SONDERBEILAGE
zum InfoBrief HEER 04/2025

Herbst-Symposium

bei Rohde & Schwarz

11./12. November 2025

„Digitale Landstreitkräfte – Führungsfähigkeit, Kommunikation und elektronischer Kampf im 21. Jahrhundert“

Foto: FKH

Die Digitalisierung unserer Landstreitkräfte befindet sich in einem noch sehr frühen Stadium. Sie ist in vielerlei Hinsicht mit sehr komplexen Herausforderungen verbunden. Dies nicht nur mit Blick auf die Systemintegration, die Funktionalität oder die Nutzerfreundlichkeit, sondern beispielsweise auch mit Blick auf die Robustheit und die Interoperabilität.

In der Realisierung kann die Digitalisierung unserer Landstreitkräfte mit der technologischen Entwicklung sowohl im Bereich der Hard- als auch in der Software, wenn überhaupt, nur ansatzweise Schritt halten. Immer schneller werdende Innovationszyklen sind eine Herausforderung für die etablierten Planungs- und Beschaffungsprozesse.

Die Digitalisierung ist gleichwohl zwingend und alternativlos für moderne, durchsetzungsfähige Landstreitkräfte, die – gemeinsam mit anderen Dimensionen – in einem umfassenden Fähigkeitsverbund von Führung, Aufklärung, Wirkung und Unterstützung einem Gegner möglichst überlegen sein sollen. Mittels Digitalisierung wird nicht zuletzt der einzelne Soldat/Kämpfer mit seinen Sensoren und Effektoren Teil eines ganzheitlichen Gefechtsführungssystems, das alle Elemente, Sensoren und Effektoren dimensionsübergreifend verbindet und die für die Operationsführung erforderlichen Informationen in Echtzeit überträgt und ebenengerecht bereitstellt.

Das Beherrschen großer Datenmengen, die Analyse und Aufbereitung von Daten und die KI-Unterstützung von Entscheidungsprozessen werden zunehmend zum Schlüssel des Erfolges auf dem Gefechtsfeld. Dies in Szenarien, die geprägt sein werden durch unbemannte, autonome Systeme mit hoher Abstandsfähigkeit, die Einbindung künstlicher Intelligenz und Bedingungen des elektronischen Kampfes.

Mit den Beiträgen des Herbstsymposiums wurde deutlich, über welch‘ ungemeine Innovationskraft und Leistungsfähigkeit unsere Sicherheits- und Verteidigungsindustrie (SVI) verfügt – und was möglich und realisierbar erscheint, um das Fähigkeitsspektrum unserer Streitkräfte zu vervollständigen, zu optimieren bzw. zu modernisieren und weiterzuentwickeln.

Ja, „Masse“ kann im Gefecht den Unterschied machen. Und genau darum werden nach meiner Überzeugung durchsetzungsfähige Streifkräfte auf moderne, möglichst überlegene Technologien nicht verzichten können und auch nicht verzichten wollen. Qualität gleich technologische Überlegenheit muss Quantität überwinden können!

Mit Blick auf unsere Streitkräfte gibt es hier erheblichen Handlungsbedarf, nicht nur im Bereich der Digitalisierung. Angesichts der Bedrohung durch Russland kommt es jetzt darauf an, unsere Streitkräfte möglichst rasch mit all dem auszurüsten, was sie für eine glaubhafte Abschreckung sowie eine erfolgreiche Landes- und Bündnisverteidigung sowie den Heimatschutz benötigen. Die dafür notwendigen Rahmenbedingungen sind noch nicht in jeder Hinsicht optimal, aber doch besser als je zuvor.

Ich danke dem Team der Rhode & Schwarz GmbH & Co. KG für die exzellente Zusammenarbeit in Vorbereitung und Durchführung unseres Herbstsymposiums sowie den Vortragenden und Experten für ihre inhaltsreichen Präsentationen.

Ohne Digitalisierung wird man weder Führungs- und Informations- noch Wirkungsüberlegenheit erzielen können. Das wird, zumindest in einer Auswahl, in den folgenden Fachbeiträgen deutlich werden. In der Nachschau haben sich die Vortragenden bereit erklärt, ihre Gedanken und Folgerungen mit Ihnen in dieser Sonderbeilage zum InfoBrief Heer zu teilen. Ich wünsche daher allen Leserinnen und Lesern eine interessante Lektüre.

Wolfgang Köpke
Generalmajor a.D. und Präsident
Förderkreis Deutsches Heer e.V.

INHALT

Foto: Bundeswehr/PlgABw

Digitalisierung des Heeres: Die Voraussetzung für MDO und zukünftige Relevanz

Generalmajor Stefan Lüth

Das Deutsche Heer ist das Fundament der Bundeswehr – die letzte Instanz, wenn alles andere versagt. Diese Rolle muss erhalten bleiben. Die Zukunft der militärischen Wirkung heißt Multi-Domain Operations (MDO). Und in MDO zählt nicht, wer die meisten Panzer hat, sondern wer am schnellsten entscheidet, am besten vernetzt ist und als System wirken kann.

In einem zunehmend komplexen, hybriden und vernetzten Konfliktumfeld – wie wir es im Krieg Russlands gegen die Ukraine sehen – ist die Fähigkeit, Wirkung über alle Dimensionen hinweg zu erzeugen, entscheidend. Luft, See, Weltraum, Cyber und Land müssen synchron agieren. Wer nicht digital vernetzt ist, wird in MDO nur eine nachrangige Rolle spielen – oder gar zum Risiko für das Gesamtsystem werden.

Ein Panzer, der nicht weiß, wo die eigenen Kräfte sind, ist kein Wirkmittel – er ist ein Angriffsziel. Ein Infanteriezug ohne Anbindung an Aufklärung ist keine Kampfeinheit, sondern eine leichte Beute. Eine Brigade ohne digitale Lageeinbindung entfaltet kaum Kampfkraft. Ohne Digitalisierung ist der Soldat allein. Mit Digitalisierung wirkt er als Teil eines Netzwerks – und Netzwerke gewinnen Kriege.

Digitalisierung bedeutet mehr als neue Funkgeräte. Es geht um durchgängige, standardisierte Daten – von der Schützenpanzerkompanie bis zur strategischen Führung. Um vernetzte Systeme, die multinational zusammenwirken. Um KI-gestützte Entscheidungsunterstützung, resiliente Kommunikation unter Störung und den Elektronischen Kampf als Echtzeitelement. Und alles muss sicher sein – nicht nur vor Raketen, sondern vor Hackern, Störsignalen und Datenmanipulation.

Grafik: Bundeswehe/Planungsamt Bw

Digitalisierung ist DIE Voraussetzung für MDO

„Software Defined Defence“ ist dabei der entscheidende Enabler. Er ermöglicht es, mit vorhandenen Mitteln MDO-fähig zu werden und Fähigkeiten schnell an neue Bedrohungen anzupassen. Die operative Überlegenheit entsteht durch datenbasierte, KI-gestützte Entscheidungen und die Synchronisation von Effekten über alle Domänen. Doch es braucht nicht nur Technik, sondern auch das richtige Mindset – Verständnis, Agilität und die Bereitschaft zum Wandel.

Das Planungsamt der Bundeswehr versteht sich als zentraler Bedarfsträger für die Zukunftsfähigkeit der Streitkräfte. Wir bauen keine Systeme, führen keine Truppen – aber wir sorgen dafür, dass Planung, Technik, Rüstung und Einsatz nicht nebeneinander her laufen, sondern als ein System gedacht werden. Gemeinsam mit allen Organisationsbereichen treiben wir Projekte wie „Drohnen“, „Operative Architektur“ und „MDO“ voran.

Internationale Rahmen wie Federated Mission Networking und nationale Initiativen wie D-LBO oder das „Digitale Gefechtsfeld“ zeigen den Weg. Doch die Zeit drängt. Wer nicht jetzt handelt, verliert die Fähigkeit, mitzureden, mitzuwirken und mitzuentscheiden. Die Digitalisierung des Heeres ist kein „nice-to-have“ – sie ist alternativlos.

Für die Sicherung unserer Freiheit braucht Deutschland ein starkes, handlungsfähiges und digital vernetztes Heer – schnell, konsequent und ohne Kompromisse. ■

Autor:

Generalmajor Stefan Lüth ist Amtschef des Planungsamtes der Bundeswehr in Berlin. Zuvor war er Inspekteur der Streitkräftebasis in Bonn.


Foto: MRV

Die Zeitenwende ist schon in vielen Bereichen angekommen!

Interview mit Alexander Philipp, Geschäftsführer der Rohde & Schwarz Vertriebs GmbH, im Rahmen des Herbstsymposiums des Förderkreis Deutsches Heer e.V.

Herr Philipp, welche Produkte und Projekte in Ihrem Portfolio sind aus Ihrer Sicht für die Landstreitkräfte derzeit von besonderer Relevanz?
Aktuell besonders im Fokus steht im Kontext der Digitalisierung der landbasierten Operationen D-LBO unser Führungsfunksystem mit unserer Funkgerätefamilie SOVERON in verschiedenen Bauformen. Aber natürlich sind für die Landstreitkräfte grundsätzlich auch weitere Systeme aus unserem Portfolio sehr interessant, beispielsweise für Aufklärung und Wirkung im Elektronischen Kampf.

Jetzt speziell auf das Projekt D-LBO bezogen: Was sind die nächsten Schritte, die Sie hier planen?
Die Planung und Gesamtführung liegen in der Hand unseres Kunden und Nutzers Bundeswehr. Wir tragen zu D-LBO mit der Lieferung des Führungsfunksystems wesentlich bei und liefern bereits seit mehr als drei Jahren nicht nur Hunderte, sondern Tausende Funkgeräte. Also Formfaktoren wie etwa Fahrzeugfunkgeräte und Handhelds sowie die Software, die nun in verschiedenen Stufen geprüft und nutzererprobt wird. Zuletzt war vor einer Woche bei der Wehrtechnische Dienststelle für Informationstechnologie u. Elektronik WTD 81 in Greding ein weiterer Nutzerakzeptanztest erfolgreich. Im Weiteren findet jetzt – darüberliegend im gesamten D-LBO-Projekt – aktuell in Munster ein sogenannter Systemnachweis statt.

Welche operativen Schritte planen Sie in Zukunft angesichts des Willens der Bundesrepublik zur Ertüchtigung der Bundeswehr und hier besonders der Landstreitkräfte und der Erwartung und Bereitstellung der hierzu erforderlichen Mittel? Welche operativen Schritte gibt es da aus Ihrer Sicht?
Auf unserer Seite, wie wir schon eindrucksvoll im Programm D-LBO unter Beweis stellen konnten, haben wir die Fähigkeit, sehr schnell, sehr stark zu skalieren. Das konnten wir für die bestellten Funkgeräte auch beweisen. Wir sind zudem auf Wunsch in der Lage, die Fertigungskapazitäten für noch größere Stückzahlen an Funkgeräten bereitzustellen. Dies wird mit Blick auf die sich im Zulauf befindliche Anzahl an neuen Plattformen sicher auch notwendig sein. Aber auch im Bereich des Elektronischen Kampfes können wir nicht nur auf Produktebene im Bereich der Fertigung skalieren, sondern auch diese Hardware und Software in entsprechende Plattformen einrüsten und zu maßgeblichen Fähigkeitspaketen integrieren.

Sind bei den bestellten Stückzahlen eigentlich schon die Umlaufreserven in einer bestimmten Stückzahlmenge enthalten?
Die uns derzeit bekannten und beauftragten Stückzahlen lassen darauf schließen, dass weder eine Vollausstattung noch eine Umlaufreserve für die aktuell kommenden Plattformen enthalten ist.

Konnten in Bezug auf die Überlegungen, die Sie auf der operativen Ebene angestellt haben, jetzt schon weitere Beauftragungen erzielt werden? Also neue Stückzahlen, weitere Geräteliefe-rungen oder auch neue Geräteprodukte, die Sie anbieten?
Im vergangenen Dezember gab es einen weiteren Abruf an Führungsfunkgeräten aus dem geschlossenen Rahmenvertrag. Da wurde sowohl die Stückzahl als auch die sogenannte Lieferkadenz, also der quartalsmäßige Ausstoß, noch mal deutlich erhöht.

Welche Möglichkeiten sehen Sie zur Verbesserung der Interoperabilität der Standardisierung für einheitliche Informationssysteme NATO und EU?
Ein großes Land wie Deutschland braucht als Anlehnungspartner zunächst einmal eigene durchgängige souveräne Führungsfähigkeit. Denn in der „Schlammzone“ kommt es darauf an, dass ich mit meinen direkten Kameraden kommunizieren kann. Die tiefe, vielfältige internationale Durchmischung der früheren Auslandseinsätze ist für die robuste Landes- und Bündnisverteidigung nicht effizient. Daher basiert die Interoperabilität auf Standards, Protokollen und vertrauenswürdigen Übergängen zueinander, nicht auf technischen Monokulturen.
Wir bieten hier bereits über die Luftschnittstelle, ausgehend von unseren Funkgeräten, mit der europäischen Wellenformfamilie ESSOR eine besondere Fähigkeit zum Zusammenwirken, die aktuell in ihre nächste Phase eintritt. In anderen Bereichen, etwa der Marine, bieten wir eine durchgängig nach NATO-Standards ausgelegte und für eine Vielfalt von Kommunikationsmitteln offene Lösung mit unserem NAVICS. Führungsfähigkeit mit vertrauenswürdigen

Übergängen ist ein wesentliches Kompetenzfeld von Rohde & Schwarz.

Thema: Bundeswehr als Auftraggeber. Welche Maßnahmen sehen Sie bei der Bundeswehr als Auftraggeber für Sie auch zukünftig als relevant, um gegebenenfalls noch schneller liefern zu können, schneller auf entsprechende Aufträge reagieren zu können? Gibt es da aus Ihrer Sicht vermeidbare Hemmnisse, auch aus dem Feld bürokratischer Prozesse und Vorgaben?
Da würde ich einmal sagen, dass es doch stark an den handelnden Personen und den Begleitumständen hängt. Den Auftrag D-LBO-Führungsfunk haben wir quasi in Lichtgeschwindigkeit in die Realisierung führen können, weil wir da nach entsprechend klaren Vergabeentscheidungen sehr konstruktiv mit dem Beschaffungsamt zusammenarbeiten konnten. Auch in anderen Bereichen können wir sehr gut mit dem Amt zusammenarbeiten. Oder auch schon im Vorgriff, wenn man sich den ganzen Planungsprozess anschaut. Deswegen bin ich weit davon entfernt, in die oft pauschale Kritik an Ministerium, BAAINBw oder Rüstungsprozess einzustimmen. Im Gegenteil, da tut sich schon einiges und es sind auch weitere Maßnahmen spürbar. Und ich denke, die Zeitenwende ist schon in vielen Bereichen angekommen.
Auf der anderen Seite ist es immer noch so, dass das BAAINBw sich anspruchsvolle Regelungen gesetzt hat, also über die zwingenden gesetzlichen Regelungen hinaus eine enorme Breite an Detailregelungen aufrechterhält, die nicht mehr zeitgemäß sind, beziehungsweise hiermit kollidieren. Davon zu unterscheiden sind EU-Gemeinschaftsrecht und national zwingende Gesetze. Hier gibt es auch von Dritten die Motivation, an den massiv gestiegenen Verteidigungsbudgets Deutschlands zu partizipieren. Die im Zuge der Nachprüfung des Führungsfunkauftrags erfolgte gerichtliche Klärung hat aber bestätigt, dass der öffentliche Auftraggeber durchaus begründet aus nationalen Sicherheitsinteressen gemäß Artikel 346 AEUV (Anm. Red.: Vertrag über die Arbeitsweise der Europäischen Union) deutlich beschleunigt direkt beschaffen kann und darf. Und das macht er zunehmend.

Bei komplexen Lieferketten sind die Abhängigkeiten von Lieferanten zurzeit in aller Munde. Haben Sie da Maßnahmen ergriffen, um diese Abhängigkeit zu reduzieren, oder welche Maßnahmen würden Sie sich von politischer Seite wünschen?
Rohde & Schwarz hat von jeher eine enorme eigene Wertschöpfungstiefe. Angefangen von der Galvanik über die Leiterplattenbestückung bis hin zur Endfertigung haben wir alles bei uns in der Hand und in eigenen Fabrikationsstandorten. Auf der anderen Seite sind wir natürlich auch abhängig von der Zulieferung von gewissen Bauteilen, etwa vielen Halbleitern. Aber wir stellen gerade bei sicherheitsrelevanten Aufträgen sicher, dass wir eine solide Reichweite haben. Das heißt, im Unterschied zur Automobilindustrie schlagen kurzfristige Engpässe oder Weltmarktstörungen nicht sofort durch und wir können unsere Kunden beliefern. Zudem haben wir aufgrund der Nähe der Entwicklung zur Fertigung die Möglichkeit, kurzfristig und schnell entsprechende Anpassungen in den Geräten und Systemen vorzunehmen, um dauerhaft nicht verfügbare Elemente zu ersetzen.

Sie haben in letzter Zeit wesentliche Kooperationen mit Unterauftragnehmern oder mit anderen Firmen abgeschlossen. Zielt das in die gleiche Richtung?
Da geht es eher um eine Ergänzung des Portfolios, vor allem, wenn man gemeinsam besser zum Ziel kommen kann. Da geht es nicht um die Absicherung von Lieferketten, sondern tatsächlich etwa konkret am Beispiel des Maschinenbauspezialisten Trumpf darum, dass wir unsere Drohnenabwehrsysteme um einen nichtkinetischen Effektor erweitern. Typischerweise fokussiert sich Rohde und Schwarz auf alles, was im elektromagnetischen Spektrum unterwegs ist, macht dann nachgelagert eine Sensordatenfusion und unser Kunde nutzt dann eben diese Daten. Das sind die Stärken von Rohde & Schwarz. Und hier wollten wir einfach unser System um einen speziellen hochmodernen Effektor erweitern, den unser Partner Trumpf technologisch bereits beherrscht.

Vielleicht noch etwas zu ESSOR, die ESSOR-Wellenformen für die Interoperabilität der Streitkräfte. Sehen Sie da vielleicht auch noch weitere Felder, wo Sie mit Ihrer spezifischen Kompetenz im Bereich des elektromagnetischen Spektrums dann Kooperationen eingehen. Haben Sie da noch mehr im Auge?
Ja, selbstverständlich. Und zwar, wie gerade schon dargestellt, liegen unsere Schwerpunkte im Bereich des elektromagnetischen Spektrums und der Sensordatenfusion, wann immer es notwendig ist, dass wir andere Sensoriken mit einfließen lassen. So beispielsweise, jetzt gerade ebenfalls veröffentlicht, haben wir die Firma Munich Innovations Labs übernommen, um uns im Bereich Open Source Intelligence zu erweitern. Das ist keine Kooperation, sondern eine Akquise. Aber so versuchen wir natürlich, weitere Sensoriken dazuzugewinnen. Und auch mit den Daten möglichst viel in der weiteren Verarbeitung anzufangen und den Nutzern entsprechend bessere Erkenntnisse zu ermöglichen.

Haben Sie drei besondere Wünsche an den öffentlichen Auftragspartner, das BAAINBw oder an die Truppe?
Weiterhin eine zuverlässige, vertrauensvolle und vor allem zielorientierte Zusammenarbeit. Da gibt es keine drei Wünsche, sondern schlicht die gute Zusammenarbeit, die wir jetzt die letzten Jahre auch erleben durften, diese so fortzusetzen und das alles zielgerichtet zur Verteidigungsfähigkeit Deutschlands zusammenzubringen.

Herr Philipp, danke für die interessanten Informationen und Ihre Zeit.

Das Interview führten Michael Horst und Wolfgang Gelpke. ■

MOTOROLA SOLUTIONS

Verteidigungsbereitschaft: Die zentrale Rolle einheitlicher Kommunikation in Zeiten hybrider Bedrohungen

Gregor Ksoll

Angesichts der zunehmend verschwimmenden Grenzen zwischen militärischen Operationen und innenpolitischen Krisen stehen die europäischen Staaten vor einer beispiellosen Herausforderung: Sie müssen allumfassende Sicherheit gegen zunehmend hybride Bedrohungen gewährleisten. Von Cyberangriffen auf kritische Infrastrukturen bis hin zu Störungen des elektromagnetischen Spektrums und Desinformationskampagnen – moderne Bedrohungen erfordern einen neuen Ansatz, der traditionelle militärische Fähigkeiten mit ziviler Resilienz und staatlicher Koordination verbindet.

Im Mittelpunkt dieser notwendigen Transformation steht ein wichtiger Wegbereiter: einheitliche, sichere und widerstandsfähige Kommunikationssysteme. Diese Systeme bilden das Rückgrat der nationalen Sicherheit und gewährleisten die Kontinuität bei der Befehlsgebung sowie eine nahtlose Zusammenarbeit bei militärischen, zivilen und staatlichen Einsätzen. Um diese Integration zu erreichen, müssen erhebliche strukturelle und technische Hindernisse überwunden werden, die mit den Altsystemen verbunden sind.

Die hybride Bedrohungsstruktur: Warum Kommunikation so entscheidend ist

Hybride Bedrohungen sind grenzübergreifend und multidimensional. Sie nutzen Schwachstellen in physischen, digitalen und psychologischen Bereichen aus. So kann beispielsweise ein Cyberangriff auf die Energieinfrastruktur schnell zu einem Zusammenbruch der öffentlichen Dienste, zu Unruhen in der Bevölkerung und zu militärischen Schwachstellen führen. Darüber hinaus ist das elektromagnetische Spektrum ein umkämpftes Gebiet, in dem Gegner die Kommunikation stören können, um Verwirrung zu stiften und Reaktionsmöglichkeiten zu beeinträchtigen.

Die NATO betont, dass Resilienz die „erste Verteidigungslinie" ist und eine Integration von militärischen und nichtmilitärischen Instanzen erfordert, um hybrider Kriegsführung entgegenzuwirken. Staatliche Akteure stützen sich heute stark auf den Einsatz von Mitteln außerhalb der kinetischen Kriegsführung, was zu einer gewissen Unklarheit führt, die eine frühzeitige Erkennung und Zuordnung unglaublich schwierig macht. Das primäre Ziel ist oft nicht die vollständige Eroberung, sondern die systemische Lähmung.

Diese Realität erfordert eine kontinuierliche, proaktive Bedrohungsanalyse und eine Echtzeit-Zusammenführung von Informationen aus militärischen, staatlichen und kommerziellen Datenströmen. Der dafür benötigte Prozess beruht gänzlich auf sicheren und einheitlichen Kommunikationskanälen.

Die europäische Verteidigungspolitik orientiert sich am Konzept der allumfassenden Sicherheit – einem „ganzheitlichen Regierungs- bzw. Gesellschaftsansatz", der drei wichtige Säulen umfasst:

- **Militärische Verteidigung:** Abschreckung und Bereitschaft zur Verteidigung der territorialen Souveränität
- **Resilienz der Regierung:** Krisenmanagement, Koordinierung der Nachrichtendienste und Strafverfolgung
- **Zivilschutz:** Schutz kritischer Infrastrukturen, Energiesicherheit und öffentliche Sicherheit

Der Erfolg dieses Konzepts hängt von der Fähigkeit ab, nahtlos über alle Bereiche hinweg miteinander kommunizieren zu können. Kommunikationssysteme sind das Nervensystem der Verteidigungsbereitschaft. Sie fördern das Situationsbewusstsein, die Entscheidungsfindung in Echtzeit sowie koordinierte Maßnahmen auf allen Ebenen.

Fragmentierung: Eine technische und strategische Schwachstelle

Trotz der kritischen Rolle, die die Kommunikation spielt, sind die derzeitigen Systeme in Europa nach wie vor fragmentiert, was Schwachstellen mit sich bringt, die von Gegnern ausgenutzt werden können.

Technische Fragmentierung

Militärische Kommunikationssysteme, Regierungsnetzwerke und kommerzielle Breitbandnetze arbeiten oft isoliert voneinander und sind nur begrenzt kompatibel. Unterschiedliche Verschlüsselungsstandards, Frequenzbeschränkungen und proprietäre Technologien können eine nahtlose, sofortige Kommunikation zwischen militärischen Einheiten und zivilen Ersthelfern erschweren.

Operative Fragmentierung

Wenn Streitkräfte zivile Behörden unterstützen, gehen oft Zeit und Ressourcen für die Einrichtung sicherer Kommuni-

Foto: Motorola

Das TETRA- und LTE-Endgerät MXP7000 bietet einsatzkritische TETRA- und 4G-LTE-Breitband-Sprach- und Datenkommunikation.

kationsverbindungen verloren, was die Koordination von Maßnahmen verzögert und gefährliche Lücken in der Lageerkennung verursacht.

Diese Fragmentierung birgt erhebliche finanzielle und strategische Risiken. Das Europäische Parlament schätzt, dass Ineffizienzen bei den Verteidigungsausgaben und mangelnde Zusammenarbeit die EU jährlich zwischen 18 und 57 Milliarden Euro kosten. Strategisch gesehen steht dieses operative Risiko dem Konzept der Multi-Domain-Operationen (MDO) der NATO im Weg, das eine Synchronisierung der Aktivitäten in allen Bereichen – Land, Luft, See, Weltraum und Cyberspace – mit nichtmilitärischen Maßnahmen fordert. Die NATO hat bestätigt, dass asymmetrische digitale Fähigkeiten unter den Bündnisstaaten „die digitale Interoperabilität erschweren oder sogar gefährden" können, und betont, dass technische Unterschiede ein existenzielles Risiko darstellen. Eine wahre Verteidigungsbereitschaft erfordert, dass alle Elemente – vom Soldaten an der Front bis zum kommunalen Versorgungsunternehmen – nach einem gemeinsamen, sicheren Prinzip agieren.

Die erforderliche Architektur für eine Vereinheitlichung

Die Überwindung der Fragmentierung erfordert einen grundlegenden Wandel in der Planung, Bereitstellung und Verwaltung von Kommunikationssystemen. Eine umfassende Verteidigungsbereitschaft erfordert eine integrierte Architektur, die militärische, zivile und staatliche Bereiche miteinander verbindet und gleichzeitig die Resilienz in den umkämpften Gebieten gewährleistet:

- **Nahtlose Integration und Interoperabilität:** Die Architektur muss eine sichere, softwaredefinierte Kommunikationsschicht umfassen – eine digitale Brücke, die eine sofortige, verschlüsselte Gruppenkommunikation über alle unterschiedlichen Netze hinweg ermöglicht. Das digitale Rückgrat der NATO soll die technischen Mittel für eine „universelle Konnektivität und Datenübertragung" über alle Bereiche und Partner hinweg bereitstellen.

- **Dual-Use-Systeme:** Die Architektur erfordert eine modulare, gehärtete Infrastruktur, die zuverlässiges Schmalband (LMR) mit dem einsatzkritischen Breitband der nächsten Generation kombiniert. Diese Infrastruktur muss für den militärischen Betrieb garantiert, jedoch auch für die unmittelbare Interoperabilität mit Zivilbehörden ausgelegt sein.

- **Datengesteuertes C2:** Bei der Kommunikation geht es heute in erster Linie um Daten, was im MDO-Rahmenwerk der NATO als strategischer Vorteil angesehen wird. Die Architektur muss eine einheitliche Befehlssoftware integrieren, um Echtzeitdaten aus dem Einsatzgebiet – Videos, Kartendaten und Sensorfeeds – in verwertbare Informationen umzuwandeln. Dieser datenzentrierte Ansatz ist entscheidend, um MDO zeitnah umzusetzen und das Situationsbewusstsein zu verbessern.

Standardisierung und Überlebensfähigkeit

Zwei strategische Anforderungen bestimmen die Zukunft der gesamten Verteidigungskommunikation: Standardisierung und Überlebensfähigkeit.

Standardisierung und Datenhoheit

Echte Verteidigungsbereitschaft erfordert ein Engagement für offene Standards (NATO/EU/zivil), um Fragmentierung zu überwinden, Größenvorteile zu erzielen und langfristige Interoperabilität zu gewährleisten. Dies steht im Einklang mit der Europäischen Strategie für die Verteidigungsindustrie (EDIS), die gemeinsame Anschaffungen fördert und bis 2030 einen Anteil von 40 % an gemeinschaftlich organisierten Investitionen anstrebt.

Darüber hinaus müssen wir in einsatzkritisches Breitband über privates 5G/LTE investieren. Denn Breitband ist die treibende Kraft für Datenhoheit und bietet dem Militär die Kapazität und digitale Autonomie, unabhängig von den Einschränkungen kommerzieller Netzwerke zu operieren. Die NATO erachtet das Potenzial von 5G als transformativ für die militärische Effektivität.

Überlebensfähigkeit

Angesichts der zunehmenden Komplexität hybrider Bedrohungen muss die Kommunikation auch in umkämpften Umfeldern funktionsfähig bleiben. Gegner setzen ausgefeilte Techniken ein, um die Kommunikation zu stören, abzufangen oder zu unterbinden.

Die Fähigkeit, Daten aus den Bereichen Führung, Information, Kommunikation, Computersysteme, Nachrichtenwesen, Überwachung und Aufklärung (C4ISR) zu verwalten, ist die neue Voraussetzung für den militärischen Erfolg. Die Erlangung und Aufrechterhaltung der Dominanz im elektromagnetischen Spektrum (EMS-Dominanz) wird nun NATO-weit als entscheidend für den operativen Erfolg angesehen

Um in diesem stark umkämpften Umfeld bestehen zu können, muss die zukünftige Architektur Folgendes umfassen:

- **Spektrumaufklärungssysteme:** Diese Systeme bieten eine kontinuierliche EMS-Echtzeitüberwachung, um feindliche Störungen (Jamming) und Beeinträchtigungen zu erkennen und abzuwehren.

- **Selbstformierende Ad-hoc-Netzwerke (MANETs):** Dynamische, selbstheilende Mesh-Netzwerke, die Daten automatisch umleiten, was die Befehlskette aufrecht erhält und die MDO-Anforderung erfüllt.

Die Herausforderungen für die Gewährleistung nationaler Sicherheit sind strategischer Natur und nicht nur technologischer. Sie erfordern von den Mitgliedstaaten, die Kommunikation in den Mittelpunkt der Verteidigungsbereitschaft zu stellen. Um diese Vision zu verwirklichen, sind sektorübergreifende Zusammenarbeit und nachhaltige Investitionen in Systeme erforderlich, bei denen Interoperabilität, Flexibilität und Überlebensfähigkeit im Vordergrund stehen.

Der Weg nach vorne ist klar: Systeme standardisieren, Dual-Use-Infrastrukturen nutzen und in robuste Technologien investieren. Diese Neuorientierung wirkt der Fragmentierung entgegen, verbessert die Fähigkeit, effektiv auf die komplexen, dynamischen Bedrohungen der modernen Welt zu reagieren, und gewährleistet den operativen Erfolg.

Es ist jetzt an der Zeit zu handeln, bevor die Schwachstellen der Fragmentierung zu den Schwachstellen der Krisen von morgen werden.

Kontakt:
Motorola Solutions Germany GmbH
www.motorolasolutions.com

Autor:

Gregor Ksoll ist Key Account Manager Bundeswehr bei Motorola Solutions

The ESSOR Programme

Lino Laganà

The **ESSOR PROGRAMME** (European Secure Software Defined Radio) is a European defence initiative aimed at developing common technology for military software-defined radio (SDR) to enhance the interoperability and security of voice and data communications among the armed forces of participating nations during coalition operations.

The programme is currently participated by six nations: Finland, France, Germany (joined in 2020), Italy, Poland, Spain and Sweden (left in 2017). Among the objectives of ESSOR are:

- Improve interoperability between radio platforms from different manufacturers and nations;
- Develop common standards in architecture and waveforms;
- Enhance security of communication;
- Foster the European defence technological by developing software defined radio technology.

The following key goals were also agreed by Nations:

- harmonise requirements;
- reduce national budget;
- exploit national assets;
- aggregate industrial expertise in Europe.

a4ESSOR S.A.S. (Alliance for ESSOR) is a multinational joint venture, participated by Bittium (Finland), Indra (Spain), Leonardo (Italy), Radmor (Poland), Rohde & Schwarz (Germany) and Thales (France), whose role is to lead and coordinate the activities of its shareholders in the performance of the ESSOR programme.

Its primary objective is to develop and promote secure, interoperable software-defined radio technology and waveforms to improve the ability of European armed forces to communicate and operate together in coalition operations. Our motto is "interoperability through portability", as we aim at exploiting national platforms of each participating nation.

As an international company, we can leverage technical competences, technical expertise and managerial experience from multinational experts spread across Europe. Fostering open discussion among team members, on both requirements and solutions, we achieve state-of-the-art products.

Starting from the different existing radios at each nation we have defined the ESSOR Architecture as a standardized, reference architectural framework for military Software Defined Radio (SDR) platforms. The ESSOR Architecture was designed to ensure waveform portability independently of the underlying radio platform. This allowed a4ESSOR to develop a single waveform that could be ported on every radio platform complying with the architecture.

Graphic: Essor

Once the waveform is ported on all the radio platforms of each nation, we will run specific laboratory tests in a common IOP Laboratory (IOP Lab) to ensure that interoperability is achieved in a number of scenarios commonly agreed with the nations, so that we can ensure that common military requirements are agreed.

Through the ESSOR programme we have successfully developed and validated the **ESSOR High Data Rate Waveform (EHDRWF)**, which was adopted by NATO as a standard (STANAG 5651). The EHDRWF supports secure transmission of high-volume data traffic, including voice (VoIP), video, and data. It provides high-performance COMSEC (Communication Security) and TRANSEC (Transmission Security), enabling information security and personnel safety, and enhanced connectivity in the field through high-performance and secure mobile IP networks (Mobile Ad Hoc Network, MANET). It is easily scalable, enabling the establishment of tailored networks that self-organize and self-repair. It is capable to operate either with or without satellite positioning systems (GNSS).

We are currently developing the **ESSOR Narrow-Band Waveform (ENBWF)** who will be based on the imminent NATO standard (STANAG 5630), whose definition we have contributed to with papers and discussion. The ENBWF is designed for secure ground-to-ground tactical communications, specifically voice and data. It provides high-performance COMSEC and TRANSEC, enabling information security and personnel safety. As a key objective, it provides a jamming-robust tactical waveform, ensuring reliable communication even in critical electromagnetic environments.

We also developed the **ESSOR 3-Dimensional Waveform (E3DWF)**, for air-ground-air interoperability, whose porting and IOP validation are still subject to discussions at NATO. It can be installed on airborne platforms and ground forces, and it uses high-performance COMSEC and TRANSEC, enabling information security and personal safety.

To allow nations to use their own **mission planning system** to plan and enable coalitions operation, we are going to define and implement common exchange formats and procedures, to allow distribution and import/export of mission planning data. After validation in the **IOP Lab**, we will allow interoperability at command-and-control (planning) system level, permitting nations to use their national assets.

In summary, we will have several national radio platforms, a common architecture, common waveforms, common mission exchange formats and procedures, national mission planning and distribution systems and, finally, a common laboratory to validate global interoperability.

- Across time a4ESSOR we have achieved a significant number of goals:
- Definition of the ESSOR architecture, that was published and made available to all nations and industries;
- Development, porting and interoperability validation of the EHDRWF in the IOP Lab, and successful filed test by the Finnish Army;
- Extension of EHDRWF features and successful validation in the IOP Lab;
- the European Commission included the ESSOR programme in the Permanent Structured Cooperation (PESCO) as a key project for common European defence;
- The European Commission decided to co-fund the ESSOR New-Capability programme as part of the European Defence Industrial Development Programme (EDIDP);
- The ESSOR 3-Dimensional Waveform was successfully implemented;
- NATO adoption of EHDRWF as STANAG 5651 for interoperability in land forces tactical communications;
- Successful contribution to NATO STANAG 5630 on ground-to-ground interoperability between the land troops and platforms;
- Regular participation to NATO CWIXs (Coalition Warrior Interoperability Exercises) to experiment and test interoperability between Allied nations.

Final consideration on a common European Defence:

The European Commission has been planning several joint defence programmes, starting from EDIDP, EDF, and SAFE, which imply at least the harmonisation of requirements. In addition, the many aggregations of European industries are leading to delivering the same system to several nations, meaning both the harmonisation of military requirements and the availability of a common system. The process is, however, slow compared to the urgent demand for joint and increased European protection.

The capability to harmonise requirements, achieve system-level interoperability, and exploit national assets is key to an interim approach to common European Defence, as it would leverage systems already deployed at national level. This is what we achieved with the ESSOR program.

Still, we need courage to formally start the process to a common European Defence.

We should consider that all steps and decisions taken to build the European Union raised lots of concerns about a loss of sovereignty. Be it the abolishment of tariffs in the 1950s, the creation of a single market in the 1990s, allowing the free circulation of people, the introduction of a common currency, the Euro, the introduction of the European Constitution, the Treaty of Lisbon. All such steps made the European Union grow to its current form, as we know it today. All the benefits coming from such decisions are now taken for granted, even though they were not easy decisions.

We need courage to take political and security decisions aiming at common European Defence. But I am sure we will never regret the decision. And one day, our children will be considering a common European Defence simply as a matter of fact. European Defence Forces will be more powerful than the aggregation of several national forces and will allow us to better defend our common democracies and values of freedom. ■

Contact:
a4ESSOR SAS
8, Avenue des Louvresses
92230 Gennevilliers – France
e-mail: info@a4ESSOR.com

Author:

Lino Laganà, President and General Manager of a4ESSOR S.A.S.

KNDS

Digitalisierung von Landstreitkräften – Praxisbeispiele bei Entwicklung, Ausbildung und Einsatz

Mathias Noehl, Max Marquardt

KNDS Deutschland nutzt seit vielen Jahren Methoden und Mittel der Digitalisierung in unterschiedlichen Anwendungsbereichen für Landstreitkräfte.

Der Digitale Zwilling

Bereits bei der Systemauslegung – also in der Frühphase eines Rüstungsprojektes - wird durch sogenannte digitale taktische Zwillinge die Möglichkeit geschaffen, unmittelbare Rückmeldungen des Nutzers mit minimalem Aufwand zu erhalten. Der „tactical twin" von KNDS kann dabei insbesondere die Bedienung im Fahrzeug sehr realitätsnah und flexibel abbilden. Durch die Kombination mit der hauseigenen Simulationssoftware kann der Nutzer in realitätsnahe taktische Situationen gebracht werden und somit entsteht ein schnelles und belastbares „Feedback".
Die Anpassungen sind im digitalen Zwilling sehr einfach umsetzbar. Für ein Vorhaben der Bundeswehr konnten auf diese Weise die Erkenntnisse innerhalb von 24 Stunden umgesetzt werden und eine erneute Testung durch den Nutzer erfolgen.

Fotos/Grafiken: KNDS (5)

Taktischer Zwilling

Eine besondere Bedeutung hat hier die virtuelle KNDS-eigene Simulation. Damit können virtuelle Simulationen flexibel und entwicklungsbegleitend angepasst werden, sodass neue Systeme und Bedienkonzepte bereits zu Beginn der Entwicklung in einer realistischen Simulationsumgebung in konkreten Vignetten durch den Nutzer selbst verifiziert und verändert werden können.

Der Einstieg in die praktische Erprobung ist bereits die frühe Phase der CAD-Entwicklung. Dafür werden die originalen CAD-Daten in der Simulation in die vollständige Bedienumgebung in einem Mix aus realen und virtuellen Bediengeräten umgesetzt. Der KNDS Tactical Twin ermöglicht die Integration von Modellen, direkt aus den Entwicklungsabteilungen wie zum Beispiel Antriebsmodelle und

Entwicklung des Human Machine Interface

Steuerungsalgorithmen. Dadurch können neue Fahrzeugfunktionen und HMI (Human-Machine-Interface) bereits sehr früh in der Entwicklung in komplexen, taktischen Szenarien evaluiert und neue taktische Konzepte bereits tiefergehend erforscht werden, ohne auf die physische Verfügbarkeit der ersten Prototypen warten zu müssen. Eine vernetzte Simulation für komplexe Szenarien bietet dabei die KNDS-eigene SW-Suite. Sie kann flexibel an neue Szenarien und Assets angepasst werden.

Manned – Unmanned – Teaming

Simulatoren in der Ausbildung

Die simulatorgestützte Ausbildung spielt national und international aufgrund der rasant steigenden Komplexität der Missionslösungen eine immer größer werdende Rolle.

Ein besonders Augenmerk liegt dabei auf einem immer höheren Realitätsgrad und der Vernetzung von verschiedenen Teil- und Funktionseinheiten in einem Simulationsumfeld. KNDS verwendet hierfür eine eigene Software mit sehr hohem Realitätsgrad und der Möglichkeit der Vernetzung verschiedener Teileinheiten und auch der Einbindung von Fahrzeugen anderer Hersteller.

Verschiedene NATO-Staaten nutzen Simulationszentren in denen beispielsweise Panzertruppe, Panzergrenadiertruppe und Artillerietruppe im Verbund ausgebildet werden kann. Mit dem Kampfpanzer Leopard 2A8 erhält Deutschland erstmals einen Gefechtssimulator, der die Ausbildung von Besatzungen auch oberhalb der Ebene Panzerzug ermöglicht. Eine weiterer Anwendungsfall der Digitalisierung in der Ausbildung ist das Live Fire Monitoring Equipment (LFME).

Train as you fight – ein Credo der taktischen Ausbildung, dass in der internen Produktentwicklung bei der KNDS Software Simulation Suite stets bedacht wurde. Die Kernaspekte der KNDS-Simulationstechnik decken somit alle Aspekte einer modernen simulationsgestützten Ausbildung vom Einzelplatztraining bis hin zu Kompanie- oder Bataillonsübungen ab. KI-unterstützte computergenerierte Kräfte (Computer Generated Forces, CGF) ermöglichen dem Ausbilder teilautomatisierte Unterstützungsfunktionen, was den Personaleinsatz insbesondere bei komplexeren vernetzten Simulationen deutlich reduziert.

Modularität und Interoperabilität

Die modulare und interoperable Ausführung der zukünftigen Landsysteme wird auch die Neugestaltung der beteiligten System-/Fahrzeugformationen mit sich bringen. Neben bemannten werden auch unbemannte und teleoperierte Systeme das Portfolio der europäischen Armeen erweitern. Erst alle drei Fähigkeiten könnten den zukünftig erforderlichen plattformübergreifenden Missionslösungsansatz mit hoher Interoperabilität vollständig abdecken.

Eine Digitalisierung beim Einsatz von Landstreitkräften ist eng verbunden mit dem zunehmenden Einsatz von unbemannten Systemen in der Luft und am Boden. Für Landstreitkräfte ist die Kombination von bemannten und unbemannten Systemen (sog. manned/unmanned teaming) besonders relevant.

KNDS ist hier an mehreren Projekten der europäischen Union und im Rahmen der Experimentalserie des Amtes für Heeresentwicklung mit verschiedenen Lösungsansätzen aktiv. Kernbestandteil sind hierbei verschiedene Systemlösungen von Führungseinrichtungen zur Einbindung von unbemannten Systemen in allen Domänen (Aufklärung, Führung, Wirkung, Unterstützung). Eine Vielzahl hochgeschützter bemannter, aber auch unbemannter Fahrzeuge, unterstützt durch unterschiedlich große UGVs und UAVs bestimmen bereits das Gefechtsfeld der Gegenwart. Die Vielfalt der Anbieter und Systeme wird den Informationsfluss nicht einfacher machen. Gemeinsame Standards, um Informationen zu teilen und voneinander zu lernen, sind zu erwarten. Auf den heutigen Gefechtsfeldern sind sich schnell verändernde Bedrohungslagen und eine rasant zunehmende Informationsvielfalt eine Herausforderung für den militärischen Entscheider. Um in solchen Situationen weiterhin die angestrebte Führungs- und Wirkungsüberlegenheit zu erhalten, müssen die richtigen Informationen zum richtigen Zeitpunkt dem militärischen Führer zur Verfügung stehen. Die Digitalisierung ist ein wesentlicher, wenn nicht sogar der entscheidende Schlüssel dabei. Doch Digitalisierung muss auch immer ganzheitlich gedacht und systemverträglich sein. Vor allem aber muss sie in bestehende Missionslösungen integriert werden können. Nur so hat sie echten Mehrwert. Sie beginnt genau da, wo der Operateur sich gerade befindet. Die neuen Technologien müssen sich nahtlos in die operationelle Umgebung der Bediener einfügen und ihn bei seinen Aufgaben unterstützen.

Auch wenn die Herausforderungen hierbei groß sind, bleibt festzuhalten, dass Technologie nur dann eine Bedrohung ist, wenn man sie ignoriert. ■

Kontakt:
KNDS Deutschland GmbH & Co. KG
Krauss-Maffei-Str. 11
80997 München / Deutschland
https://www.knds.com/

Autoren:

Mathias Noehl ist Bereichsleiter Systemtechnik, **Max Marquardt** ist in der Unternehmenskommunikation bei KNDS tätig.

SAFRAN

Führungsfähigkeit im digitalen Gefechtsfeld

Der abgesessene Soldat als Schlüssel zum vernetzten Lagebild

Marzell Schiller

Die Digitalisierung des Gefechtsfelds verändert grundlegend, wie Führungsfähigkeit, Aufklärung und Wirkung ineinandergreifen. Im Zentrum steht nicht mehr nur das Gefechtsfahrzeug oder der Gefechtsstand, sondern der einzelne Soldat – als Sensor und Entscheidungsträger im vernetzten System. Ziel ist die Realisierung einer digitalisierten Gefechtsführung bis auf Trupp-Ebene, in der jede Information in Echtzeit zur Entscheidungsgrundlage wird.

Im modernen Einsatzraum muss der abgesessene Soldat – der Infanterist – nicht länger isoliert agieren. Durch die Integration digitaler Beobachtungs- und Aufklärungssysteme wird er zu einem aktiven Bestandteil der Sensor-to-Effector-Kette. Das Prinzip lautet: Jeder Soldat ein Sensor. Damit wird Führungsfähigkeit nicht nur top-down gesichert, sondern auch bottom-up gestärkt – durch unmittelbare Rückmeldung aus der Stellung.

Die Umsetzung dieser Vision gelingt durch die Vernetzung leistungsfähiger Systeme. Im Rahmen der Experimentalserie Land 2025 konnte dies eindrucksvoll demonstriert werden. Multispektrale Beobachtungsgeräte wie etwa der NIGHTWOLF von Safran ermöglichen durch optische, thermale und SWIR-Kanäle eine umfassende Aufklärung bei Tag, Nacht und schlechter Sicht. In Kombination mit einem stabilisierten Schwenk-Neigekopf und externem KI-Server erfolgt eine automatisierte Klassifizierung und Zielerfassung. Die gewonnenen Daten werden unmittelbar an das Battle Management System (BMS) – etwa SitaWare Frontline – übermittelt. Damit entsteht ein aktuelles, einheitliches Lagebild, das allen Führungsebenen zur Verfügung steht.

Ob fahrzeuggestützt oder abgesessen: Der Operator steuert die Systeme über ein robustes Tablet oder einen Controller – er muss sich nicht gegenüber dem Feind exponieren. Auf dem Fahrzeug ist der Schwenk-Neigekopf und NIGHTWOLF auf einem Teleskopmast montiert, der sich bis auf vier Meter Höhe ausfahren lässt. Ergänzend liefern Minidrohnen wie die Black Hornet zusätzliche Perspektiven aus der Luft. So entsteht eine Multikanal-Aufklärung. Über die Safran Softwarelösungen MAPS & REPORTS können ergänzend zu einer KI-Lösung mittels digitaler Karten im NIGHTWOLF die Art einer Bedrohung, Waffengattung, die Geschwindigkeit, Richtung und Art feindlicher Kräfte präzise erfasst und mit NATO-Symbolik ebenfalls an das BMS gesendet werden. Das Lagebild aktualisiert sich in Echtzeit – Führungsfähigkeit wird zu einem kontinuierlichen, datenbasierten Prozess.

Das System mit NIGHTWOLF als Sensor auf einem Schwenk-Neigekopf und Teleskopmast.

Fotos: Safran

Der NIGHTWOLF als zentraler Sensor des abgesessenen Soldaten.

Mit dem Multikanalgerät und der Software MAPS & REPORTS lassen sich hochpräzise Aufklärungsdaten und Koordinaten übertragen.

Mithilfe von KI können Informationen zu Fahrzeug-Typ, Feuerkraft und Besatzung direkt im Observations-Gerät angezeigt werden.

Diese Form der Informationsüberlegenheit verkürzt entscheidend den OODA-Loop (Observe – Orient – Decide – Act). Zielkoordinaten mit Target Location Error (TLE) CAT I-Genauigkeit stehen den Führungsebenen unmittelbar zur Verfügung, wodurch die Sensor-to-Effector-Kette drastisch beschleunigt wird. Entscheidungen können auf einer soliden, verifizierten Datengrundlage getroffen werden.

Die enge Verzahnung von Sensorik, Kommunikation, Künstlicher Intelligenz und Wirkmittel bedeutet jedoch mehr als technische Innovation. Sie stärkt die Führungsfähigkeit durch Transparenz und Einheitlichkeit in der Entwicklung des Lagebilds. Der abgesessene Soldat wird damit nicht nur zum Datensammler, sondern zu einem integralen Bestandteil der vernetzten Operationsführung – ein „Digital Infantry Node" im taktischen Netz.

Im Verbund mit starken Partnern der Verteidigungsindustrie sowie Startups entsteht ein umsetzungsfähiges Gesamtsystem, das die taktische Aufklärung auf ein neues Niveau hebt. Der abgesessene Infanterist ist damit nicht länger das schwächste Glied der Informationskette, sondern ein entscheidender Faktor für den Erfolg im digitalen Gefecht einer Multi-Domain Operation. ■

Kontakt:
Safran Electronics & Defense Germany GmbH
Gottlieb-Daimler-Str. 60
71711 Murr
T +49 (0) 7144 8114-0
F +49 (0) 7144 8114-22

Autor:

Marzell Schiller ist CEO der Safran Electronics & Defense Germany.

DIEHL
Defence

Das Kinetic Defence Vehicle

Vernetzte, mobile und einsatzbewährte Drohnenabwehr für aktuelle Bedrohungslagen

Alexander Teufert-Schulz

Unbemannte Luftfahrzeuge haben sich innerhalb von nur drei Jahren von einer taktischen Zusatzfähigkeit zu einem dominanten Element moderner Landkriegsführung entwickelt. Die Ukraine ist der Beweis und zugleich Warnung als auch Vorbote für die NATO-Landstreitkräfte. Drohnen sind günstig, massenhaft verfügbar, präzise und adaptiv. Sie werden nicht mehr nur für die Aufklärung genutzt, sondern vor allem für den Angriff auf taktische Einsatzkräfte, Logistik, Infrastruktur und Hochwertziele. Genau in diesem Problemfeld adressiert Diehl Defence mit dem Kinetic Defence Vehicle eine Fähigkeitslücke, die in klassischen Luftverteidigungskonzepten bisher nicht vorgesehen war: der schnelle, mobile und effiziente Schutz vor kleinen, niedrig fliegenden und massenhaft auftretenden feindlichen Drohnen.

Was dieses System strategisch interessant macht

Das Kinetic Defence Vehicle (kurz: KDV) ist bewusst nicht „einfach eine weitere" Luftverteidigungslösung, sondern eine taktisch gedachte Antwort auf die operative Gegenwart: Drohnenabwehr im Nah- und Nächstbereich muss schnell wirken, bezahlbar und unkompliziert verlegefähig sein. Denn wer im 21. Jahrhundert mobile Gefechtsstände, Logistik und Einheiten vor günstigem aber hoch effizientem Feindgerät schützen will, braucht eine ergänzende Hardkill-Dimension zu hochleistungsfähigen Schutzsystemen wie z.B. dem bodengebundenen Luftverteidigungssystem IRIS-T SLM.

Kein „Mini-GBAD", sondern ein Point-Defence-Effektor für den Nahbereich

Diehl Defence hat das System auf die innerste Schicht eines „Multi-Layered Air Defence"-Ansatzes ausgelegt: Point Defence im Nahbereich – dort, wo Drohne und Wirkung zusammenfallen; dort, wo Sekunden entscheiden. Das Kinetic Defence Vehicle soll „die Truppe" schützen – und zwar hoch mobil, mit 360°-Schutz bei Fahrt und im Stationärbetrieb.
Zum System gehören:

- Zieldetektion
- KI-gestützte Identifikation und Klassifikation
- automatische Zielverfolgung
- Hardkill-Effektoren-Mix (Rohrwaffe und Abfangdrohnen)

Genau dieser Aufbau macht das KDV militärisch attraktiv: es bietet nicht „ein bisschen von allem", sondern präzise das, was aktuell fehlt.

Architektur

Das KDV kombiniert hochauflösende passive und aktive Sensorik zur Identifizierung mit KI-basierter Zielklassifikation, automatisiertes Tracking, eine direkt integrierte kinetische Waffenstation und weitreichendere Effektoren zur Erhöhung der Reichweite des Systems. Hier liegt ein Kernvorteil des KDVs: sensorische Aufklärung und Effektor kommunizieren in einem geschlossenen System auf einem Fahrzeug – keine Datenverzögerung, kein Overhead, keine Schnittstellen, die im Gefecht gestört werden könnten. Das Resultat: eine kürzere Sensor-to-Shooter-Zeit.

Foto: Diehl

Das Kinetic Defence Vehicle – KDV © Diehl Defence


Foto: Diehl

Das KDV im Verbund mit dem System IRIS-T SLM aus dem Hause Defence © Diehl Defence

Vernetzung zur Steigerung des Einsatzwertes

Die zusätzlich vorgesehene Möglichkeit der Anbindung an ein übergeordnetes Luftlagebild liefert in Verbindung mit den weitreichenden Abfangdrohnen darüber hinaus die Möglichkeit, die effektive Kampfentfernung des KDVs auf über 20 km zu steigern. Dies alles ist möglich ohne eine notwendige Zentralisierung von Entscheidungsprozessen und Fähigkeiten. In der Konsequenz ergibt sich hieraus ein redundantes Mesh-Netzwerk von Sensoren, Effektoren und frei definierbaren Entscheidungsinstanzen, welches den Anforderungen an eine resiliente Systemarchitektur für hochintensive und dislozierte Gefechtsführung Rechnung trägt.

Bedeutung für das Deutsche Heer

Für Landstreitkräfte ist Drohnenabwehr nicht mehr nur „Luftwaffen-Thema", es bedeutet viel mehr den wichtigen Eigenschutz. Gerade in Deutschland – mit seiner Doktrin von beweglicher Gefechtsführung – braucht ein Bataillon und selbst eine Kompanie die Fähigkeit, Drohnen selbstständig abzuwehren, ohne die Luftwaffe einbinden zu müssen.

Das Kinetic Defence Vehicle ist genau dort anschlussfähig:

- hochmobil
- ebenengerecht
- Eskalationsfähigkeit durch Nutzung spezieller Primär- und Sekundäreffektoren in hybriden oder zivilen Lagen (z.B. militärische Evakuierungsoperationen)
- minimaler Ausbildungsaufwand und geringer logistischer Fußabdruck
- wirtschaftliches Munitionsversorgungskonzept

Man kann sagen: es ist das erste industriell verfügbare kinetische C-UAS System, das die durch Drohnen entstandene operative Lücke der Landstreitkräfte im Nahbereich schließt – nicht perspektivisch, sondern jetzt.

Zukunftsfähigkeit und anschlussfähige Weiterentwicklung

Die Architektur ist modular: Radare, Sensoren und Effektoren sind nachrüstbar, ergänzbar und konfigurierbar. Eine Hybridisierung (Softkill + Hardkill) ist möglich. Genau diese Faktoren machen das System nicht nur kurzfristig nutzbar, sondern zukunftsfähig.
Deutschland darf nicht wieder zehn Jahre warten, bis „C-UAS" in eine Struktur eingegliedert ist. Die Zeit ist jetzt. Wir brauchen verfügbare Systeme, nicht nur Demonstratoren.

Fazit

Das Kinetic Defence Vehicle ist eine verfügbare, praxiserprobte Antwort auf die aktuellen und zukünftigen Bedrohungen aus der Luft für Landstreitkräfte. Es wirkt auch dort, wo heute am meisten drohnenbasierte Wirkung entsteht: im niedrigen, engen, schnellen Nahbereich. Der Konflikt in der Ukraine hat gezeigt, dass genau diese Fähigkeit keine Theorie, sondern eine Notwendigkeit ist. Das Deutsche Heer braucht verfügbare, effiziente und mobile Drohnenabwehr – jetzt. Das Kinetic Defence Vehicle liefert genau das. ■

Kontakt:
Diehl Defence GmbH & Co. KG
Fischbachstraße 16
D-90552 Röthenbach an der Pegnitz
www.diehl.com

Autor:

Alexander Teufert-Schulz ist Head of Kinetic Defence © Diehl Defence

HENSOLDT
Detect and Protect.

Situational Awareness, intra- und interplattform vernetzte Systeme

Mathias Laich, Michael Krutina

Hensoldt blickt auf eine über 175-Jährige Firmengeschichte zurück, als Moritz Hensoldt in Sonneberg 1847 seine Werkstatt gründete und bahnbrechende Innovationen hervorbrachte, so zum Beispiel eine erste beschussfeste Zieloptik für Gewehre, die auf der Hessischen Jägerbüchse verwandt wurde.

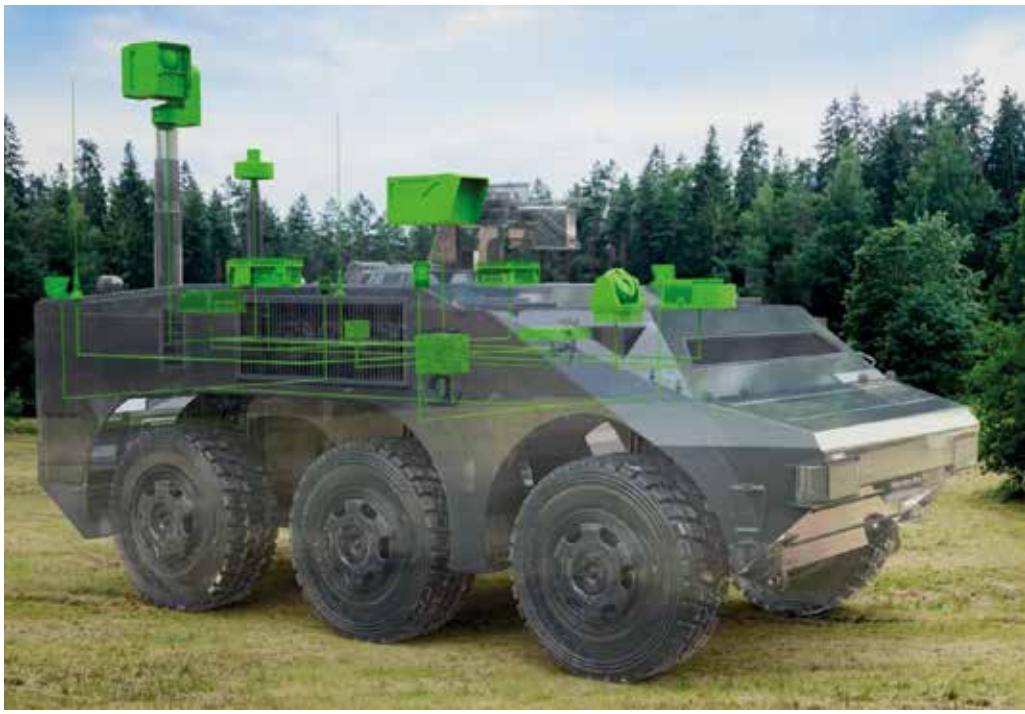
Seither haben wir uns der Sensorik in den unterschiedlichen elektromagnetischen Frequenzspektren verschrieben, vom sichtbaren Licht, über die nichtsichtbaren Lichtspektren bis hin zu Radaren.

Und wir bleiben natürlich nicht in der Vergangenheit stecken, sondern machen uns Gedanken, was als Nächstes kommt. Die Sensoren werden immer leistungsstärker und empfindlicher, dringen in Tiefe und Breite in weitere Anwendungsbereiche vor. Das bedeutet, dass wir schon heute einem massiven Informationsüberfluss gegenüberstehen, der weiter anwächst und die Schwelle zur kognitiven Überlastung der Soldaten schon längst überschritten hat.

Wir alle wissen, hiergegen muss etwas getan werden, um unseren Soldaten im Feld statt Überlastung einen taktischen Vorteil zu bieten.

Wenn wir uns aktuelle und zukünftige Gefechtsfahrzeuge ansehen, stellen wir fest, dass die verbauten Sensoren schnell eine Datenleistung im mittleren Gigabyte-Bereich generieren – pro Sekunde! Auch die hier exemplarisch dargestellten Sensoren wie Fahrzeug-Navigation, ein 360°-Sichtsystem, Beobachtungs- und Zielgeräte, Funkpeiler, das Battle Management System (BMS) und die Fahrzeugdaten sind einzeln bereits in der Lage, die Besatzung vollkommen zu überfordern. Das bedeutet, dass – wenn sie als Besatzung nicht scheitern wollen – sie vorselektieren müssen, welche Sensordaten sie in Betracht ziehen und damit Gefahr laufen, wesentliche Informationen zu übersehen oder Sie haben ein Fahrzeug, auf dem die Daten zusammengefahren und analysiert werden und durch die intelligente Kombination verschiedener Algorithmen relevante Information extrahiert und der Besatzung aggregiert und ggf. als Meta-Objekte bereitgestellt werden – und sogar mit möglichen Handlungsvorschlägen. So kann die Besatzung schneller reagieren und überleben: denn wer schneller schießt und besser trifft, gewinnt den Feuerkampf.

Quellen: Hensoldt



Verknüpfung der Sensorik und des Führungssystems am Beispiel eines Aufklärungsfahrzeuges.

Die Hensoldt-Lösung Ceretron ist eine modulare Softwaresuite mit containerisierten Services, die einzeln upgedatet, ausgetauscht oder angepasst werden können – also Software-Defined-Defence pur.

Diese Information muss aber nicht auf das Fahrzeug beschränkt sein. Stellen Sie sich vor, Informationen werden nicht wie traditionell über Sprechfunk oder Flaggen und Handzeichen übermittelt, sondern automatisiert unter Rückgriff auf die bestehende Kommunikationsinfrastruktur, beispielsweise ein Soveron Funkgerät, die Information an weitere Gefechtsfahrzeuge der Teileinheit weiterreicht.

Vorbei sind die Zeiten, als es hieß: „ALPHA an alle: Beobachtungshalt an Höhenrippe, A1 Stellung an WALDKANTER, Beobachtungsbereich von linker Grenze KUSSELGRUPPE bis rechter Grenze LICHTUNG, A2 Stellung an HOCHSITZ, Beobachtungsbereich von linker Grenze LICHTUNG bis rechter Grenze HOLZHÜTTE …". Eine Zuweisung in dieser Form war aufgrund der unterschiedlichen Blickwinkel stets fehleranfällig.

Die Zuordnung der Beobachtungsbereiche kann nunmehr durch Knopfdruck ohne Fehlerquellen an die anderen Be-

satzungen übermittelt werden. Und Ceretron steuert die Beobachtungsgeräte automatisiert von linker zu rechter Grenze und erkennt und meldet auftretenden Feind durch Änderungsdetektion, Formerkennung, Verhalten usw. Und so ein gemeldeter Feind mit gleichzeitigem Vorschlag an die Waffenanlage wird auch an das BMS übergeben und da eine bidirektionale Schnittstelle genutzt wird, auch in den anderen Gefechtsfahrzeugen dargestellt.

Änderungsdetektion und Form- bzw. Verhaltenserkennung

Ein weiteres Beispiel: Sie befinden sich in der Gefechtsaufklärung dem Angriff des Bataillons voraus. Ihr multifunktionales Selbstschutzsystem MUSS erkennt den Abschuss einer Panzerabwehr-Lenkflugkörpers, löst vorab festgelegte Abwehrmaßnahmen ein, meldet diese an die Besatzung UND an die anderen Gefechtsfahrzeuge, die ggf. den Feind direkt niederhalten können. Und im schlimmsten Fall ist die Information der feindlichen Stellung in der Combat Cloud und steht den folgenden Kräften zur Verfügung.
Oder mehrere Gefechtsfahrzeuge klären Feindkräfte auf und statt diese händisch ins BMS übertragen zu müssen, wird zunächst ein Abgleich durchgeführt - ein Feind, mehrere Beobachtungen, oder mehrere Feinde - und überführt diese auf Knopfdruck ins BMS.
Ceretron ist heute verfügbar, ressourcenschonend und effizient, dass wesentliche Fähigkeiten auf der Bestandshardware des Systems D-LBO aufgespielt werden kann und lauffähig ist. Dabei werden - oder sind bereits – unsere Sensoren oder die von Drittherstellern mit EDGE-Hardware zur Vorauswertung befähigt, das interne Kommunikationsnetz wird nicht überlastet und die verbaute Hardware im Fahrzeug ist nicht überfordert. ■

Kontakt:
Hensoldt AG
Willy-Messerschmitt-Str. 3
D-82024 Taufkirchen

Autor:

Mathias Laich ist Programmleiter Networked Systems und **Michael Krutina** ist Key Account Manager Deutsches Heer – Group Sales HENSOLDT

PLATH

Das elektromagnetische Spektrum im Wandel – Vom Funkraum zur Führungsdomäne

Ein neues Verständnis von Aufklärung

Jakob Purrucker, Leiter Vertrieb Deutschland

Wenn USB-C die universelle Schnittstelle der Gerätewelt ist – könnte CESMO (Cooperative Electronic Support Measures Operations) die Schnittstelle des elektromagnetischen Gefechtsfelds werden? Diese Frage steht sinnbildlich für eine Entwicklung, die Streitkräfte weltweit beschäftigt: Wie lässt sich ein Raum koordinieren, in dem jede Welle gleichzeitig Freund, Feind oder Störsignal sein kann?

Im modernen Einsatz existieren kaum noch eindeutige Signaturen. Kommerzielle Satelliten, Drohnenlinks, Mobilfunk und militärische Systeme überlagern sich im selben Frequenzraum. Die eigentliche Herausforderung besteht darin, aus dieser Flut elektromagnetischer Aktivität das Relevante zu erkennen – ohne selbst sichtbar zu werden.

Vom Übertragungsweg zum Gefechtsfeld – ein kurzer Rückblick

In den 1920er-Jahren war das elektromagnetische Spektrum vor allem ein Übertragungsweg. Ab Mitte der 1930er wurde es zum Sensorraum – Stichwort Radar. Wer damals früh erkannte, dass man Wellen nicht nur senden, sondern auch „sehen" konnte, erlangte im Zweiten Weltkrieg einen entscheidenden taktischen Vorteil. Funkpeilung, ENIGMA-Entschlüsselung und britische Radarnetze markierten den Beginn der elektromagnetischen Gefechtsführung – lange bevor dieser Begriff existierte.

Nach 1945 wandelte sich das Spektrum vom Sensor- zum Führungsraum: Kommunikation, Aufklärung und Störung wurden zur Lebensader moderner Streitkräfte. Mit der zunehmenden Mechanisierung des Heeres entstand ein Wettrennen um Kontrolle – zwischen Funk, Gegenfunk und Täuschung.

Ab den 1980er-Jahren brachte die Computerisierung, um hier noch nicht von Digitalisierung zu sprechen, des Gefechtsfelds eine neue Dimension. GPS, Datenlinks und Netzwerke machten die Nutzung effizienter, aber auch verwundbarer. Was früher analog rauschte, wurde digital sichtbar – und damit zum zentralen Ziel elektronischer Aufklärung.

Das elektromagnetische Spektrum heute – überfüllt, umkämpft, unverzichtbar

2025 ist das Spektrum ein hochgradig vernetzter, aber überlasteter Operationsraum. Kommunikation, Navigation, Sensorik und Wirkung sind digital verschmolzen – zivil wie militärisch.

Bereiche zwischen 1 und 4 GHz sind durch Mobilfunk, WLAN, Bluetooth und Internet of Things (IoT) - Anwendungen so stark belegt, dass militärische Nutzer nur noch begrenzt Zugriff haben und klassische Aufklärungssysteme nicht auf diesem Bereich optimiert sind

Die aktuelle Lage lässt sich in drei Begriffen zusammenfassen:

- Congested – überfüllt durch zivile und militärische Parallelaktivität.
- Constrained – eingeschränkt durch (notwendige) Regulierung und Frequenzmanagement.
- Contested – umkämpft durch aktive elektronische Stör- und Täuschmaßnahmen.

Damit wird das elektromagnetische Spektrum zum Operationsraum eigener Art, in dem jede Welle eine potenzielle Information oder Bedrohung darstellen kann.

Das veränderte Spektrum bei Landoperationen

Früher sagte man, wo ein Radar steht, da ist auch ein Funkgerät, heute steht da eine ganze Kommunikationsarchitektur. Ein Passiv-Radar strahlt nicht einmal mehr. Zwischen taktischem Funk, Datenlinks, Relaisstrecken und 5G-Netzen fließen Signale in permanenter Bewegung. Auch private Mobiltelefone, die sich im Hintergrund versuchen mit Sendemasten zu verbinden, verraten die eigene Position. Tarnung und Funkstille verlieren ihren Sinn, wenn die notwendige (Funk-)Disziplin nicht existiert.

In aktuellen Konflikten, etwa in der Ukraine, wird das deutlich: Zivile Kommunikationsmittel sind nicht nur Werkzeuge der eigenen Führung, sondern auch Sensoren für den Gegner. Satellitenbilder, Social-Media-Beiträge und Mobilfunkdaten tragen zur Lageerfassung bei – oft unbeabsichtigt. Die Folge: Jede Welle kann potenziell zur Zielinformation werden.

Von der Datenflut zur Entscheidungsüberlegenheit

Die Informationsmenge im Spektrum wächst exponentiell. Moderne Aufklärungssysteme müssen nicht nur Signale

Grafiken: Plath

Die Nutzung des Elektromagnetischen Spektrums in der Vergangenheit

Die Nutzung des Elektromagnetischen Spektrums heute

erfassen, sondern sie kontextbezogen bewerten – also erkennen, welche davon relevant, täuschend oder gefährlich sind. Klassische Verfahren stoßen hier an Grenzen.
Neue Technologien wie Edge-Processing und Distributed Sensing ermöglichen die Vorverarbeitung direkt an der Quelle: Daten werden lokal analysiert, klassifiziert und priorisiert, bevor sie an zentrale Führungsstellen weitergegeben werden. So entsteht ein verteiltes, robustes Sensornetzwerk, das auf Veränderungen im Spektrum nahezu in Echtzeit reagiert.
Zugleich führt der Einsatz operationeller KI dazu, dass Signale nicht nur erkannt, sondern „verstanden" werden. Sie verbindet Sensorik, Auswertung und Führung zu einem geschlossenen Wirkverbund. Sie erkennt Muster, bewertet Signale und initiiert Maßnahmen, noch bevor ein Mensch eingreifen muss. Das Ziel ist nicht Maschinenautonomie, sondern die Beschleunigung menschlicher Entscheidungsfähigkeit: Tempo durch Verständnis, nicht Entscheidung durch Maschine. Um einen Führungsvorteil für den Truppenführer zu erreichen!

CESMO – ein gemeinsames Protokoll im elektromagnetischen Raum

Zu Beginn stand die Frage, ob CESMO die Schnittstelle des elektromagnetischen Gefechtsfelds werden kann – so wie USB-C unsere Geräte verbindet. Tatsächlich hat CESMO das Potenzial, Sensoren, Plattformen und Führungsstrukturen über ein gemeinsames Datenprotokoll zu verbinden.
Der Erfolg entscheidet sich jedoch nicht an der Technik, sondern an der gemeinsamen Anwendung und Nutzung. Erst wenn alle Beteiligten im elektromagnetischen Raum dieselbe Sprache sprechen – also Daten in Echtzeit austauschen, klassifizieren und interpretieren können – wird Vernetzung zur Wirkung. CESMO könnte damit zum Rückgrat eines integrierten elektromagnetischen Lagebilds werden. Es muss also auch in der Bedarfslage klar gefordert werden.

Ausblick auf 2045 – das Spektrum als gemeinsame Ressource

Ein Blick auf die NATO-Readiness-Roadmap 2030 und die technologischen Makrotrends bis 2045 zeigt, dass sich diese Entwicklung fortsetzt. Zukünftige Einsatzfähigkeit wird sich weniger an Kräften und Mitteln messen lassen, sondern an der Fähigkeit, Informationen schnell und sicher in Wirkung umzusetzen.

- 6G-Kommunikation (30–300 GHz) wird hochauflösende Radar- und Datenverbindungen ermöglichen.
- Terahertz-Bereiche (300 GHz–3 THz) erschließen neue Möglichkeiten für Zielerkennung und sichere Links.
- Quantensensorik und Quantenkommunikation schaffen Resilienz gegen Spoofing und elektronische Täuschung.
- Orbitale Mesh-Netze gewährleisten globale Abdeckung – unabhängig von klassischen Infrastrukturen.

Damit wird das elektromagnetische Spektrum zur Führungs- und Wirkdomäne der Zukunft und zentrales Bindeglied für Multi-Domain Operations. Der elektronische Kampf tritt aktuell wieder absolut in den Vordergrund. Er entscheidet über Erfolg und Misserfolg, was im UKR-Krieg deutlich zu sehen ist.

Von der Technik zur Taktik

Entwicklungszyklen verkürzen sich, Technologien werden austauschbar – entscheidend ist ihre Anpassungsfähigkeit. Konzepte wie Software Defined Defence (SDD) ermöglichen, Fähigkeiten unabhängig von Plattformen weiterzuentwickeln und schnell zu aktualisieren. Damit bleibt elektronische Aufklärung handlungsfähig, auch wenn Hardware oder Frequenzen sich ändern.
Neue Datendoktrinen priorisieren vor allem Geschwindigkeit. Die operative Relevanz liegt nicht mehr allein im Schutz der Quelle, sondern in der sofortigen Nutzung taktisch relevanter Daten. Wer schneller versteht, kann schneller handeln. Das ist von entscheidender Bedeutung für jeden Truppenführer. Die Ukraine hat es verstanden, sich dies zu Nutzen zu machen und neben der Technologie insbesondere Ihre operationelle Arbeitsweise und die Datenfusion & Meldung entsprechend angepasst.

Fazit – Unsichtbare Wellen, sichtbare Wirkung

Das elektromagnetische Spektrum hat sich vom Übertragungsweg zur strategischen Führungsdomäne entwickelt. In einem Umfeld, in dem jede Welle Information oder Gefahr sein kann, gewinnt die Fähigkeit zur schnellen und richtigen Erkennung, Bewertung und Nutzung elektromagnetischer Signale stetig an Bedeutung für moderne Streitkräfte.
Aufklärung wird dynamischer, datengetriebener – und wertvoller. Wer Signale nicht nur empfängt, sondern versteht und verknüpft, schafft Informations- und damit Führungsvorsprung. Das elektromagnetische Umfeld ist keine Störung – es ist eine Quelle, wenn man sie richtig auswertet und nutzt. ■

Kontakt:
PLATH GmbH & Co. KG
Gotenstraße 18
20097 Hamburg

PLATH Systems and Integration ist ein international tätiger produktunabhängiger Systemintegrator und entwickelt und projektiert kundenindividuelle Lösungen für Spektrumsoperationen. Unter dem Dach der PLATH Unternehmensgruppe agiert PLATH Systems and Integration eigenständig am Markt. Mit eigenen Fertigungsmöglichkeiten in Deutschland stellt PLATH eine resiliente Lieferkette sicher. Als familiengeführter wehrtechnischer Mittelständler mit über 600 Beschäftigten und über 70 Jahren Branchen-Erfahrung unterstützt die PLATH ihre Kunden weltweit bei der Erfüllung ihres Sicherheitsauftrags – mit dem Ziel, die Welt zu einem sicheren Ort zu machen.

STARK

Abschreckung braucht Masse: Warum unbemannte Systeme jetzt entscheidend sind

STARK Defence

In der öffentlichen Anhörung der Nachrichtendienste im Deutschen Bundestag warnte der Präsident des Bundesnachrichtendienstes (BND), Martin Jäger, eindringlich vor einer trügerischen Sicherheit. „Wir dürfen uns nicht zurücklehnen in der Annahme, ein möglicher russischer Angriff käme frühestens 2029“, so Jäger. „Wir stehen schon heute im Feuer.“ Russland verfolge das Ziel, die NATO zu unterminieren, europäische Demokratien zu destabilisieren und seine Einflusszonen nach Westen auszudehnen.

Angesichts der aktuellen sicherheitspolitischen Lage wird deutlich: Deutschland, als zentrale europäische Führungsnation, muss in den nächsten Jahren schnell ein großes Abschreckungspotential aufbauen, um den Frieden auf dem Kontinent zu wahren.

Die nächsten vier Jahre sind für Europa entscheidend. Moskau operiert längst in der Logik einer permanenten Kriegswirtschaft – mit massivem Ausbau seiner Drohnen-, Munitions- und Waffenproduktion. Europa hingegen befindet sich erst am Anfang eines Fähigkeitshochlaufs. Entscheidende Waffensysteme – Panzer, Artilleriegeschütze, Kampfflugzeuge – werden trotz aller Anstrengungen frühestens Anfang der 2030er Jahre in der nötigen Stückzahl verfügbar sein.

Fotos: Stark

Die VIRTUS Loitering Munition

Die Rolle unbemannter Systeme

Loitering Munition ermöglicht abstandsfähige, massenhafte Wirkung sowie präzise Schläge und die Saturierung gegnerischer Verteidigung. Eingebunden in das Gefecht der verbundenen Waffen kann sie Aufklärungsüberlegenheit in unmittelbare Wirkungsüberlegenheit übersetzen und ergänzt damit bestehende Systeme und Fähigkeiten der Bundeswehr. So kann ein **asymmetrischer Vorteil im Gefecht** erzielt werden. Um eine glaubhafte Abschreckung in kurzer Zeit zu erreichen, spielen unbemannte Systeme eine besondere Rolle: Ihre Entwicklung und industrielle Skalierung verlaufen um ein Vielfaches schneller als bei klassischen bemannten Waffensystemen, deren Produktions- und Zulaufzyklen Jahre bis Jahrzehnte betragen. Genau darin liegt ihr strategischer Wert: Unbemannte Systeme ermöglichen eine Abschreckungsfähigkeit, die nicht erst 2035 wirkt, sondern innerhalb weniger Jahre aufgebaut werden kann. Dieses Tempo der Skalierung bildet den Kern einer industriellen Abschreckung, die auf schneller Verfügbarkeit, kontinuierlicher Anpassbarkeit und massiver Skalierbarkeit beruht.

Wir sind in der Lage zu kämpfen, und zu gewinnen.

Hier setzt STARK mit seiner Mission an: Wir wollen unbemannte Fähigkeiten bereitstellen, welche die NATO rasch verteidigungs- und abschreckungsfähig machen. Das bedeutet konkret: Fokus auf Modularität und Skalierbarkeit – statt ausschließlich auf langfristig hochkomplexe Plattformen zu setzen. Das ist entscheidend für das politische Signal: Wir sind in der Lage zu kämpfen, und zu gewinnen. STARK hat innerhalb eines Jahres seit Gründung seine VIRTUS Loitering Munition in der Ukraine in den Einsatz gebracht. Dort wird das System im Verbund mit Aufklärungsdrohnen eingesetzt und hat seine Wirksamkeit in der Gefechtsfeldrealität unter Beweis gestellt. Grundlage dieser schnellen Entwicklung ist eine **80-Prozent-Philosophie**: Systeme gehen dann in den Einsatz, wenn sie ihre Kernleistung sicher erfüllen und gleichzeitig ausreichend Potenzial für künftige Weiterentwicklungen haben. So können Ingenieure sich auf die wesentlichen Kerneigenschaften konzentrieren – und iterativ nachschärfen.

VIRTUS wird für den Einsatz vorbereitet

Technologieübersetzer

Die in der Ukraine gewonnenen Erkenntnisse sind jedoch nicht immer 1:1 auf die Bundeswehr übertragbar. Die NATO kämpft im Gefecht der verbundenen Waffen und hat andere Sicherheitsstandards und Integrationsanforderungen. Dies erfordert eine vollständige Interoperabilität und Integration der Systeme in bestehende Führungs- und Waffeneinsatzsysteme (C2-Systeme). Deshalb braucht es eine **technologische und militärische Übersetzung** ukrainischer Operationskonzepte in ein für die Bundeswehr relevantes CONOPS. Mit seiner Software MINERVA stellt STARK die Integration in vorhandene IT-Systeme sowie die Führung von mehreren unbemannten Systemen durch einen Operateur sicher. Der Krieg in der Ukraine ist keine direkte Blaupause, liefert jedoch einen belastbaren Referenzrahmen, um sinnvolle Anpassungen abzuleiten, künftige Entwicklungen zu antizipieren und technische Innovationen in wirksame militärische Fähigkeiten zu überführen.

Zentral für diese schnelle, iterative Arbeitsweise ist die enge Verknüpfung und eine gemeinsame Vertrauensbasis von Industrie und Streitkräften – in der Ukraine wie in Deutschland. Die Bundeswehr schafft sich mit OPEX, Experimentalserien und Innovationsformaten wichtige Räume für diese Zusammenarbeit. Es ist zentral, dass diese Räume geschützt sind, sodass Entwicklungsstände offen ausgetauscht werden, um die Anpassung der Systeme an die Bedarfe der Streitkräfte zu ermöglichen. Nur so kann man von einem 80-Prozent-System zu einem 100-Prozent-System für die Bundeswehr gelangen.

Industrielle Abschreckungsfähigkeit

Masse ist die zentrale Dimension, die unbemannte Systeme überhaupt erst abschreckungswirksam macht. Damit diese Masse jedoch in kurzer Zeit bereitgestellt werden kann, braucht es eine industrielle und technologische Grundlage, die konsequent auf Geschwindigkeit, Anpassungsfähigkeit und Hochlauffähigkeit ausgelegt ist. Nur ein solcher Unterbau versetzt Deutschland in die Lage, unbemannte Systeme nicht nur zu entwickeln, sondern im Bedarfsfall auch innerhalb weniger Wochen in strategisch relevanter Stückzahl verfügbar zu machen:

1. **Modulare System-Architekturen**, die schnelle Software-Iterationen und planbare Hardware-Upgrades ermöglichen.
2. **Eine industrielle Basis**, die unterschiedliche Innovationszyklen abbilden kann – vom hochfrequenten Software-Push über kontinuierliche Batteriefertigung bis hin zu periodischen Hardware-Refits.
3. **Scalable-by-Design**, Produktionslinien, die im Frieden effizient arbeiten, im Krisenfall jedoch binnen Wochen auf Massenfertigung umgestellt werden können.

Die notwendige, schnelle Aufwuchsfähigkeit entsteht nur im Schulterschluss zwischen Militär, Staat, etablierten Rüstungsunternehmen und jungen Defence Tech Startups. Sie stehen nicht im Gegensatz zueinander, sondern ergänzen sich. Einer unserer engsten Partner von STARK ist der Gefechtskopfhersteller TDW, denn dort gilt: Bei Munitionssicherheit gibt es keine 80-Prozent-Lösungen. STARK geht hier in Vorleistung und investiert in die eigene Lieferkette und Partner, um bei kritischen Komponenten die Lieferfähigkeit gegenüber der Bundeswehr zu garantieren.

STARK steht bereit, Verantwortung für die Sicherheit Europas zu übernehmen – mit Systemen, die im Einsatz erprobt, für die Bundeswehr angepasst und im Schulterschluss zwischen Start-ups, Mittelstand und etablierter Industrie produziert werden. ■

Kontakt:
Stark
SKD SE
Charlottenstraße 4
10969 Berlin
contact@stark-defence.com

„Kann das Heer noch ohne Weltraum?“

Sven Sünberg

Foto: MBS

Diese zugegebenermaßen reißerische Frage ist spätestens seit den 1990ern bereits zu verneinen. Weltweit, operativ sichtbar wurde es ab 1991 mit der *Operation Desert Storm* und für das Deutsche Heer faktisch seit den ersten großen Auslandseinsätzen ab Mitte der 90er Jahre. Seitdem sind verlegefähige, multinationale Operationen de facto untrennbar von Weltraumdiensten abhängig. Ohne Space ist nur noch eine eingeschränkte, kurzreichweitige und hochriskante Gefechtsführung möglich.
Militärische Wirkung entscheidet sich heute auch im elektromagnetischen und informationsdominierten Gefechtsfeld. Kommunikationsnetze, PNT (Positioning, Navigation, Timing) und Erdbeobachtung sind dabei kein „Beiwerk“, sondern tragende Säulen der Führungsfähigkeit. Zielbild ist eine resiliente, robuste Architektur, die Dienste über mehrere technische und organisatorische Ebenen absichert: Multi-Orbit, Multi-Band, Multi-Hub, ergänzt um robuste PNT-Quellen und integrierte Erdbeobachtung.

„Das Gefecht ist datenreich und gestört. Architektur muss degradieren können, nicht brechen.“

Multi-Orbit, Multi-Band und Multi-Hub klingen technisch – bedeuten für das Heer aber vor allem eines: Führungsfähigkeit bleibt verlässlich verfügbar, auch wenn der Gegner stört, das Wetter schlecht ist oder eine Bodenstation ausfällt. Statt auf einen einzigen Satellitenweg zu setzen, verteilt diese Architektur die Kommunikation auf mehrere Umlaufbahnen, mehrere Frequenzbänder und mehrere, weit auseinanderliegende und verlegefähige Bodenstationen. So entstehen echte Ausweichpfade, gesteuert durch robuste Verfahren, nicht durch Improvisation im Stress. Gleichzeitig können Daten – wo sinnvoll – nahe am Einsatzraum aufbereitet werden (lokales Breakout), um Verzögerungen zu reduzieren und Abhängigkeiten zu minimieren.

„Weltraum ist Grundinfrastruktur für das Heer. Wer Multi-Orbit-SATCOM, belastbare PNT-Alternativen und verlässliche Erdbeobachtung integriert, gewinnt Geschwindigkeit, Präzision und Wirkung.“

PNT ist die zweite Säule. Ohne verlässliche Position, Navigation und exakte Zeit geraten Marsch, Feuerleitung, Drohnennavigation und Logistik ins Wanken. Auch hier hilft Vielfalt. GNSS-Signale (Global Navigation Satellite System: etwa Galileo und GPS) werden gehärtet und gegen Täuschung überprüft, Inertialsensoren überbrücken Ausfälle, zusätzliche Referenzen am Boden stabilisieren die Zeitbasis. Moderne Empfänger erkennen Störversuche und schalten auf geprüfte Signale oder kombinieren mehrere Quellen. So bleibt die Orientierung erhalten, selbst wenn der Gegner das Satellitensignal angreift.
Erdbeobachtung aus dem Weltraum präzisiert das Lagebild. Optische Satelliten zeigen Veränderungen auf der Oberfläche, SAR-Radarsysteme (Synthetic Aperture Radar) sehen durch Wolken und bei Nacht, und signalerfassende Systeme überwachen das elektromagnetische Spektrum im Operationsraum. Entscheidend ist die Verknüpfung mit der Kommunikation: Erkenntnisse müssen schnell in die Lagekarte, zu den Führungsstellen und zu den Kräften vor Ort. Wenn ein Satellit einen möglichen Störsender oder ein Luftabwehrsystem erkennt, können Effektoren effizienter und schneller zur Wirkung gebracht werden. Aus einzelnen Hinweisen entsteht ein fundiertes Bild, das Routen sichert, Ziele aufklärt und Risiken früh sichtbar macht.
Der Weltraum ist heute die Grundlage moderner Führungs-, Aufklärungs- und Navigationsfähigkeit des Heeres. Wer Raumsegment, Bodeninfrastruktur und Datenketten beherrscht, sichert Handlungsfähigkeit auch unter Druck. Deshalb müssen Architekturen so ausgelegt sein, dass sie nur stufenweise degradieren, aber niemals brechen – notfalls mit

Foto: MBS

Die Erdfunkstelle Usingen ist eine Bodenstation zur Kommunikation mit Satelliten. Sie befindet sich in Hessen, etwa 25 Kilometer nördlich von Frankfurt am Main, und liegt auf den Stadtgebieten von Usingen und Neu-Anspach. Die Erdfunkstelle wird von der Media Broadcast Satellite GmbH betrieben.

reduzierter Qualität, aber weiter nutzbar. Genau deshalb ist der Weltraum für das Heer strategisch unverzichtbar.

„Wir sind die Linie aus den Architekturen – die Konnektivität, Befähigung und Information bedeuten."

MBS liefert dem Heer verlässliche, weltraumbasierte Dienste und hält diese auch bei Fremdeinwirkung kontrolliert im Betrieb. Mit eigenen Assets am Boden und im Weltraum, integrieren wir uns nahtlos in bestehende Führungs- und Betriebsstrukturen. Wir betonen Wirkung statt Feature-Aufzählungen: resiliente Architektur, souveräner Betrieb und robuste Verfahren, untermauert durch nachweisliche Einsatzerfahrung in Kriegs- und Krisengebieten. ■

MBS ist ein inhabergeführtes, mittelständisches Unternehmen für Satellitenkommunikation und Raumfahrt mit eigener Bodeninfrastruktur in Deutschland und Europa sowie europäischer Launchfähigkeit und eigenen Erdbeobachtungssatelliten im Orbit.
Seit Jahrzehnten sichert MBS satellitengestützte Kommunikation für Bund, Bundeswehr und Verbündete.

Kontakt:
Media Broadcast Satellite GmbH
Erdfunkstelle 1
61250 Usingen
www.mb-satellite.com
info@mb-satellite.com
+49 6081 100 2402

Autor:
Sven Sünberg ist Managing Director der Media Broadcast Satellite GmbH

Fotos: FKH

Bild rechts: v.l.: Florian R. Bokermann, Generalmajor Stefan Lüth, Brigadegeneral Wolfgang Jordan, Generalmajor a.D. Wolfgang Köpke, Alexander Philipp