D 46892

MITTLER REPORT

WEHRTECHNISCHER REPORT

1/2020

Special:

Bundeswehr Cyber Innovation Hub

IT-Report+ 2020

Teilnehmer der Allianz für Cyber-Sicherheit

ATLAS Seeminen-Abwehrfähigkeit

Erfahrung prägt die Zukunft

Maritime Machtprojektion setzt eine schnelle und effektive Entfaltung von Wirkkräften von See her kommend an Land voraus. Der Einsatz von Seeminen kann eine Entfaltung dieser Wirkkräfte stark einschränken. Deswegen müssen moderne Seestreitkräfte in der Lage sein, sich dieser Bedrohung flexibel und nachhaltig zu stellen. Flexibilität wird im Besonderen durch den Einsatz unbemannter Fahrzeuge wie dem AUV (Autonomous Underwater Vehicle) oder dem USV (Unmanned Surface Vehicle) erreicht. Diese Systeme können sowohl von dedizierten Plattformen als sinnvolle Ergänzung als auch von modularen Fähigkeitsträgern aus eingesetzt werden. Sie spielen so ihre Vorteile in Bezug auf Effizienz aus und reduzieren zusätzlich die Gefahr für den Menschen auf ein Minimum. Mit umfangreichen Paketlösungen für die Detektion, Klassifizierung, Identifizierung und Beseitigung aller Arten von Minen können Seestreitkräfte so mit einem zeitgemäßen Minenjagd-System ausgestattet werden.

Seit Jahren gibt ATLAS ELEKTRONIK in diesem Bereich international den Standard vor und ist eines der wenigen Unternehmen weltweit, die in der Lage sind, alle diese Fähigkeiten eigenständig zu entwickeln und herzustellen.

www.atlas-elektronik.com

... a sound decision

ATLAS ELEKTRONIK

Foto: Anna Neuhaus-Fischer

Liebe Leserinnen und Leser,

die Bundeswehr hat sich mit der Aufstellung des Organisationsbereiches Cyber- und Informationsraum (CIR) am 5. April 2017 eine weitere Dimension erschlossen: Wie Heer, Luftwaffe und Marine für die Dimensionen Land, Luft, Weltraum und See zuständig sind, so sind die Angehörigen des nun seit drei Jahren bestehenden Organisationsbereiches ganzheitlich für die Dimension Cyber- und Informationsraum verantwortlich.
Neben den Aufgaben Cybersicherheit, strategische Aufklärung, operative Kommunikation und Geoinformationswesen spielt natürlich auch die Informations- und Kommunikationstechnik eine tragende Rolle. Viele Fragen, die bereits zu Beginn der Aufstellung des neuen Organisationsbereiches im Kontext „Cyber" für die Bundeswehr an zentraler Stelle standen, bleiben weiterhin bestehen:

- Wie reagiert die Bundeswehr auf die weiter stark zunehmende Digitalisierung?
- Wie kann die Bundeswehr bei Einsätzen im Ausland ohne ortsfeste und erdgebundene Netzwerkleitungen störungsfrei kommunizieren und gleichzeitig sich selbst schützen?
- Wie schafft es die Bundeswehr, moderne IT-Standards des 21. Jahrhunderts zum eigenen militärischen Vorteil zu nutzen und innovative Lösungen zu finden?
- Wie werden die Soldatinnen und Soldaten der Bundeswehr für die zukünftigen Herausforderungen im IT-Bereich ausgebildet?

Das Kommando Informationstechnik der Bundeswehr (KdoITBw) als Teil des Organisationbereiches CIR leistet in der Beantwortung dieser Fragen einen eigenen, wesentlichen Beitrag, um insbesondere den Erhalt der Führungsfähigkeit für die Bundeswehr in jeder Lage zu gewährleisten. Modernste Netzwerktechnik, immer schnellere Datenübertragung im GBit/s-Bereich und hochverfügbarer Datenzugriff: Diese „IT-Services" sind für die heutige zivile Gesellschaft selbstverständlich. Für die Bundeswehr sind diese IT-Services mittlerweile ebenfalls selbstverständlich, wenn auch mit anderen, militärischen Vorzeichen.
Denn jederzeit und an jedem Ort der Erde, auch auf Schiffen und Booten der Marine, werden Services wie E-Mail, Telefonie, Video-Konferenz oder Bundeswehr-spezifische Applikationen, wie z.B. der Mission Enabling Service Bw, von vielen militärischen Nutzern „nachgefragt". Das Kommando Informationstechnik der Bundeswehr hält in seiner Rolle als „zentraler Supply-Manager" genau zu diesem Zweck ein umfangreiches IT-Serviceportfolio bereit, um sämtliche IT-Leistungen im Rahmen des Demand und Supply-Prozesses für seine „Kunden" bzw. „Demander" innerhalb der Streitkräfte erbringen zu können. Dazu zählen auch die Steuerung des Betriebs und der Schutz des IT-Systems der Bundeswehr. Für bestimmte IT-Services werden auch zivile Provider und natürlich auch unser strategischer Partner, der „Inhouse-IT-Dienstleister" der Bundeswehr, die BWI, eingebunden.
Um diese vielfältigen Aufgaben erfolgreich bewältigen zu können, bildet die Bundeswehr ihre Soldatinnen und Soldaten zukunftssicher aus. Wie diese Ausbildung neu ausgerichtet wird, können Sie in diesem IT-Report lesen. Die Schule Informationstechnik der Bundeswehr spielt eine zentrale Rolle insbesondere bei der neu strukturierten Ausbildung der IT-Feldwebel. Diese Ausbildung wurde modularisiert und auf die aktuellen Herausforderungen bei der Aufgabenerfüllung im täglichen IT-Alltag – mit besonderer Einsatzorientierung – ausgerichtet. Ebenso wurde die Ausbildung der Offiziere des Truppendienstes neugestaltet, um eine stärkere Bindung an die eigene Truppengattung im Bereich der IT-Truppen zu ermöglichen und zudem auch hier die Landes- und Bündnisverteidigung wieder stärker in den Fokus zu rücken. Auch die Universität der Bundeswehr in München bietet seit einiger Zeit spezielle Studiengänge wie z.B. den Masterstudiengang Cyber-Sicherheit an. Die Absolventen werden zukünftig in leitenden Funktionen in IT-Abteilungen mit besonderem Fokus auf Sicherheit und Entwicklung sicherer Systeme und Anwendungen eingesetzt werden können.
Um die Innovationsfähigkeit der Bundeswehr weiter zu steigern, wurde mit dem Cyber Innovation Hub der Bundeswehr (CIH) eine Schnittstelle zwischen der Startup-Szene und der Bundeswehr geschaffen. Diese Dienststelle identifiziert innovative Technologien in der internationalen Startup-Szene und entwickelt und validiert diese für die Bundeswehr.
Alle hier skizzierten Elemente tragen dazu bei, die Bundeswehr nicht nur bei der Digitalisierung weiter voran zu bringen, sondern auch Themen wie Innovationsfähigkeit und eine zukunftsorientierte IT-Ausbildung voranzutreiben. Denn die nächsten großen Aufgaben stehen bereits vor der Tür: Ein einheitliches IT-Management für die gesamten Streitkräfte und bruchfreie Interoperabilität zwischen dem IT-System der Bundeswehr und den IT-Systemen verbündeter Nationen.

Generalmajor Dr. Michael Färber

Kommandeur des Kommandos Informationstechnik der Bundeswehr

Grußwort

Inhalt

Impressum

Teilnehmer der Allianz für Cyber-Sicherheit

Wehrtechnischer Report 1/2020
IT-Report+ 2020
Herausgeber:
Mittler Report Verlag GmbH
ein Unternehmen der Gruppe

TAMMMEDIA

Geschäftsführer:
Peter Tamm
Thomas Bantle

Prokurist:
Jürgen Hensel

Leitende Redakteurin:
Dorothee Frank

Lektorat:
Peter Preylowski

Anzeigenleitung:
Waldemar Geiger
Mittler Report Verlag GmbH
Baunscheidtstraße 11
D-53113 Bonn
Tel: +49 (0) 228 35 00 887
waldemar.geiger@mittler-report.de

Layout:
CREATIV.CONSULTING GmbH
Meckenheim

Verlagsanschrift:
Mittler Report Verlag GmbH
Baunscheidtstraße 11
D-53113 Bonn
Telefon: +49(0)228 – 3500870
Telefax: +49(0)228 – 3500871
E-Mail: info@mittler-report.de
Web: www.mittler-report.de

Foto Titel: Bundeswehr Cyber Innovation Hub
Fotos Inhaltsverzeichnis: Bundeswehr, U.S. Army

Neugestaltung der Ausbildung der Offiziere im Kommando IT der Bundeswehr

Darstellung des ab dem 1. Juli gültigen angepassten Ausbildungsgangs

Oliver Mohr, Artur Mast

Die durch den Generalinspekteur der Bundeswehr im August 2017 angewiesene Untersuchung der militärischen Ausbildungslandschaft und -systematik befindet sich mit der „Offensive Ausbildung“ in der Umsetzung. Diese hat allerdings nicht umfassend die Ausbildungsorganisation selbst auf den Prüfstand gestellt.

Mit dem strategisch-politischen Dokument „AGENDA Ausbildung“ aus dem November 2018 hat der Generalinspekteur der Bundeswehr richtungsweisende Impulse gegeben, damit zukünftige Ausbildung in Qualität und Quantität den veränderten Rahmenbedingungen entspricht und zuverlässig ihren Beitrag zum Kernprozess „Einsatzbereite Kräfte bereitstellen“ leisten kann.
Die AGENDA Ausbildung hat nunmehr die militärische Ausbildungsorganisation, deren Ausbildungsinhalte und deren Methodik und Didaktik auf den Prüfstand gestellt und Veränderungsbedarfe identifiziert, insbesondere auch im Bereich des Ausbildungsgangs in der Laufbahn der Offiziere im Truppendienst (Offz TrDst) Heeresuniformträger (HUT).

Autoren

Oberstlt Oliver Mohr ist Reservist und übt derzeit als Dezernatsleiter Truppenausbildung im KdoITBw Abteilung Führung Gruppe Ausbildung Sicherheit. **OLt Artur Mast** ist Sachbearbeiter im Dezernat Truppenausbildung und arbeitet an der Konzeptionierung, Planung und Ausgestaltung der Neuausrichtung der allgemeinmilitärischen Ausbildung mit.

Zentralisierung der militärischen Ausbildung

Als Folge der Harmonisierung des Ausbildungsgangs Offz TrDst insbesondere aufgrund der Umsetzung des Bologna-Prozesses, der eine Vereinheitlichung des Studienbeginns und eine Verlängerung der Studiendauer erforderlich machte, hat man festgestellt, dass nach Entlastung der Truppe von der Durchführung der Offizierausbildung die Führungsnachwuchsausbildung weitestgehend in Form von aneinander gereihten, einzelnen Lehrgängen an zentralen Ausbildungseinrichtungen bzw. Schulen stattfindet.
Durch diese Zentralisierung der militärischen Ausbildung wurde insbesondere für HUT eine Identifikation und Bindung mit der zukünftigen militärischen Heimat nur begrenzt erreicht, ebenso gelang eine militärische Sozialisation, Bindung und Prägung nur eingeschränkt.
Die AGENDA Ausbildung formuliert den klaren Auftrag, möglichst früh Gelegenheit zu schaffen, Kompetenzen als militärischer Führer bzw. Führerin zu entwickeln und Erfahrungen aus der Praxis zu gewinnen, zugleich soll einer Verschulung und möglichen Überfrachtung mit im Schwerpunkt theoretischen Anteilen entgegengewirkt werden. Die gesamte Führungsnachwuchsausbildung soll dezentralisiert, entfrachtet und wo sinnvoll und zweckmäßig in die Truppe zurückgeführt werden.

Da die handlungsorientierte Ausbildung der Unteroffiziere, Feldwebel und Offiziere die Grundlagen für die personelle Einsatzbereitschaft der Streitkräfte legt, musste die militärische Ausbildung des Führungsnachwuchses angepasst werden, sodass sie sich noch stärker an den Rahmenbedingungen des Truppenalltags im Inland und Einsatz und an den Anforderungen der Landes- und Bündnisverteidigung ausrichtet.

Bindung an die militärische Heimat

Die Bindung des Führungsnachwuchses soll erhöht und den Männern und Frauen eine militärische Heimat geboten werden, mit der sie sich identifizieren können und die sich um sie kümmert. Gelerntes soll in der Praxis angewendet werden, um eine eigene Führungskompetenz entwickeln zu können.
Mit den Vorgaben der AGENDA Ausbildung greift nach eingehender Konzeptionierung, Planung und Ausgestaltung sowie Abstimmung zwischen den einzelnen Organisationsbereichen ab dem 90. Offizieranwärterjahrgang mit Diensteintritt 1. Juli 2020 die neu gestaltete Ausbildung der Offz TrDst HUT auch im Kommando Informationstechnik der Bundeswehr (KdoITBw), um eine stärkere Truppengattungsbindung unter anderem durch eine Dezentralisierung der Ausbildung zu erreichen.

ACCREDITATION FOR NATO
RESTRICTED CLASSIFIED
COMMUNICATION

COMMON CRITERIA
CERTIFIED
(EAL4+)

DENCRYPT

SICHERN SIE IHR SMARTPHONE SPRACHANRUFE & NACHRICHTEN

Dencrypt Communication Solution schützt Ihre Smartphone-Kommunikation – Sprache und Nachrichten – vor Abhörversuchen. Die Dencrypt Talk and Message Apps kombinieren modernste dynamische Verschlüsselung mit einfacher Bedienung und machen hierdurch die sichere Kommunikation auf Standard-Smartphones einfach anwendbar.

Dencrypt Communication Solution ist eine schnell einsetzbare, skalierbare und sichere Kommunikationsplattform mit folgenden Merkmalen:

- » Ende-zu-Ende-Verschlüsselung
- » Hohe Audioqualität
- » Unterstützt Gruppenanrufe und Nachrichten
- » Gesichertes Telefonbuch und Benutzeraktivierung
- » Konnektivität in allen zellularen und drahtlosen Netzwerken
- » Als Cloud-Service oder Unternehmenslösung verfügbar
- » Läuft auf Standard-iOS- und Android-Smartphones

Download on the App Store

GET IT ON Google Play

Distribution via **MDM**

Dencrypt ist ein führender Anbieter von sicherer verschlüsselter Kommunikation. Unsere Lösungen basieren auf Dynamic Encryption, einer patentierten dynamischen Verschlüsselungstechnologie, die zur Realisierung eines extrem hohen Schutzniveaus entwickelt wurde. Zu den Kunden von Dencrypt zählen die NATO und die dänischen Streitkräfte.

dencrypt.dk

Grafiken: Ausbildungskommando Leipzig

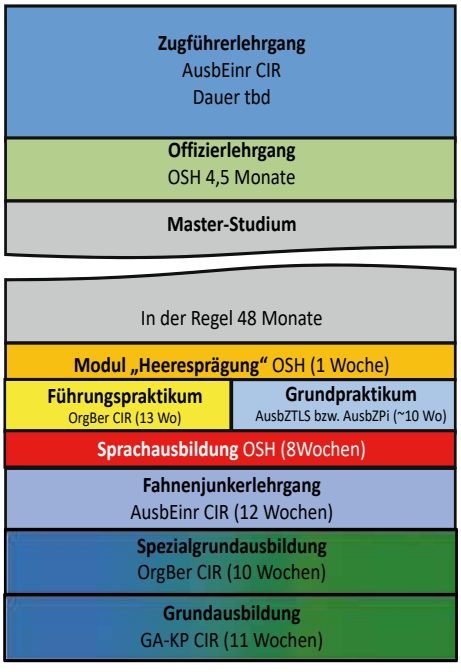
Die obige Grafik zeigt die bisherige Regelausbildung der Offz TrDst am Beispiel der Panzergrenadiertruppe.

Im bisherigen Ausbildungsgang traten die Offizieranwärter/-innen (OA) in einem der beiden OA-Bataillone ihren Dienst an und absolvierten dort innerhalb von sechs Monaten die allgemeine soldatische Grundbefähigung und schlossen den Ausbildungsabschnitt mit der Qualifikation Unteroffizier Landstreitkräfte ab. Daran anschließend folgte der Offizierlehrgang 1 an der Offizierschule des Heeres (OSH) in Dresden, ein Truppenpraktikum in einem Informationstechnikbataillon (ITBtl) sowie die Sprachausbildung. Nach erfolgreicher Laufbahnprüfung zum Offizier Landstreitkräfte trat der Offizieranwärter sein Studium an. Nach erfolgreichem Abschluss des Studiums folgten der Offizierlehrgang 2 an der OSH sowie der Offizierlehrgang 3 an der jeweiligen Truppenschule. Nach 82 Monaten an Ausbildungseinrichtungen und Schulen erfolgte der erste tatsächliche Einsatz in der Truppe in der Erstverwendung als Zugführer/-in bzw. Teileinheitsführer/-in. Dieser Ausbildungsgang war, wie deutlich in der Abbildung zu erkennen, geprägt von verschulter Theorie an Ausbildungseinrichtungen und Schulen bzw. einer der beiden Bundeswehr-Universitäten.

Neue Ausbildung ab dem 1. Juli 2020

Dem entgegen steht ab dem 1. Juli 2020 die neue Offizierausbildung für HUT. Die-

Generischer Ablauf der neugestalteten Offizierausbildung ab dem 1. Juli 2020



se wird nachfolgend exemplarisch für das KdoITBw erläutert.

Die dreimonatige Grundausbildung (GA) wird für alle OA entweder beim ITBtl 281 in Gerolstein oder beim ITBtl 292 in Dillingen durchgeführt. Jeder OA soll am Ende der GA die „Allgemeinmilitärische Grundbefähigung“ erreichen. Die Durchführung von GA und SGA in der Truppe erhöht die Transparenz und den Einblick in das spätere Tätigkeitsfeld der Offiziere. Auch das Teilen des Truppenalltags mit Unteroffizieren und Mannschaften wird das Rollenverständnis der zukünftigen Offiziere entwickeln.

Mit erfolgreichem Bestehen der GA werden die OA zur Spezialgrundausbildungseinheit (SGA-Einh) versetzt. Die dreimonatige Spezialgrundausbildung wird beim ITBtl 282 in Kastellaun, ITBtl 293 in Murnau, ITBtl 381 in Storkow und beim ITBtl 383 in Erfurt durchgeführt. Im Teil 1 der SGA werden die truppengattungsspezifischen Inhalte vermittelt wie z. B. Kernfähigkeiten, Gliederung und Auftrag der Truppengattung. Im Teil 2 der SGA werden aufbauend auf die GA querschnittliche, allgemeinmilitärische Ausbildungsthemen vermittelt.

Im Anschluss an die SGA folgt ein dreizügiger Ausbildungsabschnitt bestehend aus Fahnenjunkerlehrgang an der Schule für Informationstechnik der Bundeswehr (ITSBw), Sprachausbildung mit Sprachleistungsprofil Englisch 3332 an der OSH oder Führungspraktikum in einem IT-Bataillon bzw. Grundpraktikum für OA mit technischem Studiengang.

Nach Absolvieren dieses dreizügigen Ausbildungsabschnitts nehmen die OA an einem einwöchigen Modul Heeresprägung an der OSH teil, bevor sie dann zum Studium an eine der beiden Universitäten der Bundeswehr in München oder Hamburg versetzt werden. Die Regelstudienzeit beträgt für Masterstudiengänge 48 Monate. Nach erfolgreichem Studienabschluss nehmen die im Studium zum Leutnant beförderten Offiziere am grundlegend neu

konzipierten Offizierlehrgang an der OSH sowie im Anschluss am ebenfalls inhaltlich neu gestalteten Zugführerlehrgang an der ITSBw teil, um dann mit Beendigung des Regelausbildungsgangs ihre Erstverwendung in der Truppe anzutreten. In den ersten 12 Monaten der Erstverwendung können die Offiziere mit der Werdegangsystematik IT-Management auf eigenen Wunsch am neu konzipierten Einzelkämpferlehrgang (EKL) teilnehmen.

Einzelkämpferlehrgang für die IT

Die Fähigkeit, sich selbst und andere versprengte Kräfte, wieder zu den eigenen Linien durchzuschlagen und der Truppe so wieder die Kräfte zuzuführen, die sonst in Gefangenschaft geraten würden, soll wieder auf eine breitere Grundlage gestellt werden. Die positiven, persönlichkeitsbildenden Effekte einer solchen Ausbildung für jeden Einzelnen bleiben unbenommen, stehen jedoch nicht im Fokus.
Der Einzelkämpferlehrgang (EKL) wird in nahezu allen Aspekten angepasst. Die Lehrgangsinhalte richten sich wieder näher an der Landes-/Bündnisverteidigung aus, der Eingangstest wird verändert, die Lehrgangsdauer reduziert sich von derzeit sieben Wochen auf fünf Wochen. Auch die Bereichsvorschrift zur Einzelkämpfervorbereitung (EKV) wird überarbeitet, gestrafft und gezielt an den Anforderungen der angepassten Inhalte ausgerichtet werden. So wird der Schwerpunkt auf eine deutlich verbesserte Marschfestigkeit gelegt werden. Denn eines wird der EKL nicht werden: einfacher.

Umstellung auf die neue Ausbildung

Mit der hier in groben Zügen dargestellten Neugestaltung der Offizierausbildung ab dem 1. Juli 2020 geht der Wunsch einher, wieder einen durch die eigene Truppengattung geprägten Offizier mit Führungsanspruch und -vermögen zu formen, der in seiner Regelausbildung nicht nur die „Schulbank gedrückt", sondern den Truppenalltag und dessen Herausforderungen kennengelernt hat und in diesen als Führungskraft und Persönlichkeit bestehen kann.
Die Umstellung bedeutet sicherlich für alle Beteiligten eine große Herausforderung. Die Einheiten müssen plötzlich rund 100 Soldaten zusätzlich in der GA und in der SGA ausbilden, die bisher in den OA-Bataillonen ausgebildet wurden. Die OSH und die ITSBw müssen den Ausbildungsbetrieb anpassen, nicht mehr vorhandene Personal-, Material- und Unterkunftskapazitäten „aufgebohrt" und insgesamt die Umstellung von „Alt" auf „Neu" mit einem vernünftigen „Change-Management" bewältigt werden.
Dies muss und wird gelingen! Die Ausbildung unseres Führungsnachwuchses sollte für jeden, an der Ausbildung der jungen OA und Offiziere Beteiligten, eine „Herzensangelegenheit" sein. ■

Gruppenführer, Zugführer, Fähnrichoffizier, Kompaniefeldwebel, Kompaniechef, Kommandeur, Hörsaalfeldwebel, Hörsaalleiter oder Inspektionschef, Sie alle tragen ihren Teil dazu bei, den neuen Führungsnachwuchs auf unsere Truppengattung zu prägen und als Führungskraft und Persönlichkeit zu formen. Für diese Aufgabe wünschen wir Ihnen viel Fortune und das nötige Quäntchen Soldatenglück und rufen Ihnen ein donnerndes „Fernmelde Hurra" aus dem Kommando IT zu.

Neugestaltung der Fachausbildung der IT-Feldwebel

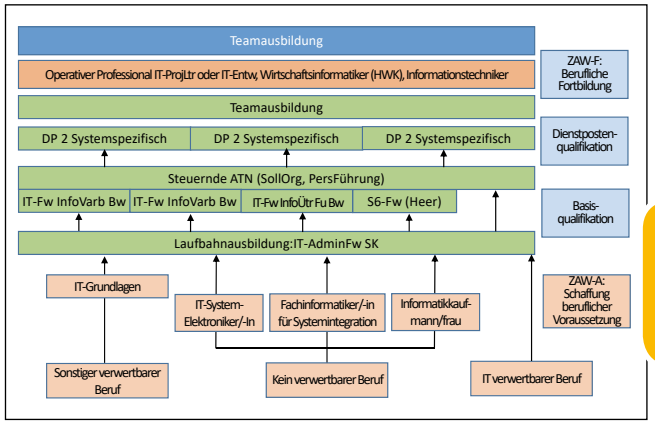
Fähigkeitsbezogene Ausbildung – „Basistraining IT-Fw“

Wilhelm Breimaier, Sebastian Bente, Janin Funke

Bedingt durch die Schnelllebigkeit im Bereich Cyber und den daraus resultierenden wechselnden Anforderungen an die IT-Feldwebel (IT-Fw), steht die Bundeswehr immer häufiger vor der Herausforderung, eine am Einsatz ausgerichtete Flexibilisierung der Qualifizierung von IT-Fw sicherzustellen.

Status Quo

Die militärfachliche Ausbildung der IT-Fw ist bisher geprägt von mehreren, aufeinander aufbauenden Trainings. Ziel der militärfachlichen Ausbildung zum IT-Fw ist es, ein dezidiertes IT-System aus dem IT-System der Bundeswehr im Einsatz administrieren zu können. Dabei kann es vorkommen, dass zwischen den einzelnen Trainings oftmals planungsbedingte Pausen liegen, zum Beispiel aufgrund fest angelegter Trainingszeiträume.
Insbesondere um eine Verzögerung innerhalb der Ausbildungsplanung möglichst gering zu halten und darüber hinaus eine umfassendere Qualifizierung zu ermöglichen, wurde die Neugestaltung der IT-Fachausbildung für die IT-Fw durch die Abteilung Ausbildung des Kommandos Informationstechnik der Bundeswehr (KdoITBw) vorangetrieben.
Die nachfolgende Grafik zeigt, wie die Ausbildung der IT-Fw bisher strukturiert ist:



Grafiken: Autoren

Abbildung 1: Bisheriger Ausbildungsgang der IT-Feldwebel

Derzeit erfolgt die Ausbildung der IT-Fw zielgerichtet für ein IT-System. Die dafür geforderte dienstpostenspezifische Qualifikation ist Grundlage der Ausbildungssteuerung. Die SOLL-Organisation der Bundeswehr ist damit eine bestimmende formale Rahmenbedingung für die dienstpostengerechte militärfachliche Individualausbildung. Grundsätzlich sind die Dienstposten (DP) für IT-Fw als DP des allgemeinen Fachdienstes ausgeplant, d.h. an eine zivile Berufsausbildung gebunden. Die Ausbildung beginnt je nach Einstellungsvoraussetzung unterschiedlich. Sollte ein Bewerber bereits einen, für die Bundeswehr verwertbaren, IT-Beruf erlernt haben, erfolgt eine direkte Einsteuerung in die Laufbahnausbildung. Hat der Bewerber bisher keinen verwertbaren IT-Beruf erlernt, absolviert dieser vor der Laufbahnausbildung eine zivilberuflich voll verwertbare und anerkannte Ausbildung in einem der drei oben angeführten, anerkannten IT-Berufe.
Nach dem Absolvieren der Laufbahnausbildung schließt sich die Dienstpostenausbildung Teil 1 (DP 1) an. Danach folgt die Ausbildung für das jeweils spezifische IT-System (Dienstpostenausbildung Teil 2; DP 2).

Defizitanalyse und Neugestaltung

Mit der Zusammenfassung der Laufbahnausbildung und der DP 1 wird zukünftig vom „Basistraining IT-Fw“ gesprochen. Dieses „Basistraining IT-Fw“ ersetzt dann die bisher aufeinander folgenden Trainings IT-AdminFw SK (Laufbahnlehrgang militärfachlicher Teil) und die daran anschließenden einzelnen Trainings der DP 1 (IT-Fw-Informationsverarbeitung, IT-Fw Informationsübertragung Weitverkehr, IT-Fw Informationsübertragung Funk und S 6 Fw (siehe Abb. 1), einschließlich des militärfachlichen Teils der Feldwebelprüfung in der Laufbahn der Feldwebel des allgemeinen Fachdienstes (Abb. 2).

Autoren

Oberstlt i.G. Wilhelm Breimaier ist Gruppenleiter im KdoITBw, Abteilung Ausbildung, Gruppe Cyber IT. Durch seine langjährige Expertise im Bereich der IT-Ausbildung hat er maßgeblich bei der Entwicklung der fähigkeitsbezogenen Ausbildung der IT-Fw mitgewirkt. **OLt Sebastian Funke** ist Sachbearbeiter im KdoITBw, Ausb Cyber IT. Funke war von Beginn an mit der Konzeptionierung, Planung und Ausgestaltung der neuen Ausbildung beauftragt und hat diese maßgeblich mitgestaltet. **OLt Janin Bente** ist Sachbearbeiterin im KdoITBw, Ausb Cyber IT, FZst BasisQ.

Mit dieser Neuordnung der Ausbildung der IT-Fw wird eine einheitliche, einsatzorientierte und breite Basisausbildung der IT-Fw sichergestellt, die Grundlage für eine flexible, modulare weitere militärfachliche Ausbildung ist. Damit wird auch eine zeitlich straffere Durchführung der Basisausbildung ermöglicht. Unverändert wird durch das Basistraining der fachliche Abholpunkt für die heutige DP 2-Ausbildung erreicht. Dieser Ansatz wird von allen Organisationsbereichen und insbesondere von dem Bundesamt für das Personalmanagement der Bundeswehr (im Speziellem die Bereiche Personalgewinnung und Ausbildungssteuerung) mitgetragen und ist durch den Inspekteur Cyber und Informationsraum in seiner Verantwortung für die für die Dimension Cyber gebilligt.

Zielvorstellung: Modulmatrix

An das „Basistraining" der Feldwebel schließt die sogenannte „Modulmatrix" an. Sie ersetzt künftig das starre System der IT-systemorientierten DP2-Ausbildung. Die Zielvorstellung der Neugestaltung der Modulmatrix ist, dass der IT-Fw im Zentrum steht, eine umfassende IT-fachliche Basisausbildung absolviert hat und an die aktuelle Bedarfssituation angepasst, eine Dienstpostenqualifikation im Rahmen von mehreren, aufeinander logisch aufbauenden, Modulen erwirbt.
So ist es möglich, individuelle Fähigkeiten und Fertigkeiten des Einzelnen und gleichzeitig wechselnde Einsatzforderungen an die Ausbildung zu berücksichtigen.

tige Ausbildung auf der Zeitschiene werden unterstützt. Bei einem Systemwechsel oder der Einführung neuer Systeme können, ausgehend von den bereits erfolgten Ausbildungen, modular die noch fehlenden Qualifikationsanteile geschult werden.
Ausbildungsbeginn für das Basistraining ist Juli 2020. Die Schule Informationstechnik der Bundeswehr stellt derzeit die Ausbildungsbereitschaft her. Bereits zur Einführung erfolgt die Vermittlung von Wissen kompetenzorientiert, sodass der Lernende im Fokus steht. Kompetenzorientierte Ausbildung orientiert sich insbesondere an den konkreten beruflichen und dienstlichen Handlungen im Alltag, auf dem Dienstposten oder in einer bestimmten Funktion. Bereits in

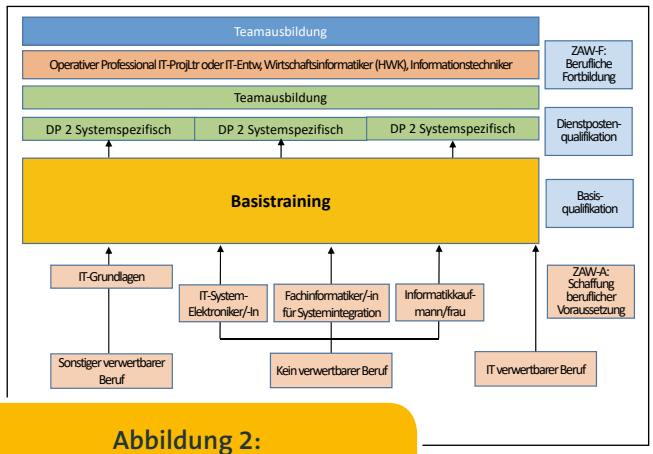


Abbildung 2: Neuer Ausbildungsgang der IT-Fw mit Einführung des Basistrainings

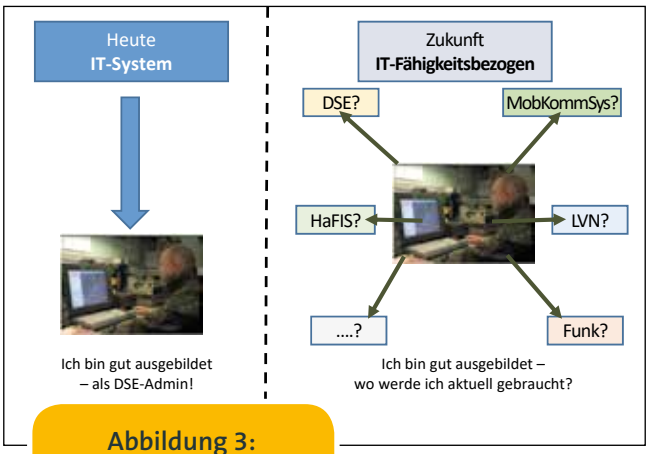


Abbildung 3: Zielvorstellung: Der IT-Fw im Zentrum

Die Zukunftsorientierung dieser Neugestaltung basiert auf den Anknüpfungspunkten zur Studie „Grundlagen für die Gestaltung einer zukunftsfähigen Cyber- und IT-Aus-, Fort- und Weiterbildung im Geschäftsbereich BMVg". Als Ergebnis dieser Studie wurde unter anderem Optimierungsbedarf im Bereich der mangelnden Flexibilität der Ausbildung, der Unterbrechung der Ausbildungszeit und mangelnde Anpassung identifiziert. Die Anknüpfungspunkte an den festgestellten Identifizierungsbedarf sind beispielsweise die Erhöhung der operativ nutzbaren Zeit, Einführung und Erhöhung der kompetenzorientierten Ausbildung sowie die Entwicklung einer modularen Clusterausbildung. Der Ansatz einer fähigkeitsbezogenen IT-Ausbildung mit dem derzeitigen Schwerpunkt gerichtet auf die Gruppe der IT-Fw ist somit zukunftsorientiert und erfolgversprechend.

Mit einer modularisierten weiterführenden militärfachlichen Ausbildung gelingt es auch, die erworbene Qualifikation von Seiteneinsteigern oder Systemwechslern gewinnbringend zu berücksichtigen.
Eine breitere Qualifikation von IT-Fachpersonal in unterschiedlichen Bereichen sowie eine bedarfsorientierte, stufenarder Ausbildung liegt der Schwerpunkt auf dem selbstständigen Handeln des Auszubildenden. Dies führt zu einer handlungssicheren und effektiven Aufgabenerfüllung in zukünftigen Verwendungen.
Zusammenfassend führt die schrittweise Umstellung auf eine fähigkeitsbezogene, modulare Ausbildung der IT-Fw zur Steigerung der Leistungsfähigkeit, Flexibilität und Attraktivität in der bisherigen Ausbildungslandschaft der Bundeswehr. ■

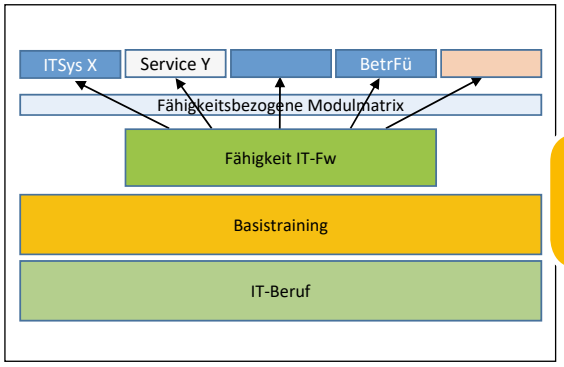


Abbildung 4: Modularisierte Systemausbildung für IT-Fw

Führungswechsel an der Schule für Informationstechnik der Bundeswehr

Nicole Herzog, Meik Rosenberger

Nach drei Jahren unter der Führung von Brigadegeneral Frank Schlösser wurde am Donnerstag, den 23. Januar 2020, die Schule für Informationstechnik (ITSBw) der Bundeswehr mit einem feierlichen Appell an Oberst Rainer Simon übergeben.

Ein letztes Mal lässt der Kommandeur Brigadegeneral Frank Schlösser seine ihm anvertrauten Frauen und Männer antreten. Über 150 Gäste, darunter auch ehemalige Angehörige der ITSBw und Vertreter der Politik, wohnten dieser feierlichen und bewegenden Zeremonie bei. Als die Begrüßung des Kommandeurs von etwa 650 Soldatinnen und Soldaten laut über den Appellplatz schallend erwidert wurde, schreitet Schlösser zum Rednerpult. Spürbar emotional reflektierte er mit seiner letzten Rede zunächst auf die bereits erreichten Ziele, im Besonderen aber auf die die anstehenden Aufgaben und Veränderungen.

Schlösser leitete die Ausbildungseinrichtung, die von vielen noch immer Fernmeldeschule genannt wird, stets spürbar mit Herz. Sein Abschied von der Truppe fiel „frostig" aus – aber nur beim Blick auf das Thermometer, das auf dem weitläufigen Appellplatz Minusgrade anzeigte. Die Soldaten waren in Ehrenformation aufmarschiert, begleitend und mit gewohnter Professionalität spielte das Gebirgsmusikkorps aus Garmisch-Partenkirchen. „Der Abschied fällt mir nicht leicht. Ich verlasse auch eine Region, die für Jahre meine Heimat war. Das geht an Kommandeur und Mensch nicht spurlos vorüber", sagte Schlösser, der gern weitergemacht hätte. Aber nun war klar, seine Zeit als Kommandeur der Schule für Informationstechnik der Bundeswehr endet heute. Nun wird er einen knapp einjährigen Auslandseinsatz in Afghanistan antreten.

Große Herausforderungen

Dem Protokoll folgend übernahm jetzt Generalmajor Dr. Michael Färber, Kommandeur des Kommandos für Informationstechnik der Bundeswehr, das Wort. Bevor dieser aber das Kommando übergab, zeigte er deutlich auf, dass sowohl auf den neuen Schulkommandeur als auch auf die Angehörigen der ITSBw in den kommenden Jahren sehr viel Arbeit zukommen werde. Neben vielen anderen Aufgaben wurden hier besonders der Umzug von Feldafing nach Pöcking, Umstellung der Ausbildung von IT-Spezialisten und Administratoren als auch neu zu etablierende Lehrgänge genannt.

Der Wechsel

Oberst Rainer Simon hielt sich als nachfolgender Kommandeur während der Verabschiedungszeremonie wie vom Protokoll gefordert im Hintergrund, bis ihm dann die offizielle Führung der ITSBw durch den Kommandeur KdoITBw übertragen wurde. Dann der erste Befehl des 54-Jährigen: „IT-Schule hört auf mein Kommando!" Ab jetzt sind die vielen Frauen und Männer der ITSBw ihm unterstellt. Einsätze und vielfältig absolvierte Verwendungen über alle Bereiche hinweg sind in der Vita des neuen Kommandeurs erkennbar. Scheint, als seien al-le Voraussetzungen gelegt um die anstehenden Aufgaben der ITSBw mit Bravour zu meistern. Was als Kommandeur auf ihn zukommt, nennt er „Große Herausforderungen". Mit Recht! Über vier Standorte verteilt und mit fast 150 Lehrgangstypen, die bis hin zu zweijährigen Ausbildungen reichen, sind aktuell und zukünftig einige Veränderungen im „Live-Betrieb" zu bewältigen. Für die Zukunft an der Schule für Informationstechnik der Bundeswehr wünscht sich der neue Kommandeur eine kontinuierliche und gute Zusammenarbeit auf allen Ebenen. „Seine Tür stehe immer und für jeden offen!" ■

Appell zur Übergabe der Schule Informationstechnik der Bundeswehr

Foto: Bundeswehr/Monika Monden

Autoren

Feldwebel Nicole Herzog ist Medienbproduktionsfeldwebel an der Schule für Informationstechnik der Bundeswehr (ITSBw). **Hauptmann Meik Rosenberger** ist Presseoffizier der ITSBw, Personalvertreter und im erweiterten Vorstand Örtlicher Personalrat ITSBw.

Masterstudium Cyber-Sicherheit

Ein Niederländer bei der Bundeswehr

Martina Pump

Eine deutsch-niederländische Kooperation existiert schon seit einigen Jahren und wird nun im Bereich Ausbildung weiter intensiviert. Im September des Jahres 2019 hat sich der niederländische Offizier Sander Wieriks auf Einladung des Kommandos Cyber- und Informationsraum (KdoCIR) an der Universität der Bundeswehr in München eingeschrieben. Er ist als erster ausländischer Kursteilnehmer für den Masterstudiengang Cyber-Security eingeplant.

Inmitten der anderen Studierenden auf dem Campus fällt er sofort auf, nicht nur, weil er die meisten mit seinen 1,93 Metern Körpergröße überragt. Zudem trägt er einen Feldanzug der Niederländischen Streitkräfte. Kapitein Sander Wieriks ist gerade auf dem Weg zur Bibliothek, um einige Mathematikbücher zur Nachbereitung der Vorlesungen auszuleihen. Im Moment heißt es für ihn nur Mathe, Mathe und nochmals Mathe. „Es ist jetzt 16 Jahre her, dass ich mein Abitur gemacht habe. Das Lerntempo hier ist sehr intensiv, daran muss ich mich erst wieder gewöhnen, aber es geht schon“, sagt Wieriks mit einem Lächeln.

Fotos: Bundeswehr/Martina Pump

Das Pensum ist nur mit eigenständiger Vor- und Nachbereitung zu schaffen

Top-Thema Cyber-Sicherheit

Er muss fit sein in den mathematischen Methoden, um die Konzepte, die etwa hinter Kryptologie oder Datenanalyse stehen, zu verstehen. „Mathematik ist die Sprache des Computers. Wenn man im Bereich Cyber-Sicherheit arbeitet, muss man wissen, wie ein Computer funktioniert, wie Verbindungen hergestellt werden. Wenn man nicht weiß, wie ein System aussehen soll, erkennt man seine Schwächen nicht“, erläutert Wieriks. Er fügt hinzu: „Ähnlich wie ein Mediziner, der den Körper und seine Funktionen kennen muss, um seinen Patienten heilen zu können.“

Bündelung der Kräfte in der Cyber-Abwehr

Dass Wieriks an der Bundeswehr-Universität studiert, hat er der verstärkten Zusammenarbeit zwischen den deutschen und niederländischen Streitkräften im Cyber- und Informationsraum zu verdanken. Beide Nationen steuern nun auch im akademischen Kontext einen vermehrten Austausch an, um in der Zusammenarbeit im Bereich der Cyber-Abwehr eine gemeinsame Sprache zu sprechen und auf gemeinsame Methoden zurückgreifen zu können. Daher hat das Kommando CIR das Defence Cyber

Autor

Martina Pump ist Redakteurin und Fotografin im PIZ CIR.

Command (DCC) der Niederländischen Armee eingeladen, einen Soldaten zum Masterstudium Cyber-Sicherheit nach München zu schicken. Und der 34-jährige Wieriks wurde ausgewählt.

Faszination für Technik und Sport

Neben einem guten Verständnis für Technik und Mathematik waren sehr gute Deutschkenntnisse Voraussetzung für seine Nominierung, da das Studienprogramm größtenteils auf Deutsch abläuft. Wieriks, der als Jugendlicher fünf Jahre in Deutschland lebte und sein Abitur in Indonesien absolvierte, kam mit 17 Jahren zurück in die Niederlande. Dort stand für ihn zunächst Rugby an vorderster Stelle, er spielte sogar in der ersten Liga. Aber Wieriks suchte nach einer Möglichkeit, seine Leidenschaft für Technik und Sport verbinden zu können. Er fand sie beim Militär: 2008 begann er eine Offiziers-Ausbildung an der königlichen Militärakademie in Breda. Danach absolvierte er eine Fachausbildung als Fernmeldeoffizier. Sein Job führte ihn immer wieder auch an Einsatzorte der niederländischen Armee im Ausland, wo er für den Aufbau von Netzwerken zuständig war.

Um analoge Bücher kommt man selbst im Studiengang Cyber-Security nicht herum

Netzwerke für die Zukunft

Neben seinem fachlichen Interesse ist das Thema internationale Zusammenarbeit seine Motivation für das Studium in Deutschland. „Hier kann ich ein gutes Netzwerk aufbauen mit Offizieren, die auch im CIR arbeiten werden." Ein gutes Fundament, um nach dem Studium die bilaterale Zusammenarbeit zwischen Deutschland und den Niederlanden weiterzuführen.

Optimale Betreuung

Wieriks ist einer von 156 Soldaten, der für den Bachelor Informatik – die Voraussetzung, um den Master Cyber-Sicherheit anzuschließen – eingeschrieben ist. Im September 2020 werden die ersten 20 Studierenden den Studiengang Cyber-Sicherheit, der im Wintersemester 2018 ins Leben gerufen wurde, beenden. Der Niederländer plant, seinen Abschluss in vier Jahren in der Tasche zu haben. Er schwärmt von der intensiven Betreuung: „Im Schnitt betreut hier ein Professor nur 18 Studierende."

Der Zugang zu den Computerhörsälen im Rechenzentrum ist über Transponder geregelt

50 bis 60 Stunden pro Woche für das Studium

Der 34-Jährige ist mit seiner Frau und seinen beiden Töchtern, von denen die Jüngste gerade zehn Monate alt ist, im Sommer nach München gezogen. Als Vater und Ehemann steht er vor der Herausforderung, sein Leben so zu organisieren, dass sowohl Studium als auch Familie darin Platz finden. Deswegen gehört er zu den wenigen, die nicht auf dem Campus wohnen und schlafen. „Ab 8 Uhr bin ich an der Uni und dann lerne ich noch einmal abends von 20 bis

22 Uhr, wenn die Kinder schlafen. So komme ich auf 50 bis 60 Stunden pro Woche Arbeitsaufwand für das Studium“, erzählt Wieriks.

Das Internet kennt keine nationalen Grenzen

So ganz ohne Vorkenntnisse aus dem Bereich Cyber-Security hat Wieriks sein Studium allerdings nicht begonnen. Seit 2017 arbeitete er im niederländischen Defence Cyber Command im Bereich Cyber Threat Intelligence. Dort analysierte er Cyber-Angriffe auf die Systeme der niederländischen Armee. Er weiß also, wie bedeutsam das Thema Cyber-Sicherheit für das Funktionieren von Institutionen und Infrastruktur ist. Und Internet und Cyber-Raum unterscheiden sich in einer Hinsicht völlig von der „analogen“ Welt. „Im Internet gibt es keine nationalen Grenzen“, sagt Wieriks. „Deshalb ist es wichtig, die Grenzen in der internationalen Zusammenarbeit abzubauen.“ ■

Master-Studiengang Cyber-Sicherheit an der Universität der Bundeswehr München

Absolventinnen und Absolventen des Master-Studiengangs Cyber-Sicherheit sind vielseitig in allen Bereichen von Bundeswehr, Behörden, Wirtschaft und Gesellschaft einsetzbar, die in besonderem Maße auf die Vertraulichkeit, Integrität und Verfügbarkeit der eingesetzten IT-Dienste und verarbeiteten Daten angewiesen sind. In der Praxis werden sie sich mit der Konzeption, Planung, Realisierung, Überprüfung, Modifikation und Wartung von informationsübertragenden und -verarbeitenden Systemen mit einem Fokus auf die charakteristischen Sicherheitsaspekte in jeder Lebenszyklusphase der IT-Systeme befassen.
Dabei kann es sich um Waffeneinsatz-Systeme und Führungsinformationssysteme der Bundeswehr handeln, um multimediale Kommunikationssysteme in Unternehmen, in Staaten oder rund um den Globus, oder um Steuerungssysteme für Maschinen, Industrieanlagen, Verkehr oder die Vermittlung von Telefongesprächen. Auch in den kleinen Dimensionen breiten sich Einsatzgebiete für Cyber-Sicherheit rapide aus: Smartphones, Smartwatches, Mobile Computing sowie medizinische Körpersonden und andere eHealth-Anwendungen weisen einen hohen Schutzbedarf auf.
Konkrete Berufstätigkeiten sind:

- Entwicklung sicherer Systeme und Anwendungen zur Datenverarbeitung und deren Betrieb,
- Einführung und Erneuerung von IT-Infrastrukturen in Umgebungen mit erhöhtem Schutzbedarf,
- Analyse und Verbesserung bestehender IT-Infrastrukturen unter IT-Sicherheitsaspekten,
- Angriffsprävention, Einsatz von Detektionsmechanismen und Reaktion auf Sicherheitsvorfälle,
- Tätigkeiten in verschiedenen Ausbildungsinstitutionen, einschließlich Lehre und Forschung.

Absolventinnen und Absolventen des Master-Studiengangs werden verstärkt im akademischen Bereich und in leitenden Funktionen in IT-Abteilungen eingesetzt.

Quelle: UniBw München, Fakultät für Informatik

Hat der Westen die Fähigkeiten der Streitkräfte der Opponenten unterschätzt?

Foto: ELETTRONICA

Interview mit Dr. Marcello Mariucci,
Geschäftsführer der ELETTRONICA GmbH

Der IT-Report hat kurz vor der Corona-Krise den Geschäftsführer der ELETTRONICA GmbH über Technologien und Weiterentwicklungen im Bereich der Elektronischen Kampfführung (EloKa) – unter anderem Radar, Störmaßnahmen und Aufklärung mittels Sensoren – interviewt. Kerngeschäft der ELETTRONICA, ein Unternehmen mit 70jähriger Erfahrung und seit 40 Jahren mit deutscher Niederlassung in Meckenheim bei Bonn.

IT-Report: Welche Bedeutung hat der Elektronische Kampf für moderne Kriegsführung und Verteidigung?
Mariucci: Es ist eine deutlich wachsende und lange unterschätzte Kompetenz im Kontext des „Non-kinetic Warfare". Bereits während der jüngsten Ukraine-Krise und nicht zuletzt bei den NATO-Manövern hat man erkannt, dass Electronic Warfare ein ganz wichtiger Bestandteil der modernen Kriegsführung ist. Auch musste man feststellen, dass die „Friedensdividende" nicht ohne Auswirkungen blieb und sich andere Staaten in dieser Periode entsprechend weiterentwickelt haben. Eine Verteidigungs- und Einsatzbereitschaft wird sich nur dann wieder aufholen lassen, wenn wir diese „überraschenden" Erkenntnisse in den Fokus unserer Kompetenzerweiterung in der NATO, EU und in Deutschland aufnehmen.

IT-Report: Haben die Russen nach dem Ende des Kalten Krieges also die EloKa weiterentwickelt, während Europa im Zuge des neuen Friedens andere Prioritäten setzte?
Mariucci: Nun, die EloKa ist und war schon immer ein Wettlauf der Technologien, Fähigkeiten und Anwendungen – eine Spirale von stetigen Kompetenzerweiterungen. Meine Erkenntnis ist, dass man in den letzten Jahren und Jahrzehnten, geprägt von den Erfordernissen der „Out-of-Area"- Einsätze, eine andere Prioritätenlage für den Einsatz und die Verwendung unserer Geldmittel gewählt hatte, während Russland sich darauf konzentrierte, eigene Möglichkeiten der EloKa-Fähigkeiten technologisch und strategisch weiterzuentwickeln. Man hat das russische Entwicklungspotential und den Willen, die Führung und Überlegenheit in diesem Gebiet zu übernehmen, wie so oft unterschätzt.
Man muss in dieser Betrachtung unbedingt erwägen, dass neben den Konfliktherden mit Einbindung von Deutschland, der EU und der NATO das Gesamtgebilde der Bedrohung einem totalen Paradigmenwechsel unterzogen wurde. Wer hatte schon in der EU vor zehn Jahren über Cyberbedrohungen als ein Teil der „non-Kinetic-Bedrohung" und hybriden Kriegsführung nachgedacht, außer eventuell weniger spezialisierter Forschungszentren?
Russland hat seine EloKa sehr gezielt weiterentwickelt. Alle Schwachstellen von denen die Experten meinten, dass Russland diese besitze, sind nun dank der konzentrierten russischen Modernisierung überwunden und zwingen uns zur Weiterführung der Counter-Counter-Strategie.

IT-Report: Würden Sie die russischen Fähigkeiten also als First Class bezeichnen?
Mariucci: First Class bedeutet nicht, dass sie allein auf diesem Niveau sind. Aber Russland ist sicherlich im First Class Waggon, in dem nur sehr wenige weitere Nationen sitzen.

IT-Report: Befindet sich die Bundeswehr ebenfalls im First Class Waggon?
Mariucci: Die Frage ist emotionslos nur schwer zu beantworten, weil es nicht nur darum geht, was man auf dem Papier aufweisen kann oder gegebenenfalls in der Technologiebewertung führt, sondern was man in der Truppe bzw. in der Beschaffung hat. Habe ich die Fähigkeiten so breit in der Truppe, dass ich im Ernstfall schnell auch wirklich solche Maßnahmen und Wirkungen erzielen kann? Das wage ich aktuell zu bezweifeln und Beispiele ließen sich da konkret für jede Teilstreitkraft nennen. Die aktuellen Zeitzyklen der Entwicklung und Beschaffung sind im Kontext der EloKa einfach zu lang.

IT-Report: Muss die Bundeswehr beim Electronic Warfare aufholen?
Mariucci: Das Kommando CIR hat durchaus erkannt, dass der Elektronische Kampf aus den Investitionen der letzten Jahre fast verschwunden ist. Hierfür gibt es mehrere Gründe.
Zum einen handelt es sich um ein sehr kompliziertes Segment. Dies bedeutet, man muss speziell geschultes Personal und erfahrene Operateure haben, diese sind sehr rar. Durch die Rotationen innerhalb der Bundeswehr ist dieses Personal zudem schwierig zu halten, weshalb der know-How Aufbau und Erhalt für die Bundeswehr nicht einfach sind. Diese Fähigkeiten sind nicht nur bei den Streitkräften gesucht, sondern auch in der wehrtechnischen Industrie.
Zum zweiten gab es in den Doktrinen ggf. die Ansicht, dass für die Landes- und Bündnisverteidigung Deutschlands der dem Elektronischen Kampf nicht unbedingt als das Wirkungsmittel Nummer 1 auch vor Ort benötigt würde. Auch dies ist ein Grund für den Rückgang des Stellenwertes, der den Elektronischen Kampf in der jüngsten Vergangenheit beigemessen wurde.
Aktuell erkenne ich allerdings, dass im CIR das Interesse eigene Kapazitäten im EK-Bereich zu entwickeln, priorisiert wird. Hier bietet die Industrie, und so auch wir, natürlich unsere Dienstleistungen an, um diese Fähigkeiten schnell und kompetent auf- und auszubauen.

IT-Report: Die Bundeswehr kann also von der Größe Ihres Unternehmens profitieren?
Mariucci: In der Sicherheits- und Wehrtechnik sind 800 bis 1.000 Mitarbeiter, wie wir als ELETTRONICA aufgestellt sind, nicht sehr viel. Da der Verteidigungshaushalt eine schwankende Größe ist und stark von der aktuellen Politik abhängt, muss ein Unternehmen eine gewisse Substanz haben, um schwierige Phasen auch durchleben zu können. Deshalb muss ich mich einerseits auf ein, bzw. auf das wahrscheinlichste Portfolio konzentrieren und andererseits selbstständig, oder besser, unabhängig sein.
Es war für ELETTRONICA daher wichtig eine eigenständige deutsche Unternehmung zu gründen, die mehr war als eine verlängerte Werkbank eines italienischen Know-how Lieferanten. Diesen Umbau habe ich in den letzten fünf Jahren vorangebracht. Als deutsches Unternehmen halten wir uns strikt an die deutsche Ausfuhrgenehmigung.
Die Wichtigkeit und Tragweite dieser letzten Aussage kann ich an einigen Beispielen benennen. Wir hatten den Auftrag unserer Muttergesellschaft zur Unterstützung bei der Auslieferung eines EloGM-Systems an einen Kunden im globalen Markt. Das Zielland, mit guten Beziehungen in den Westen, war in einen der kritischen Konfliktherde verwickelt. Da der Auftrag mit der Ausrüstung der vertraglich beauftragten Plattform verbunden war, unterlag er der deutschen Ausfuhrgenehmigung und nicht den Vorgaben aus Italien. Wenn sich die deutsche Politik dazu entscheidet, nicht an an einem Konflikt beteiligtes Land zu liefern, die italienische Politik hingegen liefern würde, dann gibt es für ein Unteenehmen ein e unüberwindbare Diskrepanz – sogar in der europäischen Allianz. Als deutsches Unternehmen halten wir uns an die nationalen Gegebenheiten. Die ausländische Gesellschafterin kann nichts forcieren, auch wenn dadurch ihr eigenes Geschäft gefährdet ist. Ich halte das Gerät seit über einem Jahr auf Halde ohne es über die Alpen zu meinem Kunden zu bewegen.

IT-Report: In welche Märkte stieß das deutsche Unternehmen ELETTRONICA?
Mariucci: Wir haben es in den vergangenen Jahren geschafft, hier in Meckenheim eine eigene Identität aufzubauen. Wir sind keine verlängerte Werkbank und wir bauen auch keine Sensoren. Wir sind also nicht im Wettbewerb mit der italienischen ELETTRONICA SpA.
Wir konzentrieren uns in der Wehrtechnik auf drei Bereiche:
Erstens, die Plattform- und Sensorhersteller-unabhängige Integration von EloKa-Sensoren in gepanzerten Fahrzeugen sowie in schnell verlastbaren, abgeschirmten Containern oder Kabinen. Hier sind wir seit Jahren ein gut akzeptierter Partner, Systemintegrator und Lieferant der Bundeswehr.
Zweitens, die Entwicklung von Systemen für den Test und die Validierung von Radar und EloKa-Sensoren. Hier nutzen wir unsere Expertise, um Herstellerunabhängig die Eigenschaften und Techniken von Sensoren und integrierten Plattformen im gesamten Lebenszyklus zu testen und zu validieren. Daraus ergeben sich Szenarien und Module, die wir zu Schulungszwecken verwenden, aufbereiten und anbieten können. Ein Beispiel hierfür ist der EK-Simulator, der Ende 2018 an die WTD71 in Surendorf ausgeliefert wurde. Unser Auftrag bestand darin, für die Test- und Ausbildungseinrichtung für den Elektronischen Kampf der Marine (EK-Range See) einen 20-Fuß-Container abzuschirmen und mit Signalsimulations- und -analysefähigkeiten auszustatten, mit dem Ziel, die Radar- und EK-Sensorik der Schiffe zu kalibrieren, testen und zu validieren, wie auch die Ausbildung der Operateure zeitgerecht zu unterstützen. Ein weiteres Beispiel ist unsere Beteiligung am NATO JEWCS Programm, bei dem wir mit der Entwicklung und Lieferung der maritimen und landbasierten Einheiten beauftragt wurden.
Die dritte Säule ist die elektromechanische Fertigung. Wir bieten uns als EN9100-zerti-

Das russische Eletcronic EloKa-System Krasukha-4 beim Army Forum 2019

Foto: Vitaly V. Kuzmin / http://vitalykuzmin.net

Die Hornisse besteht aus mehreren Systeme für Electronic Warfare integriert in einen Transportpanzer Fuchs

Foto: Bundeswehr/Junge

fizierter Lohnfertiger an, der für den Kunden, gemäß seinen Vorgaben, digitale und elektromechanische Komponenten für die Luft- und Raumfahrt fertigt. Dabei handelt es sich um Chassis mit Leiterplatten, Kabelbäume, komplexe elektrische Schaltkästen. Um den Anforderungen von fliegenden Systemen gerecht zu werden, werden gefertigte Komponenten unter Spannung unterschiedlichen vorgeschriebenen Tests, wie Rüttel- und Thermaltests, unterzogen.
Um nicht ausschließlich vom Verteidigungsetat abhängig zu sein, sind wir auch in der Sicherheitsindustrie mit Schwerpunkt Öffentliche Sicherheit tätig. Hier nutzen wir die Entwicklungs- und Integrationsfähigkeiten der Wehrtechnik, um schlüsselfertige Lösungen und verdeckte Einbauten für BOS, Kriminalämter und Geheimdienste anbieten zu können. Um einige Beispiele zu nennen, wir bauen im Auftrag des Beschaffungsamtes des BMI seit nunmehr über zehn Jahren den BeDoKW für die beweis- und dokumentationssichere Videoanalyse während Massenveranstaltungen. Oder unser Akustikpanel, das wir für das Mitlauschen von Gesprächen in öffentlichen Umgebungen in verdeckten Ermittlungen entwickelt haben.

IT-Report: Welche EloKa-Systeme haben Sie bereits in die Bundeswehr gebracht?
Mariucci: Ein prominentes Beispiel ist der in der Truppe seit Jahrzehnten eingeführte ELINT-Sensor „RMB" auf geschützter Plattform. Wir haben hierbei den Sensor auf einen vollautomatischen Mast und mitsamt Steuerungstechnik in Kabine und Transportpanzer integriert.
Dasselbe haben wir für einen mobilen landgestützten HF-Jammer gemacht. Bei diesem System stammte der Sensor von THALES, der in eine gepanzerte Plattform zu integrieren war. Spätestens jetzt konnten wird beweisen, dass wir ein sensor- und plattformunabhängiger Integrator sind, der jegliche EloKa-Sensoren und Plattformen bedienen kann.
Unser jüngstes Beispiel ist MoGeFa, bei dem die Sensorik von der Firma Plath stammt und in minengeschützten Mehrzweckfahrzeugen des Modells YAK eingebaut wurden. Auch hier haben wir wieder unsere Unabhängigkeit von Plattformen und Sensoren bewiesen.

IT-Report: Welches wäre ein Beispiel aus dem Bereich Test & Validierung von Radar- bzw. EloKa-Sensoren?
Mariucci: Das aktuellste Projekt ist die wehrtechnische Ausrüstung des NATO JEWCS Stabs mit Test- und Ausbildungseinrichtungen auf See und Land. Teil der Aufgabe des NATO JEWCS Stabs besteht darin, alle NATO-Hauptquartiere und Kommandos in der Entwicklung der eigenen EloKa-Doktrin, Konzipierung und Umsetzung zu unterstützen. Unser Anteil liegt hierbei in der Lieferung von modularen EK-Simulatoren, Stimulatoren und Störgeräten in seegestützten Containern und robusten Radfahrzeugen. Damit sollen die Auswirkungen der neuesten elektronischen Kriegsausrüstung eines Feindes während Übungseinheiten simuliert werden. Sprich, es werden „feindliche Umgebungen" geschaffen, in denen verbündete Streitkräfte in der EloKa und insbesondere im Elektronischen Kampf ausgebildet werden.

IT-Report: Zurück zur Bundeswehr, wie können Sie beim Ausbau der EloKa-Fähigkeiten helfen?
Mariucci: Da sind wir ganz flexibel. Ob wir vor Ort mit Mitarbeitern oder Reservisten unterstützen sollen, ob es über Schulungen gehen soll oder über Dienstleistungen, ich bin für alle Möglichkeiten offen.

IT-Report: Wo sehen Sie die ELETTRONICA als Partner der Bundeswehr?
Mariucci: Ich sehe die ELETTRONICA als Unternehmen, das durchaus in Deutschland unsere Soldatinnen und Soldaten unterstützen kann, mit Fähigkeiten, die sehr schwer zu finden und auch gering vorhanden sind. Auch ich habe mich bereits in einer Reserveübung eingebracht.
Ich sehe mich als deutsches Unternehmen, das in der EloKa durchaus spezialisierte und moderne, wichtige Fähigkeiten erarbeitet hat, mit einer technologiekompetenten Muttergesellschaft in Europa. Diese im globalen Markt etablierte und erprobte Kompetenz können wir der Bundeswehr anbieten. Da spielt bzw. muss die ELETTRONICA, trotz ihrer mittelständischen Struktur und Größe, aufgrund ihrer Spezialisierung meines Erachtens nach eine sehr große Rolle spielen. Und diese Fähigkeiten dürfen wir in Deutschland nicht mehr verlieren. Die muss man kontinuierlich ausbauen.
Eine Konkretisierung als Schlüsselfähigkeit wäre sicherlich hilfreich, um die Kompetenzen auch hier in Deutschland zu halten. Schließlich handelt es sich bei unseren Mitarbeitern um wirkliche Fachkräfte, die sonst in Europa nur sehr schwer zu finden sind. Aufgrund dieses hohen Maßes an notwendiger Spezialisierung war der Westen auch davon ausgegangen, dass Russland sich nicht habe weiterentwickeln können. Aber Russland konnte sich ohne unsere Beachtung weiterentwickeln und wir müssen nun aufpassen, dass unsere Armeen in der EU und der NATO den Anschluss nicht komplett verlieren.

Das Interview führte Dorothee Frank.

Im Interview verwendete Abkürzungen:

BeDoKW	*Beweissicherungs- und Dokumentationskraftwagen*
BOS	*Behörden und Organisationen mit Sicherheitsaufgaben*
CIR	*Cyber und Informationsraum, militärischer Organisationsbereich der Bundeswehr*
EK	*Elektronischer Kampf*
ELINT	*Electronic Intelligence, Elektronische Aufklärung*
EloGM	*Elektronische Gegenmaßnahmen*
EloKa	*Elektronische Kampfführung*
EN9100	*Europäische Norm für Organisationen in der Luftfahrtindustrie, der Raumfahrt- und der Verteidigungsindustrie*
EW	*Electronic Warfare*
JEWCS	*Joint Electronic Warfare Core Staff*
MoGeFa	*Mobiles Geschütztes Fernmelde-aufklärungssystem*
WTD	*Wehrtechnische Dienststelle*

BWI
IT für Deutschland

BWI – Unterstützer der Digitalisierung der Bundeswehr

Frank Leidenberger, Dr. Michael Trampert, Holger Bonnen, Thomas Haber

Digitalisierung schreitet in unserer Gesellschaft voran, sie ist notwendig und wichtig. Gerade in der aktuellen Zeit zeigt sich ihre Bedeutung umso stärker. Ohne die bereits vorhandenen digitalen Möglichkeiten wäre die Aufrechterhaltung der Arbeitsfähigkeit von Unternehmen und öffentlichen Stellen in Krisenzeiten, wie wir sie gerade bedingt durch das Coronavirus erleben, in vielen Bereichen nicht oder zumindest nur sehr schwer möglich.

Aber Digitalisierung ist mehr als der bloße Erhalt der Arbeitsfähigkeit. Sie eröffnet in nahezu allen Lebensbereichen neue und teilweise zuvor nicht vorstellbare Möglichkeiten. Dies gilt in besonderem Maße auch für die Streitkräfte.
Daher treibt die Bundeswehr ihre Digitalisierung mit Nachdruck voran, um ihre nationale und internationale Handlungsfähigkeit langfristig zu erhalten und nachhaltig zu stärken – Digitalisierung ist und bleibt eines der wichtigsten Themen der Bundeswehr in dieser Dekade und sicherlich auch darüber hinaus. Digitale Transformation spielt eine Schlüsselrolle, wenn es darum geht, die Streitkräfte effizienter und effektiver zu machen, etwa bei der Beschaffung, dem Personalmanagement und nicht zuletzt bei administrativen Aufgaben oder in den unterschiedlichsten militärischen Anwendungsbereichen. Neben neuen Denkmustern und Herangehensweisen stellt die Digitalisierung auch neue Ansprüche an die IT-Infrastruktur und -Ausstattung der Akteure. Damit ist auch die BWI als Digitalisierungspartner der Bundeswehr gefordert. Sie muss diesen Wandel aktiv begleiten und die Streitkräfte zielgerichtet bei ihrer Digitalisierung unterstützen. Wichtig dabei im Auge zu behalten sind stets Mehrwert und Nutzen, die durch die Digitalisierung erreicht werden können.

Foto: Bundeswehr/Bienert

Mit D-LBO beschreitet die Bundeswehr auch im multinationalen Kontext den Weg zur vernetzten Gefechtsführung

Virtuelle Roboter entlasten Fachpersonal

So können bereits kleine Digitalisierungsvorhaben einen großen Mehrwert erzeugen. Beispielhaft kann hier robotergesteuerte Prozessautomatisierung (RPA) genannt werden. Dabei handelt es sich um virtuelle Roboter, also Software, die so programmiert wird, dass sie repetitive, administrative Arbeitsweisen am Computer anwendungsübergreifend nachahmt. RPA-Systeme werden für die digitale Automatisierung unkomplizierter, aber zeitaufwendiger Tätigkeiten genutzt. Dadurch befreit ein RPA-System Fachpersonal von zeitintensiven sowie fehleranfälligen Arbeiten und kann diese meist effizienter ausführen als der Mensch selbst.

Autoren

Frank Leidenberger, Chief Strategy Officer BWI GmbH; **Dr. Michael Trampert**, Programmleiter Digitalisierung GesVersBw BWI GmbH; **Holger Bonnen**, Programmleitung D-LBO BWI GmbH; **Thomas Haber**, Programmleitung D-LBO BWI GmbH.

Zusammen mit dem Luftfahrtamt der Bundeswehr entwickelte die BWI eine RPA-Lösung für das Ausstellen von Fallschirmsprunglizenzen, die erfolgreich im Pilotbetrieb läuft. Hier hat früher ein hoch qualifizierter Sachbearbeiter alle Daten, wie etwa bestandene Lehrgänge und Gesundheitstests, anhand einer Checkliste abgeglichen, manuell in eine Excel-Tabelle übertragen, für jeden Kandidaten einen neuen digitalen Ordner angelegt und nach erfolgreicher Prüfung das Lizenzdokument erstellt. Heute erledigt der virtuelle Roboter diese sich wiederholenden Vorgänge und kann verschiedene Office-Anwendungen, wie E-Mail, Excel und Adobe oder auch ERP-Systeme, miteinander verknüpfen. Für solche RPA-Systeme gibt es zahlreiche andere Anwendungsmöglichkeiten. Aktuell arbeitet die BWI daher an der Umsetzung für weitere Prozesse.

Digitalisierungsprogramm für vernetzte Operationsführung

Die Digitalisierung der Bundeswehr sorgt allerdings nicht nur für höhere Effektivität und Effizienz in der Administration. Auch auf dem Gefechtsfeld der Zukunft wird Digitalisierung eine wichtige Rolle spielen. Sie wird dabei über Informations-, Führungs- und Wirkungsüberlegenheit mitentscheiden. Hier gilt es, bei IT und Rüstung mit dem Voranschreiten der technischen Möglichkeiten Schritt zu halten – sowohl konventionell in den Dimensionen Land, Luft und See als auch im Cyber-Raum sowie in hybriden Bedrohungsszenarien. Neben Möglichkeiten zur Krisenfrüherkennung spielt an dieser Stelle die Digitalisierung landbasierter Operationen (D-LBO) eine wesentliche Rolle. Mit D-LBO beschreitet die Bundeswehr auch im multinationalen Kontext den Weg zur vernetzten Operationsführung.

Aufgrund der Bedeutung des Vorhabens für die Bundeswehr hat die BWI für D-LBO – neben Cloud-Computing und der Digitalisierung der Gesundheitsversorgung der Bundeswehr – in der eigenen Organisation ein sogenanntes Digitalisierungsprogramm eingerichtet. In diesen Programmen bündelt die BWI Digitalisierungsvorhaben, die von herausragender strategischer Bedeutung für die Bundeswehr sind. Sie alle kennzeichnet darüber hinaus, dass sie von erheblicher Komplexität sind, einen großen Architektur- und Konzeptionierungsbedarf haben und einen hohen Beratungsanteil aufweisen.

Battle Management System und Tactical Edge Networking

Ziel des Programms D-LBO ist es, alle Soldaten und Fahrzeuge auf dem Gefechtsfeld in einem mobilen, durchgängigen, interoperablen Verbund digital zu vernetzen – sowohl auf Landes- als auch auf Bündnisebene. Das soll unter anderem mit einem neuen Battle Management System (BMS) gelingen, das alle Teilstreitkräfte zukünftig gleichermaßen einbindet und Führungssysteme auf taktischer Ebene bis hin zum Einzelschützen vernetzt. Hier unterstützt die BWI die Bundeswehr mit der Serviceentwicklung, dem Rollout und dem Betrieb der Services. Im ersten Schritt soll das BMS im Deutschen Anteil der Very High Readiness Joint Task Force Land (VJTF(L)) 2023 der NATO Response Forces zum Einsatz kommen.

Darüber hinaus unterstützt die BWI die Bundeswehr beim Aufbau des bilateralen Programms „Tactical Edge Networking" (TEN) mit den Niederlanden. Im Zuge von TEN sollen die Landstreitkräfte beider Länder künftig auf allen Ebenen vernetzt und die Kräftedispositive der Streitkräfte mit neuen Fähigkeiten ausgerüstet werden. Geplant ist, jeden Panzer und jedes Fahrzeug beider Armeen zu vernetzen. Außerdem sollen die Soldaten mit modernem digitalem Equipment, unter anderem Smartphones und Funkgeräten, ausgestattet werden.

Die BWI wird bei diesen Vorhaben mit ihrer IT-Expertise und den Erfahrungen aus dem Umfeld des Projekts HERKULES unterstützen.

Ergänzt werden sollen Systeme und Netzwerke, wie sie im Rahmen von TEN entwickelt und aufgebaut werden, im Sinne des Internet of Things (IoT) künftig mit einem „Internet of Military Things". Als Schlagworte sind hier beispielsweise der bruchfreie Austausch georeferenzierter Daten in nahezu Echtzeit zwischen Sensoren und Effektoren sowie Führungs- und Waffeneinsatzsystemen, die Integration unbemannter Land- und Luftsysteme (UMS) im Rahmen des Manned-Unmanned-Teaming (MUM-T) sowie der Einsatz teilautonomer UMS-Schwärme zu nennen. Bis diese Technologien mit dem Ziel der Realisierung des „Sensor-to-Shooter"-Konzepts einsatzfähig sind, bedarf es allerdings noch zahlreicher gemeinsamer Anstrengungen von Bundeswehr, BWI und weiteren Partnern aus der Industrie.

Digitalisierung der Gesundheitsversorgung

Trotz einer zunehmenden Digitalisierung des Gefechtsfelds bleiben die Soldatinnen und Soldaten dennoch die wichtigste Stütze der Streitkräfte. Die Handlungsfähigkeit der Bundeswehr steht und fällt deshalb auch abseits des Gefechtsfelds mit einsatzbereitem Personal. Daher ist eine effektive und effiziente Gesundheitsversorgung essenziell. Aus diesem Grund hat das Bundesministerium der Verteidigung die „Digitalisierung der Gesundheitsversorgung der Bundeswehr" (Digitalisierung GesVersBw) zu einem Fokusthema ihrer Digitalisierungsoffensive gemacht. Anfang 2018 wurde das gleichnamige Programm ins Leben gerufen. Von dem Pilotvorhaben wird nicht nur für den Sanitätsdienst große Strahlkraft erwartet, sondern auch ein Ausblick auf ein mögliches Zielbild der IT-Architektur der Bundeswehr: weg von vielen, unabhängigen Einzellösungen, hin zu einer ganzheitlichen und übergreifenden Architektur. Damit nimmt der Sanitätsdienst eine Vorreiterrolle ein und weist den Weg für künftige Digitalisierungsvorhaben der Bundeswehr.

Eine Taskforce, die aus dem Kommando Sanitätsdienst der Bundeswehr, dem BAAINBw und der BWI besteht, setzt das Programm derzeit um. Auch diese Konstellation markiert neue Zeiten: Mit der Taskforce in Koblenz arbeiten erstmals Bedarfs-

Für Cloud-Dienste greift die Bundeswehr auf eine leistungsfähige Rechenzentrums-Infrastruktur zurück

Foto: BWI

Foto: BWI

Die Digitalisierung der Gesundheitsversorgung der Bundeswehr ist ein Fokusthema der Digitalisierungsoffensive des BMVg

träger, Bedarfsdecker und IT-Serviceprovider sprichwörtlich Hand in Hand – alle Beteiligten sitzen in benachbarten Büros unter einem gemeinsamen Dach. Diese räumliche Nähe soll dazu beitragen, dass entsteht, was die Leitung des BMVg als erklärtes Ziel ausgegeben hat: Architektur aus einem Guss.
Kern der Digitalisierung GesVersBw ist eine durchgehende, prozessorientierte Architekturerstellung, um unter anderem die Voraussetzungen für die Einführung elektronischer Gesundheitsakten zu schaffen. Dazu gilt es, das hochkomplexe Gesamtsystem, seine Informationsbedarfe und seine operationellen Anforderungen sowie die bestehende IT-Landschaft in einer ganzheitlichen Enterprise Architecture zu erfassen und abzubilden. Erst danach kann die Gesundheitsversorgung der Bundeswehr inklusive ihrer IT-Systemarchitektur und zugehöriger IT-Projekte übergreifend ausgeplant und schließlich umgesetzt werden.

Erweiterte Infrastruktur für den Sanitätsdienst

Die Digitalisierung GesVersBw kann hier bereits erste greifbare Ergebnisse vorweisen. So wurde etwa Ende 2018 im Bundeswehrkrankenhaus Berlin die erste Anlage aus dem Projekt „MedSAN" in Betrieb genommen. Jedes MedSAN-System besteht aus einem Storage Area Network (SAN), einem Netzwerk für die Speicherung und Übertragung von Daten, sowie einer hochleistungsfähigen Serverfarm. Damit erhöhen sich in den Krankenhäusern nicht nur die Daten- und Ausfallsicherheit, sondern auch die Übertragungsgeschwindigkeiten deutlich. Nach Berlin folgte die Ausstattung der anderen Bundeswehrkrankenhäuser sowie der Sanitätsakademie der Bundeswehr in München, so dass das Rollout-Projekt bereits 2019 erfolgreich abgeschlossen werden konnte.

Nicht nur bei diesem Projekt, sondern generell ist die Gesundheitsversorgung der Bundeswehr auf verlässliche Übergänge und Schnittstellen zwischen IT-Systemen und Netzwerken angewiesen, beispielsweise bei der Zusammenarbeit in der regionalen Notfallversorgung sowie Forschungsverbünden und bei zivil-militärischen Kooperationen. Ebenso bedarf es eines rechtskonformen, bedarfsgerechten, interoperablen und zeitgemäßen Informations- und Datenmanagements. Diese Aufgabe soll künftig das geplante Health Information Management System (HIMS) übernehmen. Das IT-System gilt als Kernelement für die Digitalisierung der bundeswehreigenen Gesundheitsversorgung. HIMS bündelt und verarbeitet alle Gesundheitsdaten und stellt aggregierte Informationen bedarfsgerecht bereit, zum Beispiel in Form der geplanten elektronischen Gesundheitsakte der Bundeswehr.

Innovation für die Bundeswehr

Die Entwicklung des HIMS stellt für Bundeswehr und BWI einen Blick in die nähere Zukunft dar. Die BWI blickt für die Streitkräfte aber bereits auch auf mögliche Entwicklungen in der etwas weiteren Zukunft. Mit dem Innovation Management und dem Cyber Innovation Hub, der sich bewährt hat und nach seinem Pilotbetrieb seit Anfang des Jahres als Teil der BWI verstetigt wurde, beobachtet die BWI vielversprechende technologische Entwicklungen und das Startup-Umfeld. Dabei liegt das Augenmerk stets darauf, neue und eventuell disruptive Technologien auf ihren Nutzen für die Bundeswehr zu prüfen.
So befasst sich ein Experiment, das aktuell mit der Luftwaffe erprobt wird, mit virtuellen Lageräumen und Lagebesprechungen. Hier treten die Teilnehmer einer Lagebesprechung einem virtuellen 3D-Raum bei und interagieren in diesem mit den neuen Möglichkeiten der Virtual-Reality-Technologie. Im VR-Raum können beispielsweise ein virtuelles Whiteboard und eine sprachliche Protokollierung gemeinsam genutzt werden. Die erarbeiteten digitalen Ergebnisse werden gesichert, um sie in der Folge weiter zu verarbeiten.
Ein konkretes Szenario für diesen VR-Einsatz ist der Lufteinsatzbefehl (Air Tasking Order, ATO) der Luftwaffe, der im Experiment erprobt wird. Dieser enthält die erforderliche detaillierte Planung, um die Aktionen verschiedenster Akteure zu integrieren und zu koordinieren. Er beinhaltet die genauen Aufgaben für jedes einzelne Luftfahrzeug nach Kennnummer gegliedert und liefert die Informationen, die für deren Zusammenarbeit notwendig sind. Im Experiment werden Einsatzlagebesprechungen unter Nutzung von VR-Technologie und speziell aufbereiteten interaktiven Lagekarten durchgeführt. Auf diese Weise sollen Abstimmungen mit dislozierten Luftfahrzeugbesatzungen bei Lagebesprechungen erleichtert und beschleunigt werden.
Virtual Reality ist an dieser Stelle nur ein Beispiel, wie moderne Technologien einen Mehrwert für die digitalisierte Bundeswehr bieten können. Daher ist neben dem stabilen und sicheren Betrieb sowie der Weiterentwicklung der bestehenden Services der Blick in die Zukunft auch weiterhin ein wichtiger Baustein im Portfolio der BWI. Erst beides zusammen ermöglicht es der BWI, der für sie wichtigsten Aufgabe nachzukommen: die Bundeswehr auf dem Weg zu ihrer Digitalisierung bestmöglich zu begleiten und zu unterstützen.

BWI
IT für Deutschland

BWI GmbH
Lutz Emmelmann
External Communications & Marketing
Auf dem Steinbüchel 22
53340 Meckenheim
info@bwi.de
www.bwi.de

Bundeswehr Cyber Innovation Hub

Dr. Kai Wittek, Barbara von Wnuk-Lipinski

Mit seinem Auftrag – Accelerating Innovation to our Soldiers – bringt der Bundeswehr Cyber Innovation Hub seit 2017 Innovationen schneller in die Hand von Nutzern in der Bundeswehr und arbeitet hierzu eng mit Startups zusammen.

Der Bundeswehr Cyber Innovation Hub (CIHBw) ist die Digital Innovation Unit (DIU) des Bundesministeriums der Verteidigung und fungiert als Schnittstelle zwischen Bundeswehr und Startup-Ökosystem. Sein Auftrag ist es, die digitale Transformation zu unterstützen. Seine Mission richtet sich am Bedarf der Soldatinnen und Soldaten und zivilen Mitarbeiterinnen und Mitarbeiter im Geschäftsbereich des Bundesministeriums der Verteidigung (BMVg) aus. Deren Arbeit soll durch innovative Ideen und Lösungen aus der Startup-Welt unterstützt und erleichtert werden.

Dies realisiert der CIHBw durch verschiedene Maßnahmen:

- Er identifiziert Produkt- und Serviceinnovationen und validiert diese zusammen mit militärischen Nutzern, um sie ggf. zur Einführung in die Bundeswehr vorzuschlagen.
- Er befördert eine Innovationskultur in der Bundeswehr, indem er die Soldatinnen und Soldaten zu Intrapreneuren befähigt und diese bei der Weiterverfolgung ihrer Ideen unterstützt.
- Er schafft eine Infrastruktur zwischen Truppe und relevanten Playern aus dem Startup-Ökosystem sowie zivilen und militärischen Experten aus Wissenschaft und Technik und stellt den Know-how-Transfer zwischen den unterschiedlichen Stakeholdern sicher.

Die Säulen des Bundeswehr Cyber Innovation Hub

#STARTUP ENGAGEMENT	▪ Identifikation von relevanten Anwendungsfällen und marktverfügbaren Produkten von Startups ▪ Fokus auf dual-use ▪ Projekt werden gemeinsam mit Nutzer durchgeführt ▪ Motto: Schnell und in kleinem Umfang den realen Nutzwert für die Soldatinnen und Soldaten testen
#INTRAPRENEURSHIP	▪ Befähigung von Soldatinnen und Soldaten sowie zivilen Mitarbeiterinnen und Mitarbeitern der Bundeswehr zu Defense Intrapreneurs durch --> Ausbildung in agilen Methoden sowie --> Unterstützung bei Problemanalyse, Use Case-Definition, MVP-Building und Validierung ▪ und dadurch Beitrag zu einem Kulturwandel in der Bundeswehr hin zu mehr Innovationsbereitschaft und unternehmerischem Denken.
#Communications & Strategic Partnerships	▪ Aufbau eines Netzwerkes im internationalen Innovations-Ökosystem und mit anderen DIUs ▪ Kommunikation der Ergebnisse, um den digitalen Wandel der Bundeswehr zu fördern

Grafik: CIHBw

Soldat des CIHBw im VR-Segelflugsimulator

Foto: Bundeswehr Kraatz

Autoren

Dr. Kai Wittek ist Reservist im Bundeswehr Cyber Innovation Hub (CIHBw). **Barbara von Wnuk-Lipinski,** Leiterin Communications & Strategic Partnerships CIHBw, Member of the Management Board.

Fotos: BWI/Diehle

Verteidigungsministerin Annegret Kramp-Karrenbauer bei der MSC Innovation Night 2020

Mit seiner Gründung im Jahr 2017 war der CIHBw eine der ersten DIU im öffentlichen Sektor in Europa. Seit Anfang 2020 ist der CIHBw als Innovationseinheit in der BWI verstetigt, als Abteilung mit eigener Geschäftsordnung, strategisch gesteuert durch das BMVg und dessen Staatssekretär Benedikt Zimmer.
Der CIHBw arbeitet nach den Arbeitsprinzipien erfolgreicher DIUs, d.h. konkret, nicht nur mit Startups zu agieren, sondern selbst wie ein Startup zu arbeiten. Treiber ist dafür die Innovationsadaption und die Überwindung von Innovationshemmnissen. Hierbei handelt es sich um eine systematische Wertschöpfung, die durch den professionellen Einsatz agiler Methoden wie Scrum, UX-Design, oder Design-Thinking eine kollaborative Innovationskultur schafft.

Beschleunigung von Innovationen

Der Auftrag des CIHBw wird durch die Teams „Startup Engagement", „Intrapreneurship" und „Communications & Strategic Partnerships" realisiert.

Startup Engagement

Das Team Startup Engagement (SuE) hat zum Ziel, marktverfügbare Lösungen aus dem internationalen Startup-Ökosystem für bundeswehrspezifische Use Cases durch zügige Innovationsvorhaben zusammen mit militärischen Nutzern aus dem Geschäftsbereich des BMVg zu erproben und zu bewerten. Das Team SuE übernimmt im Rahmen eines gemeinsamen Projektes mit einem militärischen Nutzer die Steuerung der Innovationsvorhaben von der Initiierungsphase über die Durchführung bis zur potentiellen Übergabe an den Bedarfsträger innerhalb der Bundeswehr. Produkt- und Serviceinnovationen werden getestet, der Nutzwert schnell und iterativ validiert und die Lösung entweder für eine breite Einführung in die Bundeswehr empfohlen oder als noch nicht reif bzw. mit unzureichendem Nutzwert bewertet.

Intrapreneurship

Das Team Intrapreneurship (IPS) verfolgt das Ziel, Soldatinnen und Soldaten sowie zivile Mitarbeiterinnen und Mitarbeiter aus dem Geschäftsbereich des BMVg zu Defense Intrapreneuren zu befähigen und sie bei der Weiterentwicklung ihrer Ideen zu unterstützen. Damit diese „wie ein Unternehmer im Unternehmen" agieren können, sorgt das Team IPS gegebenenfalls für die erforderliche Ausbildung in agilen Methoden, die Zusammenarbeit mit Startups oder auch die Ausstattung mit nötiger Hard- und Software. Auch das „Freischaufeln zeitlicher Ressourcen" wird durch das Team IPS in enger Absprache mit den zuständigen Vorgesetzten übernommen. IPS trägt auf diese Weise nicht nur zu Problemlösungen „für die Truppe durch die Truppe", sondern auch zu einem Kulturwandel in der Bundeswehr hin zu mehr Innovationsbereitschaft und unternehmerischem Denken bei.

Communications & Strategic Partnerships

Das Team Communications & Strategic Partnerships (CSP) hat das Ziel, sich mit zivilen und militärischen Innovationstreibern auftragsbezogen über Best Practices und militärische Use Cases auszutauschen. Unterstützt wird die Auftragserfüllung des CIHBw durch das Schaffen eines Netzwerks im nationalen und internationalen Innovations-Ökosystem durch Verknüpfung zu Stakeholdern in der Bundeswehr, um als Innovationsführer und Treiber von Change in der Bundeswehr wahrgenommen zu werden. Gleichzeitig trägt das Team auf diese Weise dazu bei, dass die Bundeswehr in der Außenwahrnehmung als wichtiger Partner in den Bereichen Innovation und Digitalisierung anerkannt wird.

Das Portfolio des Bundeswehr Cyber Innovation Hub

Da der CIHBw allen militärischen Organisationsbereichen – Heer, Marine, Luftwaffe, Cyber- und Informationsraum, Streitkräftebasis und Sanität – offensteht, wird ein breites Themenspektrum bearbeitet. Es gibt keine thematischen Vorfestlegungen, der Nutzen muss aber im Kern durch eine digitale Lösung getrieben sein. Beispielsweise wurde und wird im Rahmen von Innovationsvorhaben an Apps, digitalen Plattformen, Virtual-Reality, Sensor-Fusion oder auch Mesh-Networking gearbeitet.

Erfolgsfaktor Nutzer

Alle Aktivitäten des CIHBw sind am Anwendungsfall der Nutzerinnen und Nutzer ausgerichtet und es gilt: a) Alle Projekte werden ausschließlich mit der Truppe und mit konkretem Anwendungsfall durchgeführt sowie b) Innovationen immer gemeinsam vorangetrieben.
Nur in dieser engen Interaktion kann die richtige Lösung gefunden und deren Nachhaltigkeit gesichert werden.

Erfolgsfaktor Kultur

Die Arbeitsweise orientiert sich an erfolgreichen Startups und Scaleups – Agilität, Scrum, Lean-Startup, schnelle Iterationen, fachübergreifende Teams sind gelebte Praxis. Der CIHBw dient damit auch als Labor und „Do-Tank", um Best-Practices des Startup-Ökosystems für die Bundeswehr zu vermitteln. Hierzu ist eine Eigenständigkeit und das Arbeiten außerhalb etablierter Prozesse unbedingt erforderlich.

Erfolgsfaktor Team

Ein wesentlicher Garant der Innovationsfähigkeit des CIHBw sind die ca. 40 Mitarbeiterinnen und Mitarbeiter. Das Team ist zivil und militärisch besetzt, wobei der Großteil der Soldatinnen und Soldaten Reservistendienstleistende sind.
Es ist gelungen, Entrepreneure aus dem Startup-Ökosystem und der Digitalwirtschaft zu gewinnen und ein Netzwerk aus Angehörigen der Reserve im Sinne eines Verstärkungselements zur Unterstützung der digitalen Transformation aufzubauen. Die Erfahrungen aus Startups kombiniert mit Expertinnen und Experten u.a. aus Projektmanagement, Entwicklung oder digitaler Transformation sowie den Intrapreneurinnen und Intrapreneuren aus der Bundeswehr bieten eine einzigartige Basis, um die Mission „Accelerating Innovation to our Soldiers" zu erfüllen. ■

Mitglieder des Projektteams der Innovation Challenge Einsatzflottile 1, mit der das Intrapreneurship Team des CIHBw 2019 startete

Foto: CIHBw

Die Innovationslandschaft der Bundeswehr

Dr. Simon Vogt

Die Umsetzungsstrategie „Digitale Bundeswehr" orchestriert die einzelnen Innovationsvorhaben im Geschäftsbereich des BMVg. Damit wird eine Grundlage für ein innovatives Ökosystem geschaffen – was folgt daraus für die Sicherheits- und Verteidigungsindustrie?

Digitale Bundeswehr als strategisches Ziel

Spätestens mit der Bekanntgabe der Aufstellung des militärischen Organisationsbereiches „Cyber- und Informationsraum" im Jahr 2015 schärfte sich im Geschäftsbereich des BMVg das Bewusstsein für die Notwendigkeit einer Umsetzungsstrategie für Digitalisierung in der Bundeswehr. Diese wurde im Frühjahr 2019 erlassen, definiert den Zielzustand der digitalen Transformation und spannt die entsprechende Roadmap auf, die in den drei Reifegraden

- Aktivieren,
- Umsetzen, Systematisieren & Ausprobieren,
- Gestalten & Weiterentwickeln

konkretisierende Maßnahmen für die digitale Transformation der Streitkräfte und ihrer Verwaltungsorganisation beschreibt

Autor

Dr. Simon Vogt, Startup Engagement, Bundeswehr Cyber Innovation Hub.

Diese Innovationseinheiten gibt es schon heute

Unter dem Reifegrad „Umsetzen, Systematisieren & Ausprobieren", der den Blick auf das Jahr 2020 und 2021 richtet, steht neben dem weiteren Lernen auch das Fortsetzen begonnener Digitalisierungsaktivitäten und die Analyse derer Wirkung im Zentrum der Betrachtung. Im Geschäftsbereich des BMVg sind dabei vor allem der Bundeswehr Cyber Innovation Hub und das Forschungsinstitut CODE an der Universität der Bundeswehr (UniBw) München als „wesentliche Innovationselemente" vorgesehen. Letzteres hat sich seit seiner Gründung in 2013 als Projektkoordinator des Konsortiums „Concordia" etabliert, welches beabsichtigt, für die EU den Aufbau von Cybersecurity-Kompetenzzentren voranzubringen. Darüber hinaus wird CODE

in Zusammenarbeit mit IBM als Nukleus für Quantentechnologie (Q Hub) weiterentwickelt und begründet somit neben der Cybersecurity einen weiteren Expertisepfad im akademischen Umfeld.
Der Bundeswehr Cyber Innovation Hub (CIHBw) ergänzt daneben einen zusätzlichen Schwerpunkt: Hier werden in erster Linie Technologien und Entwicklungen betrachtet, die bereits ihre Marktreife erlangt haben oder kurz davor stehen. Im Zentrum stehen Lösungen mit innovativen Ansätzen von jungen Unternehmen/Startups. Der CIHBw wurde mit dem Jahreswechsel innerhalb der BWI GmbH verstetigt, zuvor war er als zeitlich befristetes Pilotprojekt angelegt. Durch das HERKULES-Folgeprojekt hat die BWI den Auftrag erhalten, ein eigenes Innovation Management aufzubauen. Diese Aufgabe wird mit dem CIH innerhalb der BWI in der Abteilung „Innovation & Technologie" innovative Ideen und neueste Technologien der Bundeswehr und weiteren Kunden aus dem öffentlichen Sektor bereitstellen.

Foto: Bundeswehr

Bundeswehr und Startups im Austausch

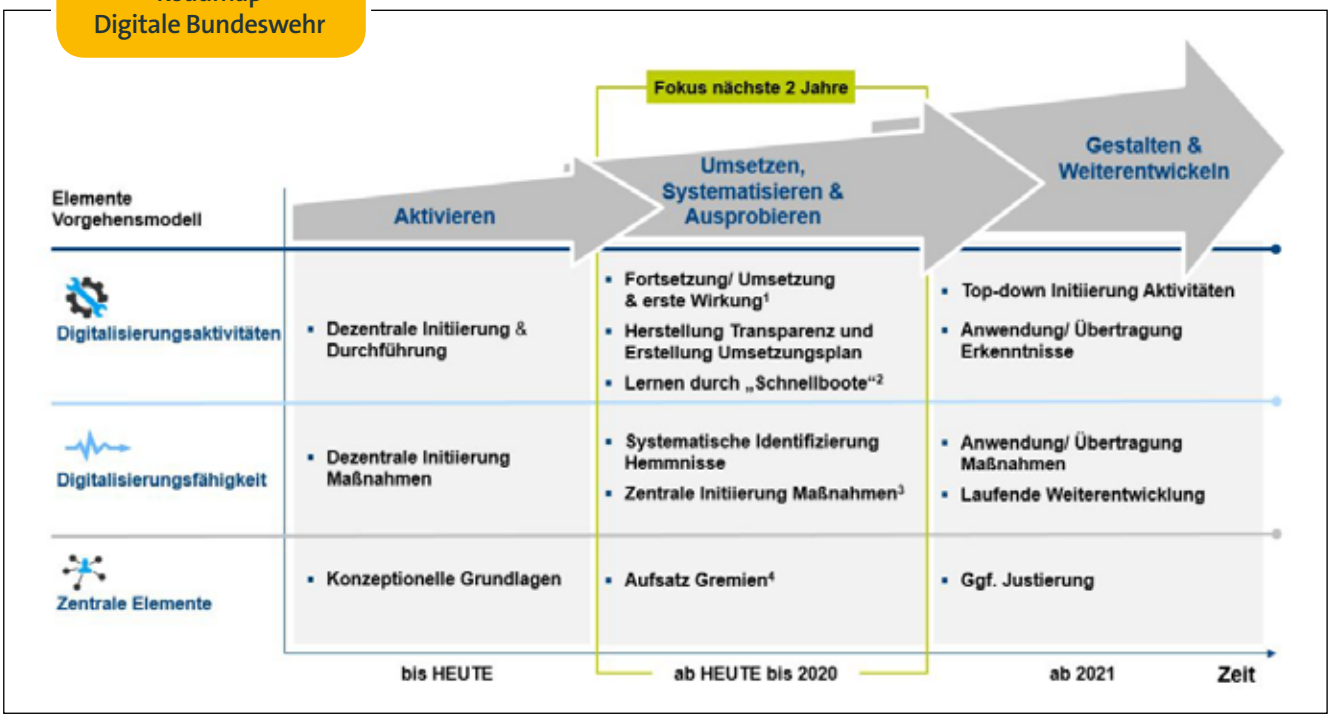
Nächste Schritte

Neben diesen bereits existierenden Innovationseinheiten wird in den kommenden zwei Jahren die Cyber-Agentur (im Verbund mit dem BMI) Forschungsvorhaben Im Blick haben, die im Kontext der gesamtstaatlichen Sicherheitsvorsorge insbesondere in Bezug auf Schlüsseltechnologien einen strategischen Vorteil bieten können.

Produkte des CIHBw oder der Cyber-Agentur in Bezug auf die Digitalisierung landbasierter Operationen sollen künftig auch im „TestBed" zusammen mit Opera-

Roadmap Digitale Bundeswehr

Grafik: Umsetzungsstrategie Digitale Bundeswehr



teuren und Technologieexperten getestet und realisiert werden können. Technische Innovationen sollen für Nutzer zudem in der Digitalgalerie erfahr- und erlebbar gemacht werden und einen Kanal öffnen, um das resultierende Feedback in die Entwicklung einfließen zu lassen.
Mit den verschiedenen Methoden und Schwerpunktsetzungen der genannten Innovationseinheiten steht der Bundeswehr in naher Zukunft ein Werkzeugsatz zur Verfügung, mit dem sich technologische Innovationen in ihren verschiedenen Reifegraden von der Grundlagenforschung, Entwicklung, Projektierung und Evaluierung gemeinsam mit dem Nutzer fördern und voranbringen lassen.

Der Weg zu einem Innovationsökosystem in der Verteidigungsbranche

Diese Ansätze von Seiten des BMVg und BMI schaffen die Voraussetzungen dafür, dass junge Unternehmen und technische Innovationen entdeckt und vorangetrieben werden können. Dieses ist eine notwendige jedoch allein nicht ausreichende Voraussetzung für das Entstehen eines Innovationsökosystems im Verteidigungssektor in Deutschland. Hierbei ist es jedoch nicht nur Aufgabe des öffentlichen Sektors als Bedarfsträger, ein Umfeld zu schaffen, in dem Innovationszyklen kurz sind und die Nutzbarmachung relevanter Ansätze und Technologien möglichst schnell und barrierefrei gelingen kann.
Die Konflikte der Zukunft werden sich vor allem auch in der Cyber-Domäne wiederfinden. Um hier gut gewappnet zu sein, sind langfristige und großvolumige Rüstungsprojekte zu komplexen Waffensystemen zu ergänzen um schnelle Innovationsprojekte. Dies erfordert auch einen Ökosystemgedanken in der Sicherheits- und Verteidigungsindustrie, der Startups und innovativen Ideen von kleinen Unternehmen nicht nur Raum gibt, sondern diese auch aktiv als Partner einbezieht und das unternehmerische Potential sowie die kurzen Entstehungszyklen neuer Entwicklungen aus jungen KMU nutzt. ■

Digital Innovation Units als Katalysator für den Fortschritt

Dr. Stephanie Khadjavi

Lange Zeit war der militärische Sektor Treiber wesentlicher Innovationen. Manche der dort entstandenen bahnbrechenden Neuerungen fanden in der Folge Eingang in den zivilen Sektor und prägen bis heute unseren Alltag. Das gilt beispielsweise für das Internet, das als „Arpanet" durch die militärische U.S.-Einheit ARPA (heute: DARPA) in den 1960er-Jahren seinen Anfang nahm, aber auch für das Ortungssystem GPS, das heute in jedem Smartphone genutzt wird.

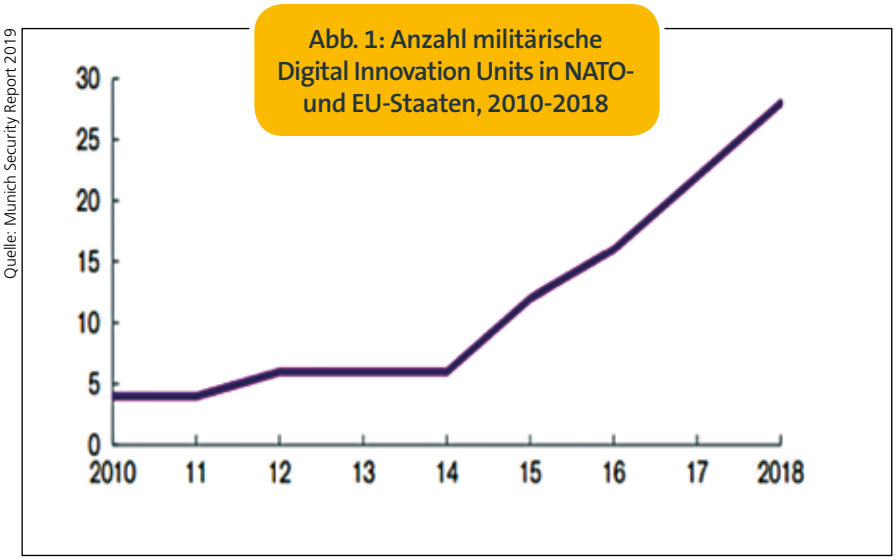
Zwischenzeitlich hat das Blatt sich gewendet. Die Staatsquote an den gesamten U.S.-amerikanischen Ausgaben für Forschung und Entwicklung (F&E) fiel zwischen 1960 und 2016 von 65 Prozent auf 24 Prozent, gleichzeitig hat sich der Unternehmensanteil an F&E von 33 Prozent auf 67 Prozent mehr als verdoppelt (vgl. Congressional Research Service). Gegenwärtig ist der Verteidigungssektor in vielen Themen gegenüber dem Technologiefortschritt der zivilen Welt im Rückstand. Insbesondere bei Software und Elektronik sind die Innovationszyklen im „Consumer"-Markt viel kürzer. Weiterhin treibt die Kostenreduktion durch Skaleneffekte Technologie in neue Anwendungen. Häufig sind die Anwendungen auch „dual use" geeignet, das heißt zivil und militärisch.

Militärische Innovationseinheiten weltweit auf dem Vormarsch

Mit der Gründung militärischer Innovationseinheiten, sogenannter „Digital Innovation Units" (DIUs) reagieren Partner und Verbündete auf die Erkenntnis, dass die Aufrechterhaltung der Wehrfähigkeit nicht allein durch etablierte Innovationsaktivitäten gewährleistet werden kann (vgl. Abb. 1). Dabei handelt sich um einen globalen Trend, der nicht auf NATO- und EU-Staaten begrenzt ist. Besonders hervorzuheben ist die „Startup-Nation" Israel. Hier antwortet das Militär auf die spezifische Sicherheitslage mit einem breiten Spektrum an Innovationsinitiativen und -programmen, vielfach organisiert in DIUs. Und das mit großem Erfolg: Zahlreiche Gründer nutzen ihr militärisch erworbenes Wissen und waren vorher in der Unit 8200. Im Thema Cybersecurity zählt Israel zu den weltweit führenden Ländern.

Autor

Dr. Stephanie Khadjavi, Communications & Strategic Partnerships, Bundeswehr Cyber Innovation Hub, und Ansprechpartnerin für Startups und Unternehmen.



Quelle: Munich Security Report 2019

Abb. 1: Anzahl militärische Digital Innovation Units in NATO- und EU-Staaten, 2010-2018

Zusammenarbeit mit Startup-Ökosystem

Die Idee der Etablierung separater DIUs zur digitalen Transformation von Großorganisationen ist nicht neu. Sie geht auf Clayton Christensen und seinen Bestseller „The Innovators Dilemma" (1997) zurück. Allgemein bezeichnen DIUs institutionalisierte Innovationseinheiten von Großorganisationen. Zu ihren spezifischen Ausprägungen zählen Innovation Hubs, Innovation Labs, Inkubatoren, Akzeleratoren, Company Builder oder Corporate Venture Capital. Die Vision dabei ist stets die gleiche: Als kleine, flexible Schnellboote sollen DIUs radikale Innovationen in den trägen Tanker, die Kernorganisation, bringen. Dabei setzen DIUs auf die Zusammenarbeit mit Startups aber auch auf Startup-Methoden und -Talente. Es geht nicht darum, bestehende Produkte, Prozesse oder Geschäftsmodelle schrittweise zu verbessern. Vielmehr sollen sie dazu beitragen, kreative Zerstörung im Schumpeterschen Sinne zuzulassen, um etwas vollkommen Neues zu erschaffen. Im Anschluss der Innovationsentwicklung steht die Herausforderung der Übergabe zurück ins Mutterschiff.

Name DIU	Gründung	Beitrag zur Landesverteidigung	Phase im Innovationslebenszyklus	Finanzierung
Defense Advanced Research Projects Agency (DARPA)	1958 als ARPA	Entwicklung neuer strategische Opportunitäten querbeet jeglicher militärischer Belange in ca. 250 parallel laufenden Projekten	Frühphase des Innovationszyklus	Über USD 3,4 Mrd. Budget p.a., finanziert durch das Department of Defense (DoD, Verteidigungsministerium)
Strategic Capabilities Office (SCO)	2012	Ermittlung neuer, innovativer Wege zur Nutzung bereits bestehender Technologie- und Waffensysteme	Spätphase; Neuverwertung bereits bestehender militärischer Technologien	Das für 2019 geplante Budget lag bei USD 1,5 Mrd. finanziert durch das DoD
Defense Innovation Unit (DIU)	2015 als DIUx	Test von „dual use“ Produkten von Unternehmen/Start-ups aus dem zivilen Sektor für militärische Anwendungsfälle	Spätphase mit bereits existentem „proof of concept“ und schneller Kommerzialisierung	Sprunghafte Budgetsteigerung auf zuletzt USD 71 Mio. (2019), finanziert durch das U.S. Army Contracting Command
National Security Innovation Network (NSIN)	2016 als Military District 5	Unterstützung von Entrepreneurship zur Entwicklung und Kommerzialisierung sicherheitskritischer Technologien mittels Bereitstellung von Tools, Trainings, Infrastruktur, Netzwerk etc.	Frühphase, Ideation, Design und Talententwicklung	Das für 2019 geplantes Budget lag bei USD 25,5 Mio. finanziert durch das DoD
SOWERX (Special Operation Forces Works)	2015	Förderung der Zusammenarbeit der besten Köpfe aus Industrie, Wissenschaft und Staat zur Lösung fordernder Spezialprobleme	Mittlere bis späte Phase des Innovationszyklus, dem agilen Design von Lösungen, dem schnellen „proof of concept“ und dem Austesten bestehender Technologien	USD 2 Mio. finanziert aus dem US Special Operation Command Budget (US SOCOM)
AFWERX	2017 (nach Vorbild SOWERX)	Verbesserung der Leistungsfähigkeit der U.S. Air Force durch die Vernetzung von Innovatoren, Vereinfachung von Technologietransfer und Beschleunigung von Ergebnissen (u.a. mittels eines Startup-Accelerator)	Mittlere bis späte Phase des Innovationszyklus, dem agilen Design von Lösungen, dem schnellen „proof of concept“ und dem Austesten bestehender Technologien	USD 11 Mio. finanziert von der US Air Force
In-Q-Tel (IQT)	1999	Förderung strategischer Vorteile für die USA durch Investitionen in neueste Technologien im Bereich Verteidigung und Nachrichtendienst (gemeinsam mit privaten Venture Capital-Gesellschaften)	Investitionen in alle Startup-Phasen von Seed bis Series C/D Finanzierungsrunden	Information nicht öffentlich zugänglich, in 2014 waren es USD 84,3 Mio., finanziert von der CIA

Grafik: Bundeswehr Cyber Innovation Hub

Abb. 2: Die U.S.-DIUs decken ein breites Spektrum ab (ausgewählte DIUs)

Fokus liegt auf radikalen Innovationen

Das darauf aufbauende Konzept der dualen Transformation – inkrementelle Innovation im Kernunternehmen, radikale Innovation in Satelliteneinheiten – ist in den USA längst etabliert und in der vergangenen Dekade auch bei deutschen Großunternehmen angekommen. Fast alle Dax-30-Unternehmen betreiben inzwischen eine oder mehrere DIUs. Zu den bekannteren zählen hub:raum (Deutsche Telekom), die BMW Startup Garage, Daimler Lab1886, der Lufthansa Innovation Hub, next 47 (Siemens) oder SAP.iO. Rund die Hälfte der Dax-30-DIUs sind Acceleratoren.

Vorbild USA

Im militärischen Sektor dominieren die USA: Sie nehmen sowohl im Hinblick auf Anzahl als auch auf Budget eine Spitzenposition im Thema militärischer DIUs ein. Deren Großteil wurde erst in der jüngeren Vergangenheit ins Leben gerufen; die verfolgten Ansätze divergieren stark und decken das gesamte Spektrum des Innovationszyklus ab (vgl. Abb. 2). In Europa sind vor allem die DIU-Aktivitäten von Frankreich (z.B. DGA, Defence Innovation Agency, Definvest) und Großbritannien (z.B. Defence and Security Accelerator, JHub) zu nennen.

Vorreiter in Deutschland ist der Bundeswehr Cyber Innovation Hub (CIHBw). Er wurde 2017 gegründet als Schnittstelle zwischen Startup-Ökosystem und Bundeswehr. Seine Mission ist es, digitale Innovationen schneller in die Truppe zu bringen und dabei Soldatinnen und Soldaten in den Mittelpunkt des Innovationsgeschehens zu stellen (dem CIHBw ist in diesem Heft ein eigener Beitrag gewidmet, vgl. S. 20.) Eine weitere deutsche DIU-Initiative ist die Cyberagentur, welche sich in der Aufstellung befindet.

Herausforderung Umsetzungsgeschwindigkeit

Eine Blaupause für militärische DIUs gibt es bislang nicht. Generell ist die Spanne ihrer konkreten Ausgestaltung breit, hängt von den nationalen Rahmenbedingungen ab und setzt an verschiedenen Phasen im Innovationslebenszyklus an. Die wesentliche Herausforderung aller DIUs ist die Umsetzungsgeschwindigkeit – in der Experimentier- und Bewertungsphase sowie in dem späteren Ausrollen der Innovation in die Breite. „Accelerating Innovation to our Soldiers“ muss Anspruch aller militärischen Organisationen sein. ■

Das Projekt Transition des Bundeswehr Cyber Innovation Hub

Foto: Bundeswehr Cyber Innovation Hub

Interview mit Dinah Rabe,
Strategy,
Member of the Management Board,
Bundeswehr Cyber Innovation Hub

IT-Report: Seit Beginn dieses Jahres ist der Cyber Innovation Hub eine Abteilung der BWI – was hat sich für Sie verändert?
Rabe: Um zu verstehen, was genau dieser Übergang eigentlich bedeutet, muss ich etwas weiter ausholen: Die Idee für den Hub wurde 2016 im Ministerium geboren. Um das damalige Momentum zu nutzen und nicht Monate mit der Gründung einer GmbH „zu verlieren", startete man den Hub als eigenständiges Projekt unter der inhaltlichen Leitung des BMVg und nutzte die BWI als administratives Element. Jetzt, als offizielle und ordentliche Abteilung der BWI, werden für uns die Regelungen und Prozesse der BWI verbindlich und wir unterliegen der Weisung und Steuerung der BWI-Geschäftsführung.

IT-Report: Sie sind von der Struktur und Kultur eher wie ein Startup, die BWI ist mit mehr als 5.000 Mitarbeitern deutlich größer – treffen da nicht zwei Welten aufeinander, die unterschiedlicher nicht sein können?
Rabe: Natürlich treffen gerade unterschiedliche Kulturen aufeinander. Es gehört zu unserem Auftrag als Innovationseinheit, ständig den Status Quo und bestehende Prozesse in Frage zu stellen. Wir brauchen flexible Strukturen, mit denen wir bei Bedarf schnell unsere Marschrichtung ändern können. Das Motto lautet „Done is better than perfect". Dieses Motto kann und sollte natürlich nicht für einen Geschäftsauftrag gelten, der sich mit kritischer Infrastruktur der Bundewehr auseinandersetzt.
Wir sind aber der Überzeugung, dass diese Diskrepanz nicht unbedingt etwas Negatives sein muss! Grundsätzlich muss man sagen, und da sind sich alle Agilitätsexperten einig, dass es absolut nicht sinnvoll ist, alle Prozesse und Aufgaben agil zu organisieren. Auch in unserer Einheit werden Finanzen nicht agil geplant, und auch in der BWI gibt es natürlich schon andere Einheiten die agil und flexibel arbeiten. Die unterschiedlichen Kulturen dienen einfach nur unterschiedlichen Zwecken. Übrigens ist die BWI mit dieser Herausforderung kein Sonderfall. Jede größere Unternehmung, die unter einem Dach unterschiedliche Ziele verfolgt, beispielsweise Stabilität und Innovation, steht vor der Aufgabe diesen Spannungsbogen auszubalancieren.

IT-Report: Was erhoffen Sie sich von der Integration des Cyber Innovation Hub in die BWI?
Rabe: Für jede Innovationseinheit ist ein kritischer Moment die Skalierung und Übergabe von Innovationen in den Mutterkonzern – in unserem Fall die Bundeswehr. Denn in diesem Moment kann eine zu große Autonomie der Innovationseinheit zum Problem werden, da Schnittstellen fehlen. Wir hoffen und glauben, dass die BWI durch ihre jahrelange Zusammenarbeit mit der Bundeswehr hier als Verbindungselement dienen kann, um unsere Innovationen im großen Stil in die Truppe und in die Hand vom Soldaten zu bringen.
In unserer derzeitigen Transitionsphase versuchen wir deshalb herauszufinden, welche Tiefe der Integration und welches Maß an Unabhängigkeit und Freiheit gebraucht wird, damit für beide Seiten und vor allem für unseren Nutzer, nämlich die Bundeswehr, etwas Positives daraus erwächst.

Die Fragen stellte Dorothee Frank.

Intrapreneurship im Bundeswehr Cyber Innovation Hub

Foto: Bundeswehr Cyber Innovation Hub

Interview mit Dr. Stephan Abel,
Leiter Intrapreneurship,
Member of the Management Board,
Bundeswehr Cyber Innovation Hub

IT-Report: Was sind die Aufgaben Ihres Teams?
Abel: „Aufgaben" greift mir hier zu kurz, lassen Sie mich ein wenig weiter ausholen: Der Begriff „Intrapreneurship" wurde geprägt durch den Yale-Professor Gifford Pinchot und bezeichnet die Vision, dass sich die Mitarbeiter eines Unternehmens so verhalten, als wären sie selbst Unternehmer.
Dieser Vision folgend ist es unsere Mission, Soldatinnen und Soldaten sowie zivile Mitarbeiterinnen und Mitarbeiter im Geschäftsbereich des Bundesministeriums der Verteidigung zu „Defense Intrapreneuren" zu befähigen, sie bei der Weiterentwicklung ihrer Ideen zu unterstützen und auf diese Weise auch zu einem Kulturwandel in der Bundeswehr hin zu mehr Innovationsbereitschaft und unternehmerischem Denken beizutragen.

IT-Report: Wie fangen Sie die Ideen in der Bundeswehr ein?
Abel: Manchmal fangen die Ideen auch uns ein.
Es gibt verschiedene Wege, an innovative Ideen aus der Truppe zu gelangen. Nicht selten werden wir einfach angeschrieben oder angesprochen, weil jemand Kenntnis von uns erlangt hat. Ein anderer Weg, den wir beispielsweise bei der „Innovation Challenge Einsatzflottille 1" beschritten haben, ist der Aufruf eines Top-Stakeholders, hier des Kommandeurs persönlich mit einem Video an alle Mitarbeiterinnen und Mitarbeiter seines Bereiches, Ideen bei uns einzureichen.
Um uns eine Idee „zuzuwerfen" kann jedes erdenkliche Format genutzt werden, Handy-Videos, E-Mails, ein persönlicher Pitch bei uns vor Ort, da sind wir völlig flexibel.

IT-Report: Bleiben die Hierarchie und die üblichen Dienstwege beim Intrapreneurship bewahrt?
Abel: Das bleiben sie und das ist auch gut so. Intrapreneurship funktioniert nämlich nicht an den Vorgesetzten vorbei, sondern nur mit den Vorgesetzten.
Aus diesem Grunde starten wir nur dort ein Programm, wo wir auch den jeweiligen Top-Stakeholder als Unterstützer „im Boot" haben, wie beispielsweise in der Einsatzflottille den Kommandeur, Flottillenadmiral Christian Bock, und in der Streitkräftebasis den Inspekteur, Generalleutnant Martin Schelleis.

IT-Report: Wie fördert die Bundeswehr solche innerbetrieblichen Ideen und Projekte durch Soldaten? Gibt es beispielsweise ein Bonussystem?
Abel: Ein Bonussystem wie beispielsweise beim Kontinuierlichen Verbesserungsprogramm der Bundeswehr gibt es bei uns nicht. Das brauchen wir auch gar nicht, denn die Leute, die wir als Zielgruppe im Auge haben, brennen so sehr für ihre Idee, dass allein die Gelegenheit, diese zusammen mit uns umzusetzen, als Antrieb völlig ausreicht.
Aber wir brauchen etwas anderes, und das dringend: Es muss sich für unsere Intrapreneure aus personalentwicklerischer Sicht lohnen, sich einzubringen. Deshalb wünschen wir uns, dass Innovationswilligkeit und nachgewiesene Innovationskompetenz auch bei uns Karrierebeschleuniger werden. In innovativen Zivilunternehmen ist das bereits der Fall. Da in der Bundeswehr wohl niemand der These widersprechen wird, dass Innovationskompetenz eine der wichtigsten Eigenschaften der zukünftigen militärischen Führungskraft ist, glaube ich, dass wir auch zeitnah dorthin kommen werden.

IT-Report: Welche Ideen ließen sich bisher aus der Truppe generieren?
Abel: Wir haben schon zahlreiche Ideen gefunden, die virulente Probleme in der Truppe lösen und bei deren Umsetzung wir als Bundeswehr Cyber Innovation Hub echte Hilfe leisten können.

IT-Report: Können Sie Beispiele für die praktische Umsetzung dieser Ideen nennen?
Abel: So haben wir beispielsweise in Zusammenarbeit mit dem Einsatzführungskommando der Bundeswehr unter Nutzung unseres Messengers „StashCat" ein Flugausfallmeldesystem entwickelt, das verhindert, dass Teilnehmer eines Einsatzkontingents infolge einer Flugverschiebung unnötig an den Verlegeort anreisen und so länger als unbedingt erforderlich von ihren Familien getrennt sind.
Eine Software zur Optimierung der Maintenance von Schiffen und Booten ist ein weiteres Beispiel für eine Lösung, die derzeit ein Kapitänleutnant der Einsatzflottille 1 entwickelt, den wir in agilen Methoden ausgebildet und mit Unterstützung des Kommandeurs der Einsatzflottille freigestellt haben.

Die Fragen stellte Dorothee Frank.

Das Startup Engagement Team im Bundeswehr Cyber Innovation Hub

Fotos: Bundeswehr Cyber Innovation Hub

Interview mit Jörg Plathner, Leiter Startup Engagement, Member of the Management Board, Bundeswehr Cyber Innovation Hub

IT-Report: Der Bundeswehr Cyber Innovation Hub (CIHBw) ist die Plattform zur Vernetzung von Bundeswehr und Startup-Szene. Sie verantworten die Innovationsvorhaben des Hubs. Was kann man sich darunter vorstellen?
Plathner: Eine der Aufgaben des Bundeswehr Cyber Innovation Hub ist es, Innovationen aus den Bereichen Cyber, Informationstechnologie und digitale Transformation schneller in die Bundeswehr und damit schneller in die Hand von Soldaten und Soldatinnen zu bringen.
Mit unseren Innovationsvorhaben wollen wir digitale Innovationen, die einen potentiellen Mehrwert und Nutzen für die Bundeswehr haben, zusammen mit Nutzern testen und für eine mögliche Beschaffung oder Weiterentwicklung empfehlen. Als Innovationen sehen wir in diesem Fall alle digitalen Lösungen, die so in der Bundeswehr noch nicht im Einsatz sind.

IT-Report: Welches Standing hat der Cyber Innovation Hub – und die daraus resultierenden Innovationsvorhaben – in der Bundeswehr?
Plathner: Wir erleben in der Zusammenarbeit begeisterte Soldaten und Soldatinnen, die voller Leidenschaft und mit enormem Fachwissen mit uns zusammenarbeiten. Viele Kameraden und Kollegen der Bundeswehr haben erkannt, dass wir dabei helfen können, Lösungen von konkreten Herausforderungen mit innovativen und digitalen Produkten aufzuzeigen. Wenn die Beschaffungsprozesse nach einer Empfehlung durch uns jetzt noch schneller werden, können wir zukünftig den Anforderungen der Digitalisierung noch gerechter werden.

IT-Report: Bundeswehrstrukturen und Startups scheinen auf den ersten Blick wenig zusammenzupassen. Wie erleben Sie die Zusammenarbeit von Startups mit der Bundeswehr?
Plathner: Das Vorurteil, dass Bundeswehr und Startups nicht zusammenkommen können, widerlegen wir ständig. Natürlich ist es für Startups, die häufig eher über wenige Ressourcen verfügen und in kürzeren Zeitzyklen planen und agieren müssen, schwierig, mit großen Behörden und Ämtern (und auch Konzernen) zusammenzuarbeiten. Gerade hier können wir die Funktion eines Hubs voll ausspielen und für ausgewählte Startups ganz konkrete Anwendungsfälle zur Verfügung stellen. Wir treten dabei wie ein normaler Kunde auf und bieten Startup-taugliche, unkomplizierte und schnelle Einkaufsprozesse. Für die Startups ist dabei nicht nur der erzielte Umsatz von Interesse, sondern häufig auch die Möglichkeit, mit militärischen Anwendern eng zusammenzuarbeiten und an deren Erfahrungen teilhaben zu können. Viele Startups erhalten so Einblicke in einen für sie neuen, interessanten Markt.

IT-Report: Wie viele Innovationsvorhaben hat der CIHBw durchgeführt und abgeschlossen?
Plathner: Seit der Gründung des Bundeswehr Cyber Innovation Hub haben wir rund 80 Projekte angestoßen. Davon wurden rund 50 als Innovationsvorhaben zur Evaluation freigegeben. Davon sind derzeit zehn im Einkauf, weitere zehn in der Evaluation mit dem Nutzer und zehn Innovationsvorhaben bereits abgeschlossen und zum Teil für die Beschaffung empfohlen worden. Es wurden dabei digitale Innovationen in Bereichen wie Gefechtsfeldkommunikation, Cyber IT, Cyber Security, Social Media, Logistik, Sanität und Ausbildung getestet.

IT-Report: Täglich erhalten Sie mehrere Anfragen von Seiten der Bundeswehr. Nach welchen Kriterien entscheiden Sie, was letztendlich ein Innovationsvorhaben wird?
Plathner: Wesentliche Entscheidungskriterien für die nähere Beschäftigung mit einem Vorhaben sind für uns:

a. Nutzen und Anwendungsfall
Voraussetzung für alle Innovationsvorhaben ist es, dass wir engagierte militärische Nutzer gefunden haben, die neue Produkte und Services an einem konkreten Anwendungsfall testen möchten und können. Dazu schränken wir zunächst gemeinsam den Anwendungsfall auf den eigentlichen Kern des Problems ein und beleuchten die Frage der Bedeutung und der Skalierbarkeit einer möglichen innovativen Lösung für einen größeren Nutzerkreis. Ohne passenden Anwendungsfall und Nutzer findet im Cyber Innovation Hub der Bundeswehr kein Innovationsvorhaben statt.

b. Ressourcen und Geschwindigkeit
Ein wesentliches Entscheidungskriterium ist, ob sich Vorhaben schnell und unkompliziert umsetzen lassen. Unsere Ressourcen, sowohl finanziell als auch personell, sind beschränkt, wir müssen unsere Kräfte somit konzentrieren. Kurze Innovationszyklen und exponentieller Fortschritt digitaler Fähigkeiten zwingen alle Akteure zu einer hohen Geschwindigkeit und konsequenten Umsetzung. Ziel bleibt es daher, innovative Produkte in kürzester Zeit in die Hand von Soldaten zu bekommen, umso möglichst schnell eine Evaluation durch den Nutzer zu erzielen.

c. Verfügbarkeit eines Produktes
Für unsere Innovationsvorhaben ist es unerlässlich, dass im Startup-Ökosystem bereits Produkte oder Services verfügbar sind, die evaluiert werden können. Diese sollten als sog. MVP (Minimal Viable Product) unsere Problemstellung lösen und mindestens einen Prototypen-Status haben. Wir gehen dabei immer davon aus, dass diese MVPs noch nicht unbedingt fertig entwickelt und militärisch gehärtet sind. In fast allen Fällen testen wir sog. Dual Use-Produkte, also Produkte, die eigentlich für den zivilen Markt konzipiert wurden, aber auch bei Anwendungsfällen in der Bundeswehr eingesetzt werden könnten.

IT-Report: Was sind für Sie Erfolgskriterien?
Plathner: Erfolg ist für uns, wenn wir innovative Produkte und Lösungen schneller und häufig auch günstiger als bisher zur Evaluation in die Hand von Nutzern in der Bundeswehr geben können und so frühzeitiger geeignete Lösungen für die Bundeswehr aufzeigen können.
Unser Ziel ist erreicht, wenn wir dazu beitragen können, dass Kameraden und Kollegen der Bundeswehr ihren Auftrag besser, sicherer und motivierter ausführen können.

Die Fragen stellte Dorothee Frank.

Managed Security Services

Proaktiver Schutz der IT-Infrastruktur vor Angriffen

Katrin Eisele

Immer häufiger hängen Unternehmensprozesse von funktionierender Informations- und Kommunikationstechnik ab. Der Umfang der kritischen Daten, die digital verarbeitet, übertragen und gespeichert werden, wächst stetig.

Mit der Anzahl der IT-gestützten Verfahren steigt die Abhängigkeit der Unternehmen von einer reibungslos funktionierenden IT. Der Schutz der IT-Infrastruktur vor Ausfall und die notwendige Belastbarkeit der IT-Systeme ist für die Aufrechterhaltung des Geschäftsbetriebs grundlegend.
Parallel dazu steigt die Häufigkeit der Angriffe auf die IT-Infrastruktur kontinuierlich an. Immer wieder werden neue Schwachstellen in Standardprodukten bekannt, die oft nicht schnell genug behoben werden können. Als Antwort auf die neuen Schwachstellen werden von Angreifern wirkungsvolle Angriffsmethoden entwickelt und passende Sabotage- und Spionagewerkzeuge zur Verfügung gestellt.
Dieser Kreislauf kann nur schwer durchbrochen werden. Es muss daher eine neue Vorgehensweise – ein systematischer Ansatz – angewandt werden.

Empfohlene Gegenmaßnahmen

Um sich vor den vorhandenen Gefahren zu schützen, setzen Unternehmen bereits zahlreiche IT-Sicherheitsmaßnahmen um. In der Regel ist die Absicherung jedoch lückenhaft oder als Insellösung implementiert. Zudem führt der rasante technische Fortschritt zu immer neuen Bedrohungen und Schwachstellen sowie daraus resultierenden neuartigen Schutzmechanismen. In den wachsenden IT-Strukturen in Unternehmen können die notwendigen IT-Sicherheitsmaßnahmen nur schrittweise berücksichtigt werden, denn häufig fehlt hierzu die Zeit sowie sicherheitstechnisches Know-how.
Der Schutz der IT-Infrastruktur hat auch nach wie vor drei klassische Ziele: die Vertraulichkeit der Informationen, die Integrität der Informationen und Systeme sowie die Verfügbarkeit der Informationen und Systeme.
Die allgemein empfohlenen Maßnahmen beinhalten:

Augmented Reality in der Nutzung. Die Technologie ist bereits erprobt und im Einsatz

- Regelmäßige Aktualisierung (Updates) der Betriebssysteme und Anwendungen,
- Schutz der Netzwerk- und Internetverbindungen durch Spam- und Virenfilter, Firewalls sowie Verschlüsselung,
- Verschlüsselung aller Endgeräte und Daten auf Servern, Desktop-PCs sowie sämtlicher Mobilgeräte,

Autor

Katrin Eisele ist Leiterin des Bereichs IT-Service Management bei der steep GmbH.

- Verwendung von personalisierten und sicheren Zugängen oder Verwendung einer Multi-Faktor-Authentifizierung,
- Regelmäßige Überprüfung und Beschränkung der Zugriffe.

Die Absicherung erfolgt dabei meist nur in einzelnen Bereichen oder Aspekten und kann damit an den Schnittstellen die IT-Sicherheit im Unternehmen gefährden. Eine lückenhafte IT-Sicherheit ist die gefährlichste Schwachstelle in der IT.

Vorteile von Managed Security Services

IT-Sicherheit geht heute weit über die Implementierung üblicher Maßnahmen als Insellösungen hinaus und sollte im Ganzen betrachtet werden. Der Einsatz vieler, nicht aufeinander abgestimmter Sicherheitslösungen erzielt das Gegenteil der sichereren IT-Infrastruktur und führt zu unerwarteten Sicherheitslücken.

Technologie alleine kann leider keinen angemessen Schutzgrad bieten. Die entsprechenden Schutzmaßnahmen erfordern ein Zusammenspiel aus Menschen, Prozessen und Technologie. Alle sicherheitskritischen Maßnahmen müssen aufeinander abgestimmt sein.

Die steep GmbH verfolgt bei der Etablierung der IT-Sicherheit im eigenen Unternehmen sowie bei Kunden eine Managed Security Services (MSS)-Strategie. Managed Security Services bieten eine zentrale Verwaltung und Sicherstellung der IT-Sicherheit von Unternehmen mit Fokus auf den Geschäftsprozessen, d.h. dem Blick von oben. Alle Maßnahmen, die in den traditionellen IT-Sicherheitskonzepten vorhanden sind (Viren-, Spam-, Firewallschutz, Monitoring usw.), werden ebenso im Rahmen der MSS durchgeführt, basierend auf dem Prinzip Plan-Do-Check-Act. Mit einem Experten-Team werden die Services aus dem Blickwinkel der technischen IT-Sicherheit geplant, koordiniert und implementiert – unabhängig davon, welche Systeme und Serverlandschaften zu Grunde liegen.

Im Rahmen der Managed Security Services werden:

- Maßnahmen zur technischen Sicherheit mit IT-Systemen und Netzwerken definiert und implementiert,
- Netzwerke und IT-Systeme intelligent überwacht,
- Sicherheitslücken proaktiv erkannt und behoben,
- und Angriffe aktiv bekämpft,

jeweils entlang der Geschäftsprozesskette. Als Basis für MSS dient die technische Dokumentation der IT-Infrastruktur. Die Überwachung der IT-Infrastruktur erfolgt weitestgehend automatisch unter Verwendung spezieller Werkzeuge und darin abgebildeter Logiken. Bei Auffälligkeiten werden automatisch Alarme ausgelöst, auf die geschulte Mitarbeiter schnell und ohne Verzögerung entsprechend der definierten, aufeinander aufbauenden Sicherheitsprozesse reagieren können. Die Sicherheitsmaßnahmen werden stetig den neuen Bedrohungsszenarien angepasst.

Bei der permanenten Überwachung der IT-Infrastruktur bleiben Probleme im IT-Sicherheitsbereich nicht unentdeckt und ein potenzieller Angriff wird schnellstmöglich erkannt. Eine proaktive Reaktion der Spezialisten kann daraus folgenden Schaden reduzieren.

Fazit

Der häufig geäußerte Standpunkt, dass es keine hundertprozentige Sicherheit gibt, gilt auch für die IT. Auch bei bestmöglicher Absicherung verbleibt ein gewisses Restrisiko, Opfer eines erfolgreichen Angriffs zu werden. Einsatz von Managed Security Services ist eine strategische Maßnahme, die IT-Sicherheit im Unternehmen stark erhöhen kann und die dabei hilft, Angriffe auf IT-Infrastrukturen erfolgreich abzuwehren.

steep GmbH
Katrin Eisele
Leiterin IT-Service Management
Söflinger Str.100
89077 Ulm
Tel.: 0731 – 933 1777
Fax: 0731 – 933 391777
Katrin.Eisele@steep.de
www.steep.de

CONET

Cyber Security & Künstliche Intelligenz – Starkes Team oder Spannungsfeld?

Cyber Security ist und bleibt ein Thema. Die Zahl der Angriffe steigt stetig und die Angreifer nutzen immer intelligentere Taktiken. Angesichts erweiterter IT-Sicherheitsrisiken, Angriffsvektoren und Angriffsmuster im Zeitalter der Digitalisierung und dem Internet der Dinge (IoT) greifen traditionelle Technik und Methoden der IT-Sicherheit oftmals zu kurz. Ist der Einsatz Künstlicher Intelligenz hier die Allzweckwaffe?

Wie überall in privater Wirtschaft und Zivilgesellschaft durchdringt die Digitalisierung zunehmend auch die Streitkräfte. Sind es zuhause der oft zitierte Kühlschrank, der vor dem Ende des Milchvorrats warnt, oder intelligente Fahrzeuge, die etwa vor der Verschleißgrenze an den Bremsen warnen, sind es im wehrtechnischen Umfeld beispielsweise die umfassende digitale Sensorik, Vernetzung und die Entscheidungen unterstützenden Computer-Systeme in Waffensystemen und der Ausrüstung des Infanteristen der Zukunft. Sie alle tauschen unentwegt Unmengen von Daten aus und bieten neue Angriffsflächen für Cyber-Attacken. Den Weg der Digitalisierung nicht mitzugehen ist für die Bundeswehr aber keine Option, betonte der Inspekteur Cyber- und Informationsraum (CIR), Generalleutnant Ludwig Leinhos, kürzlich in einem Interview. Im Gegenteil: Wenn Streitkräfte auch zukünftig relevant sein wollten, dann müssten sie die Digitalisierung mit Nachdruck vorantreiben und dabei den inhärenten Risiken aktiv begegnen, so Leinhos.

Cyber Security muss daher heute mehr sein als Virenschutz und Firewall. Es geht nicht mehr nur darum, einen Server, eine Anwendung, einen Datenspeicher oder ein Netzwerk einzeln abzusichern. Wirkungsvolle IT-Sicherheit muss den gesamten Informationsraum und sämtliche IT darin schützen: von den betroffenen mitunter kritischen Infrastrukturen über alle eingesetzten Geräte – ob privates Smartphone oder intelligentes Waffensystem – bis hin zur Schnittstelle Mensch, der in den Worten von Leinhos im Bundeswehr-Bezug „auf dem Gefechtsfeld zunehmend zum digitalisierten Sensor und Effektor" wird.

Faktor Mensch in der technischen Umsetzung

Technische Fragen der notwendigen Erfassung, Übermittlung und Integration von Interaktionen, Messwerten und Sensordaten erweitern die Anforderungskataloge für technische Architekturen erheblich. Aus einer Vielzahl von Informationsquellen müssen – mit Big-Data-Technologie und passenden Methoden – Daten ermittelt, gewichtet und ausgewertet werden. Nur so lassen sich die richtigen Rückschlüsse für die Führung von Mensch und Maschine auf dem Gefechtsfeld der Zukunft ziehen.

Dem Menschen und seinem Bewusstsein für Bedrohungen, Risiken und Angriffsvektoren kommt hier eine besondere Rolle zu. Cyber-Angreifer erkennen und nutzen verstärkt die „Schwachstelle Mensch", indem sie über Social Engineering und Phishing gezielt User-Accounts anstelle von technischen Systemen ins Visier nehmen oder versuchen, über Fake-News-Kampagnen und Reputationsschädigungen die Führungs- und Entscheidungsfähigkeit zu beeinträchtigen. Mehr als 80 Prozent der Sicherheitsbedrohungen kommen so be-

Bild: Conet/Adobe Stock

Bild: Conet/Adobe Stock

reits von innen. Dieses Bedrohungspotential lässt sich aber mit einer Kombination aus Berechtigungsmanagement mit Identitäten, Zugriffsrechten und Nutzerrollen, mehrstufigen Authentifizierungsmechanismen und Aufklärung Zug und Zug entschärfen.

Resilienz der Systeme

Angesichts dieser komplexen Anforderungen gewinnt ein strategischer Ansatz mit passenden Konzepten, Notfall-Strategien und Analysen zur Bestimmung des notwendigen Schutzbedarfs für Maschinen und Menschen zunehmend an Bedeutung. Damit Cyber Security einen wirkungsvollen Schutz und eine angemessene Resilienz gegenüber Angriffen gewährleisten kann, muss sie neben der technischen Komponente ein Kernbestandteil aller Geschäftsprozesse und Organisationsstrukturen sein. Security-Überlegungen dürfen nicht erst nachträglich in neue IT-Lösungen einfließen, sondern müssen gemäß einer „Business-driven Security" schon bei der Konzeption neuer Geräte und Anwendungen von Beginn an berücksichtigt werden. Benötigt werden eine übergreifende Cyber-Sicherheitsstrategie und eine integrierte IT-Sicherheitsarchitektur, die sich im Sinne von „Security by Design" an festgelegten IT-Sicherheitsrichtlinien und Best Practices in Prozessgestaltung, Technologieauswahl und Anwendungsentwicklung orientiert.

Aktuell allerdings hinken traditionelle statische Verteidigungsmechanismen und Auswertungsmethoden den aktuellen komplexen Bedrohungsszenarien im OODA-Loop aus Beobachten/Observe, Bewerten/Orient, Entscheiden/Decide und Handeln/Act oftmals zu träge hinterher; erst recht, da angesichts des herrschenden Fachkräftemangels auch qualifizierte IT-Sicherheitsspezialisten etwa für ein handlungsfähiges Security Operations Center (SOC) überhaupt nicht in ausreichender Zahl zur Verfügung stehen.

Künstliche Intelligenz als Lösung?

Auf der Hand liegt da der Ruf nach Künstlicher Intelligenz und selbstlernenden Systemen, die Führungspersonal und IT-Sicherheitsverantwortliche bei der Identifikation von Sicherheitsbedrohungen und entsprechenden Reaktionen unterstützen und fehlende personelle Kapazitäten ergänzen oder sogar ersetzen sollen. Folgerichtig gehören Künstliche Intelligenz (KI), elektronische Kampfführung sowie vernetzte Operationsführung und Kryptologie in Deutschland mit dem Mitte Februar vom Bundeskabinett verabschiedeten Strategiepapier zu den „nationalen verteidigungsindustriellen Schlüsseltechnologien". Aber sind Automatisierung und Technisierung der Wahrheit letzter Schluss?

Einige Vertreter der militärischen Forschung und Entwicklung geben hier als Antwort ein deutliches Ja. Die Fähigkeiten der Künstlichen Intelligenz (oder Artificial Intelligence, AI) seien längst soweit, bei der Reaktion auf diese Herausforderungen weitgehend automatisiert zu helfen. Ohne den Einsatz Künstlicher Intelligenz bleiben IT-Sicherheitsverantwortliche oftmals zum bloßen und oft verspäteten Reagieren verdammt, da sich gegebenenfalls gefährdende Vorgänge und die schiere Datenmenge im Netz ohne technische Unterstützung nicht sinnvoll beobachten und auswerten lassen – der Wald wird vor lauter Bäumen nicht gesehen.

Zudem sind statische Tools auf regelmäßige Aktualisierungen angewiesen. Viren-Signaturen, Sicherheitswarnungen, Regelwerke und Sicherheits-Updates der Hersteller können aber erst zu wirkungsvollen Maßnahmen führen, wenn sie erkannt, erstellt, entwickelt und veröffentlicht sind. Im zeitlichen Delta zwischen Entdeckung und Reaktion ist vielfach bereits immenser Schaden entstanden.

Schlummernde Viren auf den Rechnern

Neben dieser Gefahr der spontanen Ausnutzung von Sicherheitslücken durch einen zeitweiligen Vorsprung der Gegenseite beim „Cyber-Wettrüsten" liegt ein weiteres Gefährdungspotential in der besonderen Art oft langfristig angelegter Angriffe, der so genannten Advanced Persistent Threats. Hier liegen oft lange Zeiträume zwischen Exploration und mehrstufigen Angriffen. Herkömmliche Security Tools weisen in diesem Zusammenhang dann zwar auf einzelne Anomalien hin, die auch erkannt und dokumentiert, aber bisweilen als zufällig oder bedeutungslos eingestuft werden, da weder die statischen Software-Werkzeuge noch die menschlichen Bearbeiter zwin-

gend einen Zusammenhang zwischen ihnen herstellen. Security-Lösungen mit Künstlicher Intelligenz sind demgegenüber in der Lage, mögliche Muster aus einer Unmenge an scheinbar zusammenhanglosen Daten auch über große Zeiträume noch zuverlässig zu erkennen.

Foto: Bundeswehr/Christian Vierfuß

Fernspäher im Beobachtungsversteck, die absolute Sicherheit dieser Systeme muss gewährleistet sein

Dies wird auch in der internen Beobachtung und Bearbeitung von auffälligem Netzwerkverhalten oder Gefährdungslagen eine zunehmende Bedeutung gewinnen, denn „schlummernde" und über lange Zeit unentdeckt bleibende Cyber-Bedrohungen sind insbesondere im öffentlichen Bereich – ob im Umfeld der Streitkräfte, bei den Betreibern kritischer Infrastrukturen (KRITIS) oder angesichts des besonderen Schutzbedürfnisses sensibler Daten vom Gesundheitswesen bis zum Geheimschutz – ein nicht hinzunehmendes Risiko.

Die Vorteile des Menschen nutzen

Hat der Mensch damit in Sicherheitsfragen ausgedient? Unserer Überzeugung nach keinesfalls, und zu dieser Erkenntnis müssen nicht einmal düstere Science-Fiction-Visionen a la Terminator oder War Games bemüht werden. Auch aktuelle Beispiele etwa bei Experimenten mit dem autonomen Fahren zeigen hier ein deutliches Bild: Noch nicht ausgereift genug sind die entsprechenden Systeme, und zu leicht lassen diese sich manipulieren, da sie auf – wenn auch teils enorm komplexen – nachvollziehbaren Lernalgorithmen fußen. Wenn es Täuschern etwa gelingt, durch ein Verständnis der zugrundliegenden Lernsystematiken und Definitionen Verkehrszeichen so zu verändern, dass aus einem Höchsttempo-30-Schild mit minimalen und für das menschliche Auge beinah unerkannten Anpassungen Tempo 80 interpretiert wird, sind die möglichen Risiken klar illustriert. Trotz der oft propagierten Überlegenheit, Leistungsfähigkeit und Unbeeinflussbarkeit der Technik sind menschliche Akteure also auch zukünftig unverzichtbar – insbesondere solange es in KI-gestützten Systemen keine lückenlose Dokumentation und damit Nachvollziehbarkeit dahingehend gibt, an welcher Stelle der Informationsverarbeitung und anhand welcher Kriterien die KI eine bestimmte Entscheidung getroffen hat.

Sich rein auf die technischen Möglichkeiten zu beschränken, würde zudem im Umkehrschluss bedeuten, zu einem längst überwunden geglaubten Status der Technik als das Maß aller Dinge und letztlich Selbstzweck zurückzukehren. Allzu lange hat es gedauert, in der Informationstechnologie von dieser Technik-Zentriertheit abzukommen und endlich eine strategische Sichtweise einzunehmen, die die Technik als zentrales Hilfsmittel des Menschen aber eben nicht dessen Ersatz sieht.

Schwachstelle der KI

Eine so genannte schwache Künstliche Intelligenz, die sich mit der Bearbeitung konkreter Anwendungsfälle auf Basis festgelegter Entscheidungsalgorithmen und Mustererkennung befasst, wird natürlich eine zunehmend zentrale Rolle spielen, wenn es darum geht, die manuell unbeherrschbaren Mengen von Daten etwa in technischen Lösungen wie einem Security Information and Event Management (SIEM) vorzufiltern und aufzubereiten. So belegen auch aktuelle Studien deutlich, dass sich in Sicherheits-Teams mit KI-Unterstützung die Reaktionszeiten um bis zu einem Drittel verringern können, da die Grundlagen für eine fundierte Entscheidung schneller und in einer für den Menschen schnell erfassbaren, transparenten und damit beurteilbaren Form vorliegen.

Die Zukunft wird und muss unserer Ansicht nach aber auch weiterhin von einem Zusammenspiel von Mensch und Maschine geprägt sein. Das eigene militärische und zivile Personal gilt es hier entsprechend in komplexen Szenarien in ihren eigenen Systemen zu schulen und sie damit für den Ernstfall handlungs- und reaktionsfähig zu machen. Technik und Artificial Intelligence übernehmen dabei zentrale vorbereitende, begleitende und unterstützende Aufgaben. Die Entscheidungen selbst kann und muss unserer Erfahrung nach aber immer noch ein Mensch als Analyst und Überwachungsinstanz mit Urteilsvermögen und Empathie treffen.

CONET Solutions GmbH
Joachim Janz
Director Cyber Security Consulting
Theodor-Heuss-Allee 19
53773 Hennef
cyber-security@conet.de
www.conet.de

Digitalisierung des Managements von Rüstungsprojekten

Das Projekt „IT-U CPM, Ablösung EMIR und IVF/VOCON“

Dr. Oliver Zacharias

„Nichts ist stärker als eine Idee, deren Zeit gekommen ist“ – dieses Grundprinzip steht auch für die Digitalisierungsbestrebungen, die inzwischen längst in nahezu allen Bereichen der Arbeitswelt Einzug halten. Auch für die Bundeswehr ist dies längst kein Neuland mehr.

Mit dem Programm „Standard-Anwendungs-Software-Produkt-Familien“ (SASPF) verfolgt die Bundeswehr einen Paradigmenwechsel in der IT-Unterstützung in Bezug auf administrative und logistische Aufgaben; weg von individuellen, aufgabenbezogenen Anwendungen, hin zu einer bundeswehrübergreifenden, wirtschaftlich orientierten, einheitlichen IT-Lösung. Die Zielsetzung dieses Programmes umfasst die Standardisierung, Harmonisierung und Optimierung von Prozessen, Verfahren, Abläufen und der Organisation

Autor

Technischer Regierungsrat Dr. Oliver Zacharias ist Referent im Projekt IT-U CPM bei BAAINBw G4.2.

Foto: Bundeswehr/Maximilian Schulz

Beim managen von Rüstungsprojekten gilt es die verschiedensten Aspekte zu betrachten

im gesamten Geschäftsbereich des Bundesministeriums der Verteidigung (BMVg). Die Programmstrategie SASPF und deren Fortschreibung geben den Fahrplan vor. Mit den darin enthaltenen Architekturvorgaben und Projekten wird nicht nur die Taktzahl der technologischen Innovationen durch die Abteilung G im BAAINBw gesteigert, sondern darüber hinaus eine neue Phase der Digitalisierung der Bundeswehr eingeläutet.

Wesentliche Anforderungen an die Digitalisierung umfassen die Verarbeitung von Daten in Echtzeit sowie die Bereitstellung umfassender Simulations- und Analysemöglichkeiten und moderner intuitiver Anwendungen. Im Bereich der Beschaffung, die sich bisweilen immer noch auf eine Vielzahl einzelner, technisch überholter IT-Verfahren abstützt, steht die Bereitstellung einer integrierten, effizienten und durchgängigen IT-Unterstützung für sämtliche Facetten des Managements von Rüstungsprojekten im Vordergrund.

Ablösung von Altverfahren

Das Projekt „IT-Unterstützung Customer Product Management, Ablösung EMIR und IVF/VOCON", kurz: IT-U CPM wird diese Anforderungen als eines der wesentlichen Projekte zur Digitalisierung des Rüstungsmanagements umsetzen. Mit der Realisierung dieses in drei Teilprojekte unterteilten Projektes werden sechs Altverfahren, allen voran das Elektronische Management Informationssystems für die Rüstung (EMIR) sowie die dem System Vorhabencontrolling (VOCON) zugeordneten Verfahren, abgelöst werden. Neben den zentralen Projektmanagementfunktionalitäten Projektstrukturplanung, Arbeits-, Zeit-, Finanzplanung (AZF), Projektdurchführungsplanung (Gantt-Chart-Funktion) sowie ein modernes Berichtswesen beinhaltet IT-U CPM eine moderne, integrierte, effiziente und durchgängige IT-Unterstützung für das Projektmanagement von Rüstungsprojekten unter den Vorgaben der ressortinternen Verfahrensvorschrift zur Bedarfsermittlung und Bedarfsdeckung in der Bundeswehr (CPM). Des Weiteren wird den Projektleitern im BAAINBw mit Realisierung dieses Projektes eine vollständige Haushaltsintegration bereitgestellt, die eine detaillierte, bis auf Ebene der Vertragsposition herunter gebrochene und titelgerechte Haushaltsmittelplanung und -bewirtschaftung ermöglicht. Dadurch wird sich das Management der programm-/projektbezogenen Haushaltsmittelaufstellung im Vergleich zu den Möglichkeiten der abzulösenden Altverfahren künftig wesentlich transparenter und effizienter gestalten. Auch wird eine medienbruchfreie Initialisierung des Beschaffungsprozesses mit dem sich daran anschließenden, bereits digitalisierten Vergabeprozess möglich sein. Die Bereitstellung eines umfassenden Controlling-/Risikoberichtswesens sowie eine spätere Lösung für die Planung und Bewirtschaftung von Forschung & Technologie-Vorhaben (F&T) bilden weitere Schwerpunkte dieses Projektes.

Bereits 2016 wurden zwei querschnittliche Lösungsanteile in die Nutzung überführt: Zum einen die Einkaufsanalyse, die dem strategischen Einkauf der Bundeswehr seither umfassende Auswertemöglichkeiten und substantielle Beiträge für die strategische Ausrichtung des Einkaufs ermöglicht; zum anderen das Contract Lifecycle Management (CLM), das die Vertragsaktivitäten durch die Nutzung von Klauselbibliothe-

Foto: Bundeswehr/Francis Hildemann

Die Abbildbarkeit in SASPF gibt die Taktzahl der technologischen Innovationen vor

ken und die elektronische Mitzeichnung von Vertragsentwürfen zusätzlich unterstützt.

IT-Unterstützung für die Qualitätssicherung

Über die oben genannten Funktionalitäten hinaus realisiert das Projekt IT-U CPM auch eine moderne IT-Unterstützung für die amtliche Qualitätssicherung, die eine umfassende Unterstützung für die Planung und Durchführung von Güteprüfungen sowie von Lieferantenaudits bereitstellen wird. Dazu ist vorgesehen, das momentan noch in der Nutzung befindliche Altverfahren „Datenverarbeitung Güteprüfung" (DV-GP) durch die moderne, auf dem SAP QM-Modul beruhende Lösung, zu ersetzen und darüber hinaus den Funktionsumfang über den des Altverfahrens um weitere moderne Methoden erheblich zu erweitern. Dies bietet künftig für die Qualitätssicherung (QS) etwa des Ersatzteilversorgungswesens der Bundeswehr folgende Vorzüge:

- Integration der IT-Lösung für die QS in die bereits etablierte SASPF-Lösung zur Beschaffung von Waren und Dienstleistungen.
- Künftig werden erstmalig standardisierte Belege (sog. Prüflose) genutzt, mit denen eine QS während der produktionsbegleitenden Prüfung wesentlich transparenter dokumentiert werden kann. Dazu bietet die SAP-Lösung den Vorteil der Nutzung einer Vielzahl von Planungs- und Stamm-Daten bei der Erstellung des Beleges, so dass die Arbeit der Güteprüfer vor Ort erheblich vereinfacht wird.
- Durch die systematische Erfassung und Auswertung von Abweichungen und Mängeln kann eine objektive Bewertung der Leistungsfähigkeit von Auftragnehmern erfolgen.
- Vor der technischen Umsetzung wird der betriebswirtschaftliche Ablauf in Form von Geschäftsprozessen so dokumentiert, dass das digitale Beschaffungsverfahren durch die „darunterliegenden" Geschäftsprozesse vollständig transparent dargestellt wird und jederzeit nachverfolgt werden kann.

Das Qualitätsmanagementsystem der Bundeswehr beinhaltet bspw. auch die Auditierung von Luftfahrttechnischen Betrieben. Im Zuge der Umsetzung des Projektes IT-U CPM wurden Lösungen des Auditmanagements für das Luftfahrtamt der Bundeswehr entwickelt. Mit Hilfe der integrativen, eng am Standard orientierten Anwendung von SAP kann nun die Auditierung des Luftfahrttechnischen Betriebes professionell geplant, durchgeführt und dokumentiert werden. Hervorzuheben sind die mit dieser modernen IT-Anwendung einhergehenden Auswertemöglichkeiten. Damit können anhand von Kennzahlen und Metriken weitergehende Aussagen zur Leistungsfähigkeit und deren Entwicklung/Veränderung ermittelt werden.

Ein durchgängiges Qualitätsmanagementsystem verlangt einen iterativen Ansatz aus den Schritten Planen – Umsetzen – Handeln – Überprüfen. Diese Schritte können mit Hilfe der IT-Lösung und der hierin erfassten Vorgänge und Daten effizient erbracht werden.

Das Projekt IT-U CPM mit seinem Lösungsportfolio trägt in Gänze den Zielen der Agenda Rüstung zur Modernisierung des Rüstungsmanagements Rechnung; sie unterstützt die in der IT-Strategie formulierte Forderung nach einer flächendeckenden IT-Unterstützung des Organisationsbereichs AIN durch SASPF und leistet damit einen unverzichtbaren Beitrag auf dem Weg zur Digitalisierung Bundeswehr und zur Sicherstellung der materiellen Einsatzbereitschaft. ■

Unbemannte Fahrzeuge für den Einsatz

Die Digitalisierung von Fahrzeugen zur Befähigung des unbemannten Einsatzes

Arno Retterath, Dr. Johannes Pellenz, André Volk

Die Digitalisierung verändert aktuell unsere Gesellschaft grundlegend. Dies betrifft auch die Bundeswehr. Demzufolge ist die Entwicklung des Gefechtsfelds der Zukunft als wichtiger Prozess einzustufen. Wie sieht in diesem Hinblick die Zukunft der Fahrzeuge der Bundeswehr aus?

Digitalisierung von Fahrzeugen

In der zivilen Automobilindustrie wird die Digitalisierung der Fahrzeuge stark vorangetrieben. Neueste Fahrzeuge bieten unterschiedliche Assistenzfunktionen für den Fahrer (wie Adaptive Cruise Control und Spurhalteassistenten) oder übernehmen bereits teilautomatisiert die Aufgaben des Fahrers. Fortschritte gibt es auch in der zivilen Lkw-Branche (Logistik), inklusive erster Versuche zum unbemannten Fahren im Konvoi (dem sogenannten Platooning oder der elektronischen Deichsel). Dies alles erweckt den Eindruck, dass das autonome Fahren (komplett ohne Fahrer) in nicht allzu ferner Zukunft realisierbar ist.
Daher stellt sich die Frage, wie weit die Digitalisierung bei den Fahrzeugen der Bundeswehr vorangeschritten ist. Durch die Einführung von unbemannten Landfahrzeugen bei den Streitkräften könnte neben dem Schutz der Soldaten auch die Durchhalte- und Durchsetzungsfähigkeit gesteigert werden.

Autoren

Technischer Oberregierungsrat **Arno Retterath**, Referent Unbemannte Landsysteme BAAINBw U6.2; Technischer Oberregierungsrat **André Volk**, F&T Technologiefeldverantwortlicher für Unbemannte Landsysteme BAAINBw U6.2; Regierungsdirektor **Dr. Johannes Pellenz**, Teamleiter Unbemannte Landsysteme BAAINBw U6.2.

Unbemannte Landsysteme in der Bundeswehr

Die Fortschritte in der zivilen Automobilbranche werfen die Frage auf, ob diese Fähigkeiten auch im militärischen Kontext genutzt werden können. Die zivilen Erfolge lassen sich jedoch nur begrenzt auf militärische Anwendungen übertragen. Die Automobilbranche nutzt vielfach die vorhandene Infrastruktur mit befestigten Straßen, Fahrbahnmarkierungen sowie detailliertes Kartenmaterial. Dagegen finden militärische Operationen oft auf unbefestigten Wegen und in unbekanntem Gelände statt. Umwelteinflüsse wie Schlamm, Staub und Niederschlag erschweren die automatisierte Navigation, da diese die umwelterfassende Sensorik stören. Zudem muss das System in militärischen Anwendungen auch ohne GPS und am besten aus Gründen der Tarnung ohne aktive Sensoren navigieren können.
Aktuell in Nutzung befindliche, militärische unbemannte Landsysteme werden lediglich ferngesteuert und sind auf die Kampfmittelbeseitigung (tEODor und Packbot EOD) oder die Minendetektion (z. B. das German Route Clearance Package) beschränkt. Neben diesen Systemen unterstützt das kürzlich eingeführte System RABE die Infanterie. Das ferngesteuerte und sehr leichte (ca. 3,5 kg) System liefert bei abgesessenen Operationen abbildende Aufklärungsergebnisse in Echtzeit. Für typische Transportaufgaben sind die vorhandenen Systeme jedoch aufgrund ihrer geringen Größe, der geringen möglichen Zuladung und der geringen Geschwindigkeit ungeeignet.
Für den Logistikbereich und dem damit verbundenen Materialtransport per Lkw werden die Möglichkeiten der Automatisierung aktuell im Rahmen verschiedener F&T (Forschung und Technologie)-Studien der Bundeswehr intensiv untersucht. Eine militärische Lösung, entsprechend dem Platooning, könnte einer Personalknappheit im militärischen Logistikbereich (speziell dem Mangel an Lkw-Fahrern) entgegenwirken. Neben der zu erwartenden Steigerung der Transportkapazitäten könnte mit einem teilautomatisierten Konvoi die Gefährdung von Soldaten im Einsatzgebiet reduziert und eine Neuzuordnung des Personals für Kernaufgaben der Bundeswehr erreicht werden. Der Wunsch nach einem unbemannten militärischen Lkw-Konvoi mittels einer standardisierten elektronischen Deichsel ist entsprechend groß.
In der Bundeswehr werden im BAAINBw durch das Referat U6.2 Beiträge zum unbemannten Fahren im Rahmen von F&T-Studien erarbeitet. Neben kleineren Systemen dient hier der TULF (Technologieträger Unbemanntes Landfahrzeug) als Integrations- und Testplattform für verschiedene Untersuchungen und Entwicklungen zum unbemannten Fahren. Der TULF basiert auf einem Lkw vom Typ MAN HX58. Mit unterschiedlichen Sensoren (u. a. 3-D-Laserscanner, Radar sowie Hyperspektralkameras) wurden Grundlagen geschaffen und wichtige Erkenntnisse zur Erkennung von Hindernissen und zur Klassifikation von Wegen in unwegsamem Terrain gewonnen.
Die aktuellen Erfahrungen und Fortschritte werden regelmäßig auf der militärischen ELROB im direkten Vergleich zu anderen Systemen gezeigt. Die ELROB ist eine internationale Leistungsschau für die neuesten Forschungen und Entwicklungen im Bereich unbemannter Systeme sowie die Plattform für die Demonstration aktuell am Markt verfügbarer Systeme. Die Szenare der ELROB werden in enger Zusammenarbeit mit den militärischen Nutzern entwickelt und in Ko-

Foto: RMMV

Das Fahrzeug TULF (hinteres Fahrzeug) folgt dem Schwesterfahrzeug StrAsRob (Straßentransport mit Assistenz von Robotern) bei der ELROB 2018 im Szenario „Konvoifahren“

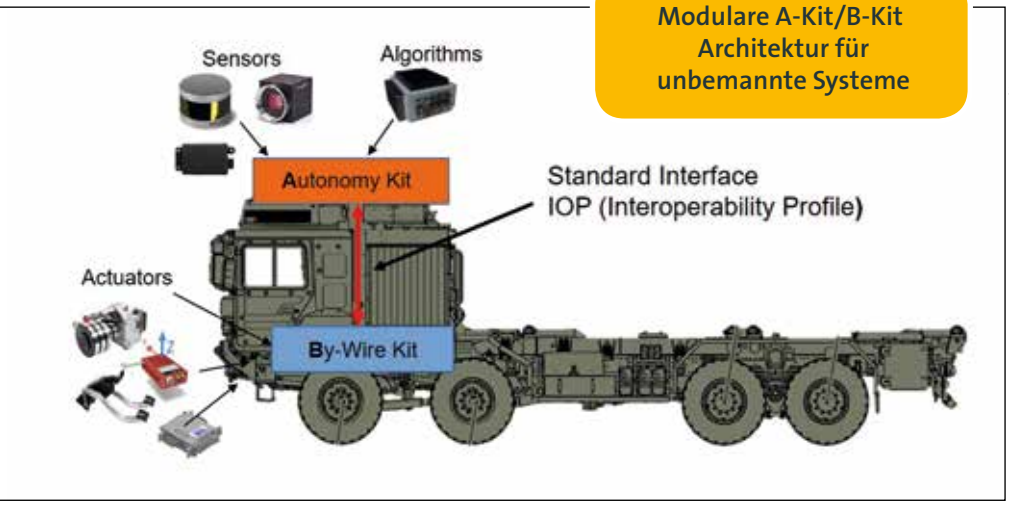
operation mit dem Fraunhofer FKIE durchgeführt und bewertet. Der TULF nahm in den Jahren 2016 und 2018 mit seinen automatisierten Funktionen an den Szenaren für das Konvoifahren und den Materialtransport für Logistik und Ausrüstung (Multifunction Utility/Logistics and Equipment – MULE) erfolgreich teil.

F&T-Vorhaben „Interoperabler Robotik Konvoi“ (InterRoK)

Die Arbeiten am TULF haben gezeigt, dass die Integration der Drive-By-Wire-Fähigkeit einen erheblichen Aufwand bedeutet. Daher wird im Nachfolgevorhaben InterRoK sehr früh auf die Integration der Drive-By-Wire-Fähigkeit Wert gelegt. Um eine hohe Wiederverwendbarkeit der F&T-Ergebnisse für spätere Beschaffungsprojekte zu erreichen, wird bei InterRoK die neueste Generation der Ungeschützten Transportfahrzeuge (UTF) verwendet. Diese aktuell in die Bundeswehr eingeführten UTFs basieren auf der neuen MAN HX2-Baureihe der Firma Rheinmetall MAN Military Vehicles (RMMV) und bieten durch das vollautomatisierte Getriebe und die elektrische Ansteuerung der Beschleunigung (E-Gas) ideale Voraussetzungen für die Digitalisierung (Drive-by-Wire-Fähigkeit).

Bei InterRoK werden die Kenntnisse aus TULF und anderen Vorhaben weiter genutzt und wichtige Vorarbeiten zur Realisierung der elektronischen Deichsel mit Fahrzeugen unterschiedlicher Hersteller geleistet. Konkret wird untersucht, wie ein unbemannter Konvoi aus verschiedenen Lkw der Bundeswehr technisch realisiert werden kann. Das Konzept sieht einen militärischen Konvoi mit nur noch einem einzigen bemannten und geschützten Führungsfahrzeug vor, dem mehrere unbemannte Lkw folgen. Die F&T-Studie InterRoK beinhaltet zuerst den Umbau zweier MAN HX2. Durch diesen Umbau werden die Fahrzeuge Drive-By-Wire-fähig gemacht. Danach wird die Sensorik und die Intelligenz eines menschlichen Fahrers durch einen Autonomie-Satz (engl. Autonomy Kit

Modulare A-Kit/B-Kit Architektur für unbemannte Systeme



Grafik: BAAINBw

oder kurz A-Kit) ersetzt. Das A-Kit besteht aus Sensorik, Rechnern und der Software zur Wahrnehmung und Interpretierung der Umgebung, der Planung des Pfades sowie zur Quer- und Längsregelung des Fahrzeugs. Mit Hilfe des A-Kits ist der Lkw in der Lage, sich selbstständig auf Grundlage des Fahrauftrags und der aktuellen Sensordaten zu bewegen. Die umgebauten Fahrzeuge sollen mittelfristig auch dazu genutzt werden, um weitere fahrzeugunabhängige A-Kits zu erproben und Erkenntnisse für das Gebiet der automatisierten Konvoifahrt mit gemischten Lkw-Typen liefern. Die Kommunikation vom A-Kit zum Fahrzeug geschieht über eine standardisierte Schnittstelle (IOP, Interoperability Profile), sodass die Integration der A-Kits verschiedener Hersteller ermöglicht wird.

In einem ersten Schritt wird ein existierendes A-Kit vom Hersteller Robotic Research aus den USA in die deutschen Fahrzeuge eingebaut und erprobt. Diese A-Kits werden im Rahmen der F&T-Kooperation zwischen Deutschland und den USA für dieses Vorhaben von der amerikanischen Seite ausgeliehen. Die Entscheidung, im ersten Schritt diese US-amerikanischen A-Kits zu verwenden, basiert auf der ausgereiften Entwicklung und erfolgreichen Erprobung der A-Kits auf der US-Seite sowie der engen Kooperation des BAAINBw mit der Dienststelle CCDC Ground Vehicle Systems Center (GVSC; ehemals TARDEC) der U.S. Army. Das GVSC arbeitet seit Jahren intensiv an einer unbemannten Konvoilösung. Es wurden bereits verschiedene Systeme erprobt, in denen die Leader-Follower-Funktion implementiert wurde, und es sind zahlreiche praktische Versuche auf militärischen Übungsplätzen der USA durchgeführt worden. Aktuell werden von der U.S. Army im Rahmen des Expedient Leader Follower Programs bis zu 90 PLS (Palletized Loader System) – Drive-by-Wire-fähige Logistikfahrzeuge der Firma Oshkosh mit dem A-Kit von Robotic Research ausgerüstet.

Im Anschluss an die Integration und die Tests der amerikanischen A-Kits sollen im F&T-Vorhaben InterRoK auch alternative A-Kits (z. B. von deutschen oder europäischen Herstellern) auf den Fahrzeugen getestet und verglichen werden. Neben dem Umbau der Fahrzeuge und der Integration der A-Kits mit den dazugehörigen Erprobungen, soll die Studie den Aufwand und das mögliche Optimierungspotenzial bei der Nachrüstung der deutschen UTFs für die teilweise unbemannte Konvoifahrt liefern.

Außer diesen technischen Untersuchungen für das unbemannte Fahren im Konvoi werden auch rechtliche Grundlagen betrachtet: Wie sieht es mit der Zulassung solcher Systeme für den öffentlichen Straßenverkehr aus? Wie können ethische Fragen zufriedenstellend beantwortet werden? Trotz möglicher Ausnahmeregelungen für die Bundeswehr bei der hoheitlichen Aufgabenwahrnehmung müssen diese rechtlichen Grundlagen geklärt werden, bevor diese Systeme eingeführt werden können.

MULE (Multifunction Utility/ Logistics and Equipment)

Ein weiteres Gebiet für den Einsatz von unbemannten Landsystemen ist die Unterstützung der infanteristischen Truppen mit einem Mehrzweck-Bodenfahrzeug. Der bisher genutzte Waffenträger Wiesel soll durch den größeren GTK Boxer ersetzt werden. Gerade für unwegsames und schwer zugängliches Gelände (z. B. im Wald) kann die Truppe den Boxer aufgrund seiner Größe nicht immer nutzen. Hier könnten kleinere unbemannte Systeme (zwischen 400 kg und 1.000 kg Masse) der Truppe bei Transportaufgaben, Überwachungsaufgaben oder dem Schutz der eigenen Soldaten helfen.

Die unbemannten Systeme sollen den Soldaten beim Tragen von schwerem Equipment (persönliche Ausrüstung oder schwere Waffen, wie z. B. die Granatmaschinenwaffe) unterstützen, sodass die Einsatzkräfte ausgeruhter und schneller am Zielort ankommen.

Diese MULE-Funktionalität soll durch mittelgroße elektrobetriebene Systeme erreicht werden. Vorerst werden die Fahrzeuge noch ferngesteuert, zukünftig

Foto: RMMV

Die eingeführten UTF der Bundeswehr, von denen zwei in der F&T-Studie InterRoK für den teilautomatisierten Konvoi verwendet werden

sollen sie dem Soldaten jedoch auch automatisiert folgen oder angelernte Wege zum Materialtransport selbstständig abfahren. Erste praktische Tests und Vorführungen mit drei MULE-Systemen unterschiedlicher Hersteller haben bereits in Zusammenarbeit mit der Truppe und den Herstellerfirmen im Jahr 2019 am Ausbildungszentrum der Infanterie in Hammelburg erfolgreich stattgefunden.

Zusammenfassung

Um Personal zu entlasten und den Schutz des Personals zu erhöhen, forscht die Bundeswehr intensiv an der Digitalisierung von Fahrzeugen mit dem Ziel, unbemanntes Fahren auf der Straße und im Gelände zu ermöglichen. Zur Kompensation des zukünftig knappen Personals im logistischen Bereich, sowie zur Risikominimierung im Einsatz kann die elektronische Deichsel helfen. Hierbei fahren mehrere unbemannte Lkw dicht hinter einem bemannten Lkw her. Entsprechende Vorarbeiten wurden in der Studie TULF erarbeitet und werden in der F&T Studie InterRoK fortgeführt, um mittelfristig einen teilautomatisierten Konvoi zu realisieren. Wann die ersten Systeme in die Bundeswehr eingeführt werden, hängt neben den technischen Umsetzungen auch stark von den rechtlichen Zulassungsvoraussetzungen ab. Zusätzlich kann die MULE-Fähigkeit – mit mittelgroßen unbemannten Systemen für die infanteristische Truppe – ein Gewinn für die Bundeswehr sein. Erste praktische Versuche zeigten marktverfügbare Systeme, die den Soldaten sinnvoll unterstützen. ■

Foto: FKIE

Soldaten bei praktischen Tests mit einem MULE-System

THALES

D-LBO – Herausforderungen hochvernetzter Systeme und Plattformen

Seit Jahrzehnten entwickelt Thales innovative Systeme und Produkte, die sich bei Streitkräften und Sicherheitsbehörden in unterschiedlichen Missionen und Einsätzen weltweit bewährt haben. Auch mit der Bundeswehr hat sich dadurch über viele Jahre vertrauensvoller Zusammenarbeit eine enge Partnerschaft entwickelt.

Traditionell nimmt Thales Deutschland mit insgesamt elf Standorten von Kiel bis nach Ditzingen und seinen 3.800 Mitarbeitern einen herausgehobenen Stellenwert für die Ausrüstung der Bundeswehr ein. Charakteristisch sind die lokal agierenden Projektteams und Ansprechpartner sowie gewachsene, über die Standorte verteilte Entwicklungs-, Produktions- und Servicekapazitäten – alles in allem Garanten für kurze Reaktionszeiten sowie einen begleitenden, konstruktiven Austausch mit allen Teilstreitkräften und in allen Phasen der Beschaffung und der Nutzung.

Ob bei integrierten Kommunikationslösungen und Sensoren für die Marine, taktischen Funkgeräten, Nachtsichtausrüstung und Kryptomanagement-Systemen für das Heer oder Radaren für die Luftraumüberwachung der Luftwaffe – die Spezialisten von Thales Deutschland sorgen für die nationale Ausgestaltung erforderlicher Funktionalität und stellen im Lebenszyklus die gesicherte Verfügbarkeit für die Bundeswehr sicher. Über die Jahre ist damit nicht nur die Entwicklung zu einem großen deutschen Systemhaus vollzogen worden, sondern darüber hinaus auch die Bildung eines „Brückenkopfs" zu weltweiten Kompetenzen und dem einzigartigem Know-how des Thales-Konzerns für digitale Technologien, die bei internationalen und insbesondere auch bei europäischen Kooperationen, wie beispielsweise Digitalisierung landbasierte Operationen (D-LBO) mit Deutsch-Niederländischem Anteil Tactical Edge Networking (TEN) sowie die Deutsch-Französischen Zukunftsprogramme Main Ground Combat System (MGCS) und Future Combat Air System (FCAS), von zentraler Bedeutung sind.

Die Digitalisierung von Streitkräften

Seit dem Beginn der digitalen Revolution sind die Herausforderungen und damit auch die Anforderungen an moderne Streitkräfte fortwährend und sich selbst beschleunigend gestiegen. Die damit einhergehende wachsende Vielfalt an Sicherheitsrisiken und Operationsszenarien fordert den Streitkräften eine nie dagewesene Flexibilität und auch Skalierbarkeit ab – zunehmend gilt das Prinzip „Klasse statt Masse!". Der daraus resultierende Bedarf an modular einsetzbaren Streitkräftedispositiven ist eine logische Konsequenz, die sich auch in den Anforderungen an die tief verwurzelten Informations- und Kommunikationssysteme der militärischen Ausrüstung widerspiegelt. Im Zentrum zukünftiger digitalisierter Streitkräfte muss vor diesem Hintergrund ein modernes, adaptierbares und Aufwuchs fähiges Führungs-, Kommunikations- und Informationssystem (C4I) stehen, das von Beginn an darauf ausgelegt ist, mit dem immer schneller werdenden Tempo digitaler Weiterentwicklungen mithalten zu können (agile Systementwicklung). Bei den Landstreitkräften wird dies durch das Programm D-LBO/TEN verwirklicht.

Eine zentrale Aufgabe wird – auch vor dem Hintergrund des Fähigkeitsprofils von Thales Deutschland – bei D-LBO/TEN dem Kommunikationsnetzwerk zugeschrieben, das zwei Anforderungen parallel erfüllen muss. Zum einen die Vernetzung von Battle-Management-Systemen (BMS) für transaktionsorientierte, asynchrone Kommunikation, wie Command & Control, Daten, Messaging oder Chat. Zum anderen den automatisierten Datenaustausch von Sprache, Daten und Video in Echtzeit zwischen den Plattformen für die umfassende Situational Awareness und durchgängige „Sensor-to-Shooter"-Ketten (All Sensor-to-All Shooter) einschließlich (Teil-) Automatisierung von Diensten und Wirkungsketten.

Die Realisierung letztgenannter Anforderungen wird die grundlegende Voraussetzung sein, gleichzeitig aber auch den entscheidenden Vorteil einer digitalisierten Gefechtsführung ergeben. Diesen Einklang von Technologie und operationellen Konzepten, nennen wir „Collaborative Combat". Thales entwickelt dafür u. a. Algorithmen der Künstlichen Intelligenz (KI), die auf Basis des jeweiligen CONOPS und teilweise unter Rückgriff auf zentralisierte Datenbanken (Data Lakes) dem „Soldier-in-the-Loop" automatisierte Entscheidungshilfen bereitstellen.

Anforderungen an die Industrie

Eine grundlegende Transformation des Einsatzkonzeptes von Streitkräften geht regelmäßig auch einher mit der Transformation des Anforderungsprofils an die Industrie. Im

Fotos: Thales

Bereits bei den Kampfpanzern hat sich die Zusammenarbeit mit den Niederlanden bewährt

Die Digitalisierung der Landstreitkräfte erfordert einen übergreifenden Ansatz, der auch luftgebundene Systeme mit einschließt

Rahmen der Digitalisierung der Streitkräfte agiert dabei die fortwährende Weiterentwicklung und Implementierung modernster Technologien als „Taktgeber". Der sich daraus ergebende Anpassungsbedarf wirkt sich sowohl auf das Produktportfolio als auch auf das erforderliche Kompetenzprofil der Mitarbeiter eines Unternehmens aus. Letzteres kann neue Anforderungen an einzelne Personen, Aufbau- und Ablaufprozesse bis hin zur gesamten Unternehmenskultur nach sich ziehen. Im Produktbereich hingegen entstehen im Rahmen der D-LBO vor allem neue Anforderungen hinsichtlich der Flexibilität und Modularität sowie der (Teil-) Automatisierung und Vernetzung.

Die Entwicklung von flexiblen und modularen Produkten erfordert große Weitsicht und eine intelligente Architektur. Die erforderliche Fähigkeit, ein solches Produkt in möglichst vielfältigen und unterschiedlichen Anwendungsfällen einbinden zu können, liegt auf der Hand. Auch die daraus ableitbaren Anforderungen an standardisierte Schnittstellen, Leistungs- und Konfigurationsparameter sowie Bedienelemente ist in der Regel keine besondere Herausforderung. Entscheidend ist vielmehr die Fähigkeit des Produktes, diese flexiblen und modularen Eigenschaften für eine möglichst lange Dauer bei sich ständig ändernden Umweltbedingungen aufrechtzuerhalten. Es geht also z. B. nicht nur darum eine Schnittstelle auf möglichst viele Standards anpassen zu können, sondern auch darum, die Schnittstelle selbst bei Bedarf möglichst schnell und aufwandsarm anpassen zu können.

Für D-LBO relevante Beispiele für eine solche Entwicklung umfassen bei Thales die Funkgerätefamilie SYNAPS, ein Software Defined Radio mit modularer Hard- und Software sowie ladbaren Wellenformen (Boden-Boden, Luft-Boden und Luft-Luft). Das kryptierbare und störresistente SYNAPS-Funknetz agiert autonom und kann mit bis zu 1.000 verbundenen Geräten über entsprechende Netzübergänge (z. B. zu Satellitennetzen, 5G-Netzen oder anderen Funk- und Leitungsnetzen) Daten austauschen.

Die SYNAPS-Plattform bietet die einzigartige Möglichkeit, einerseits ältere Wellenformen wie PR4G, die auch bei den niederländischen Streitkräften und europaweit verbreitet im Einsatz ist, zu laden. Andererseits ist Thales Gründungspartner der ESSOR-Initiative und die SYNAPS-Plattform ist nativ ESSOR-fähig.

Ein weiteres, mittelbar für D-LBO relevantes Beispiel umfasst den Einsatz von Metamaterialien und Nanotechnologien zur modularen Dislozierung und Integration von Radarantennen in die Oberfläche von Fahrzeugen und Plattformen. Eine Entwicklung, die neben einem erhöhten Eigenschutz (z. B. gegenüber gegnerischer Aufklärung) auch deutlich geringere Integrationseinschränkungen im Hinblick auf das Fahrzeugdesign mit sich bringt.

Der Bedarf einer Entwicklung von (teilweise) automatisch und vernetzt agierenden Produkten, entspringt neben dem zusätzlichen Funktions- und Fähigkeitsgewinn vor allem der steigenden Notwendigkeit, Komplexität für die Anwender zu reduzieren – häufig bei gleichzeitig niedrigeren Reaktionszeiten. Auch hier ist wieder Flexibilität gefordert, wenn es darum geht, eine (Teil-) Automatisierung und Vernetzung in Abhängigkeit individueller operationeller Bedürfnisse zu ermöglichen.

Typische Anwendungsfelder für solche Produkte finden sich bei Thales insbesondere in den Produktbereichen Sensorik oder Optronik. Durch eine flexible Definierung des Suchbereichs und relevanter Zielkategorien für ein Radar (sog. holographische Anwendung) unter Nutzung von KI eine der individuellen Operationsart kann z. B. eine angepasste Überwachung erfolgen (z. B. mit Fokus auf kleine Drohnen in einer Stabilisierungsoperation). Ein weiteres Beispiel könnte die Kombination verschiedener optronischer Sensoren, wie z. B. Infrarot, Tag-Nachtsicht, Laser-Zielbeleuchtung mithilfe KI-gestützter Datenverarbeitung sein. Mögliche Anwendungsfelder für solch eine Vernetzung sind vielfältig und werden auch im „Scorpion" Programm, dem französischen Pendant zu D-LBO, in Betracht gezogen. In diesem Umfeld macht Thales bereits erste Erfahrungen in der Integration von Künstlicher Intelligenz und komplexen Processing-Architekturen in eine echtzeitfähige Situational Awareness des Gefechtsfahrzeugs. Hier bestehen auch umfassende Zusammenhänge zum Zukunftsprogramm MGCS.

Als Gründungsmitglied von ESSOR stattet Thales seine Systeme – wie das hier abgebildete SYNAPS Software Defined Radio – mit der ESSOR-Wellenform aus

„Thought Leader Digitalisation"

Thales hat in den letzten Jahren mehrere Milliarden Euro in den Auf- und Ausbau von digitalen Technologien und Expertise investiert und sich als anerkannter „Thought Leader" für die Digitalisierungsprojekte der Bundeswehr und ihrer internationalen Bündniskräfte qualifiziert. Bei D-LBO bilden IT-/Cyber-Security, Konnektivität sowie Big Data unterstützt durch künstliche Intelligenz das unverzichtbare Rückgrat für eine erfolgreiche Implementierung von „Collaborative Combat" und „Sensor-to-Shooter"-Fähigkeiten.

Das Systemhaus Thales ist mit der einzigartigen Kombination aus einem breiten Produktportfolio – einschließlich modernster, standardisierter Sensor- und Kommunikationstechnologien – und einer tiefgreifenden Digitalisierungskompetenz ein starker Partner für die Digitalisierung der Streitkräfte. Thales Deutschland unterstützt die Bundeswehr unverändert mit umfangreichen lokalen Kompetenzen, um auch in Zukunft in der „digitalen Dimension" als führende Nation im europäischen Kontext zu agieren.

THALES

Thales Deutschland
Sven Rowley
Director Sales Defence & Security
Thalesplatz 1
71254 Ditzingen
www.thalesgroup.com

Positionierung im Raum

Die landmarkenbasierte Lokalisierung zur Navigation von autonomen Landfahrzeugen

Patrick Burger, Thorsten Lüttel, Hans-Joachim Wünsche

Autonome Landfahrzeuge (engl.: Unmanned Ground Vehicle, UGV) sind die Zukunft, sowohl im zivilen als auch im militärischen Bereich. Eine Schlüsselvoraussetzung ist die Lokalisierung und Navigation in unstrukturiertem Gelände.

Im Gegensatz zur zivilen Automobilindustrie gibt es jedoch bisher in militärischen Einsatzgebieten keine genauen Karten für UGV-Anwendungen. Somit ist maschinelle Wahrnehmung und Interpretation der Umgebung in Gebieten ohne genaue Karte deutlich wichtiger und komplexer. Dieser Artikel gibt einen Überblick über aktuelle Forschungsergebnisse der Universität der Bundeswehr München zum Thema der Landmarken-basierten Lokalisierung.

Autoren

Patrick Burger, Wissenschaftlicher Mitarbeiter am Institut für Technik Autonomer Systeme (TAS), Universität der Bundeswehr München; **Thorsten Lüttel**, Wissenschaftlicher Mitarbeiter am Institut für Technik Autonomer Systeme (TAS), Universität der Bundeswehr München; **Univ.-Prof. Dr.-Ing. Hans-Joachim Wünsche**, Leiter des Instituts für Technik Autonomer Systeme (TAS), Universität der Bundeswehr München.

Grafiken und Fotos: BAAINBw

Abbildung 1: Platooning bzw. elektronische Deichsel mit kleinen Abständen zwischen den Fahrzeugen: Ein sensorbasiertes Tracking des Führungsfahrzeugs ermöglicht auch in Engstellen eine hohe Spurtreue

Motivation

Im zivilen Bereich ist in den letzten Jahren eine massive Beschleunigung bei der Entwicklung von (teil-) automatisierten Fahrfunktionen bis hin zum unbemannten autonomen Fahren zu beobachten. Schwerpunkte der Entwicklung sind hier derzeit Lösungen wie der Highway-Pilot für die Autobahn oder unbemannte Taxidienste im städtischen Umfeld. Neben den klassischen Automobilherstellern und Automobilzulieferern sind vermehrt Tech-Konzerne wie Waymo (Google) oder Uber aktiv.

Ein aktuell in der Bundeswehr diskutiertes Einsatzszenario, das auf UGVs basiert, ermöglicht die Erhöhung der Transportkapazität bei gleichbleibender Anzahl an Militärkraftfahrern. Dies soll durch den kombinierten Einsatz von UGVs und bemannten Lkws in einem Konvoi-Szenario ermöglicht werden. Beim Platooning (elektronische Deichsel) fahren die Fahrzeuge mit sehr kurzen Abständen hintereinander her, wie in Abbildung 1 dargestellt. Durch sensorbasiertes Tracking ist es möglich, die Spurtreue des Führungsfahrzeugs zu halten. Darüber hinaus gibt es auch Ansätze, die mittels Fahrzeug-zu-Fahrzeug-Kommunikation Positionen und Geschwindigkeiten übermitteln, um spurtreu zu folgen.

Eine andere Ausprägung ist der in Abbildung 2 skizzierte aufgesplittete Konvoi mit großen Marschabständen, bei dem die Sichtverbindung zwischen den Fahrzeugen nicht immer gewährleistet ist. Dieses Thema ist derzeit Teil einer vom BAAINBw beim Institut für Technik Autonomer Systeme der Universität der Bundeswehr München beauftragten Studie, die sich mit der Fragestellung beschäftigt, wie der aufgesplittete Konvoi in unstrukturiertem Gelände navigieren kann. Zivile Anwendungen basieren derzeit häufig auf hochgenauen Karten, deren Erstellung und Wartung einerseits aufwändig und teuer, und andererseits im Einsatzgebiet nicht immer möglich ist.

Die Folgefahrzeuge nutzen hier ergänzend zu ungenauem Kartenwissen, welches a priori aus unterschiedlichen Quellen gegeben sein kann, vor allem vom Führungsfahrzeug übermittelte Landmarken- und Lokalisierungsdaten. Daraus wird eine topologisch-metrische Karte erstellt, welche anschließend zum autonomen Fahren genutzt wird. Diese Grundfunktionalität kann allgemein von UGVs für Transportfunktionen sowie Überwachungs- und Aufklärungsaufgaben genutzt werden, die dabei entweder wiederkehrenden Standardrouten folgen oder auf Basis einer topologischen Karte navigieren.

Navigation

Um in einem Gelände navigieren zu können, muss ein Umgebungsmodell erstellt werden. Das Umgebungsmodell repräsentiert die wahrgenommene Umgebung anhand von Messungen aus z. B. Kamera- oder LiDAR-Sensoren. Hier wird im Allgemeinen zwischen statischer und dynamischer Umgebung unterschieden.
Zur Wahrnehmung der statischen Umgebung gehören das Erkennen und das Tracking von Straßen, Fahrspuren und Feldwegen, das Erkennen von statischen Objekten wie Bäumen, Leitpfosten oder Hauswänden, aber auch das Erstellen von Hinderniskarten. Zur dynamischen Umgebung gehören andere bewegte Fahrzeuge, Personen oder Tiere, deren Position und Bewegung über die Zeit verfolgt werden muss. Das Umgebungsmodell ist somit die Basis für die autonome Fortbewegung eines UGV. Anhand des Umgebungsmodells werden Entscheidungen getroffen, ob ein Weg befahrbar ist oder ob einem Hindernis ausgewichen werden soll.
Darüber hinaus unterscheidet man bei der Navigation zwischen dem Explorieren und dem Pfadfolgen. Solange ein Pfad und die Karte entlang des Pfades bekannt sind, kann das UGV diesem folgen und auf dem Weg Hindernissen ausweichen. Liegt keine Karte vor, muss das UGV die Umgebung explorieren um das übergeordnete Ziel doch noch zu erreichen, wie z. B „fahre nach Norden bis die nächste Kreuzung kommt". Liegt eine Karte vor, ist die präzise Lokalisierung, d. h. die Bestimmung der Position des UGV in der Karte, die Grundvoraussetzung zur Verwendung der Kartendaten. Sind die Genauigkeit und die Verlässlichkeit der Karte nicht gegeben, so kann dies zu Unfällen führen.

Landmarkenbasiertes SLAM

Die Verwendung von Odometrie ist eine grundlegende Methode, die von UGVs und anderen Robotern zur Navigation verwendet wird. Legt der Roboter längere Strecken zurück, wird jedoch die Unsicherheit über die eigene Position größer. Vergleichbar ist diese Situation, wenn sich ein Mensch mit geschlossenen Augen in einem Raum bewegt und nur die Schritte gezählt werden. Auch hier gilt: Je weiter man geht, desto unsicherer ist man über den Standort. Man muss somit von Zeit zu Zeit die Augen öffnen, um das eigene Verständnis über den Standort zu korrigieren. Im Allgemeinen gilt, dass Odometrie-basierte Lösungen ausreichende Genauigkeit für kurze Strecken liefern. Bei größeren Distanzen erhöht sich jedoch die Unsicherheit, und die Position muss mit Messungen (externe Information) von z. B. Landmarken korrigiert werden. Dieser Prozess wird als Lokalisierung bezeichnet.
Die heutzutage gängigste und am weitesten verbreitete Möglichkeit der Lokalisierung ist mittels eines Globalen Navigationssatellitensystems (GNSS). In vielen Einsatzorten kann jedoch nicht auf GNSS oder Karten zur Lokalisierung zurückgegriffen werden. Neben der gezielten Störung von Satellitensignalen gibt es sowohl im urbanen wie auch ruralen Raum Abschattungs- bzw. Multipfadeffekte, die die Lokalisierung stören.
Ein UGV muss jedoch in der Lage sein, autonom eine neue Umgebung zu erkunden und eine Karte zu erstellen, die später zur Navigation verwendet werden kann. Die Fähigkeit zur Simultanen Lokalisierung und Kartierung (engl. Simultaneous Localization and Mapping, SLAM) ist somit eine Schlüsselvoraussetzung für autonome Roboter und wird als die Aufgabe beschrieben, eine Karte zu erstellen und dabei die Pose des Roboters relativ zu dieser Karte zu bestimmen. Dies ist eine anspruchsvolle Aufgabe, da eine Karte zur Lokalisierung des Fahrzeugs benötigt wird und gleichzeitig die Posenschätzung die Grundlage für die Kartenerstellung ist.
SLAM ist seit über drei Jahrzehnten ein sehr aktives Forschungsthema im Bereich der autonomen Robotik und des autonomen Fahrens. Das Institut für Technik Autonomer Systeme ist spezialisiert auf das autonome Fahren im unstrukturierten Bereich und hat den Fokus auf Landmarken-basiertes SLAM gelegt. Landmarken sind statische Merkmale, die sich gut von der Umgebung abgrenzen lassen. Hierzu gehören

Abbildung 2: Aufgesplitteter Konvoi mit großen Marschabständen: Das erste Fahrzeug erkennt Landmarken (rot) und Wegverläufe (blau, gelb) und kommuniziert diese an die folgenden Fahrzeuge. Diese erstellen daraus eine Karte und nutzen die erkannten Landmarken zur Lokalisierung und Navigation

klassischerweise Bäume, Büsche und sämtliche vertikalen Strukturen.
Beim Landmarken-SLAM werden Objekte von Interesse aus den Sensordaten wie z. B. LiDAR-Punktwolken extrahiert und zur Lokalisierung verwendet. Die Detektion erfolgt größtenteils mittels künstlicher Intelligenz und neuronalen Netzen, die Landmarken in Kamerabildern und Punktwolken erkennen und lokalisieren. Ein Beispiel ist in Abbildung 3 gezeigt. Im nächsten Schritt werden diese Landmarken mit Hilfe eines modernen Multi-Target-Trackers getrackt, um die 3D-Position, Geschwindigkeit und Dimension über die Zeit zu bestimmen. Hierbei wird der Zustand jeder Landmarke durch ein Kalman-Filter geschätzt und die Datenassoziation durch die Berücksichtigung von A-priori-Wissen probabilistisch durchgeführt.
Im Vergleich zu einem merkmalsbasierten SLAM-Verfahren, bei dem z. B. komplette Punktwolken oder ein mehrdimensionaler Vektor an Pixeln als Merkmal abgespeichert werden, hat der landmarkenbasierte Ansatz den großen Vorteil, dass die Karten deutlich kleiner sind und sich die Positionen und Eigenschaften von Landmarken einfach

Abbildung 3: Visualisierung der erkannten Landmarken, die mithilfe von künstlicher Intelligenz aus LiDAR-Punktwolken und Kamerabildern erkannt wurden: Bäume (grün), Büsche (rot)

über schmalbandigen Funk übertragen lassen. Dies ist zum Beispiel für den aufgesplitteten Konvoi erforderlich, damit das Führungsfahrzeug seinen gefahrenen Pfad inklusive erkannter und kartierter Landmarken an die Folgefahrzeuge übermitteln kann. Da die Landmarken als geometrische Punkte in der Karte repräsentiert werden, ist die Karte auch vom Menschen lesbar und erweiterbar. Durch die einheitliche Beschreibung der Landmarken ist zusätzlich die Unabhängigkeit von der verwendeten Sensorik gegeben. In einem Experiment wurde untersucht, inwieweit eine aus Luftbildern erstellte Karte zur Lokalisierung eines UGV verwendet werden kann. Mit einem kostengünstigen unbemannten Luftfahrzeug (engl. Unmanned Aerial Vehicle, UAV) wurde die Vermessung und Kartierung durchgeführt. Die UAV-Bilder enthielten aufgrund der geringen Flughöhe von ca. 30 m und den eingesetzten hochauflösenden Kameras einen hohen Detaillierungsgrad der Szene. In einem aufwendigen Prozess wurde aus den Einzelbildern eine dreidimensionale Punktwolke berechnet, woraus mittels moderner Clusterverfahren vertikale Landmarken extrahiert wurden. Hierzu gehören u. a. Leitpfosten, Bäume oder Schilder, aber auch Straßenverläufe und Flächen.
Im Ergebnis der Studie sind die extrahierbaren dreidimensionalen Geometrie- und Farbinformationen sowie deren semantische Beschriftung, die aus hochauflösenden Bildern rekonstruiert wurde, eine gute Grundlage zur Erstellung einer landmarkenbasierten Karte für UGVs. Darüber hinaus ist das Konzept besonders interessant für Gebiete, in denen keine Kartendaten vorhanden sind oder es starke Veränderungen seit der letzten Vermessung gegeben hat. Des Weiteren liefert die Berücksichtigung des Straßenverlaufs wertvolle Informationen zur Lokalisierung innerhalb einer Karte, aber auch zur Querführung des UGV.
In einer weiteren vom BAAINBw beauftragten Studie wird aktuell untersucht, wie man vorhandene Karteninformationen in den Lokalisierungsprozess eines SLAM-Verfahrens integrieren kann. Wie bereits erwähnt, ist SLAM definiert als die Lokalisierung in einer selbst und simultan erstellten Karte. Dieses Konzept wurde durch den „Map-Aware SLAM"-Ansatz erweitert: Bei diesem neuartigen Konzept werden Karteninformationen aus unbekannter Quelle in ein Online-SLAM-Verfahren probabilistisch integriert. Somit können zum einen die vorhandene Kartendaten helfen, die Lokalisierung zu stützen und zu verbessern, und zum anderen können die Karten bei erfolgreicher Lokalisierung erweitert werden.
Um nun die Position, Geschwindigkeit und Orientierung des UGV zu bestimmen, werden verschiedene Messungen fusioniert. Neben der landmarkenbasierten Lokalisierung zur Bestimmung der globalen Position wurde in dieser Studie die im UGV verfügbare Inertial- und Odometriesensorik verwendet und in einem probabilistischen, graphenbasierten SLAM-Verfahren zur Bestimmung der globalen Position fusioniert. Eine ausführliche Evaluierung und Erprobung wurde auf dem Standortübungsplatz München sowie auf dem Campus der Universität der Bundeswehr München durchgeführt.

Ausblick

Um Entscheidungen autonom zu treffen, benötigen autonome Fahrzeuge eine Vielzahl von Informationen. Aus diesem Grund tätigt die Automobilindustrie sehr große Anstrengungen im Bereich der Kartenerstellung für autonome Fahrzeuge.
Hochgenaue zivile Karten, wie z. B. vom Hersteller Here, werden vor allem für Autobahnen und den städtischen Bereich erstellt, in denen viele potentielle Kundenfahrzeuge mit Assistenz- und Autonomiefunktionen unterwegs sind. Neben der Kartenerstellung ist auch das Karten-Update von Bedeutung. Vor allem bei Ansätzen, die mittels Fahrzeug-zu-Fahrzeug- oder Fahrzeug-zu-Infrastruktur-Kommunikation Kartendaten austauschen, stellen sich Fragen wie „Kann ich den Daten vertrauen?" oder „Sind diese Daten besser als meine?"
Auch die Frage der Sensorik ist zu klären: Beim Einsatz von UGVs sind aus taktischen Gründen sicherlich nicht in allen Einsatzszenarien aktiv strahlende Sensoren erwünscht. Hier ist zu untersuchen, ob und wie die bisher mit LiDAR-Sensoren getesteten Algorithmen zur Landmarken-Detektion auch mit passiver Sensorik wie Stereo-Kameras nutzbar sind.
Fahrzeuge mit Assistenz- und Autonomiefunktionen sind die Zukunft, da sind sich die Experten sowohl im zivilen als auch militärischen Umfeld einig. Im zivilen Bereich hat sich die Phase der ersten Euphorie gelegt. Derzeit geht man davon aus, dass noch einiger Entwicklungsaufwand notwendig ist und gerade im innerstädtischen Bereich noch einige Jahre vergehen, bevor autonome Fahrzeuge im gemischten Verkehr wie selbstverständlich mitfahren. Der militärische Bereich profitiert allerdings nur teilweise von den Fortschritten im Zivilen, da seine Anforderungen unterschiedlich sind und die meisten KI-Datensätze für Autobahnen und innerstädtische Szenarien erstellt wurden.
Neben den vielen technischen Herausforderungen müssen auch ethische Fragen geklärt werden. Wie soll ein Fahrzeug reagieren, wenn es keine Möglichkeit zur Unfallverhinderung gibt? Soll das Auto in einem solchen Fall eine Entscheidung treffen können? ■

Aktuelle Entwicklungen im Bereich offene Architekturen wie GVA oder NGVA

Matthias Renner

Offene Architekturen wie der britische GVA-Standard (Generic Vehicle Architecture) oder NATO Generic Vehicle Architecture (NGVA, STANAG 4754) sind bei aktuellen Fahrzeugprogrammen in Großbritannien oder Australien in der Umsetzung. Auch das niederländische Programm FOXTROTT und in Deutschland D-LBO (Digitalisierung landbasierter Operationen) gehen zukünftig als bilaterales Gemeinschaftsprojekt TEN (Tactical Edge Networking) ins Rennen. Hierbei handelt es sich um die Verschmelzung der großen Digitalisierungsprogramme beider Länder unter Ausnutzung größtmöglicher Synergieeffekte. Aktuell ist davon auszugehen, dass alle zukünftigen Fahrzeugprogramme durch die Vorgaben der angesprochenen Standards maßgeblich beeinflusst werden.

Wie bereits 2018 hier im Report angekündigt, hat roda eine ganze Produktfamilie entwickelt, um alle spezifischen Bedarfe seitens der Nutzer abdecken zu können. Die Erfahrungen der letzten Jahre haben allerdings eindeutig gezeigt, dass eine hundertprozentige Umsetzung der Standards sich nicht mit den realen Nutzerforderungen deckt. Es liegt in der Natur der Sache, dass die Pflege dieser umfangreichen Architekturen und regelmäßigen Updates einer gewissen Trägheit unterworfen ist, die in keiner Weise mit der Schnelllebigkeit gerade im Bereich Digitalisierung Schritt halten kann.

roda setzt genau an diesem Punkt an und nutzt Komponenten, die bereits deutliches Aufwuchspotential aufweisen. Somit können neue Anforderungen, die über die bekannten Standards hinausgehen bereits im Vorfeld abgefangen werden und die Zukunftssicherheit der Systeme gewährleistet werden.

Autor

Matthias Renner ist Produkt-Manager roCCs12x bei der roda computer GmbH.

Gerade im Bereich Auflösung von Displays zeichnet sich ein Trend ab, dass Full HD (1920x1080) als ein Minimum angesehen wird, um das Potential moderner Kamerasysteme voll ausschöpfen zu können. „Situational Awareness" ist der Punkt, der zum Einsatz zahlreicher Kameras pro Fahrzeug führt, um z.B. eine Rundumsicht realisieren zu können. Der Einsatz zahlreicher HD-Kameras stellt enorme Anforderungen an die gesamte videoverarbeitende Infrastruktur. Gerade auch dann, wenn mehrere Quellen fusioniert werden und als Gesamtansicht dargestellt werden. Performante Prozessoren und eine leistungsfähige Bildverarbeitung werden hier eingesetzt, um Engpässe zu vermeiden und Latenzen auf ein Minimum zu reduzieren. Bezüglich Bandbreite im Netzwerk bietet roda 10-Gbit/s-Ethernet nicht mehr als Option an, sondern sieht diese Fähigkeit bereits als Grundkonfiguration vor. Der Trend geht eindeutig zu einer immer höheren Anzahl von Kameras.

Neben der reinen Hardware darf hier nicht vergessen werden, dass auch eine Softwareapplikation (Middleware) zum Einsatz kommen muss, die den Standards genügt und viele Funktionen abbildet. Die Hauptaufgabe der Software – um nur eine zu nennen – ist die Priorisierung, welche Informationen an welchem Anzeigegerät dargestellt werden.

Auch Upgrades oder Kampfwertsteigerungen von Bestandsfahrzeugen können durch den Einsatz von „Legacy Adaptern" nach aktuellen Standards realisiert werden. Diese Adapter ermöglichen die Einbindung von alten bzw. vorhandene Sensoren und Aktoren und erlauben somit auch die schrittweise Digitalisierung von Gesamtsystemen.

Im April 2020 unterzieht roda ein Vorserienmuster der „roda Common Crew Station" (roCCs) ersten Performancetests. Parallel dazu befindet sich ein Smart Display bereits in der Einsatzerprobung, was einen maßgeblichen Teil der Qualifikationsmaßnahmen ausmacht. Nach erfolgreichem Abschluss dieses Meilensteins ist ein Anlauf der Serienfertigung Mitte 2020 zu erwarten.

Foto: roda

roCCs12x – roda Common Crew Station (Smart Display)

roda hält an seinem bewährten Kurs fest, dem militärischen Kunden die größtmögliche Unterstützung zu bieten und als kompetenter Partner einen größeren Aufgabenbereich abzudecken. Zukünftig könnte durch den querschnittlichen Einsatz von immer mehr bewährter roda-IT in den Fahrzeugprogrammen die Logistikkette klein gehalten werden und auch das Änderungswesen und/oder das Obsoleszenz-Management können hiervon durch eine deutliche Vereinfachung profitieren.

roda computer GmbH
Matthias Renner
Produkt-Manager roCCs12x
Landstraße 6
77839 Lichtenau
m.renner@roda-computer.com
www.roda-computer.com

Führen und Kommunizieren mit den Systemen der ATM

Das Generieren von Informationsüberlegenheit als Voraussetzung für die Wirkungsüberlegenheit ist Aufgabe der Fahrzeug-IT. Dies erfordert das Vernetzen von Sensoren, Fahrzeugen und Befehlsständen. Zugleich ist die stete Funktionsfähigkeit der IT-Systeme zu sichern.

Die ATM ComputerSysteme GmbH entwickelt Mensch-Maschine-Schnittstellen sowie Systemlösungen für die Kommunikation. Die Life Cycle Software der ATM garantieren das Funktionieren im Einsatzraum.

Mensch und Maschine im Fokus

Als Plattformen sind die Fahrzeuge in einem Verbund digitaler Systeme zum Verarbeiten und Übertragen von Daten integriert. Zentrale Knoten dieses Netzes sind der Mensch, der Informationen im Fahrzeug in Entscheidungen umsetzt, und der taktische Router, der die Führungsmittel und Anwendungen mit dem Systemverbund vernetzt. Die Systemlösungen der ATM verknüpfen Sensoren und Anwendungen innerhalb des Fahrzeugs und verbinden nach außen.

Anbinden von Funk und Draht

Den interoperablen Austausch von Informationen von Anwender zu Anwender und von Fahrzeug zu Fahrzeug wickelt der Taktische Service Provider der ATM ab. Als das Kernelement im Kommunikationsverbund errichtet dieser ein sich-selbstorganisierendes, mobiles Ad-hoc-Netzwerk (MANET). In dieses integriert er alle Übertragungsmittel in ein einheitliches und grundsätzlich IP-fähiges Netz. Der Taktische Service Provider bindet somit bestehende wie zukünftige heterogene, schmal- und breitbandige Funk- und Drahtnetze sowie die Applikationen an. Damit erzeugt dieser die kommunikationstechnische Infrastruktur und erweist sich als Backbone der taktischen Kommunikation.

Als taktischer Router nimmt der Taktische Service Provider auf dem Gefechtsfeld die Spezialbehandlung von Blue Force Tracking, VoIP-Telefonie, Übertragen von analoger und verschlüsselter digitaler Sprache über VHF und UHF sowie latenzfreien Video- und Dateitransfer wahr. Basis bildet der im Heer eingeführte ATM Kommunikationsserver.

Die Schnittstellen zum Menschen

Der Verfügbarkeit taktischer Daten im Verbund folgen Anforderungen an die Mensch-Maschine-Schnittstelle. Für Lagebeurteilung und Entscheidungsschluss sind die Eigenschaften von Anzeige- und Bediengeräten wesentlich. Sie beeinflussen das Wahrnehmen der angezeigten Informationen und die Reaktionsfähigkeit der Mannschaft. Die ATM berücksichtigt

Der ATM-Kommunikationsserver sichert die streitkräfteübergreifende Kommunikation und gehört zur Standardausstattung des Heeres

ATM CENTURION i7 Fahrzeugrechner

Die skalierbare VistaMaster Display- und Panel-PC-Familie ist PCAP-fähig und erfüllt auf Anforderung die funktionale Sicherheit nach DIN EN 61508

Fotos und Grafiken: ATM

Life Cycle Software der ATM

onsfähigkeit der Fahrzeug-IT-Systeme. Mit Life Cycle Softwares unterstützt die ATM den Bediener im Einsatz, den Administrator und den Instandsetzer und erhöht die Einsatzbereitschaft des Fahrzeugs.
Als Online-Funktionsüberwachung sichert SysMon die Einsatzbereitschaft der IT-Ausstattung im operationellen Einsatz. SysCheck lokalisiert Fehler in KommServer, CENTURION, VistaMaster und 3rd Party Hardware.
Die Prüfsoftware DIANA diagnostiziert Fehler in IT-Rüstsätzen und unterstützt effizient das Warten in der Instandhaltungsstufe 2. Das Rescue-System dient dem Sichern und Wiederherstellen der operationellen System-Partition. Während die Admin-Tools Systemadministratoren bei der Administration von Rechnersystemen entlasten.

für ihre Bediengeräte, Display- und Panel-PC-Lösungen die Lesbarkeit und die Betrachtungswinkel unter allen Bedingungen sowie die Bedienbarkeit unter allen Umweltbedingungen. So versetzen die multitouchfähigen Displays der ATM den Bediener in die Lage, gleichzeitig mehrere Berührungspunkte zu erfassen. Dies bietet mehr Optionen zum Steuern der Anwendung.
Die Displaylösungen der ATM sind in Bezug auf Skalierung und Funktionsumfang an den Arbeitsplatz von Fahrer, Systembediener oder Kommandant adaptierbar. Das bringt Einsatzzwecke vom Display, Tochterdisplay oder Heckdisplay, über ein Display mit Terminalfunktion, bis hin zum zentralen Bedien- und Anzeigegerät hervor.

Das Herz der Fahrzeug-IT

Erfassen, Verarbeiten und Verteilen von Sensordaten und taktischen Informationen übernehmen die Server- und Computerlösungen der ATM. Sie optimieren die Informationen für Softwareoberflächen und den Kommunikationsverbund, bilden gesicherte VLANs und latenzfreies Verteilen der Informationen, führen managed/unmanaged Switche der ATM mit LWL und bidirektionale Datenübertragung durch.

Einhalten funktionaler Sicherheit

Sind sicherheitskritische Einrichtungen betroffen, zieht die ATM für ihre Systeme die funktionale Sicherheit nach DIN EN 61508 heran. Softwareentwicklungen gewährleisten, dass die Hardware das Sicherheitsintegritätslevel (SIL) erfüllt. Die ATM realisiert dies für zentrale Steuer- und Schaltgeräte, Bedien- und Anzeigegeräte und manuelle Kontrolleinrichtungen.

Sicherstellen der Funktionsfähigkeit

Das vernetzte Gefechtsfeld verlangt die permanente Funkti-

Bedien- und Anzeigegeräte der ATM, z. B. als Systembediengerät

ATM-Fahrzeugserver

Systemkompetenz für alle Situationen

Kommunizieren und Vernetzen, Steuern und Überwachen, Kontrollieren und Überprüfen – die ATM bietet individualisierte Lösungen in Hardware und Software zum Durchführen von Einsätzen auf dem digitalisierten Gefechtsfeld.

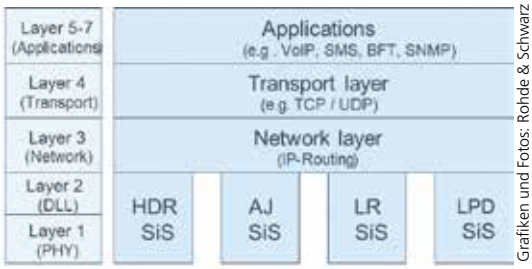
ATM Tec-Knowledge®

ATM ComputerSysteme GmbH
Max-Stromeyer-Straße 116
78467 Konstanz
Tel.: +49 7531 80 83
info@atm-computer.de
www.atm-computer.de

Technische Grundlagen der Wellenformen

Autorenteam Rohde & Schwarz

Eine Wellenform ist die Darstellung eines Signals als Verlauf der Amplitude über der Zeit. Dabei werden sämtliche Funkübertragungsfunktionen einer Verbindung Ende-zu-Ende, d. h. vom sendenden bis zum empfangenden Teilnehmer und umgekehrt, berücksichtigt.



Grafiken und Fotos: Rohde & Schwarz

HDR: High Data Rate (hohe Datenrate);
AJ: Anti-Jam (Modus gegen Störer);
LR: Long Range (große Reichweite);
LPD: Low Probability of Detection (geringe Entdeckungswahrscheinlichkeit);
SiS: Signals in Space (Funksignale im freien Raum)

- Auf der Bitübertragungsschicht (Layer 1, Physical Layer, PHY) und der Sicherungsschicht (Layer 2, Data Link Layer, DLL) des ISO/OSI-Referenzmodells lassen sich unterschiedliche Betriebsarten für eine IP-fähige Wellenform implementieren.
- Die Schichten 1 und 2 werden als Signals in Space (SiS) zusammengefasst:
  - SiS stellt die Kanalzugriffssteuerung (Channel Access Control) zur Verfügung,
  - SiS wandelt Bits und Bytes in Funksignale um und umgekehrt.
  - Die Verwendung des IP-Protokollstacks ermöglicht eine nahtlose Vernetzung über alle SiS.

Einsatzszenarien

Die unterschiedlichen Wellenformen, die mit softwaredefinierten Funkgeräten eingesetzt werden, müssen alle relevanten Anwendungen und Anforderungen abdecken wie z. B. Lagebild durch Standbild- und Live-Video-Übertragungen, operationelle Einsatzführung sowie sichere Sprachkommunikation. In der Entwicklung und dem Design von Wellenformen sind verschiedene Aspekte zu berücksichtigen:

- Robustheit und Mobilität,
- Störfestigkeit,
- geringe Entdeckungs- und Erfassungswahrscheinlichkeit
- hohe Datenraten
- große Reichweite und Abdeckung,
- Vernetzungsfähigkeit (MANET; Aufbau mobiler Ad-hoc-Netze) und Servicequalität (QoS)
- Anpassbarkeit.

Die einzelnen Eigenschaften beeinflussen sich zum Teil gegenseitig. Unterschiedliche Wellenformen sind erforderlich, um die Kommunikation (Sprache & Daten) an das jeweilige Einsatzszenario anzupassen.
Beispiel: Eine Wellenform für die Luft-Boden-Kommunikation muss auch bei der hohen Geschwindigkeit fliegender Plattformen definitionsgemäß funktionieren und daher Mechanismen zur Kompensation des Dopplereffekts aufweisen. Für Boden-Boden-Kommunikation hingegen besteht diese Forderung nicht.

Wellenformen für Line-Of-Sight (LOS)-Verbindungen

Wellenformen mit LOS-Fähigkeit (Funkübertragung analog einer Sichtverbindung) benötigen keine feste Infrastruktur wie z. B. Basisstationen. Diese Wellenformen sind für den Betrieb unter schwierigen Umgebungsbedingungen konzipiert, wobei unbedingt sichergestellt werden muss, dass mangelnde Netzstruktur nicht zu Störungen oder Ausfall der Kommunikation führt. Alle LOS-Wellenformen sind so ausgelegt, dass bei Punkt-zu-Punkt-Verbindungen sehr große Reichweiten erzielt werden können. LOS-Wellenformen für taktische Anwendungen werden hauptsächlich im Bereich von 30 MHz bis 600 MHz eingesetzt, mit dem Schwerpunkt auf wenigen Frequenzbändern. Militärische Wellenformen bieten Sicherheitsmerkmale auf höchstem Niveau, basierend auf COMSEC- und TRANSEC-Fähigkeiten wie z. B. Verschlüsselung und Frequenzsprungverfahren. Im militärischen Bereich ist durch leistungsstarke HF-Frontends außerdem Störresistenz implementiert; diese Frontends können große Signale mit engem Frequenzabstand ohne Beeinträchtigung der Empfangseigenschaften verarbeiten.
Diverse Wellenformen etwa der SOVERON WAVE-Familie bieten optimale Möglichkeiten für die sichere Übertragung hoher Datenraten in Umgebungen mit hoher Störbelastung für diverse Boden-Boden-, Luft-Luft- und kombinierte Boden-Luft-Boden-Szenarien. Mit SOVERON WAVE können Sprache und Daten gleichzeitig übertragen werden, womit sich die Anzahl zusätzlich erforderlicher Funkgeräte erheblich verringert. Mittels adaptiver IP-Vernetzung über große Bandbreiten tragen die Wellenformen zu einem verbesserten Lagebild bei. Die integrierte Fähigkeit zum Aufbau mobiler Ad-hoc-Netze (MANET) ermöglicht eine kontinuierlich stabile Kommunikation innerhalb agiler Netze, d.h. sich in Bewegung befindender Netzteilnehmer.

Wellenformen für Beyond-Line-Of-Sight (BLOS)-Verbindungen

BLOS-Verbindungen (Funkübertragung über die Sichtverbindung hinaus) dienen hauptsächlich dem Zweck, Kommunikation über große Reichweiten zu ermöglichen, ohne dass feste Infrastruktur erforderlich ist. Die Funkkommunikation im HF-Bereich bietet einen großen Vorteil: Elektromagnetische Signale zwischen 1,5 MHz und 30 MHz werden an der Ionosphäre reflektiert,

und mit diesem Effekt lassen sich extrem große Reichweiten von mehreren Tausend Kilometern zwischen Sender und Empfänger erzielen.
Moderne ALE-Standards (ALE: Automatic Link Establishment) ermöglichen den automatischen Verbindungsaufbau zwischen Kommunikationspartnern zu jeder Zeit und unter allen ionosphärischen Bedingungen. Die dabei eingesetzten Verfahren nutzen Informationen zur Sonnenaktivität, zur geographischen Position der Kommunikationspartner und der exakten Zeit. Der verfügbare Frequenzbereich wird gescannt und mit dem verfügbaren Frequenzbereich potentieller Kommunikationspartner koordiniert. Die Ergebnisse möglicher Verbindungen in Abhängigkeit von der Frequenz werden in den Funkgeräten gespeichert und laufend aktualisiert.
Mit der Entwicklung neuer Technologien wie Wideband HF (WBHF) ist die Kommunikation im HF-Bereich nicht mehr auf die Sprachübertragung bzw. die Übertragung sehr niedriger Datenraten reduziert. Sie kann nun auch Daten, Bilder und Video über IP-Technologie übertragen und somit zu einer kostengünstigen und schnell verfügbaren Alternative zur Satellitenübertragung werden.

Die taktische Kommunikation lässt sich durch den Einsatz unterschiedlicher Wellenformen optimieren

Umsetzung technischer Fähigkeiten in operativen Nutzen:

Technische Fähigkeiten	Operationelle Vorteile
▪ IP ▪ MANET	Vernetzungsfähigkeit Sprache & Daten parallel
SCA-Architektur für militärische SDR	Interoperabilität (teilstreitkräftebezogen, teilstreitkräfteübergreifend, multinational)
Lösungen mit hohem Sicherheitsstandard	Informationssicherheit (einschließlich nationaler Sicherheit)
▪ Breitband-Technologie ▪ Multiband-Technologie	Hohe Datenraten Weiter Frequenzbereich

Beispielsweise bietet die Verwendung SCA-basierter Wellenformen (SCA: Software Communications Architecture) für softwaredefinierte Funkgeräte (Software Defined Radios, SDR) folgende Vorteile:

- Unabhängigkeit der Software von spezifischen Hardwarelösungen,
- Skalierbarkeit hinsichtlich der Funkkanäle und Funkplattformen (von Handfunkgeräten bis zu Versionen für fliegende Plattformen),
- Portabilität der Applikationssoftware zwischen unterschiedlichen SCA-Implementierungen,
- verkürzte Entwicklungszeiten für neue Wellenformen durch die Wiederverwendung von Softwaremodulen.

Interoperabilität spielt nicht nur für den Schutz nationaler Interessen eine wichtige Rolle; sie ist auch unerlässlich für alliierte Missionen.

ESSOR

Mitte Dezember hat der Deutsche Bundestag im Haushalts- und Verteidigungsausschuss dem Beitritt zu ESSOR (European Secure Software Defined Radio) zugestimmt, der transeuropäischen Interoperabilitätsinitiative für Streitkräfte auf der taktischen Ebene. Mit der Billigung der Beitrittsvorlage wurde auch die nationale Realisierung der laufenden Stufe OC1 (Operational Capability) der ESSOR-Breitbandwellenform mit auf den Weg gebracht, die ein Teil des Großvorhabens „Digitalisierung landbasierter Operationen" (D-LBO) ist. Rohde & Schwarz ist als nationaler Champion benannt und in den Kreis der seit dem Jahr 2008 ESSOR realisierenden Unternehmen aus den Mitgliedsstaaten eingetreten.
ESSOR ist ein von der OCCAR (die gemeinsame Organisation für Rüstungskooperation) geführtes Langzeitprojekt, in dem Italien, Spanien, Frankreich, Finnland, Polen und nun Deutschland mit je einem „nationalen Champion" das Gemeinschaftsunternehmen a4ESSOR S.A.S. führen. Übergeordnetes Ziel ist die Weiterentwicklung der Fähigkeiten im Bereich der sicheren Kommunikationstechnologien zur Verbesserung der Interoperabilität der Streitkräfte. Konkret beschreibt ESSOR OC1 die gemeinsame Entwicklung und Fortschreibung einer interoperablen, vertrauenswürdigen, robusten und breitbandigen Funkwellenform für die Vernetzung der Streitkräfte.
Rohde & Schwarz ist auf dem Gebiet der Software Defined Radios und dazugehöriger Wellenformen durch langjährige Eigenentwicklungen sowie das für die Bundeswehr 2020 erstmals in Serie zulaufende SOVERON D (bekannt aus dem Entwicklungsprojekt SVFuA) dafür bestens aufgestellt.
Die Im Rahmen von ESSOR OC1 entstehende Wellenform HDRWF (High Data Rate WaveForm) ist für die operative wie taktische Truppenführung und IP-Vernetzung auf den Ebenen Brigade, Bataillon und darunter ausgelegt. Sie zeichnet sich durch eine flexible Konfiguration und Anpassungsfähigkeit an anspruchsvolle Szenarien aus und bietet den Soldatinnen und Soldaten auf ihren nationalen Funkgerätesystemen flexible robuste MANET-Netze für multinationale Einsätze und im Rahmen der Landes- und Bündnisverteidigung.
ESSOR wird durch den Europäischen Verteidigungsfonds auch um weitere Wellenformen wachsen, etwa für spezielle Anwendungsfälle oder für luftgestützte Operationsführung. Die Zusammenarbeit der europäischen Industrie und die Bereitstellung des modernsten am Markt verfügbaren SDR in Form des SOVERON D, wird Großvorhaben wie D-LBO der Bundeswehr einen gewaltigen Schritt in der vernetzten, gesicherten und störfesten Übertragung von Sprache und Daten weiterbringen. ■

Bittium

Lieferung der nächsten Generation robuster taktischer SDR

Die Tactical Wireless IP Network (TAC WIN) Funkgerätefamilie des finnischen Unternehmens Bittium ist weltweit im Einsatz. Nun beginnt eine groß angelegte Lieferung einer neuen Produktfamilie taktischer Software Defined Radios (SDRs) der nächsten Generation. Diese neue Generation umfasst das Bittium Tough SDR Handheld für abgesessene Soldaten und das Bittium Tough SDR Vehicular für Fahrzeugeinrichtungen.

Die taktischen Funkgeräte sind das Ergebnis langjähriger Forschung und Entwicklung von softwaredefinierten Funkgeräten sowie der Entwicklung von taktischen Netzwerklösungen. Nach dem Erfolg des Bittium TAC WIN als drahtloses Backbone-Netzwerk für die Modernisierung der taktischen Kommunikation erweitert die neue Gerätefamilie das Produktangebot auf taktische Funkgeräte für einzelne Soldaten und Fahrzeuge. Dies ermöglicht die Übertragung von Breitband-Daten und Sprache an alle mobilen Truppenteile, von der Brigadeebene bis hin zum gesamten Gefechtsfeld.

Die Handfunkgeräte und Fahrzeugfunkgeräte können allein oder zusammen mit dem TAC WIN-Netzwerk eingesetzt werden, um eine verlässliche Lage in Echtzeit zu erzeugen und auszutauschen, einschließlich Standort-, Bild-, Sprach-, Video- und Sensordaten. Dies verbessert die Leistung und die Kampfkraft der taktischen Truppen. Die Führung der Soldaten und Einheiten wird zudem auf der Grundlage des aktuellen Lagebildes und der zuverlässigeren Verbindungen erleichtert.

Taktische SDR-Lösungen von Bittium

Fotos: Bittium

Interoperabilität mit ESSOR

Die beiden Funkplattformen sind mit einem Satz von Wellenformen versehen. Sie können mit der Breitband-Bittium TAC WIN Wellenform, die bereits mit dem Bittium TAC WIN-System in Betrieb ist, und der proprietären Bittium Narrowband Wellenform verwendet werden. Die dritte Option besteht darin, die ESSOR High Data Rate Wellenform zu verwenden. Bittium ist seit der Einführung des European Secure Software Defined Radio (ESSOR)-Programms, mit dem die EU eine einheitliche Wellenform entwickeln und zur Verfügung stellen will, im Jahr 2009 ein nationaler Partner. Derzeit verbessert das Programm die operativen Fähigkeiten der ESSOR-Wellenform. Mit der Wellenform werden der Breitband-Datentransfer sowie die Zusammenarbeit und direkte Kommunikation zwischen verschiedenen nationalen Truppen auf der Patrouillenebene bereits mit ESSOR ermöglicht.

Die Hand- und Fahrzeugfunkgeräte können flexibel die am besten geeignete Wellenform mit der besten Anpassung an die Bedingungen und den Auftrag verwenden. Die Verwendung mehrerer Wellenformen, auch gleichzeitig, verbessert dabei die Kompatibilität und ermöglicht Operationen auf verschiedenen Ebenen und Missionen. Die Portabilität der Wellenformen ermöglicht die nahtlose Portierung von älteren oder nationalen proprietären Wellenformen mit den nationalen COMSEC und TRANSEC.

Das robuste SDR-Vehicular ist mit zwei unabhängigen Kanälen ausgestattet, die gleichzeitig eine Instanz von TAC WIN-, ESSOR- oder Schmalbandwellenformen

Tactical Wireless IP Network (TAC WIN) Funkgeräte ermöglichen die Übertragung von Breitband-Daten und Sprache an alle mobilen Truppenteile

ausführen können. Dadurch kann das Fahrzeugfunkgerät automatisch eine Verbindung mit dem TAC WIN-Backbone herstellen und autonom mit anderen taktischen SDRs, wie z.B. dem Tough SDR Handheld mit ESSOR oder der Schmalbandwellenform, vernetzt werden.

Lösungen für abgesessene Truppen

Das Bittium Tough SDR-Handfunkgerät liefert Sprache und Daten über einen breiten Frequenzbereich, von 30 MHz bis 2500 MHz, für den abgesessenen Soldaten sowie Trupp- oder Zugführer. Dieses einzigartig breite Frequenzband verbessert die Überlebensfähigkeit im Kampf erheblich.
Das Funkgerät eignet sich perfekt als Ersatz für ältere Handfunkgeräte, die bei verschiedenen Streitkräften immer noch im Einsatz sind. Es trägt somit zur Modernisierung der taktischen Kommunikationsinfrastruktur bei, indem es Daten aus der Bewegung, ein verbessertes Situationsbewusstsein und C2-Anwendungen für abgesetzte Truppen ermöglicht. Nicht zu vergessen eine auf den Nutzer optimierte Benutzeroberfläche für eine einfache und intuitive Bedienung.
Die Verwaltung der Geräte im Einsatz wird durch die taktische Gerätemanagement-Suite erleichtert, die es den Bedienern beispielsweise ermöglicht, den Funk über eine Web-Schnittstelle zu konfigurieren und ferngesteuerte Software-Upgrades durchzuführen. Das Funkgerät verfügt außerdem über eine sichere Anwendungs-Sandbox, die Flexibilität für die Integration verschiedener C2-Anwendungen wie das Battle Management System und/oder Blue Force Tracking sowie andere kundeneigene Konfigurationen bietet.
Zu den weiteren Merkmalen des Handheld gehören die kabelgebundene oder drahtlose Integration mit taktischen COTS-Tablets oder Smartphones, einschließlich der extrem sicheren Smartphones der Bittium Tough Mobile Produktfamilie mit Android OS.

Die Einführung beginnt in Finnland

Zunächst beginnt Bittium mit den groß angelegten Lieferungen der robusten SDR-Funkgeräte an die finnischen Streitkräfte. Die Hand- und Fahrzeugfunkgeräte erneuern den bestehenden Bestand an Funkgeräten in den finnischen Streitkräften mit modernen, breitbandigen Datenübertragungsfunkgeräten. Hierdurch wird die Neuausrichtung und Digitalisierung der finnischen Streitkräfte unterstützt, dies im Zusammenspiel mit Bittium TAC WIN, das bereits von den finnischen Streitkräften eingesetzt wird. In der ersten Phase gehen die neuen taktischen Funkgeräte an das finnische Heer.
Der Vertrag zwischen Bittium und den finnischen Streitkräften umfasst neben dem ursprünglichen Auftrag von bis zu 10,5 Millionen Euro weitere Kaufoptionen im Wert von bis zu 207 Millionen Euro. Dementsprechend haben die finnischen Streitkräfte eine Option auf den Kauf zusätzlicher taktischer Funkgeräte und des entsprechenden Zubehörs, der Ausbildung und des Systemmanagements für den Einsatz bei Heer, Luftwaffe und Marine.

Weitere Kunden

Bittium hat auch die Tough SDR Vehicular Radios zusammen mit der ESSOR HDR Wellenform an die Pilotfahrzeuge des VCR 8x8-Fahrzeugprogramms des spanischen Heeres geliefert, um die Fähigkeiten und die Leistung des Systems zu demonstrieren. Darüber hinaus begannen Ende 2019 die Lieferungen an die estnischen Streitkräfte. In Estland wird mit der Lieferung von Bittium Tough SDR-Funkgeräten und den Produkten des Bittium TAC WIN-Systems die Reform zur Verbesserung der IP-Datenübertragungsfähigkeit und -verfügbarkeit der estnischen Landstreitkräfte fortgeführt.
Auch Österreich modernisiert seine taktische Kommunikation mittels des Bittium TAC WIN-Systems als neues IP-basiertes taktisches Kommunikationssystem für die österreichischen Streitkräfte.
Die nahtlos miteinander verbundene, konfigurierbare Familie von taktischen Funkgeräten wird Kunden in aller Welt angeboten. Die Funkgeräte sind in der Lage hochmobile Truppenteile zu unterstützen, die ein widerstandsfähiges, anpassungsfähiges und sicheres Netzwerk aufbauen müssen. Zusammen mit Bittium TAC WIN spiegelt das gesamte Portfolio eine Designphilosophie wieder, die auf verbesserte Benutzerfreundlichkeit, einfache Wartung und leichte Konfigurierbarkeit abzielt.

Bittium Tough SDR

Bittium Germany GmbH
Thomas Zieger
Rosenheimer Str. 143 C
81671 München, Deutschland
Tel.: 0160 – 90633833
thomas.zieger@bittium.com
www.bittium.com

Imtradex

Kommunikation und Gehörschutz für Spezialisten

Kristallklare Kommunikation in lauten Umgebungen in Verbindung mit Gehörschutz und der hervorragenden Wahrnehmung von Umgebungsgeräuschen ist für Soldaten und Gesetzeshüter, wie beispielsweise Polizisten, ein taktischer Vorteil und im Zweifel ein Lebensretter.

Beeinträchtigung des Gehörs ist kritisch

Sicherheitskräfte und Militäreinheiten im Feld sind oft hohen und somit kritischen Lautstärken ausgesetzt, die die Einsatzkommunikation beeinträchtigen und das Gehör schädigen können. Gehörschädigung ist eine der am meisten vorkommenden Verletzungen aus dem aktiven Dienst.
Die Gehörschädigung führt zu einer reduzierten Wahrnehmung der Umgebung und reduziert die Fähigkeit, Gefährdungen, Distanzen und die Lokalisierung von Geräuschen korrekt wahrzunehmen. Darüber hinaus erschwert es die Kommunikation und Koordination für taktische Einsatzzwecke.

Erhalt der Umgebungswahrnehmung

Der Schutz des Gehörs ist nur ein Teil. Der zweite Teil ist der Erhalt der bestmöglichen Umgebungsgeräuschwahrnehmung. Die seit Jahren verfügbaren Gehörschutzsysteme sind nicht immer die beste Methode, denn einige Nutzer wollten den zur Verfügung stehenden Gehörschutz einfach nicht tragen. Der Grund ist sehr einfach, sobald der Hörsinn beeinflusst wird, fällt uns die Kommunikation schwerer und die Überlebenschance sinkt.
Die INVISIO Systeme nutzen neueste digitale Signalprozessoren, miniaturisierte Audio-Komponenten und ergonomische Headset-Designs für die beste und natürlichste Wahrnehmung der Umgebung – auch unter schwierigen Bedingungen. Moderne miniaturisierte Lautsprecher und Mikrofone reproduzieren den natürlichen Klang. Digitale Signalprozessoren sorgen dafür, dass die Umgebung natürlich und verzerrungsfrei wahrgenommen wird, gleichzeitig aber auch das Audio-Level eine gefährliche Schwelle nicht überschreitet.

Foto: Invisio

Die INVISIO-Lösung basiert auf einem vollständig interoperablen System, bestehend aus der richtigen Headset Lösung sowie den dazugehörigen Anschlusskabeln und den taktischen Kommunikationseinheiten

Kristallklare Kommunikation – auch unter schwierigen Bedingungen

Die Kommunikationssysteme von INVISIO übertragen kristallklar jeden Befehl, auch bei widrigen Bedingungen des täglichen Einsatzes. Eine Schlüsseltechnologie hierbei ist die INVISIO-Knochenschalltechnologie. Die Übertragung erfolgt – im Gegensatz zur klassischen Sprachübertragung – nicht mit Schallwellen, sondern mit Vibration. Diese wird mit einem In-Ohr-Mikrofon vom Kieferknochen abgenommen. Dadurch kann in nahezu allen Umgebungen die Sprache extrem klar aufgenommen und weitergegeben werden, auch beim Flüstern.
Die INVISIO-Systeme können einfach an unterschiedlichste Kommunikationsmittel wie Funkgeräte, Mobiltelefone, Interkom-Systeme, Computer oder ähnliches angebunden werden.

Fakten zur Hörschädigung durch Lärmbelastung

In den USA wurden im Jahr 2016 über 1,5 Milliarden US-Dollar für Verletzungen aufgebracht, die auf Hörschädigungen durch Lärmbelastungen im Militär zurückzuführen sind. Damit ist es die meist verbreitete Arbeitsunfähigkeit.
Belastung durch gefährlichen Lärm ist kritisch, da das Gehör nicht repariert werden kann.
Durch eine Hörschädigung sinkt auch die Lebensqualität.

Quelle: US Department of Veteran Affairs

INVISIO-Systeme schützen und befähigen

IMTRADEX liefert Ihnen die INVISIO-Lösung für ihre taktische Kommunikation und den Schutz des Gehörs. Basierend auf einem vollständig interoperablen System, bestehend aus der richtigen Headset-Lösung sowie den dazugehörigen Anschlusskabeln und den taktischen Kommunikationseinheiten. Bei den Headsets gibt es In-Ohr- und Über-dem-Ohr-Varianten sowie wassergeschützte oder leichte Varianten. Die Kommunikationseinheiten gehen von 1-kanaligen Varianten bis zu einer 4-kanaligen Varianten für mehrkanalige Kommunikation.
Alle Systeme werden durch die patentierte INVISIO-IntelliCable®-Technologie unterstützt. Die einzigartige Erkennung unterstützt die automatische Erkennung bei Hot-Swap und setzt automatisch die richtigen Audio-Parameter. Durch diese Funktionalität wird neues Equipment einfach mit dem richtigen Kabel angeschlossen.

Langfristige Bindung und Zusage

Bereits in über 50 Nationen wird das System verlässlich und vom Nutzer akzeptiert eingesetzt. Mehr als 200.000 Systeme sind ausgeliefert und werden weltweit in unterschiedlichsten Einsatzgebieten und Klimazonen genutzt. Die INVISIO erfüllt zahllose technische Regularien und Standards und hat ein umfangreiches Qualitätsmanagementsystem. Das Verständnis für Qualität ist ein essentieller Faktor für den täglichen Einsatz der Produkte in den härtesten Umgebungen auf der ganzen Welt.

Imtradex

Imtradex Hör-/ Sprechsysteme GmbH
Daimlerstrasse 23
63303 Dreieich
Telefon: +49 6103 485 69 40
info@imtradex.de
www.imtradex.de

SYSTEMATIC

C4I-Software für die Digitalisierung der Bundeswehr

Sven Trusch

Noch immer steht die Bundeswehr vor der Herausforderung, die Strategie zur Digitalisierung der Streitkräfte umzusetzen. Im Bereich der Führungsinformationssysteme blickt man weiterhin auf eine heterogene Systemlandschaft, die jedoch bereits sukzessive in eine durchgängig serviceorientierte Architektur überführt wird. Die Serviceerstellung des Mission Enabling Service Bundeswehr (MESBw) in den Ausprägungen Command Post, Mountable und Portable leistet dazu einen wesentlichen Beitrag.

Die Herausforderungen der Interoperabilität in multinationalen Einsätzen sowie der Intraoperabilität, also dem Zusammenwirken von Systemen innerhalb der Streitkräfte, stehen dabei weiterhin im Fokus der Aktivitäten. Die Landstreitkräfte haben mit dem Programm D-LBO eine Roadmap entwickelt, um die Führungsfähigkeit in Landoperationen signifikant und nachhaltig zu verbessern. Ein Battle Management System (BMS) wird in dieser Architektur Sensoren, Effektoren in den Führungsprozess einbinden, und einen durchgängigen Systemverbund herstellen. Aufbauend auf die Erfahrungen aus dem bereits gestarteten Projekt BMS für die Very High Readiness Joint Task Force Land (VJTF(L)) 2023 müssen bei D-LBO noch die Kommunikationsinfrastruktur modernisiert und der Grad der Integration und Automatisierung erhöht werden.

Außerhalb von D-LBO besteht ebenfalls Handlungsbedarf, um die Harmonisierung der Führungssysteme voranzutreiben. Der MESBw Command Post kann hier als einheitliche Grundlage für zukünftige Entwicklungen dienen, um die Heterogenität der Systemlandschaft weiter zu reduzieren. Wird dieser nur um die jeweils benötigten Fähigkeiten in Form von Modulen erweitert, werden erhebliche Synergien freigesetzt und die Effizienz der eingesetzten Mittel maßgeblich erhöht. Dies muss im bestehenden Rüstungsprozess jedoch durch zentrale Vorgaben umgesetzt werden, da sonst die eher projektorientierten Prozesse eine solche Harmonisierung verhindern.

Fotos: Systematic

SitaWare Headquarters und IRIS Forms für stationäre und verlegefähige Gefechtsstände sowie seegehende Plattformen

Systematic SitaWare Suite

Die Systematic SitaWare Suite stellt IT-Services über skalierbare Module bereit, welche als Lagedienst in stationären, verlegefähigen und mobilen 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 31 Nutzernationen ist SitaWare heute die meistverbreitete C4I-Suite weltweit. Die einzelnen Military-off-the-Shelf (MOTS)-Produkte 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 damit Standards für den Datenaustausch in multinationalen Operationen. In SitaWare sind alle gängigen militärischen und zivilen Standards für den Datenaustausch implementiert, wodurch sowohl die Intra- als auch die Interoperabilität gewährleistet wird. Proprietäre Systeme, beispielsweise Führungs- und Waffeneinsatzsysteme (FüWES), können risikoarm über vollständig dokumentierte und offene Schnittstellen, wie zum Beispiel Web-Services, angebunden oder integriert werden.

Autor

Sven Trusch ist Vice President Business Development bei Systematic.

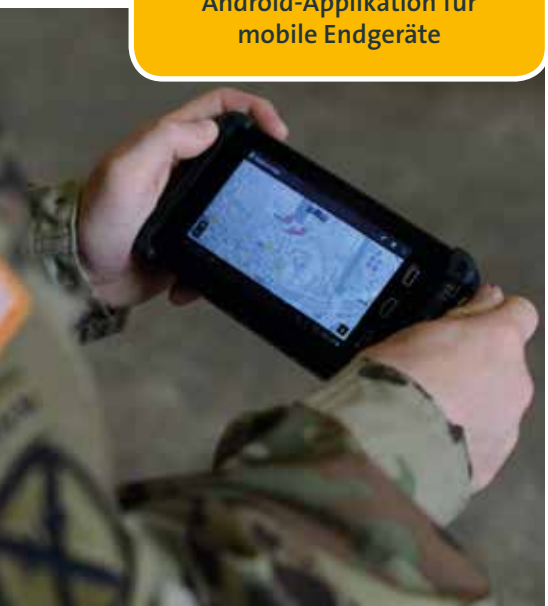
Battle Management Systeme liefern einen wesentlichen Beitrag zur Digitalisierung landbasierter Operationen

Durch vorhandene APIs sowie unter Nutzung des Software Development Kits (SDK) ist die risikoarme und herstellerunabhängige Integration in komplexe Gesamtsysteme möglich. Zahlreiche nationale und internationale Beispiele belegen die kosteneffiziente Integration in die Kommunikationsinfrastruktur – aber auch in das IT-System von Plattformen. Diese Integrationen werden oftmals durch lokale Partnerunternehmen durchgeführt, die mit Systematic zusammenarbeiten.

SitaWare Tactical Communication

Die Datenkommunikation wird durch den Kommunikationsdienst SitaWare Tactical Communication (STC) gewährleistet. STC ist ein hardwareagnostischer Dienst der speziell für die effiziente Nutzung taktischer Kommunikationsmittel entwickelt wurde. Im Vordergrund der Entwicklung stand die Anforderung, auch mit veralteten analogen Funkgeräten ein performantes Friendly Force Tracking (FFT) sicherzustellen.

SitaWare Edge ist eine Android-Applikation für mobile Endgeräte



STC unterstützt sowohl taktische Funkgeräte unterschiedlichster Hersteller, als auch moderne Kommunikationsmittel wie Sattelitenkommunikation, WiFi und LTE/5G-Technologien. Im Rahmen von verschiedenen Projekten wurden bereits viele, in die Bundeswehr eingeführte, Kommunikationsmittel integriert und die Überlegenheit in der Leistungsfähigkeit gegenüber sich in der Nutzung befindlichen Systemen unter Beweis gestellt.
Insbesondere bei einer heterogenen Ausstattung eines Truppenteils bezüglich der Funkgeräte, kann STC die medienbruchfreie und automatisierte Datenkommunikation sicherstellen. Unterschiedliche Funkkreise bzw. Subnetze werden hierbei zu einem gemeinsamen Kommunikationsverbund zusammengeschlossen und ohne Zutun des Bedieners nutzbar gemacht.
Systematic hat bereits eine Vielzahl an militärischen Funkgeräten in weltweiten Projekten integriert, bzw. unterhält hierzu Kooperationen mit den relevanten Funkgeräteherstellern. STC unterstützt somit die Kommunikationsmittel von heute – aber auch von morgen!

SitaWare @ Deutsche Bundeswehr

SitaWare steht bereits Teilen der Bundeswehr zur Verfügung. Insbesondere die Einführung von SitaWare Headquarters im Rahmen der Produktverbesserung des Führungsinformationssystems des Heeres ermöglicht die intensive Nutzung in Einsatz und Übung. Das Produkt ist hier ein wesentlicher Bestandteil für die Interoperabilität des Heeres im multinationalen Umfeld. Im Jahr 2019 konnte sich SitaWare Frontline im internationalen Wettbewerb für das BMS für VJTF(L) 2023 durchsetzen und die Einführung wird aktuell vorbereitet. Weiterhin steht SitaWare Headquarters auf der HaFIS IT-Plattform als aktuelle Ausprägung des MESBw (HaFIS) zur Verfügung. Der MESBw wird sowohl zur Lageführung des Einsatzes Resolute Support als auch für die Planung und Durchführung von Militärischen Evakuierungsoperationen eingesetzt. Komplementiert wird die Fähigkeit durch die Nutzung des Produkts IRIS Forms, welches den meldungsbasierten Informationsaustausch sicherstellt – bei der Deutschen Marine bereits seit 25 Jahren.
SitaWare unterstützt neben Landoperationen im gleichen Maße die Operationen der See- und Luftstreitkräfte. Mit dem Maritime Add-on wurden im vergangenen Jahr spezifische Funktionalitäten für maritime Anwendungsfälle entwickelt und stehen nun zur sofortigen Nutzung bereit. Andere Nationen nutzen SitaWare bereits auf seegehenden Plattformen im Einsatz sowie in Luftfahrzeugen zu Aufklärungszwecken, um das gemeinsame Lagebild zu verdichten.
Für das zukünftige IT-System der Bundeswehr kann die SitaWare-Suite ein C4I-Ökosystem sein, welches querschnittliche Funktionalitäten, beispielsweise Karten-/Lagedarstellung, Interoperabilität, Chat und Datenkommunikation, bereitstellt und dann um Truppengattungs- und Teilstreitkaft-spezifische Funktionalitäten erweitert werden kann. So können Entwicklungsrisiken zukünftig minimiert und einheitliche und durchgängige Lagedienste geschaffen werden. Bereits heute stehen entlang dieses Konzepts modulare Erweiterungen für die Feuerunterstützung, die ABC-Abwehr sowie die Luftnahunterstützung zur Verfügung. Weitere Module können durch Partnerunternehmen oder die Bundeswehr selbst entlang der spezifischen Ansprüche entwickelt werden.
Insgesamt bietet SitaWare viele Möglichkeiten, um die aktuellen Herausforderungen der Digitalisierung zu bewältigen. Insbesondere die sofortige Verfügbarkeit, die hohe Produktreife sowie die vorhersehbaren Lebenszykluskosten unterstreichen den Mehrwert der Lösung.

SYSTEMATIC

Systematic GmbH
Im Zollhafen 24
50678 Köln
Tel.: 0221 – 650783 71
more.info.de@systematic.com
www.systematic.com

ESG DEFENCE + PUBLIC SECURITY

Digitalisierung der Artillerie

Erfolgsbeispiel „Streitkräftegemeinsame Taktische Feuerunterstützung“

Andreas Schiel

1995 wurde in die deutsche Artillerie das Führungs- und Waffeneinsatzsystem (FüWES) ADLER (Artillerie-, Daten-, Lage-, Einsatz-, Rechnerverbund) eingeführt. Seitdem verfügt die Artillerietruppe über einen digitalisierten Verbund aller relevanten Daten des gesamten Gefechtsfelds einer Division.

Treiber für die Entwicklung und Einführung des Systems waren die durch die Digitalisierung erreichbaren operativen Vorteile gegenüber einem potenziellen Gegner: Dieser Verbund ermöglichte es erstmalig, dass jeder Sensor auf die Effektor-Ressourcen der gesamten Division zugreifen kann. Zuvor waren lediglich die Ressourcen in direkter Funkreichweite sinnvoll integrierbar. Durch die Nutzung der Schnittstelle zu ASCA (Artillery Systems Cooperation Activities) ist es nunmehr sogar möglich, die Ressourcen anderer Nationen nutzbar zu machen, ohne zusätzlichen Koordinierungsaufwand, da die unterschiedlichen nationalen Verfahren ebenfalls automatisiert über ASCA abgeglichen werden.
Das erweiterte Ressourcen-Management sowie die digital jederzeit sichtbare Einsatzbereitschaft aller Effektoren ermöglichte die Einführung eines dynamischen Feuerstellungskonzepts (Shoot-and-Scoot/Feuer und Bewegung). Dies wirkte sich direkt positiv auf die Überlebensfähigkeit der eigenen Effektoren aus, da die Wahrscheinlichkeit, gegnerischem Artilleriefeuer zu entgehen, signifikant erhöht wurde.
Darüber hinaus wurde die Bekämpfungszeit von Zielen auf unter fünf Minuten reduziert, was ausschließlich durch die digitale Übertragung der Ziel- wie auch Bekämpfungsdaten zurückzuführen ist. So wurde erstmalig der heute gern genutzte Begriff des Sensor-to-Shooter-Verbunds realisiert.

Autor

Andreas Schiel ist Leiter Führungssysteme & Joint Fire Support, ESG Elektroniksystem- und Logistik-GmbH.

Nächster Meilenstein: STF

Mit der Umsetzung des Konzepts der „Streitkräftegemeinsamen Taktischen Feuerunterstützung“ (STF) wurde auch die Produktverbesserung ADLER beauftragt in deren Rahmen das FüWES ADLER III entwickelt wurde. Dabei wurde die „Informationsinsel“ Artillerie an das 2006 in die Bundeswehr eingeführte „Führungsinformationssystem Heer“ (FüInfoSys Heer) angebunden und der bidirektionale Austausch von Lageinformationen, Meldung und Feueranforderungen ermöglicht.

Mit ADLER III als Rückgrat der STF und weiteren Projekten wie dem „Schnittstellentrupp Taktische Datenlinks Joint Fire Support“ (SstTrp TDL JFS) und der „Joint Fire Support Coordination Group“ (JFSCG) wurde ein gemeinsamer digitalisierter Informationsraum zur gegenseitigen Unterstützung mit Sensoren und Effektoren zwischen Heer, Luftwaffe und Marine geschaffen. Dabei muss explizit hervorgehoben werden, dass durch die Nutzung von Link 16 und VMF (Variable Message Format) auch die Anbindung an die Luftstreitkräfte anderer Nationen gewährleistet wird. In der Kombination ASCA mit seinen 27 Nationen (neun „Participants“, sieben „Sponsored Nations“, sieben „Observer Nations“ und vier „Interested Nations“) und der Anbindung über Link 16 sowie VMF ist der ADLER-Verbund der einzige multinationale wie auch teilstreitkraftübergreifende Verbund, der bereits mehrfach seine Einsatzbereitschaft in realem Umfeld und nicht nur in computergestützten Übungen erfolgreich nachgewiesen hat. In diesem Rahmen wurde erstmals auch der bidirektionale Informationsaustausch mit dem FüWES ADLER über die Sicherheitsdomänen „Verschlusssache – Nur für den Dienstgebrauch“ (VS-NFD) und „GEHEIM“ automatisiert sichergestellt und erfolgreich durch den deutschen Anteil der „military Security Authorisation Authority“ (DEUmilSAA) akkreditiert.
Die JFSCG schafft im ersten Schritt den gemeinsamen physischen Arbeitsraum aller beteiligten Elemente (d.h. Heer, Luftwaffe, Marine) mit bis zu 16 IT-Arbeitsplätzen, diversen Servern und einer Medienwand. Die Arbeitsplätze können sowohl innerhalb eines koppelbaren Containersystems (bestehend aus vier Containern) als auch in der mobilen Variante in Zelten oder ortsfester Infrastruktur genutzt werden.
Im kommenden Schritt werden mit einem „Entscheidungsunterstützenden System“

Die Schnittstellentrupps müssen in fast jedem Gelände bei fast jedem Wetter die Einsatzbereitschaft sicherstellen

Foto: ESG

(EUS) die unterschiedlichen Informationsräume der in der JFSCG eingerüsteten Softwaresysteme in einen gemeinsamen Informationsraum überführt, um so neben dem physischen auch einen einheitlichen informationsbasierten Arbeitsraum aller Zellen zur gewährleisten. Dies ermöglicht dann erstmals ein abgestimmtes Arbeiten aller verantwortlichen Teilbereiche der STF mit einem System.

D-LBO und Chancen der KI

Im Zusammenhang mit der „Digitalisierung landbasierter Operationen" (D-LBO) stellt sich die Frage, wie sich der hier dargestellte Verbund in der Zukunft weiterentwickeln kann. Trotz aller Besonderheiten in der Infrastruktur der militärischen Nutzer insbesondere bei der robusten Datenübertragung erscheint ein genauer Blick auf zivile Entwicklungen der IT-Industrie ausgesprochen sinnvoll. Daraus ließen sich künftige Anforderungen und vielversprechende Chancen ableiten.
So wird es beispielsweise immer weniger monolithische Systeme geben, die alle Anforderungen eines Nutzers einzeln erfüllen. Vielmehr ist von immer mehr spezialisierten Diensten auszugehen (d.h. Microservices), die von verschiedenen Applikationen genutzt werden können. Dies ermöglicht zum einen eine deutlich höhere Flexibilität bei der Nutzung, erhöht aber auf der anderen Seite auch den Koordinierungsaufwand bei Wartung und Pflege des Gesamtsystems.
Als fast schon klassisches Beispiel im Umfeld von Führungsinformations- bzw. Führungs- und Waffeneinsatzsystemen sei hier die Verwendung eines einheitlichen Symboldienstes für die Generierung von taktischen Symbolen genannt: Würde hier zukünftig ein Dienst von allen Systemen genutzt, könnte es nicht mehr zu unterschiedlichen Darstellungen aufgrund von verschiedenen Implementierungen basierend auf voneinander abweichenden Standards oder Baselines kommen.
Ein weiterer Treiber für Innovation im Umfeld der Digitalisierung wird „Künstliche Intelligenz" (KI) sein. KI-Technologie stellt zwar sicher keine Universal-Lösungen für sämtliche Herausforderungen dar, könnte jedoch in Spezialanwendungen ihre Stärken zur Wirkung bringen. So ermöglicht KI beispielsweise eine massive Unterstützung für den Nutzer im Bereich der bildbasierten Aufklärung durch Auswertung von Video-Streams in Echtzeit. KI bietet auch die Möglichkeit zur signifikanten Entlastung der Nutzer bei der Bedienung von komplexen Systemen, was die ESG in ihrem „KI-unterstützen Symbolgenerator" (KIS) realisiert hat. Durch den gezielten Einsatz von KI ermöglicht KIS, dass taktische Zeichen, die „wie früher" auf der analogen Karte als Skizze erstellt werden, in maschinenlesbare und dadurch interoperable Zeichen transformiert werden.
Aber auch weitere Arbeitsabläufe, zum Beispiel Bekämpfungsvorgänge durch die Artillerie oder eine (Feind-)Lagebeurteilung, könnten mittels spezifischer KI-Unterstützung massiv beschleunigt werden und so wertvolle Beiträge für den gesamten Führungsprozess und insbesondere für die Operationsführung bieten.
Seit mehr als 50 Jahren ist die ESG verlässlicher Technologie- und Innovations-Partner aller Teilstreitkräfte und militärischen Organisationsbereiche der Bundeswehr. Der Geschäftsbereich IT & Kommunikation der ESG übernimmt seit mehr als 30 Jahren erfolgreich Verantwortung für Pflege der Systeme in Nutzung, deren Weiterentwicklung und deren Anpassung an immer neue Einsatz-Anforderungen oder Einsatz-Umgebungen.

ESG DEFENCE + PUBLIC SECURITY

ESG Elektroniksystem- und Logistik-GmbH
ESG DEFENCE + PUBLIC SECURITY
Andreas Schiel
Leiter Geschäftseinheit Führungssysteme & Joint Fire Support
Geschäftsfeld IT & Landsysteme
Livry-Gargan-Str. 6
82256 Fürstenfeldbruck
Tel.: 089 – 92161 2012
andreas.schiel@esg.de
esg-defencesecurity.com

Funkkommunikation und Cyber-Lösungen von TELEFUNKEN RACOMS

TELEFUNKEN RACOMS bietet ein breites Portfolio an Funkkommunikations- und Netzwerklösungen rund um das Thema „Digitalisierung landbasierter Operationen". Zusätzlich zeichnen die Cyber-Lösungen für Behörden, Großunternehmen und Militär das Unternehmen als relevantes Systemhaus für digitale Sicherheitsherausforderungen und im Kampf gegen Cyber-Kriminalität aus.

Funkkommunikation

Durch den Einsatz modernster VHF/UHF- und HF-Kommunikation bietet TELEFUNKEN RACOMS eine umfangreiche Produktpalette für alle Teilstreitkräfte und Plattformen. Wir reagieren mit unseren Produkten und Wellenformen auf aktuelle Sicherheitsherausforderungen in den Bereichen asymmetrische Kriegsführung, neue digitale Bedrohungsszenarien und den damit einhergehenden erhöhten Informationsbedarf zwischen unterschiedlichen Plattformen und Teilstreitkräften.

E-LynX™ VHF/UHF SDR

Die Software Defined Radio (SDR)-Produktfamilie E-LynX™ ist eine moderne Funkgerätefamilie für taktische Einsätze. Mit richtungsweisenden Fähigkeiten, wie Mehrbandfähigkeit (30 MHz – 2,0 GHz), Mobile Ad-hoc Networking (MANET) und Breitbandwellenformen sowie NATO Kompatibilität erfüllt die E-LynX™ Familie jetzt schon die Anforderungen für D-LBO und ist auch für Luftfahrzeuge einsetzbar.

E-LynX™ wurde entwickelt, um schnell verfügbare und extrem robuste Netzwerke in unterschiedlichen militärischen Szenarien bereitzustellen. Das System bietet im Rahmen seiner MANET-Fähigkeit eine schnelle Verbindung von Aufklärung Führung und Wirkung. Des Weiteren verfügt E-LynX™ über integriertes Blue Force Tracking.
Das System besteht aus Handfunkgeräten, Manpacks und Fahrzeugstationen und Intercomstationen, die sich durch eine einfache und intuitive Bedienung mit einem durchgängigen User Interface auszeichnen. Mit Hilfe von kompakten und modular im Fahrzeug aufgebauten Nutzereinheiten, dem „Vehicle Intercommunication System" (VIC 500IP) kann die Kommunikationsanlage in einem Fahrzeug von allen Plätzen aus einbauunabhängig bedient werden.
Das Multi-Band und Multi-Waveform SDR E-LynX™-Familie bietet beste Kommunikationsleistung bei optimaler Frequenzökonomie. Die offene Kommunikationsarchitektur garantiert eine vollständige Abdeckung der taktischen NATO-Frequenzbänder. Im Rahmen der Concurrent Flooding Technology wird die effektive Reichweite, sowie Agilität und Widerstandsfähigkeit der Systemkomponenten der E-LynX™-Familie erhöht. Sprache, Daten und Video können simultan übertragen werden. Die Abmessungen, das Gewicht und der Energiebedarf sind niedrig gehalten. Die fortschrittliche Netzwerkarchitektur erlaubt es dem Nutzer, eine Vielzahl von E-LynX™ Geräten in einem mobilen ad-hoc-Netzwerk miteinander zu verbinden.
Die Komponenten der E-LynX™-Familie bilden automatische Netzwerke, die selbstheilend, unabhängig von GPS und ohne zentrale Masterstation agieren.

HRM 9000 – Nächste Generation HF-Funk

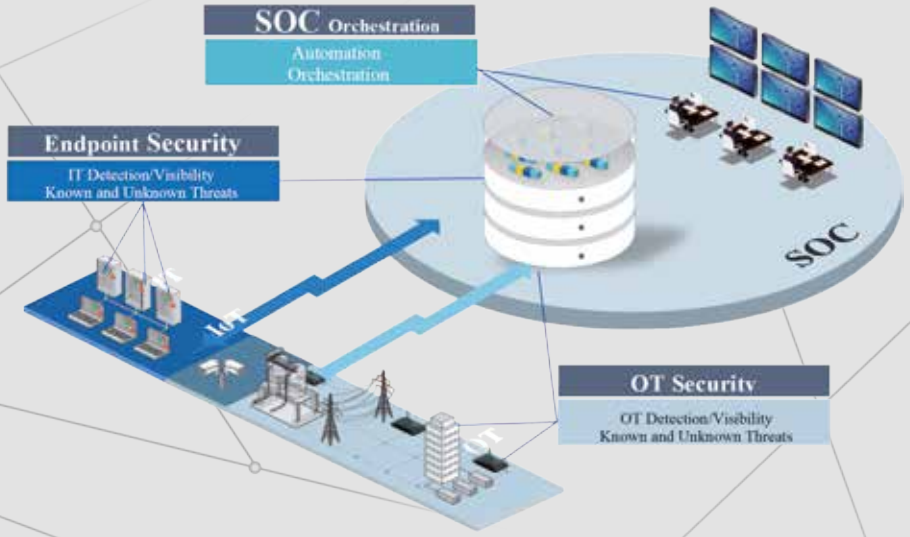
Das HRM 9000 wurde speziell auf die Anforderungen des digitalen Gefechtsfeldes hin entwickelt und kann Sprache, Daten und sogar Video übertragen. Die HF-Funkgerätefamilie HRM 9000 ist optimiert auf minimales Gewicht und Größe sowie minimalen Energieverbrauch bei maximaler Bewegungsfreiheit für den Nutzer

Militärische Einheiten im taktischen Einsatz, Spezialkräfte und Sicherheitsorganisationen brauchen Kommunikationsmittel, die störungsfrei große Reichweiten bis zu mehreren tausend Kilometern überbrücken können und gleichzeitig große Datenmengen übertragen. Für eine durchgängige Kommunikationsbeziehung und Informationsüberlegenheit von der taktischen zur strategischen Führungsebene werden weitreichende und hoch verfügbare Kommunikationsmittel benötigt. Die Produktfamilie HRM 9000 wurde für diese Einsatzszenarien entwickelt. Sie ist die neueste SDR-Generation der HF-Funkgeräte von TELEFUNKEN RACOMS und arbeitet im erweitertem Frequenzbereich von HF bis VHF. Ergänzt wird dies durch hochperformante Wellenformen und breitbandige Datenübertragung. Die Funkgeräte HRM 9000 sind voll kompatibel zur bereits querschnittlich eingeführten HRM 7000-Gerätefamilie.
Der Kern der Produktfamilie ist das Manpack HRU 9000. Es unterstützt sowohl nationale Übertragungsverfahren als auch standardisierte internationale Funkprotokolle und Wellenformen. Damit unterstützt sie bzgl. Interoperabilität alle erdenklichen Einsatzszenarien für D-LBO.

Die Optimierung von Handlungsfähigkeit, sowie Informationsüberlegenheit und verkürzte Reaktionswege spielen nicht nur auf dem Gefechtsfeld, sondern auch im Cyber-Raum eine wichtige Rolle.

Cyber Defence

Die heutigen Cyber-Angriffe sind ausgeklügelt, herkömmliche Sicherheitssysteme stellen für sie keine Herausforderung mehr dar, erfolgen in sehr hohem Umfang. Physische Geräte und kritische Infrastruktur sind mit dem Internet verbunden und müssen geschützt werden. Um Cyber Resilience zu erreichen, sind heute mehr als nur Investitionen und Personalumfang erforderlich. Unsere integrierte Cyber Resilience-Lösung bietet das Rahmenwerk, sowie die Technologien und Services für die Implementierung und das Management einer zukunftssicheren Cyber-Strategie.



Security Operations Center

Der zentrale Ort, an dem alle Cyber-Sicherheitsinformationen überwacht und verteidigt werden, ist das Security Operations Center (SOC). Das SOC ermöglicht eine vollständige Situationsanalyse aller Netzwerke und Endpunkte in der Behörde. Es priorisiert und zentralisiert den Reaktionsprozess, der durch Automatisierungs- und Orchestrierungstechnologie gesteuert wird. Für landesweite Projekte und große Organisationen richten wir lokale SOCs und zusätzliche Command SOCs ein, um das Security Operations Management zu optimieren.

Endpoint Detection & Response

Das Endgerät ist der sensibelste Teil des Unternehmens und der Ort, an dem die meisten Angriffe stattfinden, die Endgerätesicherheit ist daher eine wichtige Voraussetzung für eine angriffsresistente IT-Infrastruktur. TELEFUNKEN RACOMS benutzt einen kernelbasierten Ansatz, der kontinuierlich Endpunktdaten aufzeichnet und sie in einem Big-Data-Repository ablegt, in dem erweiterte Verhaltensanalysen stattfinden. Dieser Ansatz erkennt zielgerichtete Angriffe in Echtzeit und hat sich als zuverlässige Methode zur Erkennung von unbekannten Bedrohungen erwiesen.

SCADAShield

Unsere SCADAShield-Komponente ist eine praxiserprobte Technologie für Ihre ICS/SCADA-Sicherheit, welches die speziellen OT-Protokolle überwacht, die in industriellen Steuerungsnetzwerken verwendet werden und bietet eine automatisierte Überwachung, Anomalieerkennung, Forensik und Reaktion. Es werden sowohl OT- als auch IT-Protokolle überwacht und dabei auch die anspruchsvollsten Angriffe die das IT-Netzwerk durchdringen, erkannt. Da unser Konzern die angebotenen Systeme selbst entwickelt hat, können wir auch die Werkzeuge anbieten, um Sicherheitsprozesse nach Ihren Bedürfnissen anzupassen.

Cyber-Range

Qualifizierte Cyber-Sicherheitskräfte sind von entscheidender Bedeutung für Unternehmen und Regierungen im Kampf gegen Cyber-Angriffe, die einschließlich Cyber-Spionage, Cyber-Kriminalität und Cyber-Kriegführung eine ernsthafte Bedrohung für Behörden darstellen. Um diesem Bedarf gerecht zu werden, hat TELEFUNKEN RACOMS in der Cyber-Verteidigungsindustrie eine umfassende Cyber Range eingeführt. Die praxiserprobte Lösung bietet eine virtuelle Cyber-Verteidigungsumgebung zur Schulung von Netzsicherheitsexperten und Entscheidungsträgern in der Absicherung nationaler militärischer und ziviler Netzwerke gegen alle Formen von Cyber-Angriffen.
Die Cyber Range bietet:
- Simulierte Sicherheitsangriffe/Angriffsszenarien,
- Verbesserung der Fähigkeiten der Cyber-Mitarbeiter,
- Eine generische, isolierte und gesicherte Umgebung,
- Ein skalierbares und realistisches Trainingserlebnis,
- Verbesserung der praktischen Fähigkeiten.

Mithilfe unseres Systems werden automatisierte Szenarien ausgeführt, die in jeder Trainingseinheit wiederholt werden können, um Konsistenz und kontinuierliche Verbesserung zu bieten.

Cyber Intelligence

Für Behörden bieten wir ein neues und weltweit führendes Cyber-Intelligence-System an, welches die Ressourcen schont und die Ermittlungszeit erheblich verringert. Informationen hierzu erhalten Sie ausschließlich auf Anfrage.

CONNECTING. YOUR. MISSION. – dafür steht TELEFUNKEN RACOMS

TELEFUNKEN RACOMS

TELEFUNKEN Radio Communication Systems GmbH & Co. KG

Eberhard-Finckh-Strasse 55
89075 Ulm, Germany
Phone +49 731 15 53 - 0
Fax +49 731 15 53 - 112
info@tfk-racoms.com
www.tfk-racoms.com

JK DEFENCE & SECURITY PRODUCTS GMBH

Über den Horizont und weiter: Troposcatter hält die Verbindung

Felix Wickenhäuser

Blickt man auf die vielfältigen Einsatzprofile der Streitkräfte in den vergangen Jahren zurück, so erkennt man den durchwegs gestiegenen Bedarf nach hochdatenratigen Kommunikationsverbindungen, insbesondere auch über große Entfernung hinweg. Dies gilt umso mehr mit Blick auf die voranschreitende Digitalisierung des Gefechtsfelds, mit integrierten Sensor-to-Shooter Wirkungsketten.

Die Integration von Videostreams verlangt einerseits nach hohen Übertragungsraten, während die Anbindung von Sensoren und Effektoren niedrige Antwortzeiten (Latenzen) erfordert. Speziell im rückwärtigen Raum, wo Informationen aus unterschiedlichen Quellen kumulieren, ist deshalb der Bedarf nach hohen Übertragungskapazitäten groß. Es gilt, dass der schnelle und zuverlässige Austausch von Gefechtsinformationen die Grundlage zur Entscheidungsfindung und folglich zur Wirkungsüberlegenheit ist. Flaschenhälse, die zu verlorenen oder verzögerten Informationsübermittlungen führen, sind dabei zu vermeiden.

Für diese vielfältigen Anforderungen kommen unterschiedliche Führungsmittel in Frage.

Satelliten-Links gelten als optimale Lösung in vielen militärischen Szenarien, bei denen eine Punkt- zu- Punkt Verbindung gefordert wird. Die Erreichbarkeit von entlegenen Regionen sowie die relativ einfache Nutzung gelten als große Vorteile der Systeme. Die gewünschte Robustheit in einer sogenannten Satellite-Denied-Environment, kann indes nicht unter allen Umständen sichergestellt werden. Auch die verfügbaren Transponder-Frequenzen sind limitiert. Die Betriebskosten aufgrund der zu betreibenden Infrastruktur sind bei der total-cost-of-ownership-Betrachtung ebenfalls zu berücksichtigen. Schließlich machen hohe Latenzen von mehreren hundert Millisekunden die Nutzung von satellitengestützen Verbindungen bei zeitkritischen Anwendungen sogar gänzlich unmöglich.

Moderne HF-Kurzwellenradios wie das L3Harris AN/PRC-160 bieten mit fortschrittlichen Breitbandwellenformen Unabhängigkeit von Infrastruktur verbunden mit niedrigen Betriebskosten. Mit bis zu 120 Kilobit pro Sekunde liefern diese modernen Funkgeräte gänzlich neue Möglichkeiten im Kurzwellenband. Globale Kommunikationsfähigkeit bei schlechter Aufklärbarkeit (LPI/LPD) sowie der tragbare Formfaktor sind die Stärken dieser erprobten und verfügbaren Systeme. Der sichere Austausch von beispielsweise Aufklärungsergebnissen, auch mit Koalitionspartnern, in Bild und Ton wird ermöglicht.

Vor- und Nachteile der Verbindungen

Trotz der Vorteile der Kurzwelle bilden Mikrowellen-Richtfunkradios heute den Stand der Technik, wenn es darum geht, mit einigen hundert Megabit (Backbone)-Kommunikationswege herzustellen. Diese Funkverbindungen verlangen grundsätzlich jedoch eine sogenannte Line-of-Sight (LoS)-Verbindung, was je nach Masthöhe in einer Reichweite von rund 30 km resultiert. Die Erdkrümmung limitiert schließlich die Ausbreitung über größere Distanzen. Geographische Hindernisse oder Bebauung erfordern zudem die Nutzung von Repeaterstationen, mit bekannten Nachteilen wie höheren Latenzen und zusätzlichen exponierten Standorten zum Betrieb.

Unter Berücksichtigung der oben genannten Anforderungen und Limitierungen bekannter Systeme tritt nun ein seit Jahrzehnten bekanntes Verfahren wieder auf den Plan: das sogenannte Troposcatter-Prinzip. Als einer der bekannteren, historischen Anwendungsfälle gilt die Anbindung Berlins an das ehemalige Westdeutsche Telefonnetz. Mit großem technischem Aufwand wurden hier ab den 1960er Jahren etwa 200 km entfernte Sendestellen miteinander verbunden. Doch auch aktuelle Anwendungsfälle, wie die Anbindung der kanarischen Inseln an das Festland, zeugen von der Leistungsfähigkeit dieses Verfahrens in der Gegenwart. Durch Fortschritte in der Halbleiter- und damit Verstärkertechnik erlebt das Troposcatter, oder zu Deutsch der Troposphärenfunk, nun eine Renaissance in militärischen Anwendungen.

Autor

Felix Wickenhäuser ist Technologieberater Militärische Funkkommunikation bei JK Defence.

Der Troposcatter

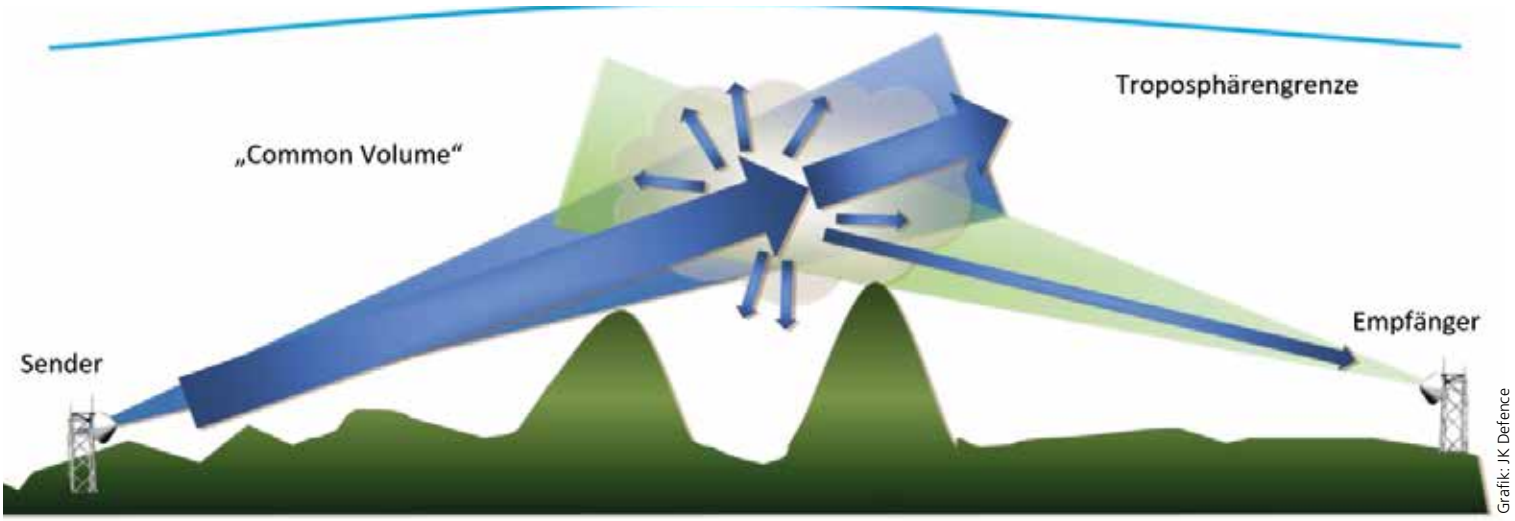
Doch was genau versteht man unter Troposcatter? Obwohl der Begriff fremd ist, kennen jedoch viele den Effekt, der sich dahinter verbirgt, ohne sich dessen bewusst zu sein. Eine Erläuterung bildet der Ausflug in die Optik: Auch bei dem für das menschliche Auge wahrnehmbaren Licht, handelt es sich um elektromagnetische Strahlung. Diese liegt im Frequenzbereich von etwa 400 THz bis 790 THz und ist für den Empfänger, das Auge, wahrnehmbar. Man stelle sich nun eine Großstadt bei Nacht vor, welche mit ihrem Lichtschein in einer dunstigen Nacht den Himmel erhellt. Genau jenen Effekt, der sich in der Troposphäre zerstreuenden (scattered) Strahlung, machen sich moderne Troposcatter-Systeme ebenfalls zunutze – wenn auch in einem anderen Frequenzbereich. Die von Comtech Systems entwickelten und gefertigten Systeme arbeiten im Mikrowellenbereich von 4,4 GHz bis 5,0 GHz und senden adaptiv mit bis 1.000 Watt in Richtung der Troposphäre. Im sogenannten „common volume", dem Schnittbereich der beiden Aussendungen, kommt es zur Zerstreuung der Strahlung. Ein großer Teil der Energie verliert sich im Weltall, während ein kleinerer Anteil vom Empfänger verarbeitet werden kann.

Aufgrund der Höhe des sogenannten „common volumes" in der Troposphäre bei etwa 13 km können geographische Hindernisse oder auch die Erdkrümmung selbst über große Strecken überwunden werden. Reichweiten von rund 200 km, bei Datenübertragungsraten mit bis zu 200 Megabit pro Sekunde sind möglich. Aufgrund des speziellen Ausbreitungswegs sind sowohl Aufklärung (detection/interception) als auch Störung (jamming) nahezu unmöglich.
Um die Wirksamkeit einer Troposcatter-Verbindung zu maximieren, werden moderne Tropo-Systeme in Konfigurationen mit zweifacher oder vierfacher Diversity konfiguriert. Diese Diversitätskonfigurationen können durch eine Kombination von Antennenabständen, mehreren Sendefrequenzen, Polarisation oder speziellen Winkeldiversity-Antennen erreicht werden. Die mit der Implementierung von Diversity-Konfigurationen verbundenen Leistungsgewinne sind deutlich effizienter als die einfache Skalierung der Leistung oder Antennengröße.

Einsatzerprobte Kommunikationsmittel

Comtech Troposcatter Systeme liefern den Streitkräften einsatzerprobte Kommunikationsmittel mit alternativlos niedrigen Latenzen. Je nach Missionsprofil bieten die unterschiedlichen Formfaktoren, von manntragbar, über 19"-TULBs, bis hin zu anhängerbasierten Systemen, die jeweils am besten passende Lösung. Die automatisierte Ausrichtung der Antennen und die daraus resultierende schnelle Verfügbarkeit des Links in etwa 15 Minuten, unterstützen den Anwender bei seiner Auftragserfüllung.
Unter abschließender Berücksichtigung der im Gefechtsfeld geforderten Eigenschaften von Kommunikationssystemen in Bezug auf Latenz, Reichweite, Datenrate und Robustheit, bietet heute kein anderes Drahtlos-System vergleichbare Leistungsmerkmale, wie moderner Troposcatter-Funk.

Exemplarische Darstellung des Ausbreitungspfads bei einer Tropscatter-Verbindung



Grafik: JK Defence

JK DEFENCE & SECURITY PRODUCTS GMBH

JK Defence & Security Products GmbH
Felix Wickenhäuser
Technologieberater
Militärische Funkkommunikation
Industriering Ost 74
47906 Kempen
Mobil: +49 170 814 2916
f.wickenhaeuser@jkdefence.de
www.jkdefence.de

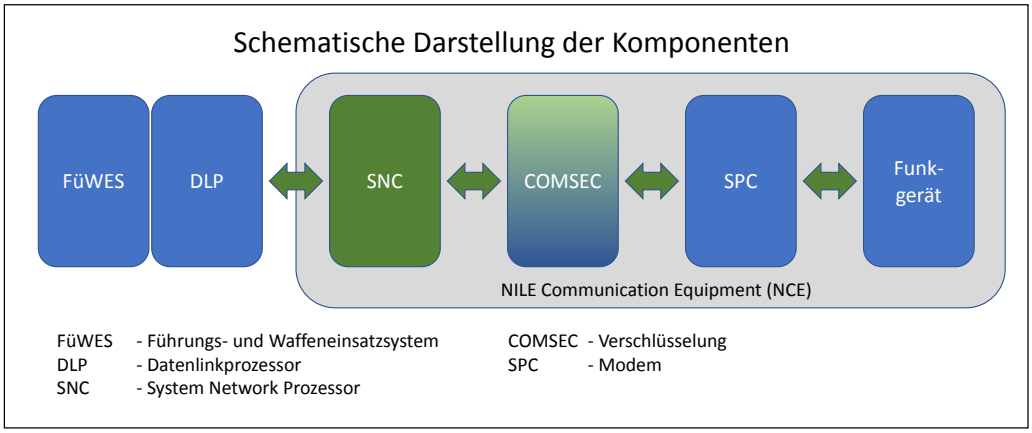
Datenlink LINK 22

Alexander von Kölln

Nach vielen Jahren der Projektarbeit sieht der Datenlink LINK 22 in der Bundeswehr seinem operativen Einsatz entgegen. Als Nachfolger des nunmehr seit über sechs Jahrzehnten betriebenen Link 11 wird die schrittweise Ablösung auch für den Nutzer erlebbar.

Mit der Indienststellung der Fregatte „Baden-Württemberg" am 17. Juni 2019 steht nicht nur das erste Schiff der Klasse 125 der Flotte zur Verfügung, sondern es beginnt gleichzeitig ein neuer Zeitabschnitt für Taktische Datenlinks (TDL) in der Deutschen Marine. Erstmals verfügt eine deutsche seegehende Einheit über die operationelle Fähigkeit zum Austausch taktischer Daten mittels LINK 22. So jedenfalls könnte man annehmen, wenn man sich die Auflistung der Fähigkeiten des Schiffes in den allgemeinen Publikationen ansieht. Anlass genug, um seitens der Projektleitung des Projektes Funktionskette LINK 22 im Bundesamt für Ausrüstung Informationstechnik und Nutzung der Bundeswehr (BAAINBw) ein wenig die Projekthistorie, den aktuellen Sachstand und die sich abzeichnende Zukunft von LINK 22 darzustellen.

Grafik: Alexander von Kölln



Nachfolger für Link 11

Der Taktische Datenlink LINK 22 hat eine lange Geschichte. Bereits früh erkennt die NATO, dass ein Nachfolgestandard für den bisherigen Datenlink Link 11 notwendig ist. Ein gemeinsames Mission Need Document der damals drei Obersten NATO-Befehlshaber im Jahr 1978 mündet 1983 in einer entsprechenden Taktischen Forderung des Marineamtes Abteilung Rüstung.
In einer Programmvereinbarung legen die Nationen Deutschland, Frankreich, Italien, Kanada, Niederlande, das Vereinigte Königreich und die Vereinigten Staaten von Amerika im Jahr 1987 den Grundstein für das Projekt namens „NATO Improved Link Eleven" (NILE). Dies stellt den Startschuss für die bis heute andauernde internationale Projektarbeit der sog. „NILE-Nationen" zu LINK 22 dar. Der Definitionsphase folgen – beginnend ab 1992 – die Design- und Entwicklungsphase sowie ab 2002 die In-Service Support Phase (Nutzung). Während die Niederlande mit Ende der Entwicklungsphase den Kreis der NILE Nationen verlassen haben, tritt Spanien 2004 dem Projekt bei.
Bereits seit 2011 betreibt Deutschland ortsfeste nationale LINK-22-Basissysteme zu Test- und Entwicklungszwecken an den Standorten Greding, Wilhelmshaven und Surendorf. Von hier aus fanden 2013 erste LINK-22-Funkversuche mit Finnland als Drittland statt.

Autor

Fregattenkapitän Alexander von Kölln, BAAINBw I6.2, Projektleiter Funktionskette LINK 22.

Halbjährliche Treffen

Basierend auf der gemeinsamen Programmvereinbarung befindet sich das multinationale Projektbüro in San Diego, Kalifornien. Das Gastgeberland USA stellt den Program Manager (PM), während die weiteren NILE-Nationen dauerhaft jeweils einen Mitarbeiter in das Program Management Office (NILE PMO) entsenden. Das oberste Gremium des Projektes NILE ist das Steering Committee (NILE SC). Halbjährlich treffen sich hierin die Repräsentanten der NILE-Nationen zur Festlegung der Projektziele und -finanzen. Für Deutschland ist dies der Projektleiter Funktionskette LINK 22 aus dem BAAINBw Referat I6.2 (Taktische Datenlinks).
Ebenfalls halbjährlich tagen die Technisch-Operationelle Arbeitsgruppe (T&OWG) sowie die Konfigurationskontrollgruppe (CCB). Die T&OWG berichtet dem NILE SC und dient allen LINK 22 nutzenden Nationen als Forum. Hier erfolgt der Austausch über gegenwärtige und zukünftige Aspekte der LINK-22- Kommunikation und Interoperabilität sowie Implementierungen und Weiterentwicklungsmöglichkeiten. Sie ist somit ein wichtiges Bindeglied zwischen den technischen und operationellen Sichten auf das Projekt. Ebenfalls dem NILE SC nachgeordnet ist das CCB. In diesem besitzen ausschließlich NILE-Nationen ein Stimmrecht, während die weiteren Nationen einen Beobachterstatus innehaben. Aufgabe des CCB ist die technische Gestaltung der NILE Pro-

dukte innerhalb der von NILE SC vorgegeben strategischen Entwicklungslinie. Dazu gehören das Priorisieren technischer Aufgabenpakete sowie das Durchführen des Konfigurationsmanagements.

Multinational statt NATO

Grundsätzlich ergeben sich aus der vereinbarten Vorgehensweise mehrere Abhängigkeiten und Zuständigkeiten, die bei der Beschäftigung mit LINK 22 zu Tage treten. Obwohl sich die Abkürzung NATO in der offiziellen Projektbezeichnung „NATO Improved Link Eleven" befindet, ist das Projekt kein NATO-Projekt, sondern ein multinationales Projekt. Die NILE-Nationen haben den Systementwurf der Funktionskette für einen Taktischen Datenlink erarbeitet und umgesetzt, der mit einer Schnittstelle zu außerhalb der Systemgrenze befindlichen Datenlinkprozessoren beginnt und mit der Schnittstellenspezifikation zu Funkgeräten endet.
Das Format, die Inhalte und die Abfolge der zu übertragenden taktischen Nachrichten werden dagegen durch die NATO in entsprechenden Standards und Publikationen festgeschrieben. Das für die LINK-22-Nachrichten maßgebliche NATO-Dokument ist die „Allied Tactical Datalink Publication – 5.22" (ATDLP-5.22). Natürlich ergeben sich hierbei wechselseitige Abhängigkeiten zwischen operativen und technischen Anforderungen. Die Projektarbeit profitiert jedoch davon, dass alle NILE-Nationen zugleich NATO-Staaten sind. Somit können die Positionen des Projektes unmittelbar in die jeweiligen NATO-Gremien eingebracht werden und operationelle Vorgaben in die Projektarbeit einfließen.

Das Link-System

Als Taktischer Datenlink hat auch LINK 22 die Aufgabe, taktische Daten aus Führungs- und Waffeneinsatzsystemen zu formatieren, als Beitrag zum gemeinsamen Lagebild oder als Weisung für die Übertragung per Funk (HF und UHF) aufzubereiten und an die beteiligten Einheiten, wie z. B. Schiffe und Luftfahrzeuge, zu übermitteln. Die Übertragung der Informationen findet in Form von einzelnen Nachrichten, sogenannten Messages, statt.
Ein LINK-22-System besteht grundsätzlich aus den folgenden Komponenten:

- Data Link Processor (DLP),
- Schnittstelle zum Führungs- und Waffeneinsatzsystem (FüWES), Netzwerkinitialisierung, Netzwerkmanagement, Message Management, Kodierung und Dekodierung der LINK-22-Messages,
- System Network Controller (SNC),
- Einrichten, Überwachen und dynamisches Anpassen des Funknetzwerkes
- Schlüsselgerät (Communication Security = COMSEC),
- Ver-/Entschlüsseln der LINK-22-Nachrichten,
- Modem (Signal Processing Controller = SPC),
- Mo-/Demodulation der Nachrichten (Hierbei stehen mehrere Wellenformen zur Verfügung, die sich hinsichtlich Robustheit und erzielbarer Bandbreite unterscheiden),
- Funkgerät und Antenne,
- Senden und Empfangen von Funksignalen,
- präzise Zeitversorgung,
- als Zeitschlitzverfahren benötigt LINK 22 hinreichend genaue Zeitinformation zum kollisionsfreien Senden der Daten.

Mit dem Begriff „NILE Communication Equipment" (NCE) werden SNC, COMSEC, SPC und Funkgerät zusammengefasst. DLP und NCE bilden eine „LINK-22-Funktionskette".
Eine Plattform (Schiff, U-Boot, Flugzeug oder Landstation), die über ein LINK-22-System verfügt, wird „NILE Unit" (NU) genannt.

Schnittstelle zum Führungs- und Waffeneinsatzsystem

Das Führungs- und Waffeneinsatzsystem (FüWES) der Plattform kommuniziert unmittelbar mit dem DLP. Neben dem hier gezeigten Schema existieren auch Varianten, die den DLP in das FüWES integrieren. Der DLP generiert aus den vom FüWES an ihn gelieferten Daten LINK 22-Messages und speist diese in das NCE ein. Umgekehrt nimmt der DLP Messages vom NCE entgegen, liest deren Dateninhalt aus und speist ihn in das FüWES ein. Aus diesen Daten generiert das FüWES u. a. einen Beitrag zur taktischen Lage.
Die Entwicklung des DLP und dessen Anbindung an NCE und FüWES obliegen der Verantwortung der integrierenden Plattformen. Die Definition der Schnittstelle zwischen DLP und SNC liegt dagegen in der Zuständigkeit des Projektes NILE ebenso wie die skizzierten Schnittstellen zwischen den weiteren Komponenten des NILE Communication Equipments. Zu den Produkten des internationalen Projekts gehören neben diesen Spezifikationen in der Hauptsache die eigentliche LINK-22-Netzwerksteuerungssoftware (SNC). Soweit möglich, strebt das NILE-Projekt Abwärtskompatibilität bei den alle zwei Jahre herausgegeben Updates dieser Software an.

Foto: Bundeswehr/Carsten Vennemann

Mit der Fregatte F222 „Baden-Württemberg" erhält die Deutsche Marine die operationelle Fähigkeit zum Austausch taktischer Daten mittels LINK 22

Entwicklung eines neuen Verschlüsselungsgerätes

Bedingt durch Dezertifizierung von Verschlüsselungsalgorithmen erfährt gegenwärtig die Landschaft der Verschlüsselungsgeräte einen Umbruch. Hiervon war auch die Funktionskette Link 22 betroffen. Unter Koordination des internationalen LINK-22-Projektbüros in San Diego (USA) wurde mit dem „Link Level Communication Security 7M Encryptor (LLC 7M)" ein neues Kryptogerät entwickelt. Dieses erhielt im Jahr 2016 erfolgreich seine NSA-Zertifizierung, so dass im selben Jahr ein erster Produktionsvertrag mit der Herstellerfirma geschlossen wer-

den konnte. Die Geräte befinden sich derzeit im Zulauf und stehen den nutzenden Projekten der Bundeswehr dann zur Verfügung.
Folge dieser auf externer Vorgabe beruhenden Neuentwicklung des Schlüsselgerätes ist eine Anpassung der LINK-22-Netzwerksteuerungssoftware (SNC). Erstmals erscheint anschließend mit der SNC 10.0 Version eine nicht mehr rückwärtskompatible Fassung.

Anpassung an die geänderte Schnittstelle

Diese Entscheidung erfordert somit, dass alle national entwickelten LINK 22 DLP an die geänderte Schnittstelle zum SNC anzupassen sind. Folglich auch der DLP der Fregatten der Klasse 125. Legt man nun die Entwicklungslinie der NILE-Produkte neben die Zeitlinie des Fregattenprojektes, so ist erkennbar, dass zum Zeitpunkt der Herausgabe der nicht mehr abwärtskompatiblen LINK-22-Produkte die Abnahmen der Fregatten begonnen haben. In dieser Phase verbietet sich ein Anpassen des TDL-Systems an neue Anforderungen. Gleichwohl wurde die Zwischenzeit bis zur Abnahme und Indienststellung für Analysen und Vorbereitungen der LINK-22-Nutzung genutzt. Das Umsetzen der notwendigen Anpassung kann jedoch nur danach erfolgen.

Notwendigkeit der taktischen Datenlinks

Taktische Datenlinks dienen dem Informationsaustausch und erfordern daher die Beteiligung kompatibler Kommunikationspartner, auch auf internationaler Ebene. Nachdem zunächst vorrangig die NILE-Nationen die Integration von LINK 22 in ihre Rüstungsprojekte vorantreiben, steigt inzwischen das internationale Interesse an NILE-Produkten. Drittstaaten erwerben nach Durchlaufen eines Genehmigungsverfahrens die NILE-Produkte gegen eine einmalige anteilige Erstattung von Entwicklungskosten. Durch jährliche Zahlung einer Gebühr an die NILE-Nationen erhalten sie einen Partnerstatus und partizipieren somit an den Unterstützungsleistungen aus dem bestehenden In-Service Support-Vertrag. Diesen schließt das NILE PMO ab. Er bildet das Instrument zum Anpassen und Pflegen der NILE-Produkte. Alle zwei Jahre erscheint ein sogenannter Block Cycle mit aktueller Software.
LINK 22 findet, nach zunächst abwartender Haltung, inzwischen weltweit Akzeptanz als Nachfolgestandard von LINK 11. Zu Beginn des Jahres 2019 haben bereits 17 Nationen LINK 22 eingeführt oder bereiten dies in aktuellen Projekten vor. Außerhalb der NATO finden sich darunter Nationen wie Australien, Japan und Südkorea in der östlichen Hemisphäre oder Chile und Mexiko in der westlichen. Die erste Nation mit operativ einsatzfähigem LINK 22 an Bord seegehender Einheiten ist Finnland.
Die weitere Verbreitung ist – vor dem Hintergrund des angekündigten Nutzungsendes des Vorgängerverfahrens – in ersten Linie eine Zeit- und Kostenfrage.

Modernisierung des LINK 22

Als Folge umfangreicher Tests sowie Erkenntnissen aus Forschungs- und Technologievorhaben erlebt auch LINK 22 schon seine erste Modernisierung. Unter deutscher Federführung seitens des Referates I6.2 des BAAINBw im Projektteam Funktionskette LINK 22 wurden neue Wellenformen für den Hoch-Frequenz-Bereich (HF) entwickelt. So wurde die bisherige Reichweite des Datenlinks von rund 300 nautischen Meilen (300 nm = 556 km) auf über 1000 nm (1.852 km) gesteigert unter gleichzeitiger Verdopplung der maximalen Bandbreite. Die Leistungsfähigkeit dieser Wellenformen wurde in Funkversuchen im Jahr 2014 von Ulm nach Kreta (Griechenland) bzw. vor Besuchern des International Data Link Symposium (IDLS) 2016 zwischen Maastricht (Niederlande), Valdepeñas (Spanien) und der Wehrtechnischen Dienststelle 81 in Greding demonstriert. Dass die Grenzen der Leistungsfähigkeit offenbar noch nicht ausgereizt sind, zeigt ein im Jahr 2017 während des Manövers EASTLANT betriebenes LINK-22-Netzwerk unter Einbindung des Wehrforschungsschiffes PLANET im Seegebiet nördlich von Tromsö (Norwegen) nach Greding und Wilhelmshaven. Es wurden Reichweiten von über 1300 nm (2400 km) erzielt.
Mit LINK 22 steht den Streitkräften nunmehr ein sicherer, robuster und weitreichender Datenlink zur Verfügung. Dieser Standard kann als Single-Link betrieben werden, entfaltet seine Vorzüge jedoch in Kombination mit weiteren Datenlinks insbesondere mit LINK 16 in einer Multilinkumgebung. Wegbereiter hierbei ist, neben der sich gegenseitig ergänzenden Kombinationen aus Reichweite in Konkurrenz zu erzielbaren Datenraten, das zwischen beiden Standards weitgehend kompatible Nachrichtenformat.
Um zukünftigen Nutzern ein bestmögliches System zum Austausch taktischer Daten über LINK 22 zur Verfügung zu stellen, untersuchen die Projektnationen weiterhin intensiv Themen wie Anwendungsszenarien, Bandbreitenerhöhung und Netzwerkmanagement. Auch hier engagiert sich Deutschland federführend. Unter Einbindung des Nutzers, den Wehrtechnischen Dienststellen 61 und 81, der Universität der Bundeswehr München, dem Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie sowie der Industrie, führt BAAINBw I6.2 umfangreiche Studien durch. Deren Ergebnisse werden dann wieder in die Anpassung der projektspezifischen Software und Hardware sowie den Anforderungskatalog zukünftiger Projekte einfließen. ■

Zusammentreffen während der Erprobungsfahrt der Fregatte F 222 Baden-Württemberg (mi) mit den Fregatten F 215 Brandenburg (li) und F 216 Schleswig-Holstein im Skagerrak

Foto: Bundeswehr/Carsten Vennemann

Sicherheitspolitik · Streitkräfte · Rüstung · Wehrtechnik · Logistik · IT · Öffentliche Sicherheit

Europäische Sicherheit & Technik

Die führende Monatszeitschrift für Sicherheitspolitik und Wehrtechnik

Wählen Sie zu Ihrem Jahresabonnement eine unserer attraktiven Werbeprämien aus!
(Nur für Neu-Abonnenten)

▶ „Beanie Lite“
von Woolpower
Farbe: Schwarz

▶ Der Reibert
Das Handbuch für den deutschen Soldaten
902 Seiten, Taschenformat

▶ Wehrtechnischer Report
Soldat und Technik 2020

Die Auslieferung der Prämie erfolgt, sobald die erste Abonnementrechnung beglichen ist.

Bestellung mit Bestellschein (**Post oder Fax**), oder per **E-Mail** an info@mittler-report.de

Jahresabo € 78,00 (zzgl. € 11, 50 Versand / Inland)
(für Bundeswehr, Reservisten, GSP- und IDLw-Mitglieder, Schüler, Studenten € 58,00 zzgl. € 11, 50 Versand / Inland)

Probekurzabo € 16,40 (inkl. Versand)
(3 Ausgaben; das Probeabo endet automatisch nach Erhalt des letzten Heftes)

Ja, ich bestelle ES&T

☐ im **Probekurzabo** ohne Prämie zu € 16,40 (inkl. Versand)
(3 Ausgaben ohne automatische Verlängerung; Dieses Angebot kann nur einmal pro Kalenderjahr in Anspruch genommen werden.)

☐ im **Jahresabo** mit Prämie zu € 78,00 (zzgl. € 11,50 Versand)

☐ im Jahresabo für Bundeswehr, Reservisten, GSP- und IDLw-Mitglieder, Schüler, Studenten (bitte Nachweise) für € 58,00 (zzgl. € 11,50 Versand)

Bitte wählen Sie Ihre Prämie aus:

☐ „Beanie Lite“ von Woolpower, Farbe: Schwarz

☐ Der Reibert

☐ Wehrtechnischer Report „Soldat und Technik 2020“

Absender

Bei **nicht dienstlichen** Bestellungen bitte die Privatadresse angeben und ggf. die abweichende Lieferanschrift zusätzlich eintragen.

Name, ggf. Dienstgrad

ggf. Firma / Institution / Dienststelle

Straße/Hausnummer

PLZ/Ort

E-Mail

Datum, Unterschrift

Widerrufsbelehrung
Widerrufsrecht: Sie haben das Recht, binnen vierzehn Tagen ohne Angabe von Gründen diesen Vertrag zu widerrufen. Die Widerrufsfrist beträgt vierzehn Tage ab dem Tag an dem Sie oder ein von Ihnen benannter Dritter, der nicht der Beförderer ist, die erste Ware in Besitz genommen haben bzw. hat. Um Ihr Widerrufsrecht auszuüben, müssen Sie uns (Mittler Report Verlag GmbH, Baunscheidtstraße 11, D-53113 Bonn, Tel.: 0228/ 3500870, Fax: 0228/ 3500871, E-Mail: info@mittler-report.de) mittels einer eindeutigen Erklärung (z. B. ein mit der Post versandter Brief, Telefax oder E-Mail) über Ihren Entschluss, diesen Vertrag zu widerrufen, informieren. Zur Wahrung der Widerrufsfrist reicht es aus, dass Sie die Mitteilung über die Ausübung des Widerrufsrechts vor Ablauf der Widerrufsfrist absenden.
Folgen des Widerrufs: Wenn Sie diesen Vertrag widerrufen, haben wir Ihnen alle Zahlungen, die wir von Ihnen erhalten haben, einschließlich der Lieferkosten (mit Ausnahme der zusätzlichen Kosten, die sich daraus ergeben, dass Sie eine andere Art der Lieferung als die von uns angebotene, günstigste Standardlieferung gewählt haben), unverzüglich und spätestens binnen vierzehn Tagen ab dem Tag zurückzuzahlen, an dem die Mitteilung über Ihren Widerruf dieses Vertrags bei uns eingegangen ist. Für diese Rückzahlung verwenden wir dasselbe Zahlungsmittel, das Sie bei der ursprünglichen Transaktion eingesetzt haben, es sei denn, mit Ihnen wurde ausdrücklich etwas anderes vereinbart; in keinem Fall werden Ihnen wegen dieser Rückzahlung Entgelte berechnet. Wir können die Rückzahlung verweigern, bis wir die Waren wieder zurückerhalten haben oder bis Sie den Nachweis erbracht haben, dass Sie die Waren zurückgesandt haben, je nachdem, welches der frühere Zeitpunkt ist.
Sie haben die Waren unverzüglich und in jedem Fall spätestens binnen vierzehn Tagen ab dem Tag, an dem Sie uns über den Widerruf dieses Vertrags unterrichten, an uns zurückzusenden oder zu übergeben. Die Frist ist gewahrt, wenn Sie die Waren vor Ablauf der Frist von vierzehn Tagen absenden. Wir tragen die Kosten der Rücksendung der Waren. Sie müssen für einen etwaigen Wertverlust der Waren nur aufkommen, wenn dieser Wertverlust auf einen zur Prüfung der Beschaffenheit, Eigenschaften und Funktionsweise der Waren nicht notwendigen Umgang mit ihnen zurückzuführen ist.

Hiermit bestätige ich, dass ich mein Widerrufsrecht zur Kenntnis genommen habe.

Datum, **2. Unterschrift**

MITTLER REPORT VERLAG GMBH
Baunscheidtstraße 11 · 53113 Bonn
Fax 0228 - 3500871

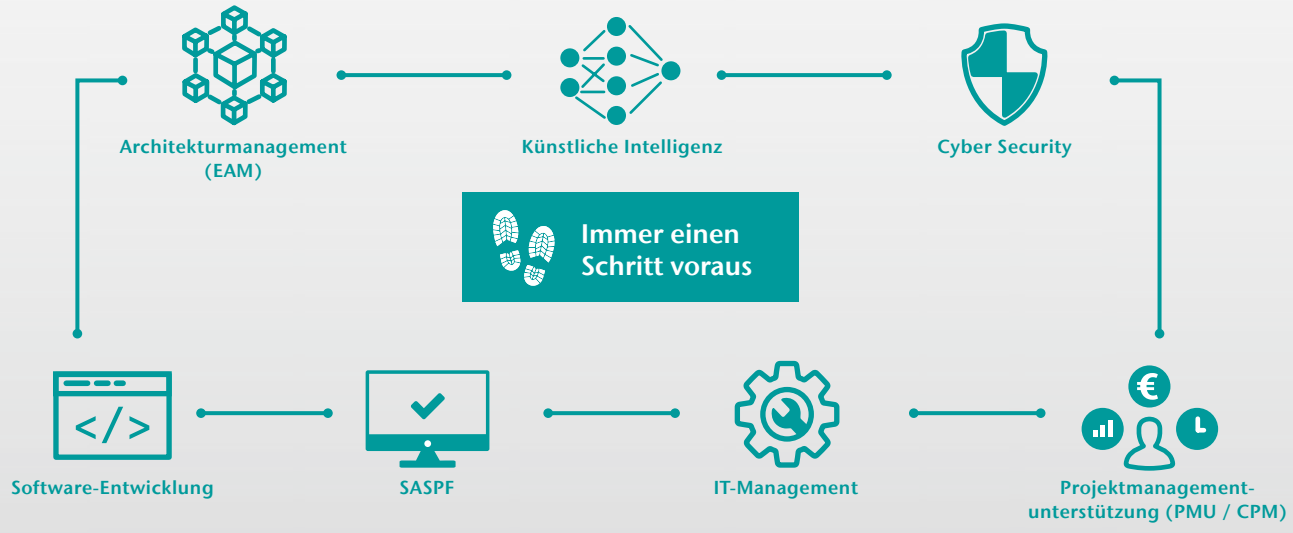
CONET

Immer einen Schritt **voraus**

Neue Herausforderungen – neue Chancen

Digitalisierung und Transformation sind für die Bundeswehr der Zukunft Chance und Herausforderung zugleich: Geräte, Systeme und Kommunikationsmittel sind zunehmend vernetzt. Dies erhöht Führungsfähigkeit und Einsatzfähigkeit, Effektivität und Effizienz. Doch gleichzeitig steigern sich die Komplexität der eingesetzten IT-Systeme, die Anforderungen an Konzeption und Integration leistungsstarker Fach-, Führungs- und Kommunikationssysteme und die Risiken durch Cyber-Angriffe.

CONET - Ihr zuverlässiger Begleiter auf dem Weg zur digitalisierten Streitkraft!



SAP • Infrastructure • Communications • Software • Consulting

www.conet.de • info@conet.de