security Products GmbH, Industriering Ost 74, 47906 Kempen, milcom@jkdefence.de, www.jkdefence.de, 02152/1445-207



Rosenberger Hochfrequenztechnik**R 12**

Rosenberger ist einer der weltweit führenden Hersteller von Verbindungslösungen in Hochfrequenz-, High-Voltage- und Faser-Optik-Technologie und entwickelt und fertigt HF-Steckverbinder und -Kabel-Assemblies für

Rosenberger

- Kommunikations- und Nachrichtentechnik
- Mobilfunkinfrastruktur
- Luft- und Raumfahrt, Sicherheit und Verteidigung
- industrielle Test- und Messtechnik
- Automobilelektronik
- Medizin- und Industrietechnik
- Datenzentren
- Telematik

Die Rosenberger-Gruppe mit Stammwerk im oberbayerischen Fridolfing/Deutschland wurde 1958 gegründet und ist seitdem in Familienbesitz. Die Rosenberger-Gruppe verfügt über Fertigungs-, Montage- und Vertriebsstandorte in Europa, Asien, Afrika sowie in Nord- und Südamerika, in denen rund 15000 Mitarbeiter (m/w/d) für Entwicklung, Produktion und Vertrieb der Produkte sorgen.

RUAG**S 70**

RUAG ist der zukunftsorientierte Technologiepartner für internationale Streitkräfte und Sicherheitsorganisationen. Unser Fokus liegt auf dem Life-cycle Management, dem Betrieb und der Verfügbarkeit militärischer Systeme. Unser umfassendes Produkt- und Dienstleistungsportfolio umfasst interoperable Informations- und Kommunikationslösungen sowie Wartungs- und Instandhaltungsleistungen. RUAG bietet maßgeschneiderte Gesamtlösungen und -systeme, die durchgängig und effizient sind. In einem komplexen und dynamischen Umfeld betrachten wir nahtlose Integrationen und umfassende Lösungen aus einer Hand als entscheidend.



Zusätzlich entwickeln wir einzigartige Teilsysteme und Komponenten für Ketten- und Radfahrzeuge, Kampffljets, Militärhubschrauber und Flugabwehr. Mit diesen Technologien, Produkten und Dienstleistungen schaffen wir die Voraussetzungen für erfolgreiche Missionen und Einsatzsicherheit. Kontakt: Alexander.vonErdmannsdorff@ruag-de.com

SAP Deutschland SE & Co. KG**F 21**

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**A 09 + F 16**

Satcube is a fast-growing Swedish technology company in the satellite communications industry focusing on developing game-changing terminals and data services to enable high-speed broadband anywhere, quickly, and cost-effectively. Satcube's headquarters are based in Gothenburg and its production facility is in Karlstad. To learn more, visit their website at www.satcube.com.

**Schönhofer Sales and Engineering GmbH****S 54**

Die 1984 gegründete Schönhofer Sales and Engineering GmbH (SSE), seit 2022 ein Mitglied der Rohde & Schwarz Gruppe, ist Wegbereiter für fortschrittliche analytische Lösungen und hochrangige IT-Systeme mit dem Fokus auf den Sicherheits- und Verteidigungssektor. Entwickelt von einem deutschen Team aus Sicherheitsexperten, gewährleistet SSE, dass Kundensysteme den strengen Sicherheitsanforderungen entsprechen. Die vom Unternehmen entwickelte, KI-unterstützte Datenanalyseplattform wandelt multi-level Sensordaten in Lösungen zur Entscheidungsunterstützung und Cybersicherheit um. Als führendes Technologieunternehmen entwickelt, konstruiert und integriert die SSE maßgeschneiderte Lösungen, die durch wirkungsvolle Beratung, Unterstützung und Schulung ergänzt wird. Als zertifiziertes Unternehmen nach Standard ISO 9001, ISO/IEC 20000-1 und ISO/IEC 27001 verkörpert die SSE Exzellenz im Qualitätsmanagement, IT-Service und Informationssicherheit.

**SCOTTY Group Austria GmbH****A 12 + N 08**

SCOTTY ist ein mittelständiges österreichisches Unternehmen mit dem Standort in Raaba-Grämbach bei Graz und ist seit über 20 Jahren tätig. SCOTTY ist für hochzuverlässige Kommunikationslösungen, welche insbesondere auch Satelliten basierenden Systeme integrieren, sowie für die sicheren und zonierte Videokonferenzanlagen bekannt. SCOTTY hat – mit großer Zufriedenheit seiner Kunden – eine Vielzahl an Individualösungen im sicherheitskritischen Umfeld entwickelt. Die SCOTTY Produkte finden in den allen Einsatzbereichen im land-mobilen, maritimen sowie aeronautischen Umfeld weltweit Verwendung. SCOTTY verfügt über außergewöhnliche Referenzen in unterschiedlichen militärischen und zivilen Bereichen.

**secunet Security Networks AG****F 19**

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 spezialisiert auf Bereiche, in denen es besondere Anforderungen an die IT-Sicherheit gibt – wie z.B. bei eingestuftem Inhalten bis GEHEIM. Über 1000 Expert*innen stärken die digitale Souveränität von Regierungen, Unternehmen und der Gesellschaft. Zu den Kunden zählen die Bundeswehr, diverse Bundesministerien, mehr als 20 DAX-Konzerne sowie weitere nationale und internationale Organisationen. secunet ist IT-Sicherheitspartner der Bundesrepublik Deutschland und Partner der Allianz für Cyber-Sicherheit. Kontakt: defencespace@secunet.com

**Secusmart GmbH****S 51**

Secusmart ist der führende Anbieter von sicheren mobilen Kommunikationslösungen für die Behörden und Institutionen des Bundes. Neben SecuSUITE for Samsung Knox wurden nach erfolgreicher BSI-Evaluierung auch iPhones und iPads in einer sicheren Konfiguration für die Verarbeitung von VS-NfD-Daten freigegeben. SecuSUITE for iOS komplettiert das Portfolio des Düsseldorfer Unternehmens für sicheres mobiles Arbeiten. SecuSUITE for Samsung Knox und SecuSUITE for iOS sind hochsichere mobile Plattformen für mobile Daten und Sprache auf Samsung- und Apple-Smartphones und -Tablets und hat die Freigabeempfehlung bis zur Geheimhaltungsstufe VS-NfD („Classified Information - For Official Use Only“).



SELECTRIC Nachrichten-Systeme GmbH**S 35**

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

SELECTRIC**SentinelOne GmbH****R 45**

SentinelOne ist ein Leader in Autonomer Cybersecurity und ein Forbes AI 50 Unternehmen. Die KI-gestützte SentinelOne Singularity™ Cybersecurity Plattform erkennt, verhindert und reagiert auf Cyber Angriffe in Maschinengeschwindigkeit und versetzt Unternehmen so in die Lage, Endgeräte, Cloud Workloads und Container, Identitäten, sowie mobile und mit dem Netzwerk verbundene Geräte schnell, akkurat und einfach zu schützen. Mehr als 10,000 Kunden weltweit, darunter Hunderte der Global 2000 Unternehmen, Regierungseinrichtungen, Gesundheitsdienstleister und Bildungseinrichtungen, vertrauen SentinelOne. Weitere Informationen unter www.sentinelone.com.

 **SentinelOne****SES****B 11**

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 führender globaler Anbieter von Konnektivitätslösungen für Inhalte besitzt und betreibt SES die weltweit einzige Konstellation aus Satelliten in der geosynchronen (GEO) und mittleren (MEO) Erdumlaufbahn, um eine weltweite Abdeckung und hohe Leistungsstärke anzubieten. Mithilfe des umfangreichen und intelligenten cloudfähigen Netzwerks kann SES an jedem Ort zu Land, zu Wasser und in der Luft hochwertige Konnektivitätslösungen bereitstellen und ist Partner weltweit führender Telekommunikationsunternehmen, Mobilfunkbetreiber, staatlicher Regierungsbehörden, Konnektivitäts- und Cloud-Dienstleistern, Rundfunkanbietern, Betreibern von Videoplattformen und Inhaltenanbietern.

SES
SPACE & DEFENCE**SIEMENS DIGITAL INDUSTRIES SOFTWARE****G 04**

Beschleunigen Sie Beschaffungsprogramme
Das Siemens Xcelerator Portfolio von Siemens Digital Industries Software unterstützt führende Unternehmen der Verteidigungs- und Sicherheitsindustrie bei der Erstellung und Nutzung digitaler Zwillinge komplexer Systeme von der Anforderung bis zum Einsatz. Der digitale Zwilling bietet neue Einblicke, Möglichkeiten zur Zusammenarbeit und einen hohen Automatisierungsgrad, um Innovation und Effizienz über das gesamte Partner-Eco-System zu beschleunigen. Durch seine Interoperabilität, Durchgängigkeit und die weite Verbreitung in der Industrie, Behörden und führenden Programmen bietet Siemens Xcelerator einzigartige Möglichkeiten zur Umsetzung der digitalen Transformation. Siemens genießt das Vertrauen von Herstellern und Behörden in die Digitalisierung. Entdecken Sie die digitale Zukunft mit Siemens! siemens.com/software.

SIEMENS**SMS System-Management Stiewi GmbH****S 56**

Das Potenzial der Digitalisierung im öffentlichen Sektor ist hoch, doch die regulatorische Dynamik und eine komplexe Compliance machen die Entwicklung von Anwendungen zur Herausforderung. Die

 **SMS**
SYSTEM-MANAGEMENT STIEWI

SMS System-Management Stiewi GmbH begleitet Bund, Länder und öffentliche Institutionen seit über 30 Jahren als Digitalisierungspartner für das Travel Management und hat sich als Marktführer für Softwarelösungen im Bereich der Reisekosten-, Trennungsgeld- und Umzugskosten der öffentlichen Verwaltung etabliert. Über 300 Bundes- und Landesbehörden sowie Anstalten des öffentlichen Rechts vertrauen auf die hoch spezialisierten Software-Produkte, die sich zu individuellen Komplettlösungen verbinden lassen – perfekt aufeinander abgestimmt, nahtlos in die IT-Landschaft integriert und von Support-Services flankiert.

Software AG**S 20**

Innovativ, leistungsstark, Partner der Bundeswehr

Software AG ist einer der führenden Anbieter von IoT-, Prozess- und IT-Lösungen für die Verteidigungsindustrie. Mit unseren Lösungen „Made in Germany“ steigern Streitkräfte die Effizienz und optimieren ihre Prozesse, um qualifizierte Entscheidungen in Echtzeit zu treffen.

Als Innovationspartner unterstützt die Software AG die Bundeswehr, ihre Prozesse agil an neue Herausforderungen anzupassen und die IT-Landschaft dynamisch zu skalieren.

 **software AG****Soldaten und Veteranen Stiftung****R 26**

Die 2013 gegründete Soldaten und Veteranen Stiftung vereint in ihrem Namen bereits das, worum es ihr geht: Förderung der gesellschaftlichen Anerkennung der Menschen der Bundeswehr. Die Stiftung setzt sich dafür ein, dass die Bundeswehr und ihre Menschen als selbstverständlicher Teil der Gesellschaft wahrgenommen werden und Wertschätzung für ihre Arbeit erfahren. Unsere Arbeit basiert auf gelebter Kameradschaft und in dem Wissen: Vertrauen verbindet! Wir unterstützen, wo eine helfende Hand benötigt wird. Wir stehen zur Seite, wenn schnell und unbürokratisch finanzielle Hilfe notwendig wird. Wir bauen Brücken zwischen den Menschen in der Bundeswehr und in der Gesellschaft. Dafür steht die SVS.


Soldaten und Veteranen Stiftung**Soldatenhilfswerk der Bundeswehr e.V.****R 25**

„Not lindern, Hoffnung geben“ – Das Soldatenhilfswerk der Bundeswehr e.V. (SHWBw) unterstützt Soldaten/-innen, beorderte Reservisten/-innen und ihre Familien, die in unverschuldete Notlagen geraten sind, wo staatliche oder versicherungsrechtliche Unterstützung noch nicht, nicht mehr oder auch gar nicht greift – durch schnelle und unbürokratische finanzielle Hilfe. Als mildtätiger Verein finanziert es seine Leistungen im Wesentlichen aus Spenden. Es erhebt keine Mitgliedsbeiträge und erhält keine staatlichen oder anderweitigen Zuschüsse. Seit seiner Gründung im Jahr 1957 hat das Soldatenhilfswerk in über 35.800 Fällen mit einem Betrag von über 27,5 Millionen Euro Kameradschaftshilfe geleistet. Dabei hilft jede Ihrer Spenden! Die vier verschränkten Hände im Logo des SHWBw stehen für die Idee des kameradschaftlichen Zusammenhalts und für die helfende Hand, die dem unverschuldet in Not Geratenen gereicht wird.

**Solifos Deutschland GmbH****S 27**

Als Spezialist für faseroptische Kommunikations- und Überwachungslösungen bietet die Solifos einzigartige Systemlösungen. Die in der Wehrtechnik bekannten, zuverlässigen und robusten taktischen faseroptischen Feldkabel werden seit über 10 Jahren im Feld eingesetzt. Unsere taktischen Feldkabel werden als Komplettsystem mit dazugehörigen Kabelrollen, Steckern oder IT-Infrastruktur ausgeliefert. Mit unseren takti-

 **SOLIFOS**
FIBER OPTIC SYSTEMS

schen Hybridkabeln können Sie im Feld mit einem Kabel Daten und Energie über mehrere Kilometer Distanz transportieren. Unser BRUmil Kabel besitzt nun offiziell die begehrte VG Zulassung VG 95218 Teil 30 Typ L. Kontakt: Dirk Mahler, Mobil +49 (0) 170 7409987, Email: dirk.mahler@solifos.com

SOPHIST GmbH

R 53

SOPHIST ist ein führendes Beratungs- und Trainingsunternehmen im Bereich Requirements- und Systems-Engineering und Künstlicher Intelligenz, sowohl im klassischen als auch agilen Projektumfeld. Bereits seit 1996 unterstützt SOPHIST Kunden bei der Entwicklung und Einführung von maßgeschneiderten und qualitativ hochwertigen Software- und Systemlösungen mit einem breiten und umfangreichen Portfolio, bestehend aus operativer Projektunterstützung, Methodeneinführung und -vermittlung, Prozessoptimierung, Trainings, Coachings und vielem mehr. SOPHIST ist TISAX-auditiert und garantiert einen hohen Daten- und Informationssicherheitsstandard. SOPHIST ist zudem ein Platinum Partner des International Requirements Engineering Board (IREB) und bereitet Teilnehmende auf die CPRE-Zertifizierung vor. SOPHIST steht für Professionalität, Innovation und Nachhaltigkeit.



Sophos Technology GmbH

S 62

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



Sopra Steria SE

S 12

Sopra Steria ist ein führendes europäisches Technologieunternehmen mit anerkannter Expertise in den Geschäftsfeldern Consulting, Digital Services und Softwareentwicklung. Das Unternehmen unterstützt seine Kunden dabei, die digitale Transformation voranzutreiben und konkrete und nachhaltige Ergebnisse zu erzielen. Sopra Steria bietet mit seinen 56.000 Mitarbeitenden in rund 30 Ländern umfassende End-to-End-Lösungen, die Unternehmen und Behörden wettbewerbs- und leistungsfähiger machen – und zwar auf Grundlage tiefgehender Branchenexpertise, innovativer Technologien und eines kollaborativen Ansatzes. Das Unternehmen stellt die Menschen in den Mittelpunkt seines Handelns mit dem Ziel, digitale Technologien optimal zu nutzen und eine positive Zukunft für seine Kunden zu gestalten. The world is how we shape it



Spleelab GmbH

R 57

Die SPLEENLAB GmbH ist ein hochspezialisiertes KI-Software Unternehmen aus Thüringen, das mit der Idee gegründet wurde, Sicherheit und KI neu zu definieren. Seit April 2018 beschäftigt sich das Unternehmen primär mit der Entwicklung und dem Vertrieb von sicheren maschinellen Lernalgorithmen für die teil- und vollautonome Mobilität, insbesondere für unbemannte Luft- und Bodenfahrzeuge.



Splunk

W 02

Splunk hilft Unternehmen, resilient zu werden. Führende Unternehmen nutzen unsere Plattform, die Security und Observability vereint, um die Sicherheit und Zuverlässigkeit ihrer digitalen Systeme zu erhalten. Sie vertrauen auf Splunk,



DIPD | DEFENCE INNOVATION PITCH DAY

SAVE the DATE

7. November 2024, München

Haus der Bayerischen Wirtschaft

Ihr wollt als Start-Up aus den Bereichen Sicherheit, Verteidigung, Luft- oder Raumfahrt beim Defence Innovation Pitch Day dabei sein und pitchten?

Dann bewirbt Euch bis zum **31. Juli 2024** mit eurem Pitch-Deck bei:
benjamin.bauer@behoerderspiegel.de

Foto: © Marc-A. Wierfeld, AFX Landsysteme

Eine Veranstaltung des Behörden Spiegel

www.defence-innovation.de


um zu verhindern, dass sich Sicherheits-, Infrastruktur- und Anwendungsprobleme zu größeren Vorfällen entwickeln, um Beeinträchtigungen durch digitale Störungen zu reduzieren und um die Transformation zu beschleunigen. Um dies zu erreichen, ermöglicht Splunk SecOps-, ITOps- und DevOps-Teams umfassende Transparenz, schnelle Erkennung und Untersuchungen sowie optimierte Reaktionen – all das in genau der Größenordnung, welche die weltweit größten digitalisierten Unternehmen brauchen.

steep GmbH

S 39

Zur diesjährigen AFCEA-Fachausstellung zeigen wir Ihnen an unserem Messestand S39 im Saal New York/Genf unsere konkreten Digitalisierungslösungen. 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



Stellar DBS GmbH

F 14

Stellar steht 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 von der Deutschen Raumfahrtagentur im 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.



SThree GmbH

S 52

Für Ihren Erfolg ist es entscheidend, einen Partner zur Seite zu haben, der Ihre Ambitionen versteht und passende MINT-Talente der Verteidigungsindustrie findet. Wir stehen mit Ihnen in engem Dialog, um Ihre speziellen Anforderungen zu verstehen und Sie mit hochqualifizierten Fach- und Führungskräften zu vernetzen, die Ihre Schlüsselpositionen und Projekte stärken. Unsere Unterstützung umfasst außerdem das komplexe Terrain der Compliance-Anforderungen. In einer sich ständig verändernden MINT-Branche unterstützt SThree Ihr Unternehmen dabei, zukunfts- sowie wettbewerbsfähig zu bleiben und agil den Herausforderungen der Zukunft zu begegnen.



SVA System Vertrieb Alexander GmbH

S 53

Die SVA System Vertrieb Alexander GmbH zählt mit mehr als 3.200 Mitarbeitenden an 27 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 Öffentlicher Dienst ist spezialisiert auf den Verkauf von Hard- und Software etablierter Hersteller sowie den Vertrieb entsprechender IT-Dienstleistungen für öffentliche Auftraggeber. Über 380 Mitarbeiter 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.

Systematic GmbH

S 47

Systematic ist Weltmarktführer für Battle-Management-Applikationen, Führungsinformationssysteme und Lösungen für militärische Interoperabilität. Mit 50+ Nutzernationen inklusive 18 NATO-Staaten ist SitaWare das meistgenutzte Führungsinformationssystem weltweit. Die Commercial-Off-The-Shelf (COTS) Produkte der SitaWare und IRIS Produktsuiten haben sich weltweit in multinationalen Einsätzen bewährt und werden permanent weiterentwickelt. Einsetzbar in stationären, verlegfähigen, mobilen und seegehenden Systemumgebungen, bietet die C4I-Software einen sofortigen operationellen Mehrwert. Intelligente Dienste zur Datenkommunikation ermöglichen die Nutzung vorhandener militärischer Kommunikationsmittel und ermöglichen damit eine gesamtheitliche Betrachtung der Digitalisierung der Streitkräfte. Die Interoperabilität mit nationalen-, internationalen- und NATO-Systemen steht dabei im Fokus. SitaWare ist in der Bundeswehr als Mission Enabling Service Bundeswehr (MESBW) eingeführt.



systerra computer GmbH

S 64

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 applikationspezifische 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, info@systerra.de, www.systerra.de



TASSTA

F 14

TASSTA ist die perfekte missionskritische Push-to-Talk-Softwarelösung, entwickelt nach ETSI 3GPP, für Sicherheitsaufgaben, die folgende Merkmale aufweist: sichere Kommunikation, Echtzeit-Standortverfolgung, anpassbare Systemoberfläche, verschlüsselte Kommunikation und die Fähigkeit, in Umgebungen mit geringer Bandbreite und über Satelliten-Kommunikation zu arbeiten. Die TASSTA-Lösung verfügt über eine benutzerfreundliche Oberfläche für Android, iOS und Windows und läuft auf PTT robusten Geräten für den Einsatz unter extremen Bedingungen. Das System kann über diverse Gateways auch in bestehende Kommunikationssysteme, wie Tetra, P25, DMR, etc., integriert werden und ermöglicht somit eine systemübergreifende Kommunikation. Eine Integration in andere Applikationen und Command Control Systemen ist ebenfalls möglich.



tde – trans data elektronik GmbH, Vertriebsbüro Dortmund

R 71

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 37. 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.

TEHTRIS

S 61

TEHTRIS unterstützt europäische Unternehmen jeder Größe und Branche bei der Bewältigung ihrer IT- und OT-Security Strategie durch automatische Entdeckung und Neutralisierung von Cyberangriffen und Spionage in Echtzeit. Ermöglicht wird dies durch die TEHTRIS XDR AI Plattform, das einzige 100% in Europa entwickelte XDR. Die Vorteile von TEHTRIS erlauben dabei einen 24/7 Schutz vor Cyberangriffen und eine globale und holistische Sicht auf die Systeme ihrer Kunden. Durch die inkludierten SIEM und SOAR-Regeln werden keine komplexen Integrationen benötigt. Eine 100%ige Kundenloyalität in mehr als 100 Ländern zeugt von der technischen Überlegenheit, die auch von Gartner als repräsentativer Anbieter für XDR“ anerkannt wird.



TEKSAM GmbH

W 03

Die Teksam GmbH als deutsche Vertriebs Tochter des belgischen Herstellers TeksamCompany NV liefert seit Mai 1994 mobile Mastsysteme für den freien Feldaufbau als auch für den Anbau an Containern sowie Fahrzeugen. Wir liefern Masten bis zu einer Höhe von 40 Metern als Sektionalmaste und bis zu 30 m Höhe als pneumatische Aluminium-Teleskopmaste. Kleine mobile tragbare Systeme „Manpack“ gehören ebenfalls zu unserem Leistungsspektrum. Kundenbezogene Anforderungen umzusetzen sowie ständige Weiterentwicklung unserer Produkte sind unsere Stärke. Unsere Produkte vertreiben wir unter den Markennamen Clark Masts sowie TekMast.

Teksam GmbH – Bergisch Gladbach



Telespazio Germany GmbH

A 10 + F 09

Telespazio Germany GmbH, eine Tochtergesellschaft von Telespazio – einem Joint Venture zwischen Leonardo (67%) und Thales (33%) – ist ein führendes Unternehmen der Luft- und Raumfahrt, das Beratungs-, Technologie- und Ingenieurdienstleistungen anbietet. Mit einem Team von mehr als 400 Mitarbeitern unterstützen wir unsere Kunden durch die Bereitstellung hochwertiger und innovativer Kontroll-, Planungs- und Datenverarbeitungssysteme und Schulungslösungen in der Raumfahrt sowie Lösungen im Bereich Cybersecurity und Informationssicherheit. Mit mehr als zwei Jahrzehnten Erfahrung ist Telespazio Germany weltweit führend im Bereich Trainingslösungen und bietet maßgeschneiderte Trainingssysteme für Piloten- und Operator-Training, sowie virtuelle Wartungstrainer und VR-basierte Lösungen für die Ausbildung von Wartungstechnikern.



Tenzir GmbH

R 63

Tenzir revolutioniert die Art und Weise, wie Cyber-Sicherheitsdaten in großem Maßstab operationell gemacht werden, indem es IT-Organisationen und Cyber-Verteidigern eine geschäftskritische, verteilte Sicherheitsdatenplattform zur Verfügung stellt. Unsere Lösung ermöglicht die Verarbeitung riesiger Mengen an Telemetrie- und Bedrohungsdaten und bricht gleichzeitig Silos zwischen Sicherheitslösungen auf. Wir sind ein leidenschaftliches, wissenschaftlich und technisch geführtes Team von 16 Mitarbeiterinnen und Mitarbeitern, das es liebt, schwierige Sicherheitsprobleme zu lösen, ohne Abstriche zu machen. Wir glauben, dass die Bereitstellung wertorientierter Software, die auf Open-Source-Prinzipien basiert, um grundlegende Probleme für alle zu lösen, das Richtige ist. Bei uns steht der Kunde immer an erster Stelle.



Thales Deutschland

S 23

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 und volle Handlungssouveränität. www.thalesgroup.com/germany



ThermoAnalytics

B 10

ThermoAnalytics (TAI) is a global thermal, fluid-flow, and infrared modeling software developer. TAI provides software and services to both commercial and government customers. Over its 25 years existence, TAI has pioneered thermal analysis tools and technologies used in automotive, architecture, aerospace, defense, manufacturing, and textiles. Our flagship product, MuSES (Multi-Service Electro-Optic Signature) is an industry-leading signature management software that provides complete thermal modeling and infrared signature prediction capabilities. MuSES allows you to simulate any environment or condition and generate accurate signature predictions.



Traversals GmbH

R 63

At Traversals, we provide governmental and non-governmental organizations with state-of-the-art tools they need to accomplish their missions. Our team has a proven track record of collaborating with various organizations, and we possess unparalleled expertise in collecting, processing, and analyzing data from diverse sources. Our mission is to provide our clients with high-quality information, enabling them to lead, decide, and shape the future. With our Software Defined Intelligence Architecture, we deliver flexible and efficient solutions tailored to meet the specific needs of our customers.



Trend Micro Deutschland GmbH

S 36

Bei Trend Micro ist es unser Ziel, die Welt für den Austausch digitaler Informationen sicherer zu machen. Wir sind davon überzeugt, dass Cyber Risiken gleichzeitig Geschäftsrisiken darstellen. Deshalb ermöglichen wir Unternehmen vollständige Transparenz und Kontrolle ihrer digitalen Assets. So verstehen sie, wie gut sie geschützt sind und welche Investitionen wichtig sind, um das Risiko zu senken. Mit uns wird die Welt sicherer, da wir schon früh erkennen, wie sich moderne Infrastrukturen, Nutzerverhalten, Applikationsentwicklung und damit auch Cyberbedrohungen verändern und darauf reagieren. Ansprechpartnerin: Karin Schall, karin_schall@trendmicro.com



Treo – Labor für Umweltsimulation GmbH

S 55

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 den Branchen Verteidigung, Luftfahrt, Schiffbau und Bahn. Für militärische Produkte können wir nahezu alle benötigten Prüfungen aus einer Hand anbieten. Wir prüfen z.B. gemäß MIL-STD 810, MIL-STD 461 und diversen AECTP- und VG-Normen.

Ultralife Corporation

S 30

Ultralife Corporation ist ein führender Anbieter von fortschrittlichen, hochwertigen Produkten und Dienstleistungen, die von Stromversorgungslösungen bis hin zu Kommunikations- und Elektroniksystemen für Kunden in aller Welt in den Bereichen Regierung und Verteidigung, Medizin, Sicherheit, Energie, Industrie und Robotik reichen. Ultralife legt großen Wert auf solide Technik und bietet ein umfangreiches Sortiment an kosteneffizienten nicht wiederaufladbaren und wiederaufladbaren Hochenergie-Batterien, Ladesystemen und kundenspezifischen Systemen. Communications Systems liefert eine Familie von kampferprobten funkunabhängigen Verstärkern für den auf- und abgesehenen Einsatz, robuste und innovative Multi-Funkhalterungen und Stromversorgungen zur Unterstützung von unterschiedlichsten Arten von Funkgeräten und Anwendungen.

JK Defence & Security Products GmbH, milcom@jkdefence.de
www.jkdefence.de, 02152/1445-207



utimaco GmbH

S 19

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. Mehr als 500 Mitarbeiter tragen Verantwortung für Kunden und Bürger weltweit, indem sie innovative Sicherheitslösungen und Services entwickeln, die ihre Daten, Identitäten und Netzwerke schützen. Partner und Kunden aus den unterschiedlichsten Industrien schätzen die Zuverlässigkeit und langfristige Investitionssicherheit der Utimaco-Sicherheitslösungen. Weitere Informationen unter www.utimaco.com



VECTED GmbH

R 43

Als Spezialist für Wärmebildtechnologie mit integrierter Künstlicher Intelligenz (KI) entwickeln und produzieren wir Wärmebildgeräte sowie Elektronikmodule und bieten unseren Kunden individuelle High-End-Lösungen. Im Bereich Rüstung sind wir in der Lage, den gesamten Entwicklungs-, Qualifikations- und Produktionsprozess zu leisten. Von der Entwicklung hauseigener optoelektronischer Hard- und Software über das Design, Training und die Evaluierung der integrierten KI sind wir in der Lage, den Prototypenbau und die Qualifikation bis hin zur Produktion ITAR-frei aus einer Hand anzubieten. Kontakt: Ralph Wilhelm, E-Mail: info@vected.de, Tel: +49 911 960 687 0



Verband der Reservisten der Deutschen Bundeswehr e.V.

B 02

Der Verband der Reservisten der Deutschen Bundeswehr e.V. (VdRBw)

Der Reservistenverband und seine rund 110.000 Mitglieder treten aktiv für die freiheitliche demokratische Grundordnung der Bundesrepublik Deutschland ein. Reservistinnen und Reservisten finden hier auch nach dem



WIR SIND DIE RESERVE
VERBAND DER RESERVISTEN
DER DEUTSCHEN BUNDESWEHR e.V.

Dienst ihre militärische Heimat. Im Auftrag der Bundeswehr betreut der Verband alle ehemaligen Soldatinnen und Soldaten der Bundeswehr und bildet sie militärisch und sicherheitspolitisch aus und fort.

Der Reservistenverband ist/ bietet:

- Sicherheitspolitischer Akteur
- Mittler in der Gesellschaft für Bundeswehr und Reserve
- Ausbilder (IGF/KLF) und Ausbildung Ungedienter
- Militärische Heimat – Reservistendienst, Schießen, Kameradschaft
- Betreuung und Fürsorge

Viasat

S 30

Seit mehr als 30 Jahren tragen die Innovationen von Viasat dazu bei, dass Unternehmen, Regierungen und Militärs auf der ganzen Welt an den entlegensten Orten kommunizieren.

Viasat ist einer der weltweit führenden Anbieter von UHF-Satcom-Technologie für die NATO und verbündete Nationen. Die Software-Plattform VISION (Visual Integrated Satellite Communications Information, Operation and Networking) realisiert eine größere Interoperabilität, Skalierbarkeit und Flexibilität bei der Kommunikation über alte und neue UHF-Satellitenplattformen und verbessert somit die Effizienz für den Übergang zur Integrierten Wellenform (IW).

Es ist das erste kommerziell erhältliche Softwarepaket, das gleichzeitig alle 25-kHz-Legacy-DAMA- und IW-Netze und -Dienste der nächsten Generation unterstützt.

JK Defence & Security Products GmbH, milcom@jkdefence.de, www.jkdefence.de, 02152/1445-207



Vitec GmbH

W 04

Seit 1988 ist VITEC weltweit führend als Anbieter von innovativen Produkten und Systemen im Bereich von professionellen „End to End“-Video Streaming Lösungen für das Militär, Behörden und Organisationen mit Sicherheitsaufgaben, Rundfunkanstalten, Telekommunikationsunternehmen und Medizintechnik. Durch die Zusammenführung und Integration der seit vielen Jahren in ihrem Spezialgebiet etablierten Unternehmen Exterity, IPtec, Optibase, Como, Focus und Stradis kann VITEC eine lückenlose Kette von professionellen Komponenten für Video über IP-Video-Streaming, Media Management, Video- & Image-Processing, Encoding/Decoding und Signalwandlung anbieten. Mit weit mehr als zweihundert Entwicklungsingenieuren realisiert VITEC innovative und kosteneffektive Hard- und Software-Lösungen, Advanced Technology Research und Custom Design Produkte für ein internationales Kundennetzwerk.



VITES GmbH

W 06

Die VITES GmbH („VITES“) ist ein innovativer deutscher Anbieter von hochleistungsfähigen Breitband-Funksystemen und kundenspezifischen Lösungen für professionelle Anwendungen. Der Schwerpunkt liegt auf der Entwicklung von elektronisch gesteuerten Flat Panel Terminals für SATCOM-on-the-Move Anwendungen (ViSAT), geeignet für GEO und NGSO-Konnektivität (MEO, LEO). ViSAT-Terminals basieren auf einer energieeffizienten aktiven Phased-Array-Technologie, die für jede Art von Fahrzeug geeignet ist. Im Bereich der öffentlichen Sicherheit ist VITES etablierter Lieferant von mobilen Kommunikationsknoten (vikomobil 2.0) sowie Netzwerkausrüstung für LTE-/5G-Netze, inklusive eSIM-Management. vikomobil 2.0 ist eine modulare Komplettlösung, die ein LTE-/5G-Netz mit SATCOM (GEO oder LEO) als Backhaul-Verbindung integriert. Eine Methanol-Brennstoffzelle gewährleistet den energieautonomen Betrieb.



Willert Software Tools GmbH

B 06 a

SodiusWillert designs and distributes software solutions for Enterprise Interoperability, Linked Data and Model Transformation to improve traceability, exchange, and sharing of engineering data in highly regulated industries. With offices in France, Germany and the USA, the company deploys its solutions worldwide in Aerospace, Automotive, Transportation, Defense and Medical industries. Today, SodiusWillert is a global leader in technology to manage complex systems leveraging the power of connected data to enable the products of tomorrow.



WORK Microwave GmbH

F 12

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

S 25

Die Xecuro GmbH ist eine hundertprozentige Tochter der Bundesdruckerei Gruppe GmbH. Sie wurde im November 2021 gegründet, um das neue digitale System für die Verschlusssachen-Kommunikation des Bundes mit aufzubauen und später zu betreiben. Das System reicht von einer verschlüsselten Telefonie- und Videokonferenz-Technik bis zum sicheren Datenaustausch zwischen Mi-



nisterien und Behörden. Xecuro betreibt dafür die Infrastruktur, betreut die Endgeräte und ist für den Service verantwortlich. In den nächsten Jahren soll das neue Unternehmen auf rund 150 Beschäftigte wachsen. Standorte der Xecuro sind derzeit Berlin und Bonn.

ZARGES GmbH

W 08

ZARGES steht seit über 80 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 Germany GmbH

S 35

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.





DEFENCE DAYS

4. September 2024

**DAS ZIELBILD DER
DEUTSCHEN MARINE –
FÄHIGKEITSDOMÄNEN UND
PLANUNGSKATEGORIEN**

30. Oktober 2024

**DAS ZIELBILD DER
DIMENSION CIR –
FÄHIGKEITSDOMÄNEN UND
PLANUNGSKATEGORIEN**

4. Dezember 2024

**DAS ZIELBILD DER
STREITKRÄFTEBASIS –
FÄHIGKEITSDOMÄNEN UND
PLANUNGSKATEGORIEN**

WEITERE INFORMATIONEN UNTER WWW.DIGITALER-STAAT.ONLINE/PROGRAMM

Foto: BS/Rheinmetall

Veranstaltungen des Behörden Spiegel

Inserentenverzeichnis

Advertorials

Adva Network Security	Seite 87
Bechtle	Seite 26
Infodas	Seite 54
Sophos Technology	Seite 64
Sopra Steria	Seite 61
Systematic	Seite 47
VECTED	Seite 67

Anzeigen

BDSV	Seite 34
Capgemini	Seite 33
Computacenter	Seite 81
CONDOK	Seite 99
dainox	Seite 19
Diamond	Seite 93
Elbit Systems	Seite 97
ESG	Seite 91
Hensoldt	Seite 10
IBM	Seite 29
infodas	Seite 85
Innosystec GmbH	Seite 83
KNDS Deutschland Mission Electronics GmbH	Seite 89
Materna	Seite 79
Materna Virtual Solution	Seite 5
OHB	Seite 95
Panasonic Connect	Seite 40
PLATH	Seite 31
Rheinmetall	Seite 17
roda computer	Seite 66
secunet	Seite 9
Secusmart	Seite 2
steep GmbH	Seite 12
systerra computer	Seite 24
VITEC	Seite 14

Berlin Security Conference 2024

19.–20. November 2024, Vienna House Andel's Berlin



Fotos: Boris Trenkel

Die Berliner Sicherheitskonferenz

- Eine der größten Veranstaltungen zur europäischen Sicherheit und Verteidigung
- 14 Tage nach den US-Präsidentschaftswahlen
- Analysiert die Entwicklung der europäischen sicherheitspolitischen und militärischen Fähigkeiten und Beschaffung, eingebettet in den sicherheits- und verteidigungspolitischen Kontext von EU, NATO und OSZE. Mit besonderem Augenmerk auf den Krieg in der Ukraine, Abschreckung und Verteidigung in und für Europa nach dem russischen Angriffskrieg, Way Ahead NATO und EU und auf die Krisenregionen im Nahen Osten
- Internationales Forum für Abgeordnete, Politiker und Angehörige der Streitkräfte, der Organisationen mit Sicherheitsaufgaben und der Industrie (einschließlich junger Führungskräfte)
- Nationale und internationale Aussteller
- Organisiert vom **Behörden Spiegel** – Deutschlands führender unabhängiger Zeitung für den Öffentlichen Dienst

Weitere Informationen (englisch): www.euro-defence.eu



Vorankündigung:

38. AFCEA-Fachausstellung

27. – 28. 05. 2025

World Conference Center Bonn

www.afcea.de