Hardthöhen-KURIER
DAS MAGAZIN FÜR SOLDATEN UND WEHRTECHNIK
FÜR EIN STARKES EUROPA

SONDERAUSGABE
zur AFCEA-Fachausstellung 2023

AFCEA Bonn e.V.

36. AFCEA Fachausstellung – 10./11. Mai 2023

MATERNA
Information & Communications

WIR DIGITALISIEREN IHRE WELT

IT-Dienstleister im Einsatz

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

Bereit für die digitale Transformation in der Bundeswehr?

Weitere Infos:
www.materna.de/bw

Der nächste Konflikt wird ein Krieg der Algorithmen sein

Von Jochen Reinhardt, AFCEA Bonn e.V., Vorstand Presse- und Öffentlichkeitsarbeit

Die 36. AFCEA Fachausstellung vom 10. bis 11. Mai im World Conference Center in Bonn (WCCB) hat einen Aussteller- und Besucherrekord aufgestellt. 250 Unternehmen und Organisationen stellten bei einer der wichtigsten deutschen IT-Messen für Verteidigung und Sicherheit aus. Mehr als 4.100 Teilnehmerinnen und Teilnehmer kamen ins WCCB.

„Wir haben turbulente Zeiten. Wir müssen Deutschland wach rütteln", sagte Brigadegeneral Armin Fleischmann, Vorsitzender AFCEA Bonn e.V. und Unterabteilungsleiter CIT 1 im Bundesministerium der Verteidigung, in seiner Eröffnungsrede zur aktuellen Relevanz der Ausstellung, die in diesem Jahr unter dem Motto „(Künstliche) Intelligenz & Innovationen – Konkrete Nutzungsmöglichkeiten" stand.

Zeitenwende anpacken: gemeinsam, mutig, schnell!

Dieser Blick auf die konkrete Nutzung ist dringender denn je: Moderne Kriege sind digital unterstützt und werden digital geführt, stellte Generalleutnant Michael Vetter, Abteilungsleiter CIT im Bundesverteidigungsministerium, in seinem Grußwort zur Eröffnung fest. „Lassen Sie uns die Zeitenwende anpacken: gemeinsam, mutig und schnell!" Vor allem an der Geschwindigkeit müsse man noch arbeiten. Kapitän zur See Stephan Mauritz aus dem Planungsamt der Bundeswehr bestätigte die Bewertung mit dem Blick auf den Angriffskrieg Russlands auf die Ukraine. Das Gefechtsfeld der Zukunft werde sehr stark vom Technikeinsatz entschieden: Das Gefecht sei „hyper": sehr schnell, umfassend, rücksichtslos, teils gläsern.

Der zweite Tag war im begleitenden Symposiumsprogramm von konkreten Anwendungen und Betrachtungen geprägt. In der #DigitalDefenceDebate blickten die Emerging Leaders AFCEA Bonn e.V. zunächst mit Ammar Alkassar, Vorstandsmitglied des GovTech Campus Deutschland, ehemals CIO Saarland, Dr. Sven Stephen Egyedy, Beauftragter für Digitalisierung, Digital- und Datenpolitik (CDO), Auswärtiges Amt, Oberst i.G. Klaus Günter Glaab, Referatsleiter Digitale Verwaltung im Stab Org/Rev BMVg, und Linda Oldenburg, Head of Consulting Business Resilience, Firma Nortal AG, auf Innovationen und KI-Anwendungen für die Verwaltung.

Softwareeinsatz ist in der ukrainischen Verteidigung entscheidend

Für eine schnelle Umsetzung fehle in Deutschland das Dringlichkeitsgefühl, stellte Alkassar fest, der sich auch in einer Diskussion zur Rolle von Software und Digitalisierung bei der Verteidigung der Ukraine beteiligte. Dr. Gundbert Scherf, Mitgründer und Co-CEO Helsing, ist sich sicher, dass bestehende Hardware und Ausstattung durch Software entscheidend – bis zu einem Faktor zehn – verbessert werden kann. Dabei würde heute jedoch noch nicht Künstliche Intelligenz in großem Ausmaß eingesetzt. „Doch der nächste Konflikt wird wahrscheinlich ein Krieg der Algorithmen." Für Franz-Stefan Gady, International Institute for Strategic Studies, ist dabei noch offen, ob die taktische Überlegenheit durch den Kampf der verbundenen Waffen die ukrainischen Streitkräfte durch Software Defined Defence die russische quantitative Überlegenheit überwinden kann.

Blick in den Ausstellungssaal New York/Genf.

©AFCEA Bonn e.V.

Der Vorsitzende AFCEA Bonn e.V., Brigadegeneral Armin Fleischmann, mit Friedrich W. Benz (li.) und seinem Nachfolger Wolfgang Quirin.

Ausstellungsleiter Friedrich W. Benz verabschiedet

Nach 17 Fachausstellungen war die 36. AFCEA Fachausstellung in diesem Jahr die letzte unter der Leitung von Friedrich W. Benz. Er hat die Ausstellung von der Godesberger Stadthalle über das Hotel Maritim über die Jahre ausgebaut und sowohl bei Aussteller- und Besucherzahlen kontinuierlich nahezu jährlich neue Rekordwerte erreicht. Heute ist die AFCEA Fachausstellung mit 250 Ausstellern im WCCB etabliert.

Die AFCEA Fachausstellung als Dialogplattform der IT-Community Bundeswehr

Was macht die AFCEA Fachausstellung für Aussteller und Besucher gleichermaßen attraktiv? Mehr als 200 Firmen stellen dort ihre neuesten Produkte in der spezifischen AFCEA-Themenpalette aus und stehen für einen intensiven Dialog mit interessierten Fachbesuchern aus dem Bundesministerium der Verteidigung, aus den Ämtern und anderen Dienststellen der Bundeswehr und Behörden im Raum Bonn-Koblenz-Köln, aus Fachhochschulen und Universitäten sowie der Industrie bereit. Wenngleich es nur eine geringe Fluktuation der Aussteller gibt, kommen jedes Jahr wieder neue Aussteller dazu. Die Firmen erreichen durch diese Ausstellung eine Vielzahl von Ansprechpartnern aus einer großen Anzahl von Dienststellen. Konzeptionäre der Bedarfsträger und Projektleiter/-mitarbeiter der Bedarfsdecker schätzen das umfassende Informationsangebot der bei der Ausstellung präsenten Firmen. Im Gegensatz zu Besuchen bei einzelnen Firmen in ganz Deutschland, die meist sehr zeitaufwendig und kostenträchtig sind, bietet die AFCEA Fachausstellung die Gelegenheit, in relativ kurzer Zeit die Produkte unterschiedlicher Firmen präsentiert zu bekommen. Ein Besuch bietet eine effiziente Weiterbildung mit hoher Informationsdichte bei in der Regel kurzem Anfahrtsweg aus dem Einzugsgebiet Köln-Koblenz.

Ausblick

In der nun 36-jährigen Geschichte hat die AFCEA Fachausstellung viele Aussteller und neue Entwicklungen der IT gesehen. Viele Firmen der ersten Stunde gibt es nicht mehr oder sie sind in anderen Firmen aufgegangen. Bei geringer Fluktuation von maximal 20 Prozent in den vergangenen zehn Jahren hat die AFCEA Fachausstellung einen großen Stamm von Ausstellern, die jedes Jahr die Fachausstellung als Portal zu Bundeswehr und BOS nutzen. Andererseits kommen immer wieder neue Firmen mit interessanten Portfolios hinzu. Auch bei veränderten Rahmenbedingungen und Bedrohungen, Schwerpunkten und Hypes in der IT-Welt wird die AFCEA Fachausstellung, das Flaggschiff von AFCEA Bonn e.V., weiterhin interessante Themen für die IT-Community Bundeswehr aufgreifen und in Zukunft bei der Fachausstellung einem breiten Publikum präsentieren. *(re/be)*

Über AFCEA Bonn e.V.:

AFCEA Bonn e.V. bietet seinen Mitgliedern und der interessierten Öffentlichkeit ein Spezialforum moderner Informations- und Kommunikationstechnologie. Das Anwenderforum für Fernmeldetechnik, Computer, Elektronik und Automatisierung (AFCEA) Bonn e.V. umfasst als gemeinnützig anerkannter Verein ohne kommerzielle Interessen über 1.000 persönliche und mehr als 100 Firmenmitglieder. Zu den Firmenmitgliedern gehören neben den Großen der IT- und Kommunikationsbranche eine Vielzahl mittelständischer und kleinerer Unternehmen vornehmlich aus der Region Bonn-Koblenz-Köln. Gegründet wurde AFCEA International 1946 von Angehören der US-Streitkräfte zur Verbesserung des Fernmeldewesens. Der deutsche Verein geht auf die Initiative von Soldaten zurück, die 1983 den Austausch rund um Informations- und Kommunikationstechnik im Verteidigungs- und Sicherheitsbereich fördern wollten. Eingebettet in eine internationale Organisation zählt AFCEA Bonn e.V. heute zu den etabliertesten Dialogplattformen für diese Themen.

roda
RUGGED IT & ELECTRONICS

Kontakt:
roda computer GmbH
Landstraße 6
77839 Lichtenau
info@roda-computer.com

Als europaweit führender Anbieter robuster IT- und Elektronik-Lösungen im verteidigungstechnischen Umfeld, bietet roda computer die Entwicklung, Modifikation und Lieferung von speziell gehärteten militärischen Endgeräten, Displays, Servern, Netzwerktechnik und Stromversorgungen. Strategische Partnerschaften erweitern das Produktportfolio um robuste Kommunikationstechnik wie auch Hochleistungsserver und unterbrechungsfreie Stromversorgungen.

Die neusten Entwicklungen aus der Kooperation roda computer mit Panasonic TOUGHBOOK ermöglichen kundenspezifische Anpassungen an dem robusten TOUGHBOOK FZ-40 durch militärische Rundstecker oder zusätzlichen Schnittstellen auf Modulbasis. Mit diesen militärspezifischen Lösungen, die in ganz Europa angeboten werden, eröffnen sich für Organisationen in Sicherheit und Verteidigung neue, flexible und zukunftsgerichtete Nutzungsmöglichkeiten von mobiler IT.

ELT
ELETTRONICA GROUP

Kontakt:
Peter Mark
Account Manager
Mobil +49 (0) 173 9987285
Büro +49 (0) 2225 8806-23
Fax +49 (0) 2225 8806-47
Am Hambuch 10
53340 Meckenheim
www.elettronica.de

Die **Elettronica GmbH** hat auf der diesjährigen AFCEA ein Trainings- und Ausbildungssystem für Radarsimulation ausgestellt und Kunden präsentiert. Das Produkt kann kundenspezifisch designt, aus einem vielfältigen Baukastensystem gebaut und betrieben werden. Die unterschiedlichen einsatzspezifischen Betriebs- und Bauformen werden gemeinsam mit dem Kunden erarbeitet. Erfahrungen eines Integrators mit Produkt- und Projekterfahrungen im Bereich Electronic Warfare (EW) liefern in kurzer Entwicklungs- und Planungszeit eine Erfüllung der Kundenwünsche bei minimalisiertem Entwicklungsrisiko. Seit 1978 ist die **Elettronica GmbH** auf dem deutschen Markt für militärische und zivile Kunden ein Partner über den gesamten Produktlebenszyklus, welcher nicht nur die EW-Systeme, sondern auch modulare Trainingssysteme zu den EW-Systemen für Bediener- und Trainerschulungen bietet.

BWI: Digitalisierungspartner der Bundeswehr in Frieden, Krise und Krieg

Im Interview mit dem Hardthöhenkurier fordert Frank Leidenberger, CEO und Sprecher der Geschäftsführung der BWI GmbH, eine intensive Diskussion um ethische Aspekte von Künstlicher Intelligenz.

BWI
IT für Deutschland

Sehr geehrter Herr Leidenberger, das Leitthema der AFCEA Fachausstellung 2023 ist Künstliche Intelligenz und Innovationen und konkrete Nutzungsmöglichkeiten für die Bundeswehr. Welche Bedeutung haben Innovationen und KI als Schlüsseltechnologie für die Bundeswehr und damit für die BWI?
KI kommt im militärischen Bereich in immer größerem Maße zum Einsatz. Dies lässt aktuell auch der Krieg in der Ukraine erkennen, etwa bei Drohneneinsätzen, der Auswertung von Social-Media-Daten oder der Erstellung täuschend echter Deepfakes. Kurz gesagt: KI beeinflusst schon heute den Ausgang militärischer Konflikte.
Als primärer Digitalisierungspartner der Bundeswehr haben wir als BWI die Aufgabe, auch mit Blick auf KI die Einsatz- und Führungsfähigkeit der Bundeswehr zu erhöhen. Künstliche Intelligenz bietet enorm viele Anwendungsmöglichkeiten, beispielsweise bei der Datenauswertung.
Bei der Entwicklung von IT-Lösungen für die aktuellen Herausforderungen der Bundeswehr im Cyberraum spielen wiederum die Entwicklung und Erprobung von passgenauen IT-Innovationen eine große Rolle. Unser Innovationsverständnis lautet „Innovativ by Design". Was heißt das? Innovationen fließen in unsere Lösungen ein. Also: Nicht Innovationen um der Innovation willen, sondern da, wo sie die Einsatz- und Führungsfähigkeit der Bundeswehr erhöhen.

Einsatz- und Führungsfähigkeit in allen Lagen: Wie sichert die BWI im Sinne digitaler Souveränität den Zugang für die Bundeswehr?
Digitale Souveränität definieren wir momentan so, dass wir nicht alles selbst machen müssen, aber für alles eine eigene Bewertungsfähigkeit haben. Wir entscheiden, welche Technologie von welchem Provider wir nutzen, weil wir verstehen, wie es funktioniert. Es gibt Open Source Software, die im Netz verfügbar gemacht wird. Da es viele Nutzer gibt, geht man davon aus, dass sie ein hohes Maß an Sicherheit haben. Nichtsdestotrotz braucht man, wenn man sie anwenden will, eine Stelle, die sie bewertet und qualifiziert. Wir haben das am Beispiel des Bw Messenger gemacht. Wir haben ein offenes Protokoll namens Matrix genommen, es mit eigenen und den Entwicklern der Firma auf unsere Bedürfnisse angepasst und den Messenger so sicher gemacht, dass er eine BSI-Zulassung für VS-NfD bekommen hat. Das ist der Weg nach vorne, der auf dem Software-Layer dafür sorgt, dass wir hinreichend souverän sind.

Stichwort „Zeitenwende": Welchen Einfluss hat die veränderte sicherheits- und geopolitische Situation auf die BWI und ihre Aufgaben?
Als IT-Dienstleister der Bundeswehr müssen wir die IT in Krise und Krieg gewährleisten. Die Bundeswehr kann das, was wir tun, nicht mehr einfach ersetzen. Wir sind integraler Bestandteil des IT-Systems und haben unser Zielbild weiter so geschärft, dass das, was wir machen, immer grüner wird. Wir betreiben schon jetzt IT-Systeme für die Bundeswehr in den Einsätzen, beispielsweise beim Luftumschlagpunkt in Niamey in Niger. Auch eine Unterstützung im Baltikum für die VJTF ist geplant. Die BWI wächst im grünen Bereich, und das in der Rechtsform einer GmbH. Das wirft manchmal Fragen nach unserer Verlässlichkeit auf. Aber wir wissen, was wir tun, und alle Mitarbeiterinnen und Mitarbeiter sind genauso da wie die Soldatinnen und Soldaten. Wir sind genauso resilient und einsatzwillig wie andere, halt ein Spiegelbild der Gesellschaft. Die BWI durchläuft also den Wandel vom „Herkules-IT-Lieferanten" hin zum IT-Systemhaus und primären Digitalisierungspartner der Bundeswehr in Frieden, Krise und Krieg.

Apropos Spiegelbild unserer Gesellschaft: Die ist ja nicht besonders durchdigitalisiert ...
Ja, genau. Digitalisierung der Streitkräfte ist ein Megathema. Wir sind teilweise schlechter als in der Wirtschaft, wo der Handlungsdruck deutlich höher ist, um Gewinn zu erzielen. In der öffentlichen Verwaltung kennen wir nur den Mittelabfluss und machen keinen modernen Controlling-Ansatz, schauen eher auf Sparsamkeit. Das behindert die Digitalisierung, bei der man erst einmal eine Investition leistet, denn man muss neue Software entwickeln, braucht neue Server und vieles mehr.

Ein weiterer Aspekt: Wenn man Digitalisierung richtig versteht, geht es nicht um Mensch-Maschine-Interfaces. Gute digitale Prozesse laufen im Hintergrund ab, brauchen eigentlich keine Menschen mehr. Sicherlich muss am Anfang ein Mensch ein Programm schreiben und Daten eingeben. Aber wenn es gut integriert ist, funktionieren Prozesse deswegen so gut, weil sie ohne Mensch-Maschine-Interface auskommen. Dann sind wir digital, dann hilft es bei der Wertschöpfung. Da sind wir für die Bundeswehr in der Perspektive der Kill Chain. Nicht zuletzt müssen wir damit umgehen, dass wir wahrscheinlich nicht mehr Soldaten haben werden als die derzeit rund 180.000. Es sei denn, wir führen die Wehrpflicht wieder ein. Aber wollen wir wirklich, dass unsere Söhne und Töchter auf dem Schlachtfeld fallen, nur weil wir keine Hochtechnologielösungen zulassen?

Der Fachkräftemangel ist seit Jahren allgegenwärtig – vor allem im IT-Sektor. Wie wollen Sie hier Wachstum generieren?
Als IT-Dienstleister ist organisches Wachstum in der aktuellen Zeit natürlich kein Selbstläufer. Trotzdem haben wir es in den letzten sechs Jahren geschafft, um den Faktor 4,2 zu wachsen – das heißt, wir haben rund 4.000 neue Kolleginnen und Kollegen an Bord geholt.
Wer bei uns arbeitet, leistet einen direkten Beitrag zur Arbeit der Bundeswehr und zum Schutz der Bundesrepublik Deutschland. Weil dieser tiefere Sinn in der Arbeit und spannende Aufgaben allein aber nicht reichen, haben wir uns zum Ziel gesetzt, der modernste Arbeitgeber im öffentlichen Sektor zu werden. Diesen Weg gehen wir konsequent.
Wir prüfen natürlich auch, wo wir selbst automatisieren können. Der ganze IT-Betrieb zielt ja grundsätzlich immer darauf, möglichst viel zu automatisieren, weil es nicht nur Menschen spart, sondern eigentlich auch verlässlicher läuft. Ein händisch aufgesetzter Server ist wesentlich störanfälliger als die Cloud als hoch automatisiertes Bereitstellungssystem.

Bei „hoch automatisiert" kommen wir wieder an den Anfang des Interviews zurück. Ist das im IT-Bereich der Bundeswehr überhaupt bis zur letzten Konsequenz gewollt?
Die BWI erhält ihre Aufträge von der Bundeswehr, nach Recht und Gesetz geprüft. Alle Punkte, die man diskutieren könnte, ob sie genutzt werden sollten oder nicht, wie etwa KI für autonome Waffensysteme, auf die die Bundeswehr ja verzichten will, sind dann schon entschieden. Wir würden solche Aufträge gar nicht bekommen.
Ich persönlich glaube allerdings, dass sich diese Haltung ändern wird, weil sie sich ändern muss. Wer dediziert auf fortschrittliche Technologien verzichtet, wird auf dem Gefechtsfeld nur zweiter Sieger sein. Ich meine, dass wir als BWI Künstliche Intelli-

Sich auch den ethischen Fragen stellen, fordert Frank Leidenberger im Gespräch mit Burghard Lindhorst.

Von der ersten Minute an ein zentraler Anlaufpunkt: der Stand der BWI.

genz als wesentlichen Baustein für autonome oder automatisierte Systeme sicher machen müssen. Wir würden gewährleisten, dass sie ausschließlich das machen, für das sie programmiert wurden. Darin sehe ich eine große Aufgabe für die Zukunft.

Da gibt es verständlicherweise auch viele ethische Fragen. Automatisierte Waffensysteme töten Menschen. Die KI hilft dabei. Aber was machen denn die Soldaten im Kriege? Etwas anderes? Das sind Diskussionen, die noch lange nicht zu Ende geführt sind. Ich erinnere mich an Afghanistan mit der Diskussion um die Bewaffnung von Drohnen. Unter dem Aspekt „Digitale Ethik von Künstlicher Intelligenz" sollten wir diskutieren, wie wir die Systeme so bauen, dass sie unseren Wertevorstellungen folgen. Da gibt es technologische Ansätze im Produktionsprozess. Wenn man KI programmiert, kann man diese Fragen berücksichtigen. Aber KI ist nicht deterministisch. Wenn sie 100.000-mal eine Lösung abfragen, kommt nicht 100.000-mal das gleiche raus. Das ist eine besondere Herausforderung. Aber ein Mensch ist auch nicht fehlerfrei. Es wird keine Maschine geben, die Grausamkeiten begeht, es sei denn, man hat ihr das einprogrammiert. Das ist eine Frage der Software.

Meine Position ist ganz klar: Es wird passieren. Wenn wir es nicht machen, die anderen machen es bestimmt. Wenn wir nicht mithalten, werden wir im Nachteil sein. Wir sollten zeigen, dass wir es können, allein schon aus Gründen der Abschreckung.

Schauen wir auf die Ukraine: Wäre sie in der NATO oder hätte sie nicht ihre Nuklearwaffen abgegeben, hätte sie über ein wirksames Abschreckungspotenzial verfügt und eine russische Regierung wäre sicherlich zu einem anderen Risikokalkül gekommen. Ich finde, wir müssen diese Diskussionen offener und aggressiver führen. Das reine Wiederholen der Verteidigungsanstrengungen aus den achtziger Jahren, wo wir wirklich top waren, wird uns nicht siegfähig machen. Für Abschreckung müssen wir zumindest in der Perzeption des Gegners als siegfähig erscheinen. Wenn wir uns mit diesen Fragen nicht auseinandersetzen, sondern dies ethisch-ideologisch in die Ecke legen, werden wir wie bei vielen anderen Dingen überrascht sein, was die Welt um uns herum so macht.

Sehr geehrter Herr Leidenberger, vielen Dank für das interessante Gespräch!

Conrad blickt auf eine erfolgreiche Messeteilnahme zurück und sagt herzlichen Dank: Key Account Manager Stefan Pahl und Dominik Glampe, Generalmajor a.D. Klaus-Peter Treche, Oberst i.G. Peter Kraus, Head of Sales Ingo Haase, INTERIM Berater Dr. Martin Rüttler (v.l.n.r.).

Kontakt:
Ingo Haase
Head of Sales North/West &
Conrad Electronic SE
Klaus-Conrad-Str. 1
92240 Hirschau
ingo.haase@conrad.de
www.conrad.de

Conrad Electronic steht als zuverlässiger Partner seit 1923 für Technik und Elektronik und bietet heute als Sourcing Platform Produkte und Services für Geschäftskunden, Behörden und auch im Besonderen für die Bundeswehr an. Einkaufsverantwortliche sowie Bedarfsträger bspw. aus dem Facility-Management, Logistik, Fuhrpark oder MRO decken auf der Conrad Sourcing Platform ihren gesamten technischen Bedarf aus einer Hand und profitieren von maßgeschneiderten E-Procurement-Lösungen.

2023 präsentierten wir neben unseren digitalen Beschaffungslösungen Highlights aus unserem Sortiment, das aktuell **neun Millionen Produktangebote** erfasst. Dabei erhielten die neuen Multimeter von Voltcraft, die DJI Mavic 3 Drohne, aber auch im Besonderen der 3D-Drucker von Renkforce als Blickfang besondere Aufmerksamkeit.

Sicherheit für unsere Kunden!

„Erkenntnisse aus Zusammenhängen, nicht nur aus Einzelinformationen gewinnen“, betont Michael Hagedorn, Vorstand Public Sector der Materna-Gruppe, im Interview mit dem Hardthöhenkurier.

Mobile Kommunikation und mobiles Arbeiten erfordern eine homogene gesicherte Umgebung, erklärt Michael Hagedorn.

Sehr geehrter Herr Hagedorn, mobile, sichere Kommunikation wird immer wichtiger. Wie lässt sich maximale Sicherheit der Daten bei gleichzeitiger Wahrung der digitalen Souveränität erreichen?
Auch wenn wir über maximale Sicherheit sprechen, ist eine hundertprozentige Sicherheit nicht erreichbar. Man kann sich ihr nur annähern. Hierbei unterstützen wir unsere Kunden.
Als Materna-Gruppe haben wir in den vergangenen Monaten intensiv in unser Portfolio und in Technologien investiert, um die Sicherheit für unsere Kunden erfolgreich und nachhaltig zu verbessern. Hierbei unterscheiden wir zwischen Daten, die eine Organisation im eigenen Rechenzentrum vorhält, und Daten, die mobil erzeugt werden und auf die mobil zugegriffen werden muss.

Die durch Cyberangriffe entstandenen Schäden haben sich in den Jahren 2018 bis 2021 auf mehr als 200 Milliarden in der deutschen Wirtschaft verdoppelt. Das ist auch ein Indikator dafür, dass es diverse Lücken gibt und das Sicherheitsniveau dahingehend nicht überall so ist, wie es eigentlich sein müsste. Auch gibt es enorm viele unterschiedliche Angriffsformate, auf die sich Organisationen einstellen müssen. Entsprechend ist unser Cyber Security Portfolio sehr breit aufgestellt.

Das gilt ja sowohl für die öffentliche Verwaltung als auch für die Bundeswehr, die ja eigentlich dafür viel sensibler sein sollte.
Wirtschaftsunternehmen werden zumeist zu Angriffszielen, um etwas zu erpressen z. B. durch Datenverschlüsselung. Attacken auf öffentliche Stellen, wie etwa die Bundeswehr, sehen sich zusätzlich anderen Gegnern gegenüber, die viel investieren, um z. B. an vorhandene Datenschätze zu gelangen. Dagegen müssen sich Organisationen umfassend aufstellen. Die wichtigsten Bausteine sind nicht nur Infrastrukturkomponenten, wie Firewalls und ähnliches, die es schon seit Jahrzehnten gibt, sondern die Einführung eines Security Operations Centers (SOC), das schrittweise auf- und ausgebaut werden sollte. Hier helfen digitale Agenten, die Auffälligkeiten identifizieren, um dann sehr schnell die Einsatzkräfte zu alarmieren. Materna liefert Expertenwissen für die schnelle Erkennung, Analyse und Bearbeitung in Echtzeit sowie Prävention von Sicherheitsvorfällen.

Was kennzeichnet ein Security Operations Center?
Entscheidend bei einem SOC ist, wie weitreichend die Intelligenz dahinter ist. In den Anfängen haben sich Menschen die Logfiles angeschaut und analysiert. Heute setzen wir auf den Einsatz Künstlicher Intelligenz für die Automatisierung, um Auffälligkeiten schneller zu entdecken. Diese Intelligenz ist das Entscheidende, um Erkenntnisse aus Zusammenhängen zu gewinnen und nicht nur aus Einzelinformationen.

Da stellt sich die Frage des Vorsprungs …
Ideal wäre es, wenn die Abwehr immer einen Vorsprung hätte. Das ist in der Realität oft nicht der Fall. Für die Experten geht es immer darum, die Angriffsvektoren zu erkennen. Können wir diese nicht erkennen, sind sie schwerer in einem SOC abzufangen. Künftig werden wir lernende Systeme einsetzen, die dann auch neue Angriffsvektoren schneller identifizieren und abfangen können.

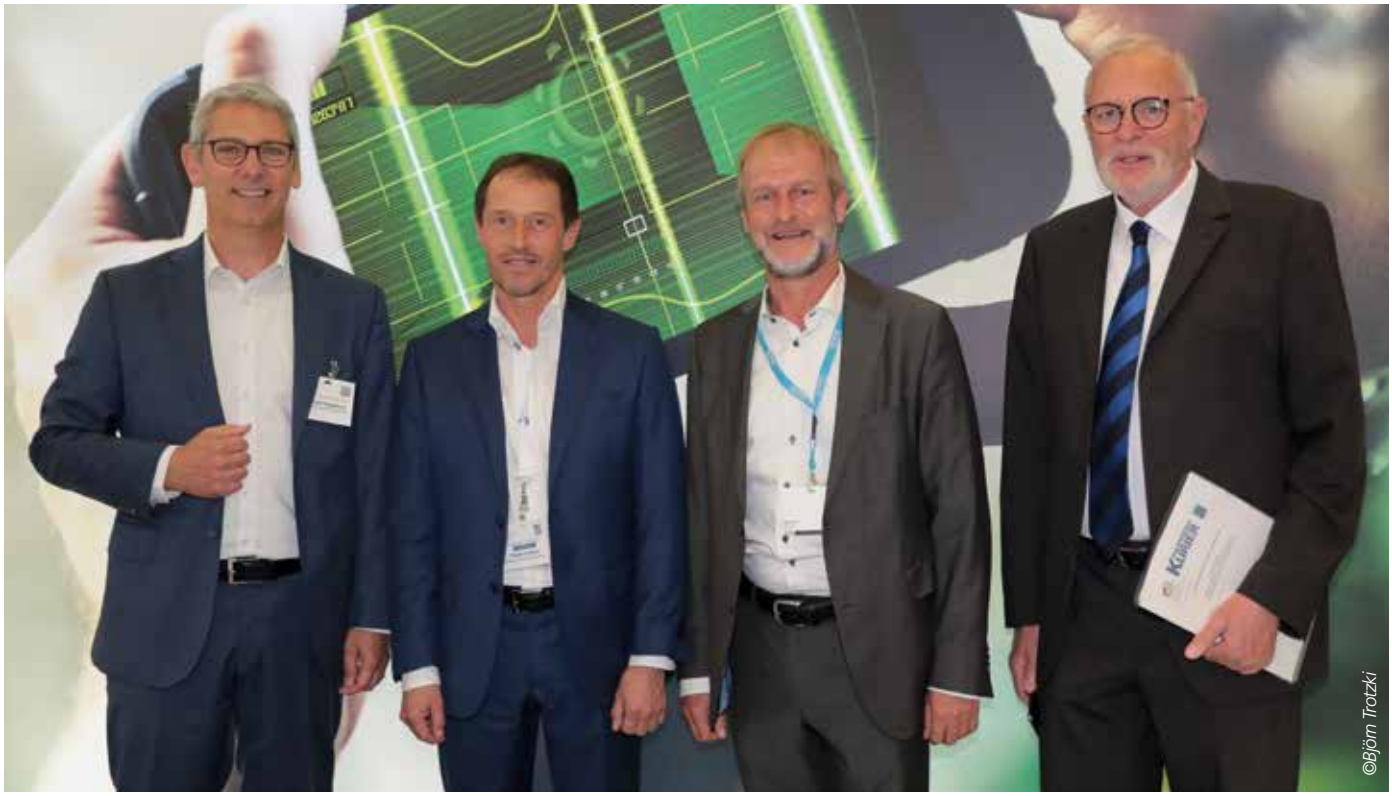
Und wie machen Sie das?
Das Entscheidende an einem SOC sind die intelligenten Erkennungs-Algorithmen. Da braucht es eine Menge Erfahrung, um bewerten zu können, welche Algorithmen für eine nahe hundertprozentige Sicherheit geeignet sind. Genau solche Lösungen bietet das österreichische Unternehmen RADAR Cyber Security, das wir im vergangenen Jahr akquiriert haben. Damit haben wir unsere Kapazitäten und Lieferfähigkeiten in diesem wichtigen Marktsegment der Cyber Security nachhaltig erweitert. Wir bieten den Aufbau von Security Operations Centern an und erbringen auch selbst die Leistungen eines eigenen SOC as a Service für unsere Kunden.

Welche Bedeutung hat Künstliche Intelligenz in diesem Zusammenhang?
KI wird in den nächsten Jahren immer mehr Einzug halten – sowohl aus sicherheitstechnischen Aspekten als auch als Folge des demografischen Wandels. Personalressourcen, die die Arbeit erledigen, werden immer knapper. Auf der anderen Seite sehen wir die Vernetzung von Prozessen. Routineaufgaben, um arbeitsfähig zu bleiben, die man zur Entlastung an eine Künstliche Intelligenz übertragen kann, werden zunehmen.
Ein dritter Bereich sind die Daten. Behörden, aber auch die Bundeswehr benötigen extrem viele und zeitkritische Daten. Das Sammeln von Daten und aufwendige Auswertelogiken gehören bald in die Vergangenheit. Werden Sensordaten in Echtzeit benötigt, um sofortige Erkenntnisse zu liefern, kommt Künstliche Intelligenz ins Spiel. Sie analysiert alle Datenquellen übergreifend und kann beispielsweise ein aktuelles, dynamisches und strategisches Lagebild generieren.

Kommen wir noch einmal zum Thema Mobile Kommunikation. Was bieten Sie da insbesondere auch unter dem Sicherheitsaspekt an?
Im Rahmen unserer Wachstumsstrategie haben wir im Februar 2022 das Unternehmen Virtual Solution gekauft, einen Spezialisten für sichere ultramobile Kommunikation. Wir können einen ultramobilen Arbeitsplatz anbieten, der VS-NfD und NATO Restricted gehärtet ist.
Mobile Kommunikation und mobiles Arbeiten umfassen eben nicht nur das eigene Office und Homeoffice, sondern findet praktisch von überall aus statt, egal wo ich mich gerade befinde. Und – speziell noch bei der Bundeswehr – auch in Einsatzszenarien. Auch und gerade dort muss Kommunikation abgesichert sein. Sie muss den mobilen Zugriff auf die aktuelle Datenlage gewährleisten und geht dabei weit über das Schreiben von E-Mails hinaus.
Kommunikationstechniken, Fachverfahren, Apps von Drittanbietern: All das muss in einer homogenen gesicherten Umgebung zusammengeführt werden. Dies ist ein Trend, auf den wir uns eingestellt haben, weil viele Behörden und auch die Bundeswehr dies zum Einsatz bringen.

Sehr geehrter Herr Hagedorn, vielen Dank für die interessanten Einblicke und zukunftsweisenden Informationen!

Video-Interview mit Michael Hagedorn



Michael Hagedorn (v.li.) mit Frank Grotheer, Sales Director Defense im Ressort Public Sector, Johannes Rosenboom, Senior Vice President Sales, BDM und Marketing im Ressort Public Sector, und Burghard Lindhorst, Hardthöhenkurier, auf dem Stand der Materna-Gruppe bei der AFCEA Fachausstellung 2023.

AFCEA Bonn e.V.

Adva
NETWORK SECURITY

Kontakt:
Adva Network Security
Justus-von-Liebig Str. 7
12489 Berlin
www.advasecurity.com
E-Mail: info@advasecurity.com

Adva Network Security hat sich auf den Schutz von Datennetzen mit hohem Sicherheitsbedarf spezialisiert. Unsere cyberresiliente Netztechnik unterstützt die digitale Transformation bei Verteidigung, Behörden und kritischen Infrastrukturen. Die ConnectGuard™ Sicherheitstechnik schützt unsere optischen Übertragungssysteme und Ethernet-Datengeräte schon heute vor zukünftigen Angriffen durch Quantencomputer. Mit Krypto-Agilität und virtualisierten Netzfunktionen können unsere Kunden schnell auf Veränderungen in der Bedrohungslage reagieren. Adva Network Security bietet zukunftsfähige Sicherheit mit BSI-zugelassener Verschlüsselungstechnik und einem umfassenden Angebot an Dienstleistungen für einen robusten und sicheren Netzbetrieb.

www.ndsatcom.com

Making Missions Possible

ND SAT COM

INSTALLING RELIABILITY

ZEITENWENDE
DIE NEUE DIMENSION DER TAKTISCHEN UND STRATEGISCHEN SATELLITENKOMMUNIKATION

©Björn Trotzki

©Björn Trotzki

©Björn Trotzki


©Lindhorst

©Björn Trotzki

Computacenter

Kontakt:
Computacenter
Christina Wiedergrün
Kokkolastraße 1
D-40882 Ratingen
Tel: +49 2102 169-1358
christina.wiedergruen@
computacenter.com
www.computacenter.com

Ging man über die diesjährige AFCEA Fachausstellung, konnte man die angeregte Stimmung fast schon greifen. Das Thema „(Künstliche) Intelligenz & Innovationen – Konkrete Nutzungsmöglichkeiten" lockte einen großen Strom an Besucher:innen trotz durchwachsenem Wetter auf die Messestände. Getreu diesem Thema fokussierte sich der Computacenter-„Container" auf die Bereiche *Verlegefähiges Rechenzentrum, Verlegefähige KI und Hochsichere IT-Logistik*. Gemeinsam mit den Partnern NVIDIA, Splunk und NetApp wurde Interessierten aufgezeigt, wie die Herausforderungen zu diesen Punkten u. a. durch den Rapid Datacenter Deployment Service von Computacenter (verpackungsfreie Anlieferung von getesteten und konfigurierten Komponenten) jetzt schon gemeistert werden können. Nach zwei sehr intensiven und produktiven Tagen ist die Vorfreude schon groß auf die nächste AFCEA Fachausstellung.

DATAGROUP

Kontakt:
DATAGROUP Defense IT Services
Ein Geschäftsbereich der DATAGROUP
Business Solutions GmbH
Andreas Wiewel
Direktor Vertrieb
Auf den Tongruben 3 | 53721 Siegburg
T +49 2241 904223
M +49 160 98673066
Andreas.Wiewel@datagroup.de
https://www.datagroup.de

DATAGROUP *Defense IT Services* bietet einen modularen und skalierbaren IT Managed Services Betrieb an. Dies beinhaltet flexible und hybride Liefermodelle „as-a-Service", sowohl in VS-NfD-Umgebungen als auch in Mischsystemen aus regulären Netzen und VS-NfD-Umgebungen. Durch unsere Expertise als deutscher Rechenzentrumsbetreiber erfüllen alle Bereiche höchste Sicherheitsstandards. Zertifizierte und sicherheitsüberprüfte Spezialisten unterstützen bei komplexen Migrations- und Transformationsprojekten, um einen sicheren und effizienten Betrieb zu gewährleisten und verhelfen Ihrem Unternehmen zu einer optimierten und hochmodernen IT. Alle Services sind auditiert und zertifiziert (ISO27001, ISO 20000, ISO 9001ff). Unsere branchenspezifischen Lösungen in den Bereichen DefenseCloud, Integrated Logistic Support (ILS), VPN/Netzwerk und Mobile Micro Datacenter haben eines gemeinsam:
Sie sind ***managed, secure*** und ***VS-NfD-konform***.

Aussteller bei der AFCEA Fachausstellung 2023

Quelle: AFCEA Bonn e. V.


RBUS
BWI
IT für Deutschland
secunet
griffity
defense
Bittium
BDSV
Bundesverband der Deutschen Sicherheits- und Verteidigungsindustrie e.V.
FUJITSU
T
rola.
CONET
CGI
AXSOL
infodas
connect more. be secure.
L3HARRIS
FAST. FORWARD.
TASSTA
Fraunhofer
IOSB
exail
MOSOLF
Imtradex
CODAN
DTC
FFG
Panasonic
CONNECT
TOUGHBOOK
Data-Warehouse GmbH
JK DEFENCE & SECURITY
Viasat
Hagenuk Marinekommunikation
ROLATUBE
ULTRALIFE
MATERNA
Virtual Solution
s|three
RADAR
CYBER SECURITY
proMegis
BACKBONE
GALVION
COMTECH
CeoTronics
bmc
Run and Reinvent
LEONARDO
software AG
THALES
Building a future we can all trust
OPITZ CONSULTING
EIZO
DELL Technologies
SELECTRIC
iesy
respons
DETECON
CONSULTING
psc_
TRANSITION
Capgemini
]pexip[
BAKO
Systemintegration
PLATH Group
THERMO
sopra steria
IABG
Computacenter
.INNO
PLATH
CHORA
CPI
vertex
GBS
PLATH
SIGNAL
PRODUCTS
NVIDIA
NetApp
bitrecords
splunk>
ND SAT COM
PROCITEC
DIAMOND
the fiber meeting
SK | serpikom
<CONDOK>
Deloitte.
Hirt
RITTAL
MOTOROLA
SOLUTIONS
CISCO
CYBERARK
DATAGROUP
EPIK
knapp
SATCUBE
HENSOLDT
Detect and Protect
KPMG
conpal
STARTUPS
PLANETFALL
PREVENCY
Immersive Simulations
KENBUN
traversals
MOTIONMINERS
DATA MACHINE INTELLIGENCE SOLUTIONS
VISENSE
XignSys
ENGINSIGHT
scalue
ALEPH ALPHA
TICK
langlauf
Inhubber
nynex
SATELLITE
PELI
HARDIGG CASES
avs
SANS
DVT
LACHEN helfen e.V.
GSP
Gesellschaft für Sicherheitspolitik e.V.
SPACE
Forschungszentrum Space
Universität der Bundeswehr München
neosat
SVS
Soldaten und Veteranen Stiftung
WIR SIND DIE RESERVE
VERBAND DER RESERVISTEN DER DEUTSCHEN BUNDESWEHR e.V.
DHL
GLOBAL EVENT LOGISTICS

Mobile Führungsfähigkeit – domänenübergreifend vernetzt!

Interview mit Dr. Daniel P. Westhoff, Leiter Division Land und Mitglied der Geschäftsleitung der ESG Elektroniksystem- und Logistik-GmbH, anlässlich der AFCEA Fachausstellung 2023

Engagierte Diskussion: Daniel Westhoff im Interview mit Burghard Lindhorst.

Sehr geehrter Herr Westhoff, mobile Führungsfähigkeit steht im Fokus der ESG auf der diesjährigen AFCEA Fachausstellung. Wie stellt sich die ESG insgesamt und Ihre Division Land im Besonderen auf, um die damit verbundenen Herausforderungen erfolgreich zu meistern?
Mobile Führungsfähigkeit muss immer im Kontext der Multi-Domain Operations betrachtet werden. Für die ESG kein neues Feld. Seit Jahrzehnten vernetzen wir Systeme auf dem Gefechtsfeld und generieren daraus den militärischen Mehrwert. Nichtsdestotrotz ist dieser Aspekt mit dem Thema Cloud in den letzten Jahren sehr stark im Fokus. Dies vor dem Hintergrund der Entwicklung neuer Waffensysteme, die jedes für sich einen hohen Grad an Spezialisierung aufweisen. Umso wichtiger, dass auf dem modernen Gefechtsfeld eine domänenübergreifende Vernetzung erfolgt, um die Effektivität der Gesamtsysteme in einem verbundenen Ansatz bestens nutzen zu können. Die ESG ist in allen Domänen aktiv und beitragsfähig.

Welche Lösungen bietet die ESG für die mobile Führungsfähigkeit?
Insbesondere das Heer hat einen hohen Bedarf an mobilen Gefechtsständen. Wir können hier auf jahrzehntelange Erfahrung aufbauen und setzen moderne Technologien ein, um die unterschiedlichsten Bedarfe zu decken. Der erste Ansatz dazu war schon in den achtziger Jahren mit dem Rechnerverbundsystem ADLER (Artillerie-, Daten-, Lage- und Einsatz-Rechnerverbund) und der damit verbundenen Digitalisierung von Gefechtsständen.
Hinzu kommt viel Erfahrung aus der erfolgreichen Realisierung unterschiedlicher Varianten von containerbasierten Gefechtsständen für die Luftwaffe – seit weit mehr als 15 Jahren. Wir bieten vielfältige Möglichkeiten an, wie etwa mit dem System NEOS (Network Enabled Operations Support): Es kann grundsätzlich in jede Plattform eingerüstet werden und ermöglicht die Vernetzung z. B. von fliegenden Waffensystemen untereinander oder mit schwimmenden Einheiten weit über die Ansätze, die wir heute haben wie etwa mittels Link 16. So kann zum Beispiel die Sensorik einer Plattform für die Wirkung eines anderen Waffensystems genutzt werden, die nicht selbst über die entsprechende Sensorik verfügt.
Und das alles auch unter dem Aspekt der Nachhaltigkeit. Ein Beispiel: Im Rahmen der Entwicklung eines neuen Konzeptes für flexible, energieeffiziente und modulare Heeresgefechtsstände mit Smart-Shelter-Technologie nutzen wir die „New Prime Power Unit", ursprünglich für das Counter Battery Radar COBRA entwickelt. Lastabhängig wird die Drehzahl reduziert und damit der Verbrauch um bis zu 50 Prozent gesenkt, und dies bei insgesamt bis zu 30 Prozent mehr an Leistung als andere klassische Stromerzeuger. Das erleichtert die gesamte Versorgung, da der logistische Footprint deutlich reduziert wird. Im Ukrainekrieg sehen wir ja die Bedeutung des Nachschubes. Und es ist als sehr positiver Nebeneffekt auch unter Umweltaspekten ein deutlicher Fortschritt.

Sie sprechen den Ukrainekrieg an. Welche Lehren oder Schlussfolgerungen lassen sich für die Bundeswehr und ihre Verbündeten bereits jetzt ziehen?
Erste Lehren haben wir auf der politischen Ebene gesehen mit der Rede des Bundeskanzlers zur „Zeiten-

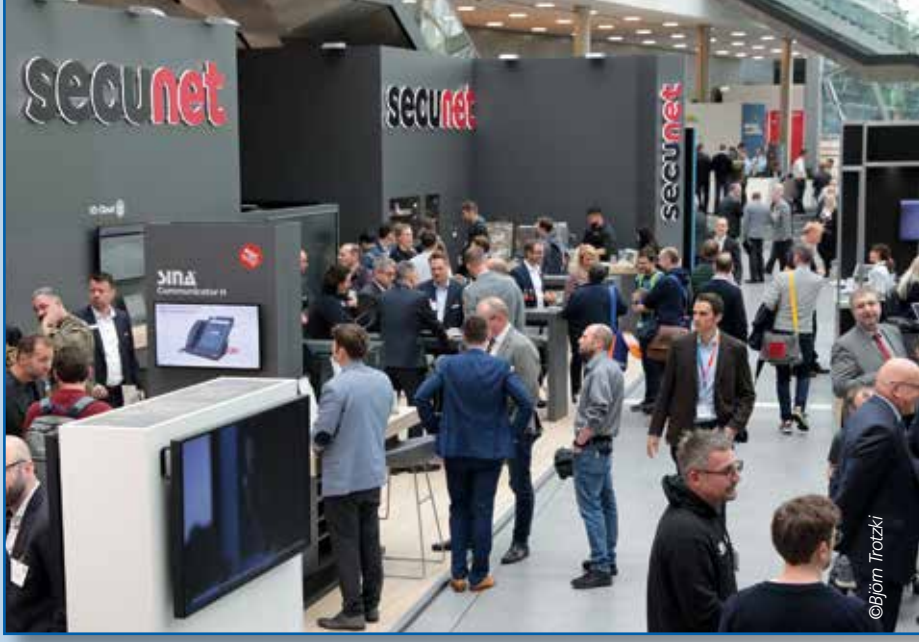
wende“ und der Einrichtung des Sondervermögens für die Bundeswehr. Militärisch konzeptionell ist die Verschiebung des Schwerpunktes vom internationalen Krisenmanagement zur Landes- und Bündnisverteidigung erfolgt; jetzt müssen diese Konzepte aber auch in der Realität ankommen. Es lassen sich schon jetzt eine Reihe von Lehren und Erfahrungen aus dem aktuellen Geschehen ziehen, insbesondere wenn wir, was wir hier auf der AFCEA auch zeigen, in Richtung der Gefechtsstände schauen. Im Bereich internationalen Krisenmanagements ging es sehr stark darum, vor allem leicht verlegbare Gefechtsstände zu haben, um diese z. B. per Lufttransport in internationale Krisenregionen verlegen zu können. Da spielte die Zeit für den Auf- und Abbau eine nachgeordnete Rolle und auch die Größe dieser Gefechtsstände war eher mit größeren Ausmaßen verbunden. Jetzt aber brauchen wir hochmobile Systeme in Containern wie auch in Fahrzeugen, miteinander auf dem Gefechtsfeld vernetzt und auf die jeweilige Führungsebene abgestimmt skalierbar. Zukünftige Gefechtsstände müssen schnell operabel sein können, ihre Arbeit verrichten und ebenso schnell wieder verlegen können, um nicht aufklärbar und verwundbar zu sein.
Der Blick in die Ukraine zeigt, dass wir wieder sehr stark im klassischen Gefechtsfeld unterwegs sein werden, allerdings auf andere Weise als in den achtziger Jahren, nämlich verbunden mit Digitalisierung und smarten Ansätzen. Ein Beispiel ist die aus den Medienberichten bekannte GIS ARTA App, mit der in der Ukraine auf recht simple Weise selbst das handelsübliche Smartphone Zieldaten generiert und die Feuerleitung leisten kann. Ich bewundere, wie die Ukraine das in die Gefechtsführung integriert hat, mit einfachen Mitteln. Aber trotzdem kann das für unsere Streitkräfte nicht der Ansatz sein, weil diese Systeme unglaublich verwundbar sind, schnell aufklärbar und leicht für einen Gegner kompromittierbar. Unter den Kriterien von z. B. Informationssicherheit ist dies kein gangbarer Ansatz für die Bundeswehr. Nichtsdestotrotz zeigt es aber, wohin der Weg geht. Wir müssen ähnliche Vorgehensweisen jedoch unter ganz anderen Kriterien der Informationssicherheit, der Integrierbarkeit und Interoperabilität mit unseren Partnern entwickeln und betreiben können.

Im Ukrainekrieg spielen Drohnen eine bedeutende Rolle …
Ja, sie sind allgegenwärtig, sowohl was die Aufklärung als auch die Wirkung angeht, selbst durch kleine, handelsübliche Drohnen. Die Bundeswehr sollte ein großes Augenmerk darauf legen, wie diese Bedrohung abgewehrt werden kann. Wir haben schon Systeme für die Bundeswehr in den Einsatz gebracht. Sie sind felderprobt, können Drohnen in unterschiedlich skalierbaren Ansätzen bekämpfen, von portablen über mobile Lösungen bis hin zu fest in Infrastruktur installierten Komponenten. Als Systemintegrator bündeln wir die einsatzspezifisch sinnvollen Fähigkeiten unterschiedlicher Typen von Sensorik und Effektorik über unser Führungssystem ELYSION in modularen, skalierbaren C-UAS-Systemen und haben zudem bereits beachtliche Erfolge dabei erzielt, C-UAS-Fähigkeiten auch in Bewegung von Verbänden („on the move“) darzustellen.
Und das nicht nur auf dem Gefechtsfeld. Es geht ganz besonders auch um den Schutz von besonders einsatzrelevanten militärischen Einrichtungen und von KRITIS (kritischer Infrastruktur) sowie von Regierungseinrichtungen. Das muss verstärkt in den Fokus geraten.
Die Konzepte der ESG im Rahmen der bodengebundenen Luftverteidigung reichen bis hin zur Abwehr von ballistischen Bedrohungen. Gerade auch aus dem Ausland beschaffte Systeme müssen in unsere nationalen Führungssysteme und -strukturen sicher integriert, mit ihnen vernetzt werden. Hier stellen wir gerne unsere Kompetenz zur Verfügung.

Stichwort „Landes- und Bündnisverteidigung“: Wo sehen Sie den größten Handlungsbedarf im Zusammenspiel von öffentlichem Auftraggeber und der deutschen Sicherheits- und Verteidigungsindustrie?
Sicherheit heißt auch Handlungs- und vor allem Planungssicherheit, um in zukünftige Ansätze, die sehr kapitalintensiv sind, überhaupt investieren zu können. Ein Beispiel, was auch viele mittlere und kleinere Firmen trifft: die Erweiterung von Flächen für Produktionsstätten. Da benötigen Sie Kapital, das im wehrtechnischen Umfeld deutlich schwerer zu bekommen ist, als wenn es sich um rein „zivile“ Aktivitäten handeln würde. Bei der Infrastruktur z. B. sind benötigte Flächen oft in Infrastrukturfonds gebunden, die sich in ihren Statuten den strengen, undifferenzierten Nachhaltigkeitskriterien der EU unterworfen haben, wodurch wehrtechnische Unternehmen per se auf Ablehnung stoßen. Ist das in der „Zeitenwende“ konsequent und nachhaltig zu Ende gedacht?
Die „Zeitenwende“ mit dem Sondervermögen ist ein guter Ansatz, aber letztlich auch nur ein erster Schritt in die richtige Richtung. Es muss umfassend und langfristig weitergedacht werden. So müssen beispielsweise die neuen Systeme auch langfristig versorgbar sein. Da werden wir über wesentlich höhere Budgets reden müssen.
Das andere sind die politischen Rahmenbedingungen in Deutschland und Europa. Die angesprochenen sogenannten „Nachhaltigkeitskriterien“ können die wehrtechnische Industrie massiv behindern. Unsere Branche wird auf europäischer Ebene gleichgesetzt mit u. a. Glücksspiel, Tabak etc. So kann es nicht funktionieren. Ich unterstreiche ausdrücklich die Aussage des Bundesverbandes der Deutschen Sicherheits- und Verteidigungsindustrie e.V.: „Sicherheit ist die Mutter aller Nachhaltigkeit.“ Die derzeitigen Regelungsabsichten stehen der Lösung der tatsächlichen gesamtgesellschaftlichen Herausforderungen entgegen.
Die politischen Rahmenbedingungen müssen so gestaltet werden, dass Streitkräfte und die wehrtechnische Industrie Hand in Hand gehen können und die Industrie die Möglichkeit bekommt, nachhaltig in Wachstum zu investieren. Nur so können die nachgewiesenen Bedarfe der Streitkräfte zur Erfüllung ihres verfassungsmäßigen Auftrags gedeckt und unser aller Sicherheit, Freiheit und Wohlstand nachhaltig gesichert werden.

Sehr geehrter Herr Westhoff, vielen Dank für die interessanten Informationen!

AFCEA Bonn e.V.



©Björn Trotzki

©Björn Trotzki


©Björn Trotzki

©Björn Trotzki

©Björn Trotzki

Kontakt:
FREQUENTIS Deutschland GmbH
Geschäftsbereich
Defence Deutschland
Graurheindorferstr. 159
53117 Bonn, Deutschland
Tel: +49 6103 30 08 60
www.frequentis.com
defence-deutschland@frequentis.com

FREQUENTIS ist seit mehr als 75 Jahren ein zuverlässiger Lieferant von sicherheitsrelevanten Lösungen in den Geschäftsbereichen Air Traffic Management, Public Safety, Public Transport, Maritim und Defence. Anlässlich der AFCEA 2023 präsentierten wir die Themen Sichere Kommunikation über alle Domains hinweg, Remote Digital Tower (RDT) und Unmanned Traffic Management (UTM) als ganzheitliche, innovative Konzepte für die Gefechtsstände sowie die Lage- und Führungszentren der Bundeswehr und anderer internationaler Streitkräfte. Auch im Bereich C-UAS zeigten wir unsere Lösungen (Incident Management System, Middleware MosaiX) für den effektiven Einsatz von Maßnahmen gegen Drohnen für alle Teilstreitkräfte zum Schutz von Infrastrukturen und den Soldaten.
Die **FREQUENTIS** ist seit über 30 Jahren als Systemhaus ein starker Partner der Bundeswehr und verbündeter Streitkräfte und bietet innovative, kundenangepasste und progressive Lösungen. Mit diesen leisten wir einen relevanten Beitrag zur Steigerung der Sicherheit und Sicherstellung der Lufthoheit.

Kontakt:
iesy GmbH
Darmcher Grund 22
58540 Meinerzhagen
Tel.: +49 (0)2354 706 55 - 0
E-Mail: sales@iesy.com
www.iesy.com

Bei der **iesy GmbH** handelt es sich um einen Anbieter für komplexe kundenspezifische Embedded Systemlösungen. Mit Leidenschaft für Technik und einem eingespielten Team in den Bereichen Hardware- & Softwareentwicklung, Materialbeschaffung, Fertigung und Geräteprüfung sind wir seit 1966 der ideale OEM- und Outsourcing-Partner zur Entwicklung und Produktion individueller Embedded Produkte. Das Unternehmen mit Sitz im nordrhein-westfälischen Meinerzhagen orientiert sich stets an den Bedürfnissen seiner Kunden unterschiedlichster Märkte und entwickelt, prüft und zertifiziert das finale Produkt bzw. begleitet bis zur finalen Zertifizierung.
Im Bereich Verteidigung bieten wir sichere und robuste Computerlösungen, welche sich an den rauen Umgebungen als auch die hohen Sicherheitsanforderungen orientieren.

©Björn Trotzki

©Björn Trotzki


©Björn Trotzki


©Björn Trotzki

Kontakt:
Bechtle AG
Zentrales Team Bundeswehr
Bechtle Platz 1
74172 Neckarsulm
www.bechtle.com
E-Mail: zpls-r1112@bechtle.com
Tel: 0228 6888 400

Bechtle ist Deutschlands größtes IT-Systemhaus und starker Partner für zukunftsfähige IT-Architekturen sowie IT-E-Commerce. Für Bechtle arbeiten derzeit mehr als 14.000 Mitarbeitende in 14 Ländern. Durch ein flächendeckendes Netz von 85 lokalen IT-Systemhäusern ist Bechtle stets nahe am Auftraggeber. Gemeinsam mit den Herstellerpartnern Dell/EMC, VMware, Sonatype und go-smart zeigte Bechtle ein eindrucksvolles Portfolio an Produkten und Leistungen aus den Bereichen Rechenzentrumsausstattung im Datacenter, Virtualisierung sowie Open Source Softwareengineering.
Ebenfalls im Fokus der AFCEA Fachausstellung standen auf dem Bechtle Messestand Themen aus den Bereichen der Informationssicherheit, verlegefähigen Rechenzentren, skalierbare 5G Funklösungen, Teilekennzeichnung von Geräten und Verpackungen bis hin zu Künstlicher Intelligenz.
Bechtle ist somit verlässlicher, langjähriger Begleiter der Bundeswehr, BWI, NATO und Sicherheitsbehörden auf deren Weg der Digitalisierung.

Warum SecuSUITE for Samsung Knox?

Lauschangriffe, Spionage, Datenklau. Es gibt viele gute Gründe, warum Regierungen, Behörden und Unternehmen weltweit auf die mobilen Hochsicherheitslösungen von Secusmart vertrauen.

Ob am Arbeitsplatz, auf Reisen oder im Home-Office: **SecuSUITE for Samsung Knox** schützt Daten, Telefonie, Apps – und ist die einzige Smartphone- und Tablet-basierte Lösung, die eine VS-NfD-sichere virtuelle Desktop-Infrastruktur (VDI) bietet.

Vertrauen auch Sie auf Secusmart. Für sicheres ultramobiles Arbeiten mit Smartphone, Tablet & Co.

Sichere Daten, Telefonie und Apps bis zur Geheimhaltungsstufe VS-NfD

Sicheres ultramobiles Arbeiten im Home-Office und Trennung von privaten und dienstlichen Apps

Aktuellste Tablets und Smartphones mit Samsung Knox

www.secusmart.com

BlackBerry® | secusmart®

Führen und Kommunizieren mit den Systemlösungen der ATM

Die sicherheitspolitische Lage erfordert das unmittelbare Bereitstellen von Informationen und das reibungslose Zusammenwirken unterschiedlicher Akteure und Teilstreitkräfte. Der Faktor Kommunikation und die schnelle Verfügbarkeit von Information nehmen aufgrund geringer Latenzzeiten im Geschehen eine Schlüsselrolle ein. Nur der streitkräftegemeinsame und interoperable Informations- und Kommunikationsverbund und die durch ihn erlangte Informationsüberlegenheit machen die Feuerkraft der verbundenen Truppenteile zum Erfolg. Hierzu braucht es einen den gegenwärtigen und künftigen Herausforderungen angepassten Kommunikations-Backbone und taktischen Router.

Die ATM KommServer sind in verschiedenen Bauformen in der Bundeswehr in Betrieb, u. a. als COMSEC oder Manpack-Variante.

Zentrales Gateway für die Kommunikation
Zentrales Element der Digitalisierung des Gefechtsfeldes ist der ATM Kommunikationsserver (in Betrieb als KommServer). Er ist mit hoher Stückzahl Bestandteil der Standardausrüstung der Heeresfahrzeuge und bewies sich im Einsatz. Als zentraler Kommunikations-Gateway stellt der KommServer das Bindeglied zwischen den verschiedenen Führungsanwendungen und dem gewachsenen, heterogenen Pool der im Heer und bei anderen Teilstreitkräften genutzten Führungsmittel dar. Gerade in Zeiten, in denen sich die Einsatzszenarien ständig ändern, sorgt das KommServer-System für einen durchgängigen, medienbruchfreien Informations- und Kommunikationsverbund von der Division bis zum einzelnen Soldaten.

Das System KommServer
Das aus KommServer-Hardware und ATM-Kommunikationssoftware bestehende KommServer-System zeichnet sich durch passgenaue Lösungen für die Problemstellungen der militärischen Kommunikation im Feld aus: Eine tiefe Integration von Sprachdiensten erlaubt das gleichzeitige, aber voneinander unabhängige Übertragen von Sprache und Daten sowohl vollständig digitalisiert als auch über vorhandene analoge Schnittstellen der zur Verfügung stehenden Übertragungsmittel. Die Implementierung eines dynamischen, situativ angepassten Routings und der Einsatz von Quality Of Service garantieren die optimale Nutzung der unterschiedlichen heterogenen Übertragungswege. Dabei kommen speziell auf die militärischen Bedürfnisse abgestimmte Kommunikations-Stacks und bewährte Standard-Routingprotokolle zum Einsatz. Über adaptive Verfahren realisiert das KommServer-System bei Bedarf eine automatische und dynamische Neuberechnung der Kommunikationswege und passt sich so der Dynamik des Netzes an. Es erkennt Fehler und gewährleistet das Übertragen von Informationen zum Empfänger – sogar nach einer Unterbrechung oder wenn Sender und Empfänger unterschiedliche Übertragungsmittel nutzen.

Passgenaue Lösungen für die taktische Kommunikation
Auf dieser Basis realisiert ATM kundenspezifische Kommunikationslösungen in Soft- und Hardware, die maximal die militärischen Anforderungen treffen. Durch langjährige Erfahrung bei der Anbindung unterschiedlicher Kommunikationsmittel, das Umsetzen von passgenauen, heterogenen Kommunikationsnetzen sowie das Realisieren militärischer Kommunikationsanwendungen und -dienste ist ATM ein qualifizierter Partner für die Weiterentwicklung künftiger Kommunikationsanwendungen.

ATM ist der Spezialist für gehärtete IT-Lösungen
Die ATM ComputerSysteme GmbH steht für hochgehärtete Rechnertechnik für Aufklärungs-, Führungs- und Waffeneinsatzsysteme sowie Life-Cycle-Systemlösungen. Ferner gehören Displays, Panel-PCs, Switche und spezialisierte Bediengeräte sowie Lösungen für die funktionale Sicherheit zum Portfolio des Konstanzer Systemhauses. ATM bietet nationalen und internationalen Kunden seit Jahrzehnten standardisierte, aber auch hochindividualisierte Systemlösungen.

ATM Tec-Knowledge®

Kontakt:
ATM ComputerSysteme GmbH
Max-Stromeyer-Straße 116
78467 Konstanz
info@atm-computer.de
www.atm-computer.de

Den magentafarbenen Produkten einen olivgrünen Anstrich verpassen

Interview mit Sebastian Bumke, Account Manager Bundeswehr,
DEUTSCHE TELEKOM GESCHÄFTSKUNDEN GMBH

©Björn Trotzki

Sebastian Bumke stellte sich auf der AFCEA Fachausstellung den Fragen von Burghard Lindhorst.

Sehr geehrter Herr Bumke, was ist Ihre Aufgabe bei der Telekom?
Als Account Manager für die Bundeswehr übernehme ich die Vertriebsverantwortung für alle Teilstreitkräfte und Organisationsbereiche des Ressorts einschließlich der BWI und einen Teil der wehrtechnischen Industrie. In dieser Rolle repräsentiere ich unser Unternehmen als führenden Digitalisierungspartner unserer Kunden und Partner und baue eine Brücke zwischen Business, IT, Portfolio und verschiedenen Interessengruppen. Ich bin stolz darauf, diese wichtige Rolle zu erfüllen und freue mich darauf, weiterhin eng mit der Bundeswehr zusammenzuarbeiten, um gemeinsam innovative Lösungen zu entwickeln

Telekom: Das verbindet man zunächst mit reiner Telekommunikation. Aber was machen Sie darüber hinaus?
Aus der Historie und von Hause aus ist die Telekommunikation die Grundlage unseres Geschäfts und heute auch jedes Digitalisierungsvorhabens unserer Kunden.
Wir versorgen die Bundeswehr, unsere internationalen militärischen Kunden und deren Partner im In- und Ausland mit Telekommunikation – Sprache, Daten und Video im Fest- und Mobilnetz über terrestrische oder über Satelliten-Verbindungen.
Digitalisierung ist neben der Kommunikation aber vor allem auch IT und hier bieten wir integrierte und konvergente Lösungen an, bei denen IT und Kommunikation zusammengehören. Ein sehr gutes Beispiel dafür, wie wir unter Nutzung moderner Kommunikationstechnologien die Digitalisierung der Bundeswehr vorantreiben, ist unsere jüngst mit dem Logistikkommando der Bundeswehr durchgeführte Studie „5G für ortsfeste logistische Einrichtungen“. Hier wurden gerade im Themenfeld „Autonome Logistik“ große Potenziale identifiziert, die durch 5G überhaupt erst möglich werden können. Durch den Einsatz von Robotern kann die Steuerung, Durchführung und Organisation des Materialflusses (Intralogistik) innerhalb des Lagerbetriebes verbessert werden.
Wir sind seit gut 40 Jahren im maritimen Umfeld mit IT-Komponenten und digitalen Bordnetzen unterwegs. Einen weiteren Schwerpunkt haben wir in der Beratung und dem Support rund um Integrated Logistics Support (ILS) und Product Lifecycle Management (PLM). In diesem Bereich haben wir gemeinsam mit der Bundeswehr eine Extended-

Reality-Lösung entwickelt – die Fernunterstützung für Instandhaltungskräfte.
Das wichtige Thema Cybersicherheit bedienen wir mit Themen wie u. a. Security Operations Center (SOC) / Security Information and Event Management (SIEM), Cyber-Resilience und Simulation/Test mit einer eigenen Tochtergesellschaft, der Telekom Security. Die Sicherheitssparte ist enger Partner des Kommandos Cyber- und Informationsraum.
Darüber hinaus zählen Rechenzentrums-Leistungen zu unserem Kerngeschäft. Software- oder Multimedia-Services runden unser Portfolio ab.

Die Bundeswehr nutzt in vielen Bereichen zivile Lösungen. Was können Sie hier anbieten?
Neben schnellen, breitbandigen und sicheren Netzen bieten wir der Bundeswehr IT-Lösungen aus unseren zivilen Sektoren, beispielsweise im Gebiet der Logistik, Sanitätswesen oder Personalwesen. Wir nutzen unser Industrie- und Produkt-Know-how und „härten" dieses Portfolio, indem wir es an die Bedarfe und erhöhten Sicherheitsanforderungen anpassen. Man könnte sagen: Wir verpassen unseren magentafarbenen Telekom-Produkten einen olivgrünen Anstrich.

Digitale Souveränität ist ein zunehmend wichtiger Aspekt. Wie sieht der bei der Telekom aus?
Wir investieren stark in souveräne Cloud-Plattformen. Wir glauben, dass eine nachhaltige digitale Wertschöpfung nur mit Souveränität in Bezug auf Daten, Technologie und Betrieb erreicht werden kann.
Die Anforderungen an digitale Souveränität sind vielfältig und erfordern komplexe Antworten. Souveränität ist mehr als Datenschutz. Wir betrachten auch digitale Identitäten und die Data Governance als wichtige Aspekte. Data Governance beantwortet dabei die Fragen, wo Daten erzeugt werden und wo sie gespeichert sind, wer sie nutzen darf und wer die Verantwortung für die „Spielregeln" übernimmt. Nicht zuletzt ist anzumerken, dass Daten, die häufig auch als das Gold des digitalen Zeitalters bezeichnet werden, die Basis für leistungsstarke KI-Lösungen sind.

Was steht bei der AFCEA Fachausstellung für Sie im Mittelpunkt?
Die AFCEA Fachausstellung ist schon seit jeher die olivgrüne CeBit. Hier treffen sich die öffentlichen Auftraggeber aus der Bundeswehr und anderen Sicherheitsbehörden mit der Informations- und Telekommunikationsbranche zum Gedankenaustausch. Die Deutsche Telekom ist als Gründungsmitglied der AFCEA e.V. von Beginn an dabei.
Wir unterstützen mehrere aktuelle Projekte mit einem Auftritt auf der AFCEA Fachausstellung, haben die Möglichkeit, unser Portfolio vorzustellen und vor allem haben wir hier den Raum, um neue Ideen und Themen mit unseren Kunden und Partnern zu diskutieren.

Sehr geehrter Herr Bumke, vielen Dank für die interessanten Informationen!

Intensive Gespräche auf dem Stand der Telekom.

©Lindhorst


©Björn Trotzki


Red Hat
S-Cloud
©Lindhorst


©Björn Trotzki


Erleben,
©Lindhorst


GSP
SATCOM-AS-A-SERVICE
> Weltweite missionskritische Kommunikation
©Björn Trotzki

C4I-Software für die Digitalisierung der Bundeswehr

Die Digitalisierung der Streitkräfte schreitet voran und die Konsolidierung der Systemlandschaft im Bereich der Führungsinformationssysteme ist im vollen Gange. Die Implementierung des Mission Enabling Service Bundeswehr (MESBw) leistet dazu einen wesentlichen Beitrag.
Die Herausforderungen der Interoperabilität in multinationalen Einsätzen sowie der Intraoperabilität, also dem Zusammenwirken von unterschiedlichen Systemen innerhalb der Streitkräfte, stehen dabei weiterhin im Fokus der Aktivitäten. Die Landstreitkräfte haben mit der Digitalisierung landbasierter Operationen (D-LBO) eine Strategie entwickelt, um die Führungsfähigkeit in Landoperationen signifikant und nachhaltig zu verbessern. Fokussiert D-LBO auf die Dimension Land, so besteht auch in den anderen Dimensionen der Bedarf für eine Einführung oder Konsolidierung der Führungsinformationssysteme, um dem Gesamtziel, der Erstellung eines einheitlichen und organisationsbereichsübergreifenden Lagebilds, näherzukommen.

Systematic SitaWare Suite
Die Systematic SitaWare Suite stellt modulare und skalierbare IT-Services bereit, die als Lagedienst in stationären, verlegefähigen, mobilen und seegehenden Umgebungen eingesetzt werden können. Im Einzelnen sind dies SitaWare Headquarters für stationäre und verlegefähige Gefechtsstände sowie seegehende Plattformen, SitaWare Frontline für Gefechtsfahrzeuge und SitaWare Edge für den abgesessenen Führer.
Mit insgesamt mehr als 50 Nutzernationen ist SitaWare die meistverbreitete C4I-Software Suite weltweit. Die einzelnen Military-off-the-Shelf-Produkte (MOTS) sind vielfach einsatzerprobt und verfügen über einen sehr hohen Reifegrad. Im Bereich der Interoperabilität gilt SitaWare mittlerweile als Benchmark für die Entwicklungen anderer Nationen und setzt Standards für den Datenaustausch in multinationalen Operationen. Proprietäre Systeme, beispielweise Führungs- und Waffeneinsatzsysteme (FüWES) sowie Waffensystem-Plattformen, können risikoarm über vollständig dokumentierte und offene Schnittstellen angebunden oder integriert werden.
SitaWare unterstützt neben Landoperationen im gleichen Maße die Operationen in den Dimensionen Luft und See. Mit dem Maritime Add-on wurden Funktionalitäten für maritime Anwendungsfälle entwickelt und stehen zur sofortigen Nutzung bereit.

SitaWare @ Deutsche Bundeswehr
Die Bundeswehr hat SitaWare als Mission Enabling Service der Bundeswehr implementiert. Aktuell existiert der Service in den Ausprägungen Command Post, abgebildet durch SitaWare Headquarters, und Mountable, welcher unter Nutzung von SitaWare Frontline realisiert wurde. Damit stehen eine Vielzahl von querschnittlichen Funktionalitäten für Führungsinformationssysteme zur Verfügung, welche in der gesamten Bundeswehr genutzt werden können. Zusammen mit dem D-LBO Tactical Core bildet der MESBw eine Kommunikations- und Software-Plattform, die das Rückgrat der Digitalisierung abbildet. Für die Bundeswehr entsteht so die Möglichkeit, ein einheitliches Ökosystem für zukünftige Projekte auf- und auszubauen.


©Systematic

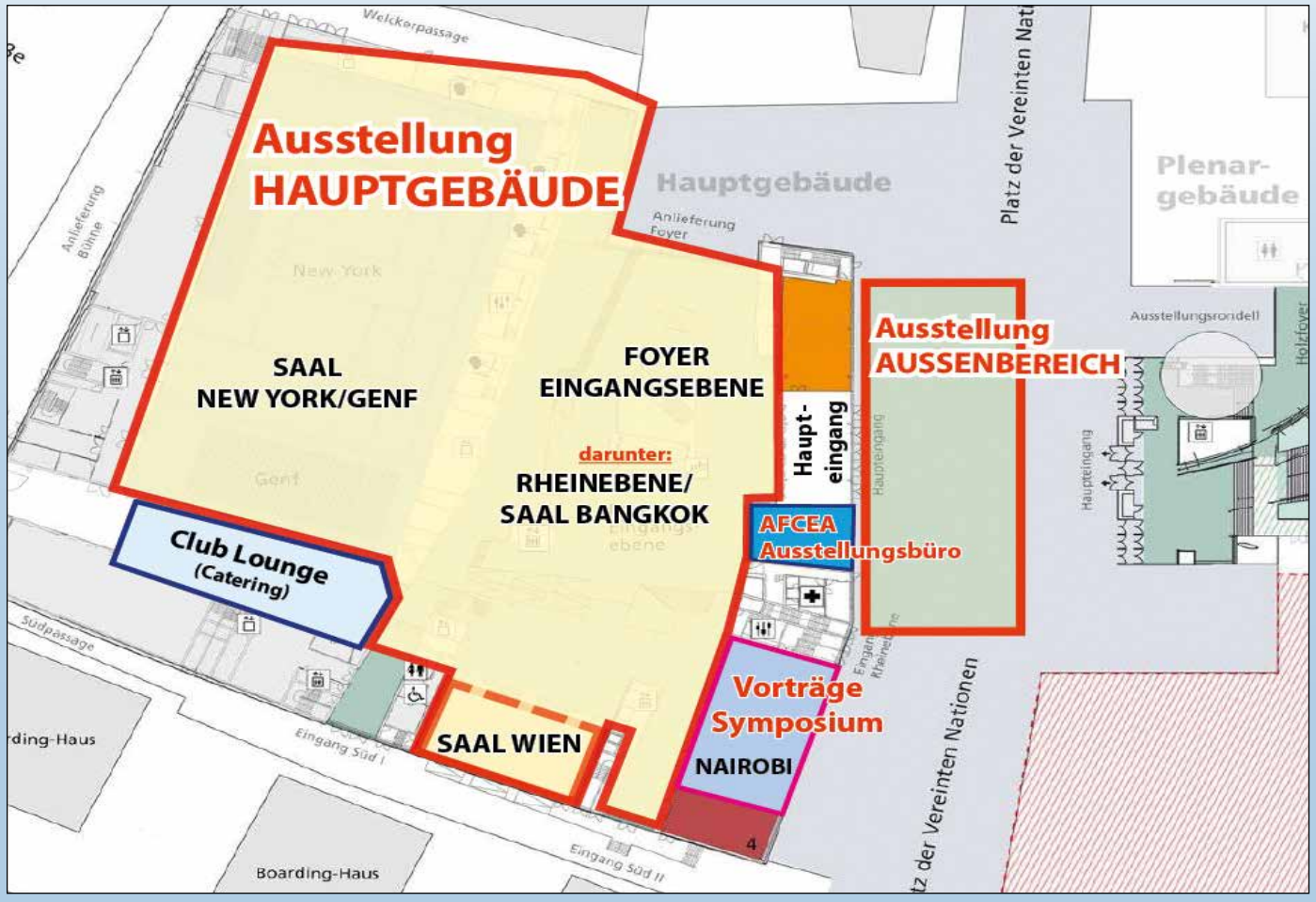
Das SitaWare Framework bietet zum einen querschnittliche Funktionalitäten für alle Organisationsbereiche und kann darüber hinaus um spezifische Module, beispielsweise durch das Maritime Add-on, erweitert werden.

Ausblick
Durch die kontinuierliche Weiterentwicklung der Produkte kommen fortlaufend neue oder verbesserte Funktionalitäten hinzu. Mittelfristig orientiert sich die Produktentwicklung an den Megatrends der IT und an der Weiterentwicklung der IT-Plattformen der Nutzernationen. Im Fokus stehen Themen wie Künstliche Intelligenz, Big Data und Cloud Computing. Spezifische Nutzergruppen, wie zum Bespiel das Militärische Nachrichtenwesen, werden im besonderen Maße von diesen Entwicklungen profitieren. Dazu wurde den Nutzernationen kürzlich das jüngste Produkt der SitaWare Suite, SitaWare Insight, vorgestellt und ist ab sofort marktverfügbar. Insgesamt bietet Systematic mit SitaWare viele Möglichkeiten, die Bundeswehr in den Herausforderungen der Digitalisierung zu unterstützen und die sich auftuenden Chancen zu nutzen.

SYSTEMATIC

Kontakt:
Systematic GmbH
Im Zollhafen 14
50678 Köln
Tel.: 0221 29294319
more.info.de@systematic.com
www.systematic.com

Ausstellungsflächen



Impressum

Sonderheft
AFCEA Fachausstellung 2023
ISSN 0933-3355

MITTLER REPORT

Verlag · Herausgeber
Mittler Report Verlag GmbH
Beethovenallee 21 · 53173 Bonn
Telefon: +49 (0) 228 / 25 90 03 44
E-Mail: info@hardthoehenkurier.de
Telefax: +49 (0) 228 / 35 00 871
www.hardthoehenkurier.de

Ein Unternehmen der Gruppe TAMM Media

Geschäftsführer
Peter Tamm

Verlagsleiter
Andreas Steinmetz
Telefon: +49 (0) 228 / 25 90 03 46
E-Mail: verlagsleitung@mittler-report.de

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

Redakteur Sonderheft: Burghard Lindhorst
Mobil: +49 (0) 171 / 28 17 474
E-Mail: lindhorst@mittler-report.de

Fotograf: Björn Trotzki

Marketing · Vertrieb · Social Media
Leiter: Achim Abele
Telefon: +49 (0) 228 / 25 900 347
Mobil: +49 (0) 176 / 84 00 85 28
E-Mail: a.abele@mittler-report.de

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

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

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

Annika Kordysch, Telefon: +49 (0) 228 / 35 00 883, E-Mail: a.kordysch@mittler-report.de

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

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

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

Druck
Lehmann Offsetdruck & Verlag GmbH
Gutenbergring 39 · 22848 Norderstedt

Offizieller Partner:

Die 37. AFCEA Fachausstellung findet am 26./27. Juni 2024 im World Conference Center Bonn statt

Das Format für die AFCEA Fachausstellung 2024 umfasst folgende traditionelle und neue Elemente:

- Ausstellung auf den fünf Ausstellungsflächen:
  FOYER EINGANGSBEREICH, SAAL WIEN, SAAL NEW YORK/GENF, RHEINEBENE, AUSSENBEREICH;
  2024 zusätzlich mit den Ausstellungsflächen SAAL NAIROBI und FOYER EINGANGSBEREICH,
- Ein Symposium mit zwei high-level Vorträgen und die #DigitalDefenseDebate live/Podiumsdiskussion, organisiert durch die Emerging Leaders AFCEA Bonn e.V. (ELA),
- zwei parallele Panels von kurzen Industrievorträgen plus Start-up Pitch Sessions,
- erstmalig steht der PLENARSAAL des ehemaligen Bundestages für die Symposiumsvorträge und die #Digital DefenseDebate sowie für die Industrievorträge des Speakercorners 1 zur Verfügung,
- ein Get-together am Mittwochabend von 18.00 – 22.00 Uhr auf der Ausstellungsfläche RHEINEBENE,
- eine Sonderausstellungsfläche für junge Start-ups,
- ein Recruitingelement, organisiert durch die Emerging Leaders AFCEA Bonn e.V. (ELA) in Kooperation mit dem Berufsförderungsdienst Köln,
- Liveberichterstattung von der AFCEA Fachausstellung durch die Emerging Leaders AFCEA Bonn e.V. (ELA).

Übergabegespräche: Friedrich W. Benz (li.) weist seinen Nachfolger Wolfgang Quirin bei einem Rundgang zu den Ausstellern ein.

Making of der Titelseite

Vielen Dank an unseren Fotografen Björn Trotzki für seine professionelle Arbeit!

Björn Trotzki

Hardthöhen-KURIER

FÜR EIN STARKES EUROPA

Das Team des Hardthöhenkurier bedankt sich bei den Organisatoren der AFCEA Bonn e.V. sowie den Ausstellern und Besuchern der Fachausstellung 2023 sehr herzlich für Ihre Unterstützung!

BWI
IT für Deutschland

Digitalisierung der Bundeswehr erleben!

Die BWI sorgt als **Innovationstreiber der Bundeswehr** für die digitale Zukunftsfähigkeit Deutschlands. Zusammen mit den Streitkräften entwickelt und erprobt sie innovative IT-Lösungen, die die **Effizienz und Einsatzfähigkeit** der Bundeswehr steigern können.

Mit dem **BWI Digital Showroom** haben diese Digitalisierungsprojekte jetzt eine neue Bühne: Erleben Sie in unserer virtuellen Ausstellung, welche **Potenziale unsere innovativen Lösungen** sowohl für die Bundeswehr als auch für andere staatliche Organisationen in Deutschland haben.

Jetzt den
BWI Digital Showroom
entdecken:

https://showroom.bwi.de/projekte

digitalinnovativ

KOMPLEXE EINSÄTZE.
Eine Kommunikationslösung.

Die CT-MultiPTT 3C mit CT-ComLink® Technologie.
Unser fortschrittlichstes Hightech-Produkt kann als interoperable Steuereinheit bis zu drei Kommunikationskreise gleichzeitig und unabhängig voneinander koordinieren.
Erfahren Sie jetzt mehr:

CT-ComLink® Technology

Seit über 35 Jahren entwickelt und produziert CeoTronics in Deutschland missionskritische Kommunikationssysteme für anspruchsvolle Einsatzbedingungen. Unsere Mission von Beginn an: Freiheit und Sicherheit verteidigen. Unsere Produkte: innovativ, flexibel und vielseitig, international im Einsatz.

Sprechen Sie direkt mit unseren Experten, um mehr über unsere Lösungen und zukunftssicheren Technologien zu erfahren:
+49 (6074) 8751-670

Foto: Rheinmetall AG

WHEN IT COUNTS

CeoTronics
Audio · Video · Data Communication