AFCEA 2019

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

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

ISBN 978-3-934401-50-1

BWI
IT für Deutschland

IT für Deutsch-land

BWI: Ihr Partner für die Digitalisierung der Bundeswehr

Die BWI hat die IT der Bundeswehr zu einem standardisierten und zentralisierten IT-System umgebaut, das bereits heute durch seine Leistungsfähigkeit überzeugt. Und die nächste Phase hat schon begonnen.

Als Innovationstreiber entwickeln wir das bestehende System weiter und weiter. Wir analysieren Trends, stellen neue Technologien auf den Prüfstand und überführen sie in konkrete Lösungen für die Bundeswehr-IT: von der „Bundeswehr-Cloud" bis zur sicheren virtuellen Desktop-Infrastruktur. Als IT-Systemhaus der Bundeswehr verstehen wir Ihre Herausforderungen in allen Bereichen und haben die passenden Lösungen schon parat – von der IT-Beratung über die Umsetzung bis hin zum sicheren Betrieb innovativer Lösungen.

@BWI_IT
/BWIITfuerDeutschland
blog.bwi.de

Erfahren Sie mehr
www.bwi.de

Benedikt Zimmer

Foto: Bundeswehr, Jane Schmidt

Sehr geehrte Damen und Herren,

Die Vernetzung sämtlicher Arbeits- und Lebensbereiche durch Informations- und Kommunikationstechnologie schreitet unverändert und mit hohem Tempo voran. Es ist daher nur konsequent, das Jahresthema 2019 jenen Herausforderungen zu widmen, die dafür Sorge tragen, dass der technologische Fortschritt zum Wohle aller besser und nutzerorientiert ausgerichtet werden kann.

Sowohl für den privaten als auch für den betrieblichen Gebrauch erwarten wir von unseren elektronischen Produkten und Dienstleistungen mehr Verzahnung und mehr Interoperabilität. Wir sprechen gerne von Konvergenz. Aus Nutzersicht ist es für uns zwingend, ein neues Verständnis von elektronischen Diensten und Anwendungen in der Weise zu entwickeln, dass künftig digitale Güter und Informationen nahtlos elektronisch abgewickelt werden können. Vielleicht ist es aktuell nur eine Vision, aber es ist jetzt an der Zeit, diesen Anspruch zu artikulieren und in nutzergerechte Produkte und Dienste umzusetzen.

Nichtstun ist hier keine Option. Und auch Nicht-Wissen ist kein Weg für die Zukunft. Wir müssen daher in Köpfe und Ideen investieren, den gestalterischen Umgang mit Technik und Technologie fördern und den digitalen Kompetenzerwerb als Handlungsschwerpunkt in Staat, Wirtschaft und Gesellschaft fest verankern. Im Digitalen kompetent zu sein, heißt explizit auch, problematische Auswirkungen analytisch-kritisch erfassen und Digitalisierung sowohl ethisch als auch sozial-verantwortlich reflektieren zu können.

Chancen, Risiken und Konsequenzen für unser eigenes Handeln müssen deutlich werden. Für diese Analysen müssen wir vorbereitet sein. Nur mit einem umfassenden und tiefen Verständnis für die Thematik wird es künftig möglich sein, Innovationszyklen und deren Implikationen zeitgerecht zu verstehen und die notwendigen Schritte einzuleiten. Ich möchte Sie daher ermutigen, sich dem diesjährigen Themenfeld frei und unverstellt zu nähern und die vielen Debatten und Diskussionen offen zu führen.

Ihr Benedikt Zimmer,

Staatssekretär im Bundesministerium der Verteidigung

AFCEA 2019

1. AFCEA Bonn e.V. – Digitale Kompetenz und Konvergenz

AFCEA Bonn e.V. – mit neuem Vorstand und neuem Jahresthema
Brigadegeneral Armin Fleischmann, Vorsitzender AFCEA Bonn e.V. und Abteilungsleiter Planung im Kommando CIR 6

Digitale Kompetenz und Konvergenz – im Zeitalter intelligenter Systeme
Oberst i.G. Heiko Mühlmann, stellvertretender Vorsitzender AFCEA Bonn e.V und Referatsleiter BMVg CIT 8

Need for Speed – wissenschaftliche Überlegungen zu Mensch und Künstlicher Intelligenz
Dr.-Ing. Michael Wunder, Vorstand AFCEA Bonn e.V.,
Abteilungsleiter „Informationstechnik für Führungssysteme“, Fraunhofer FKIE 10

Methoden zur robusten Sprechererkennung
Kevin Wilkinghoff, Fraunhofer FKIE, Abteilung KOM, AFCEA Studienpreisträger 2018 12

Digitale Kompetenz der Behörden mit Ordnungs- und Sicherheitsaufgaben im Zeitalter intelligenter Systeme
Tobias Schönherr, Dipl.-Ing., Polizeidirektor, Stabsbereichsleiter Technik und Logistik,
Bundespolizeidirektion Koblenz und Vorstand AFCEA Bonn e.V. 14

Digitale Kompetenz und Innovation in der Luftwaffe
Generalleutnant Dr. Ansgar Rieks, Vorstand AFCEA Bonn e.V. und stellvertretender Inspekteur Luftwaffe 16

Künstliche Intelligenz in Streitkräften – ein Blick über den Zaun
Oberst a.D. Friedrich W. Benz,Vorstand AFCEA Bonn e.V. und Leiter der AFCEA Fachausstellung 18

Das Nutzererlebnis im Mittelpunkt – die Entwicklung von digitalen Produkten und Services mit analogem Nutzen
Stefan Hefter, Partner, IBM Geschäftsbereichsleiter Digitalisierung Bundeswehr 20

Das Wechselspiel der Konvergenz – eine technologische Perspektive
Magdalene Kahlert, Senior Sales Direktorin Oracle B.V. & Co. KG
Oliver Burghardt, Senior Sales Manager Oracle B.V. & Co. KG 22

2. Bundesverband der Deutschen Sicherheit- und Verteidigungsindustrie e.V.

Plattformen im Zeichen der Digitalen Konvergenz
Dr. Hans Christoph Atzpodien, Hauptgeschäftsführer des Bundesverbands
der Deutschen Sicherheits- und Verteidigungsindustrie (BDSV) e.V. 26

Sichere Inter-Netzwerk Architektur: der IP-Krypto-Backbone der Bundeswehr
Dr. Michael Sobirey, Leiter der Division Verteidigung der secunet Security Networks AG 28

D-LBO unter dem Aspekt der Digitalen Konvergenz
Horst Jonuscheit, Dipl.-Ing. Dipl.-Kfm., Vice President bei Saab Deutschland 30

Digitale Konvergenz in der Bundeswehr: Innovativ denken – effektiv transformieren
Michael Exner, Geschäftsführer der CONET Solutions GmbH 34

Cyber Security Monitoring für die Marine
Andreas Beierer, Senior Manager Sales Cyber Security, Thales Deutschland 36

Digitale Konvergenz braucht Security-by-Design
Marc Akkermann, Leiter des Hauptstadtbüros und Leiter der Geschäftsfeldentwicklung bei infodas 38

Neuronale Netze, maschinelles Lernen, kognitive Systeme – Die Zukunft hat schon begonnen
Marco Kullmann, Hauptabteilungsleiter im Geschäftsbereich Spectrum Dominance von HENSOLDT 40

Gemeinsame Wege in die Digitale Zukunft
Michael Dreher, Direktor Geschäftsbereich Verteidigung, IBM Deutschland..... 42

Weiterentwicklungsbedarfe für IT-Plattformen in der Nutzung aufgrund der fortschreitenden Digitalisierung
Dr. René Purainer, Leiter Systemintegration IT, ESG Elektroniksystem- und Logistik-GmbH 44

OHB System AG: Innovative Systemlösungen aus bewährter Hand
Thomas Jakob, Key Account Manager Verteidigung, OHB System AG 46

Disruptiver Wandel: Digitale Konvergenz minimiert Reaktionszeiten
Bernhard Jungwirth, Senior Account Manager DACH, Geospatial Technologies, Carmenta 48

Raus aus der „Gedanken-Cloud“: Lösungsansätze für die Vernetzung mobiler Systeme
Jörg Eschweiler, Head of Cybersecurity & Intelligence, Simon Brünjes, Head of Digitization LandOps,
Dr. Thomas Bierhoff, Head of Technology & Innovation, Geschäftsbereich Civil & National Security, Atos Deutschland.....50

Der Ausschuss Digitale Konvergenz
Tobias Ludwig Eder, Referent des Bundesverbands der Deutschen Sicherheits- und Verteidigungsindustrie e.V. – BDSV..... 52

3. AFCEA-Fachausstellung

AFCEA-Symposium 57

Ausstellerliste..... 58

Standplan 60

Firmenprofile 62

Impressum: Sonderheft Behörden Spiegel „AFCEA 2019“ **Redaktionelle Leitung:** Reimar Scherz, Behörden Spiegel, Telefon: 0228/97097-83 **Herausgeber** (presserechtlich verantwortlich): R. Uwe Proll, Behörden Spiegel-Gruppe **Verlegt** von der ProPress Verlagsgesellschaft mbH, Berlin/Bonn **Anzeigen:** Beatrix Lotz, Helga Woll **Herstellung:** Spree Service- und Beratungsgesellschaft mbH, Berlin **Satz und Layout:** Cornelia Liesegang, Susan Wedemeyer, Behörden Spiegel **Fotos:** Autoren, AFCEA Bonn e.V., BDSV, Behörden Spiegel Archiv **Druck:** KÖLLEN DRUCK & VERLAG GMBH, Bonn **Heftpreis:** 7,50 Euro

AFCEA Bonn e.V. – mit neuem Vorstand und neuem Jahresthema

Brigadegeneral Armin Fleischmann, Vorsitzender AFCEA Bonn e.V. und Abteilungsleiter Planung im Kommando CIR der Bundeswehr

Armin Fleischmann
Brigadegeneral *Foto: Privat*

Mit dem Jahresthema „Digitale Kompetenz und Konvergenz – im Zeitalter intelligenter Systeme“ setzt AFCEA Bonn e.V. die Logik seiner Themenschwerpunkte aus den vergangenen Jahren fort. Nach Themenfeldern rund um digitale Souveränität und Sicherheit sind digitale Kompetenz, das Zusammenwirken der Systeme und die Anwendung künstlicher Intelligenz sowie der Umgang mit ihr nun ein folgerichtiger Schritt, der ohne diese Grundlage nicht funktionieren kann.

Digitale Kompetenz erfordert ein grundlegendes Wissen über Chancen und Gefahren der Digitalisierung. AFCEA wird sich diesem Thema in 2019 stellen und mit dem Aspekt der Konvergenz das Zusammenwirken Mensch-Maschine beleuchten.

Künstliche Intelligenz (KI) hält in diesem Zusammenhang mehr und mehr Einzug in die Digitalisierung und benötigt zweckmäßige und verlässliche Massendaten als Trainingsmaterial zum Lernen. AFCEA wird sich mit der Frage beschäftigen, wie man große Mengen unverfälschte und qualitätsgesicherte Daten gewinnt und mit welchen technischen Mitteln der Austausch und das Vertrauen zwischen Dateninhabern und Datennutzern ermöglicht werden kann.

Mit der zunehmenden Verbesserung der Leistungsfähigkeit „intelligenter“ Systemen nehmen der Grad der Automatisierung und damit die Geschwindigkeit bei der Operationsführung zu. Daraus leiten sich auch nicht-technische Überlegungen ab – wo liegen moralische und rechtliche Grenzen im Umgang mit technischen Fähigkeiten, wie sieht der politische Rahmen aus? Lernende, multimodale Schnittstellen werden die Mensch-Maschine-Interaktion drastisch verändern. Mit welchen Anpassungen – von Technik an den Menschen bzw. des Menschen an Technik – muss sich die Gesellschaft zukünftig auseinandersetzen?

Das Bestreben, die Leistungsfähigkeit von KI-basierten Systemen auf der Skala von der manuellen Steuerung bis zur vollständigen Autonomie immer weiter zu verschieben, erfordert einerseits Klarheit über die zu erwartende technische Machbarkeit und andererseits Klarheit über die Verantwortung bei deren Verwendung. In diesem Heft wollen wir Beiträge zu einer breiten Betrachtungsweise leisten. Sie finden wis-

AFCEA Vorstand und Aufgaben

2019 hat AFCEA Bonn e.V. eine neue Vorstandsstruktur eingenommen. Diese ist mit folgenden Vertretern besetzt:

Vertretungsberechtigter Vorstand nach §26 BGB

Armin Fleischmann, Vorsitzender

Heiko Mühlmann, Stv. Vorsitzender und Leiter Programm

Joachim Mörsdorf, Stv. Vorsitzender und Leiter Industriebeirat

Weitere Mitglieder mit ihren Zuständigkeiten

Christian Hartrott, Geschäftsführer und Schatzmeister

Dr. Ansgar Rieks, Militärische und zivile Organisationsbereiche

Andreas Höher, BSI/BOS

Tobias Schönherr, BMI

Friedrich W. Benz, Fachausstellung

Wolfgang Taubert, CIT/CIR, Ausrüstung, Berlin, Internationales

Dr. Michael Wunder, Wissenschaft und Forschung

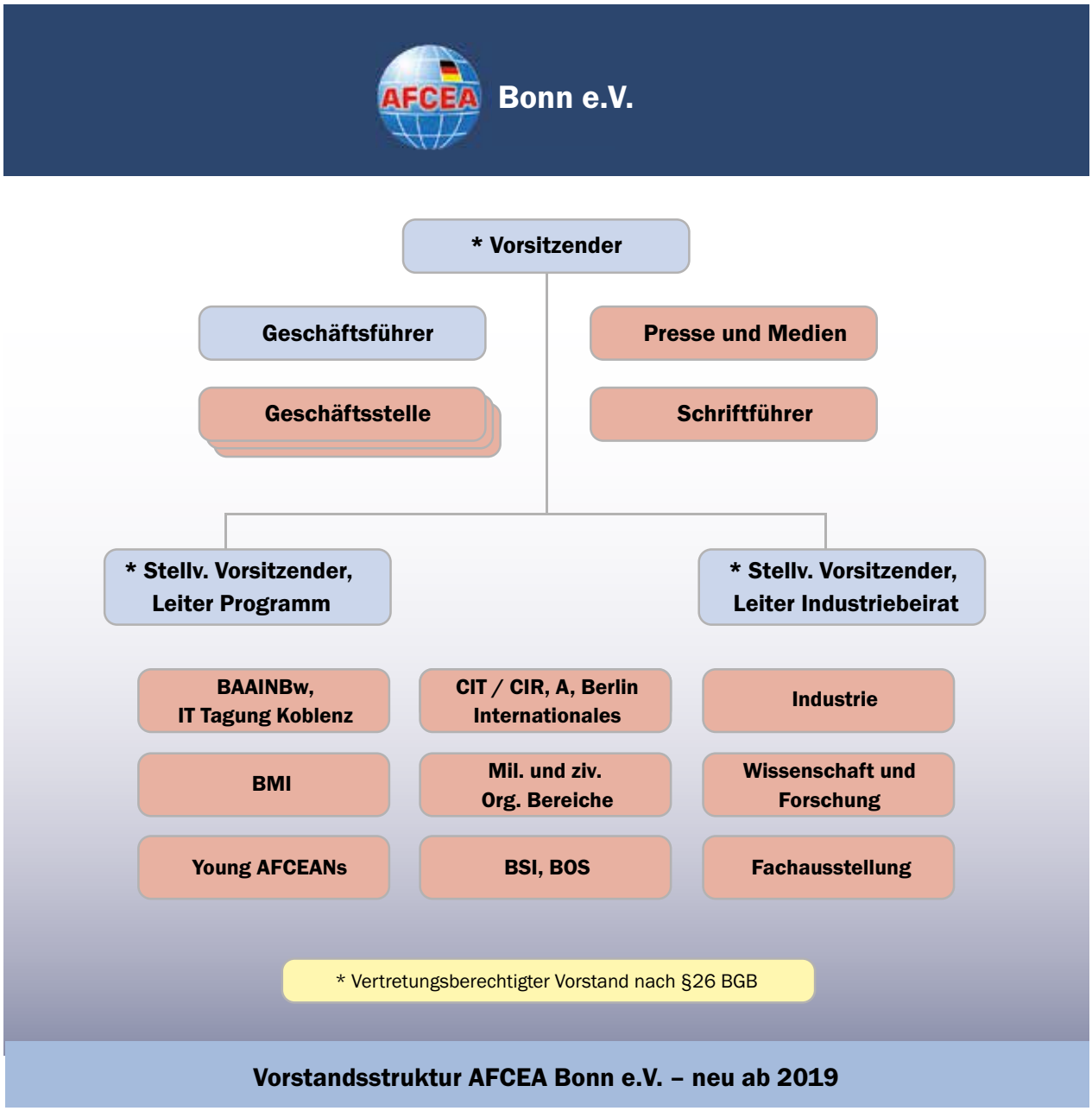
Franz Bernd Möllers, Industrie

Jochen Reinhardt, Pressesprecher

Katja Frintrop, Young AFCEANs

Roland Heckenlauer, Schriftführer

senschaftliche Überlegungen genauso wie technische Einsatzmöglichkeiten und – typisch für AFCEA als internationaler Dialogplattform – auch den Blick über den nationalen Tellerrand hinaus.
Fortsetzen werden wir diese Betrachtung und Diskussion in unserem Jahresprogramm, das sich um digitale Kompetenz und Konvergenz dreht. AFCEA Bonn e.V. will damit seinen Beitrag zur Kompetenzerweiterung leisten. AFCEA Bonn e.V. betrachtet Konvergenz als eigene DNA: Wir bringen Behörden, öffentliche Verwaltung, Wissenschaft und Industrie zusammen. Bei den aktuellen Entwicklungen ist dies wichtiger als je zuvor, denn digitale Kompetenz wird mit digitaler Konvergenz zum entscheidenden Faktor des Fortschritts und digitaler Souveränität.
Tragen Sie Ihren Teil dazu bei. Wir stehen als Plattform dafür gerne zur Verfügung.



Vorstandsstruktur AFCEA Bonn e.V. – neu ab 2019

Grafik: Behörden Spiegel-Gruppe, Quelle: AFCEA Bonn e.V.

Digitale Kompetenz und Konvergenz – im Zeitalter intelligenter Systeme

Oberst i.G. Heiko Mühlmann,
stellvertretender Vorsitzender AFCEA Bonn e.V und Referatsleiter BMVg CIT

Heiko Mühlmann
Oberst i.G. *Foto: Privat*

Die überwältigende Resonanz und das Interesse an den Themen des letzten Jahres, die sich an dem roten Faden orientierten, die digitale Zukunft intelligent, vernetzt und sicher zu gestalten, haben AFCEA Bonn e.V. als gemeinnützig agierenden Verein bestärkt, im Jahr 2019 nicht nur den technologischen Entwicklungen Rechnung zu tragen sondern mit dem Jahresthema „Digitale Kompetenz und Konvergenz – im Zeitalter intelligenter Systeme“ unsere Veranstaltungen auch weiterhin auf eine thematisch breite und zukunftsträchtige Basis zu stellen.

Die heutigen technischen Entwicklungen zur Digitalisierung gehen einher mit hohem Veränderungsdruck auf die Gesellschaft und führen zu einem grundlegenden Paradigmenwandel für die Sicherheitspolitik. Innere und äußere Sicherheit können nur noch gemeinsam wahrgenommen werden. Die vorhandene und die neu entstehende Technik lässt sich nicht in „zivil“ und „militärisch“ trennen, sondern bildet ein breites Spektrum von „Enablern“, die für die Sicherheitsvorsorge der Gesellschaft relevant sind und die geeignet sind, einem Konfliktgegner „seinen Willen aufzuzwingen“. „High-Tech“ ist schon lange keine Domäne der Militärtechnik mehr.

Insbesondere die alles durchdringenden IT-Systeme werden mit Hilfe der Künstlichen Intelligenz (KI) immer selbstständiger und leistungsfähiger – dies gilt sowohl für militärische Anwendungen als auch für Lösungen der öffentlichen Verwaltung wie auch für den gesamten zivilen Sektor.

Künstliche Intelligenz im Verständnis des maschinellen Lernens und der Verarbeitung von Massendaten (Big Data) ist bereits heute schon ein starker Treiber von Veränderungen. Mit 97 Prozent Genauigkeit bei der automatischen Bilderkennung oder 95 Prozent Genauigkeit bei der automatischen Spracherkennung ist das menschliche Vermögen bereits überflügelt worden. Es ist davon auszugehen, dass bereits ab 2025 mehr als die Hälfte von menschlichen Aufgaben automatisiert dargestellt werden können. Das heißt aber noch nicht, dass der Mensch überflüssig wird. In der Diskussion wird es zukünftig sehr darauf ankommen, zwischen Automatisierung und Autonomie zu unterscheiden.

Auch in der modernen Kriegsführung nimmt mit zunehmender Verbesserung der Leistungsfähigkeit „intelligenter“ Systeme der Grad der Automatisierung und damit die Geschwindigkeit des Wirkens zu. Doch erst vollständig autonome Waffen könnten eine Revolution in der Kriegsführung einleiten, ähnlich wie die Erfindung des Schießpulvers und der Atombombe. Vollständig autonome Waffen sind schnell und präzise, haben im Vergleich zum Menschen jedoch kein Gewissen. Daraus leiten sich nicht-technische Überlegungen ab – wo liegen moralische und rechtliche Grenzen im Umgang mit technischen Fähigkeiten, wie sieht der politische Rahmen dazu aus? Wie darf eine zukünftige Kriegsführung aussehen, in der der „Human Factor“ keine Rolle mehr spielt?

Der Umgang mit intelligenten Systemen und ihrer Autonomie verlangt eine neue Kompetenz im Umgang mit ihnen, denn lernende, multimodale Schnittstellen werden die Mensch-Maschine-Interaktion drastisch verändern. Mit welchen Anpassungen – von Technik an den Menschen bzw. des Menschen an Technik – muss sich die Gesellschaft zukünftig auseinandersetzen? Der Einsatz von Pflegerobotern steht beispielhaft für diese drastische Veränderung.

Das Bestreben, die Leistungsfähigkeit von KI-basierten Systemen auf der Skala von der manuellen Steuerung bis zur vollständigen Autonomie immer weiter zu verschieben, erfordert einerseits Klarheit über zu erwartende technische Machbarkeit und andererseits Klarheit über die Verantwortung bei deren Verwendung. Die dadurch zu führende ethische Diskussion wird den Staat als Regulativ stärker fordern als es jetzt beispielsweise in der Diskussion des autonomen Fahrens der Fall ist.

Neben den neuen Technologien und Entwicklungen gilt es natürlich auch das Feld der daraus erwachsenden (neuen) Fähigkeiten und (neuen) Risiken zu betrachten. Wird es zukünftig neben einer Sicherheit 4.0 auch eine Ethik 4.0 bzw. eine Moral 4.0 geben müssen?

Auch 2019 ist es unser Anliegen, der Rolle von AFCEA Bonn e.V. gerecht zu werden, eine breite Plattform zu bieten, den Austausch, die Diskussion mit Ihnen in diesem zukunftsweisenden Thema zu ermöglichen.

Ich darf Sie recht herzlich einladen, mit digitaler Kompetenz über digitale Konvergenz entscheidend zum Fortschritt und zur digitalen Souveränität beizutragen.

Veranstaltungen 2019 AFCEA Bonn e.V.

... nach der Fachausstellung (April – Dezember 2019)

>>> **10./11. April**
33. AFCEA Fachausstellung mit Symposium „Smarte Führungsunterstützung im 21. Jahrhundert“
10. April
Karrierestarter Forum
Young AFCEANs Gesprächsrunde für und mit jungen Führungskräften:
„Karriere in der digitalen Transformation“

>>> **15. Mai**
AFCEA Bonn e.V. zu Gast beim DHL Innovation Center
„Digital und mobil – Künstliche Intelligenz als Digitale Helfer“

>>> **5. Juni**
Gemeinsame Veranstaltung AFCEA Bonn e.V. und Kdo Luftwaffe
„Digitalisierung und KI – die DNA einer modernen Luftwaffe“

>>> **27. Juni**
Mitgliederversammlung AFCEA Bonn e.V.

>>> **3. Juli**
Gemeinsame Veranstaltung AFCEA Bonn e.V. und BWI
„Digitale Kompetenz und Konvergenz bei Bundeswehr und Bund“

>>> **5. September**
Koblenzer IT-Tagung 2019 „Digitale Kompetenz und Konvergenz – im Zeitalter intelligenter Systeme“

>>> **12. September**
Info-Veranstaltung Young AFCEANs
„Sichere Integration von intelligenten Systemen im Cyber- und Informationsraum“

>>> **18. September**
Föderales IT-System – Vernetzte Verwaltung
„Digitale Konvergenz und Kompetenz – neue Lösungswege einer modernen öffentlichen Verwaltung“.

>>> **21. Oktober**
Gemeinsame Veranstaltung AFCEA Bonn e.V. und DBwV, Berlin
„Übernehmen die Algorithmen die Führung?

>>> **8. November**
AFCEA Mittagsforum mit Fa. LUCIAD
„Fighting off the same data - Informationsgewinnung im digitalen Zeitalter“

>>> **20. November**
AFCEA Zukunfts- und Technologieforum beimFraunhofer FKIE
„Einsatz von KI zur Abwehr von Angriffen aus dem Cyber- und Informationsraum“

>>> **2. Dezember**
AFCEA Fachveranstaltung
„Gefechtsstände 4.0 – innovative und intelligente Lösungen für Command und Control“

Need for Speed – wissenschaftliche Überlegungen zu Mensch und Künstlicher Intelligenz

Dr.-Ing. Michael Wunder, Vorstand AFCEA Bonn e.V.,
Abteilungsleiter „Informationstechnik für Führungssysteme“, Fraunhofer FKIE

Dr.-Ing. Michael Wunder

Foto: Privat

Um die Jahrtausendwende warteten wir noch bereitwillig 10 Sekunden, bis sich eine Internetseite öffnete. Heute klicken wir uns spätestens nach 2 Sekunden woanders hin. Warten nervt. Wenn wir im Onlineshop auf „Kaufen“ klicken, erwarten wir eine Premiumlieferung am Folgetag. Unser Alltag hat eine hohe Taktfrequenz. Auch politische Entscheidungen sind immer schneller getaktet: In immer kürzeren Abständen werden aktuelle Entscheidungen von der nächsten hinweggefegt. Rücktritt vom Amt … nee, doch weitermachen. Staatssekretär … nee, vorzeitiger Ruhestand. Sanktionen … nee, doch nicht ganz so. Brexit … naja. Alles scheint möglich und zum Teil wenig durchdacht. Gleichzeitig oder genau deswegen freut sich eine Gesellschaft über klare Ansagen und Machtworte und nimmt dafür immer öfter in Kauf, dass sie wenig begründet sind und Fakten fehlen. Der Drang nach plakativen Erklärungen wird leicht und schnell befriedigt. Wenige Sekunden müssen für den Konsum von Meldungen auf dem Handy ausreichen. Schnell, schnell!

Ob man es gut findet oder nicht, moderne IT-Technik treibt uns und wie in einer Spirale, streben wir immer schneller nach Neuem. Beispielsweise hat die Menge an Emails, Fachberichten und Veröffentlichungen derart zugenommen, dass wir inzwischen Computer zum Auswerten und Verdichten einsetzen. Das machen wir übrigens auch zum Generieren von Texten, was die Spirale beschleunigt.

Überhaupt wird nicht alles nur schneller. Auch die zweite Ableitung ist positiv. Künstliche Intelligenz, Internet of Things, Industrie 4.0 und Big Data machen es möglich. Die enorme Faszination die von der IT ausgeht, bringt es offensichtlich mit sich, dass Gesellschaften die Begleiterscheinungen wie Rastlosigkeit, Sprunghaftigkeit und zum Teil auch unscharfe Fakten akzeptieren oder zumindest nicht als Belastung empfinden. Wir leben im Turbozeitalter.

Hyperwar

Insofern passt die Vorstellung, wie man sich in der NATO den Krieg der Zukunft vorstellt, zu der Situation in der zivilen Welt. Mit dem Begriff „Hyperwar“ wird (wie schon einmal im 2.Weltkrieg) eine neuartige Ausprägung von Krieg beschrieben. Heutzutage wird darunter die beispiellose Geschwindigkeit in nebenläufigen und aufeinander abgestimmten Aktionen verstanden, die durch KI und Cognitive Computing möglich werden soll (**https://fortunascorner.com/2017/07/10/on-hyper-war-by-gen-ret-john-allenusmc-amir-hussain**). Nicht mehr physische Stärke und Informationsüberlegenheit allein, sondern insbesondere die Schnelligkeit bei der Entscheidungsfindung ist für den Konfliktablauf entscheidend. Offensichtlich ist das beim Krieg der einzige Faktor, bei dem eine physikalische oder natürliche Begrenzung noch keine Rolle spielt und man das enorme Potenzial für militärische Überlegenheit ausschöpfen will. (Beim Hochfrequenzhandel an Börsen ist dagegen bald schon die Grenze der Lichtgeschwindigkeit erreicht: **https://www.spektrum.de/kolumne/boersenhandel-in-lichtgeschwindigkeit/1331927**.) Zur Erreichung der hohen Geschwindigkeit ist es zweckmäßig, Computer für möglichst viele algorithmisierbare Prozesse einzusetzen. Menschliche Ressourcen sollen von diesen Prozessen entlastet und insbesondere dort eingesetzt werden, wo Computer (noch) versagen.

Generell dürfte die wesentliche Hoffnung bei der Nutzung von KI die Minimierung der Dauer bei der Entscheidungsvorbereitung sein, also beim automatisierten Finden von Mustern in Massendaten, beim Vergleichen von Daten, beim Inbeziehungsetzen verteilter Informationen und beim Schlussfolgern aus extrahierten Fakten.

Der russische Präsident Wladimir Putin hat schon im Herbst 2017 zum Ausdruck gebracht, dass derjenige, der bei KI-Technologien führt, die Welt beherrscht. Er hat zwar auch die schwer vorherzusagenden Bedrohungen angesprochen und wünscht sich, dass niemand eine Monopolstellung auf diesem Gebiet erreicht. Aber angesichts der zunehmenden Aggressivität zwischen den Weltmächten muss man annehmen, dass KI auch in Russland bei der Rüstung eine wesentliche Rolle spielt und massiv vorangetrieben wird. Die Annexion der Krim und die begleitenden Informationskampagnen, zeigen, dass der Einsatz ausgefeilter IT-Techniken bei hybriden Kriegen zum Handwerk gehört.

KI ist (bereits zum dritten Mal) ein Hype mit vielen verschiedenen, marktgängigen Interpretationen. Bei der großen Bandbreite zwischen starker und pragmatischer (unsinnigerweise auch „schwacher“ genannt) KI gibt es enorme Unterschiede im Reifegrad. Vieles ist Science Fiction und bleibt es wohl auch. Ob es gelingt, den „Man in the Loop“ durch KI zu ersetzen, weil der Mensch zu langsam für den Hyperwar ist, dürfte eher nicht an moralischen Befindlichkeiten liegen. Über Jahrmillionen konnten Informationswahrnehmung, Informationsverarbeitung, Entscheidungsfindung und auch das Energiemanagement in einem höchst integrierten Gesamtsystem

optimiert werden. Ob es auf absehbare Zeit nachgebildet und ersetzt werden kann, ist zweifelhaft – wir kennen ja selbst nicht alle Details von uns. Trotz langer Zyklen bei Wehrmaterial scheint es daher sinnvoller, sich auf pragmatische KI zu konzentrieren und für erkennbare operative Bedarfe Lösungen entwickeln, als für nicht-deterministische KI-Verfahren raffinierte Anwendungen zu suchen.

Beispiel Tumor-Erkennung

Nehmen wir ein Beispiel aus der Gesundheitsbranche: In der Radiologie kann KI bei der Erkennung von Tumoren eingesetzt werden. Selbstverständlich werden KI-basierte Systeme, die mit massenhaften annotierten Daten über erkannte Tumore trainiert werden und damit das Erkennen von Tumoren erlernen, zur Unterstützung der Ärzte zukünftig immer öfter eingesetzt. Aber das „komische Bauchgefühl“ – so die Einschätzung von Fachärzten – das sie hin und wieder beim Betrachten von Aufnahmen umschleicht und das im Konzert von optischen Eindrücken und ihren Erfahrungen aus anderen Zusammenhängen entsteht, lässt sich nach ihrer Ansicht nicht in ein Modell überführen. Diese Haltung ist einerseits beruhigend: Der Einsatz von KI ist wichtig, damit können Entscheidungsvorschläge schnell vorliegen, aber das letzte Wort hat der Facharzt. Andererseits dürfen wir Bauchgefühle nicht mystifizieren. Und KI wird sich ja weiterentwickeln.

Methoden zur robusten Sprechererkennung

Kevin Wilkinghoff,
Fraunhofer FKIE, Abteilung KOM, AFCEA Studienpreisträger 2018

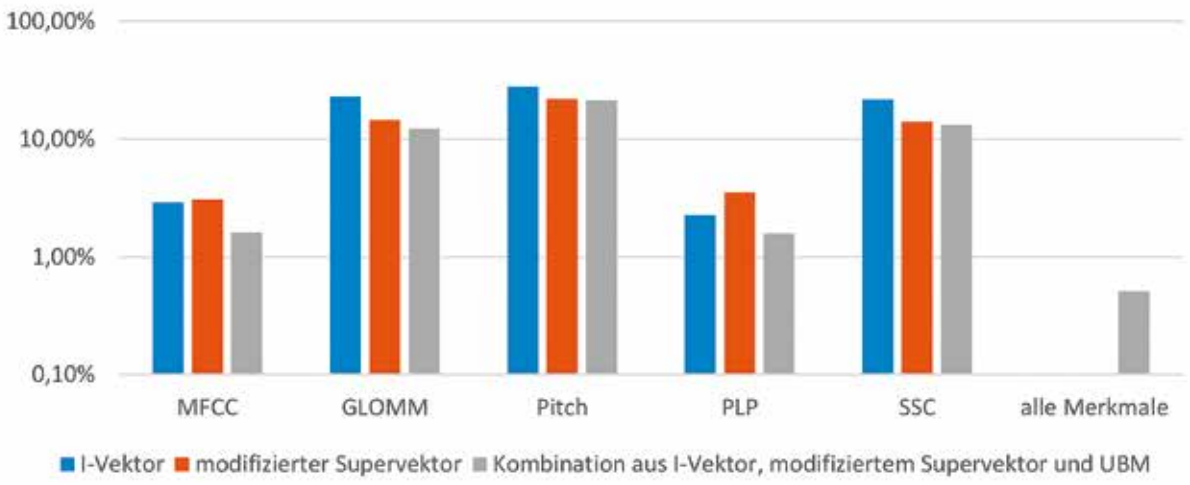
Kevin Wilkinghoff

Foto: Privat

Allein aufgrund ihrer schieren Masse sind die in der signalbasierten Aufklärung anfallenden Sprachaufzeichnungen nicht mehr manuell zu bewältigen. Gleichzeitig erschweren die teilweise extrem schlechten Signalqualitäten sowie die sich meist von der Muttersprache des Bearbeiters unterscheidenden Zielsprachen die effektive Handhabung dieser Datenmenge erheblich. In der Konsequenz ist es daher nur wenigen gut ausgebildeten Spezialisten möglich, Sprachaufzeichnungen effektiv zu erschließen. Für die Aufklärung ist es somit unerlässlich, die Unterstützung intelligenter Algorithmen zu suchen. Ein wichtiger Aspekt der Auswertungen von Sprachaufzeichnungen ist, zu einem möglichst frühen Zeitpunkt der Bearbeitung zu ermitteln, welche Sprecher an welcher Stelle in einem Signal vorkommen. Dieses Problem der automatisierten Erkennung von Sprechern steht im Mittelpunkt dieses Beitrags. Ziel soll eine sogenannte textunabhängige Sprechererkennung sein, das heißt eine Erkennung anhand einer beliebigen, vorab unbekannten, gesprochenen Wortfolge.

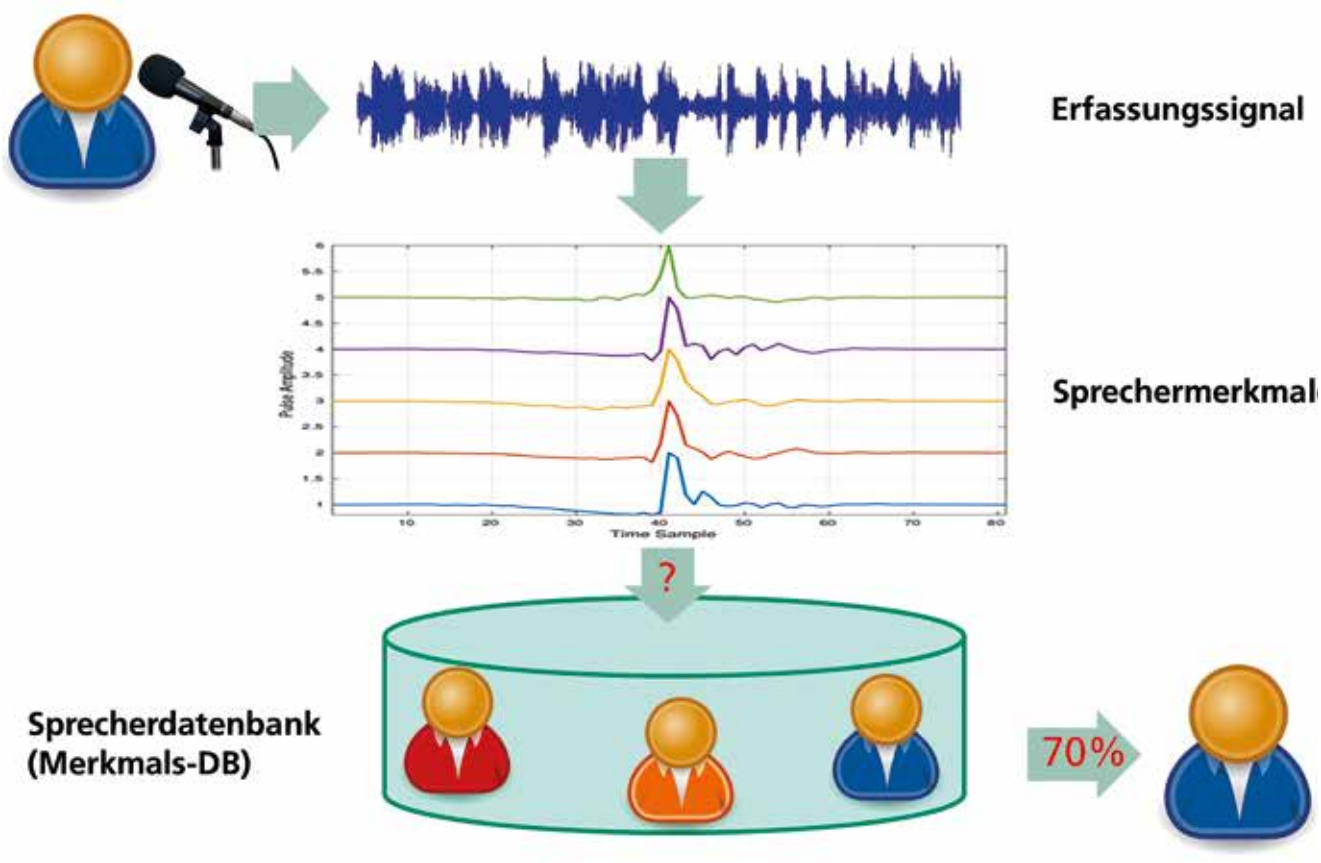
Ausgehend von aus der wissenschaftlichen Literatur bekannten „klassischen“ Methoden der Sprechererkennung erarbeiten wir verschiedene Ansätze zur Verbesserung der Erkennung von Sprechern in verrauschten Audioaufzeichnungen. Einer dieser Ansätze basiert auf der Hinzunahme weiterer charakteristischer Sprechermerkmale, die ergänzend zu den klassischen Mel-Frequency-Cepstral-Coefficients (MFCCs) aus den rohen Audiosignalen gewonnen werden. Die zusätzlichen Merkmale sind die wahrgenommene Tonhöhe (Pitch), die eigens am Fraunhofer FKIE entwickelten Glottal-Mixture-Model (GLOMM)-Merkmale sowie zwei weitere aus der Literatur bekannte Merkmalstypen, Spectral Subband Centroids (SCCs) und Perceptual Linear Prediction (PLPs). Der Verwendung verschiedener Merkmalsklassen liegt die Annahme zugrunde, dass sich die unterschiedlichen Merkmale komplementieren und somit die Erkennungsleistung verbessert wird.

Der zweite wesentliche Ansatz zur Verbesserung der Sprechererkennung besteht in der Kombination der Resultate mehrerer statistischer Modelle zur Sprecherklassifikation. Die Annahme bei der Verwendung eines solchen statistischen Modells ist, dass die aus einer Audioaufzeichnung zu einem bestimmten Sprecher extrahierten Signalmerkmale eine Punktwolke in einem hochdimensionalen Raum darstellt, deren Gestalt mittels weniger Modellparameter charakterisiert werden kann. Ein klassisches Beispiel hierfür ist das Modell, dass solche Punktwolken durch eine Kombination nur weniger (hochdimensionaler) Gaußdichten approximiert werden können. Man spricht von einem Gauß‘schen Mixturmodell (GMM). Die Modellparameter sind hierbei Mittelwerte und Form (repräsentiert vermöge Kovarianzmatrizen) dieser Gaußdichten. Wird nun jeder Sprecher durch ein solches GMM charakterisiert und unterscheiden sich die GMMs aller untersuchter Sprecher, so ist eine GMM-basierte Klassifikation dadurch möglich, dass zu einer konkreten Audioaufzeichnung derjenige Sprecher ausgegeben wird, dessen GMM am besten zu den aus der Aufzeichnung extrahierten Merkmalen „passt“. In der Praxis sind die



Übersicht zur Sprechererkennung

Grafik: Privat



Experimentelle Ergebnisse durch Auswertung mit den Korpus NTIMIT. Dargestellt sind die Erkennungsfehlerraten wobei in jedem Experiment jeweils 10000-mal ein unbekanntes Sprachsignal einem von 10 zufällig gezogenen Sprechern korrekt zugeordnet werden musste.

Grafik: Privat

extrahierten Merkmale allerdings in der Rohform nicht optimal für die Sprecherklassifikation geeignet, da sie einerseits eine sehr hohe Dimension besitzen und andererseits noch durch Komponenten nichtsprachlicher Sekundärsignale (beispielsweise Kanalrauschen oder Hintergrundgeräusche) beeinflusst sind. In diesem Kontext wurden in der Literatur zahlreiche Mechanismen sowohl zur Dimensionsreduktion als auch zur (impliziten) Separierung des Sprachanteils vorgeschlagen. In diesem Beitrag wird die gewinnbringende Kombination verschiedener solcher Mechanismen vorgestellt, wobei zusätzlich eine modifizierte Variante sogenannter Supervektoren zur Sprechercharakterisierung vorgeschlagen wird.

Für den Schritt der Sprecherklassifikation resultiert die Kombination der verschiedenen Signalmerkmale (hier: 5) und der verschiedenen statistischen Modelle (hier: 3) in einer hohen Anzahl von Einzelklassifikationen (hier: 3*5 = 15), sodass sich die Frage nach einer optimalen Kombination der Einzelklassifikationen zu einem Gesamtergebnis stellt. Da eine Bestimmung dieser sogenannten Score-Fusion-Parameter durch Ausprobieren eine nicht handhabbare algorithmische Komplexität besitzt, wird dieser Schritt durch ein hierfür speziell entwickeltes, zweistufiges neuronales Netz vollzogen.

Der Vergleich der hier vorgestellten Methoden mit klassischen Ansätzen zur Sprecherklassifikation erfolgte zunächst anhand öffentlich verfügbarer Testdaten. Hierzu wurden zwei aus verrauschten Sprachdaten bestehende Korpora (NTIMIT und Switchboard) herangezogen, bei denen es sich um Telefoniesprache handelt. Es konnte dabei eine deutliche Leistungssteigerung unter Verwendung der neuen Ansätze nachgewiesen werden (siehe Abbildung 2). Durch die Integration der hier vorgestellten Sprechererkennungstechnologie in das am Fraunhofer FKIE entwickelte Funktionsmuster SCALA (Single Channel Analyzer) ist eine gezielte Evaluation der Methoden gerade unter Einbeziehung der Nutzerseite möglich. So wurden bereits erste positive Ergebnisse zur Sprecherklassifikation für den Fall realer Daten erzielt und die Nutzbarkeit für Einsatzszenarien zusammen mit dem militärischen Anwender diskutiert.

Digitale Kompetenz der Behörden mit Ordnungs- und Sicherheitsaufgaben im Zeitalter intelligenter Systeme

Tobias Schönherr, Dipl.-Ing., Polizeidirektor, Stabsbereichsleiter Technik und Logistik, Bundespolizeidirektion Koblenz und Vorstand AFCEA Bonn e.V.

Tobias Schönherr

Foto: Privat

Mit dem Jahresthema 2019 stellt der gemeinnützig agierende Verein AFCEA Bonn e.V. seine Veranstaltungen in diesem Jahr auf eine breite und auf die Zukunft gerichtete Basis. IT-Systeme werden immer selbstständiger und intelligenter – dies gilt neben den militärischen Anwendungen immer auch für Lösungen in der öffentlichen Verwaltung. Als Angehöriger der Bundespolizei möchte ich an dieser Stelle einen Blick in die digitale Zukunft der Polizei werfen und dabei insbesondere die Kommunikation betrachten.

Polizisten im Dienst „auf der Straße“, wie es so schön heißt, kommunizieren mittels Funkgeräten, die heute flächendeckend digital funktionieren. Also Sprechknopf drücken und los, die Einsatzzentralen und die Kolleginnen und Kollegen sind im Bilde, Aufträge, Fahndungsabfragen, Lageinformationen … alles geht. Die wenigen Funklöcher kennt man und greift dann zum Mobiltelefon … geht auch. Der Ausbau des Digitalfunks für alle BOS, also auch Rettungsdienste und Feuerwehren, ist bis auf ein paar „Baustellen“ etwa in unterirdischen Bereichen von Bahnanlagen, abgeschlossen. Nun ist es ja nicht so, dass die Möglichkeiten der Digitalisierten Welt, die jeder von uns in seinem privaten Umfeld nutzt, nicht auch für den Polizisten sinnvoll wären. Also: Messengerdienste, Videoübertragung, Fahndungsdatenabfragen, Anlegen von polizeilichen Vorgängen in einer Applikation und dies alles auf einem mobilen Endgerät ist die neue Welt. Und sie funktioniert auch schon oder dieses Zeitalter beginnt gerade. Bundespolizisten können mit ihrem dienstlichen Smartphone Ausweisdokumente per NFC lesen und, natürlich nur bei Vorliegen der rechtlichen Voraussetzungen, eine direkte Fahndungsdatenbankabfrage starten. Wenn das nun mit einem einzigen Gerät funktionieren könnte … kann das Digitalfunkgerät aber nicht, Datenübertragung geht nur mit ein paar Kilobyte. Also, liebe Leser, nicht wundern über die Fülle an Ausrüstungsgegenständen, die ein Polizist so an sich trägt. Ein einzelnes Gerät, welches alles bisher beschriebene kann, gibt es bisher nur auf der Enterprise. Dazu kommt, dass Polizei und Behörden und Organisationen mit Sicherheitsaufgaben (BOS) im selben Dilemma stecken, wie ein StartUp auf einer Wiese im Westerwald oder ein Großunternehmen mit weltweiten Dependancen: Big Data benötigen dicke Datenleitungen, am liebsten natürlich über Funkwellen. Aber auch Polizeidienststellen, wie StartUps im Westerwald, hängen am deutschen Kupfer-manchmal-Glasfaserkabel-Netz. Käpt´n Kirk-Scheuer kennt seine Aufgabe.

Nun will ich an dieser Stelle nicht lamentieren und immer nur anderen die Verantwortung zuschieben. Besser machen, ist die Devise. Wie wäre es denn damit? Die Bundesrepublik nutzt die im Frühjahr 2019 anstehenden Frequenzversteigerungen für die kommende 5G-Technologie, um ein zukünftiges 5G-BOS-Datennetz über die Bundesrepublik zu legen, welches das „zivile Netz“ nutzt. Gleichwohl aber auch eine Nutzungspriorität für BOS ermöglicht, vielleicht ergänzt durch mobil einsetzbare 5G-Funkzellen der BOS, die beispielsweise bei Massenveranstaltungen oder auch in Katastrophenlagen die sogenannte Besondere Aufbauorganisation der Polizei durch Datenkommunikationsverbindungen unterstützt. Es werden wieder Milliarden von Euro bei den Frequenzversteigerungen fließen, weitere beim Aufbau des 5G-Netzes. Aber auch das derzeitige Digitalfunknetz hat viel Geld gekostet. Es überträgt, wie schon geschrieben, ein paar Kilobyte. Digitale Kompetenz heißt auch, die Entwicklungszyklen der Informationstechnologie so vorher zu sehen, dass die Polizei nach ihren neuesten Beschaffungsmaßnahmen nicht mit Pferden Verbrecher jagt, die Tesla fahren.

Wenn man nun noch bedenkt, dass Digitale Kompetenz auch heißt, dass mehr „gehen soll“ als das System gerade kann, dann sind wir bei der sogenannten „Mesh-Fähigkeit“ von Kommunikationsgeräten angekommen. Es geht dabei darum, unabhängig von funktionierenden Zellen die in einem begrenzten Gebiet eingesetzten Geräte der BOS so miteinander zu verbinden, dass Kommunikation in diesem intelligenten Netzwerk möglich ist, auch wenn die Funkzellen nicht mehr funktionieren. Das kann der heutige Digitalfunk zwar auch, nur scheitert eine Verbindung der Einsatzkräfte verschiedener Behörden oft daran, dass die Einzelgeräte nur eine begrenzte Zahl vorprogrammierter Nutzer zulassen. Und da gibt es mit BKA, Bundespolizei und Landespolizei gleich 18 verschiedene Polizeibehörden.

Wenn uns das dann alles gelungen ist, kommen wir zur künstlichen Intelligenz. Oder wir sprechen besser von maschinellem Lernen. Dazu verknüpfen wir die Daten aus Videoüberwachungssystemen mit Gesichts- und Verhaltenserkennung, führen einen Datenabgleich mit all unseren guten und verlässlichen Massendaten aus den Datenbanken der Polizeifahndung, der Einwohnermeldeämter, der KFZ-Zulassung, von Europol, Schengen, Interpol und so weiter durch und erhalten vom künstlich intelligenten Computer einen Haftbefehl oder die Direktabbuchung noch fälliger Ordnungsgelder

Hubschrauber der Bundespolizei im Küstenwachtverbund *Foto: Bundespolizei*

von den Privatkonten säumiger Zahler. Ich behaupte jetzt einfach mal: Das wollen wir nicht. Wir als Bürger Deutschlands. Trotzdem wird sich unsere Gesellschaft damit beschäftigen, mit dem autonomen Fahren tun wir es ja schon. Die Problemfelder sind die gleichen.

An dieser Stelle beende ich meine Betrachtungen zur Kommunikationstechnologie der BOS in unserem digitaler werdenden Zeitalter, aber natürlich nicht die Diskussion dazu. Sie ist in vollem Gange.

AFCEA schreibt dazu im Aufmacher für das Jahresthema 2019: „Der Umgang mit intelligenten Systemen und ihrer Autonomie verlangen eine neue Kompetenz im Umgang mit ihnen. Nicht zuletzt ist bis heute unklar, wer die Verantwortung bei Entscheidungen durch intelligente Systeme trägt. Digitale Kompetenz wird mit digitaler Konvergenz damit zum entscheidenden Faktor des Fortschritts und digitaler Souveränität."

Lassen Sie uns das in diesem Jahr 2019 diskutieren und am besten auch in Lösungen überführen.

BDSV und AFCEA Bonn vereinbaren Kooperation

Der Bundesverband der Deutschen Sicherheits- und Verteidigungsindustrie e.V. (BDSV) und AFCEA Bonn e.V. werden künftig zusammenarbeiten und so den Austausch in der Community stärken. Der BDSV ist damit die jüngste Partnerorganisation der neutralen Dialogplattform AFCEA. Zu den bisherigen Partnern gehören beispielsweise der Deutsche Bundeswehrverband (DBwV), der IT-Brancherverband Bitkom und verschiedene Verlage. AFCEA Bonn e.V., das Anwenderforum für Fernmeldetechnik, Computer, Elektronik und Automatisierung, ist ein gemeinnützig tätiger Verein ohne kommerzielle Interessen mit persönlichen und Firmenmitgliedern. Der Verein geht auf die Initiative von Angehörigen der Streitkräfte zurück, die den Austausch rund um Informations- und Kommunikationstechnik (ITK) im Verteidigungs- und Sicherheitsbereich fördern wollten. AFCEA Bonn e.V. bietet heute Fachleuten und allgemein Interessierten aus den Bereichen Verteidigung, Innere Sicherheit, öffentliche Verwaltung sowie Lehre und Forschung eine anerkannte, auch international vernetzte Informationsplattform für alle Fragen moderner ITK.

Digitale Kompetenz und Innovation in der Luftwaffe

Generalleutnant Dr. Ansgar Rieks,
Vorstand AFCEA Bonn e.V. und stellvertretender Inspekteur Luftwaffe

Dr. Ansgar Rieks
Generalleutnant *Foto: Privat*

Das Schlagwort „Digitalisierung“ prägt seit einigen Jahren in nahezu allen Lebensbereichen die öffentliche, privatwirtschaftliche und politische Diskussion. Neben einem Fokus auf die damit verbundenen Chancen und annähernd unendlich erscheinenden Innovationen, schwingt in der öffentlichen Diskussion immer die Unsicherheit ob der Risiken mit – sei es die Verletzung der Privatsphäre oder die Beeinflussung des „digitalen“ Raumes. Im Militär, und speziell in den technikorientierten Teilstreitkräften, sind diese Entwicklungen aus den gleichen Blickwinkeln aufmerksam zu verfolgen. Heutzutage besteht die Herausforderung insbesondere darin, von der Entwicklungs- und Innovationsgeschwindigkeit in der „zivilen“ Welt zu profitieren, Kompetenz aufzubauen und zu erhalten sowie bei Innovationen nicht nur den Anschluss zu halten, sondern diese auch für das eigene Fähigkeitsprofil zielgerichtet zu nutzen.

Die Luftwaffe – digital von Anfang an

Für die Luftwaffe war die Nutzung digitaler Technologien von Beginn an ein wesentliches Element in der Führung, beim Einsatz, im Betrieb und in der Ausbildung. Dabei reichte das Spektrum von der Nutzung in Waffensystemen bis hin zu luftwaffenweiten Führungssystemen.
Anwendungen, die wir erst in den letzten Jahren im zivilen Umfeld sehen, waren in Luftfahrzeugen manchmal schon lange Stand der Technik, wie beispielsweise digitale „Bordrechner“ oder Headup-Displays, welche wir in Kraftfahrzeugen derzeit erst vereinzelt unter dem Schlagwort „Augmented Reality“ sehen.
Mit dem Automatischen Führungs- und Fernmeldenetz der Luftwaffe sowie dessen späterer Erweiterung um das sog. Datentransportnetz waren wir auf der Höhe der damaligen Zeit und ein Vorreiter für die digitale Konvergenz von der analogen zur digitalen Sprachübermittlung. Ein digitales Luftlagebild, Automatisierung oder digitale taktische Datenverbindungen gehören schon lange zur DNA der Einsatzluftwaffe.
Für die Nutzung unserer Waffen- und Einsatzführungssysteme war damit schon sehr früh deutlich, dass eine Beurteilungs-, Forderungs- und Entscheidungs- sowie in entscheidenden Bereichen auch operationelle Weiterentwicklungsfähigkeit zu etablieren ist. Seinerzeit wurde dies vor allem mit den Programmierzentren der Luftwaffe für Führungssysteme in Erndtebrück und für fliegende Waffensysteme in Landsberg am Lech in die Tat umgesetzt. Hier waren die Programmierer der Luftwaffe konzentriert, um auf Augenhöhe mit der Industrie unsere Systeme zu betreuen.

Innovationsfähigkeit in der Luftwaffe

Mit einem weiteren Vordringen digitaler Systeme in die Streitkräfte und dem damit verbunden exponentiellen Wachstum von Softwareumfang und Komplexität können Streitkräfte im Personal- und Expertiseaufwuchs heutzutage oft nur schwerlich mithalten. Daher gilt es, sich auf Kernfähigkeiten zu konzentrieren und die eigene digitale, auf dem genannten Fundament gewachsene Kompetenz zielgerichtet zu nutzen.
Um das abstrakte Schlagwort „Digitalisierung“ greifbar zu machen, haben wir digitale Aktivitäten in der Luftwaffe mit einem Leuchtturmcharakter identifiziert, welche die Digitalisierung der Luftwaffe derzeit und in der absehbaren Zukunft wesentlich prägen. Bei der Auswahl wurde auf die Wirkung auf den Kernauftrag der Luftwaffe, ein weites Spektrum von Realisierungsmöglichkeiten, sowie das Potenzial zur Einbindung anderer Organisationsbereiche zur Multinationalisierung besonderer Wert gelegt. Diese fünf „Leuchtturmprojekte“ werden durch zahlreiche weitere Digitalisierungsaktivitäten der Luftwaffe ergänzt.
Mit dem **Simulationsverbund** verfolgt die Luftwaffe das Ziel, einzelne Missionen, bis hin zu komplexen Luftkriegsoperationen, auch multinational und organisationsbereichsübergreifend, realitätsnah virtuell abbilden zu können. Der Verbund leistet damit einen Beitrag zur Erweiterung der taktischen Fort- und Weiterbildungsmöglichkeiten sowie zur Verbesserung der Einsatzvorbereitung.
In einem ersten Schritt wurde mit der Simulationszentrale der Luftwaffe das zentrale Element zum Management dieses virtuellen Übungsraumes geschaffen. In den nächsten Schritten werden die bestehenden Simulatoren ausgewählter Waffensysteme sukzessive für die Verbundsimulation befähigt.
Mit dem Projekt **Luftgestützte Wirkung im Elektromagnetischen**

Teilnehmer der Ausbildung nutzen die Software COMMAND zur Visualisierung von Luftoperationen. *Foto: Luftwaffe, OSLw*

Der stellvertretende Schulkommandeur und Leiter Schulstab der OSLw, Oberst Lutz Mühlhöfer bei der Begrüßung der Teilnehmer Ausbildung „COMMAND“. *Foto: Luftwaffe, OSLw*

Blick in den Simulator für die Eurofighter Ausbildung -mit Heads Up Display- des Taktischen Luftwaffengeschwaders 73.

Foto: Bundeswehr, Bienert

Spektrum geht es um den Schutz und den Erhalt der Durchsetzungsfähigkeit fliegender Waffensysteme unter Bedrohung, und damit um eine Kernfähigkeit zur Wirkung im „Cyberraum“, von der auch alle anderen militärischen Organisationsbereiche profitieren können

Technologiegestützte Ausbildung setzt unter anderem auf Virtual- und Augmented Reality, um die allgemeinmilitärische und militärfachliche Ausbildung zu modernisieren, eine zeitliche Entlastung der Waffensysteme zu erreichen und orts- und zeitunabhängiges Lernen zu ermöglichen. Ferner trägt sie zur deutlichen Verbesserung der Ausbildung durch stärkere Praxisnähe bei.

Die **Desktop-Applikation zur Darstellung und Analyse von Luftoperationen** nutzt verfügbare Simulationstechnologie zur Visualisierung der komplexen Zusammenhänge im Verbund von Führung, Aufklärung, Wirkung und Unterstützung. Um das Potenzial dieser Software zu evaluieren, wurden in der Luftwaffe Multiplikatoren mit einer breiten technischen und operationellen Expertise ausgebildet. Diese evaluieren und testen diese Software derzeit auf die Anwendbarkeit in der Luftwaffe. Hier sind Anwendungsfälle in den Bereichen Ausbildungsunterstützung und Wargaming, militärisches Nachrichtenwesen, Weiterentwicklung und zur Nutzungsunterstützung denkbar.

Ich greife diesen Leuchtturm hier vor allem deshalb heraus, weil er den in der Luftwaffe vorhandenen innovativen Charakter deutlich macht, der im Synergiefeld zwischen technischer Expertise und operationellem Wissen innovative Lösungen und Anwendungsfälle produzieren kann. Die erste Idee zur Nutzung der Software entstand an der Offizierschule der Luftwaffe in Fürstenfeldbruck für die Offizierausbildung und wurde dann im Kommando Luftwaffe weiterentwickelt. Die Evaluierung verspricht schon jetzt zahlreiche Anwendungsfälle für die Luftwaffe.

Mit der **Nutzung von „Künstlicher Intelligenz“ bei der Planung von Luftoperationen** wollen wir im Bereich der Planung und Ausbildung erste Erfahrung mit “KI“ gewinnen. Am Ende sollen Entscheidungsabläufe beschleunigt und Personal, zum Beispiel bei Übungen, unterstützt werden. Denn eines liegt auf der Hand: Ein tradierter, komplexer und zeitlich starrer Planungszyklus macht es in einem Konflikt mit einem modern ausgestatten Gegner immer schwer, die Führungsüberlegenheit und schließlich die Luftüberlegenheit zu erringen. Dazu führt die Luftwaffe eine Studie unter Einbindung der Französischen Luftwaffe und der NATO durch. Diese Studie wird dazu den gegenwärtigen Planungsprozess des Joint Force Air Component Headquarters als multinationaler Einsatzgliederung des Zentrum Luftoperationen in Kalkar untersuchen, die Ausbildung des Personals und die Betriebsabläufe analysieren. Dazu wird ein Expertensystem und maschinelles Lernen zum Einsatz kommen. Alle zugehörigen Fragen zu KI werden dabei einbezogen.

Digitale Kompetenz als Grundlage

Gerade bei dem Themenkomplex „Nutzung von Künstlicher Intelligenz“ bewegen wir uns an einer Schnittstelle, an der technologische und operationelle mit ethischen, politischen und juristischen Fragestellungen in Einklang gebracht werden müssen.

Beispielhaft weise ich hier auf die Problematik der Nachvollziehbarkeit und damit auch der Verantwortung hin: Wie steht es um die Nachvollziehbarkeit des Gelernten in einem neuronalen Netz? Wie gehen wir mit der Zulassungsfähigkeit von nicht-deterministischen und damit per se nicht vorhersagbaren Abläufen um? Wieviel Künstliche Intelligenz und Autonomie ist hinreichend? Wieviel ist notwendig? Wie ethisch kann Künstliche Intelligenz handeln? Welche Entscheidungen und wieviel Kontrolle darf der Mensch nicht aus der Hand geben? Aber auch: „Welche Exzellenz soll die KI erreichen, und welche Fähigkeitsgrade sind dazu erforderlich?“

Für diese Fragen müssen am Ende konkrete Konzepte für spezifischen militärischen Nutzen diskutiert und entwickelt werden. Ein Pionier der Erforschung künstlicher Intelligenz, Joseph Weizenbaum sagte dazu: „Ich plädiere für den rationalen Einsatz der Naturwissenschaft und Technik, nicht für deren Mystifikation und erst recht nicht für deren Preisgabe. Ich fordere die Einführung eines ethischen Denkens in die naturwissenschaftliche Planung. Ich bekämpfe den Imperialismus der instrumentellen Vernunft, nicht die Vernunft an sich“.

Für diese Rationalität benötigen wir die klügsten Köpfe und die digitalen Kompetenzen unserer Frauen und Männer im Team Luftwaffe. Daher steht nach wie vor die gründliche Ausbildung des Menschen im Vordergrund und ist Grundlage für die innovative, sichere und verantwortungsvolle Nutzung digitaler Technologien.

Digitalisierung wird „der“ Treiber für unsere moderne Luftwaffe sein!

Künstliche Intelligenz in Streitkräften – ein Blick über den Zaun

Oberst a.D. Friedrich W. Benz,
Vorstand AFCEA Bonn e.V. und Leiter der AFCEA Fachausstellung

Friedrich W. Benz
Oberst a.D. *Foto: Privat*

Auch wenn im militärischen Umfeld beim Thema Künstliche Intelligenz und Streitkräfte oft sehr schnell eine Verengung und Projektion auf autonome Killerroboter stattfindet und es eine allgemeingültige Definition dessen, was Künstliche Intelligenz in den Streitkräften ausmacht, noch nicht gibt, ist allgemeiner Konsens, dass die KI die Kriegsführung im 21. Jahrhundert revolutionieren wird. Auch wenn das Potential von KI noch nicht gänzlich absehbar ist, vergleicht man KI bereits mit der Einführung der Elektrizität oder sieht in ihr die Dampfmaschine des 21. Jahrhunderts und mutmaßt, dass mit der Einführung von KI eine neue Dimension der Kriegsführung 4.0 verbunden ist.

Tatsächlich ist künstliche Intelligenz (KI) bei der Bundeswehr bereits in unterschiedlicher Ausprägung und Bereichen in Nutzung. In sehr viel mehr Bereichen ist eine künftige Nutzung zur Steigerung der Effizienz denkbar: zur Auswertung umfassender Datenbestände zur Krisenfrüherkennung bis hin zum hochauflösenden Lagebild eines gläsernen Gefechtsfeldes, von der vorausschauenden Instandsetzung zur fast autonomen Zuführung von Verbrauchsgütern bis in die vorderste Linie, von der Auswahl des kosteneffizientesten Bekämpfungsmittel für aufgeklärte Ziele bis zur Generierung von Optionen für die Möglichkeiten des Handelns des taktischen/operativen Führers, von selbstorganisierenden Drohnenschwärmen mit einem klaren Angriffsziel bis hin zum Schutz von Häfen mit kleinen autonomen Unterwasserfahrzeugen. Im Rahmen der Forschung für KI testet die Bundeswehr seit Dezember 2017 auch Watson, die KI Plattform von IBM, die pro Sekunde 1 Million Bücher lesen kann.

Die Bundesregierung hat im November 2018 ihre Strategie „Künstliche Intelligenz“ verabschiedet und beim Digitalgipfel am 4. Dezember 2018 vorgestellt. Mit ihr soll Deutschland als Forschungsstandort für KI entschieden gestärkt und die Förderung der Anwendung von KI in der Wirtschaft, insbesondere in kleinen und mittleren Unternehmen, vorangetrieben werden. Bis einschließlich 2025 will der Bund insgesamt etwa 3 Milliarden Euro für die Umsetzung der KI-Strategie zur Verfügung stellen.

Doch wie sind diese Anstrengungen, die von Kritikern bereits als ein Tropfen auf den heißen Stein angesehen werden, im internationalen Vergleich zu bewerten?

Russland: In einer 2017 in über 16.000 Schulen übertragenen Rede sieht der russische Präsident hinsichtlich der Künstlichen Intelligenz „kolossale Möglichkeiten und Gefahren, die sich schwer vorhersagen lassen“ und prognostiziert: „Wer in diesem Gebiet einen Durchbruch erreicht, wird zum Herrscher der Welt“. Innerhalb des russischen Verteidigungsministeriums gibt es jetzt zwei Zentren, die für die Entwicklung der neuesten bahnbrechenden Technologien wie autonome Waffen zuständig sind. Zudem hat das russische Verteidigungsministerium viele hochtechnologische Forschungs- und Entwicklungstätigkeiten zur KI in ihren zahlreichen akademischen Institutionen angestoßen.

In einer Entwicklung, die seltsam an die Sowjetära erinnert, bauen die Russen tatsächlich eine „Stadt“ für die KI und die damit verbundene Forschung am Schwarzen Meer. Bis 2020 sollen mindestens 2.000 Ingenieure und Wissenschaftler dort sein. Die russische Rüstungsindustrie hat bereits Maschinengewehre vorgestellt, die selbständig Zielentscheidungen treffen, und mit Schusswaffen ausgestattete Roboter. Und erste, wohl noch teilautonome Panzer, rollten bei einer Militärparade schon über den Roten Platz.

China: Die chinesische Führung hat mit ihrem KI-Plan öffentlich erklärt, dass China bis 2030 im Bereich der Künstlichen Intelligenz führend werden will und wird dafür 150 Milliarden US-Dollar investieren. Auf höchster Ebene legt die chinesische Regierung großen Wert auf die Unterstützung der staatlichen KI und nutzt die Dynamik der nationalen Key-Player wie Baidu, Alibaba und Tencent, die an der Spitze der chinesischen KI-Revolution stehen. In enger Kooperation mit ihnen soll die Wirtschaft innovativer gemacht und mit einer nationalen Strategie der zivil-militärischen Fusion das Militär modernisiert werden, um global an Einfluss zu gewinnen.

Kanada: Während in den 80er Jahren beim Thema „Maschinelles Lernen“ andere Nationen ihre Forschung zurückfuhren, nachdem schnelle Fortschritte ausblieben, hat Kanada frühzeitig KI als entscheidende Zukunftstechnologie identifiziert. Es setzte geduldig auf eine gezielte Universitäts- und Industrieförderung und schuf dadurch in Toronto, Montreal und Edmonton ein einzig artiges KI-Ökosystem mit einer ganzen Generation von ausgewiesenen KI-Experten, so dass alle wesentliche KI-Firmen dort Kooperationen eingegangen sind.

Vereinigte Arabische Emirate: Auch die VAE sehen ihre Zukunft in der künstlichen Intelligenz und haben dafür bereits auf Regierungsebene strukturell vorgebaut: Bereits 2017 wurde ein Ministerium für künstliche Intelligenz eingerichtet. Neben der KI-Förderung steht auch die Förderung der Blockchain-Technologie, mit der bis 2021 rund 50 Prozent aller Transaktionen abgewickelt werden sollen, ganz oben auf der staatlichen Prioritätenliste.

Südkorea: Auch ein eher unauffälliges Land wie Südkorea liegt weit vorn, was den Einsatz autonomer Waffensysteme angeht. Während die Vereinten Nationen über ein internationales Abkommen zur Ächtung autonomer Waffen verhandeln, hat Südkorea Anfang des Jahres eine große Investition in künstliche Intelligenz und militärische Systeme angekündigt. Das Besondere dabei: Südkorea verlässt dabei den abgeschirmten Bereich der reinen Rüstungsindustrie. Die neue Anlage ist ein Gemeinschaftsprojekt von Südkoreas führendem Rüstungsunternehmen Hanwha Systems mit der staatlichen Universität KAIST (Korea Advanced Institute of Science and Technology). Wie man es auch von Israel annimmt, hat Südkorea an der Grenze zum Norden bereits autonome Systeme im Einsatz, wenn es sich auch nicht um furchteinflößende Roboter im Terminator-Stil handelt. Die SGR-A1 von Samsung ist eine Art vollautomatischer Wachsoldat.

USA: Und wie stehen die Streitkräfte der USA zu KI? Die größte Herausforderung für die USA ist China, das den Einsatz von KI in ähnlicher Weise angeht, wie die USA in den sechziger Jahren den Wettlauf zum Mond. Auf den 2016 veröffentlichte National Artificial Intelligence Research and Development Strategic Plan, der Ähnlichkeiten mit Chinas KI-Plan aufweist, und in dem KI als eine der entscheidenden Herausforderungen für die Nachfolgeregierung hervorgehoben wurde, folgten unter Trumps Präsidentschaft zunächst keine erkennbaren Impulse. Obwohl in den letzten Jahren schon autonome Drohnenschwärme mit mehr als 100 kleinen Drohnen getestet und die KI in der Nationalen Sicherheitsstrategie zwar als Technologie mit strategischer Relevanz für die nationale Sicherheit der USA benannt wurde, fehlte es im Vergleich zu China bisher an einer umfassenden Vision, wie die Technologie entwickelt und genutzt werden soll.

In den USA definieren deshalb im wesentlichen Technologieunternehmen die Entwicklung von KI. Google, Amazon und Facebook sind maßgeblich für den Vorsprung der USA im Bereich KI verantwortlich.

In letzter Zeit haben die US-Streitkräfte den Fokus auf KI jedoch verstärkt. Im Juni 2018 hat das Pentagon auch organisatorisch nachgesteuert und ein neues, dem CIO des DoD unterstelltes, Joint Artificial Intelligence Center (JAIC) geschaffen, das fast alle KI-Bemühungen der US-Teilstreitkräfte und der DARPA beaufsichtigen wird. Zudem wurde im September 2018 angekündigt, dass die Streitkräfte in den nächsten 5 Jahren 2 Milliarden US-Dollar für die KI-Forschung und -Entwicklung ausgeben werden, welches im Wesentlichen in der Zuständigkeit der DARPA stattfinden wird. Bei der DARPA laufen bereits mehr als 20 Programme um KI voranzubringen und die Agentur verwendet aktuell KI in mehr als 60 weiteren Programmen. Mit dem neuen Programm „AI Next“ soll in einer „Beschleunigung der dritten Welle der KI-Technologien“ erforscht werden, wie Maschinen menschenähnliche Kommunikations- und Denkfähigkeiten erwerben können, mit der Fähigkeit, neue Situationen und Umgebungen zu erkennen und sich an sie anzupassen. Dabei soll die KI auch Erklärungen zu ihren Ergebnissen liefern. In Entwicklung ist auch eine Gehirn-Computer-Schnittstelle, die es einem Menschen ermöglichen soll, alles zu steuern, von einem Schwarm von Drohnen bis zu einem modernen Kampfflugzeug.

Mit einem gestrafften Vergabeverfahren soll erreicht werden, dass die Ergebnisse der Machbarkeit neuer KI-Konzepte innerhalb von 18 Monaten vorliegen.

Fazit

Noch führen die USA bezüglich der Anzahl von KI-Firmen und Patenten. Amerikanische Unternehmen haben außerdem den Vorsprung bei der Herstellung der leistungsfähigster KI-Chips. Auch die meisten erfahrenen KI-Talente sind bisher noch in den USA beschäftigt. Noch haben die USA einen Vorsprung in KI, doch der Vorsprung schwindet. Chinas Ambitionen führen zu der Einschätzung, dass es bereits einen neuen Technologiewettlauf in diesem Bereich gibt.

In künftigen Konflikten werden die Entscheidungszyklen wahrscheinlich deutlich schneller werden als die Fähigkeit der menschlichen Kognition, die relevanten Daten zu erkennen und zu verarbeiten. Militärische Führung und strategische Entscheidungsträger benötigen gleichermaßen künstliche Intelligenz, die Informationen verarbeiten und Optionen empfehlen kann, um Entscheidungen schneller (oder qualitativ hochwertiger) zu treffen als ein Gegner. Künftige militärische Organisationen werden wahrscheinlich Tausende oder sogar Zehntausende von unbemannten und robotischen Systemen und Sensoren enthalten, die alle eine Form der künstlichen Intelligenz beinhalten. In diesem Umfeld, in dem alle Seiten über künstliche Intelligenz und autonome Systeme verfügen können, wird der intellektuell Schnellste die Nase vorne haben.

Digitale Kompetenz und Konvergenz aus Industrie-Perspektive

Die inhaltliche Umsetzung und Ausgestaltung des Jahresprogramms bei AFCEA Bonn e.V. erfolgt durch verschiedene Gremien aus Bundeswehr, Behörden, Wissenschaft und Industrie, die sich alle dem Motto „Mehr Wissen teilen“ verschrieben haben. Der Industriebeirat (IBR) als Vertreter der rund 100 Mitgliedsfirmen bringt Themenvorschläge für Jahresthema und Veranstaltungen ein. Dieses Gremium hat zum Jahresthema zwei Beiträge aus seinem Kreis ausgewählt, die das Thema aus verschiedenen Industrie-Perspektiven beleuchten. Die digitale Transformation ist eines der akuten Handlungsfelder der heutigen Zeit. IBM ist in diesem Bereich Technologieanbieter und Transformationspartner vieler Kunden. Oracle verfolgt seit vielen Jahren in der Entwicklung seiner Produkte und Services konvergente Strategien. Die beiden IBR-Mitglieder betrachten stellvertretend für das Gremium das Jahresthema.

Das Nutzererlebnis im Mittelpunkt – die Entwicklung von digitalen Produkten und Services mit analogem Nutzen

Stefan Hefter, Partner, IBM Geschäftsbereichsleiter Digitalisierung Bundeswehr

Stefan Hefter *Foto: Privat*

Zum aktuellen Zeitpunkt ist es sicherlich unbestritten, dass eine erfolgreiche digitale Transformation für Organisationen jeglicher Art zwingend notwendig ist, um auch zukünftig am Markt relevant und geschäftsfähig zu sein. Damit dieser Wandel gelingt, darf er nicht um seiner selbst willen geschehen, sondern muss zwei essentielle Grundsätze berücksichtigen – nämlich Nutzerzentrierung und analogen Nutzen. Die Nutzerzentrierung meint hier, dass die Nutzer von Anfang an am Kreativprozess und an der anschließenden Entwicklung beteiligt sein müssen. Nutzbarkeit ist dabei ein zentraler Erfolgsfaktor der Entwicklung und ein begleitendes Change Management muss integraler Bestandteil der Umsetzung sein. Der Mensch ist vom Wesen her jedoch analog, denn wir leben in einer realen bzw. sensuellen Welt, unsere Sinne und unsere Interaktionen sind analog. Das muss bei der digitalen Transformation berücksichtigt werden, indem der gesamte Prozess messbar und verständlich geplant und umgesetzt wird, der analoge Nutzen muss ersichtlich sein.

In der IBM-Garage werden zeitnah testbare Produkte und Services entwickelt

Um die Anforderungen an die Digitalisierung mit den aktuellen technischen Möglichkeiten (wie beispielsweise das Internet of Things IoT, Blockchain oder künstliche Intelligenz) zu verbinden, hat IBM die IBM-Garage entwickelt. Sie stellt einen gemeinsamen Ort zum Arbeiten bereit, der die intensive Kommunikation und vor allem Zusammenarbeit der Beteiligten durch kreativ gestaltete, inspirierende Räume fördert. Hier findet nun ein Entwicklungsprozess statt, der aus drei Phasen besteht und die Prinzipien des agilen Arbeitens berücksichtigt. Am Anfang steht die umfassende und systematische Auseinandersetzung mit konkreten Frage- und Problemstellungen, gefolgt von der Erarbeitung von ersten Lösungsansätzen – stets unter Beteiligung der Nutzer. Dies geschieht unter Einsatz von Design-Thinking-Methoden, um zeitnah neue Ideen im kontinuierlichen Austausch mit Nutzer zu entwickeln. Zusammen mit der frühen Erstellung von Prototypen, die „greif- & fassbar“ sind, können laut Studien die Entwurfszeiten um bis zu 75 Prozent und Entwicklungszeiten um bis zu 30 Prozent reduziert werden.

Im Entwicklungsprozess folgt nun bereits die Bereitstellung von ersten testbaren Produkten und Services für die Nutzer, das sogenannte Minimum Viable Product (MVP). Dabei handelt es sich um ein Produkt, das gerade genug Funktionen hat, um für die Nutzer sinnvoll zu sein und eine schnelle Bewertung im realen Einsatz ermöglicht. Im letzten Prozessschritt der

Mögliches Design einer IBM-Garage *Foto: IBM*

IBM-Garage wird das Produkt kontinuierlich weiterentwickelt, es wird Übergang zur großflächigen Produktion vorbereitet.

Ausgezeichnete und nutzerfreundliche Ergebnisse mit der IBM-Garage entwickeln

Beispielhaft für die Effizienz der IBM-Garage ist der Relaunch der Website des Bundesministeriums der Verteidigung bmvg.de. Aperto, IBMs Digitalagentur, und das BMVg haben hier gemeinsam einen Nutzer und Service orientierten Internetauftritt aufgebaut, der für seine hohe Nutzerfreundlichkeit, eine klare Struktur und die Image bildende Wirkung mit dem Econ Award für digitale Regierungskommunikation ausgezeichnet wurde. In der IBM-Garage am Standort Berlin, einer alten Pianofabrik, wurden die Anforderungen aller Nutzer mittels Design Thinking herausgearbeitet und schließlich die Entwicklung der Website hierdurch umgesetzt. Durch die Anwendung des Scrum-Vorgehens als Form des agilen Arbeitens war die Nutzerzentrierung sowie auch die Rückkopplung mit Nutzern im gesamten Umsetzungsprozess gewährleistet.
Aufgrund des Erfolgs der IBM-Garage in der Industrie wendet IBM dieses Vorgehen im Rahmen verschiedener, auch nicht IT-bezogener Projekte im Bereich der Verteidigung an. Das IBM Team für digitale Strategie hat ein angepasstes Modell für die militärische Nutzung entwickelt und hat Anfang 2019 eine IBM-Garage für den Bereich Defense in Bonn eröffnet.

Young AFCEANs: Ausgezeichnete Angebote

Auch in 2018 konnte das Bonner Chapter mit seinen Young AFCEANs Aktivitäten überzeugen. AFCEA International zeichnete das Chapter und junge Mitglieder bis 40 Jahre erneut aus.

Interesse dabei zu sein?

AFCEA bietet für seine Mitglieder bis 40 Jahre (Young AFCEANs) neben dem Angebot der Fachausstellung, der Koblenzer IT-Tagung und Fachveranstaltungen weitere besondere Aktivitäten: Zum Vernetzen und Austauschen werden den jungen Fach- und Führungskräften sowie Hochschulabsolventen eigene Fach- und Karriereveranstaltungen im Bonner und Berliner Raum angeboten.

Im Rahmen der AFCEA Fachausstellung findet dieses Jahr am 10. April 2019 das „Karrierestarter-Forum Young AFCEANs“ statt. Das Thema der Gesprächsrunde für und mit jungen Führungskräften ist „Karriere in der digitalen Transformation“.

Aktivitäten mit anderen AFCEA Chaptern – vor allem mit Young AFCEANs aus Kaiserlautern und dem Eifeler Chapter – ergänzen das Angebot. Gemeinsam besuchen wir beispielsweise Forschungslabore verschiedener IT-Firmen oder die Air Base Ramstein.

Weitere Informationen und Termine zu aktuellen Veranstaltungen findet Ihr unter www.afcea.de. Ansprechpartnerin für die Young AFCEANs Veranstaltungen sind Katja Frintrop (Katja.Frintrop@afcea.de) und Michael Buech (Michael.Buech@CGIDEU.COM).

Das Wechselspiel der Konvergenz – eine technologische Perspektive

Magdalene Kahlert, Senior Sales Direktorin Oracle B.V. & Co. KG
Oliver Burghardt, Senior Sales Manager Oracle B.V. & Co. KG

Magdalena Kahlert *Foto: Privat*

Die Wechselwirkung zwischen technologiegetriebenen Entwicklungen von Anforderungen und nutzerinduzierter Entwicklung ist der Motor für die Informations- und Kommunikationsindustrie. Bestes Beispiel hierfür sind Innovationen, die durch die Bedienerleichtigkeit von mobilen Endgeräten und Touch-Displays Einzug in die Fachanwendungen fast aller Unternehmensbereiche gehalten haben. Mit Konvergenz beschreiben wir das Zusammenwachsen von IT- und Kommunikationstechniken und den vielen unterschiedlichen Diensten im Rahmen der Digitalisierung einer Organisation.

Im Bereich der Verteidigungswirtschaft kann Konvergenz in vielen Dimensionen wirksam werden, etwa zum Nutzen der Innovationsstärke und Agilität aus der zivilen Welt in der militärischen Welt oder für neue Technologien, die im Rahmen der Digitalisierung entstanden sind und entstehen, in den Anwendungen aller Unternehmensbereiche zur Nutzung bringen und dafür insbesondere die operativen Produktions- und Logistiksysteme öffnen.

Konvergenz verändert existierende Prozesse

Dies in aller Konsequenz auch wirksam zu erschließen erfordert eine stringente Konvergenzstrategie und die Einrichtung einer sicheren Basistechnologieschicht um die Grundlage für konvergente Lösungen zu schaffen. Diese Voraussetzungen müssen geschaffen werden, damit die mit der vollständigen Digitalisierung zwangsläufig verbundenen Risiken beherrschbar gehalten werden. Eine übergreifende Sicherheitsarchitektur ist zwingend erforderlich. Die Abwehr von Cyber-Kriminalität ist eine zusätzliche Aufgabe für die Implementierung konvergenter Systeme.

Vollständige Transparenz auf der Architekturebene und hohe Kompetenz im Umgang mit den Basistechnologien sind hierbei unabdingbar. Die Schaffung von Resilienz und Sicherheit in Verbindung mit Automatisierung stellt dabei die größte Herausforderung für die gesamte Organisation dar.

Beispiele für erfolgreiche Konvergenz-Technologien in der ITK finden wir in den verschiedensten Bereichen, sei es bei den konvergenten IT-Architekturen und Systemen, sei es im Bereich der Standard Applikationen, die kontinuierlich mit den innovativen Technologien wie Künstliche Intelligenz oder Maschinelles Lernen, Big Data, Analytics, Chatbot, Mobile „angereichert“ werden, um die Digitalisierung der Geschäftsprozesse und die Bedürfnisse der Nutzer nach höherem Komfort und Effizienz abzubilden.

In diesem Zusammenhang verfolgt Oracle seit vielen Jahren in der Entwicklung seiner Produkte und Services konvergente Strategien. Dies immer mit dem Blick auf weitgehende Plattformunabhängigkeit und damit maximale Flexibilität für Anwender.

Oliver Burghardt *Foto: Privat*

AFCEA Fachausstellung 2019

Bechtle AG: starker IT-Partner öffentlicher Auftraggeber

Ob klassische IT-Infrastruktur, Digitalisierung, Cloud, Mobility, Security oder IT als Service – Bechtle agiert bei allen Themen vernetzt, professionell und ist flexibel aufgestellt. Mit dem Geschäftsbereich Public Sector Business richtet der internationale IT-Konzern gezielt seinen Blick auf die besonderen Anforderungen öffentlicher Auftraggeber. Seit vielen Jahren schon stattet Bechtle die Bundeswehr über Rahmenverträge mit Informationstechnologie aus und erbringt als starker Partner Dienstleistungen für zukunftsfähige IT-Architekturen.
Im Juni 2017 hat das Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAAINBw) Bechtle zum dritten Mal in Folge den Zuschlag für einen Rahmenvertrag über IT-Komponenten und Dienstleistungen erteilt. Abrufberechtigte Einrichtungen können so über standardisierte Prozesse verschiedene Produkte und Dienstleistungen ausschreibungsfrei beziehen. Die Laufzeit des aktuellen Rahmenvertrags „IT-Plattform – 2./3. Rechnerebene R1112“ reicht bis 2021. Er schließt nahtlos an die bereits 2009 und 2013 geschlossenen Rahmenverträge an. Bechtle setzt damit die etablierte Partnerschaft fort und stattet auch in den kommenden Jahren die Bundeswehr mit Informationstechnologie und Dienstleistung aus. Das Kerngeschäft umfasst dabei die Bereiche Handelsware mit mobilen Endgeräten, PCs, Peripherie, Drucker, Server, Speichersysteme, USV-Anlagen, sowie hardwarenahe Softwareprodukte. Neben Lieferung von Informationstechnik plant, installiert und konfiguriert Bechtle auch gesamte IT-Umgebungen und Netzwerke. Kontinuierlich vertiefen die Partner ihre Zusammenarbeit außerdem rund um Dienstleistungen wie IT-Sicherheitskonzepte (SiKo nach Vorgaben ZdV 960/1 in SAVe), Cyber Resilience oder aber Service- & Systemsteckbriefe und Enterprise Architecture nach NATO Architecture Framework (NAF). Teilekennzeichnung (TKZ) von Geräten, Gütern und Behältern mit grafischen Codierungen und Nummernkreisen runden das Dienstleistungsportfolio ab.

Wir für die Bundeswehr.

Bechtle realisiert den Vertrag als Hauptauftragnehmer unter anderem mit seinen langjährigen Herstellerpartnern HP, NetApp, Dell EMC sowie den Dienstleistungsunternehmen CONET Solutions und GBS Tempest. Die modulare, an den Kundenanforderungen ausgerichtete Organisationsform ist mit 70 IT-Systemhäusern in lokaler Nähe zum Kundenumfeld, sowie der zentralen Stärke eines internationalen IT-Konzerns optimal an die Rahmenverträge mit der Bundewehr angepasst.
Die im IT-Systemhaus Bonn ansässige zentrale Projektleitstelle (ZPLS) dient der Bundeswehr als direkte Koordinierungsstelle für die Bereiche Vertrieb, technische Beratung und Validierung, Warenkorbmanagement sowie dem Projekt- und Servicemanagement.
Die gesamte Lagerhaltung und Lieferlogistik sowie das Auftragsmanagement erfolgen gebündelt aus der Konzernzentrale der Bechtle AG in Neckarsulm.
Bechtle ist Deutschlands größtes unabhängiges IT-Systemhaus und führender IT-E-Commerce-Anbieter in Europa. Für den IT-Konzern arbeiten derzeit über 10.000 engagierte Mitarbeiter in 70 Systemhäusern in der DACH-Region und IT-E-Commerce Gesellschaften in 14 Ländern. Ein flächendeckendes Netz, das so kurze Liefer- & Servicewege zu den einzelnen Standorten der Bundeswehr garantiert.

Kontakt: ***Bechtle AG, Gabor Jeszenoei***
Zentrales Team Bundeswehr, Telefon: 0228 6888 400
Email: zpls-r1112@bechtle.com, Web: www.bechtle.com

Bechtle Konzernzentrale *Foto: Bechtle AG*

Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr

AFCEA Bonn e.V.
Anwenderforum für Fernmeldetechnik, Computer, Elektronik und Automatisierung

„Digitale Kompetenz und Konvergenz – im Zeitalter intelligenter Systeme“

IT-Systeme werden immer selbstständiger und intelligenter – dies gilt sowohl für militärische Anwendungen als auch für Lösungen der öffentlichen Verwaltung. Die Koblenzer IT-Tagung 2019 betrachtet neben Technologien und Entwicklungen in diesem Feld auch die sich daraus erwachsenden (neuen) Fähigkeiten sowie den sich verändernden operationellen Bedarf.
Künstliche Intelligenz benötigt gute und verlässliche Massendaten als Rohstoff zum Lernen. Wir werden uns mit der Frage beschäftigen, wie man an unverfälschte und qualitätsgesicherte Daten kommt, und mit welchen technischen Hilfsmitteln der Austausch funktionieren und Vertrauen zwischen Dateninhabern hergestellt werden kann. Da mit intelligenten Systemen automatisierte Kriegsführung möglich werden könnte, leiten sich auch ethische Überlegungen ab – wo liegen moralische und rechtliche Grenzen im Umgang mit technischen Fähigkeiten, wie sieht der politische Rahmen aus?
Die technische Entwicklung hin zu intelligenteren Systemen macht Veränderungen im Umgang mit Technologien notwendig und beeinflusst die Gefechtsführung. Steht etwa die Tastatur als Universalmedium der Mensch-Maschine-Interaktion vor dem Ende? Mit welchen Anpassungen an die neue Technik müssen sich die Gesellschaft, Organisationen und vor allem Soldaten auseinandersetzen? Der Umgang mit intelligenten Systemen und ihrer Autonomie verlangen eine neue Kompetenz im Umgang mit ihnen. Nicht zuletzt ist bis heute unklar, wer die Verantwortung bei Entscheidungen durch intelligente Systeme trägt. Digitale Kompetenz wird mit digitaler Konvergenz damit zum entscheidenden Faktor des Fortschritts und digitaler Souveränität.

Diese Zusammenhänge und damit in Verbindung stehende Fragen mit ihren Auswirkungen auf die Ausrüstung der Bundeswehr zu diskutieren, ist unser Anliegen bei der Koblenzer IT-Tagung am 05. September 2019. Hierzu laden wir Sie ein und freuen uns, Ihnen ein interessantes Programm sowie einen unterhaltsamen Abend bieten zu können, verbunden mit der Möglichkeit zu vielen Gesprächen.

Ort:	Rhein-Mosel-Halle, Julius-Wegeler-Straße 4, 56068 Koblenz
Datum/Zeit:	Donnerstag, 05.09.2019 09:00 – 18:30 Uhr (Einlass 08:00 Uhr) mit „Koblenzer Abend“ 18:30 – 21:00 Uhr
Teilnehmer:	Bundesministerium der Verteidigung; Kommandobehörden, Ämter, Dienststellen und Truppenteile der Bundeswehr; Behörden, Organisationen aus dem Bereich der öffentlichen Sicherheit (BOS); Institute, Verbände; Universitäten und Hochschulen; Industrie mit Schwerpunkt Informations- und Kommunikationstechnik; internationale Gäste.
Fachliche Leitung:	Brigadegeneral Michael Hauschild, Abteilungsleiter Informationstechnik BAAINBw Oberst i.G. Heiko Mühlmann, Stellvertretender Vorsitzender AFCEA Bonn e.V.
Programm:	+ aktuelle Informationen unter www.afcea.de und www.baainbw.de
Kostenbeitrag:	+ Tagungspauschale: 70,- € + Tagungspauschale für Öffentlichen Dienst und AFCEA - Mitglieder: 20,- € + Teilnahme am Koblenzer Abend: jeweils 20,- € zusätzlich.

AFCEA Bonn e.V., Borsigallee 2, 53125 Bonn, Tel.: 02 28 / 9 25 82 52, Fax: 02 28 / 9 25 82 53
BAAINBw, Ferdinand-Sauerbruch-Str. 1, 56073 Koblenz, Tel.: 0261 / 13354 8143, Fax: 0261 / 13354 8470

BDSV

DIGITALE KONVERGENZ IN DER SICHERHEITS- UND VERTEIDIGUNGSINDUSTRIE

Plattformen im Zeichen der Digitalen Konvergenz

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

Dr. Hans Christoph Atzpodien

Foto: Illing & Vossbeck Fotografie

Wenn wir in die zivile, traditionelle Wirtschaftswelt blicken, kennt man Plattformen und Plattform-Strategien z.B. aus der Automobilindustrie (eine Plattform – verschiedene Modelle). Auch in der digitalen Wirtschaftswelt haben sich in den letzten Jahren viele innovative Geschäftsmodelle auf Basis neuer Technologien und damit bereitgestellter Plattformen etabliert. Wie etwa das Portal AirBnB, welches weltweit die größte Zahl an Übernachtungs-Buchungen im Jahr verzeichnet, aber nicht ein einziges Bett selber besitzt. Damit ist die Digitalisierung nun schon seit geraumer Zeit Treiber eines teilweise disruptiven Wandels in den Wertschöpfungsketten und kann hierbei Lösungen für aktuelle und zukünftige Herausforderungen bieten. In manchen Bereichen ähnlich, aber doch auf eine ganz eigene Art und Weise findet sich das in der Sicherheits- und Verteidigungsindustrie wieder.

Sowohl mit Sicht auf die klassische Verteidigungsindustrie mit ihren Land-, See- und Luftsystemen, als auch mit Sicht auf die gegenwärtige „grüne“ IT-Industrie ist der Gedanke einer „Plattform“ ein weitgehend etablierter und akzeptierter.

Es wird jedoch immer deutlicher, dass die bestehende Heterogenität (das heißt jede Plattform besteht für sich selbst) der digitalen Konvergenz – dem Zusammenwachsen „herkömmlicher Bereiche“ mit Digitalisierungstechnologien – in zunehmenden Maße im Wege steht. Herkömmliche Waffensysteme und Informationssysteme wachsen zwar immer enger zusammen, dennoch bildet auch heute noch jede Plattform eine eigene Welt ab.

Ausgangspunkt für Digitale Konvergenz

Die herkömmlichen Plattformen in der klassischen Verteidigungswirtschaft waren ein Schiff, ein Flugzeug oder ein Fahrzeug als Träger von unterschiedlichen Fähigkeiten – oftmals mit eigenen, teilweise sogar in sich abgeschlossenen, IT-Systemen. In der IT dagegen war die Plattform damals schon ein einheitlicher Infrastrukturansatz zur Bereitstellung von Ressourcen für die Realisierung unterschiedlichster Fähigkeiten. Damit wiesen beide zwar bereits eine sehr ähnliche Zielrichtung auf, unterschieden sich jedoch in ihrem Aufbau.

Heute steht die modulare Wiederverwendung von Komponenten in unterschiedlichen Plattformen im Vordergrund. Die weitere Abstimmung von Plattformen aufeinander, physikalisch oder digital, ist zusammen mit der weiteren Homogenisierung der IT-Landschaft aktuell die wichtigste Aufgabe und wird es auch noch in kurzfristiger bis mittelfristiger Zukunft bleiben. Ein stärker zukunftsgerichteter Gedanke ist die Betrachtung modularer, plattformunabhängiger Missionssysteme, wie z.B. im Fall von Marineschiffen, als Gesamtsystem verstanden, bestehend aus schwimmender Hülle, Führungssystem, Bewaffnung, Lazarett und Messen, die alle aber wiederum miteinander verknüpft sein müssen. Auch die „digital gerüstete“ Brigade, die aufgrund ihrer Organisation, Ausrüstung und Personalstärke in der Lage ist, operative Aufgaben selbstständig zu lösen, könnte – im Sinne des Plattformgedankens – zusammen mit mehreren – wenn will – „landseitig operierenden Fregatten“ eine integrierte, digitalisierte Division bilden. Ebenso sind Familienkonzepte über Plattformen und Teilstreitkräfte hinaus z.B. bei Radar und Führungsinformations- sowie Waffeneinsatzsystemen vorstellbar.

Dies alles sind Teile von Entwicklungen, bei denen wir schon vorangekommen sind, zumindest auf dem Papier, deren Ende aber noch längst nicht erreicht ist. Nur eines wissen wir schon heute mit Sicherheit: Dass nämlich davon die operationelle Qualität und Überlegenheit unserer Streitkräfte in höchstem Maße abhängen wird. Eine adäquate Verteidigung gegen einen technologisch mindestens als gleichwertig zu unterstellenden Aggressor wird sich vor allem auf diesem Feld beweisen müssen.

Obwohl Kreativität immer zu begrüßen ist, ergibt sich bei all diesen Bemühungen aber zugleich das Problem, dass sich viele Akteure, ob nun Industrie- oder Amtsseite, selbst als „der Innovator“ ansehen und dadurch letztlich wieder eine heterogene, womöglich unübersichtlichere Landschaft neuer Standards entsteht.

Dies gilt umso mehr, wenn – wie schon zuvor erwähnt – immer deutlicher wird, dass das Zusammenwachsen herkömmlicher Ansätze mit neuen Ideen ein entscheidender Erfolgsfaktor sein wird. Digitalisierung sprengt Grenzen – nicht nur im Bereich der Technologien oder Plattformen, sondern auch im Bereich der Organisation.

Digitale Konvergenz

Der zukünftige Plattformgedanke im Rüstungsumfeld kann nur unter dem Aspekt der Konvergenz betrachtet werden.

Unter Konvergenz wird gemeinhin das Zusammenwachsen von Bereichen beschrieben, die bisher weitgehend voneinander getrennt existierten. Da sei als ziviles Beispiel einmal die Verbindung der Haushaltsgeräte-Industrie und der IT-Branche genannt (Stichwort: Kühlschrank mit Internetzugang). Aber auch im militärischen Kontext gibt es bereits schon länger diese Konstrukte (etwa in Gestalt moderner Sensorsysteme in gepanzerten Fahrzeugen, die den Fahrer bei der Steuerung oder die Ziel- und Wirkgenauigkeit unterstützen).

Digitale Konvergenz meint nun im nächsten Schritt das Zusammenwachsen „herkömmlicher Bereiche“ oder eben „herkömmlicher Plattformen“ mit digitalen Technologien und die daraus resultierenden neuen Wertschöpfungs- oder Fähigkeitsprofile.
So gibt es heutzutage bereits Kühlschränke, die automatisiert einen definierten Lebensmittelbestand „selber halten“ können, indem sie Online-Bestellungen auslösen und somit die zuvor strikt getrennten Geschäfts- und Prozessmodelle „Haushaltsgeräte“ und „Lebensmittelhandel“ auf neue Art miteinander verknüpfen. Im militärischen Bereich gibt es hier noch viel Potenzial, wie beispielsweise einen „(teil)autonom fahrenden“ Panzer, der seine Wege auf dem Gefechtsfeld auf Basis von diversen Datenquellen (z.B. aktuelle Satellitenaufklärung und digitale Geländemodelle) effizient selbst suchen könnte.
Somit könnte der mögliche zukünftige Plattformgedanke eine Verbindung von zwei Komponenten sein: die physikalische Trägerplattform wie bisher, aber ergänzt um eine nach universellen Standards designte IT-Plattform, bei der von Beginn an auf Homogenität des IT-Systems der Bundeswehr und transparente Sicherheitsvorgaben geachtet wird.
Oder anders ausgedrückt: Es wird kein Schiff mehr gebaut, auf das dann die IT „einfach mit draufkommt“. Die IT-Plattform ist integraler Bestandteil der physikalischen Plattform und somit eine Verlängerung des Gesamtsystems. Damit würde – zumindest auf nationaler Ebene – die lange bestehende und nicht gänzlich umgesetzte Forderung nach Interoperabilität abgelöst durch die Forderung nach Integration und Modularität. Dies bedeutet insbesondere, dass nicht jede neue physikalische Plattform „einfach so“ eine eigene IT mit einrüsten sollte. Sie sollte stattdessen als Erweiterung des IT-Systems der gesamten Bundeswehr verstanden werden.
Daraus ergäbe sich dann eine allgemeine, teilstreitübergreifende digitale „Plattform Bundeswehr“, die weder auf die IT noch auf die physikalischen Träger beschränkt wäre. Im Gegenteil, sie sollte den gesamten, digital-konvergenten Ansatz widerspiegeln und somit übergreifende Rüstungsgrundlage sein.
Ganz sicher dürfte klar sein, dass diese Plattform nur mit einem passenden Architekturmanagement als relevantem Bestandteil einer effektiven IT-Steuerung funktionieren kann. Entsprechend den Leitlinien bzw. Vorgaben des zentralen Architekturmanagements würden hier bestehende Applikationen, von der App und vom Fuhrparkservice bis zu ganzen Großverbänden, auf eben diese Plattform überführt.

Anforderungen an digital-konvergierte Plattformen

Das Gefechtsfeld wird transparenter und komplexer. Informationsüberlegenheit ist somit heute, und wird es in Zukunft umso mehr sein, der wichtigste Faktor in den Szenarien unserer Streitkräfte. Zukünftige Waffensystemplattformen müssen durch weniger Personal betrieben und beherrscht werden können, denn unsere möglichen Gegner werden absehbar zahlenmäßig überlegen sein.
Das Sammeln, Aggregieren, Analysieren und Visualisieren von Daten mit dem Ziel der Umwandlung in nützliche Informationen zur weitgehend automatisierten Steuerung und Optimierung von Prozessen wird auch weiterhin der elementare Arbeitsauftrag einer jeden Plattform sein.
Ziel aller unserer Anstrengungen muss es sein, die Einsatzbereitschaft der Bundeswehr und anderer Behörden und Organisationen mit Sicherheitsaufgaben (BOS) durch Bereitstellung intelligenter und effizienter Plattformen zu gewährleisten und möglichst zu erhöhen.
Die deutsche Sicherheits- und Verteidigungsindustrie leistet hierbei einen strategischen Beitrag für die sicherheitspolitische Handlungsfähigkeit unseres Landes, der weit über seine quantifizierbare wirtschaftliche Bedeutung hinausreicht. Und gerade im beschriebenen Bereich liegt es in unserem nationalen Sicherheitsinteresse, gemeinsam mit allen relevanten Stakeholdern an einem Strang zu ziehen.
So ist die Betrachtung von Digitalisierung im Kontext Militär alleine sicherlich zu kurz gegriffen. Zumindest die Felder der inneren und der äußeren Sicherheit lassen sich hier nicht mehr getrennt betrachten. Es ist klar, dass Bedrohungsszenarien und Technologiegrenzen hier miteinander korrespondieren. Mit der zunehmenden Digitalisierung entstehen auch neue Technologien, digitalisierte Plattformen und Cyber-Bedrohungen, die für unsere Gesellschaft zu immer neuen Risiken, Angriffsvektoren und Schwachstellen führen. Wegen der immer komplexeren Zusammenhänge der daraus denkbaren Bedrohungsszenarien ist daher der Aspekt der Cyber-Security präsenter und wichtiger denn je. Aber auch ohne leistungsfähige Plattformen lässt sich eine moderne Verteidigungsfähigkeit nicht darstellen.
Daher ist bei der Ausrüstung unser Sicherheits- und Verteidigungskräfte die Umsetzung der digitalen Konvergenz von höchster Bedeutung.

Sichere Inter-Netzwerk Architektur: der IP-Krypto-Backbone der Bundeswehr

Dr. Michael Sobirey, Leiter der Division Verteidigung der secunet Security Networks AG

Dr. Michael Sobirey

Foto: FOTO WUGK

Einleitung

Streitkräfte sowie militärische Organisationen und Behörden haben einen besonders hohen Anspruch an den Schutz der Vertraulichkeit ihrer Daten. Deren Spektrum reicht von nationalen und internationalen bis hin zu Missions-bezogen klassifizierten Daten. Entscheidend für eine effiziente, bedarfsgerechte Bereitstellung und Verarbeitung dieser Daten sind intelligente IT-Sicherheitsarchitekturen. Dies gilt insbesondere für den informationstechnischen Grundbetrieb der Truppe, Führungsinformationssysteme, Bordnetze sowie multinationale Einsatznetze mit taktisch-mobilen Systemanteilen.

SINA: Zweck, Aufbau, grundlegende Funktionsweise

Zur Absicherung ihrer IT-Netzwerke, insbesondere für den Schutz von Verschlusssachen (VS), nutzen militärische Bedarfsträger – darunter das Bundesministerium der Verteidigung, die Bundeswehr und die NATO – die „Sichere Inter-Netzwerk Architektur“ SINA. Dabei handelt es sich um eine Kryptoproduktfamilie, die von der secunet Security Networks AG im Auftrag des Bundesamts für Sicherheit in der Informationstechnik (BSI) entwickelt wurde. SINA dient der sicheren Verarbeitung, Speicherung und Übertragung von VS. Seit mittlerweile mehr als 15 Jahren ist SINA elementarer Bestandteil nationaler militärischer Hochsicherheitsnetze.

Der Kerngedanke von SINA ist der Schutz unterschiedlich klassifizierter Daten, lokal, entfernt sowie beim drahtgebundenen und drahtlosen Transfer über offene Netze. Das ganzheitliche Sicherheitskonzept umfasst eine Vielzahl ineinandergreifender Schutzmaßnahmen auf verschiedenen Systemebenen.

Die gerätetechnische Basis bilden die je nach Geheimhaltungsstufe passend dimensionierten, abstrahl- und manipulationsgeschützten, optional robusten Hardwareplattformen unterschiedlicher Bauformen. Zudem beinhaltet sie FPGA-basierte Kryptomodule, Smartcards als kryptographische Anker sowie sicherheitsüberprüfte Firmware für einen sicheren Systemstart. Als softwaretechnisches Fundament der SINA Technologie fungiert die intensiv sicherheitsevaluierte SINA Systemsoftware mit eingebetteten Kryptodateisystemen.

Zahlreiche hochentwickelte und mehrstufig gestaffelte Sicherheitsmodule (insbesondere IPsec-Verschlüsselung, Zugriffskontrolle, Paketfilter, Schnittstellenkontrolle, Monitoring) schützen SINA gegen eine Vielzahl von Angriffen. Auf der obersten Ebene der SINA Systemarchitektur befinden sich – realisiert in der SINA Workstation – strikt voneinander abgeschottete Arbeitsumgebungen (Sessions) unterschiedlicher Einstufung. Dabei handelt es sich insbesondere um in virtuellen Maschinen (PCs) gekapselte marktgängige Gastbetriebssysteme und -Applikationen, nativ integrierte VoIP-Applikationen sowie Terminals.

Den virtualisierten Gastsystemen liegen Session-spezifische Kryptodateisystem-Partitionen zugrunde. Dadurch sind die auf diesen Clients gespeicherten „roten“ (eingestuften) Daten im ausgeschalteten Zustand kryptographisch „geschwärzt“, was die physischen Absicherungsmaßnahmen der Betriebsumgebungen signifikant entspannt.

Als Komponenten stehen unterschiedliche Gateways (SINA L3 Boxen), Ethernet-Verschlüsseler (SINA L2 Boxen), Datendioden und Clients zur Verfügung. Das Client-Spektrum umfasst stationäre, mobile und ultramobile Varianten und reicht von SINA Terminals über SINA Workstations bis hin zu SINA Tablets.

Um unterschiedlichen Sicherheitsanforderungen gerecht werden zu können, werden SINA Komponenten in drei grundlegenden Kategorien angeboten, die durch das BSI für verschiedene Geheimhaltungsstufen zugelassen sind – von VS-NfD (SINA S) über VS-VERTRAULICH (SINA E) bis hin zu GEHEIM (SINA H).

Referenzprojekte bei der Bundeswehr und im Bundesministerium der Verteidigung

Als zahlenmäßig größter nationaler Anwender verwendet die Bundeswehr SINA Komponenten in zahlreichen Großprojekten und IT-Systemen aller Teilstreitkräfte sowie zentralen Netzinfrastrukturen. So erfolgte ab dem Jahr 2004 der Roll-out mehrerer tausend SINA H Komponenten in die militärischen Führungsinformationssysteme (FüInfoSys) der Bundeswehr. Auch in Afghanistan waren SINA Komponenten im Einsatz.

SINA H Komponenten prägen den heutigen IP-Krypto-Backbone der Bundeswehr, sowohl Client- als auch netzseitig. Seit 2015 hat sich die SINA Workstation H als HaFIS-Client etabliert. Erst im Herbst 2018 beauftragte das Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAAINBw) secunet mit der Lieferung von weiteren hunderten SINA Komponenten zur Regeneration von SINA Clients und Gateways früherer Gerätegenerationen im Rahmen des Programms HaFIS.

In dem von der BWI GmbH betriebenen und fortlaufend weiterentwickelten Military Message Handling System NuKomBw kommen nunmehr erstmalig mehrere hundert SINA Workstations H zum Einsatz, die von der BWI Mitte 2018 beauftragt wurden. Damit reduziert sich die Komplexität der gerätetechnischen IT-Ausstattung in den NuKomBw-Betriebsstellen.
Im Jahr 2017 beauftragte das BAAINBw secunet mit der Lieferung einer größeren Anzahl SINA Clients und Gateways für die IT-Ausstattung des Multinationalen Kommandos Operative Führung / Multinational Joint Headquarters Ulm.
Auch im Bundesministerium der Verteidigung (BMVg) kommt SINA querschnittlich zum Einsatz: Die seit 2016 eingeführte mobile SINA Workstation S etablierte sich dort inzwischen als mobiler Standard-Arbeitsplatz und erfährt eine hohe Nutzerakzeptanz.

Ausblick: IT-Hochsicherheitslösungen im Kontext der digitalen Konvergenz

Heute sind Streitkräfte sowie Behörden und Organisationen aus dem Verteidigungssektor mehr denn je auf leistungsfähige moderne IT-Strukturen angewiesen, um ihre Verteidigungsfähigkeit auch im Cyber- und Informationsraum zu gewährleisten. Hinzu kommen steigende Anforderungen im Hinblick auf Mobilität, Integration, Flexibilität, kryptographische Agilität sowie ressourceneffizienten Betrieb, die an heutige und künftige Einsatzverbände und deren multinationale Missionsnetze gestellt werden.
Vor dem Hintergrund einer zunehmenden Durchdringung von Informationstechnologie und klassischer Wehrtechnik, die derzeit unter dem Schlagwort „digitale Konvergenz“ diskutiert wird, wird sich die Rolle der IT im Verteidigungssektor weiter ändern. IT-Systeme werden zu integralen Bestandteilen militärischer Gesamtsysteme, die wiederum deren Aufbau und Fähigkeiten verändern und ihrerseits neue Anforderungen generieren.
In dieser Konstellation kommt der Cybersicherheit künftig eine noch größere Bedeutung zu. Der BDSV betrachtet IT und Cybersicherheit im Zusammenhang der digitalen Konvergenz als essentiellen „Enabling Factor“ bei der Digitalisierung für die Produkte, Lösungen und Services der Sicherheits- und Verteidigungsindustrie.
SINA wird in enger Abstimmung mit der Bundeswehr und der BWI kontinuierlich weiterentwickelt, um auch künftigen Anforderungen gerecht werden zu können. secunet, seit 2004 IT-Sicherheitspartner der Bundesrepublik, kann dabei auf umfangreiche Erfahrung zurückgreifen. Als Kryptotechnologie made in Germany wird SINA auch weiterhin seinen Beitrag zur digitalen Souveränität Deutschlands erbringen.

D-LBO unter dem Aspekt der Digitalen Konvergenz

Horst Jonuscheit, Dipl.-Ing. Dipl.-Kfm., Vice President bei Saab Deutschland

Horst Jonuscheit

Foto: Saab

Einführung

Digitale Konvergenz wird vielfach verstanden als das Zusammenstreben von Informationstechnik (IT) und klassischen Produktportfolios bzw. Märkten. Diese Annäherung sollte den Kundennutzen von Produkten und Dienstleistungen fördern. Es ist keineswegs eine gerade entstehende Markt- oder Technologieentwicklung, vielmehr gehen Ansätze weit über zehn Jahre zurück.

Was bedeutet diese Entwicklung für den Nutzer Bundeswehr? In der heutigen Zeit erfordern Landes- und Bündnisverteidigung unstreitig die Interoperabilität sowie die Interkonnektivität von Systemen auf allen Befehlsebenen, auch nationenübergreifend. Gekapselte Teillösungen sind dabei ebenso wenig zielführend wie die fehlende Möglichkeit zum schnellen und sicheren Datenaustausch zwischen Systemen. Vernetzung bzw. Vernetzbarkeit einzelner Systeme ist heute eine regelmäßig zu erfüllende Forderung. IP-basierte Sprach- und Datenverkehre stehen im Fokus der Systementwickler wie auch der Nutzer.

Überblick Systemkonzept

Das Systemkonzept berücksichtigt Forderungen, die aus dem taktischen Einsatz abgeleitet werden. Heute bekannte Nutzerforderungen finden sich wieder; auf die Thesenpapiere des Kommando Heer „Wie kämpfen Landstreitkräfte künftig“ und „Digitalisierung von Landoperationen“ wird dabei verwiesen. Unser Augenmerk gilt vor allem der konzeptionellen Offenheit des Systems für die einfache Erweiterbarkeit hinsichtlich zukünftiger Forderungen. Daher betrachten wir Fähigkeiten und Funktionalitäten möglichst als Module. Die Konfigurierbarkeit dieser Module ermöglicht eine missionsbezogene Fähigkeitsoptimierung der Einsatzkräfte. Schnittstellenstandards tragen dazu bei, dass auch die Austauschbarkeit von Subsystemen unterschiedlicher Hersteller möglich wird, sofern die Hersteller die Standards unterstützen. Heute liegen Konzeptvorschläge für verschiedene mobile bzw. verlegefähige Module vor.

Saab verfügt über D-LBO relevante Produkte und Systeme, die aufgrund ihrer Architektur und Performance geeignet sind, die bekannten Kundenwünsche zu erfüllen. Flexibilität in der Auswahl von Subsystemen wird ebenso unterstützt wie die Umsetzung kundenspezifischer Systemkonfigurationen. Hierzu trägt speziell unser Command & Control-System 9CCIS bei, das durch seine “Secure Service Oriented Architecture” (SecureSOA) überzeugt. Diese Architektur ermöglicht den Aufbau eines „Secure System of Systems“ (SSoS) und stellt letztlich das Rückgrat für die Subsystemintegration. Aber auch unsere Subsysteme, z.B. der FmEloKa-Sensor CRS, folgen der Forderung nach Flexibilität und Konfigurierbarkeit, sind mehr „IT-System“ als klassischer „blackbox“ Sensor.

Command & Control-System

Saab hat sich durch jahrzehntelange Entwicklung und Lieferung zahlreicher C2-Systeme eine herausragende Expertise erarbeitet. Auch Projekte zur Digitalisierung von Streitkräften gehören zu diesem Erfahrungspool.

Heute steht bei Saab eine Technologie zur Verfügung, die wir als Secure System of Systems (SSoS) bezeichnen. Diese umfasst folgende Architektur und Tools:

- Secure Service Oriented Architecture (SecureSOA). Secure SOA ermöglicht eine netzwerkzentrierte Entwicklung und Integration, u.a. mit einem hohen Maß an Sicherheit, mit verteiltem Management, MIL-netzwerkfähig, unterstützt Bestandssysteme.
- Infrastruktur-Anforderungen
- Schnittstellen-Vereinbarungen
- Policies

In SecureSOA sehen wir eine gute Lösung, um komplexe und miteinander zu vernetzende Systeme sicher und wirtschaftlich zu realisieren und trotzdem flexibel zu sein zur Anpassung an neue Forderungen.

Das erfolgreiche Implementieren von SecureSOA erfordert das Vorhandensein und das Einhalten von Designprinzipien. Dazu zählen u.a. eine flexible, Mobilität unterstützende und dennoch Sicherheit gewährleistende Infrastruktur. Lose gekoppelte Komponenten der Infrastruktur bestehen nebeneinander und führen die spezifischen Aufgaben aus. Es ist möglich, diese Infrastrukturkomponenten neu zu konfigurieren. Die Komponenten selbst sind soweit möglich unabhängig voneinander designt. Die Unterstützung von ortsfesten aber auch mobilen Systemen, Netzwerken und Terminals wird erfüllt. Kosteneffizienz wird erreicht durch möglichst breite Verwendung von COTS-Produkten, Internetprotokollen bzw. –anwendungen sowie Netzwerkschnittstellen. Die Infrastruktur erfüllt Forderungen nach Interoperabilität verschiedener Systeme. Besondere Bedeutung kommt der sicheren Kommunikation zu.

Module und Funktionalitäten innerhalb des SecureSOA.

Grafik: Saab.

Lokalisierung gegnerischer mobiler Kräfte durch Peilung von Funksystemen. Tracking, Identifizierung der Trägersysteme et al. wird soweit möglich und automatisiert durchgeführt. *Grafik: Fraunhofer IOSB.*

Comms-ESM Sensor für den Elektronischen Kampf

Qualität und Vollständigkeit des Lagebilds werden maßgeblich von den angeschlossenen Sensoren bestimmt. Dies gilt vor allem für die Informationen und Erkenntnisse über die gegnerischen Kräfte. Im Rahmen des Elektronischen Kampfs können aus dem elektromagnetischen Spektrum wertvolle Informationen gewonnen werden. Konkret können mit Comms-ESM-Sensoren folgende wichtige einsatzrelevante Fragestellungen behandelt werden:

- Welche elektromagnetischen Emitter sind in einem bestimmten Gebiet aktiv?
- Welche Bedrohung stellen sie für die eigene Operation dar?
- Auf welchen Trägersystemen befinden sich solche Emitter?
- Was ist wohl der taktische Hintergrund für das elektromagnetische Lagebild bzw. wie ist die Lage?

Die heutigen deutschen Landstreitkräfte nutzen vor allem Erkenntnisse aus der abbildenden bzw. visuellen Aufklärung, unabhängig davon, ob die Aufnahmen von fliegenden oder fahrenden Plattformen stammen. Daneben ist der Beitrag von Spähtrupps als Beispiel für die Aufklärungskräfte des Heeres hervorzuheben, die mit oder ohne intelligente Sensorik wertvolle Informationen zum Einsatzgebiet und dem laufenden Kampfeinsatz gewinnen.

Eine direkte Informationsgewinnung aus dem elektromagnetischen Spektrum durch die Landstreitkräfte erfolgt weitgehend nicht. Das ist nachteilig, weil sich im Spektrum nämlich u.a. die gegnerische (wie auch die eigene!) Kommunikation abbildet, daneben tragen auch Radarsysteme zum Spektrum bei. Standortinformationen, taktische Informationen, Waffensysteme sind einige der bedeutenden Informationen über den Gegner, die aus Funkverkehren und durch Korrelation mit Grundlagenkenntnissen direkt bei den Landstreitkräften bestimmt werden könnten und sollten. Angemerkt sei, dass bei der Bundeswehr zumindest teilweise signalerfassende Aufklärung zum Einsatz kommt. Diese Systeme werden bis auf wenige Ausnahmen bei Marine und Luftwaffe vom KdoStratAufkl betrieben. Neben dem Beitrag zum Lagebild können die Ergebnisse aus dem Comms-ESM-System auch zur Einweisung anderer Sensoren, z.B. eines Kamerasystems, genutzt werden.

Saab bringt für diese Aufgabenstellung Systemkonfigurationen der Produktfamilie CRS ein, die von der deutschen Tochter Saab Medav Technologies aus Erlangen entwickelt werden. Die Architektur dieses Sensors ist bemerkenswert und wird als „Software Defined Intelligence Architecture“ zutreffend beschrieben. Dabei wird der Sensor aus COTS-Komponenten konfiguriert, die Datenverarbeitung erfolgt auf einer skalierbaren Anzahl von Servern. Die Funktionalität wird im Wesentlichen durch die per Konfiguration zusammengestellten Software-Module definiert. Es ist klar, dass damit funktionale Erweiterungen wie sie gerade in Zeiten des Software Defined Radio (SRD) als wichtiger Gegenstand der Aufklärung gefordert sind, einfach durchgeführt werden können. Auch die Verwendung der vorhandenen Hardwareplattform mit unterschiedlichen Software-Konfigurationen ermöglicht die optimale Missionsvorbereitung. Diese Eigenschaften gepaart mit der Möglichkeit der regelmäßigen, risikoarmen Erneuerungen der eingesetzten IT-Komponenten sichern Leistungssteigerungen ebenso wie die jederzeit „up to date“-Fähigkeiten des Sensors.

Zusammenfassung

Saab ist mit Forderungen zur Digitalisierung von Streitkräften gut vertraut, hat langjährige Erfahrung mit entsprechenden Aufgaben und Systemlösungen. Dabei ist es das Ziel, der Bundeswehr aber auch den BOS moderne, offene und leistungsfähige Lösungen anzubieten, die durch skalierbare und konfigurierbare funktionale Module ausgezeichnet sind. Moderne Systeme und Produkte im Sinne des Secure System of Systems (SSoS) sind auf Basis der Secure Service Oriented Architecture (SecureSOA) verfügbar.

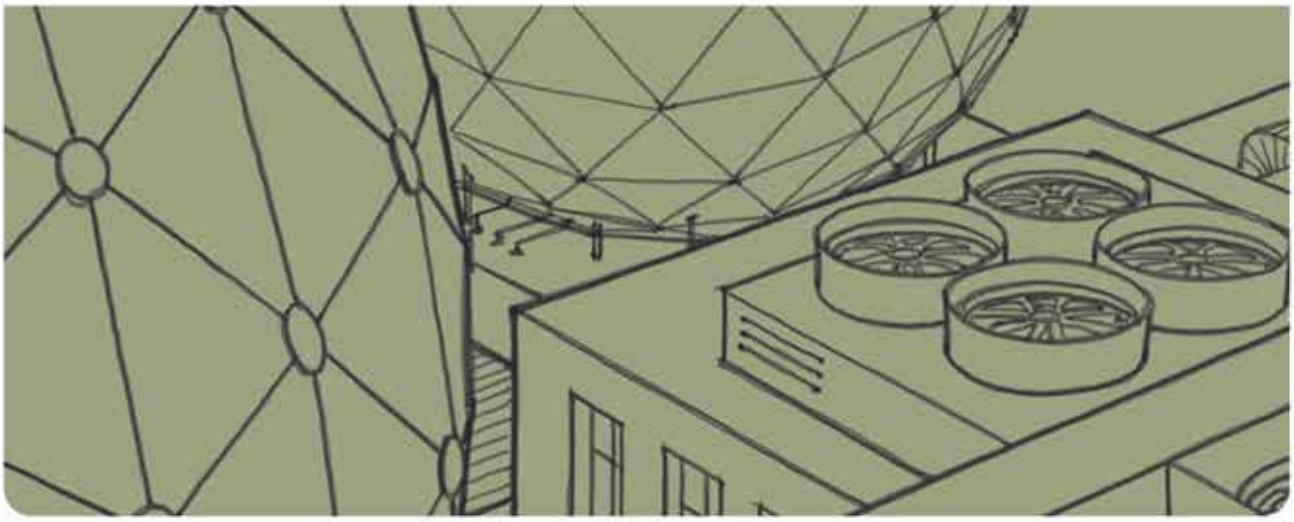
Ein wichtiger innovativer Beitrag stammt von der deutschen Saab-Tochter Saab Medav Technologies, die ein Comms-ESM-System für den Elektronischen Kampf der Landstreitkräfte als einen erheblichen und relevanten Fähigkeitsgewinn vorschlägt.

rola.
SECURITY SOLUTIONS

ZUSAMMENARBEIT STÄRKEN, SICHERHEIT SCHAFFEN.

33. AFCEA Fachausstellung Stand M26

- Aufklärungs- & Analysesoftware
- Lagebilderstellung im Cyber-Raum
- Grenzsicherung
- Gefahrenabwehr dank Biometrie & Objektidentifizierung
- Social Media Monitoring zur Risikofrüherkennung
- Anomaliedetektion durch Textanalyse & Maschinelles Lernen



www.rola.com | vertrieb@rola.com | +49 (0) 208 - 3066160

Künstliche Intelligenz: das KI-Potenzial im Alltag von BW und BOS nutzen

Wie rasant das Thema Künstliche Intelligenz (KI) Einzug in unser Leben hält, zeigen nicht nur digitale Assistenten wie Alexa und Co. Die zunehmende Bedeutung von KI eröffnet völlig neue Möglichkeiten in den unterschiedlichsten Anwendungsumgebungen. Genau das macht es so spannend.
Wie können sich alte und neue Welt annähern, voneinander profitieren und Synergieeffekte nutzen? Wie lässt sich das enorme Potenzial von künstlicher Intelligenz optimal nutzen, in den Berufsalltag einbauen, in globale Entwicklungen integrieren oder – ganz konkret: Wie können Bundeswehr-Einsätze im multinationalen Verbund davon profitieren? Gerade für Streitkräfte und BOS ergeben sich hier ungeahnte Mehrwerte.

Digitale Kompetenz und Defence-Erfahrung

CGI hat gemeinsam mit seinen Auftraggebern KI in den verschiedensten Bereichen umgesetzt und ist gleichzeitig langjähriger Dienstleister der Bundeswehr. Mit dieser Kompetenz wurden Lösungen entwickelt, die zum Beispiel im Bereich Krisenvorsorge schon heute effektive Unterstützung bieten können, indem Satellitenbilder mittels KI in Kartenmaterial umgewandelt werden. Im gleichen Kontext werden Machine-Learning-Ansätze genutzt, um im Rahmen der Terrorismus-Bekämpfung, Videostreams auszuwerten und die Analysten auf auffälliges Verhalten automatisiert hinzuweisen. So ist es beispielsweise innerhalb von HaFIS möglich, die klassischen C2-Services mit praxisorientierten KI-Funktionalitäten zu ergänzen.
Auch im Non-Defence-Bereich sind KI-Lösungen von CGI im Einsatz. Diese könnten schon heute eine intelligente Antwort auf zukünftige Anforderungen der Streitkräfte geben, zum Beispiel in der Digitalisierung des Gesundheitswesens, der Fernwartung von technischem Material im Einsatz oder der Personalrekrutierung. Ein Beispiel für den Gesundheitsbereich ist Sofia – ein Chatbot, der Patienten intelligent begleitet und als Gesundheitsassistent bei Krankheiten schnell Abhilfe verschaffen kann. Durch die Kombination von Datenanalyse und automatischer Bilderkennung ermöglicht künstliche Intelligenz in der Medizin, Krankheiten mobil zu diagnostizieren und schneller zu heilen. Im Produktionsumfeld hat CGI ein maschinelles Lernprogramm entwickelt, das hilft, Produktionsfehler zu identifizieren, Prozesse zu verfeinern und die Rentabilität zu verbessern. Der Mehrwert: Ein digitaler Assistent unterstützt den Menschen im Rahmen unterschiedlicher Prozesse als ständig hinzulernendes System, ohne seine finale Entscheidungshoheit in Frage zu stellen.
Neben den genannten Themenfeldern zeigt CGI insbesondere im regulatorischen und Compliance-Umfeld seine Expertise. Vor allem die zunehmende Kontrolle von Zahlungsverkehrsverhalten und die Überwachung der Kundenverhalten stellen Unternehmen vor eine besondere Herausforderung. Auch von regulatorischer Seite werden Unternehmen immer mehr in die Verantwortung genommen, bei Fehlverhalten drohen Strafen in Millionenhöhe. Als Lösung hierfür hat CGI ein Framework zur Analyse von Kundenverhalten und Fraud Prevention geschaffen. Mit Einsatz modernster Mittel wie künstlicher Intelligenz, Fuzzy Logic, Robotix und verhaltensbasierten Ansätzen wird der Prozess rund um die Prüfungen und die Bewertung des Hintergrunds eines Geschäftspartners gesichert.
CGI verfügt über mehr als 40 Jahre Erfahrung in der Beratung und Systemintegration für Erdbeobachtung, Navigation, Satellitensteuerung, Bodenkontrollsysteme, Flugdynamik sowie Datenspeicherung und -prozessierung. Der Fokus liegt hier auf kundenorientierten Lösungen mit entscheidender Bedeutung von Innovationen und Anwendungen neuer Technologien. Beispiele sind die Automatisierung von Satellitenkonstellationen, Satellitendatenverarbeitung mit KI oder moderne Cloud-Lösungen im Bereich Software as a Service (SaaS).

KI-Lösungen für Streitkräfte und BOS

Die CGI-Exponate auf der AFCEA-Fachausstellung zeigen, wie sich die digitale Gegenwart mit künstlicher Intelligenz verbinden lässt. Informieren Sie sich über Groupware, HaFIS, DokMBw auf Basis eGov360, Cybersecurity-Lösungen sowie Anwendungen im Bereich Space – ein Fähigkeitsbereich, der für die Bundeswehr zunehmend in den Fokus rückt.
Darüber hinaus erwartet Sie bei CGI auch eine sehr schmackhafte Anwendung von künstlicher Intelligenz in Form einer „Schokotyp-Beratung“. Neugierig? Dann auf zu Stand F09.

Weitere Informationen unter: ***www.de.cgi.com/de/defence***

Künstliche Intelligenz hat schon heute das Potenzial klassische C2-Services zu verbessern.

Foto: © CGI

Digitale Konvergenz in der Bundeswehr: Innovativ denken – effektiv transformieren

Michael Exner, Geschäftsführer der CONET Solutions GmbH

Michael Exner

Foto: CONET

Die Begriffe der Digitalisierung und digitalen Transformation geistern Zauberworten gleich durch jede aktuelle Diskussion um das Arbeiten und Wirtschaften der Zukunft. Hier unterscheidet sich die Bundeswehr grundsätzlich nicht von Gesellschaft und Privatwirtschaft.

Was aber ist unter dieser Digitalisierung eigentlich zu verstehen, beziehungsweise welche Ziele werden mit der digitalen Transformation verfolgt? Digitalisierung muss im Kern bedeuten, mithilfe digitaler Lösungen schneller und effektiver auf neue Anforderungen und Veränderungen reagieren und Lösungen flexibel auf neue Szenarien anpassen zu können.

Aber passt diese Prämisse auch zu den aktuellen Vorhaben und Zielsetzungen, die im Zusammenhang mit der Digitalisierung unternommen oder diskutiert werden?

Ende vergangenen Jahres war etwa in einem Magazinbeitrag von möglichen Einsätzen eines Digitalstifts zu lesen. So wertvoll dieser Ansatz zum Einsatz digitaler Technologien auch ist, illustriert er gleichzeitig das aktuelle Digital-Dilemma: Einzelne Technologien werden „entdeckt“, evaluiert und möglicherweise zukünftig auch eingesetzt. Sie bleiben aber dann allzu oft vereinzelt in ihrer Nutzung, das dahinterstehende Potenzial ganzheitlicher Lösungen wird nur selten erkannt, oder zumindest nicht konsequent verfolgt. Damit aber besteht die Gefahr, auch zukünftig – wie in weiten Teilen bislang – Einzelausschreibungen, Einzelbeschaffungen und Einzelvorhaben in Rüstung und IT getrennt voneinander und ohne den notwendigen Blick auf das Gesamtbild anzugehen.

Also geht es nicht ohne Innovation. Innovativ denken heißt einerseits, außerhalb der bisherigen Bahnen zu denken. Dies öffnet den Horizont für gänzlich neue oder zumindest erweiterte Möglichkeiten. Innovativ denken bedeutet aber auch, sich von bisherigen Vorgehens- und Denkweisen in der Beschaffung zu lösen.

Denn wenn die Digitalisierung auch schier unendliche neue Möglichkeiten zu bieten scheint, zwingt sie gleichzeitig dazu, in Ziel und Nutzen zu denken, statt in Technik. Innovativ denken meint daher im Wesentlichen, auch zielorientiert zu denken. Einige der ambitionierten Großprojekte der vergangenen Jahrzehnte liefen aufgrund ihrer Komplexität und ihrer zu vielen Vorgaben, Abhängigkeiten und Zielsetzungen in Schwierigkeiten. Um mit technischen Entwicklungen und sich ändernden Rahmenbedingungen Schritt halten zu können, ist mitunter eine bewusste Konzentration auf ganz konkrete Einsatzzwecke oder Zielszenarien angebracht: Eine einzige Lösung für eine einzige spezifische Aufgabe, denn der theoretisch denkbare und erreichbare Gesamtnutzen lässt sich in aller Regel nicht von Anfang an komplett abdecken.

Wie aber lässt sich dieser scheinbare Widerspruch zwischen dem notwendigen Blick auf das Gesamtbild und gleichzeitig einer sinnvollen Konzentration auf konkrete Zielsetzungen in einer erfolgreichen Umsetzung der Digitalisierung lösen?

Durch weitreichende Modularisierung, Standardisierung und entsprechende Kontrollmechanismen, die die Einhaltung von Kompatibilität und Standards sicherstellen!

Hier eröffnet sich ein weiteres zentrales Charakteristikum der Digitalisierung: Die digitale Transformation zwingt zur Kooperation. Kein Anwender, aber auch kein Anbieter von Lösungen kann sich heute noch alleine den digitalen Herausforderungen stellen. Angesichts rasanter technologischen Entwicklungen, beschränkter Haushaltsmittel und immer komplexeren Einsatzanforderungen ist es weder aus wirtschaftlichen, noch aus funktionalen Gesichtspunkten zielführend, neue Systeme als starres Ganzes aus einer Hand zu konzipieren, auszuschreiben und zu beschaffen. Wie die aktuelle Projektpraxis zur Genüge zeigt, hinken derartige Vorhaben aufgrund der oft langen Beschaffungszyklen und mitunter in der Zwischenzeit bereits veränderter Rahmenbedingungen den Anforderungen nicht selten hinterher.

Ein möglicher und in der Wirtschaft etwa in Fahrzeug- und Maschinenbau seit langem erfolgreich praktizierter Ansatz ist hier die Aufspaltung starrer Gesamtsysteme in modulare Komponenten, die sich dann flexibel zu einsatzspezifischen Lösungen kombinieren lassen.

Einem vergleichbaren Muster folgt derzeit erfolgreich beispielsweise das Projekt Mehrzweckkampfschiff (MKS) der Deutschen Marine. Eine einheitliche Plattform soll hier die Basis dafür bieten, mit einzelnen austauschbaren Missionsmodulen deutlich schneller und günstiger einsatzfähige Systeme für unterschiedliche Einsatzarten von Aufklärungs- und Kampfeinsätzen bis zur Nutzung als Lazarettschiff stellen zu können. Die bisherigen Konzeptionen und Entwicklungen weisen hier in eine viel versprechende Richtung.

Eine solche Modularisierung setzt wiederum eine entsprechende Standardisierung voraus, damit die einzelnen Systemkomponenten miteinander vollständig kompatibel und damit auch einfach austauschbar sind. Bereits bei der Ausschreibung ist es daher wesentlich, die Anbieter vollständig und bindend auf die Einhaltung entsprechend definierter formalisierter Anforderungen zu verpflichten – mitunter auch gegen Widerstände, da Hersteller naturgemäß zunächst in proprietären Lösungen denken.

Eckpunkte einer erfolgreichen Digitalisierung

Grafik: CONET

Effektiv transformieren bedeutet somit, sicherzustellen, dass einzuhaltende Vorgaben bereits projektbegleitend und erst recht abschließend strikt kontrolliert und eingefordert werden. Dies gilt für mechanische Bestandteile ebenso wie für die einzusetzende Informationstechnologie. Historisch bedingt sind „traditionelle“ Rüstungsvorhaben und IT-Vorhaben weitgehend getrennt und daher auch oftmals getrennt voneinander betrachtet, geplant und ausgeschrieben worden. In Zeiten einer zunehmenden Vernetzung, die alle Bereiche, Liegenschaften, Materialgattungen, Waffensysteme und Prozesse durchdringt, ist dies aber nicht länger ein gangbares Vorgehen. Wenn immer mehr Informationssysteme, Sensoren und Medien miteinander zusammenwirken müssen, um ein möglichst vollständiges und den klassischen ebenso wie asynchronen und Cyber-basierten Bedrohungsszenarien angemessenes Lagebild zu gewährleisten, müssen auch die entsprechenden Beschaffungen integriert und aufeinander abgestimmt konzipiert werden.

In die Zukunft gerichtet, stellt sich hier zudem die Frage, wie die weitere Ausgestaltung dieses Modulcharakters konsequent weiterverfolgt werden kann. Im Idealfall richtig zu Ende gedacht lösen sich IT-Anwendungen beispielsweise dem App-Gedanken folgend vollständig von der darunterliegenden Hardware. Denn ist die eingesetzte Basis immer dieselbe oder zumindest gänzlich offen gestaltet, ist nichts schneller und einfacher ausgetauscht, aktualisiert und an neue Gegebenheiten angepasst, als die entsprechende Software.

Als Unterstützung im Anforderungsmanagement und zur Erfassung, Definition, Dokumentation und Kontrolle von Systemkomponenten und Standardelementen bietet sich dabei die Architekturmethode als zentrales Werkzeug an. Richtig angewendet sorgt das Architekturmanagement für einen vollständigen Überblick über alle eingesetzten Systeme, Schnittstellen, Abhängigkeiten und Einsatzszenarien. Konzeptionell lassen sich so Berührungspunkte erkennen und Schnittstellen definieren, doppelte Entwicklungsaufwände vermeiden und letztlich auch die Einhaltung konzeptioneller und technischer Vorgaben prüfen. Insbesondere in die Richtung einer erweiterten Modularisierung und der oben angesprochenen Software-Betonung gedacht, ist dies unerlässlich, um die Austauschbarkeit und eine reibungslose Orchestrierung der einzelnen Komponenten miteinander zu ermöglichen.

Werden die Zielsetzungen Modularität, Standardisierung und Kontrolle im Beschaffungsprozess konsequent verfolgt, werden als überschaubare Vorhaben mit klaren Aufgaben und Zielsetzungen konzipierte scheinbare Einzellösungen letztlich nichts Anderes als in neuen oder komplexeren Szenarien einfach wiederverwendbare und austauschbare Module. Allerdings viel schneller, zielorientierter und damit wirtschaftlicher erstellt als ein überkomplexes Gesamtsystem in einem Wurf. Es geht also weniger um die Vermeidung von Silos, als vielmehr um eine von vorn herein offene und durchlässige Gestaltung dieser Einzellösungen.

Innovativ denken bedeutet damit ein modularisiertes, anforderungsorientiertes Schnittstellendenken. Effektiv transformieren bedingt eine lückenlose und gewissenhafte Kontrolle der Vorgaben und entsprechende Umsetzung. Dann ist auch eine Unterscheidung zwischen „klassischen“ Rüstungsvorhaben und IT-Projekten endgültig obsolet, die technische Basis tritt in den Hintergrund, allein die Zielsetzung bestimmt die Beschaffung. So lässt sich das Potenzial der Digitalisierung wirkungsvoll und greifbar realisieren, ohne sich in einer Vielzahl scheinbar unüberschaubarer Szenarien zu verlieren.

Cyber Security Monitoring für die Marine

Andreas Beierer, Senior Manager Sales Cyber Security, Thales Deutschland

Andreas Beierer

Foto: Thales Deutschland GmbH

Ein Sicherheitsaspekt, der in Zeiten der alles durchdringenden Digitalisierung und Vernetzung auch für Schiffe eine zunehmend wichtige Rolle spielt, ist die Cybersicherheit.

Im Hinblick auf Marineplattformen ist besonders kritisch, dass Angreifer sich Zugang zur Schiffs-IT verschaffen und so Zugriff auf Sensoren, Effektoren und Steuerungssysteme bekommen könnten. An Bord wird heutzutage via Smartphone über das Internet nach außen kommuniziert. Diese private Kommunikation muss vollständig von der Kommunikations-Infrastruktur des Schiffes isoliert sein, um Angriffe etwa über verseuchte Mails oder manipulierte USB-Sticks auszuschließen.

Es sind Szenarien denkbar, bei denen so mit vergleichsweise geringem Aufwand von Staaten oder Organisationen Angriffe auf Kriegsschiffe erfolgen, ohne dass diese ihrerseits ein einziges Kriegsschiff oder über ein einziges ausgebildete Kampfkräfte verfügen.

Potentielle Angriffsvektoren und Risikofaktoren

Hier folgt eine Zusammenstellung der potentiellen Angriffsvektoren in der Reihenfolge der Kritikalität.

1. Das FüWES (Führungs- und Waffeneinsatzsystem), bestehend aus Sensoren, CMS (Combat Management System), Feuerleiteinrichtung und Effektoren, kommuniziert über ein isoliertes Netz. Angriffsrisiken bestehen über Shared-Server-Systeme oder Maintenance-Zugänge.
2. Antriebsmotoren, Ruderanlagen und E-Generatoren
3. Schiffsautomationsanlagen
4. SATCOM-System
5. Navigationssystemen: Der Angriff erfolgt beispielsweise über GPS-Spoofing zur Vortäuschung von Positionsdaten.
6. Das Key Managementsystem für die Authentifizierung der Kommunikationspartner wird angegriffen. Dabei werden Zertifikate und kryptographische Schlüssel entwendet bzw. missbräuchlich mit dem Ziel der Informationsabschöpfung zum Einsatz gebracht.

Im Folgenden sind die wesentlichen Risikofaktoren angeführt, die häufig die Ursache für einen Angriff oder eine Kompromittierung der Bordinfrastruktur darstellen.

- Der Einsatz erfolgt zunehmend in multinationaler Kommunikationsumgebung. Bei Manövern wird hier die übergreifende Kommunikation zwischen den NATO-Ländern vorausgesetzt. Selbst bisher völlig isolierte Netze müssen für diese Anforderungen externe Schnittstellen bieten.
- Der Risikofaktor „Mensch“: Die Angriffe erfolgen über das „Social Network“ oder über das Kompromittieren von privaten Smartphones. Potentielle Bedrohungen gelangen so in das Bordnetz.
- Maintenance Schnittstellen in der Off-Board-Kommunikation und die damit verbundene unberechtigte Nutzung von Fernwartungszugängen zum Einschleusen von Schadcodes.
- IT-organisatorische Mängel, die durch das strikte Einhalten von Regeln und einem Risiko Management nach der ISO 31000 zu vermeiden sind.
- Einsatz von nicht mehr durch Updates unterstützten Software-Versionen / Betriebssystemen (zum Beispiel Microsoft Windows XP)
- Unkontrolliertes Patch-Management
- Veraltete Virenschutz-Software
- Nicht autorisierter Zugang zu Systemen z. B. durch unsachgemäßes BIOS-Kennwort

Präventives Monitoring: „Malware Detection System“ für das laufende Scanning und die Überwachung der Kommunikationsverbindungen

Das Thales Malware Detection- und Analyse-System scannt automatisch und völlig rückwirkungsfrei den ausgehenden Datenverkehr auf Anomalien. So werden bereits in der Vergangenheit erfolgte Angriffe auf die Infrastruktur des Schiffes in Echtzeit erkannt. Die Gesamtsituation aller gescannten Netzwerksegmente wird nach einer Analyse durch Cyber-Experten ausgewertet und in einem übersichtlichen Report dem Chief Information Officer (CIO) an Bord vorgestellt.

Herkömmliche Tools zur Netzwerksicherheit überwachen hauptsächlich nur den eingehenden Internetverkehr (über Sandbox, Firewalls, Antivirus usw.). Die Thales-Lösung zur Erkennung böswilliger Bedrohungen konzentriert sich ausschließlich auf die Überwachung des ausgehenden Datenverkehrs und erkennt, welche der installierten klassischen Schutzeinrichtungen wie z. B. Firewalls möglicherweise keinen ausreichenden Schutz bieten.

Das Malware Detection System von Thales besteht aus zwei Komponenten:

1. „Thales Probe“ – in separierten Netzwerksegmenten kommen häufig mehrere ‚Probes‘ zum Einsatz.
2. Der Malicious Threat Detector (MTD) ist einmal zentral im Netz vorhanden.

Thales „Probe“ extrahiert Meta-Daten aus dem Netzwerkverkehr (gespiegelte / SPAN-Daten) und transportiert diese zum MTD. Die Thales „Probe“- / MTD-Architektur ist Plug-and-Play und erkennt bösartige Inhalte oder Datenkonstellationen, die auf einen Angriff deuten, indem durch die „Probe der Netzwerkverkehr in Echtzeit für die gesamte Kommunikation mit dem Internet überprüft wird.

Die Thales Malicious Threat Detection konzentriert sich auf die Eigenschaften der ausgehenden Kommunikation von Mal-

ware, die sich auf Geräten und Netzwerken selbst installiert hat. Diese Methode bietet eine genaue Übersicht über erweiterte oder gezielte Angriffe (Advanced Persistent Threat = APT) und Malware, die durch die Firewall Systeme in das Bordnetz gelangt sind. Darüber hinaus erfolgt eine Benachrichtigung, wenn ein Gerät infiziert oder bösartiges Verhalten im Netzwerk erkannt wird (Port Scan, PAT Reversal, Heartbeat usw.).
Abschließend zur Echtzeiterkennung werden vom Thales Malware Detection System auch Angriffe detektiert, bei denen die Malware bereits vor Tagen, Wochen oder sogar Monaten in das Bordnetz eingebracht wurde.

Zusammenfassung:

- Angriffe über die Maintenance-Schnittstellen können zentrale Systeme (Führungs- und Waffeneinsatzsystem) und die Schiffsautomation stören oder außer Betrieb setzen.
- Risikofaktor „Mensch“ – über von der Mannschaft genutzte soziale Netzwerke gelangen Angreifer in das Bordnetzwerk.
- Wichtig ist ein präventives Monitoring der Kommunikationsschnittstellen und Netzwerksegmente, um Angriffe frühzeitig zu erkennen.

Digitale Konvergenz braucht Security-by-Design

Marc Akkermann, Leiter des Hauptstadtbüros und Leiter der Geschäftsfeldentwicklung bei infodas

Marc Akkermann

Foto: privat

Digitale Konvergenz,

also das Zusammenwachsen von zuvor getrennten Marktbereichen, Produktportfolios und/oder Wertschöpfungsketten durch Digitalisierung, ist in nahezu allen Bereichen der öffentlichen Hand und der Privatwirtschaft eine notwendige Konsequenz aus der technologischen Entwicklung und dem gesteigerten Bedarf an Integration von IT-Systemen und -Prozessen.

In generell eher IT-affinen Segmenten ist die digitale Konvergenz als notwendig akzeptiert und gleichzeitig sehr weit fortgeschritten (z.B. Telekommunikation, Medien, Entertainment).

Andere Industrien, vor allem die so genannte „Old Economy“, aber insbesondere auch der Bereich Sicherheit und Verteidigung erfahren seit einigen Jahren erst eine Konvergenzbewegung, die sich langsam aber sehr stetig beschleunigt.

Der BDSV e.V. hat den Ausschuss „Digitale Konvergenz“, zu dem an anderer Stelle in diesem Heft berichtet wird, gegründet, um diese Entwicklung im Kundensegment und bei seinen Mitgliedsunternehmen zu begleiten. Auch die Kooperation mit AFCEA wird genau aus diesem Grund weiter gestärkt.

Ein wesentliches Thema bei der zunehmenden Digitalisierung und der damit einhergehenden Konvergenz ist das gesamte Spektrum der Informationssicherheit. In früheren Zeiten war es oft üblich, Systeme zu entwerfen und zu realisieren und dann kurz vor oder sogar nach Inbetriebnahme IT-Sicherheitsaspekte zu betrachten.

Informationssicherheit in Gänze (also auch Aspekte, die über die technische IT-Sicherheit hinausgehen) spielte oftmals eine sehr untergeordnete Rolle.

Auch heute noch ist in vielen Projekten die Informationssicherheit nicht „von Anfang an dabei“, was letztlich zu erhöhten Projektrisiken und -kosten führen kann.

Ein Beispiel für Digitale Konvergenz ohne ausreichend betrachtete Sicherheit ist der Themenkomplex „Smart Home“. Hier wurden von vielen Anbietern die Möglichkeiten der Technik – insbesondere im Bereich des Internet of Things (IoT) – genutzt, ohne die Risiken ausreichend zu analysieren, was eine Fülle an Sicherheitslücken und -vorfällen produziert hat.

Im Umfeld von Sicherheit und Verteidigung spielt die Informationssicherheit von je her eine zentralere Rolle; in Teilen durch die gewählte Umsetzung sogar eine zu restriktive.

Historisch waren die Entwickler („Macher“) oft ein anderes Lager als die IT-Sicherheit („Verhinderer“). Selbstverständlich ist dies ein Stereotypen-Denken, das etwas übertreibt, aber auch den Bedarf des Umdenkens unterstreicht.

In zukünftigen Projekten, welche unter den Rahmenbedingungen des Plattformgedankens für (auf verschiedensten Ebenen konvergenten) Organisationen und Architekturen durchgeführt werden, ist es zwingend erforderlich, die Anforderungen an Informationssicherheit „auf Augenhöhe“ mit zu betrachten.

Es ist somit unerlässlich, dieses Thema in allen Phasen des Lebenszyklus eines Systems „mitzudenken“ und auf allen Ebenen von Anfang an umzusetzen; also:

Security-by-Design.

Das Ergebnis von Security-by-Design sind Produkte, denen die IT-Sicherheit nicht im Nachhinein „übergestülpt“ werden muss.

Statt dessen wird sie bereits konzeptionell integriert. Das bedeutet, dass auch Fehlbedienungen, Fehlfunktionen, menschliche Irrtümer und technisches Versagen nicht nur berücksichtigt, sondern geradezu erwartet werden.

Das Gesamtsystem wird deshalb so konzipiert, dass auch im Ausnahmefall – egal wie wahrscheinlich – die Sicherheitsziele nicht verletzt werden (können). Dies ist erforderlich, um der steigenden Bedrohungslage und der Vielzahl an heute vielleicht noch unbekannten Risiken entgegen zu wirken.

Unlängst wurden Spionage-Chips auf Komponenten für IT-Systeme öffentlich diskutiert. Trotz Zweifel am konkreten Einzelfall, zeigen die Berichte, dass Angriffe auf IT-Systeme und -Nutzer auf allen Ebenen erfolgen (können).

Unsere IT-Systeme sind also täglich einer Vielzahl an Bedrohungen ausgesetzt. Die genutzten Angriffsvektoren variieren dabei von benutzerzentrierten Ansätzen (z. B. Phishing) über die „klassische Schadsoftware“ (Viren, Malware, Trojaner) bis hin zur Hardware-Ebene.

Bei Angriffen direkt auf Hardware-Schwachstellen werden zum einen Design-Fehler ausgenutzt, zum anderen aber auch bewusste Manipulationen an verschiedensten Komponenten vorgenommen.

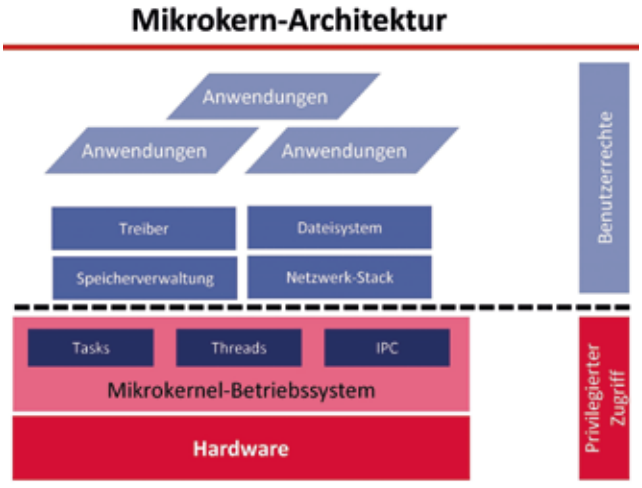
Dies ist insbesondere ein Risiko, weil die Lieferketten der meisten IT-Systeme nicht vollends kontrollierbar sind.

Die Themen „Digitale Souveränität“ und „vertrauenswürdige IT“ sind somit in diesem Kontext zu betrachten und in Teilen neu zu diskutieren. Ein Format, in dem dies getan wird, ist der Gesprächskreis 4 des Dialogs zwischen BMVg, BDSV und dem bitkom.

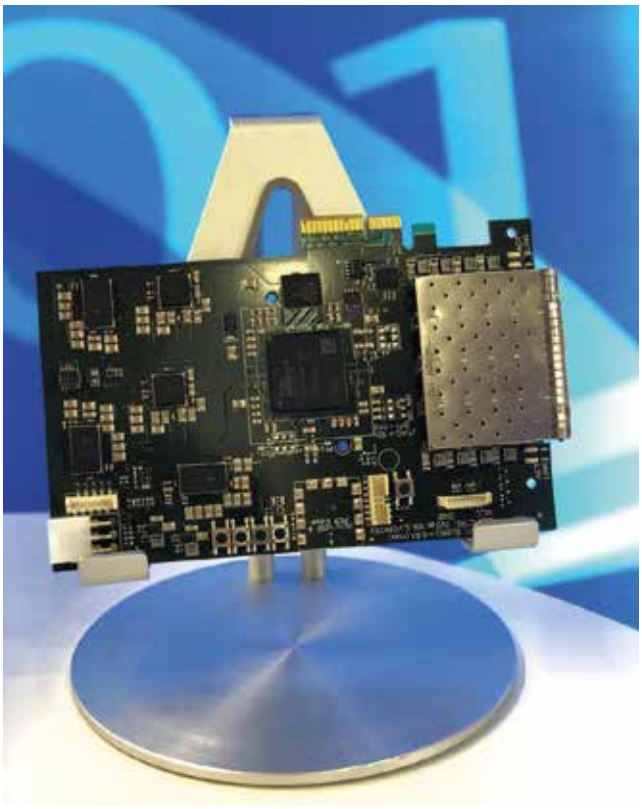
Es gibt durchaus unterschiedliche Ansätze, die das Prinzip von Security-by-Design unterstützen können, wie nachfolgende Beispiele zeigen:

Beispiel – Betriebssystem

Die zunehmende Vernetzung von Infrastruktur, Geräten und Maschinen im Zuge des IoT stellt Unternehmen und Sicherheitsbehörden vor eine völlig neue Herausforderung.
IoT-Systeme nutzen meist Betriebssysteme, wie sie auf Servern, Arbeitsplatzrechnern und Smartphones verbreitet sind. Diese haben z.T. veraltete Sicherheitsfunktionen und werden insbesondere im IoT-Umfeld regelmäßig nicht gepatcht, weswegen alte/bekannte Zero-Day-Attacken oftmals noch möglich sind.
Das Problem im Ursprung: Diese Betriebssysteme basieren auf Millionen von Codezeilen. Fehler und Sicherheitslücken sind deshalb nicht vermeidbar. Ein weiteres Kernproblem der Betriebssysteme ist die monolithische Struktur: Der wesentliche und größte Teil des Betriebssystems versteht sich als eine Einheit und verfügt über umfangreiche Zugriffsrechte auf Prozessor, Arbeitsspeicher und Peripherie. Wird eine Teilkomponente „gehackt“, ist meist das gesamte Betriebssystem kompromittiert. Monolithische Betriebssysteme sind daher prinzipiell unsicher.
Ein sicheres Betriebssystem verfügt über einen Mikrokern. Im Mikrokern laufen nur unbedingt notwendige Funktionen im so genannten privilegierten Modus. Diese Funktionen erhalten damit Vollzugriff auf alle Hardware-Komponenten.
Alle weiteren Funktionen, die für ein Betriebssystem notwendig sind, erhalten nur eingeschränkte Rechte. Damit lässt sich die monolithische Struktur aufheben.
Ein weiterer Vorteil des Mikrokerns: Eine lückenlose und intensive Kontrolle aller Funktionen des Betriebssystems ist möglich. Dies ist die Voraussetzung für eine Evaluierung, wie sie für einen Zertifizierungsprozess bspw. nach „Common Criteria“ notwendig ist. Die INFODAS GmbH hat mit nationalen Partnern ein Produkt „Made in Germany“ entwickelt – SDoT MOS (Secure Domain Transition – Microkernel Operating System), das auf einem Opensource-Mikrokern L4 basiert.



Mikrokern-Betriebssystem *Grafik: infodas.*



Sichere Netzwerkkarte *Grafik: infodas.*

Beispiel – Hardware

Spätestens seit den Enthüllungen von Edward Snowden ist bekannt, dass sich auch Hardware-Systeme im Inneren einer IT-Infrastruktur unbemerkt (vor und nach Auslieferung) manipulieren lassen. Das System bekommt so gar nicht mit, wenn die Netzwerkkarte „mehr macht, als sie soll“.
Behörden und Unternehmen können ihre sensiblen Daten in einem solchen Szenario schützen, indem sie Netzwerkkarten nutzen, die möglichst keine Angriffsflächen bieten.
Auch hierzu hat die INFODAS GmbH mit nationalen Partnern eine solche sichere Netzwerkkarte „Made in Germany“ entwickelt. Zentraler Baustein der Karte ist ein nicht-manipulierbarer Chip mit einem Field Programmable Gate Array (FPGA). Diese sichere Netzwerkkarte kann sowohl im Client- als auch im Serverbereich eingesetzt werden.

+++ News: SDoT Diode erhält zusätzlich zur Zulassung GEHEIM nun auch das Approval für NATO SECRET und EU SECRET. Details unter https://www.infodas.de/category/mitteilungen/ +++

Neuronale Netze, maschinelles Lernen, kognitive Systeme – Die Zukunft hat schon begonnen

Marco Kullmann, Hauptabteilungsleiter im Geschäftsbereich Spectrum Dominance von HENSOLDT

Marco Kullmann

Foto: Hensoldt

Die für viele militärischen Anwendungen entwickelten Sensoren, ganz gleich, ob Raketenwarner, EW-Sensoren, Radare oder Nachtsichtkameras, müssen unter den verschiedensten, und oftmals wechselnden Bedingungen Höchstleistungen erbringen. In vielen Fällen hängen davon Menschenleben ab. Unter Umständen ist vor einem Einsatz nicht einmal die Art der Bedrohung bekannt, denn das Einsatzumfeld verändert sich mit geradezu atemberaubender Geschwindigkeit. Um in diesem Umfeld die Nutzer der Systeme optimal zu bedienen, müssen die Produkte flexibler und reaktionsschneller werden und vor allem komplexe Situationen selbstständig analysieren und bewerten.

In der zivilen Welt wurden auf dem Forschungsfeld des „Deep Learning“ innerhalb der letzten Jahre massive Fortschritte erzielt. Dabei werden die Rohdaten eines Sensors in einem neuronalen Netz mit tief verschachtelten „Schichten“ von zunehmender Detaillierungstiefe angeordnet und – in Anlehnung an die Informationsverarbeitung des menschlichen Gehirns – ausgewertet.

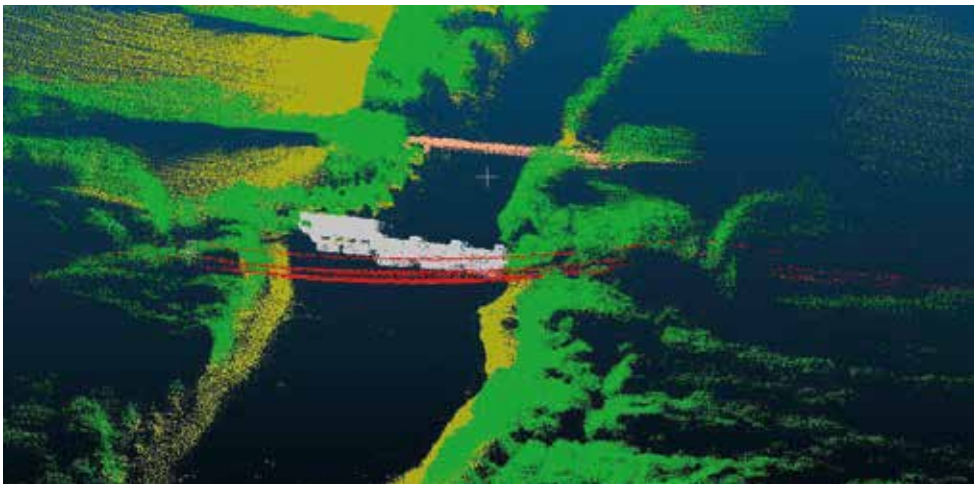
Diese neuartigen tiefen neuronale Netze sind in vielen Anwendungsfeldern, wie z.B. bei Internet-Suchmaschinen und in der Bild- oder Handschrift-Erkennung, bereits im Einsatz. Ein wesentlicher Treiber dieser Technologie sind z.B. die neu entwickelten autonomen Fahrsysteme, oder Serviceroboter, die Menschen bei alltäglichen Dienstleistungen helfen sollen. Durch die Verfügbarkeit moderner, hochleistungsfähiger Rechner sind die komplexen Strukturen dieser Netze erst möglich und alltagstauglich geworden.

Die Übertragung dieser Technologien auf militärische Anwendungen ist eines der zentralen Themen in der Technologieforschung bei HENSOLDT. In Kooperation mit Universitäten und dem Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE wird der neue Ansatz aus der Welt der Digitalisierung verfolgt: kognitive, also selbstlernende Systeme werden in naher Zukunft die Grundlage praktisch des gesamten Produktportfolios von HENSOLDT bilden. Im Vordergrund steht die Entwicklung einer Kern-Software, die es Sensoren ermöglicht, Einsatzerfahrungen und Trainingsbeispiele auf neue Situationen zu übertragen und aus Fehlern zu lernen. Der Vorteil ist, dass ein solches kognitives System flexibler reagieren kann und dass die Rahmenbedingungen nicht zuvor von Entwicklern in jedem Detail mühsam spezifiziert werden müssen.

HENSOLDT ist mit diesem Thema an der vordersten Front der Technologieentwicklung tätig und wendet diese Verfahren bereits auf mehreren Gebieten erfolgreich an. So wird für Pilotenassistenzsysteme für Hubschrauber ein Deep Learning-Netzwerk zur Hinderniswarnung eingesetzt. Das Netz lernt aus einer großen Menge aufgezeichneter Daten eines LIDAR Sensors Objekte wie Hochspannungsmasten und Leitungen, Gebäude, Bäume und sonstige Hindernisse selbständig zu erkennen (s. Foto). Hierbei konnten Forschungsergebnisse aus dem Bereich des autonomen Fahrens übernommen und auf den militärischen Anwendungsfall angepasst werden. So können z.B. Hochspannungsmasten auch dann erkannt werden, wenn sie durch andere Objekte teilweise verdeckt sind oder nicht dem in Deutschland gebräuchlichen Typus entsprechen.

In einem weiteren Anwendungsfeld erkennt ein Sensor der Elektronischen Kampfführung (EloKa) im elektromagnetischen Spektrum anhand spezifischer Muster, welche feindlichen Einheiten sich im Einsatzraum aufhalten, welche miteinander kommunizieren oder ob Signale zum Zünden von Straßenbomben darunter sind, und entwickelt Lösungsvorschläge für die jeweilige taktische Situation. Das ist besonders wichtig in Einsatzräumen, in denen die Dislozierung und Ausrüstung feindlicher Kräfte nicht bekannt ist, so dass die bisher übliche Vordefinition von Bedrohungen in speziellen Datenbanken an ihre Grenzen stößt. Hier bringen uns selbstlernende Systeme einen entscheidenden Schritt weiter. Es geht dabei nicht nur darum, bekannte Muster in einer Menge von Rohdaten „wiederzuerkennen“, sondern auch in Rohdaten aus unbekannten Szenarien neue Zusammenhänge und Gesetzmäßigkeiten zu entdecken. Auch hier werden Deep Learning-Netze eingesetzt. Die Architekturen der Netze leiten sich direkt aus denen z.B. zur Bilderkennung verwendeten Netze ab. Die Wiederverwendung geht sogar so weit, dass die im Rahmen der Bilderkennung trainierten ersten Netzwerkschichten direkt beibehalten werden können.

Die „Lernfähigkeit“ besteht darin, dass der Sensor basierend auf einer Vielzahl von Rohdaten Muster erkennt, die er nach einer vorangehenden Trainingsphase einer Bedrohung zuordnen kann. Im Unterschied zu bisherigen Verfahren, die auf heuristischen, von menschlichen Experten fest vorgegebenen Merkmalen beruhen, „lernt“ das System Muster und Gesetzmäßigkeiten direkt aus den Rohdaten selbstständig anhand einer sehr großen Anzahl von repräsentativen Beispieldaten. Kognitive Systeme und Deep Learning sind neue Techno-



Aus einer großen Menge aufgezeichneter Sensordaten lernt ein Hinderniswarnsystem für Hubschrauberpiloten Objekte im Flugweg selbstständig zu erkennen. *Grafik: Hensoldt*

logien, mit denen zukünftige Produkte die Kunden bei der Erfüllung seiner Mission unterstützen. HENSOLDT greift die neuesten Technologien auf, um mit innovativen Produkten die Nutzer bei der Erfüllung ihrer Aufgaben auch in den immer schneller wechselnden Szenarien der Gegenwart noch besser zu unterstützen.

Gemeinsame Wege in die Digitale Zukunft

Michael Dreher, Direktor Geschäftsbereich Verteidigung, IBM Deutschland

Michael Dreher

Foto: Aperto, staat-digital.de

Für die Landes- und Bündnisverteidigung einer Informationsgesellschaft muss die Bundeswehr vorausschauend handeln. Die Digitalisierung nimmt dabei einen besonderen Platz ein. Sie bietet Chancen wie zum Beispiel zur besseren Lageeinschätzung oder Optimierung der Einsatzfähigkeit und birgt zugleich Gefahrenpotential. Denn keine Organisation und kein anderes Land verzichtet auf die Kraft der digitalen Möglichkeiten. Damit wächst die Gefahr von Störungen, Gefährdungen und Cyberangriffen.

Ausgehend von der Befähigung des Menschen, über die Prozesse, bis zum Material – wir erarbeiten Lösungsvorschläge, robuste und resiliente Infrastrukturen und antworten auf die Frage der zunehmenden Datenflut. Ich sehe die Aufgabe der IBM nicht nur darin, informationstechnische Lösungen und Bundeswehr einander anzunähern, sondern vielmehr darin, als Integrator die technologische mit der militärischen Welt zu verschmelzen.

Diese Vernetzung befähigt die Bundeswehr dazu, Herausforderungen wie die der hybriden Kriegsführung, dem transnationalen Terrorismus und Cyberattacken begegnen zu können. Intensiviert man die Zusammenarbeit zwischen Bundeswehr, Sicherheitsbehörden sowie Rüstungsindustrie und Technologieunternehmen, können wir gemeinschaftlich die Handlungsfähigkeit der Bundeswehr stärken und den Einsatzerfolg im digitalen Zeitalter sicherstellen.

Technologie als Treiber digitaler Konvergenz

Das Zusammenspiel von Militär und IT ist für eine zeitgerechte und effektive Aufgabenerfüllung der Bundeswehr wichtig. Wir streben eine gemeinschaftliche Erprobung und Implementierung innovativer Technologien an, die wir aus dem Bedarf der Bundeswehr, den außen-, sicherheits- und europapolitischen Interessen sowie den Bündnisverpflichtungen ableiten.

Daneben fließen auch technologische Fortschritte ein, die außerhalb des Verteidigungssektors entwickelt wurden und zukunftsweisenden Erfolg für die Bundeswehr versprechen. In unseren europäischen Laboren und im Watson-IoT-Center in München entstehen Innovationen in Bereichen wie künstliche Intelligenz (KI), Blockchain und „Internet of Things“-Plattformen.

Plattform-Ökosysteme verbinden Fahr- und Flugzeuge, Schiffe, militärische Systeme sowie Soldaten und integrieren Produkte, Services und Technologien der Bundeswehr.

Die erleichterte Interaktion zwischen Nutzern stärkt die Handlungsfähigkeit von Bundeswehr und Verbündeten. Ein Beispiel

Im Fokus: Nutzerzentrierte Digitalisierung

Foto: Colin Anderson Productions Pty Ltd.

dafür kann die europäische Streitkräfteintegration sein: Ungehindert kann im Einsatz auf Informations- und Kommunikationssysteme sowie Versorgungs- und Transportinfrastruktur zurückgegriffen werden.

Darüber hinaus werden Daten überall und zu jeder Zeit über Sensoren, Systeme und Secure Mobile Devices generiert. Alle Akteure und Geräte einer Plattform sind potenzielle Datenquellen. Sobald diese über eine sichere Plattform verbunden sind und wertvolle Informationen aus den Datenmengen extrahiert werden, entsteht Mehrwert zur Beurteilung der Lage im Einsatz und Grundbetrieb. Der Aufbau einer solchen IoT-Plattform ist essenziell zur Datensammlung und -speicherung sowie für analytische Verfahren über Datensilos hinweg.

Basierend auf dieser modular aufgebauten Plattform können anhand von KI-basierten Services Analyse-, Beurteilungs- und Führungsfähigkeit auf allen Ebenen gewonnen werden. Die Bundeswehr kann so mithilfe von KI Krisen und Konflikte frühzeitig erkennen, eindämmen und in entsprechenden Regionen für Deeskalation und Stabilität sorgen. Dabei spielt die Sprach-, Bild- und Textanalyse von bundeswehreigenen, nationalen sowie internationalen Daten eine zentrale Rolle. Als IBM stehen wir für einen Einsatz von KI, bei dem ersichtlich ist wie KI zu Empfehlungen kommt und welche Daten mit welchen Methoden analysiert werden. Für uns ist es selbstverständlich, dass Daten und abgeleitete Erkenntnisse der Bundeswehr gehören. Der Einsatz von KI ist dann sinnvoll, wenn der Mensch im Mittelpunkt bleibt. Denn es geht darum, die menschliche Intelligenz zu erweitern und den Menschen zu unterstützen – nicht darum, ihn zu ersetzen.

Zunehmende Kooperationen verschiedener Verteidigungsbündnisse und multilaterale Einsätze verlangen nach einer Sicherung von militärischen Systemen, Gefechtsständen und Lieferketten. Der Einsatz von Blockchain Technologie ermöglicht automatisierte und rechtssichere Transaktionen. Damit wird nicht nur eine Daten- und rechtliche Sicherheit realisiert, sondern auch die Reduzierung von Dokumentations- und Organisationsaufwand. Mit der Nutzung von Blockchain Technologie agiert die Bundeswehr als zuverlässiger Kooperations- und Bündnispartner, insbesondere im Hinblick auf strategische Verlegefähigkeit und global zu sichernde Lieferketten.

Sicherheit im Fokus

Als IBM legen wir beim Ausbau von Cyberfähigkeiten der Bundeswehr den Fokus darauf, die IT-Architektur der Sicherheitssysteme zu konsolidieren und resilienter zu gestalten.
Es gilt Fähigkeiten zu verbessern, um end-to-end-Sicherheitsprozesse und -lösungen zu etablieren, sowie die Befähigung zur Cyber-Lagebild-Einschätzung mithilfe von Security Intelligence und Advanced Analytics. Besonderen Fokus legen wir auf Sicherheitsanforderungen bei Plattformen mit steigender Nutzeranzahl und internationalen Akteuren: Bei innovativen Cyber-Sicherheitslösungen sind der Grundsatz „Secure by Design“, der Transaktionsschutz im mobilen Umfeld und das Management von Identitäten und Zugriffsrechten zu berücksichtigen. Darüber hinaus gewährleisten Identitätsprüfung und Identitätsüberwachung in Cloud-Diensten die Cybersicherheit in den bundeswehreigenen Netzen.

Der Weg zum Ziel

Die Bundeswehr ist mit einem Aufgabenspektrum konfrontiert, das sich kontinuierlich aktualisiert und verändert. Um diesen Anforderungen und internationalen Erwartungen gerecht zu werden, gilt es in Kooperation mit der Industrie flexibel auf Bekanntes und Unvorhersehbares zu reagieren. So wie IT-Innovationsquellen außerhalb des Verteidigungssektors existieren, stammen bewährte Methoden zur Produkt- und Anwendungsentwicklung aus der Software-Entwicklung: Wir nutzen Military Design Thinking zur Produkt- und Servicegestaltung. Diese agile Methode stellt den Nutzer in den Mittelpunkt von Gestaltung und Transformation, um stets dessen Anforderungen zu berücksichtigen. Wir werden in Kürze eine IBM Defense Garage in Bonn eröffnen, in der wir mit Ihnen unter Anwendung von Design Thinking Einflüsse auf Fähigkeiten und Wirkung der Bundeswehr beleuchten, Abteilungen verknüpfen und Konvergenzströme frühzeitig erkennen.
Erste Schritte in Sachen Digitalisierung und Orchestration von militärischen und nicht-militärischen Mitteln sind umgesetzt. Mit Technologien transformieren und führen wir Prozesse und Produkte zusammen, um die Bundeswehr zur Bewältigung der veränderten Anforderungen zu befähigen.
In diesem Zusammenhang versteht die IBM die Digitalisierung als keinen erreichbaren Zielzustand, sondern als einen andauernden Prozess. Technologien wie künstliche Intelligenz und hybrid Cloud entwickeln wir stetig weiter und stehen der Bundeswehr so als strategischer Partner zur Seite.
Damit die Bundeswehr adaptionsfähig bleibt, setzen wir uns für eine gemeinschaftliche Weiterentwicklung und Transformation für den erfolgreichen Kampf gegen Bedrohungen aus dem Cyber- und Informationsraum und gegen neuartige Gefahren hybriden Charakters ein.
Erfolgsfaktoren für eine Konvergenz sehen wir in der Förderung von industrie- und organisationsübergreifender Kommunikation. So ist der Innovationsgeschwindigkeit und internationalen Qualität der Cyberbedrohung nur mit globaler Zusammenarbeit zwischen Industrie, Forschung und Entwicklung zu begegnen. Wir fördern das explorative Testen der Wirkung von Innovationen und wenden agile Methoden mit Nutzerzentrierung an, um mit Ihnen auf veränderte Anforderungen passend zu antworten.

Weiterentwicklungsbedarfe für IT-Plattformen in der Nutzung aufgrund der fortschreitenden Digitalisierung

Dr. René Purainer, Leiter Systemintegration IT, ESG Elektroniksystem- und Logistik-GmbH

Dr. René Purainer

Foto: ESG

Von Digitalisierung im eigentlichen Sinn, nämlich dem Umwandeln von analogen Formaten in digitale Daten, zu sprechen, ist im Kontext mit der Bundeswehr sicherlich zu kurz gesprungen. Wenn wir einen Blick auf den soldatischen Alltag im Friedens- und Einsatzbetrieb werfen, ist festzustellen, dass immer noch sehr viel auf analoge Weise be- und erarbeitet wird. Vergleichen wir dies mit unserem privaten Umfeld, dann sind die Unterschiede mehr als deutlich. Digitalisierung bedeutet im privaten und auch im industriellen (zumeist nicht öffentlichen) Bereich eine Beschleunigung von Bearbeitungsprozessen und eine nahezu echtzeitnahe Bereitstellung von (erforderlichen) Informationen. Genau diese um ein Vielfaches beschleunigte Prozessbearbeitung mittels der Bereitstellung von adäquaten Informationen annähernd in Echtzeit ist Grundlage für die erfolgreiche Auftragserfüllung der Streitkräfte – sie muss noch stärker in den Fokus der Bundeswehr gerückt werden.

Der in diesem Artikel verwendete Begriff "IT-Plattform" soll wie folgt verstanden werden: IT-Plattformen sind Systeme, mit informationsverarbeitenden und informationsübertragenden Anteilen, die aus Hardware- und Basis-Software-Anteilen bestehen, auf denen Nutzeranwendungen betrieben werden.

Die aktuell in der Realisierung bzw. noch in der Planung befindlichen Programme wie D-LBO, German Mission Network (GMN) und deren Bezüge im internationalen Rahmen, wie die Vorgaben/Philosophie der NATO zu Federated Mission Networking (FMN) sind in diesem Zusammenhang als Beispiele aus dem militärischen Bereich zu erwähnen. Parallel zu diesen Projekten werden durch den Bund weitere Digitalisierungsprojekte vorangetrieben. Ob die dabei jeweils verfolgten Strategien zusammenpassen müssen oder können, ist noch nicht umfassend bewertbar. Richtig ist jedoch, das zum Beispiel die BWI mit Betätigungsfeldern im behördlichen und militärischen Umfeld sowie weitere Unternehmen mit Standbeinen auch im zivilen Sektor mit Ihren Erfahrungen zu einem Wissens- und Technologietransfer beitragen und so den Digitalisierungsprozess nachhaltig unterstützen können.

Mit Blick auf den Consumer-Markt ist festzustellen, dass neue technologische Möglichkeiten durch Unternehmen in neue Lösungen oder Geschäftsmodelle umgesetzt und den Kunden angeboten werden. Ob diese aber wirklich im Markt erfolgreich werden, zeigt sich erst in der Realität und ist meist direkt vom Mehrwert für den Kunden – auch unter Berücksichtigung des Preises – abhängig. Im Kontext der Streitkräfte ist die Frage nach dem Kunden und dem Mehrwert sicherlich deutlich komplexer und kann hier nicht weiter thematisiert werden.

Auf einer höherer Abstraktionsebene können aber einige Paradigmen aus der zivilen Welt im Zusammenhang mit der Digitalisierung auch als für die Streitkräfte gültig postuliert werden. Unter Berücksichtigung dieser Paradigmen kann eine erfolgreiche Weiterentwicklung von IT-Systemen gelingen:

- Vermeidung von Medienbrüchen
- Vermeidung von proprietären Schnittstellen
- Trennung von Hardware und Software im Sinne einer Hardwareunabhängigkeit
- Hardwareunabhängige Serviceverfügbarkeit
- Kontinuierliche Weiterentwicklung von Hardware und Software
- Nutzerbezogene Servicebereitstellung

Paradigmen für eine erfolgreiche Weiterentwicklung von IT-Plattformen

Grafik: ESG

Zunächst geht es darum, dass Daten medienbruchfrei von einem Ort zum anderen übermittelt werden können. Hier liegt eine Herausforderung, die es gezielt anzugehen gilt, in der Bereitstellung von Daten in mehreren Informationsräumen. Weiterhin ist die Vermeidung von proprietären Schnittstellen auf Hardware- und Software-Ebene ein wesentlicher zu bearbeitender Aspekt. Denn nur wenn offene oder einheitliche Schnittstellen und Datenaustauschformate zwingend vorgeschrieben werden, ist ein durchgängiger Datenverbund bzw. -austausch überhaupt erst sinnvoll möglich.

Hierdurch ergeben sich zwei Chancen: Zum einen möglichst viele Services auf wenigen (idealerweise einer) Hardwarekomponenten bereitzustellen (Konvergenz in der Kommunikationstechnik) und zum anderen eine relativ hohe Unabhängigkeit von der einzusetzenden Hardware zu gewährleisten. Allein die Komplexität in aktuellen Projekten, die sich mit der Regeneration von IT-Systemen auseinandersetzen, zeigt, dass die Umsetzung einer Hardwareunabhängigkeit vielfach noch nicht gelungen ist. Mit dem Wechsel einer Hardware-Komponente (Nachfolge- oder Alternativprodukt) fallen in der Regel Anpassentwicklungsaufwände an, die mit- bzw. gesondert beauftragt werden müssen. Eine Trennung der Hard- und Softwareschichten kann nicht vollständig vollzogen und somit die notwendige Verringerung der Komplexität nicht erzielt werden. Sowohl Sicherheitserfordernisse als auch der stetige Wandel hinsichtlich der Nutzbarkeit/Kompatibilität erfordern eine ständige Weiterentwicklung der Software. Die Prüfung der Einsetzbarkeit von neuen Versionen ist derzeit innerhalb jedes einzelnen Vorhabensn mehrfach zu leisten, was jedoch vermeidbar wäre, wenn die zuvor genannten Gesichtspunkte Anwendung fänden.

Zwei Teilaspekte sind bei der nutzerbezogenen Servicebereitstellung von Interesse. Auf der einen Seite die Möglichkeit einzelne Services zu erhalten, wenn diese benötigt werden und das ohne zeitaufwändigen Beantragungsvorlauf. Und auf der anderen Seite, die Fähigkeit der Services, sich auf verfügbare Hardware und Bandbreiten individuell anzupassen. Hier sei als Beispiel eine beliebige Anwendung zu nennen, die sowohl auf einem Client mit eigener, üppiger Grafik- und Prozessorleistung mit stabiler, breitbandiger Netzanbindung funktioniert als auch auf einem Tablet/Smartphone im Feld mit nur sehr eingeschränkter Netzanbindung. Mit Blick auf unser eigenes Smartphone und den PC zu Hause, stellen wir fest: „Das gibt es schon! Warum nicht im militärischen Umfeld?“ Eine Antwort kann sein: „Weil dort kein wirklicher „Käufermarkt“ existiert, was uns wieder zur Frage nach dem Kunden bringt.

Die digitale Konvergenz beschreibt, wie Technologien aus dem militärischen Umfeld und dem zivilen IT-Markt zusammen neue Lösungen generieren können, die einen Mehrwert für die Streitkräfte darstellen. Aus den Ausführungen zuvor wird ersichtlich, dass von der richtigen Idee bis zur Umsetzung innerhalb der Bundeswehr noch Zeit vergehen wird.

Was leitet sich daraus heute an Möglichkeiten des Handelns ab? Proprietäre Schnittstellen schotten Systeme ab. Selbst wenn der Kunde eine Veränderung bewirken will, wird dies durch proprietäre Schnittstellen noch allzu oft behindert. Die wehrtechnische Industrie kann sich jedoch stärker kundenorientiert aufstellen. Dies müssen die auch in zivilen Märkten agierende IT-Unternehmen zwingend tun, um ihre Existenz zu sichern. Eine Ausrichtung am Kunden könnte auch zum Beispiel durch die enge Zusammenarbeit innerhalb der integrierten Projektteams (IPT) erfolgen. Dies war beispielsweise einer der Schlüsselfaktoren dafür, dass ein Projekt wie der Gefechtsstand der Luftwaffe Mission Counter Daesh durch das Konsortium GSS+ (ESG Elektroniksystem- und Logistik-GmbH und steep GmbH) so erfolgreich umgesetzt werden konnte. Ein weiterer hervorzuhebender Erfolgsfaktor dieses Projekts ist die Schaffung eines IT-Systems, in dem ein durchgängiger Kommunikationsverbund aller relevanten Systemanteile geschaffen wurde, bei dem auch der Nutzer Design- und Produktentscheidungen wesentlich mitgestalten konnte. Diese Design- und Produktentscheidungen können dann auch wiederum in andere Systeme, die durch den Auftragnehmer betreut werden, übertragen werden.

Der auch im Kontext D-LBO vorgesehene Ansatz des „Spiral-Development“ wird also in diesem und anderen Projekten bereits in der Praxis gelebt. Der Soldat als Kunde erhält auf diese Weise stets neue Funktionen, natürlich unter Berücksichtigung aller weiteren Projektelemente. Mit dem Ansatz „vom Einfachen zum Komplexen“ gilt es nun die richtigen Weichenstellungen vorzunehmen, um die künftige Weiterentwicklung der IT-Plattformen auf Basis dieser positiven Erfahrungen und Erkenntnisse zielgerichtet und erfolgreich voranzutreiben zu können.

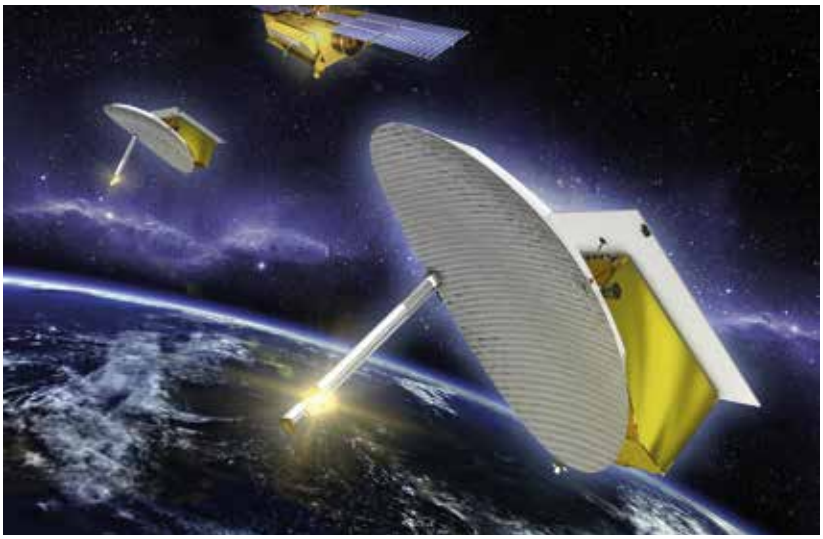
Der Gefechtsstand der Luftwaffe MCD als Beispiel im Kleinen für die erfolgreiche Anwendung der genannten Paradigmen

Fotos: Bundeswehr/Luftwaffe/Eduard Wagner

OHB System AG: Innovative Systemlösungen aus bewährter Hand

Thomas Jakob, Key Account Manager Verteidigung, OHB System AG

Die Raumfahrtgemeinschaft steht vor großen Herausforderungen beim Aufbau zukunftsweisender Satellitensysteme, im laufenden Betrieb und beim Schutz der Weltrauminfrastrukturen. Die Verfügbarkeit kritischer Weltrauminfrastrukturen ist in jedem Fall anhaltend und ausfallsicher zu gewährleisten.
Raumfahrtbasierte Lösungen der OHB System AG sind integraler Bestandteil solch kritischer Elemente für zivile und militärische Anwender und bereits zum alltäglichen Umgang geworden. OHB ist auf Komplettlösungen für Satellitensysteme für Telekommunikation, Navigation und Erdbeobachtung spezialisiert. Sie werden durch fortschrittliche Lösungen für luftgestützte Systeme ergänzt, wobei OHB Kernpartner im Vorhaben FCAS sein wird.



Künstlerische Darstellung SARah Konstellation *Foto: OHB System AG*

- Die Satellitenkommunikation wird mit der OHB-Produktlinie SmallGEO bedient. Der Satellit Hispasat H36W-1 mit flexibler digitaler Nutzlast ist seit mehr als einem Jahr störungsfrei in Betrieb. Die Heinrich Hertz-Mission mit ihrem SATCOMBw-Anteil, EDRS-C mit einer Laserkommunikations-Nutzlast sowie die vollelektrisch angetriebene Variante ELECTRA basieren auf dieser innovativen Plattform.
- Mit der Realisierung des H2SAT Bodensegments wird OHB in die Lage versetzt, eine komplette E2E Kommunikation anzubieten.
- Im Bodensegment hat OHB 2018 die Leistungsfähigkeit der Ankerstation Gerolstein um eine UHF-DAMA Fähigkeit für die Bundeswehr erfolgreich erweitert.

SmallGEO Satellit H36W-1 bei der Testkampagne

Foto: OHB System AG

- Das für die Bundeswehr entwickelte, hergestellte und betriebene System SAR-Lupe zur raumgestützten Radar-Aufklärung ist seit mehr als zehn Jahren im Einsatz und wird zukünftig durch das Nachfolgesystem SARah ergänzt und abgelöst werden.
- OHB realisiert den nationalen Hyperspektralsatelliten EnMAP, dessen Daten die Klassifikation von Landnutzungen und die Detektion von Anomalien auf der Erdoberfläche ermöglichen werden.
- Sechs MeteoSat Wettersatelliten der dritten Generation (MTG) und ein elektro-optisches System für die Bundesregierung ergänzen das Portfolio der OHB in der Erdbeobachtung.
- Durch die Beauftragung mit 34 Galileo FOC-Satelliten für die Europäische Union hat sich OHB auch im Bereich hochpräzise Positionierung, Navigation und Timing etablieren können.
- Neuartige kryptografische Systeme, die Orchestrierung von ad-hoc Netzen bei hohen Datenraten unter Zuhilfenahme von KI werden weitere künftige Handlungsfelder im Bereich der Digitalen Konvergenz sein.
- Der Bremer Raumfahrt- und Technologiekonzern OHB SE weitet mit der in 2018 gegründeten „OHB Satellitenbetrieb GmbH“ die Aktivitäten im Bereich Services aus, und bündelt zudem die zahlreichen Aktivitäten in diesem Bereich inklusive Management von Satellitenkonstellationen.

OHB sieht sich als Systemanbieter nicht nur in Deutschland im Innovationswettbewerb bestens platziert, und wird auch bei kommenden nationalen und europäischen Programmen die über Jahrzehnte aufgebaute Expertise zur Verfügung stellen.

Über die OHB System AG

Die OHB System AG ist eines der drei führenden Raumfahrtunternehmen Europas. Der Systemanbieter gehört zum börsennotierten Hochtechnologiekonzern OHB SE, in dem rund 2.700 Fachkräfte und Systemingenieure an zentralen europäischen Raumfahrtprogrammen arbeiten. Auf www.ohb.de erfahren Sie mehr über die internationalen Unternehmen in der OHB-Gruppe und ihre jeweiligen Geschäftsfelder.

Mit zwei starken Standorten in Bremen und Oberpfaffenhofen bei München und fast 40 Jahren Erfahrung ist die OHB System AG spezialisiert auf High-Tech-Lösungen für die Raumfahrt. Dazu zählen kleine und mittelgroße Satelliten für Erdbeobachtung, Navigation, Telekommunikation, Wissenschaft und Exploration des Weltraums ebenso wie Systeme für die astronautische Raumfahrt, Luftaufklärung und Prozessleittechnik.

Was Sie heute und in Zukunft von Deutschlands führendem Systemhaus erwarten können erfahren Sie unter **www.ohb-system.de.**

Künstlerische Darstellung Galileo-FOC Satelliten

Foto: OHB System AG

Disruptiver Wandel: Digitale Konvergenz minimiert Reaktionszeiten

Bernhard Jungwirth, Senior Account Manager DACH, Geospatial Technologies, Carmenta

Bernhard Jungwirth

Foto: Bernhard Jungwirth

Defence 4.0 – im Verteidigungssektor hält die Digitale Transformation Einzug. Missionskritische Echtzeit-Systeme profitieren von Entwicklungen wie Big-Data, Predictive Analytics bis hin zu Künstlicher Intelligenz sowie von Cloud- und Internet-of-Things-Systemen für vernetzte Sensortechnik in Verbindung mit Geodaten und taktischen Informationen. Das Ziel: Verbesserte dynamische, situationsbezogene Lageanalysen für Planung und Simulation von Missionen, Battle Management und Nachbereitung von Manövern.

Sensordaten verändern die Möglichkeiten der Verteidigungsindustrie

Im Sinne von Industrial Internet of Things (IIoT) schafft der Einsatz und die Vernetzung von Sensoren in Ausrüstungen und Fahrzeugen einen beispiellosen strategischen Vorteil, wenn sie mit Geodaten und taktischen Informationen verbunden werden. Die Leistungsfähigkeit heutiger IT-Systeme erlaubt es, in Echtzeit ein hochpräzises, dynamisches Lagebild der aktuellen Situation anhand von georeferenzierten Daten im Kontext zu beispielsweise Abstands-, Geschwindigkeits- und Temperaturmessungen zu schaffen. Visualisiert man diese Daten innerhalb 2D- Karten, oder auch im 3D-Umfeld – je nach unterschiedlichen Rollen – stellt dies Einsatzkräften vor Ort wertvolle Entscheidungshilfen zur Verfügung, ebenso wie der taktischen Manöversteuerung im Hintergrund. Denken wir in diesem Zusammenhang an die ständig wachsenden Herausforderungen im Zusammenhang mit Blue Force Tracking.

Die Big-Data-Herausforderung: Analyse und Visualisierung

Mehr Daten gleich bessere Information? Leider nicht ganz. Um aus Daten tatsächlich Vorteile zu generieren, stehen die Entwicklungen wie Advanced und Predictive Analytics sowie Machine Learning bis hin zu Künstlicher Intelligenz im Fokus. Ein wichtiges Ziel ist hier, Daten im Kontext aus unterschiedlichen Perspektiven zu betrachten und so darzustellen, dass daraus optimale Handlungsoptionen abgeleitet werden können – je nach Bedarf auch in Sekundenbruchteilen. Eine hochentwickelte Echtzeit-Analytik, die auf präzisen Sensor- Geo- und Lagedaten basiert, wird auch die Planung, Simulation und Nachbereitung von Manövern auf eine neue Ebene heben. Bei der Planung von Flugmissionen werden beispielsweise detaillierte Analysen von Bedrohungen in Terrainprofilen und die Echtzeitkalkulation von Abständen ermöglicht. In diesem Zusammenhang bieten realistische 3D-FlyThroughs eine effektive Trainingsressource. So kann mit moderner Analytik ein kontinuierlicher Verbesserungsprozess angestoßen werden für den effizienten Einsatz von Truppen, Geräten und Kampfmitteln in allen Zusammenhängen und Abhängigkeiten.

Vernetzte Sensoren bei Fahrzeugen *Grafik: Carmenta*

Taktische Planung mit Echtzeit-Informationen *QFoto: Carmenta*

Cloud Computing – aber mit Sicherheit

Grundlage solcher leistungsfähigen Systemumgebungen mit Echtzeitinformationen ist Cloud Computing. So verständlich Einwände gegen Cloud sein mögen – technologisch sind Cloud-Infrastrukturen mittlerweile so weit entwickelt, dass sie mit der für die Verteidigungsindustrie nötigen Robustheit und Schutzmechanismen ausgestattet und mit Desaster-Recovery-Systemen zuverlässig abgesichert werden können.
Schließlich geht es bei Cloud um mehr als nur Rechenleistung: Cloud-Strukturen ermöglichen es, weltweit sehr schnell und bedarfsorientiert auf IT-Kapazitäten und Anwendungen zugreifen zu können. Zudem bietet die Vernetzung über Cloud Computing neue Möglichkeiten im Truppenverband, um Einsatzkräfte und Divisionen übergreifend zu koordinieren und sehr viel schneller und präziser abgestimmt auf akute Situationen zu antworten.
Defence 4.0 kann und wird in allen Bereichen gewohnte Denk- und Handlungsweisen grundlegend ändern. Unabdingbar ist dabei, dass Gremien übergreifend die Gestaltung und Definition robuster Technologiestandards vorantreiben, um die nötige Sicherheit zu gewährleisten.
Abschließend bleibt zu sagen: Die fortschreitende Digitalisierung zerrt die Prozesse einer ganzen Industrie auf den Prüfstand, was konsequentes Handeln auf vielen Ebenen erfordert.

Raus aus der „Gedanken-Cloud“: Lösungsansätze für die Vernetzung mobiler Systeme

Autoren:
Jörg Eschweiler, Head of Cybersecurity & Intelligence
Simon Brünjes, Head of Digitization LandOps
Dr. Thomas Bierhoff, Head of Technology & Innovation
Geschäftsbereich Civil & National Security, Atos Deutschland

Anforderungen an digitale Informationsräume

Die adäquate und relevante Informationsversorgung mittels IT-basierter Systeme ist für Verteidigungsorganisationen der wesentliche Erfolgsfaktor für die Auftragserfüllung. Ein gemeinsamer digitaler Informationsraum ist daher Ziel der Digitalisierungsstrategie der Bundeswehr. Dies bedingt gleichermaßen die Berücksichtigung etablierter und entstehender Systeme zur Unterstützung und Durchführung von Missionen. Zudem müssen IT-basierte Funktionalitäten die anspruchsvollen Anforderungen operationeller Einsatzszenarien hinsichtlich Bedienbarkeit, Funktionalität, Verfügbarkeit, Resilienz, Ressourcenbedarf als auch Sicherheit erfüllen.
Ein interoperables Zusammenspiel von proprietären Fachanwendungen und IT-Diensten soll im Rahmen bestehender Operations- und Informationskonzepte automatisiert und unter Berücksichtigung abgeleiteter Rollen- und Rechtekonzepte sowie variabler Nutzung aller verfügbaren Kommunikationsmittel erfolgen, um neue digitale Fähigkeiten ganzheitlich und medienbruchfrei abbilden zu können. Neben Interoperabilität stellen zudem Flexibilität (z.B. zur Ermöglichung einer dynamischen Föderierung) und Anpassungsfähigkeit an sich im Laufe der Mission ändernde Bedarfe weitere kritische Erfolgsfaktoren dar. Die Etablierung und Aufrechterhaltung von Cyber-Sicherheit mittels adaptiver Mechanismen und Verfahren auf allen Ebenen der Technologie, über Prozess- und Informationsketten sowie einzelne Informations- oder Vernetzungsdomänen hinweg, ist essentiell.

Microservice-Architekturen als Enabler

Die Umsetzung serviceorientierter Architekturen für mobile Plattformen scheint angesichts der zu erwartenden Datenlast aus dem Zusammenspiel verteilter Systemkomponenten mit derzeitig verfügbaren Bandbreiten nur schwer zu bewältigen. Selbst bei ausreichender Bandbreite (etwa durch zellulare Netze) wäre für eine ausreichende (Anwendungs-)Servicequalität eine permanente Verfügbarkeit aller erforderlichen Services erforderlich. Microservice-Architektur-Umsetzungen bieten realisierbare Lösungen, die den Raum für Innovation, unterschiedliche Hersteller und Integration heterogener Produkte öffnen.
Den Schlüssel zu gemeinsamen digitalen Informationsräumen stellen hoch skalierbare, verteilte, gesicherte Middleware-Softwarelösungen auf Basis von Microservice-Architekturen dar, die eine automatisierte Vernetzung von Fachanwendungen und Diensten unter Nutzung der verfügbaren Kommunikationsmittel leisten. Dynamische Szenarien mit unterschiedlichen Lasten, variierende Bandbreitenverfügbarkeiten und Netzwerkqualitäten müssen ebenfalls durch eine solche Middleware-Lösung resilient unterstützt werden. Dies erfolgt mit Hilfe einer situativ angepassten Servicevermittlung und eines optimierten Serviceroutings. Die verteilten Service-Middleware-Instanzen sind auf den verschieden IT-Infrastrukturen des digitalen Informationsraumes ausgeprägt und stellen somit dessen „Software-Getriebe“ dar. Ein solches „Software-Getriebe“ bietet Atos mit der Softwarelösung „Unified Service Delivery“ (USD).

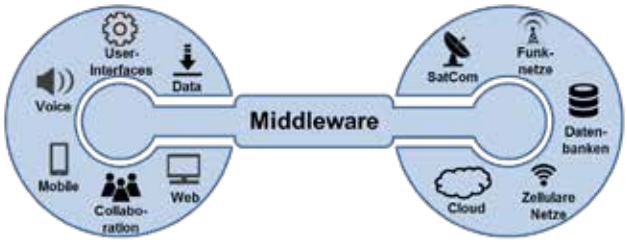


Abbildung – Middleware als „Getriebe“: Verbindung von Applikationen und Übertragungsmedien

Unser Zielbild: Der Streitkräfte-gemeinsame Informationsraum

Bisherige Führungsinformationssysteme waren zumeist silo-artig ausgeprägt und somit war ein Zusammenspiel der verschiedenen Systeme – gerade im multinationalen Kontext – kaum möglich. Mit der Harmonisierung der Führungsinformationssysteme (HaFIS) wurde ein Programm initiiert, das Serviceorientierung und moderne Architekturansätze realisiert und wesentlich von Atos als Hauptauftragnehmer unterstützt wird. Diesen Weg gilt es mit dem geplanten Portfolio der Bundeswehr bzw. den Folgeprogrammen wie GMN und D-LBO konsequent weiter zu beschreiten. Ein gemeinsamer digitaler Informationsraum ist die Schlüsselkomponente der vernetzten Operationsführung.
Um den Anforderungen moderner militärischer Einsätze gerecht zu werden, muss der künftige föderierte digitale Informationsraum alle Mobilitätsdimensionen mit stationären und verlegefähigen Rechenzentren sowie mobilen Systemen auf den verschiedenen Führungsebenen von der strategischen bis zur taktischen Ebene umfassen, um die notwendige Durchgängigkeit des Gesamtsystems sicherzustellen.
Hierbei gilt es, die aktuellen technologischen Möglichkeiten in Gänze zu berücksichtigen. Atos unterstützt proaktiv die Digitalisierung der Teilstreitkräfte durch Konzepte für einen durchgängigen Verbund digitaler Datenverarbeitungs- und

Datenübertragungssysteme. Collaborative combat, Augmented Interactive Reality (AIR), Battle Management Systeme (BMS), Tactical Communications sowie Künstliche Intelligenz als zentrales Element autonomer Systeme sind nur einige Themen, die von Atos aktiv umgesetzt werden. Dazu gehören auch Technologien zur Erhöhung der Resilienz, Ermöglichung der Bedrohungserkennung und -abwehr sowie High Performance Computing (HPC) für echtzeitnahe Analysen und Auswertungen von umfangreichen und komplexen Datenvolumina und zur Entscheidungsunterstützung.

Atos wirkt konzeptionell führend als langjähriger Partner entscheidend an der Fähigkeitsentwicklung im Rahmen des NATO Federated Mission Networking (FMN) und der DCIS-Initiativen der NATO, der Funktionalen Informationssicherheitsarchitektur (FITSA) national und multinational und den zukünftigen Programmen der Bundeswehr durch zukunftsweisende Realisierungen mit. Als Systemintegrator und Technologieanbieter mit europäischen Wurzeln unterstützt Atos seine Kunden, ihren Auftrag effektiv und effizient erfüllen zu können. Atos ist durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifizierter IT-Sicherheitsdienstleister. Ferner unterstützt Atos Kunden hinsichtlich der Etablierung, Aufrechterhaltung und Wirksamkeitsprüfung von Sicherheitsmaßnahmen mithilfe von maßgeschneiderten Lösungen, übergreifender und spezifischer Penetrationstests sowie der Realisierung von Managementsystemen und Ausprägung operationeller CERT und Cyber Defence Fähigkeiten. Atos ist Partner der Allianz für Cyber-Sicherheit und verfügt über eine Vielzahl national und international anerkannter Zertifizierungen.

Atos ist zudem ein weltweit führender Anbieter von Dienstleistungen und Lösungen zum digitalen Product Life Cycle Management über den gesamten Zyklus von Spezifikation, Entwicklung, Erprobung, Nutzung bis hin zur Obsoleszenz komplexer Technologieprodukte für anspruchsvolle Branchen wie z.B. Aerospace, Automotive, Electronics sowie der wehrtechnischen Industrie. Als Mitglied der Industrial Data Space Association e.V. und Digitalisierungspartner führender Industrieunternehmen schafft Atos Möglichkeiten zum sicheren Austausch von Daten und deren kontrollierter Nutzung und Verknüpfung zwischen Partnern.

Der Ausschuss Digitale Konvergenz

Tobias Ludwig Eder, Referent des Bundesverbands der Deutschen Sicherheits- und Verteidigungsindustrie e.V. – BDSV

Tobias Ludwig Eder, BDSV
Foto: ILLING&&VOSSBECK FOTOGRAFIE

IT und IT-Sicherheit als „Enabling Factor“

Der BDSV betrachtet die Rolle von IT und auch IT-Sicherheit heute als essentiellen „Enabling Factor“ für die Produkte, Lösungen und Services der Sicherheits- und Verteidigungsindustrie. Denn eine Plattform ist nur so gut, wie die in ihr verbaute Software mit ihren zugrundeliegenden Algorithmen und Funktionalitäten. Je mehr Erfahrung und Wissen in der Plattform in Form von elaborierten Routinen, Mustererkennung oder bereits vorkonfektionierten Prozessen eingeflossen ist, je präziser die Analysen und je zuverlässiger die Vorhersagen sind, desto größer ist ihr Nutzen. Und der steigt noch einmal, wenn Bestandteile aus dem Bereich der künstlichen Intelligenz, wie etwa Sprach- oder Bilderkennung integriert werden können.
Die in diesem Bereich führenden Unternehmen sind nunmehr im BDSV organisiert. Hierdurch wiederum fördert der BDSV maßgeblich die Verknüpfung der industrieller Cyber/IT-Kompetenz mit der Kompetenz der klassischen Rüstungsindustrie.

BDSV als Katalysator und Treiber

Das Potenzial der digitalen Konvergenz – die in anderen Marktbereichen bereits weiter fortgeschritten ist – wird unseres Erachtens derzeit im Sicherheits- und Verteidigungsumfeld noch nicht voll ausgeschöpft. Der BDSV versteht sich hierbei als Katalysator und Treiber dieser digitalen Konvergenz und möchte die genannten Welten einander näherbringen. Ein ers-

ter Schritt dazu ist nun durch die Gründung des neuen Ausschusses „Digitale Konvergenz“ geschehen.
Dieser soll zu einer entsprechenden Austausch-Plattform für unsere Mitglieder und als übergreifender Treiber zum Thema Digitale Konvergenz im deutschen SVI-Umfeld aufgebaut werden. Hier wurde ein Gremium ins Leben gerufen, welches, unter Berücksichtigung einer vorwettbewerblichen Ausrichtung der Diskussion, industrielle Cyber/IT-Kompetenz und die Fähigkeiten der klassischen Verteidigungsindustrie miteinander verknüpft.
Vor diesem Hintergrund hat sich der Ausschuss auch eine Vorsitzstruktur geschaffen, die diese Konvergenz abbildet. Der neue Vorsitzende, Marc Akkermann von der INFODAS GmbH steuert als Vertreter der Informationssicherheit das Gremium in Zusammenarbeit mit zwei Stellvertretern – je ein Vertreter aus dem IT-Umfeld und einer aus einem „klassischen“ Rüstungshaus. Damit wird auch personell das Dreieck aus der IT-Sicherheit, der reinen Rüstung und der reinen IT abgebildet.
Hiermit besitzt dieses Gremium erkennbar eine Alleinstellung in Deutschland und hat das Ziel, Synergieeffekte zu identifizieren, voranzubringen und damit den Kundennutzen unserer Industrie noch einmal deutlich zu erhöhen. Der Ausschuss wird diese Stellung nutzen, um Bewusstsein für Zukunftstechnologien im Kundensegment, im politischen und gesellschaftlichen Raum und bei den Mitgliedsunternehmen zu den neuen Herausforderungen der Digitalen Konvergenz zu schaffen und umfänglich zu informieren.
Der BDSV wird diese Entwicklung aktiv begleiten und seine langjährigen Mitgliedsunternehmen und die steigende Anzahl an neu eintretenden IT-Unternehmen in einem moderierten Dialog zur Digitalen Konvergenz einbinden.

BNET revolutioniert die Funkgerätetechnik

Einführung

Das Vorhaben „Digitalisierung-Landbasierte Operationen“ (D-LBO) der Bundeswehr zielt auf die Kräfte vorwärts des vordersten verlegefähigen und breitbandig an die Fernebene angebundenen Gefechtsstandes. Dort muss man auf Funkverbindungen zurückgreifen. Dabei gibt es zahlreiche Herausforderungen wie z.B. Bereitstellen einer hohen Übertragungsbandbreite, volle Internetprotokoll(IP)-und Netzwerkfähigkeit, parallele Übertragung von Daten und Sprache, geringe Verzögerungen, Zuverlässigkeit und Sicherheit der Übertragung, der Betrieb in der Bewegung und vor allem auch das Frequenzmanagement als Grundlage. Letzteres bildet den Schwerpunkt dieses Artikels.
Für all diese Herausforderungen bietet die BNET-Familie der Fa. Rafael die Lösung.

Übertragungsbandbreite

Jedes BNET empfängt auf mehreren Frequenzen über den gesamten zugewiesenen Frequenzbereich – der im Übrigen nicht kontinuierlich sein muss, sondern auch Lücken aufweisen darf. Diese erlauben nicht nur die parallele Übertragung von Daten und Sprache, sondern sogar die parallele Übertragung von mehreren Videostreams. Damit wird darüber hinaus eine einzigartige Frequenzökonomie erzielt. Auf Basis der MCR-Fähigkeiten kann der BNET-Empfänger mit einer Empfangseinheit Informationen auf zahlreichen Frequenzen gleichzeitig empfangen. So entsteht ein einzelnes „flaches“ Netzwerk, das mehr als vierhundert Nutzer (d.h. Funkgeräte) umfassen kann.

Netzwerkfähigkeit

Jedes BNET verbindet sich automatisch mit jedem erreichbaren anderen BNET und routet auf Basis IP über diese Verbindungen. Damit ist der Aufbau eines sogenannten „Mobile Ad-hoc Network“ (MANET) Designgrundlage und systemimmanent. Dieses MANET bietet Sprach-, Daten- und Videoübertragung auch in der Bewegung mit hoher Geschwindigkeit und sehr geringer Verzögerung.

Zuverlässigkeit und Sicherheit

Ein Funkgerät mit solchen Leistungseigenschaften darf zwangsläufig nur geringe Latenzen aufweisen und gewährleistet die Übertragungssicherheit auf allen Übertragungsstrecken und unter allen Übertragungsbedingungen.
Das führt dazu, **dass ein einziges BNET ausreicht, um den Kommunikationsbedarf einer Plattform zu erfüllen,** während bisherige Lösungen immer den Einsatz mehrerer Geräte erfordern.
Das klingt alles schon sehr ansprechend aber **das Frequenzmanagement entscheidet das Gefecht.**
Es ist eine bekannte Tatsache, dass Funkfrequenzen zu den knappsten Ressourcen einer militärischen Organisation gehören. Das Problem entsteht schon aus der Frequenzzuweisung

„Software Defined Radios“ (SDR) Foto: Rafael

in Friedenszeiten, wo zivile und militärische Nutzer um ihren Anteil ringen und setzt sich fort bei der Weiterverteilung. Im Einsatz sind Art und Umfang der Frequenzzuweisung von herausragender Bedeutung für den Erfolg militärischer Operationen.
Die militärische Frequenzzuteilung muss mehrere Parameter gleichzeitig und gleichwertig berücksichtigen. Dazu gehören

- konkrete Kommunikationsforderungen,
- getrennte Zuweisung für Luft-, See- und Landoperationen,
- technische Vorgaben und Einschränkungen.

Dieses Geflecht aus Abhängigkeiten hat im militärischen Bereich dazu geführt, dass komplette und komplexe Systeme aufgebaut wurden, um die Frequenzplanung, und -zuweisung und deren fortlaufende Verwaltung sicher zu stellen. Das ist eine schwierige Aufgabe, weil Fehler verheerende Auswirkungen haben können. Und in der Tat gibt es Fälle, in denen fehlerhaftes oder auch nur unzureichendes Frequenzmanagement zu Verlusten geführt hat.
Betrachtet man zum Beispiel zwei Truppenteile deren Bewegungen sich überschneiden, die aber auf unterschiedlichen Frequenzen arbeiten und daher nicht die Möglichkeit haben, miteinander zu kommunizieren, dann hat man schnell eine Situation die zum Beschuss eigener Kräfte führen kann.

Eine einzelne Frequenz reicht nicht

Warum muss Frequenzmanagement so schwierig sein? Zum Verständnis dieses Problems muss man etwas tiefer in die Technologie einsteigen. Für die meisten – wenn nicht für alle – der zurzeit käuflichen taktischen Funkgeräte gilt: „Die Frequenz bestimmt das Netz.“ Das heißt, dass Funkgeräte, die miteinander kommunizieren sollen, auf genau einer Frequenz arbeiten müssen. Das gilt auch für moderne „Software Defined Radios“ (SDR), die zu einem bestimmten betrachteten Zeitpunkt auch nur genau eine Frequenz nutzen. Das gilt auch bei jeder Form des sogenannten Frequenzsprungverfahrens. Auch hier wird aus einem Frequenzbündel jeweils nur eine Frequenz tatsächlich genutzt.
Nun kann man zwar die Frequenz wechseln. Das ist aber eine manuelle Tätigkeit, die nur auf Befehl und gemeinsam durchgeführt werden kann, weil sonst das Netzwerk zusammenbricht. Das muss vorab bedacht werden und bedeutet auch,

dass die Frequenzzuordnung durch die Fernmelde-/IT-Offiziere relativ starr und spekulativ durchgeführt werden muss.
Was passiert nun, wenn ein Funkgerät, das auf eine bestimmte Frequenz eingestellt ist, der Kommunikation in einer anderen Gruppe von Funkgeräten auf einer anderen Frequenz beitreten will? Das geht bisher nur, wenn es auf die andere Frequenz/das andere Frequenzbündel umgeschaltet wird. Sich auf solche weitgehend unvorhersehbaren Veränderungen vorausschauend einstellen zu müssen, ist das Problem der Fernmelde-/IT-Offiziere in aller Welt.
Diese Situation wird dadurch verursacht, wie schon oben festgestellt, dass heutige Funkgeräte zu einem bestimmten Zeitpunkt nur auf einer Frequenz senden und empfangen können.

Die Lösung – Mehrfrequenztechnik (MCR)

Es liegt gelegentlich in der Natur der Sache, dass solche Probleme als gegeben angenommen werden. Aber ab und an erscheint eine neue bahnbrechende Technologie, die eine Lösung für ein Problem darstellt, das bis dahin nach dem Motto „Physik lässt sich nicht ändern“ betrachtet wurde.
Eine solche Lösung ist die Mehrfrequenztechnik („Multi-frequency Channel Reception“ – MCR) die durch die Fa. Rafael in jahrelanger Entwicklungsarbeit fertiggestellt und anschließend patentiert worden ist. MCR ist die Fähigkeit über eine einzige Empfangseinheit (= 1 Antenne) gleichzeitig Informationen auf mehreren Frequenzen zu empfangen.
Das ist eine wahrhaft disruptive Technologie, weil sie nicht nur ein bestimmtes technisches Problem löst, sondern weil sie auch ein neues Verfahren in Bezug auf militärisches Frequenzmanagement und damit auf die Art und Weise, wie militärische Operationen geführt werden, einläutet.

Rafaels BNET – der Pionier der MCR-Technologie

Das Wissen um die Einschränkungen der Einkanaltechnik und die jahrzehntelange Erfahrung mit C4I-Lösungen haben die Fa. Rafael dazu geführt, die BNET-Familie an Funkgeräten zu entwickeln. Dabei handelt es sich um einsatzbewährte SDR, mit denen ein breitbandiges und IP-fähiges MANET (Mobiles Ad-hoc Netz) für taktische Operationen auf der Grundlage der MCR-Architektur aufgebaut wird.
Dabei gibt es keine „Flaschenhälse“, weil auf dem mittels BNET aufgebauten Netz logische Gruppen definiert werden, innerhalb derer kommuniziert wird. Dazwischen werden keine Gateways benötigt werden. Durch den verbesserten Durchsatz werden anspruchsvolle und echtzeit-nahe Anwendungen einschließlich „Full Motion Video“ und Sensor-Rohdaten gleichzeitig unterstützt.
Das ist essentiell für die Digitalisierung von Landoperationen und eine der größten Herausforderungen im Hinblick auf den Verbund von Aufklärung, Führung und Wirkung (sensor to shooter). Auch auf diesem Feld verfügt Rafael im Übrigen mit „Fire Weaver“ über ein ausgereiftes und einsatzbewährtes System.
Darüber hinaus verringern die schnellen BNET-Funktionen zum Zusammenführen und Wiederherstellen von Netzwerken – mit Reaktionszeiten im Sekunden- statt im Minutenbereich – die Risiken (z.B. eines Eigenbeschusses – friendly fire), die mit einer fehlenden Kommunikation einhergehen. Diese bereits beeindruckenden Vorzüge werden aber zweifellos von der dynamischen und automatischen Frequenzzuordnung übertroffen.
Auf Grundlage der MCR-Technologie entfällt die Notwendigkeit die Frequenzzuordnung vorauszuplanen und zu hoffen, dass diese Vorausplanung sich im Gefecht bewährt. Vielmehr wird das gesamte verfügbare Spektrum automatisch so weit wie nur irgend möglich genutzt. Damit können auch Frequenzbereiche, die bislang ungenutzt vorgehalten werden (z.B. für Ausweich- und Wechselfrequenzen) und an sich vergebene, aber zu einem bestimmten betrachteten Zeitpunkt nicht genutzte Frequenzen für die Kommunikation genutzt werden. Allein aus dem Umstand, dass bisher regelmäßig zu einer Frequenz eine (zunächst unbenutzte!) Ausweichfrequenz zugewiesen wird, erhöht sich damit die Effizienz – und entsprechend auch die verfügbare Bandbreite – um 100%!
Ein BNET-Kunde hat das kürzlich so ausgedrückt: „Mit BNET kann ein Fallschirmjäger irgendwo landen, sein BNET Funkgerät einschalten und einfach anfangen Sprache, Daten und sogar Videos zu senden und zu empfangen, ohne sich jemals fragen zu müssen, welche Frequenz er einstellen muss oder ob in seinem Einsatzgebiet nur irgendeine spezielle Frequenz unterstützt wird. Dank BNET sind dieser Soldat und seine Vorgesetzten von der Mühe des Frequenzmanagement, befreit.

Zusammenfassung

Mit der BNET-Familie hat die Fa. Rafael Funkgeräte entwickelt, die in jeder Hinsicht wesentliche und ggf. kampfentscheidende Fortschritte aufweisen.
Das operationelle Problem mit der Frequenzverfügbarkeit und dem Frequenzmanagement wird durch diese neue revolutionäre Technologie völlig aus der Welt geschafft. Der Mehrfrequenzempfang, der durch Rafael entwickelt und patentiert wurde, verkündet ein neues Zeitalter auf dem Gefechtsfeld – eines in dem man sich keine Sorgen mehr darüber machen muss, ob die Frequenzzuweisung und -verteilung hinreichend ist oder nicht. Dass damit auch mindestens eine Verdopplung der verfügbaren Bandbreite erreicht wird, ist nicht nur ein zusätzliches Feature, sondern schafft überhaupt erst eine Grundlage für die „Netzwerkbasierte Operationsführung“.
Das ist die Natur einer disruptiven Technologie – sie verändert bisher gültige Grundlagen und führt zu einer neuen Entwicklungsebene. Die MCR-Technologie von Rafael tut genau das mit BNET und wird damit die Art und Weise verändern wie militärische Operationen in Zukunft geführt werden.

Besuchen Sie uns bei der AFCEA Fachausstellung 2019 Messestand M12

Der Fachkongress Deutschlands für
IT- und Cybersicherheit bei Staat und Verwaltung

www.public-it-security.de

PITS
Public-IT-Security
2019

2.–3. September 2019
Hotel Adlon, 10117 Berlin

PITS 2019:

Die agile hybride Bedrohungslage

Herausforderung – Entwicklung – Austausch – Lösungen

IT-Sicherheit schafft Vertrauen und Vertrauen ist die Basis für das E-Government der Zukunft. Die medienbruchfreie, integrierte und elektronische Bearbeitung von Verwaltungsdienstleistungen, z.B. im Rahmen der europäischen Dienstleistungsrichtlinie, lässt sich nur mit einer sicheren Kommunikation von Behörden untereinander bzw. von Behörden zu Unternehmen und Bürgern erreichen. Der Schutz vor Malware, Spam, unerlaubten Zugriffen oder Manipulationen ist die Grundvoraussetzung für eine breite Akzeptanz des E-Governments und der vollen Nutzung der damit verbundenen Effizienzvorteile.

PITS, der Verwaltungskongress der Behörden Spiegel-Gruppe, greift dieses wichtige Handlungsfeld speziell für den öffentlichen Sektor auf – **PITS steht dabei für Public-IT-Security.**

Fachforen der PITS 2019

- Cyber Stability
- Internet Security / Endpoint Protection / DDoS-Attacken
- IT-Konsolidierung: Welche Strategie für ein Plus an mehr Sicherheit
- Mitarbeiterzentrische Sicherheit
- Künstliche Intelligenz
- SPAM, Phishing und Ransomware
- Netzwerksicherheit
- Sichere Zugriffsrechte
- IT-Security made in Germany
- Sichere mobile Kommunikation
- Datenschutz als Treiber für die Digitalisierung
- IT-Sicherheitsgesetz 2.0
- Computer Emergency Response Teams (CERT's): Angriffsflächen erkennen und schließen
- Cloud Security
- Ernstfall Social Engineering / Security Awareness
- Die sichere Landesbehörde
- Herausforderung: Strafverfolgung im Internet
- Das Zeitalter der Digitalisierung
- Kritische Infrastrukturen

Eine Veranstaltung des

Behörden Spiegel

AFCEA Bonn e.V.

Anwenderforum für Fernmeldetechnik, Computer, Elektronik und Automatisierung

33. AFCEA-Fachausstellung

Informations- und Kommunikationstechnik

„Smarte Führungsunterstützung im 21. Jahrhundert“

10./11. April 2019 • Maritim Hotel Bonn

10. April 2019

09:00 – 18:00 Uhr	**Ausstellung • Vorträge im Saal REGER** *Moderation:* Brigadegeneral Armin Fleischmann, AbtLtr Kommando CIR und Vorsitzender AFCEA Bonn e.V.
10:00 Uhr	**Begrüßung / Eröffnung der 33. AFCEA-Fachausstellung** Brigadegeneral Armin Fleischmann, AbtLtr Kommando CIR und Vorsitzender AFCEA Bonn e.V. Oberst a.D. Friedrich W. Benz, Leiter der AFCEA Fachausstellung Bonn
10:20 Uhr	**“Das Cyber Security Cluster Bonn“** Prof. Dr. Peter Martini, Institutsleiter Fraunhofer FKIE und Professor an der Universität Bonn
14:00 Uhr	**„Herausforderung Zukunft: Das `Future Operating Environment` und der schwierige Umgang mit der Hype um KI und autonome Systeme“** LWissDir Dr. Jan Teiler, Referatsleiter Zukunftsanalyse, Planungsamt der Bundeswehr, Berlin
16:00 – 17:45 Uhr	**Karrierestarterforum Young AFCEANs** *Informationsveranstaltung "Karriere in der digitalen Transformation" mit und für junge Fach- und Führungskräfte sowie Studenten zu den Themen Berufseinstieg und Karrieregestaltung.* *Moderation:* Frau Esra Ünal, BWI GmbH
18:00 – 21:00 Uhr	**Get-together AFCEA Fachausstellung** *AFCEA Bonn e.V. lädt Besucher und Aussteller der AFCEA Fachausstellung 2019 ein zu* ***Kölsch mit Snacks*** *im Ausstellungsbereich Foyer I/II*

11. April 2019

09:00 – 17:00 Uhr	**Ausstellung • Vorträge im Saal REGER** *Moderation:* Brigadegeneral Armin Fleischmann, AbtLtr Kommando CIR und Vorsitzender AFCEA Bonn e.V.
10:00 Uhr	**“Digitalisierung Land“** Oberst i.G Frank Pieper, Chief Digital Officer Heer/Landbasierte Operationen, Kommando Heer, Strausberg
14:00 Uhr	**“Zukunft und Chancen von Cloud-Diensten am Beispiel von Microsoft“** Frau Sabine Bendiek, Vorsitzende der Geschäftsführung von Microsoft Deutschland, Köln
Abschluss	Brigadegeneral Armin Fleischmann, AbtLtr Kommando CIR und Vorsitzender AFCEA Bonn e.V.

Ausstellerliste AFCEA-Fachausstellung 2019

	Ausstellende Firma/Organisation	Stand
1	A.WEIDELT Systemtechnik GmbH & Co. KG	F 30
2	accenture GmbH	ME 17
3	ACT	F 05
4	Adder Technology Ltd	F 65
5	Airbus	M 20
6	Alcatel-Lucent Enterprise	F 63
7	Amazon Web Services (AWS)	ME 15
8	AOC Red Baron Roost	ME 09
9	Arrow ECS AG	F 66
10	ARTEC IT Solutions AG	F 46
11	Aruba, a Hewlett Packard Enterprise company	S 07
12	ATM ComputerSysteme GmbH	M 09
13	Atos Information Technology GmbH	M 07
14	Avitech GmbH	S 10
15	AVS Systeme GmbH	ME 20
16	BAAINBw - Abt. G	F 47
17	BAKO Systemintegration GmbH & Co. KG	F 51
18	BDSV e.V.	F 61
19	Bechtle AG	F 11
20	Behörden Spiegel/ProPress Verlagsgesellschaft mbH	F 20
21	Bell Computer-Netzwerke GmbH	S 03
22	best Systeme GmbH	ME 16
23	Bittium	S 02
24	blackned gmbh	M 01
25	Broadcast Solutions GmbH	F 55
26	BWI GmbH	M 19
27	CANCOM on line GmbH	B 13
28	Carl-Cranz-Gesellschaft e.V.	ME 08
29	Carmenta Geospatial Technologies AB	F 21
30	Cellebrite	F 54
31	CeoTronics AG	M 31
32	CGI Deutschland Ltd. & Co. KG	F 09
33	CHIFFRY GmbH	F 49
34	Cisco Systems GmbH	B 12
35	Citrix Systems GmbH	ME 21
36	cloudera	F 23
37	Cobham Mast Systems	ME 01
38	Computacenter	M 06
39	Comrod Communication AS	F 24
40	Condok GmbH	S 05
41	CONET	F 05
42	conpal GmbH	S 09
43	Cordsen Engineering GmbH	F 12
44	CP Cases	F 51
45	cpm communication presse marketing GmbH	M 06
46	crisis prevention / BETA Verlag & Marketing-gesellschaft mbH	ME 07
47	Cubic Mission Solutions	S 02
48	Cyber Security Cluster Bonn e.V.	F 04
49	dainox GmbH	M 25
50	DataVision Deutschland GmbH	ME 12
51	Dell Technologies	M 03
52	DEUTSCHE GESELLSCHAFT FÜR WEHRTECHNIK e.V. (DWT)	F 48
53	DICOTA SCHWEIZ AG	F 57
54	DIGITTRADE GmbH	F 49
55	DriveLock SE	S 09
56	DSI Datensicherheit GmbH	B 01
57	DXC Technology Deutschland GmbH	B 06
58	ECOS Technology GmbH	F 29
59	EGL Elektronik Vertrieb GmbH	M 29
60	ELESIA S.p.A.	S 02
61	ELNO GmbH	B 02
62	EMW Exhibition & Media Wehrstedt GmbH	ME 10-2
63	Endace Europe Ltd	ME 16
64	EPSON Deutschland	ME 12
65	ESG Elektroniksystem- und Logistik-GmbH	M 08
66	Esri Deutschland GmbH	B 07
67	FFG Flensburger Fahrzeugbau Gesellschaft mbH	S 02
68	Fraunhofer FKIE	M 04
69	Fraunhofer IOSB	S 02
70	Frequentis Comsoft GmbH	M 17
71	Frequentis Deutschland GmbH	M 17
72	GAF AG	ME 19
73	GBS TEMPEST & Service GmbH	S 04
74	Gebr. Friedrich Industrie- und Elektrotechnik GmbH	S 05
75	General Dynamics Mission Systems UK	F 56
76	genua gmbh	M 24
77	GovSat	Fo8
78	griffity defense GmbH	S 02
79	Hagenuk Marinekommunikation GmbH	S 08
80	Haivision Network Video	F 28
81	Harris Geospatial Solutions GmbH	S 02
82	Harris Global Communications	F 41
83	Heinen ICS	M 29
84	Hexagon Geospatial | Luciad	B 10
85	Hitachi Vantara GmbH	M 23
86	IABG mbH	M 27
87	IBM Deutschland GmbH	B 09
88	iesy GmbH & Co. KG	F 50
89	IMTRADEX	F 43
90	Indra Sistemas S.A.	S 10
91	INFODAS GmbH	M 22
92	Intel Deutschland GmbH	M 03
93	ISEC7 Group + Teamwire	F 42
94	itWatch GmbH	F 26
95	iXblue GmbH	S 02
96	JK Defence & Security Products GmbH	F 41
97	JOWO – Systemtechnik AG	F 64
98	K&K Medienverlag-Hardthöhe GmbH/ Hardthöhenkurier	ME 02
99	Kommando Cyber- und Informationsraum	ME 11
100	Lachen helfen	ME 10
101	Leonardo	B 05

Ausstellerliste AFCEA-Fachausstellung 2019

Ausstellende Firma/Organisation		Stand
102	Luciad ››› Hexagon Geospatial	B 10
103	Materna Information & Communications SE	F 07
104	Media Broadcast Satellite GmbH (MBS)	F 27 + S 02
105	Mellanox Technologies Ltd.	F 67
106	MICCAVIONICS GmbH	F 44
107	Microsoft Deutschland GmbH	F 10
108	Mittler Report Verlag GmbH	ME 04
109	Mönch Verlagsgesellschaft mbH	ME 03
110	Motorola Solutions	M 30
111	MSAB	S 11
112	msg systems ag	S 02
113	ND SatCom GmbH	S 02
114	Newsletter Verteidigung - VDS Verlag Deutsche Spezialmedien GmbH	ME 05
115	NYNEX satellite OHG	F 27
116	OHB System AG	F 01
117	OnTime Networks AS	F 69
118	ORACLE Deutschland B.V. & Co. KG	F 13
119	Panasonic Computer Product Solution	F 02
120	PELI HARDIGG	S 01
121	powerBridge Computer Vertriebs GmbH	F 62
122	promegis GmbH	M 05
123	PWA Electronic Service- und Vertriebs-GmbH	F 02
124	QGroup GmbH	ME 14
125	Rafael Advanced Defense Systems Ltd.	M 12
126	roda computer GmbH	F 03
127	Rohde & Schwarz	M 14
128	rola Security Solutions GmbH	M 26
129	RolaTube LTD	F 41
130	RSA	F 66
131	RUAG Defence	F 06
132	Samsung Electronics GmbH	M 01
133	SAP Deutschland SE & Co. KG	B 11

Ausstellende Firma/Organisation		Stand
134	Schenker Technologies GmbH	ME 18
135	SCHNEIDER DIGITAL	F 22
136	Schönhofer Sales and Engineering GmbH	F 25
137	SciEngines GmbH	B 04
138	secunet Security Networks AG	M 16
139	Secusmart GmbH	B 08
140	SELECTRIC Nachrichten-Systeme GmbH	ME 13
141	Sennheiser Vertrieb und Service GmbH & Co. KG	F 32
142	SFC Energy AG	S 06
143	SINUS Electronic GmbH	F 31
144	Software AG	M 18
145	SolarWinds	F 53
146	SOLIFOS AG	B 03
147	Sopra Steria Consulting	M 15
148	steep GmbH	M 10
149	SVA System Vertrieb Alexander GmbH	F 23
150	systematic GmbH	M 21
151	systerra computer GmbH	F 68
152	TASSTA GmbH	F 52
153	TELEFUNKEN Radio Communication Systems GmbH & Co. KG	M 13
154	Tesat-Spacecom GmbH & Co. KG	M 28
155	Textron Systems	M 05
156	Thales	M 11
157	Trend Micro GmbH	B 13
158	T-Systems International GmbH	M 26
159	Ultralife Communications Systems	F 41
160	Utimaco	S 09
161	Verband der Reservisten der Deutschen Bundeswehr e.V.	F 45
162	ViaSat	F 41
163	VITES GmbH	S 06


Saal BEETHOVEN
Saal SCHUMA
Saal MARITIM
FOYER II
Catering
Secusmart
griffity defense GmbH
Gemeinschaftsstand
S 02
PELI HARDIGG
S 01
SciEngine GmbH
B 04
SOLIFOS AG
B 03
ELNO
B 02
DSI Daten-sicherheit GmbH
B 01
B 05
B 06
B 07
Esri Deutschland GmbH
SAP
DXC Technology Deutschland GmbH
Hexagon Geospatial LUCIAD
B 10
B 11
B 12
B 13
Leonardo
IBM
CISCO Systems
CANCOM on line GmbH
Trend Micro GmbH
B 09
Kontakt Aussteller
Condok
Gebr. Friedrich Industrie- und Elektrotechnik GmbH
S 05
SFC Energy AG
VITES GmbH
S 06
Hagenuk Marine-kommuni-kation GmbH
S 08
Conpal
DriveLock SE
Utimaco
S 09
Avitech
Indra Sistem
S 10
ORACLE Deutschland
F 13
Bechtle AG
F 11
CGI
Cordsen Engineering
F 12
Microsoft
F 10
Behörden Spiegel
F 20
Carmenta Geospatial Technologies AB
F 21
SCHNEIDER DIGITAL
F 22
F 23
F 24
F 25
F 26
SVA System Vertrieb Alexander GmbH
cloudera
Comrod Communi-cation AS
Schönhofer Sales and Engineering
itWatch
F 27
F 28
F 29
F 30
F 31
F 32
NYNEX satellite Media Broadcast Satellite
Haivision Network Video
ECOS Technology
A.Weidelt System-technik
SINUS Electronic
Sennheiser Vertrieb und Service
EGL Elektronic Vertrieb Heinen ICS
M 29
Motorola Solutions
M 30
CeoTronics AG
M 31
Fraunhofer FKIE
M 04
blackned gmbh
Samsung Electronics GmbH
M 01
DELL Technologies
Intel Deutschland GmbH
M 03
promegis
M 05
Textron Systems
M 06
Computa-center
Atos
M 07
steep GmbH
M 10
secunet Security Networks AG
M 16
Frequentis Deutschland
Frequentis Comsoft
M 17
Thales
M 11
ESG
M 08
ATM ComputerSysteme GmbH
M 09
Hitachi Vantara
M 23
genua GmbH
M 24
Software AG
Rafael Advanced Defense Systems Ltd.
M 12
TELE-FUNKEN RACOMS
M 13
dainox
M 25
BWI
M 18
M 19
Rohde & Schwarz
M 14
M 15
T-Systems
M 26
rola Security Solutions GmbH
Airbus
M 20
Systematic GmbH
Sopra Steria Consulting
IABG
M 27
TESAT
M 28
M 21
Infodas
M 22
F 44
MICCAVIONICS
F 45
Cobham Mast Systems
Hardhöhenkurier
ME 01
ME 02
ME 03
ME 04
ME 12
Epson Deutschland GmbH
DataVision Deutschland GmbH
ME 13
SELECTRIC
Nachrichten-Systeme GmbH
ME 17
accenture GmbH
ME 18
Schenker Technologies GmbH
ME 19
GAF AG

AFCEA Fachausstellung 2019

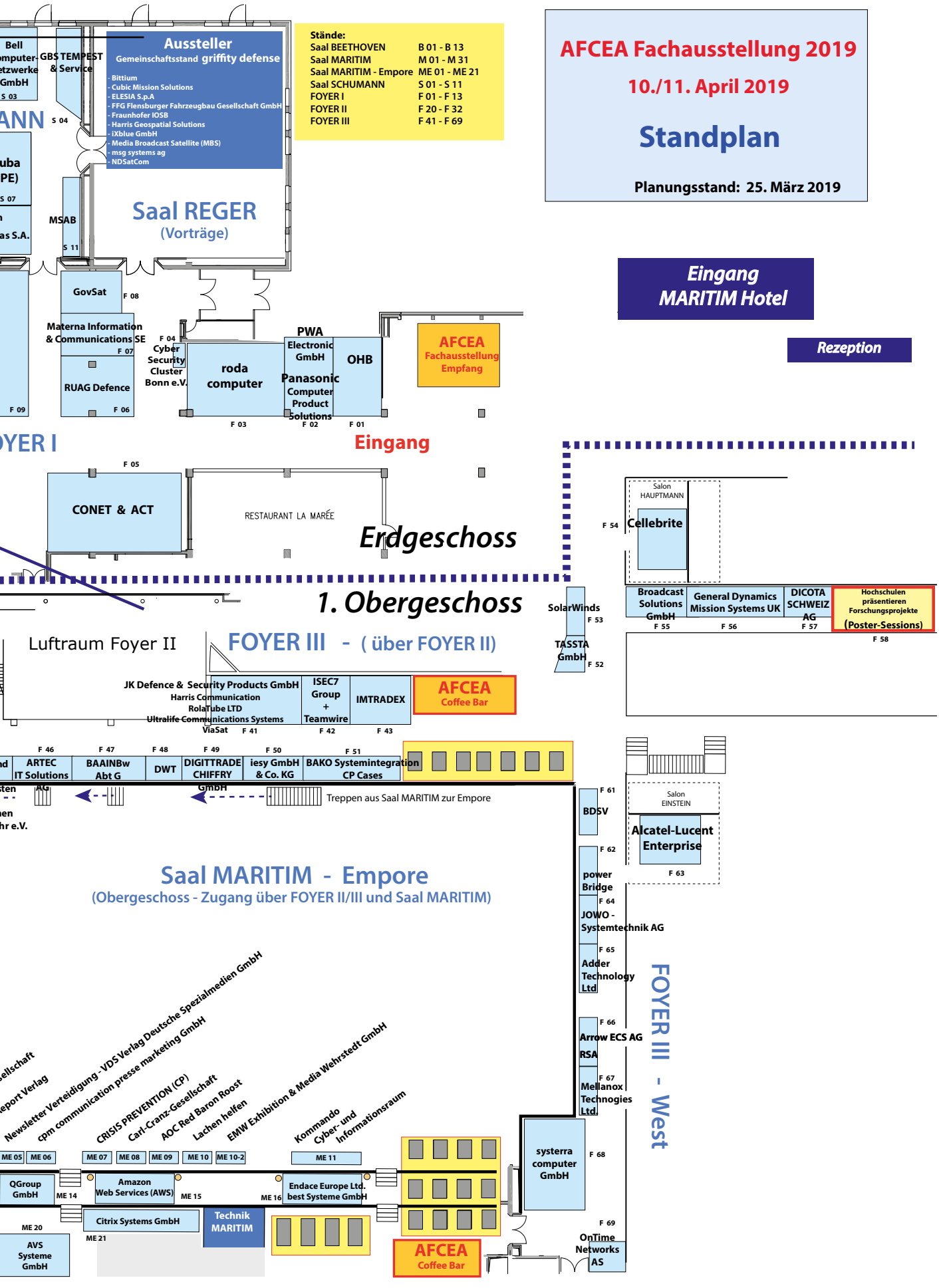
10./11. April 2019

Standplan

Planungsstand: 25. März 2019

Stände:

Saal BEETHOVEN	B 01 - B 13
Saal MARITIM	M 01 - M 31
Saal MARITIM - Empore	ME 01 - ME 21
Saal SCHUMANN	S 01 - S 11
FOYER I	F 01 - F 13
FOYER II	F 20 - F 32
FOYER III	F 41 - F 69



Aussteller AFCEA-Fachausstellung 2019

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

Stände:			
FOYER I	F 01 – F 15	Saal BEETHOVEN	B 01 – B 14
FOYER II	F 20 – F 32	Saal MARITIM	M 01 – M 31
FOYER III	F 41 – F 53	Saal MARITIM – Empore	ME 01 – ME 21
		Saal SCHUMANN	S 01 – S 10

A.WEIDELT Systemtechnik GmbH & Co. KG F 30

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.

accenture GmbH ME 17

accenture ist einer der weltweit größten IT-, Technologie- und Outsourcing-Dienstleister und erwirtschaftete mit etwa 449.000 (2018) Mitarbeitern im Geschäftsjahr 2017 einen Nettoumsatz von insgesamt 34,9 Milliarden US-Dollar. Als Marktführer für integrierte IT-Services und IT-Lösungen unterstützt und begleitet Accenture seine Kunden bei der Umsetzung der digitalen Transformation ihrer Geschäftmodelle. Mit dem Defense-Bereich in Deutschland richtet sich Accenture gezielt an die Bedürfnisse der Bundeswehr und präsentiert auf der AFCEA innovative Lösungskompetenzen u.a. in den Bereichen Künstliche Intelligenz, Cybersecurity und Digitalisierung der Streitkräfte.

Kontakt: Accenture GmbH; Friedrichstraße 78; D-10117 Berlin
Dr. Timo Noetzel (Leitung Defense); +49 (175) 5767966
timo.noetzel@accenture.de

ACT F 05

ACT – ein Unternehmen der CONET-Gruppe „Keep IT moving“ Seit mehr als 37 Jahren unterstützen wir als IT-Dienstleister bei der Optimierung von IT-Landschaften und sorgen für einen reibungslosen IT-Betrieb. Als ein Unternehmen der CONET-Gruppe planen wir, richten ein und überwachen Infrastrukturen und entwickeln Customer-Communication-Management-Lösungen, analysieren Geschäftsprozesse und unterstützen die Betriebsorganisationen durch qualifizierte Dienstleistungen. Wir gestalten die Zukunft und schaffen durch Anwendung neuester Technologien Vorteile. Unser Ziel: Entwicklungen vorantreiben und dem Wettbewerb immer eine Nase voraus sein. Damit heben wir uns nicht nur ab vom klassischen IT-Dienstleister – sondern bringen Bewegung ins Business, indem wir immer einen Schritt weiterdenken.

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

ADDER Technology Ltd. F 65

ADDER TECHNOLOGY ist ein globaler Spezialist für Konnektivitäts- und High Performance IP-KVM-Lösungen. ADDER entwickelt und fertigt eine breite Palette von Signal-Extender-, Switch- und Matrixlösungen, die die Ergonomie, Effizienz und Zusammenarbeit in geschäftskritischen Umgebungen revolutionieren. Durch ADDERs sichere und zuverlässige Technologie stehen dem Bediener alle Visualisierungs- und Überwachungssysteme sofort zur Bearbeitung zur Verfügung. Somit ermöglicht ADDER eine Echtzeit-Konnektivität zwischen Servern und Benutzern in kritischen Umgebungen.

Airbus M 20

Airbus ist ein weltweit führendes Unternehmen im Bereich Luft- und Raumfahrt sowie den dazugehörigen Dienstleistungen. Airbus bietet die umfangreichste Verkehrsflugzeugpalette mit 100 bis über 600 Sitzen sowie Produkte für den Geschäftsflugverkehr. Das Unternehmen ist europäischer Marktführer bei Tank-, Kampf-, Transport- und Missionsflugzeugen und eines der größten Raumfahrtunternehmen der Welt. Die zivilen und militärischen Hubschrauber von Airbus zeichnen sich durch hohe Effizienz aus und sind weltweit gefragt.

Alcatel-Lucent Enterprise F 63 / Salon EINSTEIN

Wir von der Alcatel-Lucent Enterprise (ALE) sind ein weltweiter Netzwerk- und Kommunikationsspezialist und entwickeln Verteidigungslösungen, mit denen Teams verbunden bleiben und die Datensicherheit verbessert wird.
Zu unseren Kunden gehören Verteidigungsorganisationen auf der ganzen Welt. In Frankreich betreiben wir ein spezielles Service-Center für sichere Kommunikation und Netzwerkinfrastruktur innerhalb der EU.
ALE hat eine lange Tradition in der Entwicklung von zertifizierten Lösungen auf Basis von Militärstandards (MIL STD, Zone 2, Common Criteria), die Behörden und Verteidigungsorganisationen helfen, ihre Ziele zur sicheren Kommunikation zu erreichen. Unsere Lösungen ermöglichen moderne Kommunikation und bieten Verteidigungsorganisationen aktuelle Technologien, die Sicherheit und Datenschutz respektieren.

Amazon Web Services (AWS) ME 15

Amazon Web Services (AWS) ist Pionier und Innovationstreiber im Bereich Cloud Computing und wird weltweit von Verwaltung, Bildungs- und Forschungseinrichtungen eingesetzt. Kunden und Partner nutzen AWS als günstige, skalierbare, flexible und sichere Plattform, um Kosten zu senken, die Effizienz zu steigern und innovative IT-Lösungen zu realisieren.
Mit AWS bezahlen Sie nur für das, was Sie nutzen, ohne im Voraus physische

Infrastrukturkosten oder langfristige Verpflichtungen. Öffentliche Unternehmen jeder Größe nutzen AWS, um Anwendungen zu erstellen, Websites zu hosten, große Datenmengen zu nutzen, Informationen zu speichern, Forschung durchzuführen, den Online-Zugang für Bürger zu verbessern und vieles mehr.

Erfahren Sie mehr über AWS im öffentlichen Sektor und wie Sie anfangen können: https://aws.amazon.com/government-education/

AOC Red Baron Roost ME 09

Der AOC Red Baron Roost ist das deutsche Chapter der internationalen Fachinteressengemeinschaft für den Elektronischen Kampf, der in den 1960'ziger Jahren gegründeten Association of Old Crows. Wir bieten unseren Mitgliedern aus den Streitkräften, den wehrwissenschaftlichen und wehrtechnischen Instituten und der Rüstungsindustrie ein anerkanntes Forum zum fachlichen Erfahrungs- und Interessenaustausch. Neben dem für unsere Mitglieder kostenfreien monatlich erscheinenden Fachmagazin „Journal of Electronic Defence (JED)" bieten wir regelmäßige Informationsveranstaltungen und Themenabende zu aktuellen Themen rund um die Bereiche EW, IO, EMSO und CEMA an.

Sie finden weitere Informationen unter www.aoc-redbaronroost.de und www.crows.org

Arrow ECS AG F 66

Die Arrow ist ein Value-Add IT Distributor, der sich auf die Bereitstellung von Produkten und Lösungen führender Technologieanbieter für den unternehmensweiten Einsatz in den Bereichen Enterprise und Midrange Computing fokussiert hat. Zu den Geschäftsbereichen zählen Server, Storage, Virtualisierung, Desktop Delivery, Networks & Security und ergänzende Services. Wir blicken auf über 25 Jahre Erfahrung und Fachkompetenz im IT-Umfeld zurück und unterstützen Fachhändler bei der Realisierung maßgeschneiderter Lösungen für deren Endkunden vom Pre-Sales über Konzeption und Planung eines Projekts bis hin zu Installations- und Support-Services.

Kontakt: Arrow ECS AG, Elsenheimerstraße 1, 80687 München |
Tel: 089093099-0 | www.arrowecs.de | info.ecs.de@arrow.com

ARTEC IT Solutions AG F 46

ARTEC IT Solutions ist führender Hersteller für umfassende Informationsmanagement-Lösungen. Die Produkte decken den kompletten Lebenszyklus aller relevanten Unternehmensdaten ab: Von der zentralen Erfassung in einem System über die effiziente Nutzung und sichere Speicherung bis hin zur rechtskonformen Archivierung.
Neben dem modular aufgebauten Informationsmanagement-System EMA® runden der performante Massenspeicher VSTOR® sowie firegate VPN mit ARTEC Trusted-Computing-Technologie zur sicheren Anbindung von Cloud-Diensten das Leistungsangebot optimal ab.
ARTEC deckt so das gesamte Spektrum des digitalen Informationsmanagements ab – sowohl in lokalen Umgebungen als auch global und über mehrere Standorte hinweg. Ermöglicht wird so die Umsetzung eines modernen und bedarfsgerechten Datenmanagements unter Einhaltung aktueller Gesetzgebungen.

Aruba, a Hewlett Packard Enterprise company S 07

Aruba, a Hewlett Packard Enterprise company, ist ein führender Anbieter von Netzwerkinfrastrukturlösungen für Unternehmen und öffentliche Einrichtungen jeder Größe weltweit. Neben kabelgebundenen und drahtlosen Netzwerkkomponenten bietet das Unternehmen auch Softwarelösungen zur Verwaltung und für die Netzwerksicherheit an. Die Lösungen von Aruba zeichnen sich durch eine Orientierung an den Anforderungen mobiler Benutzer aus und erfüllen gleichzeitig die höchsten Sicherheitsanforderungen. So hat Aruba ClearPass als erste Network Access Control-Lösung die Common Criteria-Zertifizierung in der Cybersicherheitsbranche erhalten. Referenzkunden von Aruba sind unter anderem die US Army oder die US Airforce, aber auch viele namhafte Unternehmen, Schulen, Universitäten und Krankenhäuser auch in Deutschland.

ATM ComputerSysteme GmbH M 09

Die ATM ComputerSysteme GmbH ist ein international aktives Systemhaus für gehärtete IT-Hardware und Software. Als langjähriger Partner der Bundeswehr ist die ATM seit mehr als drei Jahrzehnten erfolgreich. Fokus der Entwicklungen sind Computer- und Displaysysteme, Panel-PCs, mobile wie stationäre Kommunikationsanwendungen sowie die Erstellung leistungsfähiger und passgenauer Software. Die IT-Systeme trotzen härtesten Umweltbedingungen, wie sie zu Land, zu Luft und zu Wasser herrschen. Wer im internationalen Markt bestehen will, muss maßgeschneiderte Produkte präsentieren. Die ATM verwirklicht dies mit ihren innovativen Lösungen. Dienstleistungen und Beratung rund um das Produkt charakterisieren die Unternehmens- und Produktphilosophie.

Kontakt: ATM ComputerSysteme GmbH, Max-Stromeyer-Str. 116, 78467 Konstanz, Tel. 07531 8083, info@atm-computer.de, www.atm-computer.de

Atos Information Technology GmbH M 07

Atos ist ein weltweit führender Anbieter für die digitale Transformation mit Sitz in Bézons/Paris und München. Mit rund 120.000 Mitarbeitern erzielte die Atos Gruppe 2017 circa 13 Milliarden Euro Umsatz.
Als europäischer Marktführer für Big Data, Cybersecurity, High Performance Computing und Digital Workplace unterstützt Atos Unternehmen weltweit und begleitet die digitale Transformation von Kunden aus allen Branchen. Atos präsentiert auf der AFCEA seine Lösungskompetenz bei der Entwicklung und Betriebsunterstützung von einsatzfähigen IT-Plattformen (insbesondere Führungsinformationssystemen) und bietet Informationen zu Technologietrends.

Kontakt: Atos Information Technology GmbH
Franz-Geuer-Str. 10; D-50823 Köln
Hubert Geml (Leiter Defense), Tel: +49 (173) 9793 804, hubert.geml@atos.net;

Avitech GmbH S 10

Avitech GmbH, eine Tochtergesellschaft der Indra Sistemas S.A., ist seit über 20 Jahren kompetenter und verlässlicher Systempartner der Bundeswehr für das FSInfoSysBw und InfoDADBw. Unsere Kompetenzen liegen im Bereich der Aeronautischen und Hindernis Datenbank, Luftfahrtkarten, sowie Flugplan- und Pilotenbriefingssysteme inklusive Schnittstelle zur zivilen Flugsicherung und zu Eurocontrol. Darüber hinaus sind Meldungsvermittlungs- und Kommunikations-systeme sowie SWIM Lösungen bei der Bw im Einsatz. Avitech Produkte werden bundeswehrweit und von den in Deutschland stationierten Bündnispartnern an ca. 100 Standorten genutzt. Auf der AFCEA 2019 ist Interoperabilität, Datenversorgung für Missionsplanung und Datenvisualisierung unser Schwerpunkt.

Kontakt: Thomas Mattick, Program Manager Bundeswehr, Bahnhofplatz 3, 88045 Friedrichshafen, Telefon: +49(0)7541/282-0, www.avitech.aero

AVS Systeme GmbH ME 20

Der lebenswichtige Notruf, die entscheidenden Informationen oder die visuelle Unterstützung von Entscheidungsträgern in spezifischen Situationen – in jeder Branche gibt

es Momente, die nicht unterbrochen oder gestört werden dürfen. Die AVS hat sich auf die Planung und Realisierung von hoch technisierten Visualisierungssystemen in Leitstellen und Führungsräumen spezialisiert. Dank langjähriger Unternehmenserfahrung kann AVS Technologien und Lösungen garantieren, die zukunftsweisend und zuverlässig sind.
Hinter AVS steckt ein Team, das mit persönlichem Einsatz und Begeisterung für ihre Kunden über das Mögliche hinausdenkt. Nur so hat sich AVS in den letzten Jahren zum Markführer entwickelt, der in den entscheidenden Momenten den Unterschied macht.

Kontakt: AVS Systeme GmbH, Steinhäuserstraße 12, 76135 Karlsruhe,
Tobias Baader, COO, Telefon: +49 (0)721 96470 0, Direkt: +49 (0)721 96470 11,
Tobias.Baader@avs-systeme.com, www.avs-systeme.com

BAAINBw – Abt. G F 47

Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr

Die Deckung des Sachbedarfs der Streitkräfte wird innerhalb der Bundeswehrverwaltung im Bereich AIN wahrgenommen. Als Teil dieses Bereiches haben das **Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAAINBw) und sein Geschäftsbereich** die Aufgabe, die bedarfs- bzw. forderungsgerechte Ausstattung der Bundeswehr mit moderner Technik und modernem Gerät zu wirtschaftlichen Bedingungen zu gewährleisten.
Die Abteilung G - IT-Unterstützung im BAAINBW ist der zentrale Dienstleister für die administrative und logistische IT-Unterstützung in der Bundeswehr. Als wesentlichen Bestandteil digitalisiert die Abteilung G die Prozesse der Bundeswehr und stellt qualifiziert und zuverlässig IT-Services für die gesamte Bundeswehr bereit.

BAKO Systemintegration GmbH & Co. KG F 51

BAKO Systemintegration

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

BDSV F 61

BDSV

Der Bundesverband der Deutschen Sicherheits- und Verteidigungsindustrie vertritt rund 80 privatwirtschaftlich organisierte Unternehmen aus den Bereichen Sicherheit, Verteidigung & Digitales und unterstützt in seiner Arbeit den Erhalt und die Stärkung der Wettbewerbs- und Zukunftsfähigkeit der deutschen Sicherheits- und Verteidigungsindustrie (SVI) und des Technologie- und Wirtschaftsstandortes Deutschland. Wir sind Ansprechpartner für Politik, Ministerien, andere Staaten sowie Medien und Öffentlichkeit. Der Verband agiert als branchenübergreifende Interessenvertretung, sowohl national als auch international. Dies beinhaltet sowohl die Wahrnehmung als Point of Contact für die NATO Industrial Advisory Group (NIAG) als auch die Koordination der Aktivitäten innerhalb der AeroSpace and Defence Industries Association of Europe (ASD), www.bdsv.eu

Bechtle AG F 11

BECHTLE

Bechtle AG: starker IT-Partner öffentlicher Auftraggeber
Über den Rahmenvertrag 2./3. Rechnerebene R1112 stattet Bechtle die Bundeswehr mit Informationstechnologie und Dienstleistung aus. Das Kerngeschäft umfasst dabei den Bereich Handelsware mit mobilen Endgeräten, PCs, Peripherie, Drucker, Server, Speichersysteme, USV-Anlagen sowie systemnaher Software. Daneben zählen Dienstleistungen wie Planung, Installation und Konfiguration von IT-Umgebungen & Netzwerken, IT-Sicherheitskonzepte (SiKo nach Vorgaben ZdV 960/1 in SAVe), Cyber Resilience oder aber Service- & Systemsteckbriefe und Enterprise Architecture nach NATO Architecture Framework (NAF) zum Leistungsportfolio. Teilekennzeichnung (TKZ) von Geräten, Gütern und Behältern mit grafischen Codierungen und Nummernkreisen runden das Dienstleistungsportfolio ab.

Besuchen Sie uns auf dem Stand F11 im Foyer I der AFCEA Fachausstellung.
Mehr erfahren Sie zu Bechtle unter: www.bechtle.com

Behörden Spiegel / ProPress Verlagsgesellschaft mbH F 20

Behörden Spiegel

Seit 35 Jahren berichtet der Behörden Spiegel über die Belange des Öffentlichen Dienstes. Mit einer Druckauflage von 114.000 Exemplaren und nachweislichen Verbreitung von 113.386 (IV. Quartal 2018, IVW), ist der Behörden Spiegel das Medium bei Staat, Ländern und Kommunen. Der Behörden Spiegel widmet sich intensiv auch der Sicherheitspolitik und Wehrtechnik. Die Digitalisierung steht dabei im Vordergrund. Dafür arbeiten Redaktionen in Berlin und Bonn intensiv an diesen Themen.
Der Behörden Spiegel hebt ab: er ist in den Zeitungsauslagen und Lounges der Lufthansa zu finden. Quantität und Qualität müssen stimmen. Hohe Auflage, Visibilität auch in der Allgemeinheit und Präzision in der Berichterstattung – damit können die Belange auch der Sicherheitspolitik und Verteidigung erfolgreich platziert werden!
Der Behörden Spiegel ist zudem Veranstalter großer Sicherheitskongresse, u.a. der Berliner Sicherheitskonferenz, des Europäischen Polizeikongresses, des Europäischen Katastrophenschutzkongresses und der PITS (Public IT-Security).
www.behoerdenspiegel.de

Bell Computer-Netzwerke GmbH S 03

BELL COMPUTER-NETZWERKE

BELL Computer-Netzwerke GmbH ist ein führendes herstellerneutrales IT-Systemhaus. Seit mehr als 25 Jahren entwickeln qualifizierte IT-Spezialisten innovative und serviceorientierte Lösungen in den Bereichen Networking, IT-Security, Mobility und Voice. Verfügbarkeit, Automatisierung und Visualisierung stehen dabei im Vordergrund sowie sichere Kommunikation durch Endgeräte von deutschen Herstellern, die bereits den Rufaufbau verschlüsseln. Zu den Kunden gehören zahlreiche Bundesbehörden sowie mittelständische Unternehmen. Diese schätzen allesamt die Qualität, Erfahrung, Kompetenz und Flexibilität des Unternehmens. Eine intensive Partnerschaft mit führenden Herstellern ermöglicht ein kontinuierliches Wachstum und reflektiert die Marktpräsenz der BELL Computer-Netzwerke GmbH. www.bell.de
Kompetenz: Enterprise Network & Security Infrastructure, SDN, Network-Access-Control (NAC), Firewall, UTM, IPS/SIEM, Network-Analytics & Monitoring, Voice over IP

best Systeme GmbH ME 16

best SYSTEME GMBH

Gegründet 1994 als Systemintegrator für Enterprise Rechenzentren, ist heute ein auf **Rechenzentrumstechnologie spezialisiertes Beratungshaus**.
25 Jahre waches Interesse an neuester Technologie, bilden die Basis für eine herstellerunabhängige Beratung.
Im Rahmen eines geförderten Verbundprojektes des BMBF demonstrierten wir eine technologische Spitzenposition im Bereich **„Big Data Analytics“**.

Zusammen mit unserem Partner Endace Europe Ltd präsentieren wir Ihnen Lösungen für High Performance Network Recording – 100% des Netzwerksverkehrs stehen für forensische Analysen (z.B. bei Datenschutzverletzungen) zu Verfügung. Nur wer 100%-ig weiß, was in seinem Netzwerk passiert, kann Angriffe abwehren oder Ursachen von Performance-Einbrüchen identifizieren.

Kontakt: best Systeme GmbH, Münchner Straße 123A, 85774 Unterföhring, 089/20603080, www.best.de

Bittium S 02

Bittium ist ein renommiertes finnisches Unternehmen mit über 30 Jahren Erfahrung in Technologien für Funkkommunikation mit bewährten Informationssicherheitslösungen für mobile Geräte und tragbare Computer.
Für den Verteidigungs- und Sicherheitsmarkt bietet Bittium modernste Produkte und Lösungen für taktische und sichere Kommunikation, die allen Truppen auf jeder Position Breitbanddaten und Sprache garantieren. Im Gesundheitswesen bietet Bittium Produkte und Dienstleistungen in der Biosignalmessung in den Bereichen Kardiologie, Neurologie, Rehabilitation, Arbeitsmedizin und Sportmedizin an. Bittium erbringt professionelle Ingenieursdienstleistungen und Technologieexpertise auf den Gebieten drahtlose Geräte, Netzwerkinfrastruktur und IoT-Lösungen sowie in den Bereichen 5G, künstliche Intelligenz (KI), robotergesteuerte Prozessautomatisierung (RPA) und Cloud Solutions. Bittium ist an der Nasdaq Helsinki gelistet. www.bittium.com.

blackned gmbh M 01

Die blackned gmbh ist Softwarehersteller und Beratungsunternehmen für sichere Kommunikations- und Datenübertragungslösungen mit Sitz in Süddeutschland. Mit ihrem Beratungs-und Produktportfolio stellt die blackned gmbh Ihren Kunden ganzheitliche Systemlösungen für Kommando-, Kontroll- und Kommunikationsanwendungen für unterschiedlichste Branchen und Industriesegmente zur Verfügung.
Im militärischen Bereich ist das Unternehmen führender Kompetenzpartner in der Konzeption und dem Betrieb mobiler und verlegefähiger Netzwerke. Für den zivilen Bereich bietet die blackned gmbh Lösungen für private, zellulare Daten- und Kommunikationsnetzwerke auf Basis der eigenentwickelten Softwareplattform RIDUX .
blackned – critical command and control solutions. anywhere.

Broadcast Solutions GmbH F 55

Mit mehr als 120 Mitarbeitern weltweit und Dependancen in Europa, Asien und Middle East ist die Broadcast Solutions GmbH einer der größten Systemintegratoren Europas im Bereich Broadcast-Technik. Mit jahrelanger Erfahrung im Broadcast-Bereich bietet das Unternehmen das nötige Know-how und die technischen Möglichkeiten, um dem BOS-Bereich komplett neue und innovative Produkte und Komplettlösungen für den taktischen und strategischen Einsatz anzubieten. Wir stellen unseren Kunden neuartige Lösungen zur Verfügung, die für Up- und Downlink im Bereich der Satellitenkommunikation (VSAT), moderner COFDM Übertragungstechnologie oder drahtloser Kommunikation mit Mesh-Netzwerken zur Übertragung von Daten, Audio und hochauflösendem Video-Material entscheidende Vorteile bieten.

Kontakt: Broadcast Solutions GmbH, Alfred-Nobel-Str. 5, D-55411 Bingen am Rhein

BWI GmbH M 19

Die BWI GmbH gehört als 100-prozentige Bundesgesellschaft zu den Top-10-IT-Service-Unternehmen in Deutschland. Neben dem verlässlichen und sicheren Betrieb von weiten Teilen des IT-Systems der Bundeswehr entwickelt die BWI die IT-Infrastruktur der Bundeswehr weiter und bietet dieser zukunftsweisende und sichere Services. Zusätzlich zu IT-Dienstleistungen für die Bundeswehr bietet die BWI als IT-Dienstleistungszentrum des Bundes ihre Lösungen auch anderen Ressorts der Bundesregierung an und spielt eine wichtige Rolle in der „IT-Konsolidierung Bund“. Die BWI präsentiert sich bei der AFCEA Fachausstellung 2019 als kundenorientiertes IT-Systemhaus und als verlässlicher Partner der Bundeswehr. www.bwi.de

CANCOM on line GmbH B 13

Die CANCOM on line GmbH ist aufgrund seiner mehrjährigen Erfahrung im Public-Sektor optimal darauf eingestellt, die dedizierten Anforderungen von Bund, Ländern und Kommunen zu erfüllen. Darüber hinaus unterstützen wir seit Jahren Sicherheitsbehörden sowie die Bundeswehr. Unser bundesweit agierendes Team erfasst Ihre speziellen Ansprüche und bietet maßgeschneiderte Lösungen und Dienstleistungen für diesen Bereich an.
Seit 2016 hält die CANCOM den Rahmenvertrag für Virenschutz der Bundesverwaltung, auf den auch die Bundeswehr als Bedarfsträger beschaffen kann.
Mit CANCOM Public Solutions betreuen wir Sie umfassend in verschiedenen Bereichen des Öffentlichen Sektors:

- Gewährleistung einer sicheren und störungsfreien IT Infrastruktur
- Umfassender Schutz personenbezogener Daten
- Individuelle Beratung und Konzeptionierung einer IT Architektur für Ihre Bedürfnisse
- Branchenspezifische Lösungen und umfassendes Know How im Public Bereich, seit 25 Jahren

Carl-Cranz-Gesellschaft e.V. ME 08

Gesellschaft für 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 mehr als 55 Jahren. Gemeinsam mit führenden Experten aus Forschung & Entwicklung sowie Industrie erarbeiten wir das Potenzial zukunftsträchtiger Technologien und stellen bedarfsgerechte, praxisorientierte Fort- und Weiterbildungen in unserem Seminarzentrum in Oberpfaffenhofen, an weiteren Standorten in Deutschland, Frankreich, Österreich, der Schweiz 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 Aufklärungssystemsysteme, Mobilität / Transport- und Verkehrssysteme, Sensorik, Verteidigung- und Sicherheitstechnik, Werkstoffkunde und Werkstofftechnologie sowie fachgebietsübergreifende Querschnittsthemen.

Carmenta AB F 21

Carmenta Geospatial Technologies AB
Seit mehr als 30 Jahren entwickelt Carmenta erstklassige Software für missionskritische Systeme wie Anwendungen für Verteidigung und Public Safety, bei denen Superior Situational Awareness unerlässlich ist. Carmenta hat ein umfassendes Portfolio leistungsstarker Softwareprodukte zur Missionsoptimierung mit Geodaten in Echtzeit entwickelt. Unsere Produkte und Lösungen werden derzeit von mehreren Streitkräften in allen drei Bereichen eingesetzt: Luft, Land und See. Eine enge Zusammenarbeit mit unseren Anwendern ermöglicht es uns, unsere Lösungen so zu optimieren, dass sie alle neuen oder zukünftigen Anforderungen erfüllen.

Kontakt: Carmenta Germany GmbH, www.carmenta.com , Bernhard Jungwirth, Hopfenstrasse 8, D-80335 München, Tel: +49 162 2718891, bernhard.jungwirth@carmenta.com

Cellebrite F 54/Salon HAUPTMANN

Digitale Datengewinnung für eine sicherere Welt.
Digitale Daten spielen zunehmend eine wichtige Rolle bei Ermittlungen und Operationen aller Art. Diese Daten macht Cellebrite verfügbar, gemeinsam nutzbar und verwertbar.
Wir bieten Strafverfolgungsbehörden, Militär, Geheimdiensten und Unternehmen die umfangreichsten bewährten Lösungen für die digitale Forensik, Sichtung und Analyse.

Unsere Produkte, Lösungen, Service- und Schulungsangebote unterstützen unsere Kunden dabei, ihre komplexesten Fälle schnell zu lösen, indem wir ihnen das Abrufen, die gemeinsame Nutzung und die Analyse der digitalen Daten von mobilen Endgeräten, den sozialen Medien, Cloud-Diensten, Computern, Mobilfunkbetreibern und anderen Quellen ermöglichen.
Cellebrite ist der beliebteste Komplettanbieter von Lösungen für die digitale Datengewinnung und macht die Welt jeden Tag etwas sicherer. www.cellebrite.com

CeoTronics AG M 31

Stärkung der äußeren Sicherheit durch bessere Kommunikation
Die Entwicklung von Kommunikationssystemen für den militärischen Einsatz erfordert ein hohes Maß an Erfahrung und Fachwissen über mögliche Einsatzszenarien. Im Zuge der wachsenden Auslandseinsätze ändern sich zudem die speziellen Anforderungen der Nutzer, nicht nur in Bezug auf die klimatischen Umgebungsbedingungen. CeoTronics verfügt über mehr als 30 Jahre Erfahrung in der Entwicklung und Herstellung von komplexen Kommunikationssystemen, die die geforderten Schutzprüfungen, wie z. B. MIL STD 810G, 461F und IP65/IP66/IP67, erfüllen.
CeoTronics ist „registered NATO supplier“ und als offizieller Zulieferer der NATO anerkannt.

Kontakt: CeoTronics AG, Audio • Video • Data Communication, Adam-Opel-Str. 6, 63322 Rödermark (Germany), Tel. +49 6074 8751-0, Fax +49 6074 8751-265, verkauf@ceotronics.com, www.ceotronics.com

CGI Deutschland Ltd. & Co. KG F 09

CGI, gegründet 1976, ist ein globaler Dienstleister für IT und Geschäftsprozesse, der mit 70.000 Mitarbeitern Business- und IT-Beratung, Systemintegration und Outsourcing-Services auf Top-Niveau anbietet. Unsere langjährige Erfahrung in der Zusammenarbeit mit Auftraggebern aus Militär und BOS ist der Garant für höchste Qualität, Innovation und Einsatzorientierung unseres Portfolios an marktverfügbaren Produkten und Dienstleistungen. Wir präsentieren Lösungen für den Einsatz (HaFIS) sowie für die Herausforderungen im Bereich der Cyber-Sicherheit. Mit DokMBw demonstrieren wir die Zukunft für die Stabs- und Verwaltungsarbeit. Wir freuen uns auf spannende Gespräche und den Erfahrungsaustausch im Kontext von strategischer Ausrichtung, Outsourcing und Cloud für die Bundeswehr und BWI.

Kontakt: CGI Deutschland Ltd. & Co. KG, Andreas Pankratz, T. +4922036993-0, andreas.pankratz@cgi.com, de.cgi.com

CHIFFRY GmbH F 49

Chiffry Unterstützungssystem für sichere Einsatzkommunikation
Chiffry ist eine Kommunikationsplattform für Smartphone 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 abgehärtete Betriebssysteme, Container-Lösungen wie beispielsweise MobileIron und Samsung Knox sowie in die VPN-Infrastrukturen.
www.chiffry.de

Cisco Systems GmbH B 12

Netzwerke sind heute wichtiger Teil der Infrastruktur im Bereich der Verteidigung. Die von Cisco entwickelten Produkte auf Basis des Internet-Protokolls sind Grundlage dieser Netzwerke und machen Cisco zum weltweit führenden Anbieter. Für Institutionen im Bereich der Verteidigung eröffnet die Vernetzung über die Domänen Heimatland, verlegefähige Systeme, mobile Infrastrukturen und abgesessene Einheiten sowie mit Koalitionspartnern zahlreiche Möglichkeiten: Durch intelligentes Zusammenspiel von Personen, Prozessen, Daten und Dingen können Prozesse optimiert, Ressourcen effizienter und sicher genutzt und Vorteile in allen Domänen für Aufklärung, Gefecht, Logistik und Sanitätswesen realisiert werden.
Im Geschäftsjahr 2017/18 erzielte Cisco einen Umsatz von 49,33 Milliarden $ mit weltweit mehr als 70.000 Mitarbeitern.

Citrix Systems GmbH ME 21

Citrix entwickelt Lösungen für eine Welt, in der Menschen, Organisationen und Dinge sicher miteinander vernetzt sind, um das Außergewöhnliche zu erreichen. Citrix unterstützt seine Kunden dabei, die Zukunft der Arbeit neu zu denken, indem das Unternehmen den umfassendsten sicheren digitalen Arbeitsplatz anbietet. Dieser vereint Anwendungen, Daten und Services, die Menschen brauchen, um produktiv zu sein und hilft der IT-Abteilung, komplexe Cloud-Umgebungen einfacher einzuführen und zu verwalten.
Mehr als 400.000 Organisationen, inklusive 99 Prozent der Fortune 100 und 98 Prozent der Fortune 500, setzen weltweit auf Lösungen von Citrix. Weitere Informationen unter http://www.citrix.de.

cloudera F 23

Cloudera, Inc. (NYSE: CLDR), the enterprise data cloud company,
About Cloudera: At Cloudera, we believe that data can make what is impossible today, possible tomorrow. We empower people to transform complex data into clear and actionable insights. Cloudera delivers an enterprise data cloud for any data, anywhere, from the Edge to AI. Powered by the relentless innovation of the open source community, Cloudera advances digital transformation for the world’s largest enterprises. Learn more at cloudera.com.

Cobham Mast Systems ME 01

Mastsystem Int´l Oy trading as Cobham Mast Systems
Cobham Mast Systems is the leading manufacturer and supplier of lightweight telescopic composite masts and mast systems.
Cobham Mast Systems’ know-how and understanding of customers’ specific needs and requirements are based on more than 30 years of experience. It’s lightweight telescopic masts are used extensively around the world by defence forces, police and other emergency services.
There are seven main product lines: TM-, TR-, EX-, EXL- and EXB-masts, telescopic lifting poles and tripods including accessories for deployment. In addition to the industry’s widest product range, Cobham Mast Systems also provides custom, fully integrated solutions precisely tailored to the application. All products are designed to meet the most demanding requirements of transportable communication, intelligence, surveillance, reconnaissance and broadcast systems.

The company has certified quality system ISO9001, ISO14001 and AQAP2110.

Kontakt: Tel. +358 20 775 0810, Fax. +358 13 737 7113, Email: mastsystem(at) cobham.com, www.cobham.com/mastsystems

Computacenter M 06

Computacenter ist Europas führender herstellerübergreifender Dienstleister für Informationstechnologie. Kundennähe bedeutet für uns, Geschäftsanforderungen zu verstehen und präzise darauf einzugehen. Auf dieser Basis entwickeln, implementieren und betreiben wir für unsere Kunden maßgeschneiderte IT-Lösungen.
Darüber hinaus hält Computacenter diverse Rahmenverträge mit Landesministerien und Dienstleistungszentren verschiedener Länder und Kommunen, sowie dem Bund.
Weitere Informationen erhalten Sie gerne an unserem Stand oder über Patrick Pensel, Direktor Geschäftsfeldentwicklung für den Bereich Öffentliche Auftraggeber (Patrick.Pensel@computacenter.com).

Comrod Communication AS F 24

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 ComPact series power supplies and battery chargers provide the best power to size density available on the market today.
For all product enquiries please email sales@comrod.com

Condok GmbH S 05

Die CONDOK GmbH ist ein Systemhaus für technische Dienstleistungen, System-Entwicklung und Realisierung. Neben der Spezialisierung auf die Erstellung von IETD nach S1000D/ S2000M werden vielfältige und umfangreiche Technische Dokumentationen, Bebilderte Teilekataloge, Technische Übersetzungen und Computer Based Trainings erstellt. Als Systemhaus entwickelt und realisiert CONDOK Einrüstungs- und Umrüstungsmaßnahmen in Kabinen und Fahrzeugen und führt Instandsetzungsleistungen durch. Das Portfolio wird durch die Bereiche der Produkt- und Betriebssicherheit sowie Themen des Integrated-Logistic-Support abgerundet. Mit mehr als 130 Mitarbeitern in Kiel, Hamburg und Koblenz unterstützt die CONDOK mit umfangreichen technischen und logistischen Dienstleistungen die Bundeswehr sowie eine große Anzahl von Unternehmen der Wehrtechnik und der zivilen Industrie.

Kontakt: www.condok.de

CONET F 05

„Erfolg. Unsere Leidenschaft.“ Die CONET-Gruppe ist das kompetente IT-System- und Beratungshaus für SAP, Infrastructure, Communications, Software und Consulting in den Schwerpunktbereichen Cyber Security, Cloud, Mobility und Big Data. Seit mehr als 30 Jahren unterstützt CONET als IT-System- und Beratungspartner die Bundeswehr und begleitet sie zuverlässig auf dem Weg zur digitalisierten Streitkraft. Durch partnerschaftliche Zusammenarbeit, Innovationsfähigkeit, Betriebs-Know-how und hohe Dienstleistungsqualität entstehen erfolgreiche Implementierungen für Fach- und Führungsinformationssysteme, SAP, Kommunikationsarchitekturen und IT-Infrastrukturen. An ihrer Plan-Bar (Stand F 06) präsentiert die CONET-Gruppe aktuelle Lösungen etwa für Cyber Security, strategisches IT-Management mit EAM und Entwicklungsansätze für schnellere und gleichzeitig einfachere Prozesse mit SAP HANA.

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

conpal GmbH S 09

Die conpal GmbH ist ein Anbieter von Lösungen im Bereich IT-Sicherheit mit Fokus auf den Themen Endgeräte-Sicherheit, Authentisierung, sowie Identity und Access Management. Grundlage des Angebotes sind eigenentwickelte Standard-Software-Lösungen und Technologien sorgfältig ausgewählter Partnerunternehmen. Durch kontinuierliche Analyse von Markt- und Technologieentwicklungen erreichen wir in unserem Portfolio einen optimalen Mix zukunftssicherer Technologien in Verbindung mit praxisorientierter Umsetzung. Die Lösungen von conpal sind konsequent an den Bedürfnissen der Kundenumgebungen ausgerichtet, einfach einzuführen und verhalten sich robust im Betrieb.

Cordsen Engineering GmbH F 12

CORDSEN Engineering GmbH entwickelt und fertigt eine breite Palette an militärisch gehärteten (Ruggedized) Workstations und Peripheriegeräten nach MIL-STD-810F / MIL-STD-461E für mobilen und stationären Einsatz, sowie abstrahlsichere (TEMPEST) Produkte nach SDIP 27 Level A , wie Workstations, Server, TFT-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 Kurzmessungen nach dem Zonenmodell des BSI (Zone 1/2/3). Als Dienstleistungen bieten wir u. a. Platform-Testing an.
Kontakt: Cordsen Engineering GmbH, Am Klinggraben 1A, D-63500 Seligenstadt Tel. 06182-9294-0, Fax 06182-9294-45, www.cordsen.com

CP Cases F 51

CP Cases designs and manufactures high-performance, protective cases and racks used for transport, operation and storage of essential equipment in commercial and military applications. Our products are designed to achieve optimum standards and accreditations with many rated to MIL-STD-810 and IP65 / IP66 and carry NATO stock numbers.
Field ready for extreme weather conditions our range of product are designed with an additional range of customised features; climate control (compressor and thermoelectric air conditioning units), EMC shielding; also fire resistance, and anti-static capabilities.
For more information about CP Cases and our partners BAKO visit us on stand: F51

CPM GmbH ME 06

Das 1989 gegründete Unternehmen mit Sitz in Bonn ist seit Jahren enger Partner von Streitkräften, Politik und Industrie. Das etablierte Fachmagazin cpm forum bietet eine seriöse Plattform in den Bereichen Rüstung, Streitkräfte und Sicherheit. Veranstaltungen wie das Anwenderforum Logistik (LOG.NET), das Anwenderforum Rüstung und Nutzung (RÜ.NET) oder diverse Vortragsreihen im In- und Ausland bieten den Teilnehmern und Ausstellern ein hochkarätiges Format mit Expertenvorträgen. Im Dienstleistungssektor stehen wir unseren Partnern mit Erfahrung und Fachexpertise in Public Affairs und Marketing beratend zur Seite.
Kontakt: www.cpm-verlag.de

crisis prevention / BETA Verlag & Marketinggesellschaft mbH — ME 07

CRISIS PREVENTION (CP) ist das behördliche Fachmagazin für Gefahrenabwehr, Innere Sicherheit und Katastrophenhilfe und deckt das breite Spektrum an redaktionellen Inhalten ab, was fach- und ressortübergreifend notwendig ist, um die Leserschaft umfassend auf dem aktuellen Stand zu halten und eine Hilfestellung zur täglichen Aufgabenbewältigung und Einsatzoptimierung zu leisten.
CP ist die geeignete Plattform für ihre Unternehmenskommunikation, um Entscheidungsträger branchenübergreifend mit nur einem Magazin direkt zu erreichen. Sie haben Interesse an einer Zusammenarbeit? Sprechen Sie uns einfach an! crisis-prevention.de

Kontakt: André Birr, Objektleitung / Media Sales, CRISIS PREVENTION (CP), BETA Verlag & Marketinggesellschaft mbH | Celsiusstraße 43 | 53125 Bonn, Tel.: +49(0)228 / 91937-68 | Mobil: +49(0)178 / 4486720 | Fax: +49(0)228 / 91937-23, andre.birr@beta-publishing.com | www.crisis-prevention.de | www.beta-publishing.com

Cubic Mission Solutions — S 02

Sichere Netzwerklösungen
Cubic entwickelt Netzwerk- und Kommunikationstechnologien für den mobilen taktischen Bereich, die extreme Modularität, Redundanz, Zuverlässigkeit und Leistungsfähigkeiten bieten.
Durch ein ineinandergreifendes Schienensystem können die Module schnell, sowohl horizontal als auch vertikal, zusammengeschoben bzw. wieder getrennt werden.
Die Produktpalette umfasst Router, Switche und Lösungen die die Übertragung von Sprache, Daten und Video über ein breites Spektrum von Technologien hinweg ermöglichen (z.B. PTT-Radios, zellulare Netze, WLAN, SatCom).

Cyber Security Cluster Bonn e.V. — F 04

Das Cyber Security Cluster Bonn e.V. bündelt alle in der Region Bonn/Rhein-Sieg ansässigen Security-Einrichtungen aus Wissenschaft, Wirtschaft und öffentlichen Institutionen. Ziel der Initiative ist es, dazu beizutragen, die Region zu einem international beachteten Cyber-Security Standort auszubauen und Bonn als „Herz der Cyber Security in Europa“ erlebbar zu machen.
Dies geschieht über verschiedene inhaltliche Schwerpunkte. Dazu zählen die Organisation von Veranstaltungen zur Sensibilisierung von Unternehmen und Gesellschaft, die Unterstützung von Security Startups, der Einsatz eines Wise Councils of Cyber Security Experts, die kooperative Weiterentwicklung von Aus- und Weiterbildungsprogrammen sowie die Unterstützung kooperativer Forschung.

Kontakt Cyber Security Cluster Bonn e.V., Godesberger Allee 139, ,53175 Bonn, Tel.: +4915143862131, E-Mail: christian.schmickler@mail.de, Web: https://cyber-security-cluster.eu

dainox GmbH — M 25

dainox ist ein Hersteller verlegefähiger Kommunikationslösungen der Bundeswehr und etablierter Dienstleistungsanbieter in den Themengebieten Internetworking, Computing und Virtualisierung. dainox unterstützt bei der Planung, Implementierung, Dokumentation und dem Betrieb von IT Infrastrukturen. Mit Hilfe der dainox Strategie- und IT Architekturberatung werden nachhaltige und langlebige IT Lösungen geschaffen.
In unseren Projekten wird über eine enge Zusammenarbeit mit dem Kunden ein effizienter Ablauf mit einem optimalen Know-how Transfer garantiert und so eine hohe Wertschöpfung ermöglicht.
Gebündeltes Fachwissen auf den Punkt gebracht – dainox ®.

Konatkt: dainox GmbH, info@dainox.net, www.dainox.net

DataVision Deutschland GmbH — ME 12

Moderne Kommunikation mit zeitgemäßer Technik – DataVision Deutschland GmbH ist Ihr bundesweiter Partner für professionelle Konferenz- und Präsentationstechnik und garantiert Ihnen innovative und zukunftsweisende Beratung und Betreuung.
Profitieren Sie von unserem umfassenden und aufeinander abgestimmten Produktsortiment mit über 8.000 Artikeln führender Hersteller, maßgeschneiderten Konferenzräumen mit
intuitiver Medientechnik, sowie von modernsten Lösungen zur interaktiven Zusammenarbeit.
Komplettlösungen aus einer Hand: Ein Anruf genügt und schon steht Ihnen unser kompetentes Team engagiert mit einem kundenorientierten Full-Service-Angebot zur Seite.

Kontakt: DataVision Deutschland GmbH, Gesellschaft für audio-visuelle Kommunikationssyteme, Am Trippelsberg 45, 40589 Düsseldorf, Telefon: +49 (0)211 / 74008-0, Telefax: +49 (0)211 / 74008-30, E-Mail: info@datavision.net. Webseite: www.datavision.net

Dell Technologies — M 03

Dell Technologies (www.delltechnologies.com) ist eine einzigartige Unternehmensfamilie, die Organisationen mit der nötigen Infrastruktur ausstattet, damit sie ihre Zukunft digital gestalten, ihre IT nachhaltig transformieren und Informationen als ihr wichtigstes Gut wirksam schützen können. Das Unternehmen unterstützt Kunden jeder Größenordnung mit dem branchenweit umfangreichsten und innovativsten Portfolio, vom Client über Lösungen für das Rechenzentrum bis in die Cloud.

DEUTSCHE GESELLSCHAFT FÜR WEHRTECHNIK e.V. (DWT) — F 48

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.

DICOTA SCHWEIZ AG — F 57

Das DICOTA Fundament basiert auf den Säulen **Passion * Kompetenz * Verbindlichkeit * Präzision * Fairness** und wird von einem engagierten und motivierten Team getragen. Deutsche Produktentwicklung, Schweizer Qualitätsverständnis und internationales Flair in einem inhabergeführten Unternehmen ermöglichen den Blick fürs wichtige Detail.
Mit Kunden, Lieferanten und Mitarbeitenden pflegen wir eine offene, ehrliche

und nachhaltige Partnerschaft.
Profitieren Sie von über 25 Jahren Erfahrung in der Entwicklung und Herstellung von erstklassigen Tragelösungen und setzen auf «Die Computer Tasche – DICOTA». Unser Name ist ein Versprechen.

Kontakt vor Ort:
Danny Weber, Account Manager, Danny.weber@dicota.com, 0173-450 95 05

DIGITTRADE GmbH F 49

Externe verschlüsselte Festplatten mit BSI-Zertifizierung
Mit der externen Festplatte HS256 S3 bietet die DIGITTRADE GmbH Behörden und Unternehmen eine professionelle Lösung zum sicheren Transport von sensiblen Daten und zur Erstellung von datenschutzkonformen Backups. Dieser Datenträger schützt zuverlässig sensible Informationen vor unbefugten Zugriffen falls er verloren, gestohlen oder anderweitig entwendet wird.
KOBRA Stick - verschlüsselter USB-C Speicherstick mit Smartcard und PIN-Eingabe
Der KOBRA Stick ist eine Ausstellungsneuheit, die ebenfalls für Behörden und Unternehmen bestimmt ist. Die Vertraulichkeit der Daten wird durch die 256-Bit AES-Verschlüsselung mittels Verwendung zweier 256-Bit-Kryptoschlüssel, die Zwei-Faktor-Authentifizierung mittels Smartcard und PIN sowie die Verwaltung der Krypto-Schlüssel gewährleistet.
www.digittrade.de

DriveLock SE S 09

Das deutsche Unternehmen DriveLock SE ist seit über 15 Jahren einer der international führenden Spezialisten für die IT- und Datensicherheit. Mit seiner Endpoint Protection Platform hat sich das Unternehmen weltweit einen Namen gemacht.
Herausragend ist DriveLock insbesondere aufgrund seiner extrem granularen Konfiguration im Device Control für USB- und anderen Schnittstellen sowie bei der Verschlüsselung von Festplatten (FDE) und Daten auf mobilen Datenträgern. Mit Smart AppGuard und integrierter Artificial Intelligence, sowie Predictive Whitelisting und Machine Learning können Applikationen und Geräte umfassend geschützt werden. Somit bietet DriveLock einen vollen Rundumschutz vor digitalen Gefahren für alle Endgeräte.

DSI Datensicherheit GmbH B 01

„Data Security for Harsh Environments“
DSI Datensicherheit GmbH entwickelt seit vielen Jahren hochsichere Kommunikationslösungen u.a. für den Space Bereich. Space Missionen stellen die höchsten Anforderungen sowohl an die Elektronik wie auch an die Sicherheit/Verschlüsselung der Kommunikation. Abgeleitet aus diesen Projekterfahrungen im technologischen Grenzbereich der Satelliten- und Drohnenprojekte realisiert DSI Datensicherheit innovative, hochsichere Übertragung- und Kryprografiesysteme, auch für Projekte außerhalb des Aerospace Bereichs. Hochsichere Kommunikation und Abstrahlsicherheit (TEMPEST) gehören in vielen öffentlichen Projekten zusammen. DSI Datensicherheit GmbH verfügt über beide Kernkompetenzen im Unternehmen und realisiert Projekte von der Studie bis zur komplexen Elektronik- und Softwareentwicklung, inklusive der TEMPEST Zertifizierungen im firmeneigenen Labor.

Kontakt: www.dsi-ds.de / Dirk.Stabenow@dsi-ds.de

DXC Technology Deutschland GmbH B 06

DXC Technology (DXC: NYSE) ist der weltweit führende unabhängige End-to-End IT-Dienstleister. Das Unternehmen führt die digitale Transformation für seine Kunden durch, indem es die klassische IT modernisiert und integriert sowie digitale Lösungen passgenau einsetzt, um bessere Geschäftsergebnisse zu erzielen. Die technologische Unabhängigkeit des Unternehmens, seine globalen Talente und das umfangreiche Partnernetzwerk ermöglichen es 6.000 privaten und öffentlichen Kunden in 70 Ländern, von Veränderungen zu profitieren. DXC ist ein anerkannter Marktführer im Bereich Corporate Responsibility. Weitere Informationen finden Sie unter dxc.technology und erkunden Sie hier THRIVE, die Thought Leadership Plattform von DXC für Changemaker und Innovatoren.

Kontakt: DXC Technology Deutschland GmbH, Valoisplatz 2, 26382 Wilhelmshaven, Sascha Sterly, Head of Defense, ssterly@dxc.com, +49 4421 9479 612, Mobil: +49 160 963 263 93

ECOS Technology GmbH F 29

ECOS TECHNOLOGY GMBH
ECOS hat sich auf die Entwicklung und den Vertrieb von IT-Lösungen für den sicheren Fernzugriff auf zentrale Daten und Anwendungen zur Gewährleistung eines erhöhten Schutz vor Spionage und Cyberangriffen bei gleichzeitiger Senkung der Kosten spezialisiert.
Die BSI-zugelassene Lösung **ECOS SECURE BOOT STICK [SX]** ermöglicht einen hochsicheren Fernzugriff auf Citrix, VMware Horizon oder Webanwendungen der Bundeswehr, von jedem beliebigen PC oder Mac aus.
Unsere Themenschwerpunkte auf der AFCEA 2019:
- Hochsicherer Remote-Zugriff (z.B. auf VS-NfD-Daten)
- Stärkung der Bundeswehr als attraktiver Arbeitgeber
- Remote Access in Weiterbildung und Schulung
- Einbindung von Reservisten in die IT-Infrastruktur
- Ortsunabhängiger Zugriff auf SASPF oder LoNo

EGL Elektronik Vertrieb GmbH M 29

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

ELESIA S 02

Elesia S.p.A. wurde 1981 in Rom als Militärisches Systemhaus gegründet. Die Zielmärkte sind:
- Home-Land Security (HLS)
- Wideband HF / SOTM Ku/Ka / Wave Relay® MANET
- Verkehrstechnik
- Naval / Air / Vehicular MFC Konsolen

Elesia hält eine führende Position im italienischen und internationalen Markt zur Lieferung von Composite-Leichtbau-Konsolen und Embedded ComputerPlattformen als „Turnkey-Lösungen für anspruchsvolle Defence-, HLS- und Verkehrstechnik-Anwendungen“.
Elesia’s Stammsitz liegt in Rom, heimische und internationale Vertriebs-Repräsentanzen befinden sich in Bologna, Turin, München, Madrid, Paris, Tel Aviv, Bangalore und Peking.
Lokaler

Kontakt (Deutschland): Elesia S.p.A. – Branch Office Munich, www.elesia.it, Tel.+49-151-22631505, mailto:tomas.vonluepke@elesia.it

ELNO GmbH B 02

Die ELNO GmbH ist Mitglied der internationalen Unternehmensgruppe ELNO bestehend aus mittelständischen Firmen in Frankreich, Italien und Deutschland. Firmensitz ist Grünstadt in der Pfalz. Wehrtechnischer Umsatzanteil 90%. **ELNO ist Hersteller elektronischer Kommunikationsgeräte und –systeme und verfügt über:**

- eine Entwicklungsabteilung mit moderner CAD/CAE Ausstattung
- langjährige Erfahrung in der Herstellung professioneller Elektronikprodukte
- langjährige Erfahrung als Lieferant für den öffentlichen Auftraggeber
- eigene Abteilung für Kundenschulungen
- ein Qualitäts-Management System ISO 9001:2000

Produkte:

- Funktechnik: Handfunksprechgeräte, tragbare Funkgeräte, Fahrzeugfunkanlagen, professionelle und militärische Antennen
- Kommunikationstechnik: Neu: IP-basierende Intercom-Systeme für Ketten und Radfahrzeuge IP-basierende Feldtelefone auch für weite Entfernungen
- Audiotechnik: Handapparate, Kopfsprechsätze, Audiohelme für Piloten- und Fahrzeugbesatzungen

Kontakt: Kirchheimer Str. 49D – 67269 Grünstadt – Tel. +49 6359 9463 643 – Fax +49 6359 9439 817 - s.eulenhofer@elno.fr - www.elno.fr

EMW Exhibition & Media Wehrstedt GmbH ME 10-2

Die EMW Exhibition & Media Wehrstedt GmbH ist Veranstalter von Fachmessen und Tagungen und ein Verlag für das Aufgabengebiet Innere Sicherheit. Inhaber und Geschäftsführer ist Dr. Uwe H. Wehrstedt.
EMW veranstaltet zwei eigene internationale Fachmessen, die nur für Behörden zugänglich sind:
GPEC General Police Equipment Exhibition & Conference®, www.GPRC.de, seit dem Jahr 2000 und
GPEC® digital, www.GPECdigital.com, Erstveranstaltung 2019.
Jährliche Fachtagungen zu Terrorabwehrsperren sowie mit der Deutschen Polizeigewerkschaft und dem Bund Deutscher Kriminalbeamter ergänzen des Veranstaltungsportfolio.
Außerdem ist EMW Inhaber und Verlag der polizeitechnischen Fachzeitschrift für Innere Sicherheit pvt POLIZEI VERKEHR + TECHNIK.
Weitere Information: www.wehrstedt.org

Endace Europe Ltd ME 16

Seit 2001 produziert Endace Network- Visibility-Hochleistungsprodukte für Betreiber der größten und komplexesten Netzwerke der Welt, darunter Militär und Regierungen. Die Endace-Produkte liefern verfolgbare Netzwerk-Daten, die Kunden benötigen, um Sicherheits-und Netzwerkleistungs-Probleme zu identifizieren und zu beheben. Die aufgezeichneten Daten dienen den Kunden zur forensischen Analyse von Datenschutzverletzungen sowie anderen Sicherheitsvorfällen.
EndaceProbes™ ermöglichen eine präzise und hundertprozentige Paketerfassung, während zur gleichen Zeit eine große Auswahl von Software aus dem Bereich der Netzwerksicherheit und Performanceanalyse auf dieser Plattform betrieben werden können. Darunter fallen Tools zur Bedrohungserkennung wie IDS, aber auch Anwendungen zur Überwachung von Netzwerk- und Applikationsperformance.
United Kingdom, www.endace.com

Epson Deutschland GmbH ME 12

Die Epson Deutschland GmbH ist ein führender Anbieter von Druckern, Scannern und Projektoren für Unternehmen, öffentliche Auftraggeber und Privatkunden. Speziell für Handel und Industrie bietet Epson Produkte und Lösungen für den Großformat-, Kassen-, Etiketten- und Ticketdruck. Die Epson Deutschland GmbH wurde 1979 als Tochter der japanischen SEIKO EPSON CORPORATION gegründet. Das in Meerbusch (NRW) ansässige Unternehmen beschäftigt rund 290 Mitarbeiter und verantwortet die Vertriebsgebiete Deutschland, Österreich und die Schweiz..
www.epson.de

ESG Elektroniksystem- und Logistik-GmbH M 08

Als unabhängiger Technologie- und Innovationspartner ebnet die ESG DEFENCE + PUBLIC SECURITY für das Militär sowie für Behörden & Organisationen mit Sicherheitsaufgaben (BOS) den Weg zu einsatzbereiten Systemen. Die komplexen Herausforderungen auf technischer sowie logistischer Ebene löst sie seit über 50 Jahren erfolgreich durch ihre Kernkompetenzen in der Systementwicklung und -integration.
Diese Kompetenzen führt das ESG-Tochterunternehmen CYOSS erfolgreich in der digitalen Geschäftswelt weiter. Mit integrierten Lösungen für Data Analytics und Cyber Security hebt und schützt sie für Kunden aller Branchen das hohe Wertpotenzial ihrer Daten.

Kontakt: ESG Elektroniksystem- und Logistik-GmbH, Livry-Gargan-Straße 6, 82256 Fürstenfeldbruck, Tel. 089 92161-0, E-Mail: defenceandsecurity@esg.de, https://esg-defencesecurity.com

Esri Deutschland GmbH B 07

Esri ist Anbieter der ArcGIS Plattform für alle Sicherheitsorgane. ArcGIS strukturiert Informationen über Raumbezug und visualisiert Ergebnisse und Zusammenhänge in 2D, 3D und 4D. Damit vernetzt die Technologie alle Beteiligten – vom Analysten bis zum Entscheider – mit einem einheitlichen, räumlichen Verständnis zur Operationsführung.

Kontakt: Esri Deutschland GmbH, Niederlassung Bonn, Rheinallee 24, 53173 Bonn, Tel.: +49 89 207 005 1720, E-Mail: info@bonn.esri.de, esri.de

FFG Flensburger Fahrzeugbau Gesellschaft GmbH S 02

Neben Modernisierungen, Umrüstungen und Instandsetzungen bietet die FFG zunehmend auch Eigenentwicklungen.
Die Fahrzeugplattformen ACSV, G5 und WiSENT 2 bieten dem Kunden mit ihrer Modularität eine Vielzahl von Einsatzmöglichkeiten. Ein Technologie-Demonstrator als möglicher Nachfolger für den BV206 befindet sich zurzeit in der Endphase der Entwicklung.
Unter Berücksichtigung aktueller Forderungen nach standardisierten Rüstsätzen auch in bestehenden Fahrzeugen hat die FFG mit Partnern eine Reihe von Konzepten erarbeitet. Diese bieten Lösungsansätze u.a. für das Vorhaben „D-LBO“ und ähnliche Projekte wie in Norwegen und den Niederlanden.
Auf der AFCEA 2019 präsentiert FFG zusammen mit Partnern Beispiele aus diesen Arbeiten.

Fraunhofer FKIE M 04

Das Fraunhofer FKIE entwickelt anwendungsorientierte Technologien für die vernetzte Operationsführung. Mit dem Experimentalsystem „InSAne“ (Intelligent Situational Awareness) demonstriert das Fraunhofer FKIE neue Architekturkonzepte für interoperable, resiliente und skalierbare Führungsinformationssysteme auf Basis aktueller Cloud-Technologien. Mit dem „C2 Newsfeed“ wird exemplarisch ein intelligenter Micro-Service vorgestellt, der den Nutzer in Form von kurzen, prägnanten Textmeldungen über Lage-Updates informiert.
Anhand des Exponats „RA2T“ (Requirements Analysis und Architecture Toolsuite) wird vorgestellt, wie Machine Learning und Natural Language Processing eingesetzt werden können, um Anforderungsbestände aufzubereiten, ihre Qualität zu sichern, Anforderungen zu klassifizieren sowie mit Funktionalitäten vorhandener IT-Services abzugleichen und schließlich IT-Services im Unternehmensportfolio zu identifizieren, die diese Anforderungen umsetzen.

Kontakt: kontakt@fkie.fraunhofer.de, Web: www.fkie.fraunhofer.de

Fraunhofer IOSB S 02

Das Geschäftsfeld Verteidigung des Fraunhofer IOSB steht unter dem Leitthema “Beratung und Technologie für die Verteidigung” und entwickelt aus wehrtechnischer Grundlagenforschung 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 Sensorsignalen, die dazugehörige Signalverarbeitung und die Nutzung von Bildern in 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.
Auf der AFCEA 2019 zeigen wir auf dem griffity defense Gemeinschaftsstand u.a. Implementierungen des Digitalen Lagetischs sowie dessen Virtual Reality Ausführung DigLTVR.

Frequentis Comsoft GmbH M 17

Als Anbieter individueller Systeme und Dienstleistungen beliefert Frequentis Comsoft zivile und militärische Flugsicherungsbehörden weltweit. Unsere Lösungen sind in Flugkontrollzentren und Flughäfen in mehr als 80 Ländern im Einsatz. Über 200 Mitarbeiter engagieren sich täglich für unsere anspruchsvollen Kunden, zu denen u.a. die Deutsche Bundeswehr und Armasuisse gehören. Zukunftsweisende Technologien, eine enge Zusammenarbeit mit dem Kunden auch nach Projektabschluss sowie die Implementierung und Einhaltung internationaler Standards sind die Eckpfeiler für unsere Arbeit in einem sicherheitsrelevanten Umfeld. Die Frequentis Comsoft GmbH ist Teil der global sehr erfolgreich agierenden Frequentis Firmengruppe.

Kontakt: Frequentis Comsoft GmbH, Wachhausstr. 5a, 76227 Karlsruhe, Germany, sales-comsoft@frequentis.com, www.frequentis-comsoft.com

Frequentis Deutschland GmbH M 17

Frequentis-Lösungen für sicherheitskritische Informations- und Kommunikationssysteme basieren auf über 70 Jahren Erfahrung und zeugen von einer wahren Technologieführerschaft.
Mit branchenübergreifender Erfahrung in ziviler Luftfahrt, Verteidigung, öffentlicher Sicherheit, Schifffahrtsindustrie und Verkehrswesen, baut Frequentis seine Expertise in diesen Kernbereichen weiter aus – basierend auf dem ursprünglichen Fokus der Sprachkommunikation für Control Center.
Frequentis ist seit Jahrzenten verlässlicher Partner der Bundeswehr im Bereich sicherheitskritischer Informations- und Kommunikationslösungen, wobei der Fokus auf einem Nutzer-spezifischen Design liegt, welches den Nutzer mit all seinen Aufgaben in den Mittelpunkt stellt.
Dies umfasst Lösungen für alle Teilstreitkräfte, vom Air Traffic Management, bis zur Unterstützung von Landstreitkräften auf dem Weg der Digitalisierung.

Kontakt: Frequentis Deutschland GmbH, Team Bundeswehr, Graurheindorferstr. 159, 53117 Bonn, +49 (6103) 30086 54, team-bw@frequentis.com, www.frequentis.com

GAF AG ME 19

Die GAF AG ist ein international agierendes Unternehmen mit führenden Kompetenzen und Expertise in den Bereichen Fernerkundung, Geodaten und Informationssysteme. Seit der Gründung 1985 in München wurden mehr als 1000 Projekte in Deutschland und über 144 weiteren Ländern erfolgreich durchgeführt. Ausgehend von Vertriebspartnerschaften mit allen führenden, kommerziellen Satellitenbetreiberorganisationen und dem Vertrieb und der Verarbeitung von Geodaten aller Art, nimmt das Unternehmen aufgrund seines herausragenden Know-Hows auch eine internationale Spitzenposition in den Bereichen Softwareentwicklung, GIS- und Datenbankanwendungen, Datenveredlung sowie im Geo-Consulting ein. Zurzeit beschäftigt die GAF über 220 Mitarbeiter und hat eine Vielzahl an erfolgreich abgeschlossenen und laufenden Geoinformationsprojekten unter anderem aus den Bereichen Sicherheit, Infrastruktur und Landmanagement vorzuweisen.

GBS TEMPEST & Service GmbH S 04

Die GBS GmbH, mit Sitz in Diepholz, betreibt ein vom BSI anerkanntes Abstrahlprüflabor. Für das Geschäftsfeld TEMPEST, verfügt die GBS GmbH über drei firmeneigene TEMPEST-Labore.
Neben der Berechtigung zur Durchführung von Zonenkurzmessungen ist die GBS GmbH auch ein vom BSI anerkanntes Abstrahlprüflabor für Zulassungsmessungen nach SDIP 27 Level A, Level B und Level C (International) und dem Zonenmodell (National).
Kontakt: GBS TEMPEST & Service GmbH, 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

Gebr. Friedrich Industrie- und Elektrotechnik GmbH (GFE) S 05

Die Gebr. Friedrich Industrie- und Elektrotechnik GmbH (GFE) ist seit vielen Jahren Rahmenvertragspartner des BAAINBw. Ganz egal ob es sich um die Einrüstung von Kabinen und geschützten Fahrzeugen oder um Instand-setzungsmaßnahmen handelt. In den Bereichen Kommunikationstechnik, IT oder Maschinenbau kämpft das Team der Gebr. Friedrich Industrie- und Elektrotechnik GmbH (GFE) an vorderster Front. GFE stellt sich den Forderungen der Bundeswehr und liefert einsatzfertige Systeme. Selbstverständlich werden dabei die strengen Maßstäbe der VG-Normen erfüllt. Auch ein weltweiter Einsatz ist für GFE selbstverständlich: Überall, wo Einheiten technische Hilfe benötigen, ist GFE vor Ort: auf Zypern genauso wie am Horn von Afrika.
Weitere Informationen: www.gfelektro.de

General Dynamics Mission Systems F 56

General Dynamics Mission Systems verfügt über eine 25 Jährige Erfahrung im Bereich der Digitalisierung von Landoperationen und hat dabei eine einzigartige Marktstellung entwickelt.
Verschiedene Programme zur digitalen Transformation von Streitkräften und der Digitalisierung von Landstreitkräften sind bereits in Canada, den Niederlanden

und dem Vereingten Königreich erfolgreich implementiert, wo wir ebenfalls die künftige Generation von taktischen Kommunikations- und Informationssystemen als Initialphase des UK MORPHEUS Programms weiterentwickeln.
Unser neuer Ansatz einer offenen Systemarchitektur bietet volle NATO Interoperabilität.
Wir laden Sie herzlich ein, mehr über unsere führenden Systeme einer vernetzten, digitalisierten Gefechtsführung zu erfahren und uns am Stand F 56 zu besuchen.

genua gmbh — M 24

Die genua GmbH ist ein deutscher Spezialist für IT-Sicherheit. Seit der Firmengründung 1992 beschäftigen wir uns mit der Absicherung von Netzwerken und bieten hochwertige Lösungen. Unser Leistungsspektrum umfasst:

- die Absicherung sensibler Schnittstellen im Behörden- und Industriebereich
- die hochsichere Vernetzung kritischer Infrastrukturen
- die zuverlässig verschlüsselte Datenkommunikation via Internet
- Fernwartungs-Systeme für Maschinen, Anlagen und IT-Systeme
- Remote Access-Lösungen für mobile Mitarbeiter und Home Offices

Unsere Lösungen werden in Deutschland entwickelt und produziert. Viele Firmen und Behörden setzen zum Schutz ihrer IT auf usnere Lösungen. genua ist ein Unternehmen der Bundesdruckerei-Gruppe.

GovSat — F 08

GovSat ist eine Luxemburger Gesellschaft und wurde Anfang 2015 als Partnerschaft zwischen der Luxemburger Regierung und der Firma SES. Ziel der Firma GovSat ist es sichere und flexible Satellitenkommunikation für behördliche Nutzer auf nicht-präemptiver Basis anzubieten.
Zu diesem Zweck wurde ein erster Satellit, GovSat-1, mit eigenen Sicherheitsmerkmalen beschafft, der zusammen mit weiteren Sicherheitseinrichtungen bzw. Leistungen auf dem Bodensegment solche Leistungen anbietet. GovSat-1 hat eine hochflexible Nutzlast mit leistungsstarken und steuerbaren Beams im militärischem X Band und militärischem KA Band. Der Satellit ist seit Mitte März 2018 auf der Orbitalpostion 21.5 Grad Ost in Betrieb und die Abdeckung des Satelliten beinhaltet unter anderem Europa, Mittler Osten, Afrika, Indischer Ozean und große Teile des Atlantischen Ozeans. https://www.govsat.lu/

griffity defense GmbH — S 02

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 klaren, umfassenden, zukunftssicheren Strategien und integrierten technischen Lösungen um für die unterschiedlichen Einsatzszenarien bestmögliche Werkzeuge und Infrastruktur bereitzustellen.
Unter dem Motto „Modulare Missionsausstattung für land- und luftbasierte Operationen“, zeigen wir auf der AFCEA 2019 mit unseren Partnern Bittium, Cubic, ELESIA, FFG, Fraunhofer IOSB, Harris Geospatial Solutions, iXblue, Media Broadcast Satellite, msg systems und NDSatCom beispielhaft modulare Lösungen, die einen wesentlichen Beitrag zur Digitalisierung der Landstreitkräfte in der taktischen Ebene leisten können.

Kontakt: griffity defense GmbH, Hanns-Schwindt-Str. 8, 81829 München, +49 (0) 89-43 66 92-0, info@griffity-defense.de, www.griffity-defense.de

Hagenuk Marinekommunikation GmbH — S 08

Die Hagenuk Marinekommunikation GmbH (HMK) ist eine Tochtergesellschaft der ATLAS ELEKTRONIK. Als einer der führenden Hersteller von zertifizierten, schlüsselfertigen internen/externen Kommunikationssysteme für Marineschiffe und HF-Sende-/ Empfangsanlagen für Landstationen liefert HMK Systemlösungen und Geräte für alle Schiffe der Deutschen Marine. Weltweit nutzen 29 Marinen mehr als 560 Systeme.
Zum Portfolio der HMK gehören:

- HF-Sender / Transceiver der 3000er Serie bis 10 kW (1,5 – 30 MHz)
- VLF/HF-Empfänger (10 kHz – 30 MHz)
- HF-Verstärker mit Antennenanpassgeräten für das Programm SVFuA
- HF-Breitbandsysteme
- Digitale Audio- und Datenverteilungssysteme
- Message Handling und Steuerungssysteme
- Subsysteme der internen/externen Kommunikation

Kontakt: Hagenuk Marinekommunikation GmbH, 24220 Flintbek,
Tel .: +49 (0) 4347-714-0, www.hmk.atlas-elektronik.com,
info@hmk.atlas-elektronik.com

Haivision Network Video — F 28

Haivision bietet End-to-End Lösungen für die schnelle und sichere Übertragung von Video zusammen mit zeitkritischen Metadaten (KLV oder Sensorik-Daten) über verschiedene IP-Netzwerke oder Satellitenverbindungen.
Haivision Video Encoder / Decoder Produkte erfüllen NATO und MISB Standards (STANAG 4609) und werden bereits weltweit im Bereich C4ISR Ultra Low Latency Videoübertragung auf unterschiedlichsten Plattformen und Programmen erfolgreich eingesetzt.
Haivision ist ein globales Unternehmen mit Hauptsitz in Montreal / Kanada und in Chicago, sowie weiteren regionalen Niederlassungen Europa / Deutschland und in Asien. Haivision Produkte sind ITAR free und werden weltweit über zertifizierte Distributoren, Reseller und Systemintegratoren vertrieben.
Weitere Informationen finden Sie unter: www.haivision.eu / www.haivision.com

Harris Geospatial Solutions — S 02

Der Harris-Konzern liefert integrierte Lösungen für Verteidigung und Sicherheit weltweit und besteht aus den drei Geschäftsbereichen
Space and Intelligence Systems Payload und Sensoren für Satelliten und Luftfahrzeuge, militärisches GPS, Erd- und Wetterbeobachtung, Prozessierung und Analyse von Fernerkundungs- und Geodaten,
Communication Systems Netzwerke, Funk- und Satellitensysteme für Sprachkommunikation sowie Nachtsichtsysteme,
Electronic Systems Elektronische Systeme, Radar- und Sonarsysteme, Flugsicherung, Kompositstrukturen für Luftfahrzeuge.

Informieren Sie sich auf unserem diesjährigen Stand auch speziell über
Jagwire Vernetzte Systeme für Fernerkundungsdaten aller Sensoren (v. a. Video, WAMI),
ENVI & SARscape Lösungen für die Bildaufbereitung und –analyse (z. B. RGB, IR, SAR, LiDAR),
GSF & Machine Learning
Servicegestützte Bildauswertung mit höchsten Detektionsraten für offene und eigene Datenquellen (Drohnen, Flugzeuge, Satelliten),
Geiger-mode LiDAR Sensorik, Datenprozessierung und Analytik für die großflächige und hochgenaue 3D-Topografieerfassung (Höhemodelle, Klassifikation, Objektextraktion).

Kontakt: www.harrisgeospatial.com,
Tel. +49 (0)8105 378 120, rene.guenzkofer@harris.com

Harris Global Communications F 41

Harris wird auf der AFCEA-Fachausstellung mit den folgenden Geräten einen kleinen Einblick in seine neuesten Entwicklungen von Software-Defined-Radios geben.
AN/PRC-160(V): einzige Stand-Alone-Lösung auf dem Markt für BLOS Kommunikation (Beyond Line-Of-Sight) ohne Satelliten. Weltweit erstes HF-Manpack, das die neuen Krypto-Standards für sichere Type 1 TOP-SECRET Sprach- und Datenkommunikation erfüllt, bei 10-fach höherer Datenübertragungsrate.
AN/PRC-158: modulares Zweikanal-Manpack-Funkgerät, deckt den gesamten Frequenzbereich von 30-2500 MHz ab. U.S.-TOP-SECRET-SECAN-zertifiziert und JTRS-COMSEC und TRANSEC-konform, bei 30% kleinerem Formfaktor.
AN/PRC-163: sichere Zweikanal-Konnektivität für taktische Kommunikation. Kann gleichzeitig Sprache, Daten und Lageinformationen über mobile Ad-hoc-Netzwerke, VHF/UHF-LOS und alte SATCOM-Anwendungen übertragen. Implementierung weiterer Wellenformen mittels Software-Updates.

Kontakt: www.harris.com / funktechnik@jkdefence.de

Heinen ICS M 29

Nach der Übernahme des früheren Düsseldorfer Unternehmens ICOS GmbH im Jahr 2015 und Neugründung des Unternehmensbereichs Heinen ICS Individuelle Computersicherheit hat sich das Haaner Unternehmen **Heinen Elektronik GmbH** im Markt für militärisch genutzte IT-Komponenten und IT-Sicherheit neu positioniert. Auf der Basis von kommerzieller am Markt verfügbarer Computer-Hardware werden von Heinen ICS neben den ICOS Produkten ergänzende Hardware-Komponenten und Strukturen entwickelt, die ein Höchstmaß an Hardware-Sicherheit für den zukünftigen Computer-Arbeitsplatz garantieren bei minimaler Belastung durch regulative Prozesse/ Abläufe des Computer-Nutzers, um damit eine hohe Anwender-Akzeptanz zu erzielen. Dazu zählen die neuen Sicherheits-Hardwareprodukte NoSpy-Box® und NOSPY WORKSTATION.

Hexagon Geospatial B 10

Hexagon Geospatial hilft Ihnen, die sich dynamisch verändernde Welt zu verstehen. Weltweit als Hersteller von Spitzentechnologien bekannt, ermöglichen wir es unseren Kunden, Daten einfach in verwertbare Informationen umzuwandeln und verkürzen dabei den Lebenszyklus vom Moment der Veränderung bis zur Handlungsentscheidung.
Hexagon ist ein weltweit führendes Unternehmen für digitale Lösungen zur Schaffung autonom verbundener Ökosysteme. Hexagon beschäftigt rund 19.000 Mitarbeiter in 50 Ländern und erzielt einen Umsatz von rund 3,5 Mrd. EUR. Erfahren Sie mehr unter hexagon.com und folgen Sie uns unter @HexagonAB.

Hitachi Vantara GmbH M 23

Hitachi Vantara unterstützt Unternehmen und Behörden weltweit, ihre datenorientierten Innovationen im Zeitalter der digitalen Revolution voranzutreiben. Nutzen Sie unsere umfangreiche Expertise aus über 100 Jahren OT und mehr als 58 Jahren IT, um den vollen Wert Ihrer Daten auszuschöpfen und auch unser öffentliches Leben sicherer und angenehmer zu machen. Unsere Lösungen adressieren sämtliche Aspekte eines ganzheitlichen Data Management: eine integrierte IT-Infrastruktur mit hochverfügbarer Speichertechnologie, Data Analytics unter anderem zur intelligenten Videoüberwachung, Big Data, IoT, AI und Predictive Maintenance, Object Storage und Data Governance. Dies macht uns zum idealen Partner für den öffentlichen Bereich. Besuchen Sie uns an unserem Stand M23.

IABG mbH M 27

Die IABG arbeitet an Lösungen für eine sichere und zuverlässige Kommunikation und IT-Unterstützung für Streitkräfte und BOS. Hierbei betrachten wir die gesamte Prozesskette und den Lebenszyklus von ITK-Systemen.
Wir beschäftigen uns u.a. mit Ausbildungs- und Trainingskonzepten zum Thema Cyber Security, Risikoanalysen sowie Detection & Response Mechanismen für Cyberangriffe. Mit der IABG Cyber Range stellen wir eine Testplattform für die virtualisierte Abbildung der Umgebung der Bundeswehr bereit, in der wir auch komplexe Cyberszenare simulieren und die Widerstandsfähigkeit von ITK-Systemen beurteilen können. Zudem unterstützen wir bei der Erstellung und Weiterentwicklung von IT-Sicherheitskonzepten auf Basis der neuen zentralen Dienstvorschrift A-960/1.

IBM Deutschland GmbH B 09

IBM ist das IT-Unternehmen mit der am breitesten gefächerten Erfahrung, wurde vor über 100 Jahren gegründet und hat sich seither immer wieder neu definiert.
Die strategischen Felder Künstliche Intelligenz/Business Analytics, Cloud Computing, Security, Internet der Dinge (IoT) und Blockchain-Technologien bilden für IBM sowohl die Basis ihres stetig erweiterten Lösungsportfolios als auch die Grundlage ihrer fortschreitenden Transformation hin zu einem Cognitive-Solutions- und Cloud-Plattform-Anbieter.
Der kognitiven Erschließung komplexer und großer Datenmengen trägt IBM Rechnung durch die 2014 neu gegründete Watson Group mit dem Geschäftsbereich Watson IoT, der gemeinsam mit dem ersten europäische Watson Innovation Center in München seine Zentrale hat.

Kontakt: IBM Deutschland GmbH, Godesberger Allee 127, D-53175 Bonn
Klaus Lilge, klaus_lilge@de.ibm.com, Mobile: +49-175-5813842

iesy GmbH & Co. KG F 50

Individuelle Lösungen für Verteidigung und Sicherheit
Marktführende Unternehmen aus den Bereichen Avionics & Defence setzen auf iesy, wenn es um die Entwicklung und Anpassung von Elektronik oder Mechanik für raue Umgebungen geht. iesy ist ein Systemhaus für Embedded Computing. Mit Leidenschaft für Technik und einem eingespielten Team in den Bereichen Soft- und Hardwareentwicklung, Materialbeschaffung, Fertigung und Geräteprüfung sind wir seit 1966 ein idealer OEM- und Outsourcing-Partner zur Entwicklung, Serienfertigung und Pflege individueller Elektronikprodukte. Als Full-Service Dienstleister für Embedded Computing begleiten wir Sie beim gesamten Entwicklungsprozess von Ihrer Idee bis zum fertigen Produkt.

Kontakt: iesy GmbH & Co. KG, Darmcher Grund 22, 58540 Meinerzhagen,
T: +49 (2354) 70655 0 | E: sales@iesy.com, www.iesy.com

IMTRADEX F 43

Die IMTRADEX Firmengruppe zählt zu den führenden Herstellern von Headsets auf dem europäischen Markt. Unter dem Motto „command&control“ unterstützt Imtradex sicherheitskritische Anwendungen mit höchster Präzision und Zuverlässigkeit, bspw. für BOS, Leistellen und Luftfahrt. IMTRADEX führte auch das weltweitführende INVISIO Hör-/Sprechsystem in den deutschen Markt ein. Imtradex präsentiert u.A. seinen neusten Teil der Firma – platform X – ein vollumfängliches, modulares System für die Unterstützung und Digitalisierung der täglichen Polizeiarbeit.

Kontakt: IMTRADEX Hör- / Sprechsysteme GmbH, Daimlerstraße 23, 63303 Dreieich, Tel: + 49 (0) 6103 - 4 85 69 – 40, Fax: + 49 (0) 6103 - 4 85 69 – 60, Mail: info@imtradex.com, Web: www.imtradex.com / www.platform-x.de

Indra Sistemas S.A. S 10

Indra Sistemas S. A. ist ein börsennotierter Konzern und "Global Player", der in zwei Sparten organisiert ist: Digitalisierung und Transport & Verteidigung. Das Technologieportfolio Verteidigung und Sicherheit umfasst:

- Bemannte und unbemannte Fahrzeuge,
- Radar-Technologie,
- Elektronische Kampfführung (EloKa),
- Satellitenkommunikation,
- Space Surveillance & Tracking,
- Simulation & Training,
- Cyberdefence,
- Führungsinformationssysteme und
- Schutz kritischer Infrastrukturen.

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

INFODAS GmbH M 22

Die INFODAS ist seit 1974 als unabhängiges und herstellerneutrales Software- und Beratungsunternehmen ein verlässlicher Partner der Bundeswehr.

Kernkompetenzen sind:

- SDoT Security Gateway, bidirektionale Netzkopplung unterschiedlicher Informationsräume/Sicherheitsdomänen
- SDoT Diode, hochsichere High-Speed-Datenübertragung von LOW- auf HIGH-Netzwerke
- SDoT Labelling Service, Kennzeichnung/Auswertung von Security Labeln
- SDoT SIS & SD, elektronische VS-Registratur zur vorschriftenkonformen Bearbeitung und Verwaltung digitalen Verschlusssachen
- SDoT Secure Network Card (SNeC) für sichere Ethernet-basierte Datenkommunikation
- SAVe, IT-Sicherheitsdatenbank mit integrierten Sicherheitsvorgaben ZDv A-960/1
- PATCH.works, Patch-Managementsystem für geschlossene IT-Systeme
- Informationssicherheitsberatung und Erstellung von IT-Sicherheitskonzepten
- Projekt-, Anforderungs-, Nutzungs-, Konfigurations-, Qualitätsmanagement sowie weitere Beratungsleistungen und Analysen

Kontakt: Frank Thelen, Tel. 0221 70912-0, vertrieb@infodas.de, www.infodas.de

Intel Deutschland GmbH M 03

Intel verwirklicht die faszinierendsten Dinge der Zukunft

Wahrscheinlich kennen Sie uns wegen unserer Prozessoren. Wir sind aber auch auf vielen anderen Gebieten aktiv. Intel erweitert mit seinen Erfindungen ständig die Grenzen der Digitaltechnik, um für die Wirtschaft und die Gesellschaft und letzten Endes für jeden Einzelnen auf der Welt Neues und Faszinierendes erlebbar zu machen. Mit der Erschließung des Potenzials der Cloud, der Allgegenwart des Internet des Dinge, der neuesten Fortschritte in der Speichertechnik und bei programmierbaren Lösungen und des vielversprechenden 5G-Ntzes mit Always-on-Vernetzung revolutioniert Intel ganze Branchen und trägt zur Lösung weltweiter Probleme bei. Mit seiner führenden Rolle in puncto Firmenpolitik, Diversität, Inklusion, Bildung und Nachhaltigkeit schafft Intel Werte für seine Aktionäre, Kunden und die Gesellschaft.

ISEC7 Group +Teamwire F 42

Die ISEC7 Group ist ein global agierender Anbieter von Dienstleistungen und Softwarelösungen für Enterprise Mobility:

Teamwire ist ein schneller, intuitiver und sicherer Messenger für Organisationen mit Sicherheitsaufgaben. Die stark verschlüsselte WhatsApp-Alternative verbessert die Einsatzkommunikation und erfüllt alle europäischen Datenschutzanforderungen und Sicherheits-Richtlinien von Behörden. Innovative Funktionen zur Alarmierung und Krisenkommunikation runden die Lösung ab.

Die prämierte **ISEC7 EMM Suite** ist eine ganzheitliche Monitoring-Lösung für mobile User, Devices und Infrastrukturen.

ISEC7 Mobile Exchange Delegate gewährleistet den sicheren, mobilen Zugriff auf Microsoft Outlook-Kalender, E-Mails und Kontakte von Dritten, wie beispielsweise von Funktionsrollen, Teams oder Stellvertretern/innen.

Kontakt: info@isec7.com

itWatch GmbH F 26

itWatch ist im zersplitterten Markt der IT-Sicherheitshersteller in Deutschland eines der wenigen vollständig unabhängigen, inhabergeführten Unternehmen. Erste Produkte der itWatch wurden 1997 entwickelt und in 2000 patentiert. Der Fokus liegt auf dem Schutz gegen Datendiebstahl über alle möglichen Kanäle, bis zum Ausdruck (Data Loss Prevention), technischer Vertrauensketten von der Tatstatur bis zu den Daten, deren organisatorische Einbettung durch rechtsverbindliche Dialoge, Endgeräte-Sicherheit (Endpoint Security), sowie Mobile Security und Verschlüsselung. Integrierte Lösungen für Datenschleusen mit Datenwäsche und PrivateDataRoom bringen hohe Kundenmehrwerte. Die Lösungen der itWatch Enterprise Security Suite (itWESS) werden ohne Zukauf im Hause der itWatch hergestellt.

iXblue SAS GmbH S 02

iXblue is a global leader in the design and manufacturing of innovative solutions devoted to navigation. Using its unique in-house technology, the company offers turnkey solutions to its Defense customers with optimum efficiency and reliability. Employing a workforce of 600 people worldwide, iXblue conducts its business with over 35 countries.

iXblue is recognized throughout the industry for its pioneering work on the development of ultimate performance fiber-optic gyroscopes (FOG). In all these areas, the group works to ensure that its products provide high accuracy, as well as unrivalled performance and reliability.

JK Defence & Security Products GmbH F 41

Seit mehr als 25 Jahren. JK DEFENCE & SECURITY PRODUCTS GMBH

Sensible taktische Kommunikation von digitalisierten Streitkräften - geschützt vor feindlichen Störungen und feindlicher Aufklärung.

Wir finden für Sie die passende Lösung mit unseren Partnern HARRIS COMMUNICATIONS, Ultralife, ViaSat und RolaTube.

Informieren Sie sich persönlich über die neusten Entwicklungen: Harris PRC-163 Multichannel Handfunkgerät, PRC-158 Multichannel Manpack mit SATCOM, sowie das PRC-160 HF Wideband Manpack und die neuen Airborne Radios.

Das Portfolio umfasst dazu Fahrzeughalterungen, Antennen, Batterien und Ladegeräte. Aber auch leicht transportier- und schnell installierbare Masten, zum Teil mit integrierten Antennen.

JK Defence & Security Products GmbH,
www.jkdefence.de / funktechnik@jkdefence.de

JOWO – Systemtechnik AG F 64

JOWO – Systemtechnik AG (www.jowosy.de) ist Hersteller und Vertreiber von elektrischen und optischen Steckverbindern, LWL- und elektrischen Verkabelungen, sowie kundenspezifischen Lösungen seit 1995.

In Zusammenarbeit mit namhaften Herstellern erstellen wir für sie die beste Lösung, mit Expertise und bestem Service.

- Elektrische Steckverbinder für Militär, Industrie, Luft- u. Raumfahrt,
- Marine, Öl und Gas (Ex-Lösungen)
- Endgehäuse, Schutzkappen, Werkzeuge
- LWL-Steckverbinder Multi- und Singlemode als „PC“ oder mit Linsentechnik
- Reinigungs- und Testkoffer
- Kabelbäume militärisch/zivil in LWL, Signal, Leistung, HF, Hybrid
- Systemlösungen
- Eigene Konstruktion für kundenspezifische Lösungen
- Drucktests bis zu 1000 bar mit eigenen Tanks
- Schnellfertigungslinie für Marinebronzestecker nach MIL und VG

Zugelassen nach EN9120, NATO C6689 und VG96927, Typen C, D und E

K&K Medienverlag-Hardthöhe GmbH/ Hardthöhenkurier — ME 02

Der Hardthöhenkurier ist ein periodisch erscheinendes Magazin, das sich seit 35 Jahren mit aktueller Berichterstattung an Soldaten der Bundeswehr wendet und sich als Bindeglied zwischen der Bundeswehr, der wehrtechnischen Industrie und der Wirtschaft versteht. Der Hardthöhenkurier informiert über sicherheitspolitische Rahmenbedingungen, Einsätze der Bundeswehr, aktuelle Vorhaben der Streitkräfte sowie Neuerungen in der Wehrtechnik und der Rüstungsindustrie. Das Fachmagazin ist eine in Deutschland und in den europäischen Nachbarländern anerkannte Informationsquelle für Streitkräfte und Wehrtechnik.

Kontakt: Verlagsdirektion Bonn • Postanschrift: Borsigallee 12, 53125 Bonn, Telefon: +49 (0)228 / 25900-344 • Telefax: +49 (0)228 / 25900-342, E-Mail: redaktion@hardthoehenkurier.de • Internet: www.hardthoehenkurier.de

Kommando Cyber- und Informationsraum der Bundeswehr — ME 11

Das Kommando Cyber- und Informationsraum der Bundeswehr

Im April 2017 wurde das Kommando Cyber- und Informationsraum (KdoCIR) in Bonn in Dienst gestellt. Mit dem jüngsten Organisationsbereich stellt sich die Bundeswehr den immer weiter ansteigenden Gefahren aus dem Cyber- und Informationsraum. Bereits vorhandene Expertise wurde dafür unter dem KdoCIR gebündelt. Dazu gehören das Kommando Strategische Aufklärung inklusive des Zentrums für Operative Kommunikation der Bundeswehr, das Kommando Informationstechnik der Bundeswehr sowie das Zentrum für Geoinformationswesen der Bundeswehr. Weitere Expertise wird/ wurde aufgebaut, um die Fähigkeiten „Cyber-Operationen“, „Cyber-Sicherheit“ und „Softwarekompetenz“ zu stärken. Im Jahr 2021 wird der Organisationsbereich CIR rund 15.000 militärische und zivile Dienstposten umfassen.

Lachen helfen — ME 10

Im ehemaligen Jugoslawien beschlossen Bundeswehrsoldaten Mitte der 90er Jahre, sich neben ihren dienstlichen Aufgaben auch privat für humanitäre Projekte zugunsten von Kindern zu engagieren. Um den traumatisierten, verwundeten oder elternlosen Kindern dauerhaft, schnell und unbürokratisch zu helfen, gründeten sie 1998 einen gemeinnützigen Verein. Die gute Zusammenarbeit mit der Polizei führte 2009 zu dem Entschluss, sie in den Verein zu integrieren. Seitdem ist Lachen Helfen e.V. die „Initiative deutscher Soldaten und Polizisten für Kinder in Kriegs- und Krisengebieten“. Seit dem Jahre 2001 sind wir nach wie vor in Afghanistan und auf dem Balkan tätig. Momentan werden jedoch insbesondere im Irak, in Mali, im Südsudan, in Somalia, in der Ukraine und seit einiger Zeit auch in Syrien Hilfsprojekte erkundet.

Leonardo — B 05

Leonardo ist ein führender Produzent (Top Ten) von Systemen der Luftfahrtbranche und im Verteidigungsmarkt. Die Firmenzentrale von Leonardo befindet sich in Italien. Leonardo beschäftigt über 48.000 Mitarbeiter in 180 Standorten weltweit. Das Unternehmen verfügt in Europa und in den USA über eine konsolidierte industrielle Präsenz und weltweit über ein leistungsstarkes Netzwerk von Partnern. Leonardo teilt seine Geschäftsaktivitäten in vier Bereiche (Helicopter / Aeronautics / Electronics, Defence Systems & Security Systems / Space). 13% des Konzernumsatzes werden in Forschung und Entwicklung investiert.
Leonardo ist in Deutschland durch die LEONARDO Germany GmbH mit 220 Mitarbeitern vertreten. Kernbereiche der LEONARDO Germany GmbH sind Radar- und Kommunikationstechnologie sowie die Vermarktung von Produkten des Leonardo Konzerns.

Kontakt: info@selex-es-gmbh.com, Tel.: +49 (0)2137-782-328 , www.leonardo-company.com

Materna Information & Communications SE — F 07

Materna ist ein Full-Service-Dienstleister im Premium-Segment und realisiert seit fast vier Jahrzehnten als Familienunternehmen sehr erfolgreich ITK-Projekte für ihre Kunden. Weltweit arbeiten mehr als 2.000 Mitarbeiter für die Materna-Gruppe. Wir betreuen Behörden in allen Phasen der Wertschöpfungskette: von der Beratung, Konzeption, Realisierung über die Einführung bis zum Betrieb mithilfe standardisierter und skalierbarer Lösungen. Das Leistungsspektrum umfasst die Konzeption und Einführung von Internet-/ Intranet-Lösungen sowie von Kollaboration und Wissens-Management, die Optimierung und Digitalisierung von Verwaltungsabläufen, IT-gestütztes Personalmanagement, die Einführung von IT-Service-Management, die Entwicklung und Integration ressortspezifischer Fachverfahren und Kombination mit innovativen Themen wie Künstliche Intelligenz, Chatbot, Blockchain- und VR/AR- und Cloud-Technologien.

Media Broadcast Satellite GmbH (MBS) — F 27 + S 02

MBS ist Betreiber von Deutschlands größtem Teleport und langjähriger Serviceprovider von maßgeschneiderten Kommunikationslösungen für Regierungsorganisationen und dem Militär.
Für eine agile und robuste Vernetzung von temporären oder ortsfesten Standorten sowie mobilen Einheiten, bietet MBS skalierbare und einsatzerprobte Kommunikationslösungen an. Neben Satellitenanbindungen nutzt MBS Glasfaser-, Funk- und Mobilfunkverbindungen, die eine Bandbreite an Anwendungen zu Land, Luft und See ermöglichen. Die hochverfügbaren Kommunikationslösungen sind hardwareunabhängig und lassen sich in bereits existierende Systeme integrieren und an sich wechselnde Anforderungen flexibel anpassen.
MBS arbeitet EU/US/NATO sicherheitskonform und betriebt eine ISO 27001 zertifizierte Infrastruktur. Die Services reichen von standardisierten bis hin zu vollständig gemanagten Lösungen.

Mellanox Technologies Ltd. — F 67

Mellanox Technologies ist der führende Anbieter von Hochgeschwindigkeits-Netzwerklösungen für leistungsfähige Server- und Speichersysteme, basierend auf dem InfiniBand- und Ethernet-Protokoll. Die Firma hat ihren Sitz in Yokneam, Israel und Sunnyvale (CA), USA. Das an der NASDAQ notierte Unternehmen (MLNX), beschäftigt über 2.500 Mitarbeiter an den weltweiten Standorten. Als selbst produzierender Halbleiterhersteller stellt Mellanox Technologies eine Vielzahl an Kommunikations-

technologie her, darunter Netzwerkadapter, Switches, Kabel und Software, die in Anwendungsbereichen mit besonderen Anforderungen an große Bandbreiten und Echtzeitkommunikation Verwendung finden.
Neben den Infrastruktur-Komponenten stellt Mellanox Technologies Hochleistungs-plattformen auf Basis von FPGA und Multicore ARM CPUs her. Diese werden hauptsächlich in den Bereichen Encryption, Deep-Packet Inspection, Content Filtering und Realtime Data Analysis eingesetzt.

MICCAVIONICS GmbH F 44

MICCAVIONICS – ein deutscher, konzernfreier Anbieter netzwerkzentrierter Situation-Awareness und Mission-Managementsysteme zur Unterstützung digital vernetzter Operationsführung in luft-/landgestützten militärischen/zivilen Einsätzen.

Produkte:
- **SIMAS:** Situation Awareness und Mission Managementsystem *
- **ULTIMAS:** SIMAS mit Video-Overlay/Video-Recorder
- **Ultichart:** Tactical Mapping System mit Video-Overlay/Video-Recoder
- **TAMAP:** Taktischer Missions-Arbeitsplatz für Führungshubschrauber (H225M, AS330) *
- **DZMx:** All-in-one satellite-cellular, voice/data communication and GPS tracking system with Iridium Push-to-talk (PTT)

Services: System-/Software-/Hardwareentwicklung gemäß V-Modell XT® – Wartung – Schulung – Support

Qualität made in Germany – gemäß Miltär-/Luftfahrt-Standards ISO9001, EN9100, EN9110, EN9120.

** Basiert auf den für die französische Heeresfliegertruppe realisierten und mehrfach kampferprobten Systemen SIT-ALAT/Kit HM-PC für Kampf-/Führungshubschrauber.*

Microsoft Deutschland GmbH F 10

Microsoft ist weltweit führender Hersteller von Standardsoftware, Services und Lösungen. Unsere Mission ist, jede Person und jedes Unternehmen auf dem Planeten zu befähigen, mehr zu erreichen. Sicherheit und Zuverlässigkeit, Innovation und Integration sowie Offenheit und Interoperabilität stehen bei der Entwicklung aller Microsoft-Produkte im Mittelpunkt.
Microsoft unterstützt die Transformation von essenziellen Verteidigungsdienstleistungen, bei denen es zum Beispiel darum geht, die beteiligten Akteure wesentlich besser und effektiver einzubinden, militärische Operationen zu optimieren und Befehlshaber und Akteure bei der Entscheidungsfindung zu unterstützen. Microsoft engagiert sich mit kompetenten Partnern aus Wirtschaft und Wissenschaft in diesem Umfeld, unter anderem mit der Defense System Integrators Initiative.

Mittler Report Verlag GmbH ME 04

Der Mittler Report Verlag gilt als führender Fachverlag für Sicherheitspolitik, Streitkräfte, Wehrtechnik, Rüstung, IT und Logistik im deutschsprachigen Raum. Das Portfolio umfasst Zeitschriften, Broschüren, Informationsdienste und Fachtagungen. Dazu zählen die in vertraglich geregelter Zusammenarbeit mit dem Bundesministerium der Verteidigung herausgegebene Monatszeitschrift „Europäische Sicherheit & Technik“, die zehnmal jährlich erscheinende internationale Fachzeitschrift „European Security and Defence“, die Fachzeitschrift „MarineForum“, die Broschürenreihen „Wehrtechnischer Report“ und „Sicherheitstechnischer Report“ sowie die Online-Newsletter „ESD Spotlight“ und „Wehrwirtschaft“. Daneben gelten die jährlich stattfindende Sicherheitspolitische und Wehrtechnische Tagung in Bonn sowie die NATO LCM Conference in Brüssel als etablierte Foren für den Informationsaustausch unter Experten und Entscheidungsträgern.
www.mittler-report.de

Mönch Verlagsgesellschaft mbH ME 03

MÖNCH ist einer der weltweit führenden Zeitschriftenverlage in den Bereichen Verteidigung und Sicherheit. Die Zeitschriften erscheinen auf deutsch, englisch, arabisch, spanisch und auf italienisch und sind sowohl in Druckform wie auch Digital erhältlich. Zusätzlich bietet MÖNCH unter www.monch.com den Mönch Online News Service (MONS) mit den aktuellsten Nachrichten online.

Zu den Zeitschriften :
- WEHRTECHNIK: Erscheinungsweise zweimonatlich
- MILITARY TECHNOLOGY: erscheint monatlich
- NAVAL FORCES: Erscheinungsweise zweimonatlich
- SAFETY & SECURITY INTERNATIONAL: Erscheinungsweise zweimonatlich.
- HANDBUCH der BUNDESWEHR

Kontakt: Herr Christian LAUTERER, MÖNCH Verlagsges.mbH, Christine-Demmer-Str. 7, 53474 Bad Neuenahr-Ahrweiler, Tel.: 02641 3703-0, e mail: info@moench-group.com, www.monch.com

Motorola Solutions M 30

Motorola Solutions (NYSE: MSI) ist ein Technologieunternehmen, das sicherheitskritische Kommunikations-, Software-, und Videolösungen bietet, die die Sicherheit im öffentlichen und nicht-öffentlichen Raum erhöhen. Streitkräfte, Behörden und Organisationen mit Sicherheitsaufgaben sowie Unternehmen vertrauen weltweit auf die Digitalfunkgeräte, Breitband-Lösungen, Videoüberwachungs- und Analyselösungen, Dienstleistungen und Software von Motorola Solutions.
Der Hauptsitz der Motorola Solutions, Inc. befindet sich in Chicago, USA. In Deutschland ist die Motorola Solutions durch die Motorola Solutions Germany GmbH mit Sitz in Idstein präsent. In Berlin befindet sich darüber hinaus das weltweite Motorola Solutions Kompetenzzentrum für den TETRA-Digitalfunk.
Weitere Informationen unter www.motorolasolutions.de sowie auf Twitter unter @MotSolsDE oder in der Motorola Solutions LinkedIn-Community.

MSAB S 11

MSAB ist weltweit führend in der Mobilgeräte-Forensik-Technologie, um Daten von mobilen Geräten, Apps, Fahrzeugen und Drohnen zu extrahieren, zu analysieren und zu managen. Wir konzentrieren uns zu 100% auf Mobilgeräte- Forensik.
Wir entwickeln die besten Systeme der Mobilgeräteforensik und unterstützen damit Regierungen, Militär und Nachrichtendienste dabei, Bedrohungen zu erkennen und Fälle mit vertretbaren Beweisen schneller lösen zu können.
Als Innovationsführer in diesem Bereich bieten wir ein komplettes System der Mobilgeräte-Forensik für alle Anforderungen und Missionen - von internen Untersuchungen bis hin zu strategischen Operationen.
Erfahren Sie mehr an unserem Stand S 11.

msg systems ag S 02

Strategischer und technischer Partner für Politik und Verwaltung auf dem Weg in die digitale Zukunft
Wir beraten und unterstützen die öffentliche Hand bei den Führungsaufgaben, die mit dem digitalen Transformationsprozess verbunden sind. Und wir finden und implementieren die passenden Lösungen: „Made in Germany“. Zu unseren Auftraggebern zählen Bundesministerien, Bundesverwaltung, Landesverwaltungen und Kommunen.
Als inhabergeführtes, mittelständisch geprägtes Beratungsunternehmen steht msg für eine starke individuelle Beratung und weitreichendes technisches Verständnis – mit zugänglichen, aber auch kritischen und kreativen Köpfen.
Wir geben Impulse für einen zukunftsfähigen Staat und schaffen innovative Lösungen. Erfahren Sie mehr über msg für den Public Sector unter https://www.msg.group/public-sector.

ND SatCom GmbH S 02

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.

Newsletter Verteidigung – VDS Verlag Deutsche Spezialmedien GmbH ME 05

Der Newsletter Verteidigung (NV) berichtet wöchentlich aus den Bereichen Sicherheits- und Verteidigungspolitik sowie Beschaffung, Bedarf, Ausbildung, Personal, Technologie, Forschung und Veranstaltungen von Seiten der Bedarfsträger und der Wehrtechnischen Industrie. Er wird kostenpflichtig abonniert per E-Mail verbreitet und gewährleistet so eine branchenaffine Leserschaft, die zum großen Teil in verantwortlichen Positionen tätig ist. Darüber hinaus wird der NV an die von der Thematik betroffenen politischen Gremien kostenlos versandt, um den Informationsfluss an die Beschafferseite sicherzustellen.
Der NV ist meinungsbildend, unabhängig und objektiv. Er zielt darauf ab, als Argumentationshilfe die bedarfsgerechte Ausstattung der Deutschen Bundeswehr mit Material und Personal bestmöglich zu unterstützen.

Kontakt: VDS Verlag Deutsche Spezialmedien GmbH, www.Deutsche-Spezialmedien.de

NYNEX satellite OHG F 27

Als ein führender Integrator von satellitenbasierenden Datenverbindungen für Europa, Afrika und dem Nahen Osten verfügt die NYNEX satellite OHG über eigene HUB-Infrastruktur und über eigene Satellitenkapazität - somit ist ein techniknaher Support, ein individuelles Consulting sowie die professionelle Integration von VSAT-Projekten aus einer Hand möglich.
Die Produktpalette reicht von Internet- bzw, Intranet-Anbindungen land- oder seebasierter Einzelstandorte bis zur Realisierung von länder- oder kontinentübergreifenden Mehrstandort-Netzwerken.
Wir betreiben unsere Satellitennetzwerke von Darmstadt aus, verfügen über ein weltweites Installateurnetzwerk und haben umfangreiche Erfahrungen bei Planung, Betrieb und Aufbau von internationalen Sattelitennetzwerken im Bereich Ministerien und Behörden.
Professional satellite services made in Germany!

OHB System AG F 01

Kreative und verlässliche Konzepte für die Raumfahrt
Der Systemintegrator OHB System AG ist erfolgreich in umfangreichen Anwendungsbereichen für raum-, boden- und luftgestützte Systeme etabliert. Für die Bundeswehr realisiert OHB die raumgestützte Aufklärung SAR-Lupe und SARah inklusive des Bodensegmentes und Betrieb. Zudem realisiert OHB den EnMAP Hyperspektralsatelliten, die sechs Wettersatelliten MTG und ein elektro-optisches System für die Bundesregierung und 34 Galileo FOC Navigationssatelliten. Die SmallGEO Produktlinie bedient die Satellitenkommunikation in Missionen wie Heinrich-Hertz mit ihrem SATCOMBw Anteil, sowie weiteren Satelliten für Laserkommunikation (EDRS-C), flexiblen digitalen Nutzlasten (H36W-1) und vollelektrischen Antrieben (ELECTRA). Im Bodensegment hat OHB kürzlich die Leistungsfähigkeit der Ankerstation Gerolstein um eine UHF-DAMA Fähigkeit erweitert und ist im Luftfahrtbereich ein Kernpartner im Vorhaben FCAS. www.ohb-system.de

OnTime Networks AS F 69

OnTime Networks ist ein führender Anbieter von robusten (fully-rugged) Netzwerklösungen, die speziell auf die besonderen Produktanforderungen im Luft-und Raumfahrt, Verteidigungs- und Energiebereich angepasst sind. Wir haben einen Schwerpunkt auf robuste Gigabit Ethernet-Switches mit IEEE 1588 PTP Referenz Zeitsystemen, sowie Router und anderen Ethernet-Technologieprodukten. Wir bieten eine vollständige Palette von zuverlässigen, widerstandsfähigen Hochleistungsnetzwerkkomponenten, welche speziell auf die hohen technischen und umweltbedingten Anforderungen der Luft-und Raumfahrtindustrie, sowie der Wehrtechnik angepasst sind. Unsere „gehärteten“ Produkte sind Technologie führend, innovativ und bieten Lösungen für vielfältige Einsatzmöglichkeiten in Luftfahrzeugen, bodengebundenen Militärfahrzeugen und Marineanwendungen. Unsere Netzwerksysteme sind modular und skalierbar und bieten höchste Flexibilität und Leistung.

Kontakt: Markus Schmitz, Managing Director, OnTime Networks LLC,
Email: markus.schmitz@ontimenet-us.com, Cell: (214) 797-6071

ORACLE Deutschland B.V. & Co. KG F 13

Für mehr als 400.000 Kunden in allen vertikalen Märkten in mehr als 145 Ländern bietet Oracle ein umfassendes und komplett integriertes Portfolio an modernsten Technologien und Anwendungen an, die in hybriden Umgebungen, in Private oder Public Clouds und On Premises zum Einsatz kommen. Dies ermöglicht höchste Flexibilität für den Einsatz von Anwendungen auf unterschiedlichsten Plattformen bei gleichzeitiger Nutzung von Innovationen.
Auf dem Weg zum Cloud Computing und angesichts der Cyber Herausforderungen sind Resilienz, Sicherheit und Automatisierung die größten Herausforderungen. Oracle antwortet darauf mit sich selbst absichernden Systemen und ausgereiften technischen Sicherheitsfunktionen.
https://www.oracle.com/de/industries/public-sector/

Panasonic Computer Product Solution Fo2

Mit Panasonic TOUGHBOOK Notebooks, Tablets und Handhelds erhalten Unternehmen und Behörden besonders robuste, zuverlässige und energieeffiziente mobile Computing-Lösungen für Outdoor- oder Büroumgebungen.

- „Full-Ruggedized“ Schutz gemäß aller notwendigen Standards (IP65- und teils IP68-Zertifizierung) sowie Militär-Standards (MIL-STD 810G, MIL-STD 461F) ,
- ergonomische Formfaktoren und geringes Gewicht,
- leuchtstarke Outdoor-Displays für ideale Ablesbarkeit auch unter Sonnenlicht,
- äußerst lange Akklaufzeiten und Hot-Swap Funktionen für unterbrechungsfreien 24-Stunden-Einsatz
- für besondere IT-Sicherheit auch mit dem speziell gesicherten und zentral verwalteten Android-basierten Betriebssystem „R&S Trusted Mobile“ und der gesicherten Messanger App „R&S Trusted Communicator“.

Kontakt: www.toughbook.de/kontakt oder Tel. +49 611 1252

Peli-Hardigg™ S 01

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 unverwüstlich, 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.

powerbridge Computer Vertriebs GmbH F 62

powerBridge Computer Vertriebs GmbH works as an integrator and supplier for standard and customized systems. We design and manufacture computer systems based on PICMG and VITA platforms. Our product offering includes VPX, VME, CPCI and SFF rugged systems for the defence market, and MTCA, ATCA and OPC server solutions for research, communications and security applications. Customized systems are designed and built as required under our guidance and quality control. Experienced engineers advise and support our customers for all hardware requirements. We do support operation systems like Windows, Linux, QNX, VxWorks with BSP´s and driver.
Continuity, reliability and long-term availability are our strength.

promegis GmbH M 05

Als Spezialist für Geoinformatik, Geoinformationssysteme, Bildverarbeitung, Bildauswertung, Softwareentwicklung und IT-Servicedienstleistungen entwickelt unser Unternehmen Anwendungen und fachspezifische Systemlösungen für die Bereiche der öffentlichen Verwaltung, der Behörden und Organisationen mit Sicherheitsaufgaben (BOS), des militärischen Nachrichtenwesens (MilNW) und der militärischen Aufklärung sowie der Energie- und Versorgungswirtschaft. Darüber hinaus unterstützen wir unsere Kunden bei der Umsetzung umfangreicher IT-Projekte.
Die promegis setzt auf innovative und gleichzeitig zukunftssichere Lösungen und steht Ihnen mit langjähriger Erfahrung bei der Realisierung komplexer, integrationsfähiger Systemlösungen zur Seite. Als deutscher Vertriebs- und Entwicklungspartner der Firma Textron Systems bieten wir Ihnen die volle Bandbreite der High-End GIS und Image Analysis Lösungen.

Kontakt: Klaus Scholle, Tel. +49 (0) 541 600196-0,
E-Mail: klaus.scholle@promegis.de, www.promegis.de.

PWA Electronic Service- & Vertriebs-GmbH F 02

Die PWA Electronic Service- & Vertriebs-GmbH hat sich sowohl auf den Vertrieb von gehärteten Panasonic Notebooks/Tablets, als auch auf Komponenten und Peripherie für mobile Anwendungen spezialisiert.
Beratung und Support gehören ebenso zum Service des geschulten PWA-Teams, wie auch die Entwicklung und Umsetzung von Sonderlösungen oder speziellen Kundenanforderungen.
Als autorisierter Servicepartner, mit über 20jähriger Erfahrung, für Panasonic Toughbooks/Toughpads ist es PWA möglich, den individuellen Service zu Ihrer speziellen Militär-Lösung anzubieten.
Unsere robusten Geräte sind kompatibel für spezielle Schnittstellenanforderungen wie z.B. Rugged USB auf Basis leistungsstarker Hardware.
Zu Ihrer individuellen Computing-Lösung ist es nur ein Schritt... PWA – alles aus einer Hand.
Weitere Informationen finden Sie auf unserer Homepage: www.pwa-electronic.de

QGroup GmbH ME 14

Die QGroup besteht seit dem Jahr 1993 und ist als Unternehmen im Bereich IT-Sicherheit und IT-Hochverfügbarkeit tätig. Das Unternehmen hat seinen zentralen Sitz in Frankfurt am Main und zudem Mitarbeiter in den USA und Kanada. Für das Unternehmen General Dynamics ist die QGroup Center of Excellence IT Security und hat langjährige Erfahrungen mit Kunden aus dem Bereich militärische IT-Sicherheit sowie dem behördlichen wie auch dem kommerziellen Sektor. Die QGroup berät Unternehmen in Sicherheitsfragen, unterstützt mit Penetrationstests und unterhält ein 7x24h Security Incident Response Team für Kunden. Dabei überträgt die QGroup pragmatische militärische Sicherheitsstrategien auf nichtmilitärische Kunden, um den Sicherheitsanforderungen von heute besser begegnen zu können.

Rafael Advanced Defense Systems Ltd. M 12

Während der AFCEA Ausstellung 2019 wird Rafael Advanced Defense Systems Lösungen für das Bundeswehr Digitalisierungsprogramm D-LBO vorstellen.

Fire Weaver – ist ein ausgereiftes taktisches System, das im Einsatz alle Sensoren und Effektoren verbindet und so ein hochentwickeltes und vernetztes Einsatzsystem bildet.
Taktische Kommunikationssysteme:
BNET: ein fortgeschrittenes SDR, das eine verbesserte und patentierte MANET-Fähigkeit bietet.
BSAT: Lösungen für SATCOM on the Move.
MARS: taktische Router.
Rafael entwickelt und fertigt ein weites Spektrum an Rüstungsgütern für Einsätze in den Domänen Luft, Land, See, Weltraum und Cyber-Raum. Z.B. TROPHY ASPS, die SPIKE Familie, IRONE DOME, SAMSON RCWS und mehr.

roda computer GmbH F 03

... hat sich auf die Entwicklung, Herstellung und den Vertrieb gehärteter Rechnersysteme, Netzwerke und Stromversorgungen spezialisiert. Als führender Anbieter von robuster, mobiler und kundenspezifischer IT-Lösungen kann roda auf mehr als 30 Jahre Erfahrung zurückblicken und ist seit über 16 Jahren mehrfacher Rahmenvertragspartner der Bundeswehr für gehärtete IT.
Aktuelle Entwicklungen zielen darauf ab, bestehende und bewährte Plattformen sowie neue internationalen Standards wie GVA/NGVA gerecht zu werden, um auch künftige Bedarfe, die über Projekte wie „Digital LBO“ und „Morpheus“ entstehen, decken zu können. Dazu kommt deployable Cloudtechnologie (AzureStack) für moderne und performante Apps in autarken Umgebungen.

Kontakt: roda computer GmbH, Landstr. 6, 77839 Lichtenau,
Tel.: +49 7227/9579-0, info@roda-computer.com, www.roda.computer

Rohde & Schwarz M 14

Der Technologiekonzern Rohde & Schwarz entwickelt, produziert und vermarktet innovative Produkte der Mess-, Informations- und Kommunikationstechnik für professionelle Nutzer.
Das international aufgestellte Familienunternehmen liefert Streitkräften und Sicherheitsbehörden so hochsichere, unabhängige, robuste Kommunikationsmittel, die nationale Souveränität ebenso gewährleisten wie die Interoperabilität mit Freunden und Partnern. Gerade für die digitalisierten Truppenteile ab der „Ersten Meile“ bieten die interoperablen, digitalen Software Defined Radios verfügbare wie zukunftsweisende Lösungen. Der Auftrag der Bundeswehr zur Lieferung der streitkräftegemeinsamen, verbundfähigen Funkgeräteausstattung (SVFuA) für die Landstreitkräfte ist die erste Säule des Großprojekts D-LBO (Digitalisierung landbasierter Operationen) der Bundeswehr.

Rohde & Schwarz Cybersecurity schützt mit seinen Sicherheitslösungen Wirtschaft und Behörden vor Sabotage-Angriffen und Spionage.
www.rohde-schwarz.com

rola Security Solutions GmbH M 26

rola entwickelt, vertreibt und integriert IT-Verbundlösungen für die Innere und Äußere Sicherheit. Nationale und internationale Sicherheits- und Ermittlungsbehörden vertrauen unserer Kompetenz. Wir versorgen Sie mit intelligenten und auf den jeweiligen Nutzer perfekt zugeschnittenen IT-Systemen.
Im Rahmen komplexer Ermittlungen, Gefährdungsanalysen oder der Auswertung von Angriffen kommt es darauf an, relevante Informationen zeitnah zu erkennen, zusammenzuführen und zu analysieren. Ohne diese Möglichkeiten trägt die reine Information im Zeitalter des Datenüberflusses kaum noch zur Problemlösung bei.
Sie wollen jederzeit von jedem Ort auf relevante Informationen zugreifen können? Wir helfen Ihnen dabei: • Militärische Lagebilderstellung, • Massendatenanalyse, • Biometrie, Bild- & Videoerkennung, • Social Media Auswertung, • Grenzsicherung, • Cyber Threat Intelligence
www.rola.com

RolaTube Technology Ltd. F 41

Zusammen mit unserem exklusiven deutschen Vertreter JK Defence & Security Products GmbH ist RolaTube Technology Ltd. in der Lage, die gesamte Palette einzigartiger (Funk-)Masten anzubieten.
RolaTube Masten verwenden ein einzigartiges und patentiertes, bi-stabiles, aufgerolltes Verbundmaterial, um leichte und kompakte, aber dennoch robuste und zuverlässige Mastsysteme herzustellen.
Zusätzlich zu den RolaTube-Masten und Stativen sind in die RolaTube IAM Masten (Integrated Antenna Masts) Funk-Antennen in die Struktur des Mastes integriert. Dies stellt den schnellen Aufbau einer Funkverbindung mit deutlich geringerem Gewicht als bei einem herkömmlichen Antennensystem sicher. Sie bieten ein konkurrenzloses Maß an Robustheit und Portabilität für eine schnelle Einsatzverfügbarkeit von Funkübertragungen.
www.rolatube.com / funktechnik@jkdefence.de

RSA F 66

RSA, ein Geschäftsbereich von Dell Technologies, bietet geschäftsorientierte Sicherheitslösungen („Business-Driven Security"), die Geschäftskontext und Sicherheitsvorfälle in einzigartiger Weise verknüpfen, um Unternehmen bei der Bewältigung digitaler Risiken zu unterstützen und zu schützen, was am wichtigsten ist. Die preisgekrönten Cybersecurity-Lösungen von RSA wurden entwickelt, um Advanced Threats effektiv zu erkennen und darauf zu reagieren; Benutzeridentitäten und –zugriffe zu verwalten; Geschäftsrisiken zu reduzieren sowie Online-Betrug und Cyberkriminalität. RSA schützt Millionen von Benutzern auf der ganzen Welt und hilft mehr als 90% der Fortune 500-Unternehmen in einer unsicheren und risikoreichen Welt.

Kontakt: RSA, a Dell Technologies Business, Osterfeldstr. 84, 85737 Ismaning, Martin Issakhani, Tel.: +49 (173) 6535156, E-Mail: martin.issakhani@rsa.com

RUAG Defence F 06

Wir von RUAG «MRO Schweiz» leisten einen wesentlichen Beitrag zur Sicherheit der Schweiz. Als zukunftsorientierter Technologiepartner der Schweizer Armee stehen bei uns Life-Cycle-Management, Betrieb und Verfügbarkeit militärischer Systeme im Vordergrund. Sämtliche Geschäftstätigkeiten orientieren sich demnach stark an den Beschaffungsprogrammen unseres Hauptkunden, der Schweizer Armee.
Zu unserem umfassenden Produkt- und Dienstleistungsportfolio zählen einzigartige Teilsysteme und Komponenten für Ketten- und Radfahrzeuge, Kampfjets, Militärhubschrauber und die Flugabwehr. Hinzu kommen zuverlässige Informations- und Kommunikationslösungen sowie umfassende Wartungs- und Instandhaltungsleistungen.
Unsere Kunden sind in erster Linie nationale und internationale Streitkräfte, Behörden sowie zivile Sicherheitsorganisationen.

Samsung Electronics GmbH M 01

Samsung Electronics GmbH inspiriert Menschen und gestaltet die Zukunft mit Ideen und Technologien, die unser Leben verbessern. Das Unternehmen verändert die Welt von Fernsehern, Smartphones, Wearables, Tablets, Haushaltsgeräten, medizintechnischen Geräten, Netzwerk Systemen, Speicher, System LSI und LED-Lösungen. Entdecken Sie die neuesten Nachrichten, Hintergrundinformationen und Pressematerialien auf www.samsung.de und im Samsung Newsroom unter news.samsung.com/de

SAP Deutschland SE & Co. KG B 11

Das Leben der Menschen verbessern
SAP hat nur ein Ziel: Wir wollen jedem Kunden helfen, mehr zu erreichen. Mit ERP- und Personalwirtschaftslösungen sowie Cloud- und In-Memory-Computing, mobilen Apps und Analyseanwendungen bieten wir Software und Services für jede betriebswirtschaftliche Herausforderung.
Als Marktführer im Bereich Unternehmenssoftware mit rund 93.000 Mitarbeitern weltweit hilft SAP Unternehmen und Organisationen jeder Größe und Branche, profitabel zu wirtschaften, Prozesse schlanker und effizienter zu gestalten, neue Möglichkeiten für Innovation und Wachstum zu schaffen und sich im Wettbewerb zu behaupten. Das SAP Portfolio für Defense und Security umfasst Unternehmenssoftware, Business Intelligence-Lösungen sowie mobile und Cloud-Lösungen.

Schenker Technologies GmbH M 18

Schenker Technologies ist ein führender Anbieter von IT-Hardware sowie den neuesten Extended-Reality-Technologien. Mit den individuell konfigurierbaren Laptops und Desktop-PCs der Gaming-Kultmarke XMG richtet sich das Unternehmen an Privatanwender, während das SCHENKER-Portfolio professionelle Nutzer und gewerbliche Kunden adressiert.
Die E-Commerce-Plattform bestware.com bietet einen darüber hinausreichenden Produktkatalog: Neben den Geräten der beiden Eigenmarken umfasst das Angebot auch ausgewählte Drittanbieter-Lösungen sowie ergänzendes Zubehör.
Zudem agiert das Unternehmen europaweit als Spezialdistributor für Augmented- und Virtual-Reality-Hardware und unterstützt seine Kunden in diesem Bereich bei der ganzheitlichen Umsetzung ihrer gewerblich-kreativen Projekte.
Robert Schenker und Melchior Franke sind Geschäftsführer des 2002 gegründeten Unternehmens, das rund 70 Mitarbeiterinnen und Mitarbeiter am Standort Leipzig beschäftigt.

SCHNEIDER DIGITAL F 22

Schneider Digital – Full-Service Lösungsanbieter für professionelle 3D-Stereo-,VR/AR- und 4K-Hardware
Schneider Digital ist ein weltweit tätiger Full-Service Lösungsanbieter für professionelle 3D-Stereo, 4K- und VR/AR-Hardware und zuverlässiger, zertifizierter Lieferant für Behörden und öffentliche Ämter. Das Schneider Digital Produktportfolio umfasst die richtige professionelle Hardware-Lösung für die jeweilige Anforderung in den Anwendungsbereichen Mapping, Scanning, GIS, Bildauswertung u.v.a. Unsere Produkte und Lösungen umfassen High Resolution 4K-Monitore

(UHD), 3D-Stereo und Touch-Monitore bis 4K-Auflösung und Größen von 27“ bis 98“, VR/AR-Lösungen, von Desktop-System bis hin zur Powerwalls und Multi-Display-Walls, Profi-Grafikkarten von AMD FirePro/Radeon Pro und NVIDIA Quadro, Performance-Workstations sowie innovative Hardware-Peripherie (Tracking, Eingabegeräte u.v.a.). Schneider Digital ist Hersteller einer eignen Powerwall-Lösung (smart VR-Wall) sowie des passiven 3D-Stereo-Monitors 3D PluraView.

Schönhofer Sales and Engineering GmbH F 25

Die Schönhofer Sales and Engineering GmbH ist ein führender, unabhängiger Anbieter von Systemlösungen zur Analyse von Massendaten für Behörden und Privatunternehmen. Unsere Lösungen decken die Datenerfassung (Sensoren), die Verarbeitung und Informationsgewinnung so wie das Datenmanagement und die IT-Infrastruktur ab.
Basis vieler Lösungen ist die Schönhofer TARAN Suite®. Die TARAN Suite® bietet für jeden Auswerteschritt und Analysebedarf das richtige Werkzeug: Signal-, Netzwerk- und Geoanalysen, umfangreiche Text- und Medienanalyse, statistische und lernende Verfahren sowie flexible Berichts- und Ausgabewerkzeuge.
Bestandteile unserer Lösungen sind Robot-basierte Komponenten auf Basis der Kofax Kapow Software und die IBM i2 Analysesoftware. In Kombination unterstützen diese Komponenten den Anwender bei der effizienten Datenerhebung und bringen Transparenz in komplexe Zusammenhänge im Kontext von Ermittlung, Analyse und Auswertung.

SciEngines GmbH B 04

Die SciEngines GmbH bietet spezialisierte Hochleistungsrechner sowie weltweit einzigartige Kryptanalyse Lösungen.
„The SciEngines GmbH RIVYERA S6-LX150 system is the only system that can reasonably be expected to meet the Government’s requirements relative to performance, space, and power consumption.“
Diese Aussage einer NATO Streitmacht wird durch die Vorteile der verwendeten FPGA Technologie ermöglicht. Im Vergleich zu herkömmlichen Computern ist das Preis-Leistungsverhältnis für spezialisierte Anwendungen 10x verbessert. Platz- und Energieeffizienz 20x.
Naheliegende Anwendungen für solch massive Rechenleistung:
- **Cyber** (reaktive defense, -warfare, CNO)
- **Aufklärung** (SIGINT/COMINT) und **„ethical hacking“**
- Überprüfung eigener **IT-Sicherheit / Penetrationstests**

Weitere Informationen: www.SciEngines.com oder info@sciengines.com bzw. 0431-90862000.

secunet Security Networks AG M 16

secunet ist einer der führenden europäischen Anbieter für anspruchsvolle IT-Sicherheitslösungen. Die secunet Division Verteidigung unterstützt militärische Kunden – fokussiert auf Verschlüsselung und Cybersicherheit – beratend, konzeptionell und systemintegrativ. Unsere in nationalen Hochsicherheitsnetzen etablierte, querschnittlich eingesetzte Kryptoarchitektur SINA schützt sensible Informationen im Verteidigungssektor. Sicherheitstechnologien aus den Bereichen digitale Identitäten sowie biometrische Sicherheitslösungen runden das Leistungsportfolio ab.
Unsere Ausstellungsschwerpunkte:
- HaFIS s/v-Clients: SINA Workstation H Client III, SINA Workstation H R RW11
- Data centric Security mit USB Data Safe
- Mobile Anwendungsszenarien am Beispiel des Einsatzes der SINA Workstation S im BMVg
- SINA S (R) Ausstattungsoptionen für VJTF und D-LBO
- SINA H Lösungen für GEHEIM-Telefonie, Messaging und Collaboration
- Erste für GEHEIM einsetzbare VS-Nachweisführung
- sichere Kopplung von Sprachnetzen mittels dem secunet Session Border Controller (in CC EAL 4+ Zertifizierung)

Secusmart GmbH B 08

Secusmart, ein Tochterunternehmen von BlackBerry, bietet Regierungen, Behörden sowie Unternehmen weltweit mit ihren SecuSUITE-Produkten die Möglichkeit der hochsicheren **mobilen, verschlüsselten Sprach- und Datenkommunikation**. Das Düsseldorfer Unternehmen erfüllt von der Infrastruktur bis zum Endgerät alle Anforderungen ihrer Kunden. Der Service umfasst die Analyse und Beratung sowie die Integration von abhörsicherer mobiler Kommunikation in eine bestehende Device- und Server-Infrastruktur. Ebenso die laufende Wartung. Secusmart bietet volle Sicherheit vor einem Lauschangriff. Dabei bleibt der gewohnte Bedienkomfort von modernen Smartphones und Tablets erhalten.

SELECTRIC Nachrichten-Systeme GmbH ME 13

Bereits über 40 Jahre bietet das Familienunternehmen SELECTRIC Nachrichten-Systeme GmbH aus Münster zuverlässige, innovative und wirtschaftliche Hard- und Softwarelösungen sowie Dienstleistungen für die BOS, Industrie, Geschäfts- und Privatkunden. SELECTRIC bietet ein umfassendes Servicekonzept, das u.a. Reparaturpauschalen für BOS-Funkgeräte und Pager, Reparaturen ex-geschützter Endgeräte sowie ein kostenloses Shuttlebox-System zur Minimierung von Ausfallzeiten enthält. Zu den Kernkompetenzen des Unternehmens gehört zudem die Systemtechnik sowie die Projektierung, Realisierung und Wartung kompletter Infrastrukturen für die flächendeckende Funkversorgung.

Kontakt: SELECTRIC Nachrichten-Systeme GmbH, Jacqueline Vogler, Unternehmenskommunikation & Marketing, Haferlandweg 18, 48155 Münster, Email: uk_marketing@selectric.de, www.selectric.de

Sennheiser Vertrieb und Service GmbH & Co. KG F 32

Professionelle Headset-Lösungen für ATC und Contact Center & Office
Sennheiser ist einer der führenden Hersteller von hochwertigen kabellosen und kabelgebundenen Headsets sowie Telefon-/Web-Konferenzlösungen. Die innovative Technologie unterstützt Sie einfach und intuitiv in jeder Business- und Meeting-Situation.
Die Headsets überzeugen durch HD Sound, erstklassiges Design, robuste Verarbeitung und benutzerfreundliche Handhabung. Sie eignen sich besonders für ATC, Contact Center, Offices, Unified Communications-Umgebungen und mobiles Business.
Die perfekte Ergonomie der Sennheiser Produkte garantiert den notwendigen Tragekomfort für langes, ermüdungsfreies Arbeiten. Der Einsatz hochwertigster Materialien lässt Sie selbst und Ihren Gesprächspartner von glasklarer Sprachqualität profitieren.
Besuchen Sie uns auf: www.sennheiser.com/cco

SFC Energy AG S 06

Die SFC Energy AG (www.sfc.com) ist ein führender internationaler Anbieter von stationären und mobilen Hybrid-Stromversorgungslösungen. Mit über 41.000 verkauften Brennstoffzellen steht SFC Energy auf Platz eins der Brennstoffzellenhersteller. Seine zahlreichen mehrfach ausgezeichneten Produkte vertreibt das Unternehmen in der Öl- und Gasindustrie, in Sicherheits- und Industrieanwendungen und im Endverbrauchermarkt. Das Unternehmen hat seinen Hauptsitz in Brunnthal bei München, Deutschland, und betreibt Produktionsstandorte in den Niederlanden, Rumänien und Kanada sowie Vertriebsniederlassungen in den USA und Kanada. Die SFC Energy AG notiert im Prime Standard der Deutschen Börse (WKN: 756857 ISIN:DE0007568578).

SINUS Electronic GmbH F 31

Smarte Feldlagervernetzung im digitalen Zeitalter
Seit mehr als 28 Jahren entwickelt, integriert und liefert die **SINUS Electronic** innovative Produkte an das deutsche Militär.
Mit unseren kundenorientierten Verbindungsschnittstellen für Kommandofahrzeuge und -Shelter sorgen wir für schnellen und sicheren Datenaustausch, Anwendungssicherheit und hohe Verfügbarkeit. Unsere Produkte entsprechen den strengen Anforderungen der Bundeswehr, NATO und MIL-STD.
Mit unserer **SINUS Power-Line-Solution** und **SINUS Hybrid-Solution** bieten wir komplette Infrastrukturen für mobile Gefechtsstände:

- Strom, Daten und Telefonie – alles in einem Kabel
- One-of-a-kind Lösung ermöglicht eine schnelle Bereitstellung im Feld
- Das System kann an die bestehende Infrastruktur angepasst werden
- Das SINUS-Induktiv-Mobil-Telefon bietet eine bis jetzt ungeahnte Flexibilität

info@sinus-electronic.de

Software AG M 18

INNOVATIV, LEISTUNGSSTARK, PARTNER DER BUNDESWEHR
Die Software AG hilft Unternehmen, Behörden und Streitkräften ihre Prozesse zu digitalisieren. Mit Lösungen für Military Internet of Things, Prozessmanagement und IT-Management steigern Streitkräfte die Effizienz und optimieren ihre Prozesse, um qualifizierteEntscheidungen 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.www.SoftwareAG.com

Kontakt: Software AG , Uhlandstr. 9, 64297 Darmstadt, Christoph Reich, Director Defense Business, +49 6151 92 4111, +49 170 4549 537, christoph.reich@softwareag.com

SolarWinds F 53

SolarWinds ist ein führender Anbieter von leistungsfähiger und erschwinglicher IT-Infrastruktur-Management-Software. Mit unseren Produkten können Unternehmen weltweit unabhängig von Typ, Größe oder Komplexität der IT-Infrastruktur die Leistung ihrer IT-Umgebungen überwachen, und zwar sowohl vor Ort als auch in der Cloud oder in Hybridmodellen.
SolarWinds bietet praktisch jedem Ministerium und jeder Zweigstelle des britischen Verteidigungsministeriums leistungsstarke und kostengünstige IT-Managementsoftware. Wir konzentrieren uns ausschließlich auf IT-Experten und bemühen uns, die Komplexität zu beseitigen, zu der sie gezwungen waren. SolarWinds kommt dieser Verpflichtung mit überraschender Einfachheit nach und bietet die Möglichkeit, alle IT-Management-Probleme zu lösen.
Erfahren Sie mehr unter www.solarwinds.com/government

SOLIFOS AG B 03

Solifos ist für Signal- und Energiekabel weltweit bekannt. In der **Wehrtechnik** besticht **Solifos** durch **besonders robuste taktische fiberoptische Feldkabel,** konfektioniert mit verschiedensten **Militärsteckertypen**. Diese Stecker sind zu tausenden seit über 10 Jahren im harten Feldeinsatz. Die breite Zubehörpalette, **zur Feldverlegung,** die **Test-, Unterhalts-** und **Reparaturkits** werden von anspruchsvollen Militärkunden gefordert. Die angebotenen **Lösungen** sind in der **Schweizer Armee,** der **Bundeswehr**, bei weiteren **NATO-Mitgliedern** und **Streitkräften weltweit** beliebt. Der große **Erfahrungsschatz** in **Design und Systemintegration** fließt in die **Lösungspalette,** sowie in **Kundenschulungen** ein. **Am Stand Bo3 im Saal Beethoven präsentieren wir als Hauptthema unsere neuste NATO-Kabelrolle mit optischem Schleifring und Motorantrieb.**
Kontakt: Solifos Deutschland GmbH, 63263 Neu-Isenburg
Vertrieb Deutschland, Edi Lützenkirchen Tel. +49 170 188 20 71

Sopra Steria Consulting M 15

Sopra Steria Consulting zählt zu den Top Business Transformation Partnern in Deutschland. Als ein führender europäischer Anbieter für digitale Transformation bietet Sopra Steria eines der umfassendsten Angebotsportfolios für End-to-End-Services: Beratung, Systemintegration, Softwareentwicklung, Infrastrukturmanagement und Business Process Services. Unternehmen und Behörden vertrauen auf unsere Expertise, komplexe Transformationsvorhaben, erfolgreich umzusetzen. Im Zusammenspiel von Qualität, Leistung, Mehrwert und Innovation befähigen wir unsere Kunden, Informationstechnologien optimal zu nutzen.
Themenschwerpunkte:

- IT-Service-Management
- IT-Architektur-Management
- ILS, Technische Dokumentation
- Master Data Management & Governance
- Application Management
- IT-Sicherheit
- Organisationsmanagement
- Digitalisierung der Verwaltungsarbeit

steep GmbH M 10

Die steep GmbH ist ein international erfolgreicher technischer Dienstleister mit mehr als 30 Standorten und rund 750 Mitarbeitern in Deutschland und Europa. Neben den Kernfähigkeiten in den Bereichen Radar Systems Support, IT-Services, Systemintegration, Training und Mobile Netze zeichnet sich steep durch ein weiteres großes Kompetenzspektrum aus: In Kombination mit den Geschäftsbereichen Logistik und Technische Dokumentation, Material Management, EMV-Service, Managed Services in Partnership und Facility Management profitieren unsere Kunden von der einzigartigen Möglichkeit, alle aufeinander abgestimmten Einzelleistungen in einer gesamtheitlichen Lösung aus einer Hand zu erhalten.
In Anlehnung an das diesjährige Thema der AFCEA-Fachausstellung zeigen wir Ihnen an unserem Messestand M 10 unsere neuesten Lösungen für die vernetzte Operationsführung. www.steep.de

SVA System Vertrieb Alexander GmbH F 23

SVA System Vertrieb Alexander GmbH:
Das System- und Beratungshaus
Die SVA System Vertrieb Alexander GmbH ist einer der führenden deutschen System-Integratoren im Bereich Rechenzentrums-Infrastrukturen und beschäftigt etwa 1.000 Mitarbeiter an 18 Standorten in Deutschland. Das unternehmerische Ziel der SVA ist es, hochwertige IT-Produkte und -Lösungen unterschiedlichster Hersteller mit dem Know-how und der Flexibilität von SVA zu verknüpfen, um optimale Lösungen zu erzielen.
SVA Experten bieten hochwertige Dienst- und Beratungsleistungen im Bereich Informationstechnik mit besonderem Fokus auf äußere und innere Sicherheit an. Das zertifizierte Solution Center der SVA in Wiesbaden steht unseren Kunden mit umfassenden Demo-, Entwicklungs- und Schulungsszenarien mit aktuellsten Hardware- und Software-Lösungen zur Verfügung.

Systematic GmbH M 21

Systematic ist Weltmarktführer für Battle-Managament-Applikationen, Führungsinformationssysteme und Lösungen für die militärische Interoperabilität. Die Military-off-the-Shelf (MOTS) Produkte der SitaWare und IRIS Produktsuiten haben sich weltweit in multinationalen Einsätzen bewährt und werden permanent weiterentwickelt. Einsetzbar in stationären, verlegefähigen, 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 ist dabei stets im Fokus. SitaWare Headquarters ist in der Bundeswehr bereits seit sieben Jahren in der Nutzung. Mit aktuell 28 Nutzernationen ist SitaWare das meist genutzte Führungsinformationssysteme weltweit.

Kontakt: Systematic GmbH, Im Zollhafen 24, 50678 Köln, www.systematic.com, more.info.de@systematic.com

systerra computer GmbH F 68

systerra computer GmbH ist seit über 15 Jahren Anbieter von **MIL-konformen Rechner-, Speicher- und Netzwerkplattformen** für den erweiterten Betriebstemperaturbereich.
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 auch gerne applikationsspezifische Hardware- Sonderlösungen oder beraten bei der Projektierung.
Partner sind u.a.: MPL, Mercury (Themis) Computer, Moxa, RTD, Trenton Systems und Acromag

Kontakt: systerra computer GmbH, Kreuzberger Ring 22, 65205 Wiesbaden, Tel. 0611 / 44 88 9 – 470, E-Mail: info@systerra.de, Internet: www.systerra.de

TASSTA GmbH F 52

TASSTAs Push-To-Talk Lösung verhindert die Grenzen all Ihrer Kommunikation.
Unsere Lösung ist mit den sichersten und verlässlichsten Netzwerken ausgestattet, um die umfangreichste Bereichsdeckung und die höchste Sprachqualität zu bieten. Somit können Sie sich sicher sein, dass Ihr Team Sie immer klar und deutlich versteht.
Sie können den effizientesten Weg für die Kommunikation mit Ihrem Team haben, mit Breitband, WLAN und dem besten Träger-, Gerät- und Applikationsoptionen. Zögern Sie nicht, diese Option jederzeit und überall zu erreichen.
Die multiplattform Software „TASSTA“ präsentiert sich als eine Alternative oder Ergänzung zum klassischen Funk für Smartphones, Tablets und PCs.

TELEFUNKEN Radio Communication Systems GmbH & Co. KG M 13

Wir entwickeln und vertreiben Funkkommunikationssysteme für moderne, sicherheitsrelevante und hochtechnologische Anwendungen. Zur militärischen Nutzung steht ein breitgefächertes Angebot an taktischen und strategischen HF-Funksystemen sowie taktischen VHF- und UHF-Funksystemen zur Land-, Wasser- und Luftanwendung zur Verfügung. Unsere Kompetenz umfasst alle Bereiche der Produktentstehung – vom Systemdesign, der Entwicklung hochperformanter Produkte und der Produktion, bis zur Komplettintegration von Funkübertragungssystemen.
Neben dem Kerngeschäft Funkkommunikation erweitern wir kontinuierlich unsere Geschäftstätigkeiten auch auf Gebieten wie Cyberintelligenz & -sicherheit, Elektrooptische Systeme und Sensorik und reagieren somit auf den wachsenden Bedarf der Bundeswehr an zuverlässigen und leistungsstarken Systemen zur Unterstützung der Auftragserfüllung in den Einsatzgebieten.
www.tfk-racoms.com

Tesat-Spacecom GmbH & Co. KG M 28

In den über fünf Jahrzehnten Auf- und Ausbau der Kompetenzen auf dem Gebiet der nachrichtentechnischen Nutzlasten für Satelliten hat sich Tesat-Spacecom in diesem Bereich als einer der Marktführer etabliert.
Auf 60.000 m² entwickeln, fertigen, integrieren und testen rund 1.100 Mitarbeiter in Backnang, bei Stuttgart, Systeme und Geräte für die Telekommunikation via Satellit. Bis heute wurden über 700 Raumfahrtprojekte durchgeführt.
Unser Produktspektrum umfasst hochzuverlässige Geräte, wie zum Beispiel Wanderfeldröhrenverstärker, Multiplexer, Schalter und Modulatoren, die ebenso wie komplette Systeme an alle führenden Satellitenhersteller weltweit geliefert werden. Damit bieten wir die gesamte Kommunikationstechnik, die notwendig ist, um beispielsweise Fernsehprogramme über Satelliten in jeden Haushalt zu bringen. Mehr als die Hälfte aller Telekommunikations-Satelliten im Orbit haben Tesat-Geräte an Bord.

Textron Systems M 05

Textron Systems Geospatial Solutions flagship software products, ELT®, GIV® and RemoteView™, deliver an extensive set of GEOINT collection tools to enhance the intelligence gathering and analysis process.
From imgery analysis and radar exploitation, to terrain feature extraction and advanced 3D visualization, Textron offers a proven solution for situational understanding and interoperability. Textron Systems Geospatial Solutions are used across a broad spectrum of industries: military and defense, border security, disaster relief, environmental engineering, ecosystems monitoring, urban planning, insurance, oil and gas exploration, utility companies and more to provide unmatched fidelity and accuracy in mission planning, actionable intelligence and rapid decision making.
See www.textronsystems.com for more information.

Kontakt: Kevin Opitz, E-Mail: geosalesteam@overwatch.textron.com

Thales M 11

Thales ist seit Jahrzehnten bei Ausrüstung und Service von Mobilen Taktischen Kommunikationssystemen Partner der Bundeswehr und der NATO. Durch ein hochmodernes, im Einsatz erprobtes Portfolio steht Thales als Systemanbieter der Bundeswehr bei der Umsetzung des D-LBO-Programms mit Beratung, Entwicklung, Design, Inbetriebnahme und Service zur Seite.
Thales verfügt über ein Produktportfolio, das modular an den einsatzbedingten Kommunikationsbedarf angepasst werden kann. Eine moderne Systemarchitektur ermöglicht eine nahtlose, medienbruchfreie Kommunikation und bildet einen wichtigen Beitrag zum Missionserfolg. Einsatzerprobte C2-Kommunikationssysteme sowie die Entwicklung der Breitbandwellenform ESSOR bilden die Säulen einer dienste-orientierten Kommunikation.
Moderne Funksysteme wie die neue Software-Defined-Radio-Produktfamilie SYNAPS, leistungsfähige Kryptologie- und Schlüsselmanagementlösungen und moderne SOTM-Systeme stellen die notwendigen Kommunikationsplattformen zur Sicherstellung eines “Quality of Services” sicher.
www.thalesgroup.com/germany

Trend Micro GmbH B 13

Als einer der weltweit führenden Anbieter von IT-Sicherheitslösungen verfolgt Trend Micro das Ziel, eine sichere Welt für den digitalen Datenaustausch zu schaffen. Die innovativen Lösungen für Privatanwender, Unternehmen und Behörden bieten mehrschichtigen Schutz für Rechenzentren, Cloud-Workloads, Netzwerke und Endpunkte.
Die miteinander kommunizierenden Produkte bilden einen vernetzten Schutzmechanismus, der durch zentrale Transparenz und Kontrolle eine schnellere und bessere Absicherung ermöglicht.

Mit mehr als 6.000 Mitarbeitern in über 50 Ländern und der weltweit fortschrittlichsten Erforschung und Auswertung globaler Cyberbedrohungen bietet Trend Micro Schutz für eine vernetzte Welt.
Weitere Informationen: www.trendmicro.com.

T-Systems International GmbH M 26

Mit Standorten in über 20 Ländern, 37. 900 Mitarbeitern und einem externen Umsatz von 6,9 Milliarden Euro (2017) ist T-Systems einer der weltweit führenden herstellerübergreifenden Digitaldienstleister mit Hauptsitz in Europa.
T-Systems ist Partner seiner Kunden auf dem Weg der Digitalisierung. Das Unternehmen bietet integrierte Lösungen für Geschäftskunden. Bei der Tochtergesellschaft der Deutschen Telekom kommt alles aus einer Hand: vom sicheren Betrieb der Bestandssysteme und klassischen IT- und Telekommunikations-Services über die Transformation in die Cloud einschließlich internationaler Netze, bedarfsgerechter Infrastruktur, Plattformen und Software bis hin zu neuen Geschäftsmodellen und Innovationsprojekten im Internet der Dinge.
Grundlage dafür sind globale Reichweite für Festnetz- und Mobilfunk, hochsichere Rechenzentren, ein umfassendes Cloud-Ökosystem mit standardisierten Plattformen und weltweiten Partnerschaften sowie höchste Sicherheit.
www.t-systems.com

Ultralife communication Systems F 41

Ultralife, ein globales Unternehmen mit Hauptsitz in Newark, New York, nutzt seine Design- und Engineering-Expertise und liefert innovative und maßgeschneiderte Lösungen.
Mit seiner Sparte Battery & Energy bietet Ultralife eine breite Palette an hochenergetischen, wiederaufladbaren und nicht wiederaufladbaren Batterien sowie Ladegeräte für militärische und kommerzielle Anwendungen, zum Teil mit höchsten realisierbaren Energiedichten.
Eine weitere Sparte, die Communications Systems Engineering, bietet innovative taktische Kommunikationslösungen für sich ständig ändernde Aufgabenstellungen. Das Portfolio reicht von einsatzerprobten plattformunabhängigen Verstärkern für den fahrzeuggebundenen und abgesessenen Einsatz bis hin zu unterschiedlichen robusten und innovativen Funkgerätehalterungen und Stromversorgungen zur Unterstützung des Gefechtsfunks und der Einsatzkräfte.
www.ultralifecorp.com / funktechnik@jkdefence.de

Utimaco S 09

Utimaco ist ein weltweit tätiger Anbieter von professionellen IT-Sicherheitslösungen mit Sitz in Aachen, Deutschland und Campbell, USA. Utimaco entwickelt Hardware-Sicherheitsmodule, Festplattenverschlüsselung und Compliance-Lösungen für Telekommunikationsanbieter im Bereich der Regulierung als einer der führenden Hersteller. Über 220 Mitarbeiter haben sich dem unternehmerischen Ziel verschrieben, Menschen, Ideen und Daten zu schützen. Utimaco Hardware-Sicherheitsmodule (HSM) erzeugen und verwalten kryptografische Schlüssel und sichern digitale Identitäten. Damit bilden HSM den Vertrauensanker zum Schutz digitaler Daten und kritischer Infrastrukturen – etwa im Finanzsektor, in der Automobilindustrie, für Cloud-Dienstleister oder den öffentlichen Dienst. Die Utimaco Festplattenverschlüsselung ist für VS-NfD zugelassen und wird in Behörden und Industrie eingesetzt.

Verband der Reservisten der Deutschen Bundeswehr e.V. F 45

Der Reservistenverband – gegründet im Januar 1960 in Bonn – ist für die Betreuung aller Reservisten der Bundeswehr zuständig. Der Verband bekam vom deutschen Bundestag und der Bundesregierung 1971 den Auftrag, aus der Bundeswehr ausscheidende Offiziere, Unteroffiziere und Mannschaften nach den Richtlinien des Verteidigungsministeriums im Rahmen des Wehrrechts zu betreuen und fortzubilden.

Grundsätzliches ...

- Staatsbürger, die sich freiwillig und überparteilich für Staat und Streitkräfte engagieren wollen
- VdRBw ist einziger Verband, der offiziell für die Betreuung und Weiterbildung von Reservisten beauftragt ist und dafür Mittel bezieht → mit Zustimmung des Parlaments

Reservistenverband als ...

- 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 F 41

Viasat ist der weltweit führende Anbieter von UHF-Satellitenkommunikation, UHF-Netzwerk-Interoperabilität und UHF-Modernisierung für Verteidigungsorganisationen. Vom Einzelplatzterminal bis hin zu kompletten UHF-Systemen für hoheitlich kontrollierte Satellitenkanäle bietet Viasat Terminals, Modems, Simulatoren, Netzwerkmanagement und RF-Infrastruktur. Viasat Terminals sind Joint Interoperability Test Command (JITC) und NSA-zertifiziert, um die Einhaltung der alten Wellenformen DAMA (Demand Assigned Multiple Access) IW (Integrated Waveform) gem. MIL-STDs sicherzustellen und die Sprach- und Dateninteroperabilität mit den eingesetzten UHF-SATCOM-Terminals zu gewährleisten.
www.viasat.com / funktechnik@jkdefence.de

VITES GmbH S 06

Die VITES GmbH (“VITES”) ist ein junges Unternehmen, das sich auf Produkte der Breitband-Funktechnik für professionelle Einsatzgebiete spezialisiert hat. Fokusgebiet des Unternehmens sind SATCOM-on-the-Move (SOTM) Lösungen und breitbandige Datenlinks mit vollelektronischer Strahlformung und –nachführung auf Basis von Phased-Array-Antennentechnologie und Software-Defined-Radio (SDR).
Ein weiterer Schwerpunkt ist „HiMoNN“, die robuste, ausgereifte und kosteneffiziente Lösung für breitbandige und mobile Ad-Hoc-Funkysteme im Bereich der öffentlichen Sicherheit und im Katastrophenschutz, die auch in Defense-Szenarien einsetzbar ist.
Standort des Unternehmens ist Ottobrunn bei München.

Kontakt: VITES GmbH, Einsteinstraße 32, 85521 Ottobrunn, www.vites.de,
Ansprechpartner: Theodor Fokken, Senior Solution Sales Mgr.,
Tel.089 6088-4604, mail:fokkent@vites-gmbh.de

23. Europäischer Polizeikongress

Save the Date

04. – 05. Februar 2020

Europa: Rechtsstaat durchsetzen

www.europaeischer-polizeikongress.de

Eine Veranstaltung des **Behörden Spiegel**

Magazinreihe

Moderne POLIZEI

neue Schriftenreihe

Themen 2019:

- Die Cyber-Polizei
- Ausrüstung
- Mobilität der Polizei

Informationen zur Bestellung eines Probe-Exemplars unter:
https://www.behoerden-spiegel.de/sonderpublikationen/

BSC Berlin Security Conference

18th Congress on European Security and Defence

Impressions BSC 2018

For further photos and information please see

www.euro-defence.eu

BSC Berlin Security Conference

18th Congress on European Security and Defence

Berlin Security Conference 2019

Europe and its external challenges – a 360° approach in uncertain times

Berlin 26 – 27 November 2019, Vienna House Andel's Berlin

Visit us on Europe's leading event for European Security and Defence

Photos: Dombrowsky

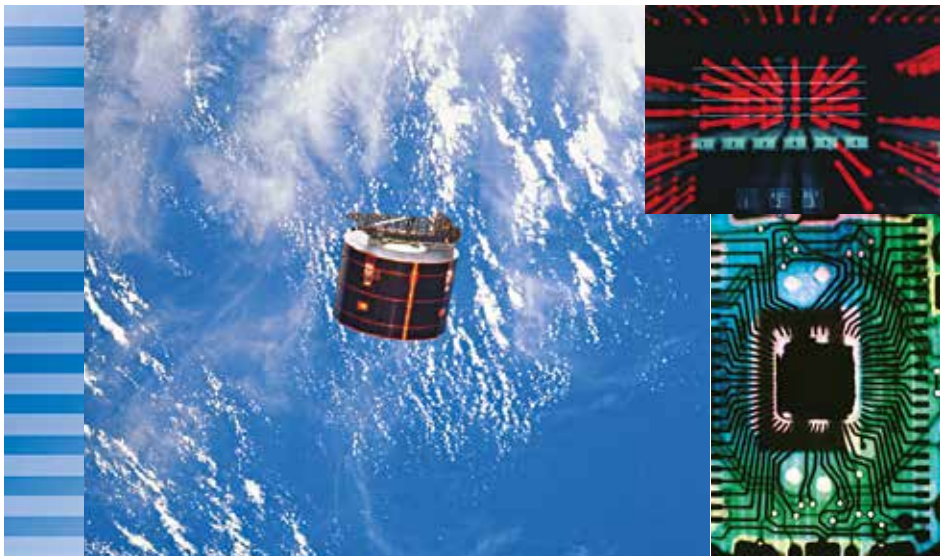
Impressions of the BSC 2018

The Berlin Security Conference

- One of the largest yearly events on European Security and Defence
- Meeting place for about 1 000 participants from more than 50 countries
- International forum for members of parliament, politicians and representatives of the armed forces, security organisations and industry
- Partner in 2019: Italy
- Former Partners: Russia, United Kingdom, Turkey, USA, France, Sweden, Netherlands
- Exhibitions with companies from Europe and abroad
- Organised by the Behörden Spiegel – Germany's leading independent Newspaper for Civil and Military Services

Further Information:

www.euro-defence.eu



Vorankündigung:

34. AFCEA-Fachausstellung

1./2. April 2020

Im World Conference Center Bonn

www.afcea.de