CIR 2.0

cpm FORUM

FÜR RÜSTUNG, STREITKRÄFTE UND SICHERHEIT

13,90 €
15,50 CHF

+ CIR 2.0 VON DER IDEE ZUR DIMENSION

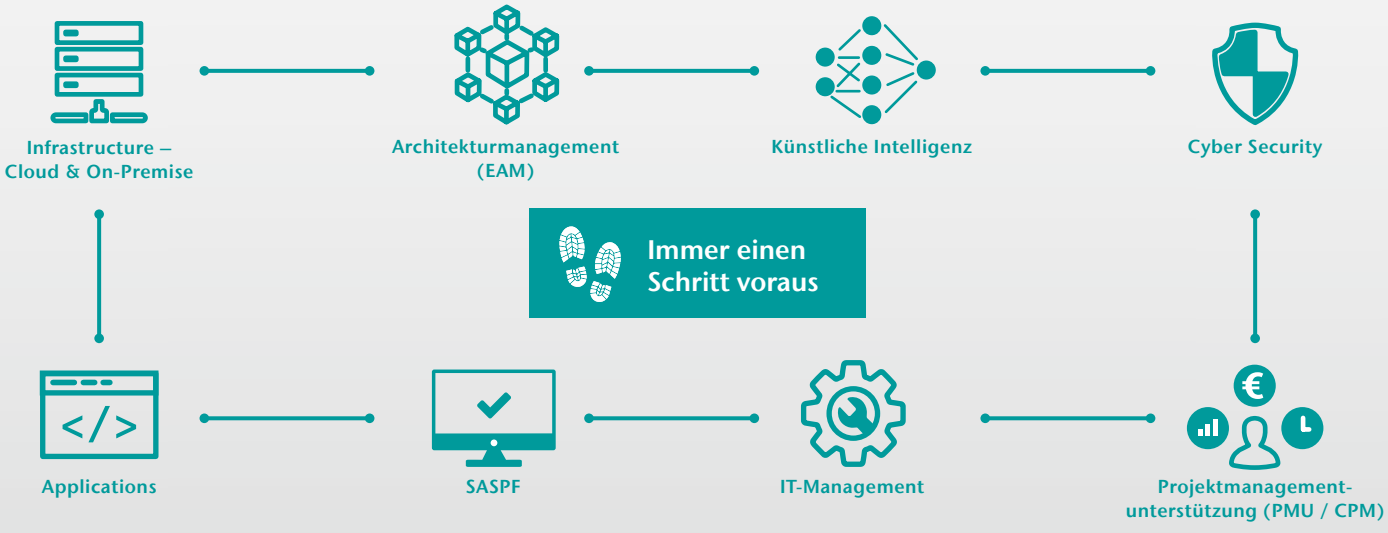
CONET

Gemeinsam einen Schritt **voraus**

Neue Herausforderungen – neue Chancen

Digitalisierung und Transformation sind für den Verteidigungssektor 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 zu digitalisierten Prozessen und Lösungen!**

Mehr als 30 Jahre **verlässlicher Partner** der Bundeswehr-IT!



SAP • Infrastructure • Communications • Software • Consulting

www.conet.de • info@conet.de

Von Anfang an galt es, die klassischen Teilstreitkräfte als „Enabler“ und „Force Provider“ zu unterstützen, gleichzeitig jedoch den Auftrag zum Planen und Führen eigenständiger CIR-Operationen umzusetzen.

Der Organisationsbereich CIR schützt nicht nur die Systeme der Bundeswehr, er leistet auch einen Beitrag zur gesamtstaatlichen Sicherheit.
Foto: Bundeswehr/Broschinsky

DIENSTSTELLEN-PROFIL

KOMMANDO CYBER- UND INFORMATIONSRAUM

Das Kommando Cyber- und Informationsraum stellt in der Dimension CIR Führung, Aufklärung, Wirkung, Schutz und Betrieb des IT-Systems der Bundeswehr aus einer Hand sicher. Der OrgBer CIR ist damit sowohl eigenständiger Fähigkeitsträger für CIR-Operationen als auch wesentlicher Unterstützer in Operationen der anderen Teilstreitkräfte. Zudem ist das Kommando Treiber der Digitalisierung für die Bundeswehr im Teilportfolio Cyber/IT eng verbunden mit der Fähigkeitsentwicklung im CIR.

AUFGABEN

- Planung und Führung von CIR-Operationen.
- Treiber der Digitalisierung in der Bundeswehr.
- Aufklärung, Wirkung, Betrieb und Schutz im CIR.
- Sicherstellung des Militärischen Nachrichtenwesens.
- Beitrag zum Schutz kritischer Cyber-/IT-Infrastruktur im Rahmen gesamtstaatlicher Sicherheitsvorsorge.
- Chief Information Security Officer Bundeswehr (CISOBw).
- Gewinnung, Entwicklung und Halten von Fachpersonal.

AUFTRAG

Das Kommando Cyber- und Informationsraum (KdoCIR) plant und führt, als Führungskommando des Organisationsbereichs, CIR-Operationen zur Unterstützung der operativen Ebene/NATO und anderer Dimensionskommandos. Dies umfasst Aufklärung und Wirkung sowie den Betrieb und Schutz des IT-Systems der Bundeswehr (ITSysBw). Es trägt die operationelle Dimensionsverantwortung und kann nationale CIR-Operationen, auch als Beitrag im Bündnis, führen. Damit leistet es einen essentiellen Beitrag zur Landes- und Bündnisverteidigung (LV/BV) und unter anderem durch Präsenz im Nationalen Cyber-Abwehrzentrum zur gesamtstaatlichen Cybersicherheit.

Neben der Synchronisation von Aufklärung – Wirkung – Betrieb und Schutz, verantwortet das Kommando die Bereitstellung der streitkräftegemeinsamen militärischen Nachrichtenlage durch das JIC, die Steuerung der Sensorik (z.B. Fernmelde- und Elektronische Aufklärung, weltraumgestützte Aufklärung) und die Sicherstellung des Betriebs des ITSysBw.

Das Kommando trägt die Verantwortung für die Gewährleistung der Informationssicherheit und den Schutz des ITSysBw. In der Abteilung Planung CIR und Digitalisierung Bundeswehr werden Vorgaben für die Umsetzung der Digitalisierung der Bundeswehr entwickelt.

In seiner Dimensionsverantwortung entwickelt das Kommando konzeptionell Fähigkeiten der Bundeswehr zur Cyberverteidigung bereits unterhalb der Schwelle zum bewaffneten Konflikt bis hin zur LV/BV.

Der Inspekteur CIR verantwortet die dimensionsübergreifenden fachspezifischen Werdegänge Cyber/IT, Operative Kommunikation, Militärisches Nachrichtenwesen und die Laufbahn Geoinformationsdienst der Bundeswehr.

ANSCHRIFT
Johanna-Kinkel-Straße 2-4,
53175 Bonn

DIENSTSTELLENLEITUNG
Vizeadmiral Dr. Thomas Daum

STAMMPERSONAL
~1260

AUFSTELLUNG
05.04.2017

ZIELSTRUKTUR **CIR 2.0**

BEWERTUNGS- UND ENTSCHEIDUNGSEBENE

Abteilung Operation

Aufklärung in allen Dimensionen

Wirkung im CIR

DURCHFÜHRUNGSEBENEN

- **Zentrum Operative Kommunikation der Bundeswehr** (S. 13)
- **Kommando Aufklärung und Wirkung** (S. 15)
- **EloKaBtl 911** (S. 27)
- **EloKaBtl 912** (S. 31)
- **EloKaBtl 931** (S. 39)
- **EloKaBtl 932** (S. 47)
- **Fernmeldeaufklärungszentrale Nord**
- **Fernmeldeaufklärungszentrale Süd**
- **Zentrum Cyber-Operationen** (S. 55)
- **Zentrale Abbildende Aufklärung** (S. 61)
- **Zentrale Untersuchungsstelle der Bundeswehr für Technische Aufklärung** (S. 65)

Chef des Stabes

Inspekteur Cyber- und Informationsraum

StvInspCIR/ CISOBw

Abteilung Führung

Abt Planung CIR/ Digitalisierung Bundeswehr

Betrieb des IT-SysBw

Kommando Informationstechnik-Services der Bundeswehr (S. 75)

- **ITBtl 281** (S. 79)
- **ITBtl 282** (S. 85)
- **ITBtl 292** (S. 89)
- **ITBtl 293** (S. 97)
- **ITBtl 381** (S. 109)
- **ITBtl 383** (S. 113)
- **DDO/DtA 1st NATO Signal Battalion Wesel** (S. 119)

Schutz der ITBw

Zentrum für Cyber-Sicherheit der Bundeswehr (S. 127)

Unterstützung

Zentrum für Geoinformationswesen der Bundeswehr (S. 133)

Ausbildungszentrum CIR*

Schule Informationstechnik der Bundeswehr (S. 147)

Schule für Strategische Aufklärung der Bundeswehr (S. 161)

Digitalisierung

Zentrum Digitalisierung der Bundeswehr und Fähigkeitsentwicklung Cyber- und Informationsraum (S. 183)

ZUR ZIELSTRUKTUR **CIR 2.0**

Zum 01. Oktober 2022 haben das Kommando CIR, das Zentrum Digitalisierung der Bundeswehr und Fähigkeitsentwicklung CIR sowie das Zentrum für Cyber-Sicherheit der Bundeswehr, das nun dem Stellvertreter Inspekteur CIR unterstellt ist, bereits ihre Zielstruktur eingenommen. Zum 01.04.2023 werden das Kommando Aufklärung/Wirkung und das Kommando IT-Services der Bundeswehr aufgestellt. Ebenso werden die ortsfesten Anteile des EloKaBtl 911/931 ausgegliedert, die zukünftig die Fernmeldeaufklärungszentralen Nord/Süd abbilden. Die Wappen dieser Dienststellen sind noch im Gestaltungsprozess.

* Ab dem 01.04.2024 werden die beiden Schulen, Schule Informationstechnik der Bundeswehr und Schule für Strategische Aufklärung der Bundeswehr, in dem Ausbildungszentrum CIR aufgehen.

Sehr geehrte Leserin, sehr geehrter Leser,

seit über fünf Jahren existiert nun der jüngste Organisationsbereich Cyber- und Informationsraum (CIR) der Bundeswehr. Schon mit den ersten Überlegungen wurde die Dimension bewusst weiter gefasst als seinerzeit international mit „cyber as a military domain of operations" betrachtet.

Im militärischen Operationsraum CIR haben wir den Cyberraum, das elektromagnetische Spektrum und das Informationsumfeld zusammengeführt. Alle drei Bereiche werden als Einheit betrachtet und aus einer Hand gestaltet. Dieser Ansatz hat sich gerade angesichts der jüngsten sicherheitspolitischen Entwicklungen bewährt und gewinnt für die Landes- und Bündnisverteidigung weiter an Bedeutung. Dies wird mittlerweile auch international anerkannt, wie konzeptionelle Weiterentwicklungen in Partnernationen in der jüngsten Zeit andeuten.

Im Unterscheid zu den anderen Dimensionen Land, Luft/Weltraum und See gilt, dass wir im CIR bereits lange vor einer Krise oder einem Konflikt gefordert sind, uns unter Friedensbedingungen in einem permanenten Wettbewerb zu behaupten und zur gesamtstaatlichen Cybersicherheit beizutragen.

Damit wird deutlich, was unseren Markenkern ausmacht. Zum einen ist dies unsere Fähigkeit zum Planen und Führen von CIR-Operationen, die dabei das gesamte Spektrum von Aufklärung, Wirkung, Betrieb und Schutz durchgehend abdeckt. Zum anderen ist dies unsere Rolle als „Treiber der Digitalisierung" für die Bundeswehr, wodurch wir gewährleisten, dass alle Bereiche der Bundeswehr von der Digitalisierung profitieren, die Streitkräfte zum gemeinsamen Kampf der verbundenen Dimensionen befähigt werden, die Verwaltungsarbeit modernisiert wird und technologische Innovationen erschlossen werden.

Auch 2022 ist ein bewegtes Jahr. Eine große Krise wurde nahezu verzugslos von einer nächsten Krise abgelöst. Hat uns bis zum 24. Februar 2022 vor allem die Corona-Pandemie in Atem gehalten, so war es ab dann eine kriegerische Auseinandersetzung mitten in Europa. Mit dem brutalen Angriffskrieg von Russland gegen die Ukraine wurde uns die Bedeutung des Cyber- und Informationsraums im Vorfeld eines Konflikts und während der bewaffneten Auseinandersetzung besonders verdeutlicht.

Das notwendige Fokussieren der Streitkräfte auf die Fähigkeit zur Landes- und Bündnisverteidigung und die Fähigkeit zum schnellen Anpassen an neue Gegebenheiten wurde durch die Ereignisse gleichermaßen und erneut unterstrichen. Dies gilt aufgrund der kurzen Innovationszyklen der relevanten Technologien und der besonderen Dynamik bei der Kriegsführung im Cyber- und Informationsraum in ganz besonderer Weise.

Mit „CIR 2.0" verschlanken wir daher unsere Strukturen und beschleunigen unsere Prozesse. Mit Vollendung des Umbaus werden nur noch eine Führungsebene und die Durchführungsebenen bestehen. Mit den dabei möglichen Ressourcengewinnen stärken wir unsere Fachlichkeit.

Die besten Ideen und die beste Technik sind nicht genug, denn für die Umsetzung innovativer Ansätze bleibt Personal der entscheidende Faktor. Deshalb steht der Mensch im Mittelpunkt. Die Bereitschaft zum Denken außerhalb eingefahrener Wege und der Wille zum aktiven Mitgestalten sind gleichermaßen unabdingbar. Flexible Methoden und Instrumente für die Personalgewinnung und für die Personalbindung sind in Zeiten des demografischen Wandels zwingend, um konkurrenz- wie handlungsfähig zu bleiben. Für die Belange unserer Dimension entwickeln wir daher personalpolitische Instrumente.

Seit der Aufstellung im April 2017 haben wir uns in unserem Organisationsbereich stetig weiterentwickelt. Von Anfang an galt es, die klassischen Teilstreitkräfte als „Enabler" und „Force Provider" zu unterstützen, gleichzeitig jedoch den Auftrag zum Planen und Führen eigenständiger CIR-Operationen umzusetzen. Gleichzeitig übernehmen wir gesamtstaatliche Verantwortung und tragen in enger Zusammenarbeit und im Austausch mit den anderen Ressorts zur Cybersicherheit Deutschlands bei.

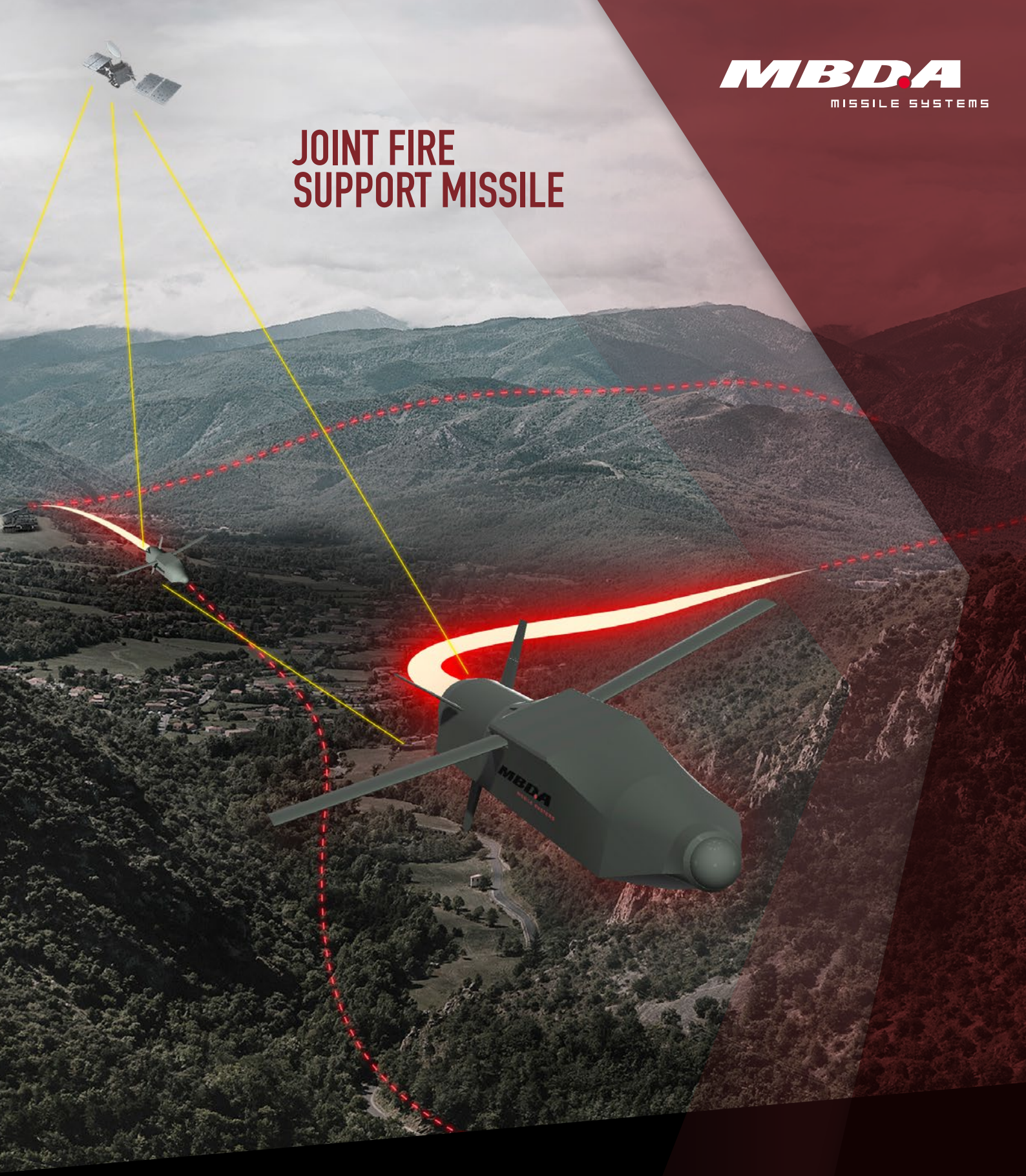
Die vielfältigen Aspekte, die unsere Dimension besonders kennzeichnen, werden nachfolgend in unserem Sonderheft „CIR 2.0 – Von der Idee zur Dimension" dargestellt. Gerne lade ich Sie nun zu einem Streifzug durch unseren Organisationsbereich Cyber- und Informationsraum ein.

Ihr

Dr. Thomas Daum
Vizeadmiral

MBDA
MISSILE SYSTEMS

JOINT FIRE SUPPORT MISSILE



JFS-M ist ein intelligenter Lenkflugkörper für das zukünftige System Indirektes Feuer. Fähigkeitsgewinn durch variable Einsatzmöglichkeiten in komplexen Gefechtsszenarien: Aufklärung, Wirkung, Elektronischer Kampf und Ausbildung.

SECURING THE SKIES
PROTECTING YOUR ASSETS
MASTERING THE SEAS
COMMANDING THE COMBAT ZONE

Mehr Informationen:
www.mbda-deutschland.de

INHALT

BILDNACHWEISE:

Cover: Zentrum für Softwarekompetenz der Bundeswehr am Standort Euskirchen.
Foto: Bundeswehr/Martina Pump; Collage: cpm

◄ Außenansicht der SARah-Satelliten-Antenne der Zentrale Abbildende Aufklärung in Grafschaft.
Foto: Bundeswehr/Müller

Grußwort **Bundesministerin der Verteidigung**

Das fünfjährige Jubiläum des militärischen Organisationsbereichs Cyber- und Informationsraum (CIR) fällt in eine Zeit größter Herausforderungen. Inmitten des digitalen Wandels sind wir mit einem weiteren Umbruch von epochalem Ausmaß konfrontiert: einer sicherheitspolitischen Zeitenwende. Und diese Zeitenwende verstärkt den Druck auf unseren digitalen Fortschritt ganz gewaltig. Der brutale russische Angriffskrieg gegen die Ukraine hat nicht nur die europäische Friedensordnung erschüttert. Er führt uns auch sehr deutlich vor Augen, welch zentraler Schlüssel der digitale Raum – und damit Ihr Kompetenzgebiet – für unsere Sicherheit ist: für unsere militärische Verteidigungsfähigkeit genauso wie für unsere gesamtgesellschaftliche Widerstandskraft.

Zum einen sehen wir die sich mutig verteidigende Ukraine. In atemberaubender Geschwindigkeit haben ukrainische Techniker, Informatiker und Ingenieure das Satellitensystem STARLINK von Elon Musk mitten im Krieg eingeführt und für die eigene Gefechtsführung anwendbar gemacht: für Aufklärung, Logistik, Command and Control. So laufen nicht nur die russischen Angriffe auf die kommunikative Infrastruktur teilweise ins Leere. Es gelingt den ukrainischen Streitkräften sogar, durch eine überlegene Führungs- und Aufklärungsfähigkeit eine zahlenmäßige Unterlegenheit auf dem Schlachtfeld erheblich zu kompensieren.

Zum anderen sehen wir, wie Russland den Konflikt systematisch in den digitalen Raum trägt. Social Media gestützte Hass- und Desinformationskampagnen mit dem Ziel, unsere demokratischen Gesellschaften zu spalten, sind längst ein weit verbreitetes Phänomen. Seit Beginn des Krieges wird zudem versucht, russische Kriegspropaganda durchzusetzen und so die Unterstützung für die Ukraine zu schwächen. Insgesamt beobachten wir eine deutliche Zunahme von Aktivitäten im Cyber- und Informationsraum, gerade auch Cyberangriffe auf kritische Infrastruktur: Verwaltungen, Krankenhäuser, Kraftwerke. Immer wieder richten sich solche Angriffe auch gegen die Bundeswehr.

Vor diesem Hintergrund stellen sich zwangsläufig unbequeme Fragen: Wie steht es um die digitalen Fähigkeiten unserer eigenen Streitkräfte? Wie gut sind wir in Deutschland gegen Angriffe jeglicher Art im Cyber- und Informationsraum gerüstet? Gerade auch dank des militärischen Organisationsbereichs CIR haben wir hier in den vergangenen Jahren wichtige Fortschritte erzielt. Wahrheit aber bleibt: Deutschland und die Bundeswehr haben noch einen Weg vor sich.

Entscheidend ist, dass wir die Cybersicherheit als gesamtstaatliche Aufgabe annehmen. Bei Angriffen und Bedrohungen aus dem digitalen Raum verschwimmen die Grenzen zwischen außen und innen, staatlich und nicht staatlich, Krieg und Kriminalität. Für Schutz und Vorsorge brauchen wir daher sowohl militärische als auch zivile Beiträge. Und diese Beiträge müssen sich wechselseitig ergänzen und verstärken. Daher danke ich Ihnen im Organisationsbereich CIR, dass Sie schon heute intensiv mit dem Bundesamt für Sicherheit in der Informationstechnik und dem Nationalen Cyber-Abwehrzentrum zusammenarbeiten – und so bereits laufende ressortübergreifende Aktivitäten verstärken. Auch mit dem Lagebild CIR leisten Sie einen wichtigen Beitrag zur gesamtstaatlichen Cybersicherheit. Wir müssen diese Zusammenarbeit weiter ausbauen, auch über Ländergrenzen hinweg. Vor allem aber müssen wir das Fundament der gesamtstaatlichen Cybersicherheit stärken, das heißt: den Digitalstandort Deutschland fördern (nationale Schlüsseltechnologien, Innovationsfähigkeit, ausgeprägte digitale Kompetenzen), die Verfügbarkeit sicherer und interoperabler IT-Systeme sicherstellen und umfassende Datensouveränität erlangen.

All dem muss unsere (Cyber-)Sicherheitsarchitektur künftig Rechnung tragen. Mit der ersten Nationalen Sicherheitsstrategie werden wir Deutschland konsequent auf diese Ziele ausrichten. Damit knüpfen wir nahtlos an das neue Strategische Konzept der NATO wie auch an den kürzlich verabschiedeten Strategischen Kompass der EU an. Beide Dokumente erklären die Cybersicherheit mit Recht zu einer vordringlichen gemeinsamen Aufgabe.

Ebenso entscheidend ist es, dass wir bei der Digitalisierung der Bundeswehr einen großen Sprung nach vorne machen. Es ist nicht das einzelne Fahrzeug, Schiff oder Kampfflugzeug, das unser Land wehrhaft macht. Es ist das Zusammenwirken von allen Bereichen – aus der Luft, auf dem Boden, zur See, im Weltraum und im Cyber- und Informationsraum. Daher legen wir mit dem Sondervermögen von 100 Milliarden Euro einen Schwerpunkt auf Führungs- und Aufklärungsfähigkeit: moderne Satelliten, leistungsfähige Rechenzentren, sichere Kommunikation. Dies sind die Schlüsselfähigkeiten, von denen alles andere abhängt. Es geht nicht nur darum, in der Bundeswehr auf der Höhe der Zeit miteinander kommunizieren zu können, sondern vor allem auch um unsere internationale Anschlussfähigkeit. Es muss selbstverständlich werden, dass unsere Soldatinnen und Soldaten mit ihren amerikanischen, niederländischen oder französischen Kameradinnen und Kameraden verschlüsselt miteinander funken und Informationen austauschen können.

Daran zeigt sich einmal mehr auch die grundlegende Bedeutung Ihres Organisationsbereichs CIR. Hier liegen die Verantwortlichkeiten und Strukturen zur Digitalisierung in einer kompetenten Hand. Hier wird die Informationssicherheit der gesamten Bundeswehr gesteuert und überwacht. Und hier schreiten Sie voran, wenn es darum geht, die Fähigkeiten und Wirkmittel im Cyber- und Informationsraum zu entwickeln und auszubauen. Das hier vorhandene Spektrum an hochspezialisierten Fähigkeiten ist bemerkenswert. Davon konnte ich mich bei meinen Besuchen an Ihren verschiedenen Dienststellen selbst überzeugen. Auf diese Fähigkeiten können Sie stolz sein! Genauso wie auf Ihren unersetzlichen Beitrag zur Ausbildung in der Bundeswehr. Ihre digitalen Lernplattformen und Virtual Reality-Simulationen von Gefechtsszenarien haben mich beeindruckt. Digitale Kompetenzen gepaart mit dem richtigen Mindset, von der Führungsspitze bis zur Truppe, sind Garant für eine erfolgreiche digitale Transformation unserer Streitkräfte. Und dafür stehen Sie!

Ich danke Ihnen sehr für diese Leistungen, Ihr großes Engagement und die gute Zusammenarbeit! Sehr zu schätzen weiß ich auch, dass Sie sich nicht auf dem Erreichten ausruhen, sondern daran arbeiten, noch wirksamer und wirtschaftlicher zu werden: mit der Strukturreform CIR 2.0. Klar ist: nur mit Ihrem hohen persönlichen Einsatz können wir die Bundeswehr zu der hoch modernen, interoperablen, informations-, führungs- und wirkungsüberlegenen Armee machen, die wir in dieser Zeitenwende brauchen. Ihr Beitrag zur gesamtstaatlichen Cybersicherheit in Deutschland ist gerade jetzt unverzichtbar. Gratulation zu fünf Jahren Organisationsbereich CIR!

Ihre

Christine Lambrecht
Bundesministerin der Verteidigung

DIENSTSTELLEN-PROFIL

ZENTRUM OPERATIVE KOMMUNIKATION DER BUNDESWEHR

Die Angehörigen des Zentrums Operative Kommunikation unterstützen die Operationsführung eigener und multinationaler Streitkräfte in den verschiedenen Einsatzgebieten der Bundeswehr mit Wirkmitteln der Operativen Kommunikation.

AUFGABEN

- Wir sind das „I" in CIR.
- Wir wirken im Informationsumfeld – mit unseren Analystinnen und Analysten, Redakteurinnen und Redakteuren, interkulturellen Einsatzberaterinnen und -beratern und Kräften der taktischen Direktkommunikation.
- Wir erstellen Audio-, Video-, Print- und Social Media-Produkte.
- Wir berichten live für die Führung mit unseren Einsatzkameratrupps.
- Wir betreuen und informieren die Truppe mit Radio Andernach und Bundeswehr TV.

AUFTRAG

Erkennen. Beraten. Beeinflussen: Teams des Zentrums Operative Kommunikation (ZOpKomBw) analysieren die Situation der Bevölkerung und der gegnerischen Streitkräfte in den Einsatzgebieten und wirken mit audiovisuellen Medien konventionell und digital auf Zielgruppen außerhalb der Bundeswehr. Immer mit dem Ziel, die Operationsführung der eigenen Kräfte zu unterstützen. Dort wo andere Medien nicht eingesetzt werden können, bieten weitreichende Lautsprecher und selbst verbrachte Flugblätter die Möglichkeit zur zielgerichteten Kommunikation. Grundlage aller Kommunikation ist eine detaillierte, kulturspezifische Analyse der Zielgruppe. So verfügt die Operative Kommunikation über die Fähigkeit, das Informationsumfeld verschiedener Regionen zu analysieren und stellt diese als „Lage im Informationsumfeld" dar. Ebenso stellt das ZOpKomBw die Einsatzkameratrupps, die der politischen Leitung und militärischen Führung der Bundeswehr ein visuelles Lagebild aus Krisen- und Einsatzgebieten in Echtzeit zur Entscheidungsfindung bereitstellen. Auch der Truppenbetreuungssender Radio Andernach und Bundeswehr TV zählen zu den Unterstützungsaufgaben des ZOpKomBw. Radio Andernach, das Einsatzradio, bildet neben der täglichen Truppeninformation und -betreuung eine emotionale Brücke zwischen Einsatz und Heimat. Es wird nicht nur aus dem heimischen Funkhaus, sondern auch aus den Einsatzgebieten gesendet und von Korrespondententeams berichtet.

ANSCHRIFT
Oberst-Hauschild-Kaserne,
Kürrenberger Steig 34,
56727 Mayen

DIENSTSTELLENLEITUNG
Oberst Dr. Ferdi Akaltin

STAMMPERSONAL
~1.000

AUFSTELLUNG
01.10.1959

Grußwort **Generalinspekteur der Bundeswehr**

Zum fünfjährigen Bestehen des militärischen Organisationsbereichs Cyber- und Informationsraum (CIR) gratuliere ich allen Angehörigen recht herzlich.

Die Gründungsmotivation im Jahr 2017 ist damals wie heute uneingeschränkt relevant. Die Bundeswehr bündelt ihre Dimensionsverantwortung, um die Chancen des digitalen Raums zur Modernisierung zu nutzen und die dimensionsübergreifende Einsatzbereitschaft und Verteidigungsfähigkeit zu verbessern.

Wir haben bereits nach der völkerrechtswidrigen russischen Annexion der Krim im Jahr 2014 begonnen, die Bundeswehr in ihrer gesamten Breite für den Kernauftrag der Landes- und Bündnisverteidigung aufzustellen, zum einen durch erhöhte Personalumfänge, zum anderen durch Fokussierung auf Materialausstattung und Modernisierung. Der abscheuliche Angriffskrieg Russlands gegen die Ukraine hat uns allen klar vor Augen geführt: die Ausrichtung der Streitkräfte auf diesen Kernauftrag muss mit aller Dringlichkeit und Schnelligkeit weiterverfolgt werden.

Dieser Krieg bestätigt auch, dass militärische Konflikte zunehmend in allen Dimensionen ausgetragen werden. Die gezielte Nutzung der Dimension CIR ist ein Teil komplexer hybrider Bedrohungen sowohl unterhalb der Schwelle des offenen militärisch geführten Konfliktes als auch nach Ausbruch offener Kampfhandlungen. Wir müssen mit dieser zunehmenden Komplexität und Dynamik umgehen. Es ist daher unerlässlich, selbst Fähigkeiten in dieser Bandbreite aufzubauen, vorzuhalten und ständig weiterzuentwickeln.

Bei der Planung und Führung von Operationen müssen militärische Führungsentscheidungen ohne Verzögerung, basierend auf einem aktuellen, digitalen Lagebild, ortsunabhängig und technologisch unterstützt getroffen werden. Zeit und vertrauenswürdige Information sind dabei kritische Faktoren. Um im Verbund mit multinationalen Partnern schnell reaktionsfähig und flexibel zu sein, müssen wir interoperabel agieren können. Die Digitalisierung trägt maßgeblich dazu bei, die Informationen und Erkenntnisse aus dem System Militärisches Nachrichtenwesen zur Wirkung zu bringen. Nationale und internationale Kooperationen in diesem Bereich sind Voraussetzung für die Bereitstellung eines umfassenden digitalen Lagebildes.

Gleichzeitig nutzen gegnerische Akteure den CIR bereits im Vorfeld eines Konfliktes gezielt für Angriffe. Deutschland ist dabei ein Hochwertziel. Die Bundeswehr selbst steht dabei mit ihren vielfältigen Waffensystemen, ihrem IT-System und ihrer Einbindung in (inter-)nationale Informationsflüsse im Fokus.

Dieser dynamischen Bedrohungslage muss im Sinne der gesamtstaatlichen Resilienz auch mit einer effektiven ressortgemeinsamen Zusammenarbeit der für Krisenmanagement, Kommunikation, Nachrichtenwesen und Cybersicherheit zuständigen Akteure begegnet werden.

Im Rahmen der Gesamtverteidigung leistet Ihr militärischer Organisationsbereich mit seinen Hochwertfähigkeiten nicht nur in der Dimension CIR hinsichtlich Führungsfähigkeit, Aufklärung, Wirkung und Unterstützung einen entscheidenden Beitrag. Er bündelt dazu die Fähigkeiten zur Planung und Führung von Operationen im CIR, zum Betrieb und Schutz von Informationstechnik, zur Elektronischen Kampfführung, zur Operativen Kommunikation und für Cyberoperationen. Er bildet außerdem den zentralen Anteil zur Bereitstellung von Geoinformationen und das Militärische Nachrichtenwesen ab.

Um dimensionsübergreifende Synergien zu schaffen, plant und führt der Organisationsbereich CIR zum einen Operationen in nationaler Verantwortung, bei denen das gesamte zuvor genannte Fähigkeitsportfolio zum Einsatz kommen kann. Zum anderen integriert der Organisationsbereich CIR seine Fähigkeiten in die Kräftedispositive bei Land-, Luft- und maritimen Operationen sowie Operationen der Spezialkräfte im multinationalen Kontext.

Unsere Fähigkeiten im CIR ergänzen also das Portfolio Deutschlands und unserer Partnernationen zur strategischen Abschreckung sowie Verteidigung. Um die nationale wie multinationale Führungs- und Einsatzfähigkeit unserer Streitkräfte zu gewährleisten, bedarf es zukunftsorientierter, interoperabler Lösungen: im Rahmen der NATO vorrangig für die NRF bzw. VJTF, zur Stärkung der NATO-Ostflanke sowie künftig für die ARF und die neue NATO Force Posture, im Rahmen der EU bei den EU Battlegroups, künftig für die European Rapid Deployment Capacity.

Eine dieser Lösungen ist das Battle Management System (BMS). Dank Ihrer Vorarbeit hinsichtlich Implementierung, Testung und Zertifizierung dieser Software kann Deutschland als führende Rahmennation der NATO VJTF 2023 das BMS zur Verfügung stellen, das dann erstmalig in Zusammenarbeit mit unseren Bündnispartnern eingesetzt wird.

Außerdem richten wir die eigene Fähigkeitsentwicklung an den Vorgaben des Federated Mission Networking (FMN) aus, um gemeinsame, agile und interoperable Streitkräfte auf das Gefechtsfeld zu führen. FMN ist damit ein Schlüsselelement zur Erlangung einer „Day-Zero-Interoperability", also der Kaltstartfähigkeit der Bundeswehr im CIR.

Darüber hinaus werden wir mithilfe des Sondervermögens Bundeswehr die durchgängige Aufklärungs- und Führungsfähigkeit weiter verbessern. Wir werden vorrangig die Digitalisierung unserer landbasierten Operationen, die Ausstattung mit modernen Kommunikationssatelliten, die Beschaffung von verlegefähigen Rechenzentren und sicheren, mobilen, taktischen Kommunikationsmitteln finanzieren. Dabei möchte ich hervorheben, dass diese Projekte den gesamten Streitkräften zugutekommen.

In diesen bewegten Zeiten bietet das fünfjährige Bestehen des Organisationsbereichs CIR Anlass zur Reflexion: wir sind auf dem richtigen Weg und haben viel geschafft. Gleichzeitig befinden wir uns mitten in einem Prozess des Umbruchs und der Erneuerung. Das gilt auch für die Struktur und Organisation des Organisationsbereichs CIR. Hier wurden neue Wege beschritten, Führungsebenen zweckmäßig zusammengeführt, Entscheidungsprozesse vereinfacht und so beschleunigt. Die Erfahrungen aus diesem Prozess bitte ich Sie mit den übrigen Organisationsbereichen zu teilen.

Ich danke Ihnen für Ihr Engagement, für Ihre hohe Motivation und Ihren klaren Fokus darauf, unter oft schwierigen Rahmenbedingungen und mit einem stets vollen Auftragsbuch die Umstrukturierung zu CIR 2.0 mitzugestalten.

Lassen Sie uns den weiteren Weg gemeinsam gehen und das Aufgaben- und Fähigkeitsprofil der Bundeswehr im CIR zukunftsgerecht schärfen.

Eberhard Zorn
General

DIENSTSTELLEN-PROFIL

KOMMANDO AUFKLÄRUNG UND WIRKUNG

Der „Enabler" für einsatzbereite Kräfte und Fähigkeiten Aufklärung und Wirkung im Organisationsbereich CIR.

AUFGABEN

- Wir stellen unsere Aufklärungsmittel weltweit zur Verfügung.
- Wir stellen die erforderlichen technischen Netzwerke bereit.
- Wir leisten damit täglich einen Beitrag zur politischen Entscheidungsfindung und unterstützen somit die Vorbereitung und Durchführung der Einsätze.
- Wir produzieren und entwickeln mediale Print-, Foto- und Video-Produkte für das gesamte Militärische Nachrichtenwesen.

AUFTRAG

Das Kommando Aufklärung und Wirkung (KdoAufkl/Wirk) hat seinen Zielstandort zum 01.04.2023 in Daun in der Eifel mit Außenstellen in Grafschaft, Süddeutschland und Flensburg. Die Auswertezentrale Elektronische Kampfführung am Standort Daun wird wiederum zum 01.04.2023 aufgelöst und geht im Kern im neuen KdoAufkl/Wirk auf.

Das KdoAufkl/Wirk stellt Kräfte und Fähigkeiten der Elektronischen Kampfführung (EloKa) und Cyberoperationen sowie Fähigkeiten der Abbildenden Aufklärung und der Offenen Informationsgewinnung bereit. Zudem nimmt das Kommando die streitkräftegemeinsamen Aufgaben der zentralen Medienproduktion des militärischen Nachrichtenwesens (MilNW) sowie des IT-Betriebs und Systemunterstützung der EloKa und des MilNW wahr. Die etwa 3.700 Frauen und Männer des Kommandos inklusive der unterstellen Dienststellen und Verbände sind Spezialistinnen und Spezialisten und leisten einen wichtigen Beitrag für den Schutz der Angehörigen der Bundeswehr in Einsätzen im Rahmen der Landes-/Bündnisverteidigung sowie des internationalen Krisenmanagements.

Die beiden wesentlichen Pfeiler des Kommandos sind die Bereiche Aufklärung und Wirkung.

In seinem gesamten Kommandobereich werden die Ergebnisse der Fernmelde- und Elektronischen **Aufklärung**, der Abbildenden Aufklärung, der Aufklärung im Cyberraum sowie der Aufklärung offen zugänglicher Quellen erzielt und den unterschiedlichen Bedarfsträgern bereitgestellt. Die Informationen aus den verschiedenen Elementen werden im Kommando Cyber- und Informationsraum zusammengefasst und zu einer Gesamtlage fusioniert.

Im Bereich der **Wirkung** stellen die Kräfte des Elektronisches Kampfes und die Kräfte des Zentrums für Cyberoperationen einzigartige Fähigkeiten im Portfolio der Bundeswehr dar und ermöglichen den militärischen Führern und der politischen Leitung zusätzliche Handlungsoptionen.

ANSCHRIFT
Heinrich-Hertz-Kaserne,
Heinrich-Hertz-Straße 10,
54550 Daun

DIENSTSTELLENLEITUNG
n.n.

STAMMPERSONAL
~3.700
(inkl. unterstellter Bereiche)

AUFSTELLUNG
01.04.2023

DR. REINHARD BRANDL (MDB)

Fünf Jahre Erfolgsgeschichte **Organisations-bereich CIR**

Vom Start-Up zum Full-Service-Dienstleister für die Sicherheit Deutschlands im Cyber- und Informationsraum

GRÜNDUNG DES ORGANISATIONSBEREICHS CIR – START-UP DER BUNDESWEHR IN EINEM DYNAMISCHEN UMFELD

Unsere Streitkräfte im In- und Ausland werden mehr denn je gefordert. Multinationale Einsätze auf drei Kontinenten, integrierte multinationale Gefechtsführung, komplexe Herausforderungen durch hybride Einflussnahme, die Refokussierung auf Landes- und Bündnisverteidigung und eine digital vernetzte Welt lassen die Anforderungen an die Bundeswehr stetig wachsen. Sie muss sich in allen Bereichen kontinuierlich hinterfragen und weiterentwickeln. Ihre Aufbauorganisation als das stabile, aber auch statische Rückgrat der Bundeswehr muss als Antwort auf diese Herausforderung deutlich flexibler, agiler und resilienter werden. Sie wird sich immer wieder an neue Herausforderungen anpassen müssen. Wir müssen uns daran gewöhnen, dass die Organisation der Bundeswehr nicht mehr über Jahre hinweg stabil bleiben kann. Vielmehr muss sie sich dauerhaft auf neue Herausforderungen einstellen. In diesem dynamischen Umfeld wurde der Organisationsbereich Cyber- und Informationsraum (CIR) im April 2017 aufgestellt, um auf die Bedrohungen und die Verwundbarkeit der Bundeswehr im Cyber- und Informationsraum besser und aus einer Hand reagieren zu können.

STETIGE ANPASSUNG AN DAS DYNAMISCHE UMFELD – AUFBAUPHASE DES ORGANISATIONSBEREICHS CIR

Auf die gegenwärtigen Entwicklungen des sicherheitspolitischen Umfelds – vor allem mit Blick in Richtung Osten des europäischen Kontinents – darf die deutsche Außen- und Sicherheitspolitik nicht nur reagieren. Vielmehr muss die Ausrichtung der Streitkräfte auch neu justiert werden. In einem multipolaren sicherheitspolitischen Umfeld vor dem Hintergrund real existierender hybrider Einflussnahme und in Anbetracht potenzieller Konfliktszenarien über alle Dimensionen hinweg, musste und muss insbesondere auch der Organisationsbereich CIR den sich wandelnden Anforderungen gerecht werden. Gleichzeitig muss er die bruchfreie Planung und Führung auf der operativen Ebene sicherstellen können.

ETABLIERTER AKTEUR IN EINEM DYNAMISCHEN UMFELD – FULL-SERVICE-DIENSTLEISTER DER BUNDESWEHR FÜR DIE SICHERHEIT DEUTSCHLANDS IM CYBER- UND INFORMATIONSRAUM

In der modernen Informationsgesellschaft werden aktuelle Bedrohungen häufig als hybride Kriegsführung charakterisiert. Diese Form des Konflikts fokussiert neben den klassischen militärischen Instrumenten vor allem Einsatzmittel aus den Bereichen Medien und Kommunikation sowie aus dem Cyber- und IT-Bereich. Durch die intensive Nutzung dieser modernen Technologien entstehen gleichzeitig Abhängigkeiten und Verwundbarkeiten, die missbraucht und für Angriffe in Form von Propaganda, Desinformationskampagnen und Cyberattacken ausgenutzt werden können. Die Angriffe erfolgen meist unterhalb der offiziellen Schwelle zum bewaffneten Konflikt, können ihn aber auch begleiten. Der Organisationsbereich CIR bietet heute mit all seinen Fähigkeiten Mittel und Wege an, den Bedrohungen aus dem Cyber- und Informationsraum die Stirn zu bieten. Inzwischen betreibt und schützt er etwa die eigenen militärischen Fernmelde- und IT-Netzwerke. Dabei kooperiert er eng mit dem Bundesamt für Sicherheit in der Informationstechnik und anderen Akteuren im nationalen Cyber-Abwehrzentrum. Darüber hinaus verfolgt der Organisationsbereich CIR Aufklärung und Wirkung im Cyberraum und im Informationsumfeld. Zudem stellt er wesentliche Informationen für ein aktuelles Lagebild für die politische und militärische Führung auf allen Ebenen bereit. Dazu zählt alles von Aufklärungsergebnissen aus dem militärischen Nachrichtenwesen über Geoinformationen bis hin zu Wetter- und Flugdaten.

Für die Zukunft wünsche ich dem Organisationsbereich CIR nur das Beste. Ihn aufzustellen war eine wichtige und richtige Weichenstellung. Seine Bedeutung wird in den kommenden Jahren weiter steigen.

UNSER BEITRAG FÜR SICHERHEIT IM CYBER- UND INFORMATIONSRAUM

Aufklärungssysteme und Elektronischer Kampf, Cyber-Resilienz, BSI-Grundschutz, Informationssicherheit, SW-Entwicklung und Cyber Aus- und Weiterbildung

esg.de

GRUSSWORT

Generalleutnant a. D. Ludwig Leinhos

Liebe Leserinnen und Leser,
als im September 2015 die damalige Verteidigungsministerin Ursula von der Leyen in einem Tagesbefehl die Aufstellung eines „herausgehobenen Organisationsbereiches" für den Cyber- und Informationsraum ankündigte, überraschte sie viele, nicht nur in der Bundeswehr. Vielerorts herrschte ungläubiges Staunen, oftmals war zu hören, dass sie dies „nicht so gemeint habe". Ich kann mich allerdings noch sehr gut daran erinnern und … sie hatte es genau so gemeint!

Es war eine strategische Richtungsentscheidung, um der wachsenden Bedeutung der Dimension Cyber- und Informationsraum für die Streitkräfte nunmehr in der Grundaufstellung der Bundeswehr Rechnung zu tragen. Auch sollte so auf die rasant zunehmende Digitalisierung mit ihren vielen Vorteilen, aber auch den damit einhergehenden Risiken und neuen Gefahren reagiert werden. In der Summe war es aus vielen Gründen ein logischer Schritt und eine Notwendigkeit, diese Dimension in der Bundeswehr auf Augenhöhe mit den Dimensionen Land, Luft und See zu platzieren.

Nach einer intensiven und spannenden Aufbauphase wurde der Organisationsbereich am 5. April 2017 formal ins Leben gerufen. Inzwischen sind seit der Aufstellung mehr als fünf Jahre vergangen, Zeit für eine Bestandsaufnahme, zu der dieses Sonderheft einen wichtigen Beitrag leistet.

Im Organisationsbereich Cyber- und Informationsraum (CIR) wurden die Aufgaben Cyber-Sicherheit, IT-Betrieb, Cyber-Operationen, der Elektronische Kampf, die operative Kommunikation, das Militärische Nachrichtenwesen und das Geoinformationswesen der Bundeswehr gebündelt. Vereinfacht gesagt, im CIR wurden die nicht-kinetischen Wirkmittel und Fähigkeiten zur Verteidigung Deutschlands zusammengeführt. Mittel und Fähigkeiten, die einen unmittelbaren Bezug zum höchsten Gut einer modernen Wissensgesellschaft haben – den Informationen.

In meinen dreieinhalb Jahren als Inspekteur CIR wurden über viele aufbau- und ablauforganisatorische Maßnahmen Strukturen so angepasst, dass erhebliche Mehrwerte und Synergien erzielt wurden. Insbesondere wurde das Stove Pipe-Denken zwischen den einzelnen CIR-Elementen konzeptionell und strukturell aufgebrochen. Ebenso sahen wir uns von Anfang an als Treiber und Initiator für neue Ansätze der Zusammenarbeit unter Nutzung moderner Technologien, für flache Führungsstrukturen und damit für kritisches Hinterfragen von Hierarchien, für neue Formen der Personalgewinnungs- und Personalbindungsansätze und vieles mehr. Dies war – und ist auch jetzt noch – nicht immer einfach, galt es doch und gilt es noch immer festgefahrene Strukturen und Widerstände zu überwinden.

Vieles wurde in den ersten fünf Jahren bereits erreicht, auf das die Angehörigen des Organisationsbereichs CIR zu Recht stolz sein können. Nur genauso wie Informationstechnik regelmäßige „updates" benötigt, so unterliegt auch die Dimension CIR stetigem Wandel!

Der Cyber- und Informationsraum ist eine eigenständige Dimension, durchzieht aber in besonderem Maße auch alle anderen militärischen Dimensionen und ist zugleich wichtiger Baustein einer gesamtstaatlichen Sicherheitsarchitektur. Er ist somit einerseits klar in die militärischen Strukturen integriert, bedarf aber andererseits auch einer breiteren Ausrichtung.

Der Angriffskrieg Putins in der Ukraine hat uns auf drastische Art und Weise die Komplexität und Vielschichtigkeit hierfür notwendiger Sicherheitsarchitekturen vor Augen geführt:

Einschränkungen der Medienvielfalt, falsche oder tendenziöse Nachrichten („fake news"), gezielte und manipulative Wortwahl („Spezialoperation") sind plakative Beispiele für Maßnahmen im Informationsraum. Bedrohungen und Angriffe auf kritische Infrastrukturen sowie Regierungsnetze durch Cyberaktivtäten können nachhaltig unsere Gesellschaft schädigen.

An beiden Beispielen wird deutlich, die Sicherheit Deutschlands im CIR ist heute nicht mehr alleinige Aufgabe der Bundeswehr. Auch die insbesondere in Deutschland über viele Jahre hervorgehobene und gepflegte Trennschärfe von äußerer und innerer Sicherheit geht in Zeiten zunehmend hybrider Bedrohungen verloren. Hier gilt es gesamtstaatlich zu denken. Dies erfordert neben einem ressortübergreifenden Ansatz auf Seiten des Staates auch eine enge Einbindung von Wirtschaft und Gesellschaft. Unsere militärischen Fähigkeiten im CIR sind damit viel stärker in eine ressortübergreifende Gesamtverteidigung einzuordnen. Diese zu organisieren und zu strukturieren ist eine der vielen politischen Herausforderungen.

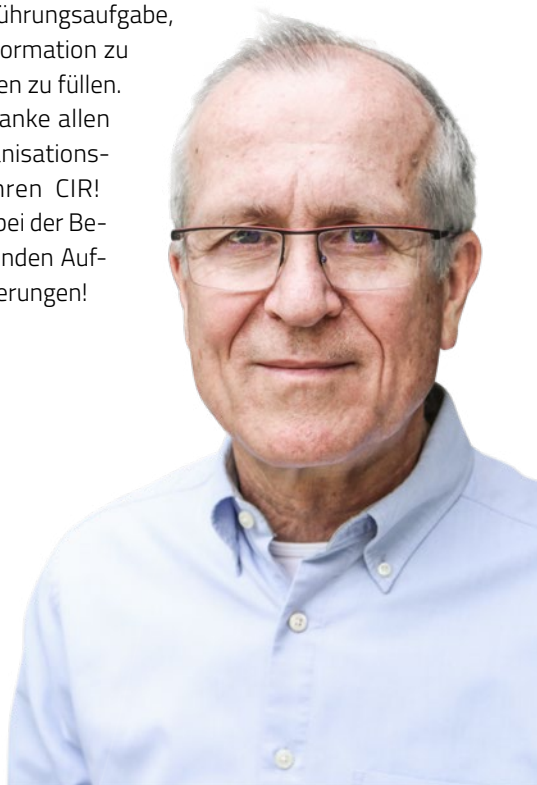
Das Verteidigungsressort hat durch die organisatorische Aufstellung des Organisationsbereichs CIR und damit durch die Abbildung der Dimension CIR unter einer Führung eine erste zukunftsweisende Antwort gegeben. Mit der Stärkung der Rolle des Nationalen Cyber-Abwehrzentrums, in dem auf Bundesebene alle hierfür relevanten staatlichen Organisationen vertreten sind, wurden für die gesamtstaatliche Verteidigung im CIR wichtige Schritte eingeleitet. Gleichwohl sind noch einige „dicke Bretter zu bohren".

Die Bundeswehr und insbesondere der Organisationsbereich CIR kann und muss aus meiner Sicht hier seinen Beitrag leisten – natürlich immer innerhalb der rechtlichen Grenzen und gesetzlichen Vorgaben.

Der jüngste Organisationsbereich der Bundeswehr steht wie kein anderer für die heutigen Herausforderungen durch hybride Bedrohungen in einem sich rasant verändernden sicherheitspolitischen Umfeld. Digitale Kompetenz und Ausstattung entscheiden über die Zukunftsfähigkeit der Bundeswehr, sie sind essenziell für die Sicherheit Deutschlands. Es ist Führungsaufgabe, die notwendige Transformation zu etablieren und mit Leben zu füllen.

Ich gratuliere und danke allen Angehörigen des Organisationsbereichs zu fünf Jahren CIR! Weiterhin viel Fortune bei der Bewältigung der anstehenden Aufgaben und Herausforderungen!

Ludwig Leinhos
Generalleutnant a. D.



◀ Aufstellung des Kommandos CIR am 5. April 2017 in Bonn.
Foto: Bundeswehr/Marcus Rott

▶ Foto: Ludwig Leinhos

Die Bundeswehr selbst stellt ein hochwertiges Ziel für gegnerische Akteurinnen und Akteure im CIR dar und muss neben täglichen Malware-, Spam- oder Phishing-Attacken jederzeit mit komplexen und professionellen Cyberangriffen rechnen. Sie muss ihre Systeme, in denen Kommunikations- und Informationstechnik (IT) zum Einsatz kommt, schützen – insbesondere die vielfältigen Waffensysteme und das IT-System der gesamten Bundeswehr. .

Foto: Bundeswehr/Sebastian Lehmann

PIZ CIR

TOUR D'HORIZON

FÜNF JAHRE ORGANISATIONSBEREICH CIR

Vor mehr als fünf Jahren wurde der militärische Organisationsbereich Cyber- und Informationsraum aufgestellt, um auf die neuen Bedrohungen und Verwundbarkeiten in einer zunehmend vernetzten Welt auch in der Dimension Cyber- und Informationsraum (CIR) besser, schneller und aus einer Hand reagieren zu können. Damit wurden erstmals alle relevanten Akteure der Bundeswehr in der Dimension CIR unter einem Dach zusammengefasst. Dies geschah nicht nur vor dem Hintergrund bereits bestehender und zukünftiger Herausforderungen sowie Aufgaben, sondern auch im Hinblick auf die Refokussierung auf die Landes- und Bündnisverteidigung.

Bereits in den 2010er Jahren wuchs mit der steigenden Häufigkeit von Hackerangriffen das Bewusstsein, dass diese in einer zunehmend vernetzten Welt weitreichende Folgen für Wirtschaft, Gesellschaft und auch den Staat haben können. Denn oftmals waren auch Betreiber sogenannter kritischer Infrastrukturen, beispielsweise Krankenhäuser, von Cyberattacken betroffen und durch den Ausfall ihrer IT-Systeme zum Teil handlungsunfähig. Auch die Bundeswehr mit ihrer gesamten IT-Infrastruktur stellt ein Ziel für Cyberangriffe dar und muss diese nicht nur betreiben, sondern auch schützen – innerhalb Deutschlands und in den Einsatzgebieten der Bundeswehr.

Als Reaktion hat die Bundesregierung mit der Cybersicherheitsstrategie vom November 2016 einen ressortübergreifenden, strategischen Rahmen geschaffen, um die Cybersicherheit in Deutschland zu verbessern. Die Zuständigkeit dafür ist auf verschiedene Stellen verteilt. Grundsätzlich wird zwischen Cyberabwehr und Cyberverteidigung unterschieden. Die Cyberabwehr liegt in der Verantwortung des Bundesministeriums des Innern, während das Auswärtige Amt für die Cyber-Außenpolitik und internationale Cybersicherheitspolitik zuständig ist. Das Bundesministerium der Verteidigung verantwortet die Cyberverteidigung, die als verfassungsgemäßer Auftrag der Bundeswehr zugewiesen ist.

▲ Vizeadmiral Dr. Thomas Daum, General Eberhard Zorn und Generalleutnant Ludwig Leinhos bei der Übergabe des Kommando Cyber- und Informationsraum im Jahr 2020.
Foto: Bundeswehr/Stefan Uj

Zur Umsetzung dieser Aufgaben wurde im Oktober 2016 die Abteilung Cyber/Informationstechnik (CIT) im Bundesministerium der Verteidigung aufgestellt. Sie plant und steuert nationale und internationale Aktivitäten für den Bereich CIT. Zu ihren Aufgaben gehört es, alle Verteidigungsaspekte gesamtstaatlicher Cybersicherheit entlang der nationalen Cybersicherheitsstrategie zu planen und umzusetzen.

Zusätzlich stellte die damalige Verteidigungsministerin Ursula von der Leyen am 5. April 2017 das Kommando Cyber- und Informationsraum (CIR) mit Generalleutnant Ludwig Leinhos als erstem Inspekteur CIR offiziell in Dienst. Mit der darauffolgenden Unterstellung des Kommandos Informationstechnik der Bundeswehr, des Kommandos Strategische Aufklärung und des Zentrums für Geoinformationen der Bundeswehr im Juli 2017 wurden die Anteile Digitalisierung, IT-Bereitstellung, -Betrieb und -Schutz, Aufklärung und Wirkung, Fähigkeiten der Operativen Kommunikation sowie die Bereitstellung von Geoinformationen im Organisationsbereich CIR zusammengeführt. In weiteren Schritten wurden die Zentren für Cybersicherheit, Cyberoperationen und Softwarekompetenz aufgestellt, um der zunehmenden Digitalisierung der Bundeswehr und den damit verbundenen Herausforderungen, aber auch der wachsenden Bedeutung der spezifischen Fachlichkeiten, zu begegnen. Von anfangs rund 13.500 militärischen und zivilen Angehörigen ist der Organisationsbereich CIR auf aktuell etwa 16.000 Personen aufgewachsen.

DIE DIMENSION CYBER- UND INFORMATIONSRAUM ALS OPERATIONSRAUM

Mit der Aufstellung des Organisationsbereichs CIR wurde der Bedeutung der Dimension CIR für die Bundeswehr organisatorisch Rechnung getragen und mit Kräften hinterlegt. Der Cyber- und Informationsraum ist so zu einem neuen Operationsraum für die Bundeswehr geworden, gleichrangig neben den bisherigen Dimensionen Land, Luft und See sowie dem Weltraum. Dem namensgleichen Organisationsbereich CIR wurde eine umfassende Auftragslage zugeordnet. Er verantwortet alle Aspekte der Dimension CIR – von der Planung und Führung von CIR-Operationen über die Rolle als Enabler anderer Truppenkontingente durch Bereitstellung einsatzbereiter Kräfte bis hin zum Beitrag zur gesamtstaatlichen Cybersicherheit und schließlich der Weiterentwicklung seiner Fähigkeiten.

Ein weiterer wesentlicher Markenkern des Organisationsbereichs CIR ist seine Rolle als Treiber der Digitalisierung für die gesamte Bundeswehr. Er bewertet nicht nur technische Innovationen hinsichtlich ihrer Nutzbarkeit für die Bundeswehr und deckt den Bedarf der Truppe. Vielmehr koordiniert und harmonisiert der Organisationsbereich CIR bestehende Digitalisierungsprojekte der anderen Bereiche der Bundeswehr. Er zeigt weiteren Handlungsbedarf auf und öffnet die Perspektiven für die weitere Digitalisierung der Bundeswehr.

Für das Teilportfolio Cyber/IT ist der Organisationsbereich CIR in planerischer Verantwortung für die gesamte Bundeswehr. Hierfür übernimmt das Kommando CIR die Rolle, die sonst dem Planungsamt der Bundeswehr obliegt. Zu diesem Zweck erfolgt die enge Zusammenarbeit im Clusterdreieck **Kommando CIR/Zentrum Digitalisierung der Bundeswehr** mit dem **Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr** und der **Abteilung Cyber/Informationstechnik (CIT)** des BMVg, bei gleichzeitiger Einbindung der BWI GmbH sowie der übrigen Organisationsbereiche.

BEITRAG ZUR GESAMTSTAATLICHEN SICHERHEIT

Die Bundeswehr selbst stellt ein hochwertiges Ziel für gegnerische Akteurinnen und Akteure im CIR dar und muss neben täglichen Malware-, Spam- oder Phishing-Attacken jederzeit mit komplexen und professionellen Cyberangriffen rechnen. Sie muss ihre Systeme, in denen Kommunikations- und Informationstechnik (IT) zum Einsatz kommt, schützen – insbesondere die vielfältigen Waffensysteme und das IT-System der gesamten Bundeswehr. Diese Aufgabe übernimmt das Zentrum für Cyber-Sicherheit der Bundeswehr. Seine Exper-

tinnen und Experten gewährleisten 24/7 einen umfassenden Schutz der IT-Systeme und -Services der Bundeswehr.

Doch der Organisationsbereich CIR schützt nicht nur die Systeme der Bundeswehr, er leistet auch einen Beitrag zur gesamtstaatlichen Sicherheit. Das Kommando CIR trägt zu einem gesamtstaatlichen Lagebild bei. Aus Lagen und Analysen eigener und anderer Dienststellen, Fachbereiche, Organisationsbereiche und Ressorts erstellt es ein korreliertes Lagebild CIR. Dieses unterstützt die Entscheidungsfindung des Inspekteurs CIR für eigene Maßnahmen zur Sicherung der Informationsversorgung und der Führungsfähigkeit. Im Rahmen der gesetzlichen Möglichkeiten werden im Nationalen Cyber-Abwehrzentrum (Cyber-AZ) – in Zusammenarbeit mit anderen Bundesbehörden – Informationen aus relevanten Lagebildern geteilt, bewertet und den Entscheidungsträgern Handlungsoptionen aufbereitet. Bereits seit Anfang des Jahres 2019 ist das Kommando CIR mit mindestens einem Vertreter permanent vor Ort. Zudem stellt das Kommando einen stellvertretenden Koordinator im Cyber-AZ.

HERAUSFORDERUNGEN DER LETZTEN JAHRE

Der Ausbruch der Corona-Pandemie und der darauffolgende Lockdown im März 2020 stellten die Bundeswehr vor besondere Herausforderungen. Schnell etablierten sich Telearbeit und mobiles Arbeiten im Homeoffice, wofür durch den Organisationsbereich CIR schnell die Voraussetzungen geschaffen wurden – im Zusammenwirken mit anderen Bereichen der Bundeswehr, der BWI GmbH, dem Bundesamt für Sicherheit in der Informationstechnik und dem Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr. So konnte zum Schutz der Mitarbeitenden der Präsenzbetrieb vielerorts zügig heruntergefahren werden. Dennoch wurden viele Projekte ohne erkennbaren Qualitätsverlust weiter vorangetrieben. Die Nutzung von Kollaborationstools, Video- und Telefonkonferenzen sind mittlerweile arbeitstäglicher Standard der ortsunabhängigen Abstimmung und Zusammenarbeit geworden. Ende März 2020 nahm die Operationszentrale Corona im Kommando CIR ihre Arbeit auf. Neben der Unterstützung der Corona-Hotels zur isolierten Unterbringung von Einsatzsoldatinnen und -soldaten gab es vielseitige Einsätze im Rahmen der Corona-Amtshilfe, zum Beispiel in Krankenhäusern, Seniorenzentren, Gesundheitsämtern und ab 2021 zusätzlich in den Impfzentren. Auch im Jahr 2022 beeinflusste Corona das Arbeiten im Organisationsbereich. Die während der Pandemie erprobte und etablierte Möglichkeit von Homeoffice ermöglicht einen Dienstbetrieb in „maximaler Auflockerung", wann immer nötig.

Auch die Flutkatastrophe im Westen Deutschlands im Juli 2021 forderte die Bundeswehr außerhalb des originären militärischen Auftrags. Die Folgen der Flut betrafen den Organisationsbereich CIR stark. Zunächst infrastrukturell, weil sich eigene Liegenschaften im Zentrum des Hochwassergebietes befanden, etwa in Euskirchen, Rheinbach oder Bad Neuenahr. Zudem waren über 500 Angehörige des Organisationsbereichs durch überflutete Wohnungen oder Autos bis hin zum Totalverlust direkt betroffen. Bis Ende November 2021 waren Truppenteile bei den Sofort- und Amtshilfen im Einsatz, entweder mit „Helfenden Händen", aber auch durch Einbringen ganz spezifischer Fähigkeiten des Organisationsbereichs CIR, zum Beispiel die Verfügbarmachung von Kartenmaterial, Geo-Gutachten, Luftbildern sowie moderner Kommunikationstechnik wie SatCom und Tetrapol.

NRF-Übung des IT-Bataillons 282: Reicht die Reichweite des Funksystems Tetrapol für das gesamte Gebiet aus?
Foto: Bundeswehr/Stefan Uj

SDoT
COMP_LAND

Die taktische Cross Domain Lösung.

COMP-LAND ermöglicht unidirektionalen Datentransfer oder bi-direktionalen Austausch und Filterung von strukturierten Daten in Fahrzeugen unter extremen Umweltbedingungen

Mehr Informationen.

Cybersecurity & Cross-Domain-Lösungen für Militär und Behörden seit 1974
www.infodas.de • +49 221 70912-0 • vertrieb@infodas.de

infodas
connect more. be secure.

LANDES- UND BÜNDNISVERTEIDIGUNG – ORGANISATIONSBEREICH CIR UNTERSTÜTZT NRF UND VJTF

In diesem Jahr begann das „Stand-up"-Jahr für die NATO Response Force (NRF), die schnelle Eingreiftruppe der NATO. In einem Konfliktfall kann sie rasch weltweit verlegen und leistet so einen wichtigen Beitrag zur Abschreckung im Rahmen der Landes- und Bündnisverteidigung. Deutschland ist für die Jahre 2022-2024 verantwortliche Rahmennation und wesentlicher Truppensteller, auch für die Very High Readiness Joint Task Force (VJTF) 2023. Mit einer festgelegten Vorbereitungszeit könnte ein Einsatz der Soldatinnen und Soldaten aus dem Organisationsbereich CIR zur Verstärkung der NRF/VJTF jederzeit möglich sein. Das gilt für die abzustellenden Elemente der IT-Bataillone genauso wie für die aus allen EloKa-Verbänden des Organisationsbereichs CIR zusammengestellte Task Force Elektronischer Kampf sowie für die Elemente der Operativen Kommunikation und der modularen Geoinformationsfähigkeiten. Dabei ist klar, dass kein Einsatz ohne vom Organisationsbereich CIR bereitgestellte Kräfte und Fähigkeiten möglich ist.

AUF DEM WEG ZU CIR 2.0

Der Organisationsbereich CIR hat sich in den vergangenen fünf Jahren permanent verändert und dabei stetig sein Profil geschärft. Zeitgleich sind in den letzten Jahren die Anforderungen und die Auftragslage an ihn stetig gestiegen. Unter diesen Bedingungen wurde bereits im Zeitraum 2019 bis 2020 eine Strukturanalyse des gesamten Organisationsbereichs durchgeführt mit dem Ziel, die Effizienz unter den gegebenen Voraussetzungen zu erhöhen und dadurch Ressourcen freizusetzen, um diese in zu priorisierende Aufgaben zu reinvestieren. Im August 2021 hat das Kommando CIR seine Arbeitsstruktur auf dem Weg zu „CIR 2.0", der Neustrukturierung des Organisationsbereichs, eingenommen. Gleichzeitig wurde das Zentrum Digitalisierung der Bundeswehr und Fähigkeitsentwicklung Cyber- und Informationsraum (ZDigBw), zum 1. Oktober 2022 aufgestellt.

Die bis zum Jahr 2025 angelegte Neuausrichtung „CIR 2.0" wird den gesamten Organisationsbereich CIR umfassen. Für den Organisationsbereich ist dieses Projekt und die damit einhergehende Anpassungsfähigkeit Voraussetzung für die Bewältigung aktueller und zukünftiger Herausforderungen. Das Gelingen erfordert von allen Angehörigen, nicht nur offen für Veränderungen zu sein, sondern diese auch als Chance zu verstehen und an deren Ausgestaltung aktiv mitzuwirken.

▲ Die bis zum Jahr 2025 angelegte Neuausrichtung „CIR 2.0" wird den gesamten Organisationsbereich CIR umfassen.
Foto: Bundeswehr/Broschinsky

▼ Mit einer festgelegten Vorbereitungszeit könnte ein Einsatz der Soldatinnen und Soldaten aus dem Organisationsbereich CIR zur Verstärkung der NRF/VJTF jederzeit möglich sein.
Foto: Bundeswehr/Stefan Uj

DIENSTSTELLEN-PROFIL

BATAILLON ELEKTRONISCHE KAMPFFÜHRUNG 911

Das nördlichste Bataillon Deutschlands klärt 24/7 auf und verfügt über mobile EloKa Kräfte.

AUFGABEN

- Weltweite signalerfassende Aufklärung 24/7 und 365 Tage im Jahr aus der Aufklärungsstellung Bramstedtlund.
- Vier mobile EloKa-Kompanien zur Unterstützung des Heeres und für Auslandseinsätze.
- Betrieb einer Ausbildungswerkstatt für angehende Elektronikerinnen und Elektroniker.

AUFTRAG

Das Bataillon Elektronische Kampfführung 911 (EloKaBtl 911) ist ein teilmobiler Verband der Fernmeldeaufklärung der Bundeswehr. Der Verband besteht aus zwei Komponenten: der mobilen landgestützten und der ortsfesten signalerfassenden Aufklärung. Die vier mobilen EloKa-Kompanien verfügen über spezielle Aufklärungssysteme zur Unterstützung des Heeres in der Landes- und Bündnisverteidigung sowie für Auslandseinsätze im Rahmen des internationalen Krisenmanagements. Die mobilen EloKa-Kompanien können hierzu bei Bedarf einem taktischen Bedarfsträger, zum Beispiel einer Brigade des Heeres, unterstellt werden. Die hochmobilen Aufklärungssysteme befähigen die Kompanien auch zur Aufklärung im hochintensiven Gefecht. Zudem können mit Störsystemen gegnerische Funkausstrahlungen gestört sowie fernausgelöste Sprengfallen unterdrückt werden.

In der ortsfesten Aufklärungsstellung Bramstedtlund werden elektromagnetische Ausstrahlungen rund um die Uhr aufgeklärt und ausgewertet. Die so gewonnenen Aufklärungsergebnisse werden den Bedarfsträgern im System Militärisches Nachrichtenwesen zur Verfügung gestellt und fließen in das Lagebild der militärischen und politischen Führung ein. Die Fernmeldeaufklärungszentrale umfasst sowohl militärische als auch zivile Dienstposten.

Im Rahmen von strukturellen Änderungen des Projekts CIR 2.0 wird der ortsfeste Anteil zum 1. April 2023 ausgegliedert und als eine eigenständige Dienststelle Fernmeldeaufklärungszentrale Nord aufgestellt.

ANSCHRIFT
Südtondern-Kaserne,
Am Tannenberg 1,
25917 Stadum

DIENSTSTELLENLEITUNG
Fregattenkapitän Marcus Gegner

STAMMPERSONAL
~1.020

AUFSTELLUNG
01.04.2013

FREGATTENKAPITÄN ANNE MALUCHA,
STABSOFFIZIER FÜR VERÄNDERUNGSMANAGEMENT IM PROJEKT CIR 2.0

CIR 2.0

Auf dem Weg in eine moderne Organisations- und Führungskultur

Der Organisationsbereich Cyber- und Informationsraum (CIR) befindet sich inmitten grundlegender Veränderungen. Unter dem Projekttitel „CIR 2.0 – Gemeinsam die Dimension gestalten" strukturiert sich der Organisationsbereich komplett neu. Dahinter steht das Ziel, die vorhandenen Ressourcen besser zu nutzen. Dafür müssen Hierarchien flacher und Querschnittsaufgaben gebündelt werden. Das erfordert Anpassungen in der Organisations- und Führungskultur. Denn klar ist schon jetzt: Innovationen, Veränderungen und Anpassungsfähigkeit sind gerade in der Dimension CIR eine ständige Herausforderung, um Wirküberlegenheit erreichen zu können.

Um in einem hochkomplexen dynamischen Umfeld auf die Verwundbarkeit unseres Staates in einer weitreichend vernetzten Welt im Cyber- und Informationsraum als eigenen Operationsraum reagieren zu können, wurde der Organisationsbereich CIR 2017 aufgestellt. Damit der Betrieb und die Arbeitsfähigkeit in allen Bereichen schnell sichergestellt waren, wurden bestehende Strukturen nahezu unverändert übernommen. Damit einhergehend blieb zum Teil das Denken und Handeln in bestehenden Strukturen (Silodenken) stecken und war meist geprägt von der Konzentration auf die eigene Fachlichkeit.

AUSRICHTUNG AUF LANDES- UND BÜNDNISVERTEIDIGUNG

Bereits kurz nach Aufstellung unseres Organisationsbereichs wurden mit der Übertragung neuer zusätzlicher Aufgabenbereiche und einer grundsätzlichen Neuausrichtung der Bundeswehr in Richtung Landes- und Bündnisverteidigung (LV/BV) wesentliche Rahmenbedingungen geändert. Eine sachgerechte Aufgabenerfüllung erschien vor diesem Hintergrund nur schwer möglich. Daher wurde in den Jahren 2019/2020 eine interne Strukturanalyse durchgeführt, um Optimierungsmöglichkeiten und Ressourcenfreiräume zu identifizieren, damit der bestehende Auftrag sowie weitere zukünftige Aufgaben mit vorhandenem Personal erfüllt werden können.

Zu viele Entscheidungs- und Bewertungsebenen, Silodenken, wenig Agilität, ein fehlender Fokus auf die Digitalisierung der Bundeswehr und eine zu starre Ausbildungsorganisation, die nach Fachlichkeiten getrennt ist und damit der Mindset-Bildung für die Dimension CIR entgegenwirkt: der Optimierungsbedarf wurde durch die Strukturanalyse sehr deutlich aufgezeigt. Daraus abgeleitet wurde der Organisationsbereich CIR grundlegend neu strukturiert. Das Ergebnis – die neue Grobstruktur – wurde im April 2021 durch die damalige Bundesministerin der Verteidigung, Annegret Kramp-Karrenbauer, gebilligt.

CIR 2.0 – MEHR ALS NUR EINE NEUE STRUKTUR

Die Maxime aller strukturellen Überlegungen ist das Ziel, Bewertungs- und Entscheidungskompetenz an jeweils nur einer Stelle im Organisationsbereich auszubringen und damit die konsequente Nutzung einer Matrixorganisation zur Wahrnehmung aller fachlichen und operativen Führungsaufgaben. Die Zwei-Sterne-Kommandos Kommando Strategische Aufklärung und Kommando Informationstechnik der Bundeswehr werden hierfür aufgelöst. Dadurch werden Schnittstellen minimiert und Querschnittsaufgaben gebündelt. Somit freifallende Dienstposten werden in die Fachlichkeit reinvestiert.

CIR-OPERATIONEN AUS EINER HAND UND TREIBER DER DIGITALISIERUNG

Alle CIR-Kräfte werden damit zukünftig direkt aus dem Kommando CIR geführt – CIR-Operationen aus einer Hand. Gleiches gilt für den zweiten Auftragsschwerpunkt, Treiber der Digitalisierung für die Bundeswehr zu sein. Das Herz der Digitalisierung der Bundeswehr schlägt in unserem Organisationsbereich. Alle dem Kommando CIR nachgeordneten Dienststellen bilden die Durchführungsebene. Mit der Aufstellung des Zentrums Digitalisierung der Bundeswehr und Fähigkeitsentwicklung CIR (ZDigBw) bündeln wir alle Digi-

talisierungskompetenzen an einer Stelle. Über die bisherige Zusammenarbeit hinaus wird mit der BWI eine strategische Partnerschaft aufgebaut. So wird CIR zum zentralen Kompetenzträger für alle Digitalisierungsthemen in der Bundeswehr.

MODERNE ORGANISATIONS- UND FÜHRUNGSKULTUR – VERTRAUEN UND ZUSAMMENARBEIT AUF AUGENHÖHE

Diese Neustrukturierung erfordert ein konsequentes Umdenken. Im Rahmen dieser Veränderungen wurden und werden die Kameradinnen und Kameraden sowie zivilen Mitarbeiterinnen und Mitarbeiter des Organisationsbereichs CIR besonders gefordert. Denn die neue Grobstruktur beinhaltet nicht nur eine veränderte Aufbauorganisation. Die dahinterstehenden Prozesse sind letztlich von den Menschen des Organisationsbereichs mit Leben zu füllen. Dies ist eine große Herausforderung, aber auch eine große Chance. Hier wird den Expertinnen und Experten der Dimension CIR Gestaltungsspielraum ermöglicht. Das ist der Weg hin zu einer modernen Organisationskultur.

Aber gerade auch die Führungskultur muss zukunftsweisend sein. Um sich von Hierarchie- und Silodenken zu lösen und den Organisationsbereich CIR in agilen Strukturen unter moderner Führung weiterzuentwickeln, sind die Führungskräfte in besonderem Maße gefragt. Denn sie definieren die Schlüsselerfolgsfaktoren der Organisations- und Führungskultur und sie müssen die gemeinsame Vision CIR 2.0 erarbeiten und für alle verständlich machen. Gemeinsam mit dem Zentrum Innere Führung hat sich die Führungsspitze des Organisationsbereichs dazu auf den Weg gemacht und den Prozess des Neudenkens angestoßen.

Das Vertrauen in die Expertise des anvertrauten Personals spielt eine sehr wichtige Rolle im Führungsprozess. Eine moderne Organisation kann es sich nicht leisten, mit jedem Vorgang auf der Hierarchieleiter hoch und runter zu klettern und so wertvolle Zeit zu verlieren. Bezogen auf das Kommando CIR liegt die fachliche Kompetenz in den Referaten. Und genau dort muss bewertet werden, welche Vorgänge an die Führung des Kommandos zur Entscheidung gebracht werden müssen. Nur so ist eine höhere Geschwindigkeit zu erreichen und – trotz notwendiger Hierarchie – eine Begegnung auf Augenhöhe möglich. Das bewährte Prinzip des Führens mit Auftrag wird im Organisationsbereich CIR deutlich gestärkt und muss einhergehen mit gelebter Fehler- und Feedbackkultur.

PROZESS DER KULTURENTWICKLUNG

Kultur kann man nicht befehlen. Diese muss entwickelt, gelebt und vor allem weiterentwickelt werden. Der jüngste Organisationsbereich der Bundeswehr steht hier noch am Anfang. Nach nur fünf Jahren des Bestehens ist er in einem umfangreichen Veränderungsprozess, der auch für Unruhe sorgt.

Grafik: Bundeswehr/KdoCIR

▲ Truppenfahnen beim Übergabeappell Kommando Informationstechnik der Bundeswehr und Informationstechniktruppen.
Foto: PIZ CIR/Martina Pump

◀ Grafik: Bundeswehr/KdoCIR

CIR 2.0
GEMEINSAM DIE DIMENSION GESTALTEN

Daher ist der Austausch von Entwicklungen, Erwartungen und Forderungen mit dem Personal besonders wichtig. Ein Baustein hierzu ist die sogenannte CIR 2.0-Reise, in der jede Dienststelle des Organisationsbereichs CIR vom Inspekteur Vizeadmiral Dr. Daum oder dem Projektleiter und Chef des Stabes Konteradmiral Obersteg besucht wurde, um dort mit Personal aller Ebenen ins Gespräch zu kommen. In einem nächsten Schritt wird die Kulturentwicklung in den Fokus genommen. Was versteht man unter CIR? Was zeichnet CIR aus? Was ist das Gemeinsame und wie will man sein? Diese Fragen können nur die Menschen des Organisationsbereichs selbst beantworten und nur sie können treibende Kraft des Kulturwandels sein. Ein dazu notwendiger partizipativer Ansatz wird momentan entwickelt und ausgeplant. Um dem Slogan „Gemeinsam die Dimension gestalten" gerecht zu werden, werden Status- und Dienstgradgruppen aller Ebenen gehört. Denn CIR-Operationen aus einer Hand kann man nur mit Menschen erfolgreich führen. Und Treiber der Digitalisierung ist man nur, wenn Innovationen erkannt, Veränderungen gestaltet und Anpassungsfähigkeit bewiesen wird.

CIR 2.0 ist herausfordernd. Die Last der Veränderungsgestaltung muss auf viele Schultern verteilt werden. Die Fachleute brauchen den Freiraum, ihre Prozesse selbst mitzuentwickeln und zu gestalten. Dem Anspruch, ein moderner und zukunftsorientierter Organisationsbereich zu sein, wird nur gerecht, wer flexibel, agil und veränderungsbereit ist.

DIENSTSTELLEN-PROFIL

BATAILLON ELEKTRONISCHE KAMPFFÜHRUNG 912

„Wir sind EloKa! Zu Wasser, in der Luft und an Land. Aufklärung in jeder Dimension!“

AUFGABEN

- Auf See! Wir besetzen die Flottendienstboote mit EloKa-Fachpersonal und klären weltweit von See auf.
- Aus der Luft! Wir unterstützen die Luftwaffe in ihrer Operationsführung durch Erkenntnisse zu Luftfahrzeugen.
- Zu Land! Wir klären das elektromagnetische Spektrum auf. Und zwar mobil und unabhängig.

AUFTRAG

Das Bataillon für Elektronische Kampfführung 912 (EloKaBtl912) ist mit einem vielfältigen Auftrag zur Unterstützung der Dimensionen Land, Luft und See ausgestattet. In vier Kompanien werden Erkenntnisse gesammelt, ausgewertet und für die Bedarfsträger aufbereitet. Zeitgleich wird in einer weiteren Kompanie der soldatische Nachwuchs inklusive der Offizieranwärterinnen und -anwärter des Organisationsbereichs CIR ausgebildet und auf diesen geprägt. In der Dimension See stellen die EloKa-Spezialistinnen und Spezialisten des Verbandes in Bordeinsatzteams auf Flottendienstbooten der Marine die seegestützte signalerfassende Aufklärung sicher. Weiterhin unterstützen die Aufklärer des Bataillons Luftwaffenoperationen in ganz Europa sowie leisten in der Dimension Land einen wichtigen Beitrag zu Very Joint High Readiness Task Force (VJTF). Die gewonnenen Erkenntnisse laufen zusammen, werden ausgewertet und vervollständigen Lagebilder für die politische und militärische Führung. Viele Angehörige des Bataillons waren und sind in ungezählten Einsätzen weltweit unterwegs, um ihre Expertise und ihr Fachwissen als Beitrag zur Friedenssicherung einzubringen.

ANSCHRIFT
Clausewitz-Kaserne,
Am Rehagen 10,
31582 Nienburg

DIENSTSTELLENLEITUNG
Oberstleutnant Marcus Sarnoch

STAMMPERSONAL
~650

AUFSTELLUNG
17.09.2003

Aufklären im Gefecht: Das EloKa Bataillon 911 bereitet sich auf die Landes- und Bündnisverteidigung vor.
Foto: Bundeswehr/Broschinsky

BRIGADEGENERAL ARMIN FLEISCHMANN,
WAR BIS 30. SEPTEMBER 2022 „LEITER AUFBAUSTAB ZENTRUM DIGITALISIERUNG“ UND
HAT DIE ROLLE „ZUKÜNFTIG KOMMANDEUR ZENTRUM DIGITALISIERUNG“ WAHRGENOMMEN.
AB 1. OKTOBER 2022 BUNDESMINISTERIUM DER VERTEIDIGUNG, UNTERABTEILUNGSLEITER CIT I.

Das Zentrum Digitalisierung der Bundeswehr und Fähigkeitsentwicklung Cyber- und Informationsraum – ***„Unser Beitrag als Treiber der Digitalisierung der Bundeswehr“***

Die digitale Transformation unserer Gesellschaft, der privaten Wirtschaft und der öffentlichen Verwaltung bleibt weiterhin eines der bestimmenden Zukunftsthemen und steht gleichsam als Garant für moderne Leistungs- und Wettbewerbsfähigkeit. Digitalisierung fordert Staat und Gesellschaft auf vielen Ebenen heraus. Je mehr Vorgänge digitalisiert und Systeme vernetzt werden, umso mehr Nahtstellen entstehen zwischen verschiedenen Akteuren. Eine einsatzorientierte Bundeswehr muss die Digitalisierung für ihre täglichen Prozesse, vor allem aber für ihre Kernaufträge in der Landes- und Bündnisverteidigung (LV/BV), kontinuierlich und effizient voranbringen sowie zielgerichtet nutzen. Digitalisierung ist kein Selbstläufer, deshalb hat sich der Organisationsbereich Cyber- und Informationsraum (CIR) in seiner Neuausrichtung „CIR 2.0“ das Ziel gesetzt, „Treiber der Digitalisierung der Bundeswehr“ zu sein. Das „Waffensystem“ dafür wird das Engagement und die Begeisterung der Menschen sein, die im Zentrum Digitalisierung der Bundeswehr und Fähigkeitsentwicklung Cyber- und Informationsraum – kurz: Zentrum Digitalisierung – in Bonn, Euskirchen und weiteren fünf Außenstellen ab Oktober 2022 ihren Dienst leisten werden. Dieser Beitrag stellt das neue Zentrum mit seiner Kernaufgabe „Digitalisierung“ des Organisationsbereichs CIR und der Bundeswehr vor.

DIE ZENTRALE ROLLE DES ZENTRUMS DIGITALISIERUNG IM WIRKVERBUND DER DIGITALISIERUNG DER BUNDESWEHR

Auch um die Digitalisierung in der Bundeswehr zu stärken, wurde der militärische Organisationsbereich CIR eingerichtet. Seit der Aufstellung 2017 und dem Auf- und Ausbau der Strukturen entwickelt sich dieser innovative, moderne und agile Organisationsbereich konsequent weiter. Sein Markenkern besteht aus dem Auftrag „Wahrnehmung der Dimensionsverantwortung im Rahmen von CIR-Operationen aus einer Hand“ und der Aufgabe als „Treiber der Digitalisierung der Bundeswehr“, verbunden mit der „Fähigkeitsentwicklung im CIR“.

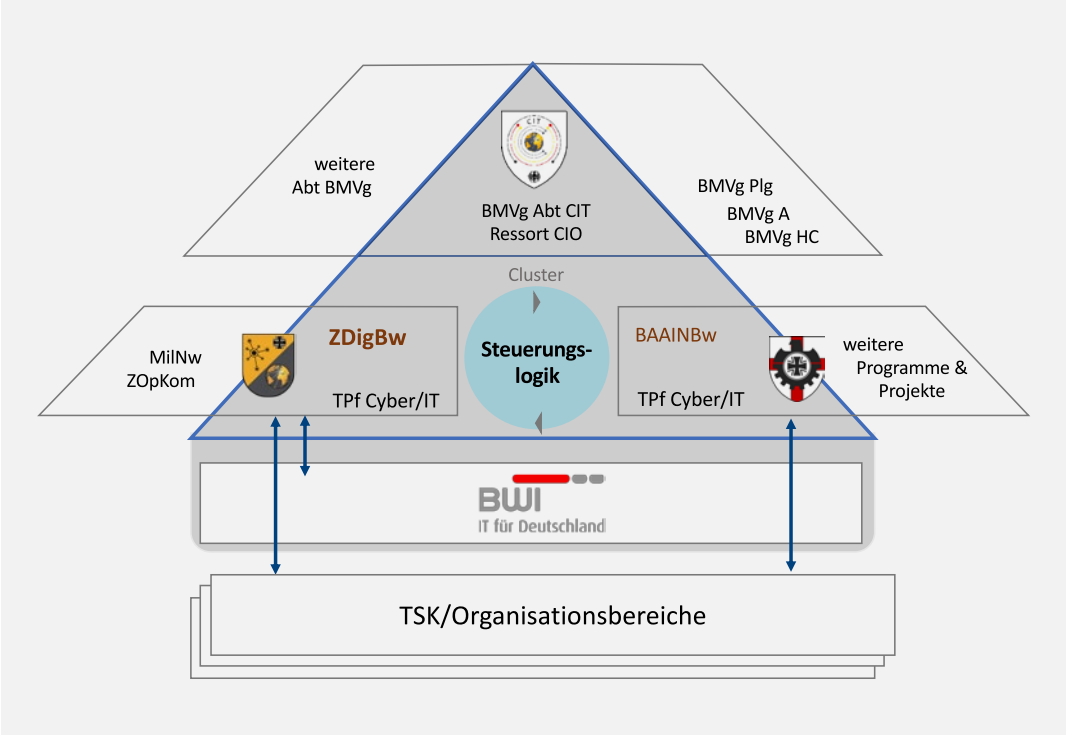
Der militärische Organisationsbereich CIR tritt dabei als zentraler Bedarfsträger der Bundeswehr für das Teilportfolio „Cyber und Informationstechnik“ (CIT) auf und agiert für diesen Bereich komplementär zum Planungsamt der Bundeswehr. Im Kern wird die Digitalisierung dabei durch zwei Säulen vorangetrieben.

Dies geschieht zunächst durch den Aufbau einer zentralen Digitalisierungsplattform für den Geschäftsbereich des Bundesministeriums der Verteidigung (GB BMVg). Dieser aus der verzahnten Aufstellung und Zusammenarbeit bestehende Wirkverbund verfolgt eine durchgängige, ebenenübergreifende Steuerungslogik zum Realisieren und Betreiben von IT-Services. Er besteht aus den Clusterreferaten der Abteilung Cyber/Informationstechnik im BMVg (ministerielle Fachaufsicht), den Kompetenzzentren des Zentrums Digitalisierung und den dazugehörigen Programmen und Projekten im Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAAINBw).

Die zweite Säule setzt sich zusammen aus der umfassenden Beratung, fachlichen Anleitung und Unterstützung der gesamten Bundeswehr bei der Planung und Realisierung von Digitalisierungsprojekten durch das Zentrum Digitalisierung auf Basis der vorgenannten Plattform.

Ziel der Plattform ist es, die Vielfalt von IT-Systemen zu harmonisieren, die Interoperabilität zu verbessern, die Datenübertragungskapazitäten zu erhöhen, Finanzbedarfe zu reduzieren, die Projektrealisierung zu beschleunigen, die Qualität zu sichern und den Betrieb zu vereinfachen, um damit die Digitalisierung in allen Bereichen zukunftsorientiert zur Wirkung zu bringen.

Die Digitalisierungsplattform wird zukünftig modular aufgebaute, wiederverwendbare, skalierbare, leicht und schnell adaptierbare sowie nach einem einheitlichen Regelwerk aufgebaute IT-Services zur Verfügung stellen. Diese sind aufgestellt nach den IT-Servicegruppen in neun funktionalen Clustern – angelehnt an die NATO C3 Taxonomie.



◀ Der Wirkverbund der Digitalisierungsplattform Geschäftsbereich Bundesministerium der Verteidigung.

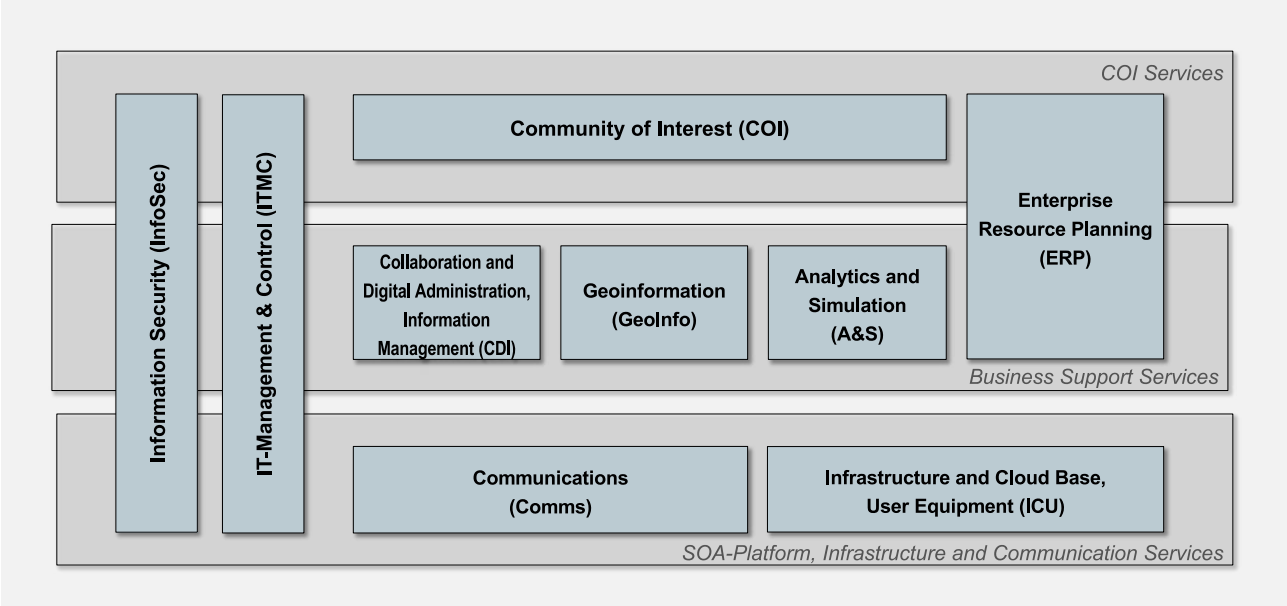
▼ Die neun Cluster der Digitalisierungsplattform Geschäftsbereich Bundesministerium der Verteidigung.

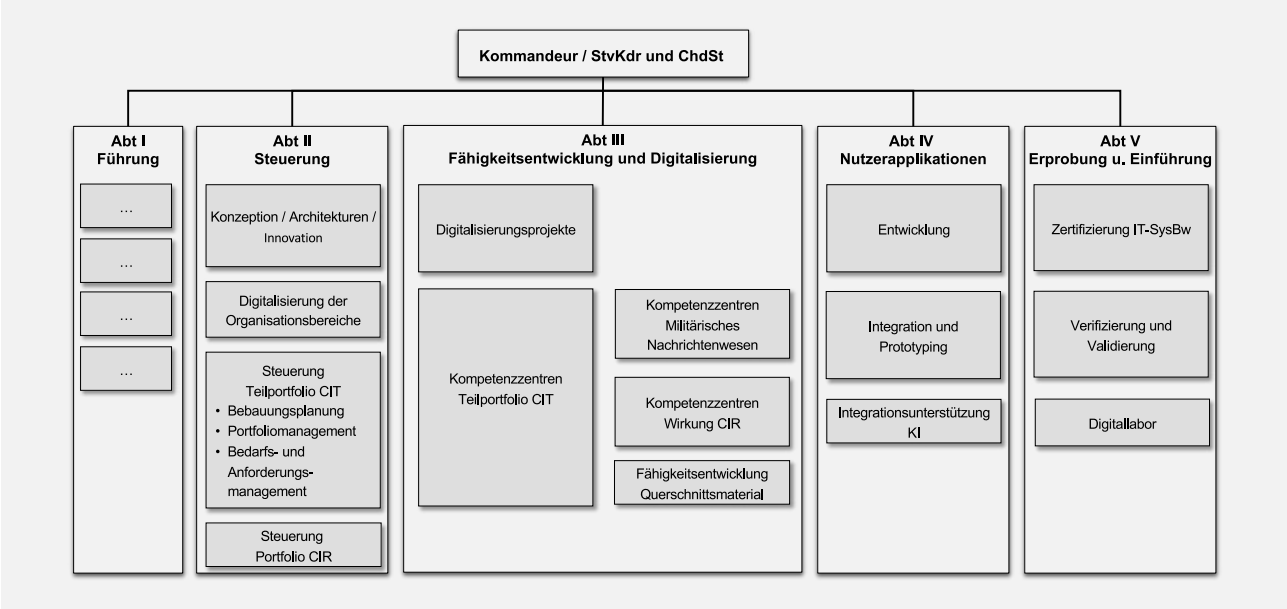
Grafik: BMVg CIT

Damit entsteht zunehmend ein „IT-Baukastensystem", das dem Nutzer, Operateur oder Organisationsbereich zur Wahrnehmung seines Auftrags angeboten werden kann. Jedes dieser Cluster entwickelt dedizierte IT-Services seines Verantwortungsbereiches und stellt diese dann anderen Clustern, komplexeren Digitalisierungsprojekten oder neuen Projekten zur Verfügung. In der Struktur des Zentrums Digitalisierung wurden – der Steuerungslogik folgend – hierfür neun kongruente Kompetenzzentren ausgeplant.

Digitalisierungsprojekte stellen dem Nutzer Lösungen zur Verfügung, die im Idealfall vollständig aus Komponenten der Plattform zusammengestellt werden können. Finden sich fehlende funktionale Elemente, für die ein nachgewiesener Bedarf besteht, werden diese harmonisiert, migriert oder (weiter-)entwickelt. Finden sich Elemente „Off-the-shelf" – am Markt verfügbar –, werden sie zugekauft. Diese Komponenten gilt es im Anschluss zu integrieren und als Element in die Digitalisierungsplattform zu überführen. Die Digitalisierungsbedarfe im Geschäftsbereich BMVg frühzeitig zu erfassen, zu bewerten, zu steuern und zu leistungsfähigen IT-Services im IT-System der Bundeswehr zusammenzustellen, ist eine Kernkompetenz des Zentrums Digitalisierung.

Neben den genannten Kernaufgaben wird das Zentrum als „Trusted Advisor" eine Rolle bei der Aufnahme neuer IT-Services und Technologien bieten. Zukunftsthemen wie Cloud, Künstliche Intelligenz (KI) oder Virtual Reality werden im Zentrum aufgenommen und mit anderen Organisationsbereichen auf Verwendbarkeit geprüft. Eine nicht unbedeutende Rolle





▲ Gliederung des Zentrums Digitalisierung.
Grafik: BMVg CIT

▶ Brigadegeneral Armin Fleischmann.
Foto: Bundeswehr / PIZ CIR

kommt dem Zentrum bei der Begutachtung der Anwendung und Umsetzung der digitalen Souveränität zu. Daten aus den unterschiedlichsten Quellen, mit denen interoperiert und Entscheidungen getroffen werden können, stellen eine wichtige Funktion der Cloud-Lösungen dar. Die Bundeswehr sollte zukünftig bei Multi-Domain-Operationen (siehe auch Seite 138) eine Combat-Cloud als Grundlage haben, um relevante Informationen zur richtigen Zeit zur Verfügung zu stellen und die Durchführung von Operationen mit hochintegrierter IT für oder in Waffensystemen zu ermöglichen.

Wesentlich ist der Fokus auf die durchgehende, leistungsfähige und interoperable Führungsfähigkeit von der strategischen bis zur untersten taktischen Ebene.

Um all dies zu erreichen, wird das Zentrum Digitalisierung als „Steuerungselement" in der Bundeswehr gebraucht.

HAUPTAUFGABEN, STRUKTUREN UND RESSOURCEN DES ZENTRUMS DIGITALISIERUNG

Zur Umsetzung der vorgenannten Absicht hat der Organisationsbereich CIR zum 1. Oktober 2022 das „Zentrum Digitalisierung Bundeswehr und Fähigkeitsentwicklung Cyber- und Informationsraum" mit der Masse der Kräfte in Bonn und Euskirchen sowie den Standorten Munster, Berlin, Dresden, München und Amersfoort in den Niederlanden aufgestellt. Das Zentrum Digitalisierung geht aus dem Großteil der bisherigen Abteilung Planung des Kommandos CIR in Bonn und dem Zentrum Softwarekompetenz der Bundeswehr in Euskirchen hervor und soll die bisherigen sowie neue, zusätzliche Rollen und Aufgaben wahrnehmen. Im Wesentlichen sind dies neben der Fähigkeitsentwicklung CIR die Rolle als Bedarfsträger für das Teilportfolio Cyber/IT sowie die Rolle als „Treiber der Digitalisierung der Bundeswehr".

Aufbauend auf den bisherigen Erfahrungen aus der Arbeit der Abteilung Planung im Kommando CIR wurde die Struktur des Zentrums Digitalisierung unter Beantwortung der Leitfrage ausgeplant: „Wie ist das Zentrum Digitalisierung zu gestalten, um die Kernaufgaben mit dem größtmöglichen Mehrwert für die Bundeswehr wahrzunehmen?".

Insbesondere mit Blick auf die zahlreichen Akteure in den relevanten Prozessen und Zusammenarbeitsbeziehungen bedeutete dies, interaktionsfähige und agile Strukturelemente innerhalb flacher Hierarchien auszubringen.

Damit das neue Zentrum nicht ausschließlich vom Reißbrett entsteht, wurde bereits im August 2021 eine kombinierte Arbeits- und Projektgliederung eingenommen, die sich eng an der geplanten Zielstruktur orientierte. Dies ermöglichte das frühzeitige Etablieren von internen Abläufen, das Aufnehmen und Einspielen externer Arbeitsbeziehungen und – ganz entscheidend – die kontinuierliche Feinjustierung der einzunehmenden Zielstruktur auf Grundlage gemachter Erfahrung.

WIE IST DAS NEUE ZENTRUM AUFGESTELLT?

Geführt wird das Zentrum Digitalisierung mit seinen über 700 Mitarbeiterinnen und Mitarbeitern als Ein-Sterne-Kommando aus Bonn heraus. Neben der Sicherstellung der Führung durch die Abbildung der Führungsgrundgebiete in der Abteilung I verfügt das Zentrum über vier Fachabteilungen.

Abteilung II – Steuerung: Diese Abteilung verantwortet die Erstellung der konzeptionellen Grundlagen für die Fähigkeitsentwicklung CIR und die Digitalisierung der Bundeswehr. Mit Blick auf die Digitalisierung bewertet, ordnet und priorisiert sie die im Geschäftsbereich artikulierten Bedarfe zur Planung, Realisierung und Nutzung von IT-Services im Rahmen der Digitalisierungsplattform. Dazu wird in der Abteilung II innovativ die Expertise zur Digitalisierungsunterstützung der anderen Dimensionen (Land, Luft/Weltraum, See) eingebunden sowie die digitale Zusammenarbeit mit den zivilen Organisationsbereichen und NATO/EU sichergestellt.

Die Abteilung bindet ebenso die vielfältigen Innovationselemente außerhalb des Organisationsbereichs CIR ein. Durch

Nutzung der Innovationskraft (siehe auch Seite 42) des Cyber Innovation Hub, der universitären Forschung, zum Beispiel im Forschungsinstitut CODE der Universität der Bundeswehr München, sowie der Berücksichtigung disruptiver Innovation durch die Cyberagentur und weiterer Akteure, wird das Tempo der technologischen Entwicklung für die Bundeswehr aufgenommen. So wird sichergestellt, dass digitale Innovationen aus Forschung, Wissenschaft und Industrie Eingang in die Digitalisierung der Bundeswehr finden können. Die Abteilung strukturiert und priorisiert die Digitalisierungsbedarfe sowie deren „Abbildung" auf die Bundeswehr („Wer braucht was und wann in welcher Qualität und Quantität?"). Die Ergebnisse dieser Arbeit werden zur Umsetzung an die anderen Fachabteilungen übergeben.

Abteilung III – Digitalisierung und Fähigkeitsentwicklung: Diese Abteilung entwickelt entlang der Priorisierung die Fähigkeiten des Organisationsbereichs CIR und den weiteren Aufbau der Digitalisierungsplattform der Bundeswehr weiter. Dazu verantwortet sie die Projekte und Clusterprogramme des Organisationsbereichs, insbesondere durch deren kontinuierliche Entwicklung. Sie berät und begleitet unter anderem alle Dimensionen und Organisationsbereiche bei großen Digitalisierungsprojekten, zum Beispiel im Bereich der „Digitalisierung Landbasierter Operationen" oder des „German Mission Network".

Kernelement zur Umsetzung der Digitalisierungsplattform ist die Einrichtung von Kompetenzzentren für jedes der neun Cluster. Diese sind Denkfabriken für den Einsatz von Informations- und Kommunikationstechnologien und zeichnen sich dabei durch ihre übergreifende Aufstellung und fachliche Expertise aus.

In Abstimmung mit nationalen und internationalen Partnern sowie den weiteren Kompetenzzentren – für das Militärische Nachrichtenwesen sowie Wirkung CIR, die jedoch erst zukünftig in die Clusterlogik eingebunden werden – und dem „Querschnittsdezernat" für die Fähigkeitsentwicklung CIR erfolgt die Standardisierung, Konsolidierung, Harmonisierung und kontinuierliche methodische wie auch technologische Weiterentwicklung. Dies umfasst auch die Informationssicherheit – einschließlich Ausbildung – unter Hinzuziehung des Daten-und Geheimschutzes. Hier findet eine enge Zusammenarbeit mit dem BAAINBw, der Industrie und Kompetenzzentren statt.

Abteilung IV – Nutzerapplikationen: Diese Abteilung entwickelt selbstständig oder in Kooperation mit anderen Stakeholdern Anwendungssoftware für den Geschäftsbereich und passt selbst- und fremdentwickelte Softwareprodukte den spezifischen Forderungen der Bundeswehr an. Hierzu werden IT-Services nach den vorgegebenen Architektur-, Design- und Qualitätsstandards in das IT-System der Bundeswehr integriert und bei Bedarf zu (neuen) IT-Servicemodulen zusammengefasst. Als ein prominentes Beispiel ist die Aufgabenwahrnehmung für den Bereich „Digitalfunk Behörden und Organisation mit Sicherheitsaufgaben" als mobiler Service außerhalb des IT-Systems der Bundeswehr für die gesamte Bundeswehr zu nennen. Ebenso werden Prototypen zur Evaluierung von Anforderungen an IT-Services und zur vorläufigen Deckung akuter Sofortbedarfe im Auftrag BAAINBw aufgebaut. Darüber hinaus leistet die Abteilung eine fachliche Begleitung der Integration zur operativen Anwendung von KI in IT-Services für das IT-System der Bundeswehr. Mit dieser Fähigkeit wird sichergestellt, dass die Bundeswehr Anschluss an die rasante Entwicklung dieser Technologie hält.

Abteilung V – Erprobung und Einführung: Diese Abteilung schließt die Wertschöpfungskette zur Realisierung von Digitalisierungsvorhaben in der Bundeswehr ab. Mit der Befähigung zur Unterstützung der Realisierungsverantwortlichen mit Test- und Referenzanlagen, von der Erhebung der technischen Softwareanforderungen über die Nachweisführung der Produkte bis hin zur Sicherstellung einer kontinuierlichen Qualitätssicherung, werden wesentliche Grundlagen für die Einführung und Nutzung von IT-Services erbracht. Als weiterer Baustein steht die Möglichkeit der funktionalen Nachweiserbringung für IT-Systeme zur Verfügung.

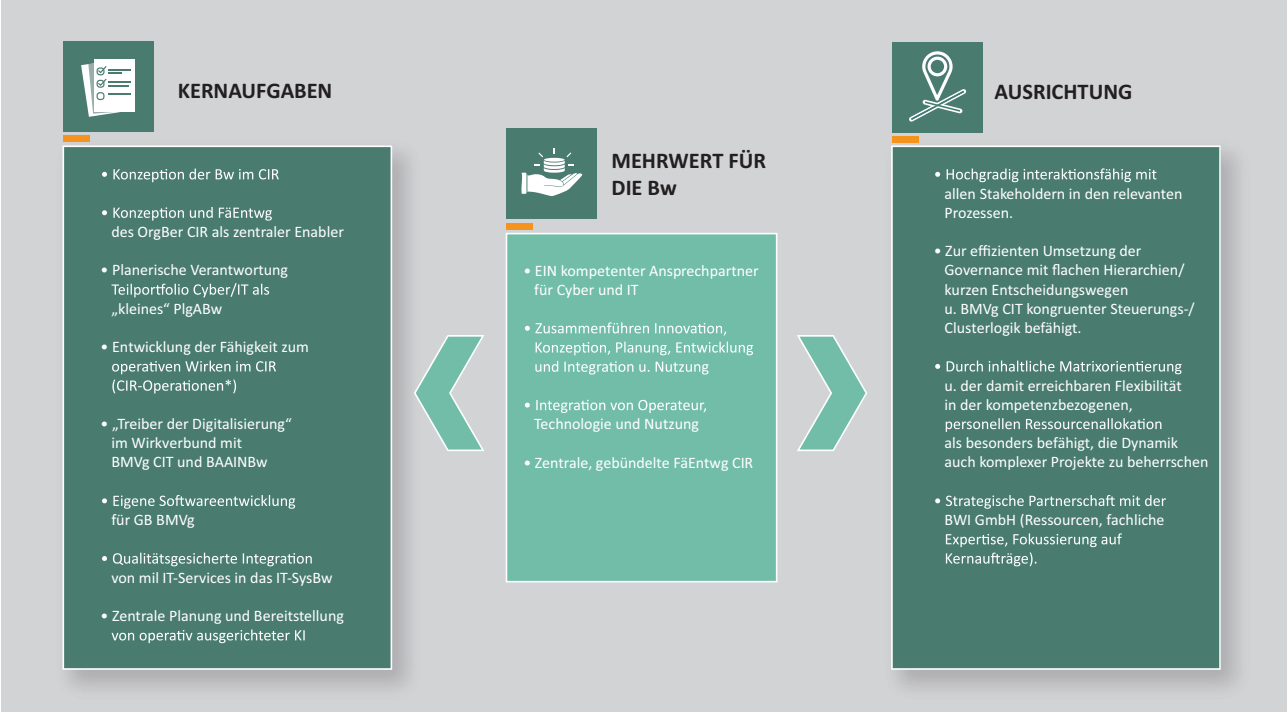
Die Systeme durchlaufen eine nationale Abnahme, bevor sie, konform dem Federated Mission Networking, im multinationalen Umfeld verifiziert und validiert werden. Multinationale Arbeitsbeziehungen mit dem Ziel der Interoperabilität für Missionen und Einsätze stehen damit auch den militärischen Organisationsbereichen offen.

Das Digitallabor der Abteilung V stellt serviceorientierte Produkte zur Verfügung, in dem (Test-)Systeme erzeugt und bereitgestellt werden. Die Ausgestaltung dieser Systeme orientiert sich für jeden Einzelfall am jeweiligen Servicebedarf und entlang der Bedürfnisse und Vorgaben des Nutzers.

ZUSAMMENFASSUNG UND AUSBLICK

Die genannten Fähigkeiten des Zentrums Digitalisierung wachsen derzeit auf. Aufgaben werden sukzessive übernommen. Mit der Indienststellung am 1. Oktober 2022 wird bereits eine vorläufige Arbeitsfähigkeit erlangt. Um im Jahr 2024 die vollständige Einsatzfähigkeit – und damit den beabsichtigten gesamten Mehrwert für die Bundeswehr – zu erreichen, bedarf es neben der Weiterentwicklung der internen und externen Arbeitsprozesse insbesondere des zeit- und qualifizierungsgerechten Aufwuchses des Personals. Letztendlich sind es motivierte und befähigte Menschen, die im Zentrum die Digitalisierung vorantreiben werden.

Eine neue und dauerhafte, strategische Kooperation mit der BWI GmbH befindet sich in Vorbereitung, um auf die qualitativ und quantitativ wachsenden Anforderungen an das Zentrum Digitalisierung schnell reagieren zu können. Diese Kooperation soll nicht nur personelle Ressourcen er-



schließen und eine agile Skalierbarkeit ermöglichen, sie ist vielmehr eine strategische Partnerschaft mit einem hochmotivierten und expertenreichen Unternehmen des Bundes, das mit Kompetenz und Erfahrung zur Qualität der Digitalisierungslösungen in exzellenter Weise beitragen kann. Qualitätsgesicherte Produkte und Services mit klaren Abnahmekriterien in einer fest definierten Zusammenarbeitsstruktur ermöglichen ein integriertes Zusammenspiel beider Partner. Der Bundeswehr ist es in dieser flexiblen Organisation möglich, auf IT-fachliche Unterstützung und klar definierte Rollen, Aufgaben und Verantwortlichkeiten zuzugreifen.

Im Kern wird sich der Erfolg der Digitalisierung der Bundeswehr an der zeitnahen Bereitstellung von Fähigkeiten messen lassen müssen, welche die digitale Überlegenheit über potentielle Gegner und die Interoperabilität der Dimensionen und das Zusammenwirken mit unseren Verbündeten in Operationen verbessert. Klare Priorisierung auf einsatzorientierte Digitalisierung und das Aufgreifen von Ideen und Lösungen aus der Forschung, Wissenschaft und Industrie sind erforderlich und unverzichtbar. Denn die Erfahrungen durch den Ukraine-Krieg zeigen deutlich, dass auch im Rahmen der Landes- und Bündnisverteidigung in einem erheblichen Umfang mit begleitenden oder auch ausschließlich hybriden Bedrohungsszenarien zu rechnen ist.

Um Informations- und Wirkungsüberlegenheit zu erreichen, kommt es daher besonders darauf an, einem möglichen Gegner den Zugriff auf bundeswehreigene IT-Infrastruktur sowie Führungs- und Waffeninformationssysteme zu verwehren und ihn bei der Nutzung der eigenen Systeme weitestgehend einzuschränken.

Die Entwicklung der hierzu erforderlichen Fähigkeiten der Bundeswehr ist eine wesentliche Aufgabe des Zentrums Digitalisierung.

Da die Digitalisierung in allen Lebensbereichen ansetzt, gibt es eine hohe Erwartungshaltung an den Organisationsbereich CIR und das Zentrum Digitalisierung. Birgt der Grundbetrieb die Möglichkeit, Digitalisierung standardisiert und skalierbar auf- und umzusetzen, muss die unbedingte Verwendbarkeit im Ernstfall gegeben sein. Nur wenn die Digitalisierung den Soldatinnen und Soldaten einen Mehrwert und Nutzen im Einsatz bringt, stellt sie einen Dienst und nicht nur ein Produkt dar. Das ist der wesentliche Grund für den Aufbau des Zentrums. Die Menschen, die an der Ausgestaltung dieser Dienststelle arbeiten, haben den festen Willen, die Digitalisierung in der Bundeswehr voranzutreiben. Das Zusammenführen von Bedarf und Innovationen innerhalb der Digitalisierungsplattform durch kreative Menschen, die die Möglichkeiten der Digitalisierung erkennen und in IT- und Waffensystemen nutzbar machen wollen, ist eine wesentliche Voraussetzung für den Erfolg – und diese Plattform ist das Scharnier für eine moderne und leistungsfähige Bundeswehr.

Das Zentrum muss sich hochgesteckten Erwartungen stellen. Es sieht sich als dimensionsorientierte, zentrale Ansprechstelle zur Koordination aller konzeptionellen und planerischen Entwicklungs- und Digitalisierungsaktivitäten aller Organisationsbereiche. Mit der schlanken, effizienten und agilen Struktur des Zentrums Digitalisierung wird es die Verantwortung für die Fähigkeitsentwicklung des Cyber- und Informationsraums und die planerischen Aufgaben im Teilportfolio Cyber/IT und CIR für die Bundeswehr konsequent umsetzen können.

Das Zentrum Digitalisierung mit seinen Aufgaben ist nicht nur der Beitrag des Organisationsbereichs CIR als Treiber der Digitalisierung der Bundeswehr, sondern mit Sicherheit auch eine attraktive Dienststelle für digital begeisterte und innovative Angehörige der Bundeswehr.

▲ Kernaufgaben, Mehrwert und Ausrichtungsparameter.
Grafik: BMVg CIT

DIENSTSTELLEN-PROFIL

BATAILLON ELEKTRONISCHE KAMPFFÜHRUNG 931

„Das Ohr zur Welt“ leistet mit seiner stationären und mobilen Aufklärung seinen Beitrag zur weltweiten Krisenfrüherkennung, Konfliktbeobachtung und zur Unterstützung der Soldatinnen und Soldaten sowie der Partner im Auslandseinsatz.

AUFGABEN

- Auftragsbezogene Erfassungen, Auswertungen und Meldungen aus einer ortsfesten Stellung.
- Mobile Fernmeldeaufklärung zum Erfassen von Fernmelde-ausstrahlungen sowie Aufbereitung für Lagebilder.
- Elektronische Gegenmaßnahmen zum Stören feindlicher Sprech- und Datenfunkverbindungen.

AUFTRAG

Das Bataillon Elektronische Kampfführung 931 (EloKaBtl 931) erfüllt eine Vielzahl von Aufgaben im militärischen Organisationsbereich Cyber- und Informationsraum. Sie lassen sich unter den Schlagwörtern „Aufklären“ und „Schützen“ zusammenfassen. Die Spezialistinnen und Spezialisten der Elektronischen Kampfführung schützen die eigene Truppe zum Beispiel bei Patrouillen durch das Unterdrücken gegnerischer Signale vor fern-gesteuerter Auslösung von Sprengfallen und Minen.

Außerdem wird die gegnerische Kommunikation erfasst, ausgewertet sowie die Erkenntnisse weitergemeldet. Somit leisten die Einsatzkräfte einen entscheidenden Beitrag zur Erstellung eines umfassenden Lage-bildes vor Ort und warnen eigene Kräfte vor erkannten Bedrohungen. Auch vom Standort Daun aus wird mit modernster Technik ununterbrochen aufgeklärt, um Konflikte und Bedrohungen zu erkennen, noch bevor sie in den Nachrichten erscheinen.

Im Rahmen von strukturellen Änderungen des Projekts CIR 2.0 wird der ortsfeste Anteil zum 1. April 2023 ausgegliedert und als eine eigenständige Dienststelle Fernmeldeaufklärungszentrale Süd aufgestellt.

ANSCHRIFT
Heinrich-Hertz-Kaserne,
Heinrich-Hertz-Str. 33,
54550 Daun

DIENSTSTELLENLEITUNG
Oberstleutnant Andreas Hartmann

STAMMPERSONAL
~1.000

AUFSTELLUNG
01.07.1957

Kommando Cyber- und Informationsraum – Enabler der digitalen Souveränität

Der Organisationsbereich Cyber- und Informationsraum (CIR) wurde aufgebaut, um die Digitalisierung in der Bundeswehr zu stärken und alle vorhandenen Kräfte und Fähigkeiten zu bündeln. Mit der „Wahrnehmung der Dimensionsverantwortung im Rahmen des Planens und Führens von CIR-Operationen" und in der Funktion „Treiber der Digitalisierung der Bundeswehr" stellt sich das Kommando CIR zwei sehr herausfordernden Kernaufgaben.

Für CIR-Operationen stellt das Kommando CIR die Fähigkeiten Aufklärung, Wirkung, Betrieb, Schutz und Unterstützung bereit. Als „Treiber der Digitalisierung der Bundeswehr" ist ein erster Schritt der Aufbau einer zentralen Digitalisierungsplattform (gemäß der Cluster-Logik) für den Geschäftsbereich BMVg.

Ziel ist die Bündelung der Clusterprogramm-bezogenen Maßnahmen, Harmonisierung von Portfolios, maximale Wiederverwendbarkeit, Modularität und Skalierbarkeit der einzelnen Produkte, um Effizienz und Wirtschaftlichkeit in der Beschaffung sowie der Nutzung nachhaltig zu verbessern. Zukünftig sollen dadurch Lösungen im Idealfall komplett aus Komponenten der Digitalisierungsplattform zusammenzustellen sein und die Digitalisierung der Bundeswehr zur Wirkung gebracht werden.

Als Hilfsmittel zur Strukturierung und Priorisierung der anfallenden Aufgaben werden die Methoden IT-Architekturmanagement, IT-Bebauungsplanung, IT-Bedarfs- und Anforderungsmanagement sowie IT-Servicemanagement genutzt. Ergänzend verfügt das Zentrum Digitalisierung Bundeswehr (ZDigBw) über die wesentlichen Fähigkeiten zum Umsetzen der Fähigkeitsentwicklung.

Die Industrie begrüßt diese Ansätze und unterstützt die jeweiligen Fähigkeiten und Methoden unmittelbar. Wie aber kann eine solche Unterstützung konkret aussehen?

Es gilt die „digitale Souveränität" zu erhalten. Die hybride Kriegsführung in der Landes- und Bündnisverteidigung bedeutet, dass künftige Konflikte zunehmend über alle Dimensionen – Land, Luft/Weltraum, See, Cyber- und Informationsraum – hinweg ausgetragen werden, mit wechselnden Schwerpunkten und digitalen Kampagnen gezielt überlagert. Ob militärische Operationen erfolgreich sind, hängt immer stärker von Umfang und Qualität der Digitalisierung beteiligter Streitkräfte ab. Des Weiteren sind der Schutz und sicherer Betrieb der IT-Systeme der Bundeswehr, das Aufklären und Wirken im Cyber- und Informationsraum und die Unterstützung für alle Bereiche der Bundeswehr mit verlässlichen Lage- und Geoinformationen zu gewährleisten.

Wie gelingt es zukünftig, Cyber-Angriffe, etwa auf Bundeswehr- oder auch relevante Regierungsnetze, schneller und zuverlässiger und automatisiert zu erkennen und Prognosen für die umfassende Cyber-Sicherheitsvorsorge abzuleiten?

Die Herausforderung in der Prävention liegt in der Analyse der angewendeten Security-by-Design-Prinzipien und der Härtung der IT-gestützten Einsatz- und Waffensysteme sowie dem IT-Systemverbund. Ziel ist die Identifikation und Minimierung ausnutzbarer Schwachstellen in IT-Systemen und eingebetteten Komponenten.

Besondere Bedeutung erlangt hierbei die erklärbare Künstliche Intelligenz (KI), die in kommerziellen Standardprodukten (Commercial off-the-Shelf, COTS) und modifizierten Standardprodukten (Military off-the-Shelf, MOTS) immer häufiger zum Einsatz kommt. KI soll auf allen Ebenen regelbasierte Entscheidungen unterstützen, das sogenannte Deep Learning ermöglichen oder andere Arten von Algorithmen zielgerichtet zum Einsatz bringen.

Wie lassen sich unzählige Einzelevents und Incidents bei wachsenden Datenmengen automatisiert und präziser korrelieren, annotieren und anreichern und anhand von Indicators of Compromise (IOC) beispielsweise in Zusammenarbeit mit dem Nationalen Cyber-Abwehrzentrum zu einem gemeinsamen Lagebild verbinden? Dies ist gerade im Hinblick auf neue Übertragungstechnologien wie 5G/6G, moderne Satellitenkommunikation oder Operational Technology (OT) auch eine Frage des Zugriffs auf Schlüsseltechnologien und Aufgabenverteilung.

Im Fall von gezielten hybriden Angriffen einschließlich Desinformationskampagnen sind stärker automatisierte Verfahren gefragt, mit denen Cyber-Angriffe verhindert, eingedämmt, isoliert und rasch anhand der gewonnenen Erkenntnisse mittels IT- und Netzwerk-Forensik ausgewertet werden können. Mit dem NATO Cyber Security Services Framework (CSSF) werden Cyber-Defense-Kernfähigkeiten, wie eine Cyber Defence

Platform, Security Log Collection, Network Intrusion Protection und Full Packet Capture, Online Vulnerability Assessments und Online Computer Forensics bereits adressiert.

Die wichtige Fähigkeit der Attribution von Cyber-Angriffen betrifft zur Gewährleistung der inneren und äußeren Sicherheit die Organisationen mit Sicherheits- und Verteidigungsaufgaben zur Bekämpfung von Cyber-Sabotage, Cyber-Spionage oder militärische Operationen im Kontext von Cyber Warfare. Die Eindeutigkeit und Unbestreitbarkeit (Non Repudiation) muss hierbei technologisch sichergestellt werden. Das „Joint Intelligence Centre" ist das neue, zentrale Element des Militärischen Nachrichtenwesens. Die Cyber and Information Domain Task Force könnte die Aktivitäten in einem „Cyber and Information Domain Warfare Centre" bündeln.

Für das zentrale IT-Service- und ein integrales IT-Sicherheitsmanagement wird umso mehr vertrauenswürdige IT benötigt, die neue IT-Architekturen (beispielsweise Zero Trust beziehungsweise Secure Access Service Edge, Multi Domain Cloud, Multi Level Security) berücksichtigt. Zudem muss sie die Interoperabilität im Verbund sicherstellen und Testhausfähigkeiten im „Systemhaus-Prinzip" für die Validierung, Verifikation und Nachweisbarkeit von Funktionalität im Beschaffungsprozess erlauben.

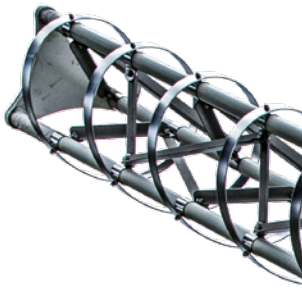
Die nachhaltige Sicherstellung der „digitalen Souveränität" bei der Landes- und Bündnisverteidigung mit der notwendigen Qualität und Agilität ist der Schlüssel zum Erfolg und kann nur in einem funktionierenden Ökosystem von nationalen Herstellern und Dienstleistern als Partner der Bundeswehr gewährleistet werden.

Und gerade hier sehen wir das Kommando Cyber- und Informationsraum als den Key Player, den Enabler der digitalen Souveränität. Es steuert maßgeblich die Sicherstellung des Betriebs der IT-Infrastrukturen und Plattformen. Zudem ist es im Bereich Cyber Security befähigt, komplexe Angriffe auf die eigene IT frühzeitig zu erkennen und negativen Auswirkungen, die akut die Sicherheit der Bundesrepublik Deutschland beeinträchtigen können, vorzubeugen.

Die Industrie und insbesondere die IT-Unternehmen stehen dabei als verlässliche, kompetente Partner zur Verfügung.

Seit mehr als 30 Jahren ist CONET in der IT-Beratung der Streitkräfte, bei Behörden und in der Industrie als innovativer Partner aktiv. Tiefgehendes System-Know-how, der Einsatz von State-of-the-Art-Tools, ein hohes Maß an Methodenkompetenz und bestausgebildete Spezialisten zeichnen uns aus. CONET ist Ihr zuverlässiger Begleiter auf dem Weg zu digitalisierten Prozessen und Lösungen.

CONET



OBERST I.G. FRANK ENDLER, ABTEILUNGSLEITER STEUERUNG
DES ZENTRUMS FÜR DIGITALISIERUNG DER BUNDESWEHR UND FÄHIGKEITSENTWICKLUNG CIR

DER ORGANISATIONSBEREICH CYBER- UND INFORMATIONSRAUM ALS ZENTRALER BEDARFSTRÄGER FÜR DAS TEILPORTFOLIO CYBER- UND INFORMATIONSTECHNIK

Das Teilportfolio Cyber/IT, als Teil des gesamten Planungsportfolios der Bundeswehr, umfasst alle IT-Projekte und ist damit das technische Rückgrat der Digitalisierung der Bundeswehr. Hier pulsieren die digitalen Nervenbahnen, die alle Elemente der Bundeswehr verbinden. Der Inspekteur Cyber- und Informationsraum hat dabei eine einmalige Aufgabe: Er trägt planerische Verantwortung als zentraler Bedarfsträger für alle IT-Projekte der Bundeswehr.

Diese Verantwortung ist zentral für die Aufgabe als „Treiber der Digitalisierung". Für das Planungsportfolio in seiner Gesamtheit ist auf Ämter- und Kommandoebene das Planungsamt als zentraler Bedarfsträger der Bundeswehr zuständig. Der Organisationsbereich CIR als „Treiber der Digitalisierung" arbeitet das Teilportfolio „Cyber und Informationstechnik" (Cyber/IT) eigenverantwortlich zu und ist damit komplementär zum Planungsamt der Bedarfsträger für die Bundeswehr in diesem Portfolio.

2017-2022: DER ORGANISATIONSBEREICH CIR ALS TREIBER DER DIGITALISIERUNG

Ein Ziel der Aufstellung des Organisationsbereichs CIR war die Schaffung agiler Planungsprozesse für Cyber/IT, um den schnellen Innovationszyklen der Informationstechnik Rechnung zu tragen. Zunächst wurden die IT-Projekte der Bundeswehr in einem Teilportfolio zusammengefasst. Insgesamt sind dies über 500 Projekte in allen Projektphasen von Planung, über Rüstung und Realisierung bis zur Nutzung, die schrittweise nahezu alle aus der Verantwortung des Planungsamtes der Bundeswehr in die Verantwortung des Kommandos CIR übergingen.

Das Teilportfolio Cyber/IT wird mit einem Planungshorizont von bis zu 15 Jahren ausgeplant und realisiert. Es umfasst derzeit ein Finanzvolumen von etwa 33 Milliarden Euro. Damit werden die inhaltlichen planerischen Voraussetzungen für die Rüstung („Was" und „Wie") und die Einplanung im Haushaltsaufstellungsverfahren („Womit") geschaffen. Die Umsetzung und Rüstung erfolgt auf Grundlage der vom Parlament gebilligten Haushaltslinien.

„Die Digitalisierung ermöglicht die Durchsetzungsfähigkeit der Streitkräfte auf dem digitalisierten Gefechtsfeld und verbessert das unterstützende Verwaltungshandeln. Damit trägt sie entscheidend zur Auftragserfüllung der Bundeswehr bei."

Umsetzungsstrategie Digitale Bundeswehr, 14.06.2019

Zeitgleich mit der Aufstellung des Organisationsbereichs CIR entwickelte sich die digitale Transformation der Bundeswehr als strategischer Ansatz. Voraussetzung für agile Planungsprozesse ist ein Kulturwandel, der von einem ebenenübergreifenden Veränderungsmanagement begleitet und mit erforderlichen Haushaltsmitteln alimentiert wird, und eine Konzeption, die Innovationen auf der Höhe der Zeit berücksichtigt und fördert. Die Bundeswehr hat unter Federführung des Organisationsbereichs CIR seit 2017 eine digitale Innovationslandschaft aufgebaut, die viele Elemente umfasst.

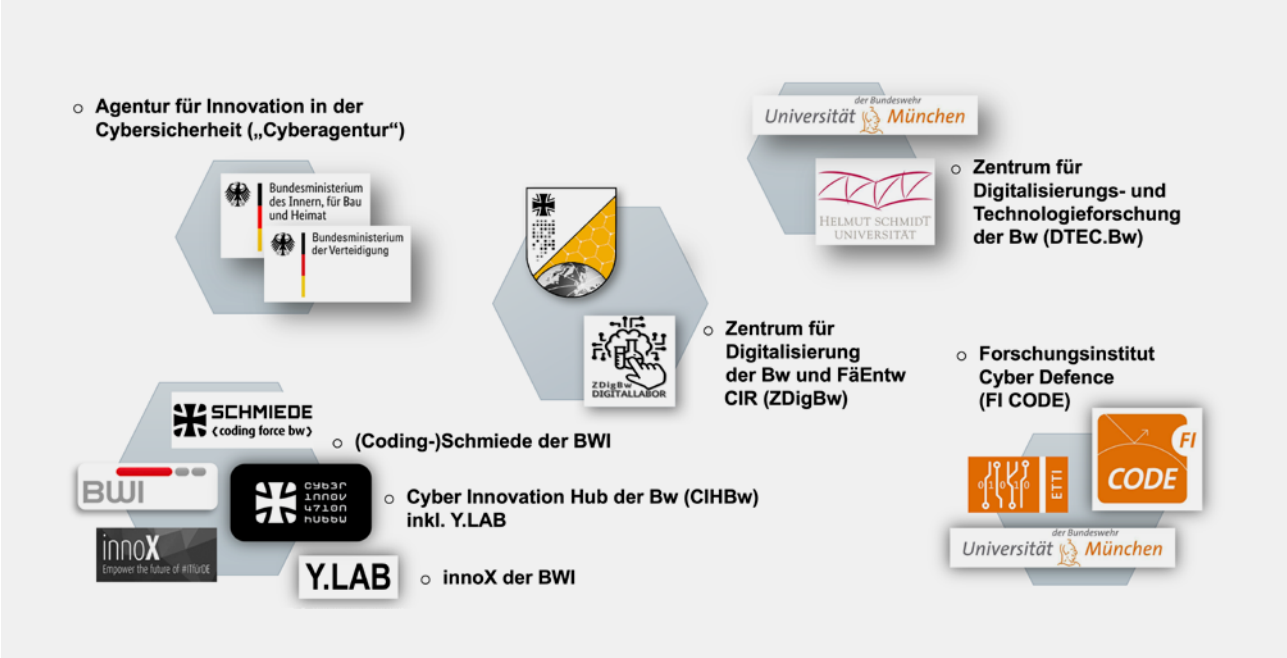
Das Forschungsinstitut CODE der Universität der Bundeswehr München und das Zentrum für Digitalisierung- und Technologieforschung (DTEC.Bw) sowie die Zusammenarbeit mit der Cyberagentur erschließen der Bundeswehr wissenschaftliche Erkenntnisse.

Der Cyber Innovation Hub der Bundeswehr schlägt dabei eine direkte Brücke von der Truppe zu innovativen Start-Ups. Mit den Innovationseinheiten Schmiede und innoX und in enger Zusammenarbeit mit der BWI Innovation & Technology wird auch die Innovationskraft der bundeseigenen BWI GmbH als IT-Systemhaus der Bundeswehr eingebunden. Seit 2017 ist somit ein übergreifendes Innovationsökosystem CIR entstanden, dessen Begleitung und Ankerpunkt das Kommando CIR war und seit 1. Oktober 2022 das Zentrum Digitalisierung der Bundeswehr und Fähigkeitsentwicklung CIR (ZDigBw) ist. Die COVID-19-Pandemie wirkte seit 2020 als Katalysator der Digitalisierung. In kürzester Zeit wurden unter anderem die vorhandenen Fähigkeiten für Videokonferenzen und mobiles Arbeiten hochskaliert und verstetigt sowie die temporäre Nutzung einer OpenVPN-Lösung erwirkt.

Im Rahmen von Innovationsvorhaben entwickelte Prototypen deckten als Ausnahme und Übergangslösung in der pandemischen Lage kurzfristige Bedarfe. Ein Beispiel ist die Online-Video-Sprechstunde, die kurzfristig vom Prototyp für den Bundeswehr-Krankenhausbetrieb auf die Nutzung für die Personalgewinnung und die Truppenpsychologie ausgeweitet wurde. Gleichzeitig konnten „unter Last" wichtige Erkenntnisse im Zuge der zugehörigen Innovationsvorhaben gewonnen werden. Mit dem Sonderprogramm Resilienz der Bundeswehr durch Digitalisierung wurden 1,45 Milliarden Euro aus dem Konjunkturpaket der Bundesregierung für Ausbau und Verstetigung der neuen Fähigkeiten ausgeplant.

▲ Das Thema SATCOMBw in den Stufen 2 und 3 ist eines der wichtigen Projekte der kommenden Jahre.
Foto: Bundeswehr/Martina Pump

◀ Beispiele für IT-Projekte der Bundeswehr.
Grafik: Bundeswehr/KdoCIR



Seit Gründung des Kommandos CIR konnten zahlreiche IT-Projekte aus verschiedenen Bereichen der Bundeswehr in den letzten drei Jahren vorangetrieben werden. Prominente Beispiele sind:

- **Satellitenkommunikationssystem der Bundeswehr (SATCOMBw):** Sicherstellung der Führungsfähigkeit der Bundeswehr in Auslandseinsätzen und zur Landes- und Bündnisverteidigung durch gesicherten Zugriff auf Kommunikationssatelliten zum weltweiten Daten- und Informationsaustausch mit hohen Übertragungsraten.
- **Dezentrale Serversegmente Einsatz (DSE):** Hauptaufgabe des Projektes DSE ist die Bereitstellung von einheitlichen, dezentralen und autarkiefähigen Serversegmenten als Server-Plattform (Hardware) für Einsätze der Teilstreitkräfte und militärischen Organisationsbereiche. Die Serversegmente sind als Teil der IT-Plattformen des Kommunikationssystems der Bundeswehr für den Einsatz querschnittlich nutzbar. Die DSE sind zur Sicherstellung der Führungsfähigkeit der Very High Joint Task Force 2023 (VJTF) relevant. Der Zulauf der Systeme erfolgt ab August 2022. Sie werden bis zum ersten Quartal 2023 an die Truppe ausgeliefert.
- **IT-Ausstattung I. Deutsch-Niederländisches Korps:** Das I. Deutsch-Niederländische Korps übernimmt die Rolle als Land Component Command (LCC) für VJTF 2023. Hierfür sind verlegefähige Teilsysteme erforderlich. Zu diesem Zweck wurden die erforderlichen IT-Services in geeignete Container eingerüstet. Die Umsetzung erfolgte risikoarm durch Beschaffung von bereits in die Bundeswehr eingeführten Produkten.
- **IT-Unterstützung (IT-U) Planung:** Die IT-U Planung soll die zentrale Plattform für alle Planungsaktivitäten der Bundeswehr werden und diebisherigen heterogenen IT-Tools (z.B. MISPL) ablösen. Sie wird schrittweise in mehreren Bausteinen seit 2019 bis 2028 realisiert: Multinationale Planung (NATO/EU), „Harmonisiertes Projektmanagement“, Planungsumsetzung, Fähigkeitsentwicklung, „Sofortinitiative für den Einsatz“, Innovationsmanagement und „Wissenschaftliche Unterstützung Nichttechnische Studien“.

Der Organisationsbereich CIR hat sich damit als Akteur der Planungsorganisation der Bundeswehr etabliert und verantwortet eigenständig die ihm im Leistungsprozess „Integrierte Planung durchführen“ übertragenen Planungsaufgaben für das Teilportfolio Cyber/IT und arbeitet in diesem Sinne dem Planungsamt der Bundeswehr im gesamtplanerischen Kontext zu.

SEIT 2022: DER ORGANISATIONSBEREICH CIR ALS TREIBER DER DIGITALISIERUNG

Um die Chancen und die Innovationskraft der Digitalisierung zu nutzen, bedarf es agiler Planungsverfahren, angepasst an zu Grunde liegenden IT-Technologien. Daher wurden neue Wege im IT-Bedarfs- und Anforderungsmanagement eingeschlagen und entwickelt. Im Kern wird die Digitalisierung dabei durch den Aufbau einer zentralen Digitalisierungsplattform für den Geschäftsbereich BMVg (GB BMVg) – abgeleitet aus den ministeriellen Vorgaben zur sogenannten Clusterlogik – dynamisch ausgebaut.

Die bisherige Planung der IT-Projekte der Bundeswehr erfolgte in mehr als 500 Einzelprojekten. Deren Entwicklung, Beschaffung und Einsatz wurde häufig organisationsbereichsspezifisch, also monolithisch, aufgebaut. Jeweils für sich genommen wurde zwar die geforderte Funktionalität erbracht, einer gemeinsamen Architektur und damit einem verbindenden Systemgedanken wurde damit jedoch nur unzureichend gefolgt.

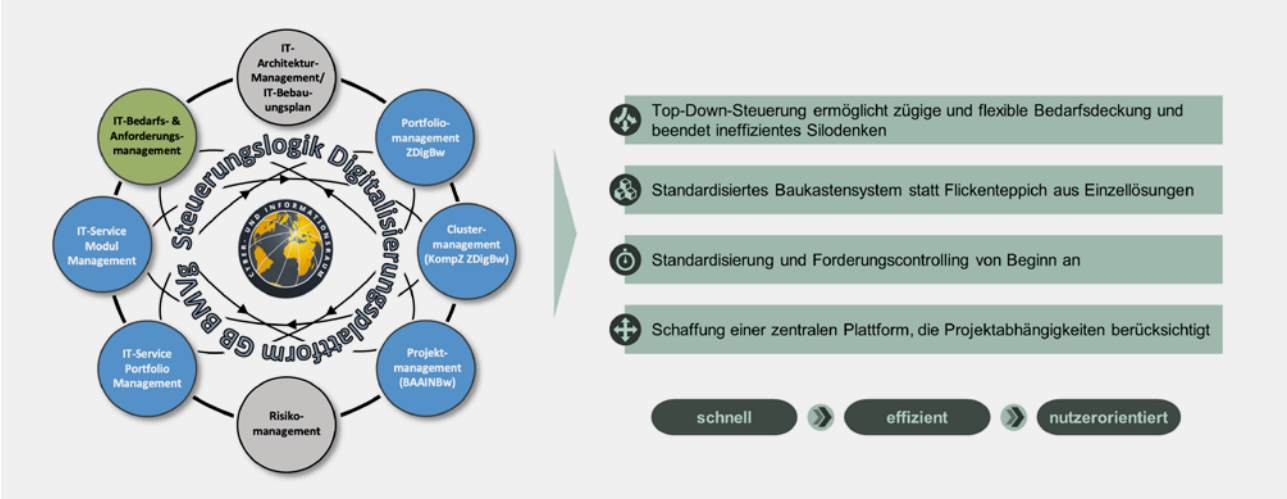
▲ Innovationslandschaft.
Grafik: Bundeswehr/KdoCIR

5G für die Bundeswehr – Der Enabler im Kampf um Informations- und Wirkungsüberlegenheit.

5G-Campus-Netze in Verbindung mit Edge Computing garantieren die schnelle und sichere Datenübertragung und ermöglichen Datenanalyse in Echtzeit auf einem neuen Level.

Lassen Sie uns gemeinsam das volle Potential von 5G ausschöpfen!

Erleben,
was verbindet.



▲ Steuerungslogik Digitalisierungsplattform:
Die Digitalisierungsplattform soll zukünftig modular aufgebaute, wiederverwendbare, skalierbare, adaptierbare und nach einem einheitlichen Regelwerk aufgebaute IT-Services zur Verfügung stellen.
Grafiken: Bundeswehr/KdoCIR

Die Digitalisierungsplattform GB BMVg wird die Vielfalt von IT-Systemen durch eine konsequente Steuerung des Gesamtsystems serviceorientiert bündeln, reduziert Finanzbedarfe durch Skaleneffekte, beschleunigt die Projektrealisierungen und vereinfacht den Betrieb, um damit die Digitalisierung der Bundeswehr in allen Bereichen zukunftsorientiert und angelehnt an NATO-Planungsverfahren zur Wirkung zu bringen.

Schlüssel zum Erreichen der Agilität ist dabei die Bündelung von IT-Services in Clusterprogrammen, die jährlich aktualisiert werden. Dadurch entsteht eine neue Dynamik, die langjährig laufende Projekte mittels inkrementeller Entwicklung von IT-Services ablöst. An die Stelle langjähriger Planungen im Wasserfallmodell tritt die kontinuierliche schrittweise tatsächliche Verbesserung in definierten Sprints, wie sie für ein agiles Vorgehen typisch sind. Nicht das Wünschenswerte soll im Vordergrund stehen, sondern das Machbare.

Das Pilotcluster, das diese Ansprüche während der Pandemielage Corona verwirklichte, war das Cluster Infrastructure Cloud Base und User-Equipment (ICU). Die weiteren acht Cluster befinden sich im Aufbau. Zahlreiche Projekte, auch außerhalb des Clusters ICU, werden nun nach der neuen Clusterlogik ausgeplant: Beispiele sind der Gefechtsstand für den Inspekteur der Streitkräftebasis, der Gefechtsstand für den Befehlshaber Einsatzführungskommando, das Gefechtsstand Access Netz (GAN) oder das Taktische Wide Area Network (TaWAN).

▼ Erprobung des Battle Management Systems in Munster.
Foto: Bundeswehr/Stefan Uj

Der Aufbau der Digitalisierungsplattform folgt der Logik vom Einfachen zum Schweren: nach der Erprobung mit vorwiegend handelsüblicher ziviler IT wechselt damit der Fokus insbesondere auf militärische Projekte, die für die Steigerung der Fähigkeiten zur Landes- und Bündnisverteidigung unerlässlich sind.

Die konzeptionellen Grundlagen für den Cyber- und Informationsraum, die neben dem Teilportfolio Cyber/IT auch die streitkräftegemeinsamen Grundlagen für das Militärische Nachrichtenwesen, das Wirken im Cyber- und Informationsraum, das Geoinformationswesen und die Weltraumnutzung umfassen, werden dabei zukünftig in der gleichen Abteilung erstellt, in der auch die Portfoliosteuerung des Organisationsbereichs CIR erfolgt. Damit gehen Konzeption und Fähigkeitsentwicklung des Teilportfolios Cyber/IT nahtlos ineinander über. Deshalb werden hier die meisten Überlegungen und dann im Weiteren auch die Umsetzung von Maßnahmen zur Förderung der Resilienz im Cyber- und Informationsraum bezüglich der Landes- und Bündnisverteidigung wahrgenommen.

Auf diese Weise wird eine neue Qualität der Entwicklung des IT-Systems als Rückgrat der Digitalisierung erreicht. Die Aufgaben des Organisationsbereichs gehen dabei zukünftig über die technische Dimension immer weiter hinaus: Ziel ist die umfassende Beratung, fachliche Anleitung und lebenszyklusbegleitende Unterstützung der gesamten Bundeswehr bei der Planung und Realisierung von Digitalisierungsprojekten auf Basis der Digitalisierungsplattform der Bundeswehr, um Führungsfähigkeit von der strategischen bis zur untersten taktischen Ebene zu etablieren.

Denn auch für die Digitalisierung gilt: der Mensch steht im Mittelpunkt, und in der Bundeswehr die Truppe, nie die Technik. Dem fühlt sich das neu aufgestellte Zentrum Digitalisierung der Bundeswehr verpflichtet. Das ist der Weg in die Zukunft, in der effektive Digitalisierung eine entscheidende Voraussetzung für den erfolgreichen Einsatz der Bundeswehr ist.

DIENSTSTELLEN-PROFIL

BATAILLON ELEKTRONISCHE KAMPFFÜHRUNG 932

Das mobile Bataillon der Elektronischen Kampfführung unterstützt Einsatzverbände, Spezialisierte Kräfte und Spezialkräfte der Bundeswehr mit Fähigkeiten des Elektronischen Kampfes.

AUFGABEN

- Unterstützung in Evakuierungsoperationen und Operationen der Spezialisierten Kräfte und der Spezialkräfte der Bundeswehr mit Fähigkeiten des Elektronischen Kampfes.
- Durchführung von elektronischen Gegenmaßnahmen, womit die eigene Operationsführung unterstützt und die gegnerische Operationsführung erschwert werden kann.
- Unterstützung der Operationsführung durch mobile und quasi stationäre Aufklärung zur Vervollständigung des Lagebildes.

AUFTRAG

Das Bataillon Elektronische Kampfführung 932 (EloKaBtl 932) verfügt über einen Stab und fünf Kompanien, nimmt Aufgaben der Elektronischen Aufklärung wahr und führt Maßnahmen des Elektronischen Kampfes durch. Dazu gehört die unmittelbare Unterstützung von Einsatzverbänden mit Systemen zur mobilen Aufklärung der Kommunikation gegnerischer Kräfte. Das Bataillon ist in der Lage, elektronische Gegenmaßnahmen durchzuführen: es kann die Kommunikation des Gegners stören oder diesen gezielt täuschen. Speziell ausgebildete EloKa-Kräfte unterstützen darüber hinaus militärische Evakuierungsoperationen und Einsätze von Spezialkräften der Bundeswehr. Durch moderne Technik und Softwareanwendungen können die im Schichtdienst eingesetzten Soldatinnen und Soldaten des Bataillons aus dem Heimatland heraus die Kräfte in den Einsatzländern unmittelbar unterstützen. Aktuell ist das Bataillon mit der Aufstellung und Ausbildung einer kurzfristig verlegbaren Einheit zur Unterstützung der Speerspitze der NATO (Very High Readiness Joint Taskforce, VJTF) beauftragt. Damit stellt der Verband nicht nur Personal für die aktuellen Einsätze der Bundeswehr, sondern hält zusätzlich etwa 200 Soldatinnen und Soldaten in ständiger Bereitschaft. Die jährliche Beteiligung an nationalen und internationalen Großübungen, die Kooperationen im Rahmen der internationalen Zusammenarbeit, zum Beispiel mit niederländischen und österreichischen Kräften der elektronischen Aufklärung und eine seit über 35 Jahren bestehende Patenschaft mit einem US-Bataillon in Wiesbaden, runden das Portfolio des Bataillons ab.

ANSCHRIFT
Burgwald-Kaserne,
Marburger Str. 75,
35066 Frankenberg (Eder)

DIENSTSTELLENLEITUNG
Oberstleutnant Daniel Renkl

STAMMPERSONAL
~750

AUFSTELLUNG
01.06.1962

AUTORENTEAM ZENTRUM DIGITALISIERUNG DER BUNDESWEHR

FÄHIGKEITSENTWICKLUNG IM CYBER- UND INFORMATIONSRAUM

Herausgehobene Projekte aus dem Zentrum Digitalisierung der Bundeswehr

Im Bereich der Fähigkeitsentwicklung und Digitalisierung werden zukunftsweisende Projekte für die zwingend erforderliche Digitalisierung im Cyber- und Informationsraum (CIR) bearbeitet und vorangebracht. Diese Projekte decken eine große Palette ab, die von der **Digitalisierung Landbasierte Operationen** bis zur weltweit abbildenden **Aufklärung** reicht.

OBERSTLEUTNANT RUDOLF STEGMAIER

Digitalisierung Landbasierte Operationen

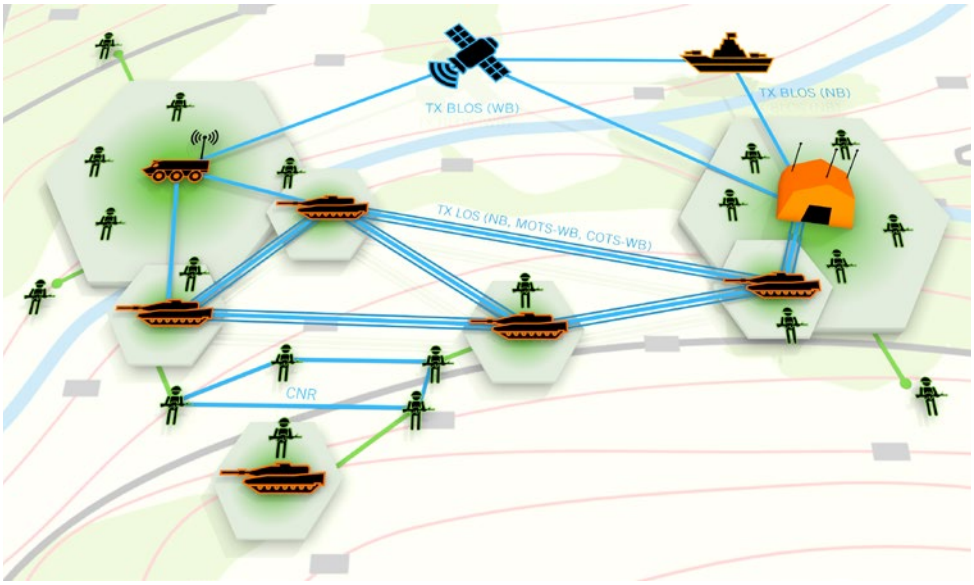
Das Programm Digitalisierung Landbasierte Operationen (D-LBO) ist das wichtigste Vorhaben zur Digitalisierung von Plattformen (Fahrzeuge, Container/Kabinen, Soldatenausrüstung) aller an landbasierten Operationen beteiligten Organisationsbereiche der Bundeswehr.

Durch das Programm D-LBO wird mehr als „nur" neue Technik eingeführt. Neben neuen Standards in der Technik werden, als wichtige Rahmenbedingung, grundsätzliche Vorgaben zu standardisierten Rüstsätzen für die Einrüstung neuer Funk- und IT-Technik in Plattformen der Bundeswehr etabliert.

Dies beinhaltet technologische Quantensprünge in der Funktechnik und der vernetzenden Gesamtkonzeption, verbunden mit einer zukunftsfähigen technischen Ausrichtung auf weitere IT-Themenfelder, wie zum Beispiel Multi Domain Combat Cloud und Künstliche Intelligenz. Durch die geplante Anbindung über die durch das German Mission Netzwerk bereitgestellte Schnittstelle ist eine Informationsanbindung an das IT-System der Bundeswehr sichergestellt.

Die dafür erforderlichen und heutigen Standards entsprechenden digitalen Funkgeräte, sogenannte Software Defined Radios (SDR), lösen die veralteten analogen Funkgeräte der Bundeswehr schrittweise ab. Doch nicht nur neue Funktechnik, sondern vor allem ein Paradigmenwechsel im Bereich der Vernetzung öffnet neue Wege und Möglichkeiten, Kommunikations- und Informationsversorgung an vorderster Front zur Verfügung zu stellen. Mit dem Konzept von „Open Transport" und Ende-zu-Ende-Verschlüsselung vom Entstehungsort der Daten bis zum Empfänger, werden bisherige Verschlüsselungskonzepte jedes einzelnen Übertragungsweges abgelöst.

Das Programm D-LBO spannt einen übergreifenden und verbindenden Bogen von Kommunikationstechnik über mobile Netzwerke bis hin zu Plattformeinrüstungen. D-LBO stellt damit zwar einen wichtigen Meilenstein für eine aktive Teilhabe der Bundeswehr auf dem digitalisierten Gefechtsfeld dar, kann aber nur als Auftakt für weitere, unbedingt erforderliche Digitalisierungsvorhaben verstanden werden.



◀ Aufbau der Richtfunkanlage Tetrapol bei der Übung Common Roof, einer internationalen Übung des DACH-Verbandes in Murnau.
Foto: Bundeswehr/Martina Pump

▶ Durch das Programm D-LBO wird mehr als „nur" neue Technik eingeführt.
Grafik: blackned

MAJOR MICHAEL GÜNTHER-WÖLKERT

RECHENZENTRUMSVERBUND GESCHÄFTSBEREICH BMVG

Das Digitalisierungsprojekt „Rechenzentrumsverbund Geschäftsbereich BMVg" ist ein zentrales und überaus vielschichtiges Vorhaben mit eng verflochtenen Abhängigkeiten. In der Zielstruktur wird ein skalierbarer und modular erweiterbarer Verbund von georedundanten, hochverfügbaren, stationären Rechenzentren – inklusive eines „Disaster-Backup-Centre" im Inland samt verlegefähigen Rechenzentren – bereitstehen. Gemeinsam mit den Kommunikationssystemen der Bundeswehr bilden diese Elemente das technische Fundament des IT-Systems der Bundeswehr mit speziell geschützter Infrastruktur und resilienter IT-Hardware.

Neben der deutlichen Erhöhung der Kapazitäten trägt der Rechenzentrumsverbund wesentlich zur Steigerung der Verfügbarkeit und Verbesserung der Interoperabilität sowohl im Bereich der administrativen IT-Unterstützung als auch bei Einsätzen, Dauereinsatzaufgaben, einsatzgleichen Verpflichtungen und Übungen bei. Der Verbund muss als eigenständige Fähigkeit im Katastrophen-, Spannungs- und Verteidigungsfall durchhaltefähig und eine autarke Kernführungsfähigkeit des Geschäftsbereichs im gesamten Aufgabenspektrum mit Kernfähigkeiten IT (KFIT) unterstützen.

Abgesehen von Bau und Rüstung müssen die betrieblichen Prozesse aller beteiligten Gewerke, darunter Liegenschaftsmanagement, IT-Betrieb und Absicherung, für diesen Komplex kooperativ und homogen weiterentwickelt, realisiert und betrieben werden –dies über verschiedene Betreiber, Organisationsbereiche und Bundesländer hinweg.

Wesentliche Herausforderung ist die ganzheitliche, langfristige Entwicklung im verflochtenen System bei paralleler Aufmerksamkeit für innovative Technologien (Hypes) aus den Bereichen Cloud, BigData, Künstliche Intelligenz und Quanten.

OBERSTLEUTNANT DANIEL NAHLEN

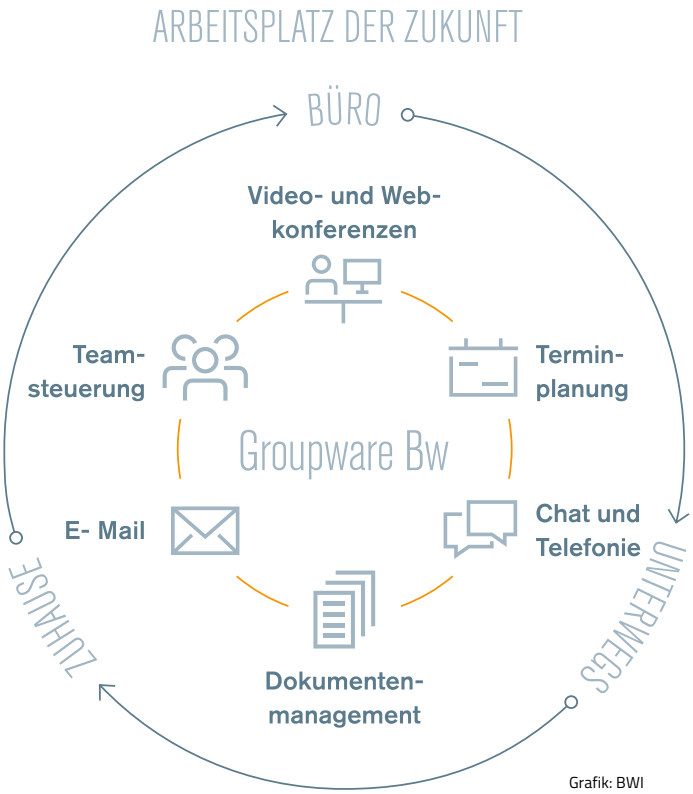
SATELLITENKOMMUNIKATION BUNDESWEHR UND TAKTISCHES WIDE AREA NETWORK

Im Projekt Satellitenkommunikation Bundeswehr Stufe 2 (SATCOMBw Stufe 2) werden mittels der beiden bundeswehreigenen Satelliten COMSATBw 1 und 2 weltraumgestützte Übertragungskapazitäten für die weitreichende Anbindung von Truppenteilen, Verbänden und Kontingenten in Übung, Einsatz und Grundbetrieb sichergestellt. Ergänzt werden diese durch weitere Übertragungskapazitäten, die bei kommerziellen Anbietern angemietet werden. Zum Projekt SATCOMBw Stufe 2 gehören zudem die für die Kommunikation notwendigen transportablen Bodenstationen sowie drei ortsfeste Bodenstationen in Deutschland, über welche die Verbindungen in die Kommunikationsnetze übertragen werden. Über diese sogenannten Ankerstationen werden die Führungs- und Kontrolldaten der gesamten Übertragungsstrecken verteilt, die aus dem Betriebszentrum IT-System der Bundeswehr heraus überwacht und koordiniert werden. Da die im Projekt SATCOMBw Stufe 2 beschafften Satelliten mit einer durchschnittlichen Nutzungszeit von 15 Jahren in naher Zukunft ihr Lebensdauerende erreichen, wurde bereits frühzeitig

SATCOMBw Stufe 3 als Nachfolgeprojekt aufgesetzt. Dieses wird in einer Anfangsbefähigung die Nachfolgegeneration der beiden COMSATBw bereitstellen. Im Zuge der Vollbefähigung wird ein deutlicher Fähigkeitsgewinn bezüglich Bandbreite und Frequenznutzung sowie eine deutliche Reduktion der Typenvielfalt bei den Bodenstationen erreicht.

Im Projekt „Taktisches Wide Area Network Landbasierte Operationen" (TaWAN LBO) soll ein breitbandiges, satellitenunabhängiges und robustes Netzwerk für landbasierte Operationen realisiert werden. Die hierzu notwendigen Elemente orientieren sich jeweils am Schutz- und Mobilitätsniveau der zu unterstützenden Truppenteile und Verbände. Hierzu sollen in einem ersten Schritt die führungswichtigen Elemente einer Division – im Sinne eines durchgängigen Informationsverbundes – mit den notwendigen Systemen ausgestattet werden.

Im Zielbetrieb werden voraussichtlich sieben Varianten mit unterschiedlichen Schutz-, Mobilitäts- und Reichweitenparametern die Informationsversorgung sicherstellen.



Grafik: BWI

OBERSTLEUTNANT MICHAEL DEPENHEUER

GROUPWARE BUNDESWEHR

Mit dem Projekt „Groupware Bundeswehr" wird eine moderne, bundeswehrgemeinsame Kollaborationsplattform eingeführt. Auf der Basis von marktverfügbaren Produkten wird damit erstmalig eine Plattform geschaffen, die ein ortsunabhängiges und zeitgleiches Zusammenarbeiten an gemeinsamen Dokumenten ermöglicht. Damit schafft das Projekt die IT-seitige Voraussetzung für eine moderne Form kollaborativer Team- und Projektarbeit, die es bisher nur in einzelnen Bereichen der Bundeswehr gab. Zusammen mit weiteren Vorhaben werden damit die Forderungen des E-Government-Gesetzes und des Regierungsprogramms „Digitale Verwaltung 2020" umgesetzt.

Derzeit wird das Projekt durch die BWI als Auftragnehmer realisiert. Ein großer Meilenstein ist für Ende 2023 vorgesehen. Bis dahin sollen die Produkte aus dem Projekt an alle Nutzer des durch die BWI bereitgestellten IT-Systems „HERKULES Folgeprojekt" ausgerollt sein.

Dabei stellt eine Herausforderung die Anpassung der bisherigen Arbeitsabläufe an die neuen technischen Möglichkeiten dar.

Nach einem erfolgreichen Rollout in der Bundeswehr können die bisher für diese Aufgabe genutzten IT-Lösungen, die entweder nur einzelnen Bereichen mit einem vergleichbaren Funktionsumfang zur Verfügung standen oder aufgrund der verfügbaren Funktionen Einschränkungen mit sich brachten, abgelöst werden.

Spätestens ab 2024 soll es dann möglich sein, „Gemeinsam digital Einfach.Zusammen.Arbeiten." zu können.

◀ Zum Projekt SATCOMBw Stufe 2 gehören beispielsweise transportable Bodenstationen sowie drei ortsfeste Bodenstationen.
Foto: Bundeswehr/Martina Pump

OBERSTLEUTNANT A.D. KLAUS RIEMER

GERMAN MISSION NETWORK (GMN)

Mit dem Programm German Mission Network (GMN) werden – in Deutschland und weltweit – Fähigkeiten zur nationalen und multinationalen Einsatz- und Operationsführung auf einer streitkräftegemeinsamen Plattform durchhaltefähig bereitgestellt. Ein durchgängiger Informationsaustausch über alle Ebenen und die Zusammenarbeit in einem System werden unter Berücksichtigung des Schutzbedarfs der Informationen – mit der Fähigkeit zur Integration multinationaler Partner – sichergestellt, sowohl im Einsatz, bei Übungen und in der Ausbildung. Mit GMN wird die Führungsfähigkeit der deutschen Streitkräfte nachhaltig auf einem internationalen Spitzenniveau gewährleistet:

- Aufbauend auf den bisherigen Fähigkeiten hält GMN die national definierten stationären und verlegefähigen Kapazitäten vor.
- Eine umfassende, ebenengerechte und schnelle Verarbeitung und Weitergabe auch von eingestuften Informationen wird gewährleistet.
- Flexible und skalierbare Schnittstellen integrieren führungsrelevante Anteile in Waffensysteme.
- Deutschland wird in der Rolle als Rahmennation in die Lage versetzt, einerseits IT-Services der Partner zu integrieren und andererseits IT-Services in unterschiedlichen, multinationalen Formaten (z.B. NATO, EU, UN) bereitzustellen.

Das Programm GMN wird in mehreren Blöcken beziehungsweise Projekten realisiert:

Mit GMN 1 werden für die Streitkräfte verlegefähige Rechenzentren und Endgeräte bereitgestellt.

Durch GMN 2 werden bereits schon jetzt die Sicherstellung und der Erhalt der Führungsfähigkeit der Deutschen Marine ermöglicht und am Standort Rostock die Funktionalitäten des Fleet Entry Point, Maritime Operations Center und Maritime Command Center zur Führung der Flotte bereitgestellt. GMN 3 ist zur zukunftsfähigen Sicherstellung der Führungsfähigkeit der Landstreitkräfte noch zu beauftragen. Mit GMN 4 wird über die Bereitstellung der IT-Services auf seegehenden Einheiten die Führungsfähigkeit der maritimen Fähigkeitsträger sichergestellt. Hierzu werden die führungsrelevanten Informationen durch nationale und multinationale IT-Services mittels autarkiefähiger Rechenzentren an Bord bereitgestellt.

Die künftige homogene IT-Ausstattung des GMN wird im Sinne einer skalierbaren und modularen „Software Oriented Architecture" Obsoleszenz im Bereich der IT-Services beseitigen. Durch die vollständige Kompatibilität mit nationalen und internationalen Informationsräumen wird die Führungsfähigkeit der Bundeswehr in der voranschreitenden globalen Digitalisierung langfristig sichergestellt werden können.

Mit der Umsetzung des Programms GMN wird ein wesentlicher Beitrag zur digitalen Transformation der Bundeswehr und auch der NATO geleistet und somit die Durchsetzungsfähigkeit der Streitkräfte auf dem digitalisierten Gefechtsfeld im internationalen Kontext ermöglicht.

MAJOR STEFAN REINIGER

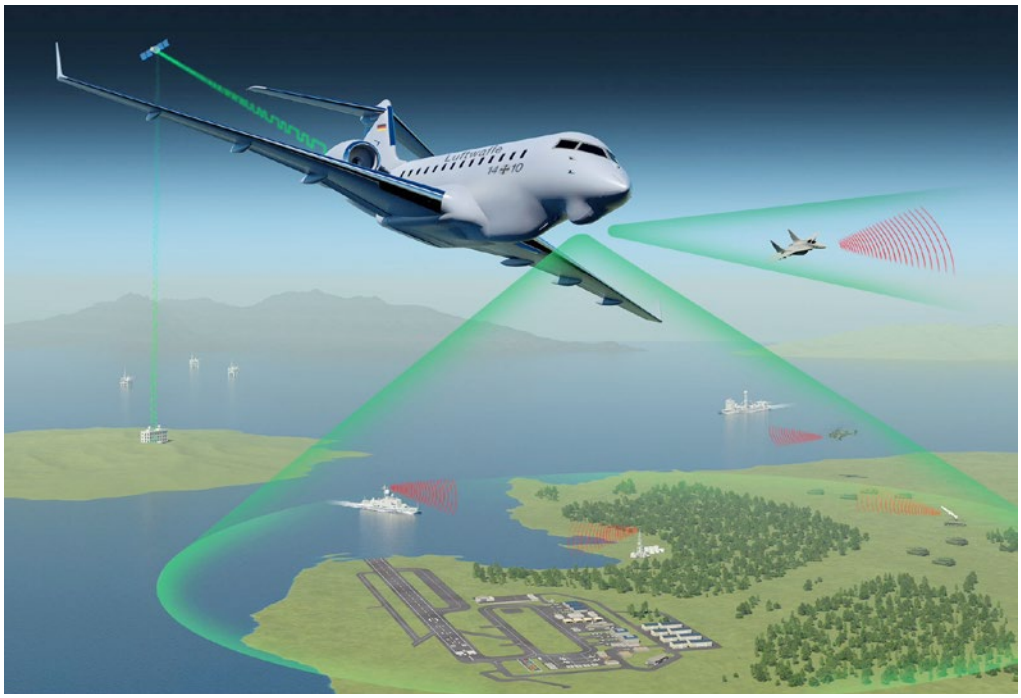
Aufklärung im CIR

Für die Operationsführung im CIR sind Fähigkeiten in den Domänen Aufklärung und Wirkung entscheidend. Mit dem Spektrum seiner Systeme trägt der Organisationsbereich CIR zur Operationsführung auf strategischer, operativer und taktischer Ebene bei. Sowohl der Erhalt bestehender Fähigkeiten als auch die Realisierung neuer Bedarfe stehen im Fokus der Fähigkeitsentwicklung im CIR.

Mit seinen teils strategischen und damit einzigartigen Aufklärungsmitteln und zugehörigen Auswertesystemen tragen CIR-Kräfte wesentlich zur nationalen Beurteilungsfähigkeit bei.

PEGASUS

Mit der Unterzeichnung des Realisierungsvertrags für das Aufklärungssystem PEGASUS im Juni 2021 wurde eine wesentliche Voraussetzung geschaffen, um die seit der Außerdienststellung des Aufklärungsflugzeugs Breguet Atlantic SIGINT (Signals Intelligence) seit Juni 2010 bestehende Fähigkeitslücke im Bereich der signalerfassenden luftgestützten weiträumigen Überwachung und Aufklärung zu schließen. Im Wesentlichen besteht das Aufklärungssystem PEGASUS aus drei für den Einsatzzweck modifizierten Luftfahrzeugen vom Typ GLOBAL 6000 und einem SIGINT-System. PEGASUS wird damit den Forderungen an ein äußerst flexibel einsetzbares Aufklärungsmittel, das einen Beitrag zur Landes- und Bündnisverteidigung leistet, gerecht. Mit PEGASUS verfügt der Organisationsbereich CIR zukünftig über ein weiteres, in der Bundeswehr einzigartig strategisches Aufklärungssystem, mit dem ein maßgeblicher Beitrag zur strategischen Urteils- und Entscheidungsfindung der Bundesrepublik Deutschland geleistet werden wird.



◀ Mit PEGASUS verfügt der Organisationsbereich CIR zukünftig über ein weiteres strategisches Aufklärungssystem.
Grafik: Hensoldt

OBERSTLEUTNANT SÖNKE FIGUTH

SARah

Mit den Startkampagnen der Satelliten des „Radarsatellitensystems zur Weltweiten Abbildenden Aufklärung SARah" im Jahr 2022 und der ab 2023 geplanten Inbetriebnahme wird die bruchfreie satellitengestützte abbildende Aufklärung in der SAR-Linie (Synthetic Aperture Radar) als strategische Aufklärungsfähigkeit fortgeschrieben. SARah folgt hierbei SAR-Lupe und wird über deutlich verbesserte Systemleistungswerte, unter anderem bei der Bildanzahl und Verarbeitungszeit, verfügen. Wie SAR-Lupe, wird SARah – ohne geographische und hoheitsrechtliche Beschränkungen – nahezu allwetterfähig und tageszeitunabhängig weltweit Radarsatellitenbilder aufnehmen, die von der Zentrale Abbildende Aufklärung ausgewertet werden. Zudem werden mit SARah die Fortsetzung der deutsch-französischen und der Einstieg in die deutsch-schwedische Kooperation erfolgen.

Dabei erhält Frankreich SARah-Bilder und Deutschland elektro-optische Bilder aus dem französischen System Composante Spatiale Optique. Weiterhin übermittelt Deutschland im Gegenzug für die Bereitstellung einer schwedischen SARah-Bodenstation SARah-Bilder an Schweden.

TECHNISCHER REGIERUNGSDIREKTOR GUNAR WEICHERT

AUSWERTESYSTEM DER SIGNALERFASSENDEN AUFKLÄRUNG DER BUNDESWEHR (AstABw)

Die durch die Aufklärungsmittel gewonnenen Daten müssen durch spezifizierte Auswerte- und Unterstützungssysteme verarbeitet werden, um dem jeweiligen Bedarfsträger maßgeschneidert verwertbare Produkte zur Verfügung zu stellen.

Die diesbezügliche Systemwelt der Signalerfassenden Aufklärung der Bundeswehr besteht heute noch zum Teil aus älteren „starren" IT-Systemanteilen und Softwareanwendungen, die für eine schnelle und flexible Anpassung auf sich ändernde strategische Lagen beziehungsweise Vorgaben ungeeignet ist.

Zur Lösung der nicht mehr zeitgemäßen Struktur soll mit dem in der Analysephase befindlichen Auswertesystem der Signalerfassenden Aufklärung ein standardisiertes, flexibles und modulares System realisiert werden, das den Plattformgedanken in der Signalerfassenden Aufklärung umsetzt und die funktionalen Kernfähigkeiten des Militärischen Nachrichtenwesens mit querschnittlichen und fachspezifischen IT-Services unterstützt.

OBERSTLEUTNANT KAI MARQUARDT

WIRKEN IN DER DIMENSION CYBER- UND INFORMATIONSRAUM

Oftmals dient Aufklärung auch zur Vorbereitung von Wirkeffekten im Cyber- und Informationsraum, für die der Organisationsbereich CIR ebenfalls in weiten Teilen unikale Fähigkeiten vorhält. Der Erhalt bestehender Wirkfähigkeiten wie auch die materielle Entwicklung zukünftiger Wirksysteme liegen ebenfalls in Verantwortung der Abteilung III des Zentrums für Digitalisierung der Bundeswehr und Fähigkeitsentwicklung CIR.

WIRKEN IM CYBERRAUM

Wirkung im Cyberraum wird durch Cyber-Operationen (CO) erzielt. Für militärische CO, die grundsätzlich aus ortsfesten Anlagen geplant, vorbereitet und durchgeführt werden, befindet sich beim Zentrum Cyber-Operationen (ZCO) die zentrale Infrastruktur. Für den verlegefähigen oder mobilen Einsatz von CO steht das System „Kleines operationelles Element CO im Einsatzgebiet" (SysKopECE) zur Verfügung. Zum zeitlich begrenzten autarken Betrieb befähigt, ermöglicht es die Anbindung der ortsfesten Einrichtungen an Zielsysteme, die über das Internet nicht erreichbar sind. Die Vereinigung, Harmonisierung und Modularisierung dieser genannten Systeme zu einem „IT-System CO" ist langfristiges Ziel der Fähigkeitsentwicklung in diesem Bereich.

WIRKEN IM INFORMATIONSUMFELD

Die Informationsverbreitung über das Internet und die Kommunikation über soziale Netzwerke/Medien verdrängen zusehends klassische Medien und Mittel der Interaktion. Die Lage im Informationsumfeld hier eingehend zu erfassen und zu analysieren ist essentiell, um das eigene Handeln bezüglich der Auswirkungen auf freigegebene Zielgruppen in den Einsatzgebieten bewerten und steuern zu können.

Die am Zentrum Operative Kommunikation der Bundeswehr verortete Analyse- und Bewertungsausstattung stellt für diese Aufgabe die wesentliche technische Unterstützung bereit. Sie befähigt die Bundeswehr zur detaillierten Ursache- und Wirkungsanalyse im Informationsumfeld und zum Planen eigener Informationsaktivitäten. Weiterhin stellt sie ein wirkungsvolles Instrument zur Erkennung von Desinformationskampagnen gegnerischer Kräfte in einem hybriden Umfeld und zur Bereitstellung von Beiträgen zur NATO Strategic Communications sowie deren nationaler Umsetzung dar.

Die Analyse- und Bewertungsausstattung umfasst IT-Werkzeuge zum Monitoring und zur Analyse sozialer Netzwerke, zur Modellierung und Simulation sowie zur strukturierten Datenablage und Zusammenarbeit zwischen stationären und mobilen Elementen.

WIRKEN IM ELEKTROMAGNETISCHEN SPEKTRUM

Ein Kernelement elektronischer Gegen- und Wirkmaßnahmen ist das System HUMMEL 0506 auf Basis des Transportpanzers FUCHS. Das Störsystem hat die Aufgabe, taktischen Truppenfunk sowie gegnerische Mobilfunknetze zu stören oder Täuschmaßnahmen durchzuführen. Das System wurde seit seiner Einführung mehrfach durch Produktverbesserungen und Modernisierungen auf den aktuellen Stand der Funktechnik gebracht, jedoch stoßen solche Maßnahmen inzwischen an ihre Grenzen. Die Nachfolgelösung „Geschütztes System zum Stören gegnerischer Kommunikation" (GeSys SgK) wird die Kräfte des Elektronischen Kampfes künftig befähigen, auf aktuelle sowie auf künftige Bedrohungen im elektromagnetischen Spektrum adäquat reagieren zu können.

Ein Kernelement elektronischer Gegen- und Wirkmaßnahmen ist das System HUMMEL 0506 auf Basis des Transportpanzers FUCHS.
Foto: Bundeswehr/Martina Pump

DIENSTSTELLEN-PROFIL

ZENTRUM CYBER-OPERATIONEN

Im Zentrum Cyber-Operationen (ZCO) werden Cyberoperationen vorbereitet und durchgeführt. Leitmotiv und Selbstanspruch des gesamten Zentrums: „Keiner hört uns, keiner sieht uns, keiner kennt uns."

AUFGABEN

- Planen, Vorbereiten, Führen, Durchführen und Nachbereiten von Cyberoperationen zur **Aufklärung**, um so Beiträge zur Verdichtung des militärischen Lagebildes und zur Warn- und Schutzfunktion der eigenen Truppe sowie Entwicklung von Wirkoptionen als zusätzliche, nichtkinetische Effekte für militärische Führer bereitzustellen.
- Planen, Vorbereiten, Führen, Durchführen und Nachbereiten von Cyberoperationen zur **Wirkung**, um durch den Cyberraum in der realen Welt militärische Effekte zu erzielen und die Handlungshoheit im Cyberraum zu erhalten beziehungsweise zu gewinnen.
- Durchführen simulierter Angriffe auf eigene Systeme, um Sicherheitslücken aufzuzeigen und diese anschließend schließen zu lassen.

AUFTRAG

Die Fähigkeit, Cyberoperationen durchzuführen, ist ein wichtiges Instrument moderner Kriegsführung. Das Zentrum Cyber-Operationen (ZCO) ist die einzige Dienststelle der Bundeswehr, in der die dafür notwendigen hochspezialisierten Fähigkeiten vorhanden sind.

Kernauftrag des ZCO ist das Planen, Vorbereiten, Führen, Durchführen und Nachbereiten von Cyberoperationen zur Aufklärung und Wirkung sowohl im Rahmen der Landes- und Bündnisverteidigung als auch in mandatierten Einsätzen der Bundeswehr. Zusätzlich werden von hier mit Hilfe des Red Teaming die eigenen IT-Systeme der Bundeswehr simuliert angegriffen, um so einen wichtigen Beitrag zur Steigerung der eigenen Informationssicherheit zu leisten. Darüber hinaus kann das Personal aus dem ZCO in akuten Krisenreaktionen flexibel andere Bereiche der Bundeswehr unterstützen.

Um diesem Auftragsportfolio gerecht zu werden, durchlaufen die Angehörigen des ZCO ein anspruchsvolles Auswahlverfahren. Geeignete Bewerberinnen und Bewerber werden im Anschluss im ZCO ausgebildet.

ANSCHRIFT
Tomburg-Kaserne,
Münstereifeler Str. 75,
53359 Rheinbach

DIENSTSTELLENLEITUNG
Oberst Christian Pawlik

AUFSTELLUNG
01.04.2018

CIR-OPERATIONEN

AUTORENTEAM DER ABTEILUNG OPERATION, UNTERABTEILUNG J5/7, KOMMANDO CIR

Die operationelle Ausrichtung des Militärischen Organisationsbereichs Cyber- und Informationsraum orientiert sich an den Erfordernissen des Szenarios der „Landes- und Bündnisverteidigung" im Kontext der gesamtstaatlichen Sicherheitsarchitektur.

Neben der Gestellung von Fähigkeitspaketen zur Unterstützung der Dimensionen Land, See, Luft und Weltraum sowie der Bereitstellung von Unterstützungsleistungen für die gesamten Streitkräfte werden in der Dimension Cyber- und Informationsraum (CIR) eigene Operationen geplant und geführt: CIR-Operationen. Die Planung und Führung dieser CIR-Operationen ist Schwerpunktaufgabe der Abteilung Operation im Kommando CIR. Das Kommando CIR bündelt alle Fähigkeiten der Streitkräfte zur Planung und Führung von Operationen in der Dimension CIR. Kräfte und Mittel des Organisationsbereichs leisten mit CIR-Operationen einen entscheidenden Beitrag für die Landes- und Bündnisverteidigung (LV/BV) und tragen so aktiv zur gesamtstaatlichen Sicherheitsvorsorge bei.

Im Zuge der Neustrukturierung des Organisationsbereichs CIR im Projekt CIR 2.0 wurde mit der Abteilung Operation ein zentrales Element geschaffen, um den geänderten Anforderungen und hier insbesondere der Fokussierung auf die Aufgaben im Kontext der LV/BV Rechnung zu tragen. Künftig werden Aufklärung, Wirkung, Betrieb und Schutz aus einer Hand geplant und geführt. Mit der Bündelung von Kompetenzen wird eine zentrale Entscheidungsebene innerhalb des Kommandos CIR geschaffen, die die nachgeordneten Verbände und Zentren unmittelbar führt und gleichzeitig die Verantwortung für die Operationsplanung und -führung der CIR-Streitkräfte trägt.

Zusätzlich sind auch Situationen denkbar, in denen Fähigkeiten und Fertigkeiten der CIR-Streitkräfte – im Inland – außerhalb eines „klassischen militärischen Einsatzes" benötigt werden. Zwingende Voraussetzung für einen solchen Einsatz im Rahmen der „digitalen Katastrophenhilfe" ist aber, wie in allen CIR-Operationen, die Beachtung des rechtlichen Rahmens für den Einsatz der CIR-Streitkräfte. So unterstützte der Organisationsbereich CIR im August 2021

◀ Mehrwert auf der taktischen Ebene im Szenario der Landes- und Bündnisverteidigung – zum Schutz eigener Kräfte bei der Formung des Gefechtsfelds: EloKa-Kräfte im Zuge der Gewässerüberquerung, hier bei der Übung KÜHNER WETTINER 2021.
Foto: Bundeswehr/Carl Schulze

nach dem Cyberangriff auf den Landkreis Anhalt-Bitterfeld und der erstmaligen Ausrufung des „Cyber-Katastrophenfalls" in Deutschland die dortigen Behörden im Rahmen der Amtshilfe mit IT-Spezialisten.

Es ist unerlässlich, kontinuierliche Aufklärung innerhalb des bestehenden Rechtsrahmens bereits im Frieden durchzuführen. Nur so lassen sich durch den Organisationsbereich CIR Militärisches Nachrichtenwesen aus einer Hand, „J2 Bundeswehr", einzelne Risiken und potentielle wie auch identifizierte Krisengebiete präventiv aufklären, analysieren und entsprechend priorisieren (Kalt- beziehungsweise Warmstartfähigkeit). Die Spezialistinnen und Spezialisten des Militärischen Nachrichtenwesens, der Elektronischen Kampfführung, der Abbildenden Aufklärung, der Aufklärung offen zugänglicher Quellen oder öffentlich zugänglicher und durch das BMVg freigegebener Zielgruppen im Informationsumfeld erfassen und analysieren konstant die Lage. Nach Analyse und Bewertung aller zur Verfügung gestellten Informationen aus eigenen Quellen sowie auch von Partnern stellt der Organisationsbereich CIR in seiner Dimensionsverantwortung ein konsolidiertes Lagebild CIR für das Bundesministerium der Verteidigung (BMVg) und andere Dimensionen zur Verfügung.

Auf Grundlage der kontinuierlichen Aufklärung und der so gewonnenen und zwingend benötigten Vorlaufzeit plant die Abteilung Operation CIR-Operationen, um gezielte Effekte erwirken zu können. Wirken in der Dimension CIR bietet das Potential, gegen die in der Tiefe des gegnerischen Raumes befindlichen, strategisch und operativ wichtigen Ziele zum Einsatz gebracht zu werden, Schwerpunkte schnell zu bilden oder zu verlagern oder eine entscheidende Wirkung zu erzeugen. Diese umfasst das Erzielen von nicht-letalen und reversiblen Folgen im CIR gegenüber allen relevanten Akteuren in militärischen Operationen sowie die zur Vorbereitung erforderlichen Tätigkeiten. CIR-Operationen können aufgrund der Besonderheiten der Dimension CIR eine besonders hohe Relevanz und Reichweite für die gesamte militärische Operationsführung entwickeln. Sie sind entweder Teil von streitkräftegemeinsamen Operationen oder werden eigenständig durchgeführt. Die geforderten Kräfte zur Wirkung im CIR können zeitlich und räumlich mit Land-, Luft-, Weltraum-, See-, und Spezialoperationen harmonisiert bereitgestellt werden.

Der Organisationsbereich CIR trägt mit den IT-Kräften auch die zentrale Verantwortung für den Betrieb der im Einsatz befindlichen IT. In der Rolle „J6 Bundeswehr" stellt der Organisationsbereich CIR damit, gegebenenfalls in Zusammenarbeit mit zivilen Anbietern, auch aus dem Inland heraus die IT-Services im gesamten Aufgabenspektrum der Bundeswehr sicher. Dazu zählen unter anderem die Anbindung der Einsatzgebiete an das Heimatland und die Interoperabilität mit Verbündeten. Die Bereitstellung von IT-Services und der Betrieb des IT-Systems der Bundeswehr durch die mobilen IT-Kräfte, der Betriebsführungseinrichtung IT-System der Bundeswehr und die Koordination der IT-Kräfte aller Dimensionen ist eine wesentliche Daueraufgabe des Organisationsbereichs CIR.

Laufender Schutz durch Herstellung und Aufrechterhaltung der Informationssicherheit ist permanenter und vitaler Bestandteil der Auftragserfüllung in der Dimension CIR. Dazu erfolgt die Synchronisation von CIR-Operationen in enger Abstimmung mit dem Chief Information Security Officer der Bundeswehr (CISOBw). Die Aufgabe der Informationssicherheit wird durch dezentrale Elemente in allen Dimensionen sowie in der Dimension CIR zentral durch das Zentrum für Cyber-Sicherheit der Bundeswehr wahrgenommen.

CIR-Streitkräfte können in Kontingente oder Formationen anderer Dimensionen integriert werden, so ist das Kommando CIR Truppensteller, beispielsweise einer EloKa Taskforce für eine Landoperation. Diese Kräfte können rein unterstützende Aufgaben wahrnehmen, etwa durch den Betrieb eines IT-Systems im Rahmen streitkräftegemeinsamer Unterstützungsleistungen. Sie kommen in CIR-Operationen eigenständig oder als Teil dimensionsübergreifender Operationen zum Einsatz. Charakteristisch ist dabei, dass alle Fähigkeiten der Dimension CIR zu einer Gesamtoperation verknüpft werden können. Hierzu zählt die weltweite und weiträumige Aufklärung, die Operative Kommunikation, die Elektronische Kampfführung, Fähigkeiten für Cyberoperationen und Cyberverteidigung sowie Betrieb und Schutz der IT der Bundeswehr.

▲ Erste Erprobung eines Cyber and Information Domain Teams während der Heeres-Übung ALLIGATOR SWORD 2021, hier bei der Einweisung von Generalleutnant Andreas Marlow, Kommandierender General I. Deutsch-Niederländisches Corps.
Foto: Bundeswehr/Michael Sowa

Eine **CIR-Operation** ist definiert als:
Koordinierter Einsatz von Fähigkeiten der Dimension CIR, der zum Zweck von Aufklärung, Wirkung, Betrieb und/oder Schutz im CIR durch einen militärischen Führer geplant und geführt wird.

Deutsche CIR-Operationen werden dabei in nationaler Verantwortung durch ein sogenanntes Cyber and Information Domain Component Command (CIDCC) geführt.

CIR-Operationen werden immer national auf höchster taktischer Ebene durch das Cyber and Information Domain Component Command (CIDCC) aus dem Kommando CIR heraus aus einer Hand geführt. Lage- und auftragsbezogen können CIR-Operationen aus den anderen Dimensionen heraus unterstützt werden (supported) oder ebendiese unterstützen (supporting). Denkbar ist, in einer frühen Phase vor einer krisenhaften Entwicklung, CIR-Operationen eigenständig und im Zuge der Entwicklung oder Zuspitzung der Lage zusätzlich unterstützend zu „konventionellen" Operationen durchzuführen.

Cyber and Information Domain Component Command
Das CIDCC ist aufgrund der hybriden Bedrohungen und der laufenden CIROp bereits jetzt als „standing HQ" ablauforganisatorisch im KdoCIR ausgebracht. Im Spannungs- und Verteidigungsfall wächst es dann im „Crisis Establishment" (CE) weiter auf und unterstützt die beiden operativen FüKdos als supporting Command.

Es handelt sich somit nicht um ein „Kommando im Kommando", sondern um eine ablauforganisatorische Gliederung von Teilen des Kommandostabes (im Schwerpunkt der Abteilung Operation), die bei Alarmierung entsprechend verstärkt wird.

Bislang existiert das Cyber and Information Domain Component Command lediglich konzeptionell. Im Jahr 2022 wird diese Fähigkeit schrittweise ausgebaut und beübt. Hierzu wird die Übungsserie „Chronos Evolver" etabliert, die als „Testbett" dient, um Planung und Führung von CIR-Operationen im Zusammenspiel der einzelnen Stabselemente miteinander und mit dem nachgeordneten Bereich zu trainieren.

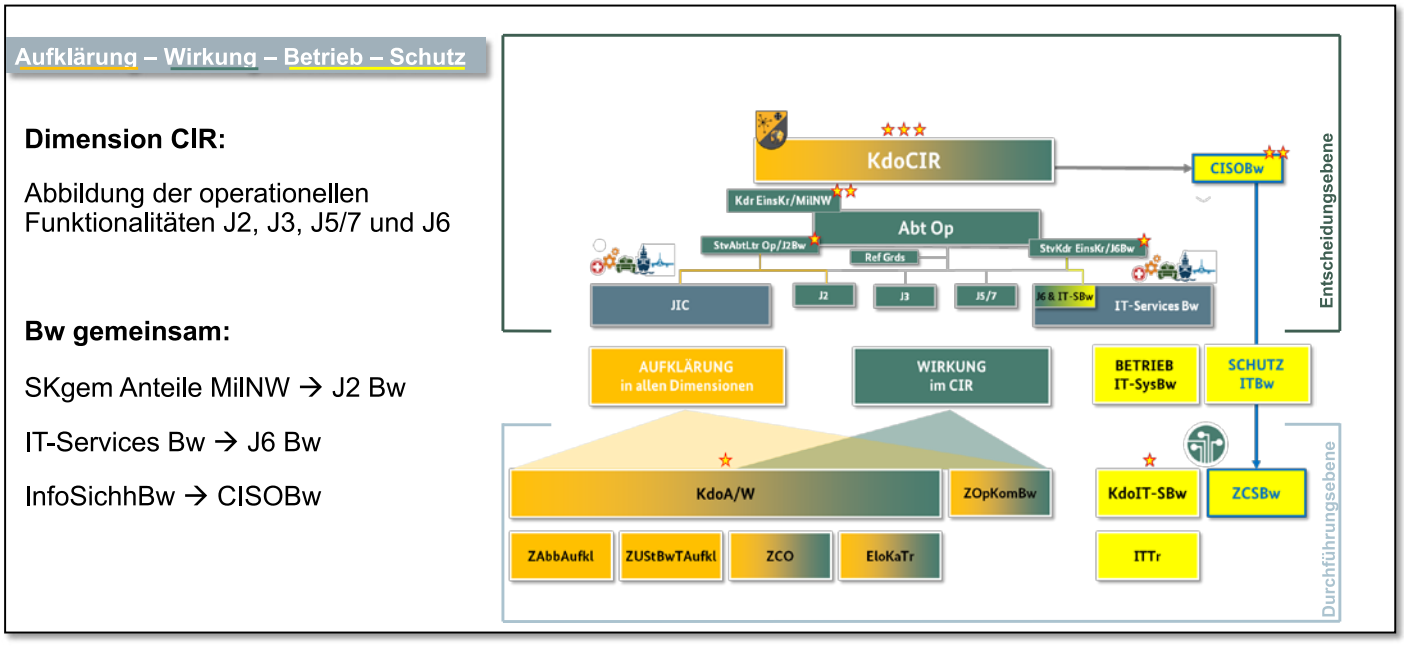
Darüber hinaus werden bedarfsgerechte Cyber and Information Domain Teams (CIDT) bereitgestellt, die CIR-Expertise, insbesondere für CIR-Fähigkeiten aus dem Reachback, zur Unterstützung von Verbänden im gesamten Führungsprozess als ganzheitliche Beratung einbringen. Der Einsatz des CIDT wurde bereits Ende 2021 im Rahmen der Übung „Alligator Sword" geübt. Hierbei wurde das 1. Deutsch-Niederländische Korps durch die Experten des Kommandos CIR beraten.

Cyber and Information Domain Teams (CIDT) sind im Bedarfsfall durch das Cyber and Information Domain Component Command entsandte Beratungs- und Verbindungselemente zu anderen taktischen oder operativen Führungskommandos (z.B. Land Component Command oder Joint Forces Command). Das CIDT berät aktiv im Rahmen der Operationsplanung/ -führung zu ergänzenden Unterstützungsleistungen aus dem Fähigkeitsportfolio CIDCC, insbesondere unter Rückgriff auf die Reachback-Fähigkeiten der Dimension CIR.

Die Abteilung Operation steht damit im Zentrum der operationellen Neuausrichtung des Organisationsbereichs CIR, verantwortet fortan aber auch die streitkräftegemeinsamen Funktionalitäten „J2 Bw und J6 Bw". Die dem Organisationsbereich CIR zugewiesenen bundeswehrgemeinsamen Aufgaben des Militärischen Nachrichtenwesens und des Betriebs zentraler Anteile des IT-Systems der Bundeswehr sind ein wesentliches Standbein und Markenzeichen. So verbunden gewährleisten sie Integrität nach innen und außen. Hierbei ersetzen die zentralen Funktionalitäten „J2 Bw und J6 Bw" nicht die Elemente und Aufgaben in anderen Bereichen der Bundeswehr. Sie ermöglichen vielmehr eine schlanke, auf den Kernauftrag fokussierte Abbildung der Aufgaben und Verantwortlichkeiten, was zu klaren Zuständigkeiten, einem ressourcenoptimierten Einsatz der IT-Kräfte und den Kräften des Militärischen Nachrichtenwesens führt und Doppelstrukturen vermeidet.

Dimensionsübergreifend in den Fokus gerückt ist zudem die stetig zunehmende – auch militärische – Nutzung des Weltraums (siehe auch Seite 144). Die Leistungsbereitstellung im und durch den Weltraum (Aufklärung, Bereitstellung von IT-Services, Geoinformationen) liegt in der Verantwortung der Dimension CIR. Der Organisationsbereich beteiligt sich daher

▼ Aufklärung, Wirkung, Betrieb und Schutz aus einer Hand in der neuen Struktur CIR 2.0.
Grafik: Bundeswehr/KdoCIR



im engen Schulterschluss mit der Luftwaffe am Aufbau des neu aufgestellten Weltraumkommandos der Bundeswehr, um die Nutzung des Weltraums aufrechtzuerhalten, Bedrohungen aus dem Weltraum zu erkennen und diesen aktiv begegnen zu können sowie eine gegnerische Weltraumnutzung zu militärischen Zwecken zu verwehren.

Nicht nur dimensions- sondern auch ressortübergreifend leistet das Kommando CIR aus der Abteilung Operation heraus einen wichtigen Beitrag zur gesamtstaatlichen (Cyber-)Sicherheitsarchitektur Deutschlands, indem das Nationale Cyber-Abwehrzentrum (Cyber-AZ) an entscheidender Stelle personell und fachlich unterstützt wird. Der permanente Informationsaustausch ist unter anderem durch ein Verbindungselement der Abteilung Operation beim Cyber-Abwehrzentrum (siehe auch Seite 106) sichergestellt.

Mit den Möglichkeiten zum Einsatz der CIR-Streitkräfte für Aufklärung, Wirkung, Betrieb und Schutz durch das Cyber and Information Domain Component Command ist die Voraussetzung für die Operationsplanung und -führung in einem digitalisierten, sich ständig wandelnden und unübersichtlichen Umfeld geschaffen. Auf Grundlage einer ständig aktualisierten Analyse der Lage im CIR (Lagebild CIR) stellt der Organisationsbereich CIR seine Fähigkeiten zur Operationsführung sowie gleichermaßen die Unterstützung anderer militärischer Dimensionen sicher und agiert angepasst auf sich kontinuierlich weiterentwickelnde Bedrohungslagen.

SYNCHRONISATION DER **FÄHIGKEITEN UND HANDLUNGSLINIEN**

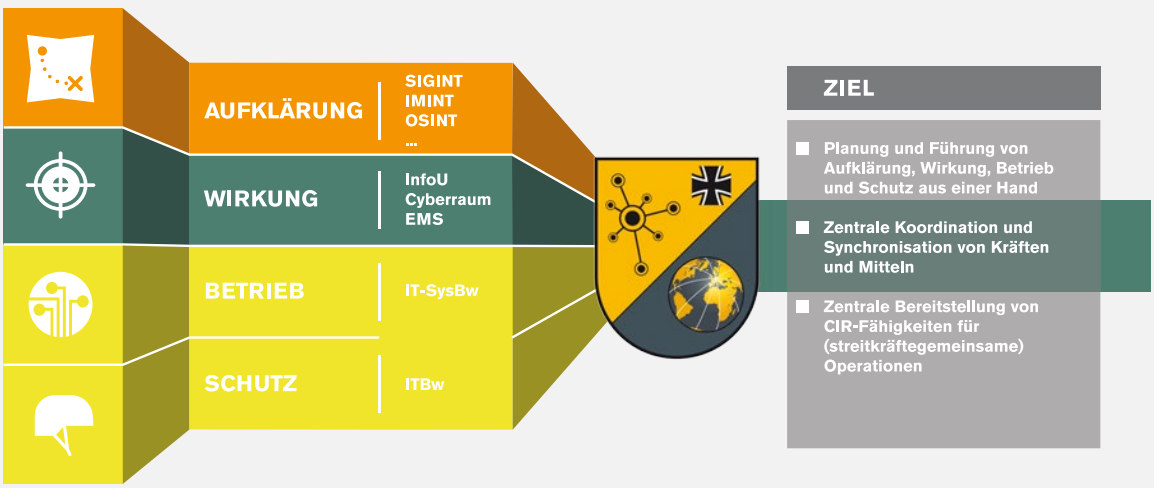
CIR-Operationen in den Bereichen Aufklärung, Wirkung, Betrieb und/oder Schutz werden in nationaler Verantwortung durch CIR-Streitkräfte in der Dimension CIR durchgeführt. Im Rahmen einer CIR-Operation kommen eine oder mehrere Fähigkeiten der Dimension CIR zum Einsatz. In CIR-Operationen werden die Bereiche zu einer Gesamtoperation verknüpft.

Die durch den Organisationsbereich CIR einzubringenden Fähigkeiten sind die streitkräftegemeinsamen Elemente der weltweiten und weiträumigen Aufklärung, die operative Kommunikation, die Elektronische Kampfführung, Fähigkeiten für Cyberoperationen und Cyberverteidigung sowie Betrieb des IT-SysBw und Schutz der IT der Bundeswehr. Diese Fähigkeiten werden aus einer Hand geplant und geführt, um Aufklärung, Wirkung, Betrieb und Schutz in der Dimension CIR bestmöglich sicherzustellen.

▼ Synchronisation der Handlungslinien Aufklärung, Wirkung, Betrieb und Schutz unter Einbeziehung aller CIR-Fähigkeiten. CIR-Operationen werden aus einer Hand geplant und geführt.
Grafik: Bundeswehr/KdoCIR

Für die Bereiche **Aufklärung und Wirkung** lassen sich dabei unterscheiden:

- **Cyberoperationen (CO)** sind Aktionen/Aktivitäten im und durch den Cyberraum mit der Absicht, die eigene Handlungsfähigkeit im Cyberraum zu erhalten, aufzuklären und/oder Wirkungen im Cyberraum zu erzielen.
- **Elektromagnetische Operationen (EMO)** sind Operationen, bei denen das Elektromagnetische Spektrum (EMS) innerhalb eines zu definierenden elektromagnetischen Umfelds (EMU) für offensive und defensive Ziele genutzt oder beeinflusst wird, um Erkenntnisse über die Lage und Absicht potentieller Gegner zu erlangen.
- **Operative Kommunikation/Wirken im Informationsumfeld (InfoU)** ist die Fähigkeit, zielgerichtete Effekte im Informationsumfeld zu erreichen und dazu die Lage im Informationsumfeld auf allen Führungsebenen im Führungsprozess zu erfassen, zu analysieren, zu bewerten und darzustellen sowie darauf aufbauend Informationsaktivtäten zu planen und mit eigenen Mitteln umzusetzen.



DIENSTSTELLEN-PROFIL

ZENTRALE ABBILDENDE AUFKLÄRUNG

Die Dienststelle der Bundeswehr zur Bearbeitung von Satellitenbildern für militärische Aufklärungszwecke. Sie wurde 2013 als Zusammenschluss unterschiedlicher Bereiche der Satellitenbildaufklärung aufgestellt.

AUFGABEN

- Beiträge für die allgemeine Lagebeurteilung, Krisenfrüherkennung sowie Unterstützung der Einsätze der Bundeswehr mit Erkenntnissen der Satellitengestützten Abbildenden Aufklärung,
- Unterstützung der Bundeswehr durch Erfassen, Verifizieren und Erarbeiten von krisenvorsorgerelevanten Daten,
- Aufbereitung und Bereitstellung entsprechender Bildprodukte wie Stadtübersichten, Detailpläne kritischer Infrastruktur und Evakuierungsrouten, deren Ergebnisse als Grundlage für die Planung und Durchführung von beispielsweise Evakuierungsoperationen dienen.

AUFTRAG

Die Zentrale Abbildende Aufklärung (ZAbbAufkl) ist das Auge der Bundeswehr zur Aufklärung aus dem Weltall. Sie steuert für den militärischen Organisationsbereich CIR den Einsatz der Aufklärungssatelliten der Bundeswehr und wertet die gewonnenen Satellitenbilder 24/7 aus. Über 160 Mitarbeitende sind in Spezialverwendungen wie Bildauswertung, Geowissenschaften und IT-Unterstützung sowie klassischen militärischen Stabsaufgaben beschäftigt. Dazu betreibt die ZAbbAufkl heute SAR-Lupe, das erste satellitengestützte Aufklärungssystem der Bundeswehr und zukünftig das Radar-Aufklärungssystem SARah: Ein bildgebendes Radarsatellitensystem, das weltweit tageslicht- und wetterunabhängig höchstauflösende SAR (Synthetic Aperture Radar) -Bilddaten gewinnt, dessen Rohdaten vor Ort aufbereitet werden. Die Erkenntnisse fließen z.B. in das Lagebild „Militärisches Nachrichtenwesen" ein und werden durch weitere Aufklärungsergebnisse ergänzt. In Kooperation mit Frankreich kann die Bundeswehr das Aufklärungssystem Composante Spatiale Optique (CSO) nutzen. Auch Satellitenbilder von kommerziellen Systemen oder Material anderer Quellen, etwa dem European Satellite Centre, werden ausgewertet.

Satelliten können ohne das Verlegen von Truppen weltweit, risikofrei und ohne Verletzung von Hoheitsrechten eingesetzt werden. Die optimale Beauftragung der verschiedenen Systeme und Sensoriken (Radar, elektrooptisch schwarz-weiß und farbig, Infrarot, multispektral) sowie deren bedarfsgerechte Auswertung stellt eine besondere Herausforderung dar. Dies beinhaltet etwa Informationen für die Truppenführung im Einsatz, Beiträge zur allgemeinen Lagebeurteilung oder Krisenfrüherkennung sowie strategische Fragestellungen für das Verteidigungsministerium.

ANSCHRIFT
Philipp-Freiherr-von-Boeselager-Kaserne,
Max-Planck-Straße 17,
53501 Grafschaft

DIENSTSTELLENLEITUNG
Oberst Dirk Gleinig

STAMMPERSONAL
~160

AUFSTELLUNG
01.01.2013

HAUPTMANN ALEXANDRA WEBER,
ABTEILUNG OPERATION, UNTERABTEILUNG J2,
KOMMANDO CIR

Das Militärische Nachrichtenwesen in der Dimension CIR

Einhergehend mit der „Evolution" der Dimensionen – von Land über See und Luft – bis hin zum Weltraum entwickelte sich die Notwendigkeit, Fähigkeiten eines (potenziellen) Gegners in all diesen Bereichen aufzuklären. Die Entwicklung blieb nicht stehen. Der Mensch erschuf neue Infrastrukturen und darauf aufbauend „virtuelle" Räume, die aus der modernen Gesellschaft und Lebensweise nicht mehr wegzudenken sind sowie oftmals sogar deren Rückgrat bilden. Folglich müssen die Streitkräfte in der Lage sein, Vorgänge, Verhalten und Fähigkeiten militärischer Gegner auch im Cyber- und Informationsraum (CIR) aufzuklären.

Die Unterabteilung J2 in der Abteilung Operation des Kommandos Cyber- und Informationsraum (CIR) fungiert als Leitkommando Militärisches Nachrichtenwesen für den Organisationsbereich CIR. Ihr wesentlicher Auftrag ist die Erstellung einer Militärischen Nachrichtenlage für die Dimension CIR. Im Fokus stehen dabei insbesondere die Einsatzgebiete der Bundeswehr, Krisengebiete sowie Länder von besonderem sicherheitspolitischen Interesse für die Bundesregierung.

Hauptaufgaben der Unterabteilung J2 sind die Steuerung der rechtzeitigen und ebenengerechten Deckung des Informationsbedarfs der jeweiligen Bedarfsträger als Grundlage für Entscheidungen sowie die Planung der Aufklärung und Analyse in allen Teilbereichen der Dimension CIR (Cyberraum, Elektromagnetisches Spektrum, Informationsumfeld). Gedeckt wird der Informationsbedarf auf Grundlage von Aufklärungsergebnissen und Erkenntnissen des Militärischen Nachrichtenwesens. Die Aufklärung findet in allen Teilbereichen der Dimension CIR in verschiedenen Aufklärungsdisziplinen statt. So koordiniert die Auswertezentrale Elektronische Kampfführung mit Hilfe ortsfester und mobiler Anteile der vier Bataillone für Elektronische Kampfführung die Signalerfassende Aufklärung (SIGINT). Von der Zentrale Abbildende Aufklärung wird die bildgebende Aufklärung (IMINT) durch Aufklärungssatelliten der Bundeswehr verantwortet. Künftig wird zudem die zentrale Fähigkeit „Open Source Intelligence" (OSINT) als weitere Aufklärungsdisziplin im Organisationsbereich CIR einen Beitrag zur Deckung der Informationsbedarfe des Militärischen Nachrichtenwesens der Streitkräfte leisten.

Darüber hinaus leisten sowohl das Zentrum Cyber-Operationen (ZCO) als auch das Zentrum Operative Kommunikation der Bundeswehr als Teil ihres Kernauftrags jeweils wesentliche Beiträge zu einem gemeinsamen Lagebild im Cyber- und Informationsraum und tragen damit zur Warn-, Schutz- und Informationsfunktion des Militärischen Nachrichtenwesens bei.

Die in der Unterabteilung J2 tätigen Analystinnen und Analysten erarbeiten auf Grundlage der Aufklärungsergebnisse sowie in Abhängigkeit der Lage und den Anforderungen unterschiedlicher Bedarfsträger verschiedene Produkte: der „Intelligence Summary" erscheint als periodische Berichterstattung, fasst die relevanten Ereignisse des betrachteten Zeitraums zusammen und dient der permanenten Aktualisierung des Lagebilds. Mit den „Intelligence Reports" werden anlassbezogen einzelne Aspekte oder besondere Ereignisse vertiefend betrachtet und hinsichtlich ihrer Auswirkungen vor allem auf deutsche Kräfte und Interessen bewertet. Darüber hinaus werden gezielte Fragestellungen in Bezug auf den Cyber- und Informationsraum, sog. „Requests for Information" beantwortet.

Das Joint Intelligence Center (JIC) – als zentrales Element des Militärischen Nachrichtenwesens auf operativer Ebene – nutzt die durch J2 erarbeitete Militärische Nachrichtenlage CIR als Teillage der Dimension, führt sie mit den Teillagen der Dimensionen Land, See, Luft und Weltraum zusammen, und erstellt daraus die streitkräftegemeinsame Militärische Nachrichtenlage. Diese Lagebilder dienen auch als Grundlage für die Planung und Führung von CIR-Operationen durch das Kommando CIR –

innerhalb der Abteilung Operation verantwortet durch die Elemente „Planung und Übung" (J5/7) und „Operationsführung" (J3). Diese Vorgänge verdeutlichen das komplexe Zusammenspiel und die Vernetzung der jeweiligen Funktionen, um Aufklärung, Wirkung, Betrieb und Schutz aus einer Hand sicherzustellen.

In der Unterabteilung J2 sind unter anderem auch die zentrale Fähigkeit OSINT und die Funktion „Intelligence Support to Targeting CIR" beheimatet, die im Folgenden detaillierter vorgestellt werden. Beide Fähigkeiten befinden sich noch im Aufbau und werden den Werkzeugkasten des Militärischen Nachrichtenwesens in der Dimension CIR wesentlich erweitern.

SACHGEBIET „INTELLIGENCE SUPPORT TO TARGETING CIR"

Die Fähigkeit „Intel Support to Targeting" leistet den Beitrag der Dimension CIR zur Zielaufklärung und echtzeitnahen Zielzuweisung. Targeting ist ein Prozess, bei dem legitime militärische Ziele ausgewählt, priorisiert und unter Berücksichtigung der rechtlichen Vorgaben, der operationellen Erfordernisse und Fähigkeiten mit einem bestimmten Effekt belegt werden. Im Unterschied zum konventionellen Verständnis einer physischen beziehungsweise kinetischen Bekämpfung militärischer Ziele müssen diese durch Nutzung des CIR jedoch nicht immer zerstört werden, um den angestrebten Effekt zu erreichen.

Ziel ist es vielmehr, durch Wirkung im Cyberraum, im elektromagnetischen Umfeld oder auch durch Beeinflussung von Verhalten, Einstellungen oder Wahrnehmung von Menschen im Informationsumfeld einen Effekt zu erzielen, der zum beabsichtigten Operationserfolg beiträgt. Unter Umständen reicht dafür schon ein Computer mit Internetverbindung aus.

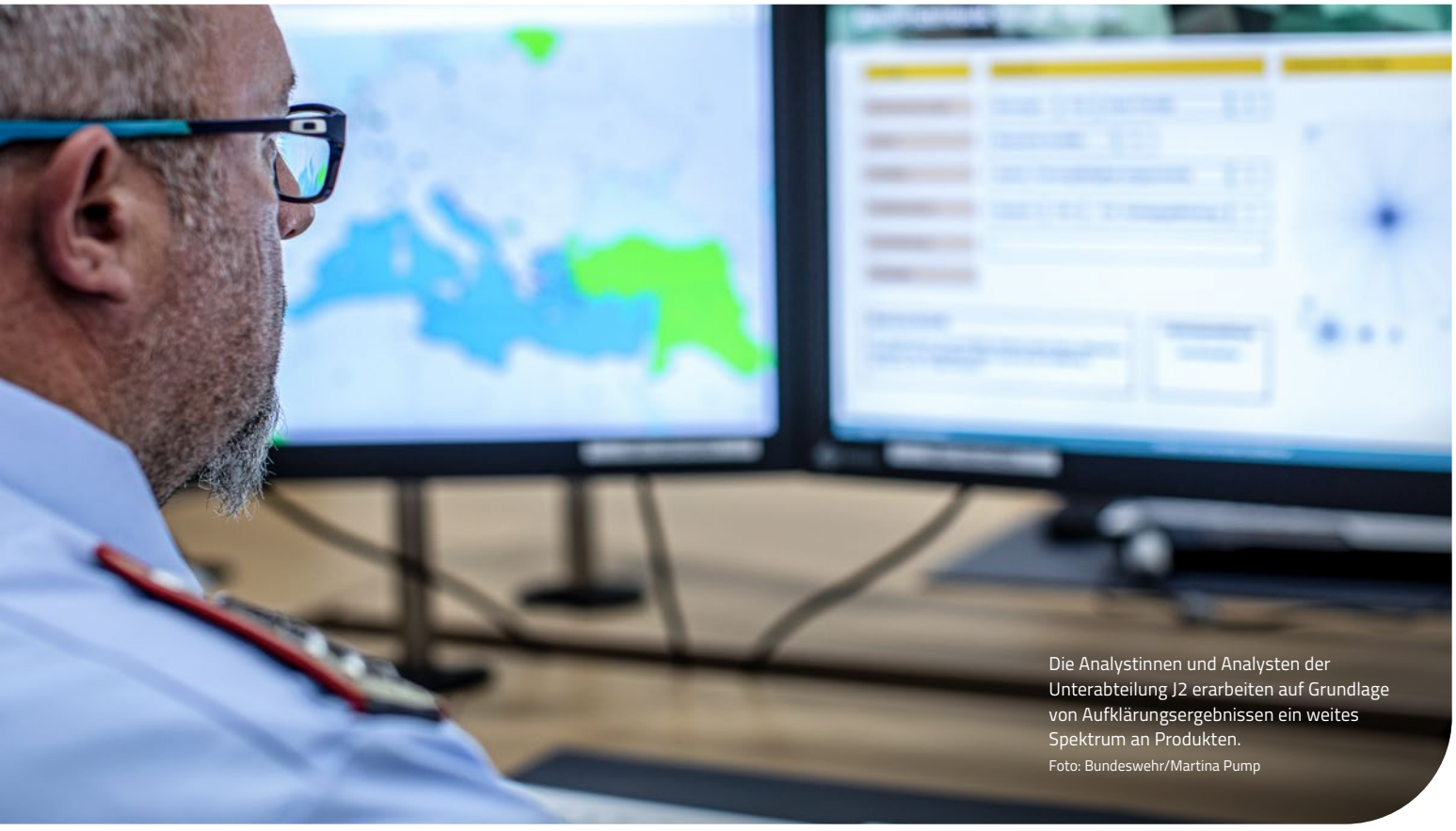
Die intensive und umfassende Aufklärung und Analyse, die dafür nötig ist, gewährleistet in der Dimension CIR die Unterabteilung J2. Ziel ist dabei, dass die bereitgestellten Informationen den Operateuren eine Auswahl an Zielen ermöglichen, damit der Gegner präzise und überraschend an der geeignetsten Stelle getroffen wird, um die im Operationsplan geforderten Effekte zu erreichen.

AUFBAU DER ZENTRALEN FÄHIGKEIT OSINT DER STREITKRÄFTE

Die im Aufbau befindliche Aufklärungsdisziplin „Open Source Intelligence der Streitkräfte" (OSINT SK) gewinnt weltweit Schlüsselinformationen aus frei verfügbaren öffentlichen Quellen. Aus diesen unterschiedlichen Informationen gewinnt speziell ausgebildetes Fachpersonal verwertbare Erkenntnisse und Ergebnisse zur Deckung konkret geforderter Informationsbedarfe.

Diese Quellen können kostenlos, kommerziell, online oder offline, digital wie auch analog sein. OSINT ist somit nicht auf das Internet beschränkt, sondern kann als Quelle auch frei zugängliche Massenmedien nutzen, wie Tages- und Fachzeitschriften, Blogging-Dienste sowie Radio und Fernsehen.

Die Aufklärungsdisziplin OSINT unterstützt das Ziel, den eigenen Streitkräften einen Informationsvorsprung zu verschaffen. Zudem liefert sie einen wertvollen Beitrag im komplementären Ansatz aller Aufklärungsdisziplinen des Militärischen Nachrichtenwesens im gesamten Spektrum von der taktischen bis zur strategischen Ebene. Dies kommt vor allem bei Ad-hoc-Informationsbedarfen oder sich rasch entwickelnden Lageveränderungen zum Tragen.´



Die Analystinnen und Analysten der Unterabteilung J2 erarbeiten auf Grundlage von Aufklärungsergebnissen ein weites Spektrum an Produkten.
Foto: Bundeswehr/Martina Pump

Dabei darf OSINT nicht mit dem durch das Zentrum Operative Kommunikation der Bundeswehr eingebrachten Beitrag zur Erfassung, Analyse und Bewertung des Informationsumfeldes – auch als „Open Source Analysis" (OSA) bezeichnet – verwechselt werden. Während OSINT als Aufklärungsdisziplin die gegnerischen Kräfte und Fähigkeiten im Fokus der Betrachtung hat, liegt der Schwerpunkt bei OSA vielmehr auf den Stimmungsbildern, Wahrnehmungen, Meinungen von Zielgruppen sowie der Bedienung von Narrativen und Propagandamaßnahmen. OSA erfolgt dabei im Schwerpunkt zur Vorbereitung von Effekten durch das Zentrum Operative Kommunikation und liefert im Ergebnis ebenfalls einen wichtigen Beitrag zur Militärischen Nachrichtenlage, stellt aber keine Aufklärungsdisziplin dar.

Obwohl auf den ersten Blick, aufgrund der Nutzung offen und öffentlich zugänglicher Quellen, Gemeinsamkeiten bestehen, unterscheiden sich OSINT und OSA wesentlich hinsichtlich der jeweiligen Bedarfsträger, Inhalte sowie Ergebnisse und sind dementsprechend voneinander abzugrenzen.

Die Referatsgruppe „Zentrale Fähigkeit OSINT der Streitkräfte" in der Unterabteilung J2 bildet zugleich die konzeptionelle Werkbank und den Arbeitsmuskel dieser Aufklärungsdisziplin für die Streitkräfte ab. Die Ausbildung des Fachpersonals OSINT hat im ersten Halbjahr 2022 begonnen, um den Aufbau zu einer Anfangsbefähigung OSINT der Streitkräfte ab 2023 sicherzustellen.

FAZIT

Als integraler Bestandteil der Abteilung Operation im Kommando CIR dient die Unterabteilung J2 innerhalb der geschilderten Fähigkeiten und Verantwortlichkeiten als essentielle Beraterin der Abteilungs- und Kommandoführung in sämtlichen Angelegenheiten des Militärischen Nachrichtenwesens und der Dimension CIR. Sie deckt dabei die Informationsbedarfe der Streitkräfte für die Dimension CIR, steuert die zugewiesenen dimensionsspezifischen Aufklärungsfähigkeiten und bildet damit einen Grundpfeiler für die zukunftsorientierte Ausrichtung des Organisationsbereichs Cyber- und Informationsraum.

▲ Mit der Fähigkeit „Open Source Intelligence" (OSINT) werden Informationen aus frei verfügbaren offenen Quellen weltweit gesammelt und mithilfe entsprechender Analysetools in verwertbare Erkenntnisse und Produkte für das Militärische Nachrichtenwesen überführt.
Grafik: Bundeswehr/KdoCIR

DIENSTSTELLEN-PROFIL

ZENTRALE UNTERSUCHUNGSSTELLE DER BUNDESWEHR FÜR TECHNISCHE AUFKLÄRUNG

Die Zentrale Untersuchungsstelle der Bundeswehr für Technische Aufklärung ist die zentrale Fachkompetenz für die Entwicklung und Untersuchung neuer technischer Aufklärungsfähigkeiten im Aufklärungsspektrum der Bundeswehr.

AUFGABEN

- Untersuchung, Entwicklung, Bereitstellung von Verfahren und prototypischen Labormustern,
- Erfassung, technische Analyse, Auswertung,
- Zusammenarbeit mit nationalen Sicherheitsbehörden.

AUFTRAG

Die Zentrale Untersuchungsstelle der Bundeswehr für Technische Aufklärung (ZU-StelleBwTAufkl) integriert wissenschaftliche Fähigkeiten, technische Fertigkeiten, militärisch technische Analysekapazitäten und die Fähigkeit zur Entwicklung und Untersuchung neuer technischer Aufklärungsfähigkeiten für die Bundeswehr. Durch die Kombination hoch qualifizierter ziviler und militärischer Kompetenz leistet sie einzigartige technisch wissenschaftliche Unterstützung für unsere Streitkräfte. Die ZU-StelleBwTAufkl betreibt als einzige Dienststelle technisch-wissenschaftliche und technische Analysen in der Bundeswehr. Sie untersucht, entwickelt, realisiert und stellt Verfahren und prototypische Labormuster bereit. Die Disziplinen der technischen Aufklärung sind über hoch qualifizierte zivile und militärische Arbeitsplätze abgebildet, auf denen vom erfahrenen militärischen Analysespezialisten über den Elektroniker, Techniker und Meister bis hin zu Ingenieuren, Physikern, Informatikern und Mathematikern eine Vielzahl an Spezialistinnen und Spezialisten im Team eingebunden sind. Diese führen ihre Mess- und Entwicklungsaufgaben im Labor, im kontrollierten Freiraum, auf Übungsplätzen oder aber auch in Einsatzgebieten der Bundeswehr durch.

Die Untersuchungsstelle ist einsatzorientiert und -unterstützend ausgerichtet. Als Bindeglied zwischen technisch-wissenschaftlicher Grundlagenarbeit bis hin zur praktischen Umsetzung der Ergebnisse für den Einsatz der Bundeswehr trägt sie mit ihrem umfassenden Ansatz deutlich zur Erhöhung des Schutzes und der Überlebensfähigkeit deutscher Streitkräfte bei.

ANSCHRIFT
Oberfranken-Kaserne,
Kulmbacher Str. 58-60,
95030 Hof/Saale

DIENSTSTELLENLEITUNG
Oberst Torsten Grefe

STAMMPERSONAL
~450

AUFSTELLUNG
01.04.1996

OBERSTLEUTNANT OLIVER SECKLER UND OBERLEUTNANT PETER LAMATSCH,
DEZERNAT PLANUNG VON WIRKUNGEN IM INFORMATIONSUMFELD,
ABTEILUNG INFORMATIONSUMFELD, ZENTRUM OPERATIVE KOMMUNIKATION DER BUNDESWEHR

DAS INFORMATIONS-UMFELD ALS MILITÄRISCHER HANDLUNGSRAUM

It's all about perception! Die Wahrnehmung militärischen Handelns in einer modernen, schnelllebigen Welt, die durch Smartphones und vielerlei Gadgets gläsern ist, wo Raum und Zeit nachrangig erscheinen und der Faktor Information an Bedeutung gewinnt, entscheidet mit über den Ausgang einer Operation, über Sieg und Niederlage. Das Informationsumfeld muss als Schlüsselgelände verstanden werden!

DER EINSATZRAUM

In allen denkbaren Konfliktformen werden Informationen durch Menschen aufgenommen, auf mannigfaltigen Wegen verbreitet und schließlich in unseren Köpfen verarbeitet. Im Informationsumfeld entstehen Meinungen, Einstellungen und auch die Grundlagen für Verhalten und Handeln. Dies gilt es im eigenen Sinne zu nutzen und einen Gegner gleichermaßen in seinen Handlungsmöglichkeiten einzuschränken.

Es geht darum, die Deutungshoheit über reale wie dargestellte Ereignisse zu erlangen, im Folgenden zu halten und ausgeplante Effekte zu erzielen. Dabei spielt jeder und alles eine Rolle, vom Verhalten des einzelnen Soldaten in der Öffentlichkeit über das Statement eines Kommandeurs bis zum Schuss des Kampfpanzers oder der CIR-Operation aus dem Reachback. All dies erfolgreich zu integrieren und zielgerichtet wie zeitgerecht abrufen zu können, ist die Fähigkeit, die es kontinuierlich bereitzustellen gilt.

Wenn die Wahrnehmung entscheidet, ist auch eigenes Handeln der Gefahr ausgesetzt, rücksichtslos von möglichen Gegenübern ausgenutzt zu werden: Desinformation, Propaganda und bewusstes mediales Ausschlachten von teils vermeintlichen Fehltritten sind ständige Begleiter. Daher ist es umso wichtiger, dass in Einsatzszenarien der Bundeswehr im Zusammenspiel mit ihren Bündnispartnern das Prinzip integrierter Kommunikation angewendet wird – das heißt, die gesamte Organisationskommunikation muss einheitlich, abgestimmt und widerspruchsfrei sein. Eine sogenannte „Say-Do-Gap", also ein Versatz zwischen dem, was ver- und gesprochen wird und dem Charakter unseres Handelns, ist im Informationsumfeld der Moderne nicht tragbar. Einen wesentlichen Bestandteil von militärischen Operationen und stets Kern und Anker eigener Kommunikation bildet daher ein Narrativ, eine prägnante und umfassende Darstellung der Ziele, des Zwecks einer Operation und die Beschreibung des beabsichtigten Weges. Dies ist damit nicht nur bestimmendes Element in der Phase der Planung, sondern muss auch verständlich und passgenau während der Durchführung vermittelt und verkörpert werden.

DIE OPERATIVE KOMMUNIKATION DER BUNDESWEHR

Die Operative Kommunikation der Bundeswehr leistet jene Expertise, die zwingend notwendig ist, um das Informationsumfeld mit seinen speziellen Charakteristika als militärischen Handlungsraum erfolgreich nutzen zu können. Der Auftrag der Operativen Kommunikation der Bundeswehr ist es, zu erkennen, wie im Informationsumfeld gehandelt werden muss, die Truppenführerinnen und -führer der eigenen und verbündeten Streitkräfte bei ihrer Planung und Operationsführung zum Faktor Information zu beraten und damit auch mit eigenen Kräften die für die Operation relevanten Akteure, Themen, Medien sowie Informationssysteme zu beeinflussen.

◀ Boots on the Ground: unmittelbare Unterstützung durch taktische Direktkommunikation.

▼ Autark und aus einer Hand: von der Medienproduktion bis zur Verbringung.
Fotos: Bundeswehr/ZOpKomBw

Am Zentrum Operative Kommunikation der Bundeswehr in Mayen finden sich alle für das Arbeiten am und im Informationsumfeld erforderlichen, teils sehr speziellen Fähigkeiten, an einem Ort. In einem Systemverbund untrennbar miteinander verknüpft, werden hier zwei wesentliche und einzigartige Aufgaben für die Bundeswehr wahrgenommen: Die Bearbeitung der Lage im Informationsumfeld und das Wirken im Informationsumfeld mit eigenen Kräften, Mitteln und Methoden.

DIE LAGEBEARBEITUNG

Um im Informationsumfeld handeln zu können, muss die Bundeswehr in der Lage sein, Akteure, Themen, Medien und Informationssysteme komplexer Systeme zu erkennen. Aus Unmengen von Daten, Beiträgen und Äußerungen gilt es, mit wissenschaftlichen Erhebungsmethoden und teilautomatisiert mithilfe von Künstlicher Intelligenz, auch komplizierte Stimmungslagen sowie Wahrnehmungen zu erfassen und punktgenau aufzubereiten.

Diese Lage im Informationsumfeld wird durch die Dezernate der Abteilung Informationsumfeld erfasst und analysiert. Mit regionalspezifischer Expertise und zukünftig auch mit modernster IT-basierter Analyse- und Bewertungsausstattung sowie mit unseren Regionalteams der Analyse, den Dezernaten Wirkungskontrolle und Propaganda Awareness, wird jenes umfassende Lagebild erstellt, das zum Gesamtlagebild der Bundeswehr beiträgt. Auf dieser Grundlage berät die Operative Kommunikation Truppenführer und Stäbe über alle Führungsebenen hinweg in der Planung und Durchführung ihrer Operationen hinsichtlich möglicher Auswirkungen im Informationsumfeld sowohl von eigenen Informationsaktivitäten als auch den Aktivitäten unserer Gegenüber.

Dadurch entstehen auch die entscheidenden Grundlagen für das eigene Wirken im Informationsumfeld. Dies ist nicht einfach und erfordert besondere Fähigkeiten, da wir uns hier im kognitiven Bereich – sprich zwischen den Ohren – bewegen. Um hier die Aussagen treffen zu können, die das eigene Handeln für eine Zielgruppe passgenau vorbereiten und damit die Wirksamkeit der eigenen Informationsaktivitäten erhöhen, kommen neben unseren militärischen Spezialisten unsere Fachberater aus den Bereichen Soziologie und Psychologie zum Einsatz.

Anhand dieses Lagebildes werden auch die Interkulturellen Einsatzberater der Abteilung befähigt, um zusätzlich zu ihrem außerordentlichen Erfahrungsschatz vor Ort im Einsatzland den zu beratenden Truppenführerinnen und -führern mit tagesaktuellem Wissen beiseite zustehen.

DIE WIRKMITTEL

Im Einsatzbereich Operative Kommunikation finden sich die mobilen Einsatzkräfte in fünf Einsatzstaffeln wieder, die mit ihren Wirkmitteln im Bereich der Massenkommunikation und Direktkommunikation in der Lage sind, unsere Botschaften auf vielfältige Art und Weise zu transportieren und das Umfeld somit im Sinne der eigenen Operationsführung zu beeinflussen. Nahezu autark von fester Infrastruktur einsetzbar, wirken sie mit Massenmedien vom gedruckten Flugblatt über den Podcast bis zur TV-Werbung und durch digitale Direktkommunikation auf gängigen Plattformen und Kanälen. Bei Operationen hoher Intensität wie beispielsweise bei der Landes- und Bündnisverteidigung, liegt der Schwerpunkt der Aktivitäten und Beratungsleistungen darauf, eine unmittelbare Änderung im Verhalten des Gegenübers zu erzeugen. Bei Operationen niedriger Intensität wie bei langfristigen Stabilisierungsoperationen ist beabsichtigt, Einstellung und intrinsischen Willen des Gegenübers zu verändern. Auf den Wechsel zwischen den Intensitäten wie auch deren Parallelität sind die Kräfte der Operativen Kommunikation selbstverständlich vorbereitet.

Zusätzlich zu journalistischen und redaktionellen Mitteln bietet die Operative Kommunikation mit den Kräften der Taktischen Direktkommunikation der Kampftruppe auf den letzten hundert Metern ein effektives Mittel. Diese tief integrierten, hochmobilen Kräfte sind zur unmittelbaren Unterstützung der Kampftruppe auch unter Gefechtsbedingungen befähigt. Durch eine besondere Ausbildung im Bereich Gesprächsführung wirken diese hochspezialisierten Soldaten Face-to-Face und können mithilfe von Lautsprechern auch auf Distanz unmittelbar sichtbare Effekte im Sinne der eigenen Operationsführung erzeugen. Mit dem Schwerpunkt auf Landbasierten Operationen erstreckt sich das Spektrum dabei vom Informieren und Lenken von Menschenansammlungen bis zum Täuschen oder Zermürben eines Gegners.

Die Grundlage des Handelns ist die psychologische Lage der Zielgruppen, die individuell durch Zielgruppenanalysten mit wissenschaftlichen Methoden erarbeitet wird und die zentralen Ansatzpunkte für einen erfolgreichen und zielgerichteten Einsatz eigener Wirkmittel bildet. Sie unterstützen damit Redakteuroffiziere, Medienproduktionsfeldwebel, aber auch die Taktischen Kräfte bei der Gestaltung und Vorbereitung jedes einzelnen Produkts vom Druckerzeugnis über Lautsprecheraufruf bis zum Tweet.

DIE KONTROLLE

Wenn für die Kampftruppe der Grundsatz gilt, dass eine ununterbrochene und lückenlose Gefechtsfeldbeobachtung der Schlüssel zum Erfolg im Kampf ist, so gilt dies auch sinngemäß für das Wirken im Informationsumfeld. Hier kommen Einsatzkameratrupps zum Einsatz, die mit ihren Einsatzdokumentationen die militärische Führung und politische Leitung mit Lageinformationen in Echtzeit versorgen können und damit auch unser eigenes Handeln vor Verzerrung schützen.

▲ Reduktion der Komplexität: Lagebearbeitung des Informationsumfelds durch Expertise und Künstliche Intelligenz.

◀ Medieneinsatz: mobil und flexibel in allen Szenarien.
Fotos: Bundeswehr/ZOpKomBw

Um den unterstützten Truppenteilen und Hauptquartieren eindeutige und präzise Rückmeldung über die Erfolge ihrer Kommunikationsanstrengungen und Wirkungen im Informationsumfeld zu liefern, arbeiten die Kräfte der Taktischen Direktkommunikation, der Zielgruppenanalyse und des Dezernates Wirkungskontrolle eng zusammen. Durch empirische Methoden, von Umfragen über Fokusgruppenbefragungen hin zu digitaler Analyse und natürlich der Auswertung von Lagebeiträgen, kann die Operative Kommunikation eigene geplante Wirkungen beobachten und somit Aussagen zur Zielerreichung treffen. Diese Erkenntnisse liefern unseren Planern und Analysten wertvolle Ansatzpunkte für das weitere eigene Vorgehen und zur Bewertung des Verlaufs der gesamten Operation.

DAS BESONDERE

Die Operative Kommunikation blickt auf mehr als 60 Jahre eigene Geschichte zurück, in der sich Bezeichnungen und Organisationsstrukturen geändert haben, sich aber vor allem das Informationsumfeld als Einsatzraum rasant weiterentwickelt hat. Dies geschieht nach wie vor und erfordert Spezialisten, die hohe militärische Professionalität mit einer teils recht unkonventionellen Herangehensweise und dem Denken out of the box vereinen.

Das Leistungsspektrum der Operativen Kommunikation im Systemverbund zur Bearbeitung der Lage des Informationsumfeldes und zum Erzielen von Wirkung im Informationsumfeld ist breit gefächert: vom abgesessenen Einsatz taktischer Kräfte im Rahmen militärischer Evakuierungsoperationen über die Unterstützung von Großverbänden in landbasierten Operationen über Beiträge zum nationalen Risiko- und Krisenmanagement bis hin zu Teillagen, Dokumentationen und Planungsbeiträgen für die operative Ebene im nationalen und internationalen Umfeld unterstützen die Kräfte des Zentrums Operative Kommunikation der Bundeswehr im gesamten Fähigkeitsspektrum der Streitkräfte.

▼ Aus einer Hand: passgenaue Kommunikation durch Einsatz von Medien.
Foto: Bundeswehr/ZOpKomBw

B&W Cases of Success

MEHR SCHUTZ FÜR DEN CYBER- UND INFORMATIONSRAUM: **TULB-LÖSUNGEN FÜR DIE IT DER TRUPPE**

Der Cyber- und Informationsraum hat keine Wände aus Stahl. Er ist ein sensibles Netzwerk aus Soft- und Hardware, das Informationen generiert, managt, auswertet und verarbeitet. Damit ist er ein potenzielles Angriffsziel – und das nicht nur virtuell.

Bedrohungen für den eigenständigen Organisationsbereich der Bundeswehr sind insbesondere auch physischer Natur. Schnelle Verlegungen, der Einsatz im Feld und die allseits geforderte Mobilität verlangen dem technischen Equipment viel ab. Staub, Regen, Kälte, Hitze, Transport: jede Erschütterung, jeder Stoß kann sensible Radartechnik, Funk- und IT-Systeme beschädigen oder außer Gefecht setzen. Was bedeutet: damit moderne Aufklärungs- und Kommunikationssysteme selbst unter härtesten Belastungen ihren Dienst tun, ist ihr Schutz von zentraler Bedeutung.

Die Einsatzbereitschaft in der Dimension CIR hängt folglich entscheidend davon ab, ob passende Transport- und Lagerbehälter (TuLB) verfügbar sind, die Rüstzeiten beschleunigen, das Equipment schützen und zugleich leicht zu handhaben sind.

MOBILITÄTSLÖSUNGEN NACH NATO-STANDARDS

Als Industriepartner der Streitkräfte hat der Spezialkofferhersteller B&W International hochmobile, flexible Schutzlösungen für IT-Systeme entwickelt. Diese Mobilitätslösungen erfüllen von Haus aus die militärisch relevanten Zertifizierungen STANAG 4280, DEF STAN 81-41, ATA 300 und MIL-STD 810 H zur Nutzung als Transport- und Lagerbehälter. Garantiert wird nicht nur der zuverlässige Schutz vor dem Eindringen von Staub und Wasser nach der IP67-Zertifizierung. Erfüllt werden außerdem die strengen Anforderungen der UN-Spezifikationsverpackungen 3480 und 3481 sowie 3090 und 3091. Grundsätzlich entsprechen B&W Militärschutzkoffer den Standards von Streitkräften der NATO, der US Air Force und der US Navy.

Weltweit einzigartig sind B&W-TuLB aus PP, die für den Transport von Lithium-Ionen-Akkus entwickelt worden sind. Sie tragen das UN-Zertifikat 4H2, das den Transport von gefährlichem Frachtgut wie Hochleistungsbatterien, die explodieren oder Feuer fangen können, sogar im Flugzeug erlaubt. Eine Lösung, mit der sogar defekte Batterien gefahrlos transportiert werden können, befindet sich gerade in der Zulassungsphase.

ZERTIFIZIERTE LÖSUNGEN FÜR DEN TRANSPORT VON LITHIUM-IONEN-AKKUS

„Mit der Entwicklung von Schutzkoffern, die der 4H2-Gefahrgutnorm entsprechen, haben wir bestehende Transportprobleme in Zusammenarbeit mit Streitkräften aus der Welt geschafft", sagt Dirk Uhlenbrock, geschäftsführender Gesellschafter von B&W International.

Die Stärke dieser Innovation liegt darin, dass sie Militärtechnik und Logistik in einem System zusammenführt. „Plug & Protect" nennt B&W International diese Form sofort einsatzbereiter, smarter Transportlösungen, die speziell für den Verteidigungs- und Überwachungseinsatz entwickelt wurden. Mehr als 200 solcher Lösungen werden bereits von Streitkräften und der Rüstungsindustrie in allen militärischen Anwendungsbereichen genutzt.

▼ Für die schnelle Kaltstartfähigkeit konzipiert: TuLB´s von B&W International gehören zum Rüstzeug der Streitkräfte.
Foto: B&W International

KONTAKT:
B&W International GmbH
Ansprechpartner: Dirk Uhlenbrock
dirk.uhlenbrock@b-w-international.com
Tel. +49 (0)5451/8946-120
www.b-w-international.com

Die Elektronische Kampfführung ist bereits seit Jahrzehnten ein elementarer Bestandteil in militärischen Szenarien aller Intensitäten.
Foto: Bundeswehr/Broschinsky

HAUPTMANN STEFFEN WERNER, ELOKA FACHDIENSTOFFIZIER, VERANTWORTLICH FÜR DEN STÄNDIGEN AUFKLÄRUNGSAUFTRAG UND DIE FACHLICHE AUSBILDUNG DER SOLDATEN, ELOKA-BATAILLON 932 UND NEBENAMTLICHER PRESSEOFFIZIER

DIE ELOKA TASKFORCE FÜR DIE VJTF L 2023

Die Elektronische Kampfführung (EloKa) ist auf dem modernen Gefechtsfeld im Kampf um Informationsüberlegenheit von immenser Bedeutung. Die Kräfte des Elektronischen Kampfes stellen sprichwörtlich die „Ohren" und „Blitze" des eingesetzten Truppenkontingents dar. Dieser Bedeutung für die Kräfte der NATO Response Force (NRF), der schnellen Eingreiftruppe der NATO, Rechnung zu tragen, ist Aufgabe der EloKa Taskforce.

GRUNDSATZ

Die Elektronische Kampfführung ist bereits seit Jahrzehnten ein elementarer Bestandteil in militärischen Szenarien aller Intensitäten. Mit Aufstellung des Kommandos Cyber- und Informationsraum (CIR) wurde diese Fähigkeit zur Aufklärung und Wirkung gemeinsam mit den übrigen Fähigkeiten des Organisationsbereichs Cyber- und Informationsraum zusammengeführt. Die Elektronische Kampfführung operiert grundsätzlich in die zwei Handlungsfelder Aufklärung („Ohren") und Wirkung („Blitze").

Im Bereich der Aufklärung werden Informationen durch Auswertung von gegnerischen Signalen und Sendern jeglicher Art gewonnen, aufbereitet und den militärischen Bedarfsträgern für die weitere Operationsplanung ausgewertet zur Verfügung gestellt. Dies erfolgt in einem engen Zusammenspiel zwischen den in die Truppe integrierten Kräften der EloKa sowie den rückwärtigen Auswerte- und Analysekapazitäten der EloKa, zum Beispiel der Auswertezentrale; gemeinsam bringen sie einen wesentlichen Mehrwert für die eingesetzte Truppe.

Im Bereich Wirkung kann die EloKa durch gezielte elektronische Gegenmaßnahmen direkt gegen gegnerische Einrichtungen und Einheiten wirken. Hier können zum Beispiel Funkstörsender Kommunikationswege unterbrechen oder mit Täuschsignalen gezielte Irritationen in den gegnerischen Reihen erzeugt werden.

DER READINESS ACTION PLAN – WEG ZUR GLAUBWÜRDIGEN ABSCHRECKUNG UND WIRKSAMEN LANDES- UND BÜNDNISVERTEIDIGUNG

Der auf dem Wales-Gipfel 2014 vereinbarte Readiness Action Plan (RAP) war ein wesentlicher Meilenstein der militärischen Anpassung der NATO an das verändernde und sich entwickelnde Sicherheitsumfeld. Er leitete die bedeutendste Verstärkung der kollektiven Verteidigung der NATO seit dem Ende des Kalten Krieges ein. Der RAP umfasst militärische Aktivitäten im östlichen Teil des Bündnisses („Assurance Measures") wie beispielsweise die Truppenkontigente enhanced Forward Presence (eFP) sowie Maßnahmen der Luftraumüberwachung im Rahmen von Air-Policing. Der Bedarf für eine erhöhte Reaktionsfähigkeit der NATO auf internationale Krisen und Bedrohungen führte zu einer verstärkten und reaktionsfähigen NRF im Rahmen von Anpassungsmaßnahmen, den „Adaptation Measures".

ADAPTATION MEASURES

Anpassungsmaßnahmen sind längerfristige Änderungen an den Streitkräften und der Kommandostruktur der NATO, welche die Fähigkeit des Bündnisses verbessern, schnell und entschieden auf plötzliche Krisen zu reagieren, unabhängig davon, wo diese entstehen.

Ein Ziel dieser Maßnahmen war, die Reaktions- und Leistungsfähigkeit der NATO Response Force zu verbessern. Im Jahr 2015 hat sich die Größe der NRF von 13.000 auf etwa 40.000 Soldaten mehr als verdreifacht. Diese erweiterte NRF umfasst Land-, See-, Luft-, CIR-Kräfte und Spezialeinheiten.

Weiter wurde die NRF-Struktur um ein Element erweitert: den schnellen, einsatzbereiten Eingreifverband, die „Spearhead Force" genannte Very High Readiness Joint Task Force (VJTF).

Die NATO hält im Rahmen der enhanced NATO Response Force (eNRF) Kräfte vor, um schnell auf krisenhafte Entwicklungen reagieren zu können. Teil davon ist die Speerspitze Very High Readiness Joint Task Force Land (VJTF L), die innerhalb einer sehr kurzen Reaktionszeit von fünf bis sieben Tagen verlegen kann. Dieses Kräftedispositiv umfasst circa 20.000 Soldaten und Soldatinnen, davon etwa 5.000 bei den Bodentruppen.

Deutschland stellt 2023 die Rahmennation der VJTF L, die im Kern aus einer verstärkten, multinationalen Panzergrenadierbrigade besteht. Kräfte, die im Rahmen der VJTF L 2023 eingesetzt werden, sind grundsätzlich von 2022 („Stand-Up" als Initial Follow-on Forces Group mit Reaktionszeit 45 Tage) bis 2024 („Stand-Down" als Initial Follow-on Forces Group mit Reaktionszeit 30 Tage) gebunden. Die Bereitschaft wird mit dem 31. Januar 2025 (Nachlaufphase) enden.

Die VJTF- und NRF-Elemente bleiben in ihren Heimatländern stationiert, können aber von dort aus überall in Übungen oder zur Krisenreaktion eingesetzt werden. Führung und Zusammensetzung der VJTF und NRF wechseln jährlich. Für das Jahr 2023 wird Deutschland, nach 2019 erneut, die Führung übernehmen. Der Panzergrenadierbrigade 37 aus Frankenberg (Sachsen) wird dazu vom Organisationsbereich CIR unter anderem eine EloKa Taskforce beigestellt, die für die Brigade den Elektronischen Kampf führt.

DIE ELOKA TASKFORCE

Um eine Electronic Warfare Taskforce (EWTF) für NRF 2022 bis 2024 aufzustellen, müssen die verschiedenen mobilen Systeme und Fähigkeiten aus dem Bereich Aufklärung und Wirkung interoperabel zusammengeführt werden. Daher setzt sich die EWTF aus den vier EloKa-Verbänden 911 in Stadum, 912 in Nienburg, 931 in Daun – und als EloKa-Leitverband 932 in Frankenberg (Eder) – zusammen.

In der EloKa Taskforce sind 220 Soldatinnen und Soldaten aus mindestens 14 Einsatzkompanien dieser vier Standorte zusammengefasst, die unter der Führung einer Kompanie des Bataillons Elektronische Kampfführung 932 üben und dann gemeinsam in die Bereitschaftsphase übergehen. Die Soldaten und Soldatinnen haben insgesamt über 80 Fahrzeuge mit verschiedensten Sensoren und Systemen zur Verfügung, um ihren Auftrag durchzuführen. In über zehn Übungen, von reinen Stabsrahmenübungen auf dem Papier bis hin zu Volltruppenübungen auf Truppenübungsplätzen oder freilaufend in Deutschland mit allen Soldatinnen und Soldaten, Fahrzeugen und Material, hat sich die EloKa Taskforce auf ihren Auftrag vorbereitet. Dabei wurden vor allem der Wandel der sicherheitspolitischen Lage und der neue Schwerpunkt auf die Landes- und Bündnisverteidigung miteinbezogen.

LANDES- UND BÜNDNISVERTEIDIGUNG

Das Hinwenden zur Landes- und Bündnisverteidigung bedeutet die teilweise Abkehr von Einsatzgrundsätzen der letzten zwei Dekaden und das Wiederaufgreifen bewährter Grundsätze der EloKa, ergänzt um hybride Elemente und an digitalisierte Einsatzumgebungen angepasst. Diese Grundsätze zu beüben und teils neu zu erarbeiten, ist in den letzten Monaten Hauptaufgabe des federführenden Verbandes in Frankenberg (Eder) gewesen. In den Übungen wurde die Erkennung und Ortung von Fernmelde- und Radarstellungen, noch vor der Auswertung von Inhalten, im Gefechtsstreifen abgebildet. Stetes Augen- und „Ohren"merk auf Ausrüstung und Verfahren möglicher gegnerischer Kräfte schafft dafür die Grundlagen.

Eine wesentliche Führungsleistung ist es, die EloKa-Fähigkeiten mit eigenständig abgesetzt operierenden Kräften in einem systemischen EloKa-Verbund taktisch so einzusetzen, dass sie im Aufklärungs- und Wirkungsverbund der Landstreitkräfte Lagebeiträge sowie dem Operationsverlauf angepasste Störwirkung bereitstellen können. Dabei sind physikalische Gesetzmäßigkeiten mit taktischen Einsatzgrundsätzen in Einklang zu bringen.

In Zukunft wird die Inhaltsauswertung im digitalen Gefechtsfeld und im hochdynamischen Gefecht eine nur untergeordnete Rolle spielen. Digitale Signale erfordern zuvorderst eine technisch-betriebliche Sofortauswertung, also das verstärkte Befassen mit Metadaten, sodass bereits der „Erfasser als der erste Auswerter" fungiert. Während der zurückliegenden Übungen konnten äußerst gewinnbringende Erfahrungen in der Zusammenarbeit der Systeme und im Auswerteprozess erprobt werden. Die strategische Sicherheitslage an der NATO-Nordostflanke führt dabei täglich den Ernst der Lage vor Augen.

▼ Um eine Electronic Warfare Taskforce (EWTF) für NRF 2022 bis 2024 aufzustellen, müssen die verschiedenen mobilen Systeme und Fähigkeiten aus dem Bereich Aufklärung und Wirkung interoperabel zusammengeführt werden. Gut getarnt: Teile der EloKa Taskforce.
Foto: Bundeswehr/Steffen Werner

DIENSTSTELLEN-PROFIL

KOMMANDO INFORMATIONS-TECHNIK-SERVICES DER BUNDESWEHR

Das Kommando Informationstechnik-Services der Bundeswehr erfüllt als dem Kommando Cyber- und Informationsraum (CIR) nachgeordneten Kommando im Organisationsbereich Cyber- und Informationsraum streitkräfte- und bundeswehrgemeinsam ausgerichtete Aufgaben der Bereitstellung von IT-Services.

AUFGABEN

- Truppendienstliches Führen der unterstellten Verbände und Dienststellen und Bereitstellen einsatzbereiter Kräfte.
- Bereitstellen von IT-Services für die Bundeswehr und Gewährleisten der Führungsfähigkeit der Bundeswehr und Streitkräfte im Einsatz.
- Gewährleisten des sicheren Betriebs des IT-Systems Bundeswehr zur Aufrechterhaltung der Kernführungsfähigkeit im Bereich der bundeswehrgemeinsamen IT-Services.
- Bereitstellung von Kräften und Mitteln der streitkräftegemeinsamen stationären und verlegefähigen IT-Unterstützung für Ausbildung, Übung und Einsatz.
- Planen, Überwachen und Steuern der stationären und verlegefähigen Anteile des IT-SysBw für LV/BV, Dauereinsatzaufgaben, Einsätze, Missionen, Einsatzgleiche Verpflichtungen, Nationales Risiko- und Krisenmanagement, Übungen und Grundbetrieb.

AUFTRAG

Das Kommando Informationstechnik-Services der Bundeswehr (KdoIT-SBw) nimmt die Verantwortung für Einsatz und Betrieb des IT-Systems Bundeswehr (IT-SysBw) – im Sinne der Einhaltung und Umsetzung der durch den IT-Process Owner vorgegebenen Richtlinien und Standards als Prozessmanager Informationstechnik Serviceprovider – wahr. Im Auftrag des Kommandos CIR vertritt es die betrieblich-operativen Interessen der Bereitstellung von IT-Services in der Bundeswehr.

Das KdoIT-SBw stellt die Kräfte und Mittel der streitkräftegemeinsamen stationären und verlegefähigen IT-Unterstützung für Ausbildung, Übung und Einsatz bereit und stellt so den sicheren Betrieb des IT-SysBw zur Aufrechterhaltung der Kernführungsfähigkeit im Bereich der bundeswehrgemeinsamen IT-Services sicher. Dazu plant, überwacht und steuert das Kommando weltweit die stationären und verlegefähigen Anteile des IT-SysBw, in enger Abstimmung mit der BWI GmbH, für Landes- und Bündnisverteidigung (LV/BV), Dauereinsatzaufgaben Einsätze, Missionen, Einsatzgleiche Verpflichtungen, Nationales Risiko- und Krisenmanagement, Übungen und Grundbetrieb im Auftrag des Kommandos CIR.

ANSCHRIFT
Tomburg-Kaserne,
Münstereifeler Straße 75,
53359 Rheinbach

DIENSTSTELLENLEITUNG
Brigadegeneral Jörg Rüter

STAMMPERSONAL
~750

AUFSTELLUNG
01.04.2023

OBERST I.G. NICOLAS VON THADEN, VERANTWORTLICHER STABSOFFIZIER JIC-POLICY

Die streitkräftegemeinsamen Aufgaben des **Joint Intelligence Center** (JIC)

WARUM BRAUCHT MAN EIN LAGEBILD?

Unabhängig von sich wandelnden Konfliktszenarien und weitreichender hybrider Einflussnahme gilt auch heute unverändert, dass jedem militärischen Führer ein umfassendes Lagebild zur Verfügung stehen muss, um zur richtigen Zeit zweckmäßige Entscheidungen treffen zu können, die hohe Aussicht auf Erfolg haben.

Im Militärischen wie auch im Zivilen werden Entscheidungen auf der Basis einer Lagefeststellung getroffen. Hierzu gehört die Erfassung der Situation unter Berücksichtigung aller Einflussfaktoren, zum Beispiel der Frage, welche Kräfte und Mittel zur Verfügung stehen oder dem eigenen Handeln entgegenwirken.

Das Ziel ist in der Absicht der übergeordneten Führung beschrieben, aus welcher der eigene Auftrag abgeleitet wird. Zum Erreichen dieses Ziels werden eigene Kräfte und Mittel eingesetzt. Das lässt sich knapp und deutlich formulieren; die zur Verfügung stehenden Mittel lassen sich aus den Kräften und Wirkmitteln im Raum ebenfalls leicht ermitteln. Komplexer stellt sich die Beurteilung der Lage gegnerischer Kräfte dar, da die benötigten Informationen oftmals nicht direkt zugänglich sind.

Ein Lagebild kann unmöglich von einer Einzelperson in kurzer Zeit erfasst, geschweige denn bewertet werden. Hierzu bedarf es Fachpersonals, synchronisierter Arbeitsabläufe und -verfahren sowie darüber hinaus geeigneter Strukturen. Mit den Informationen über potentielle Gegner befassen sich in der Bundeswehr die Kräfte des Militärischen Nachrichtenwesens. Es muss deutlich gesagt werden: ohne Lagebild sind wir „blind". Fehlt ein Lagebild der gegnerischen Kräfte, agieren wir ins Leere und unsere Chancen auf Erfolg sind fraglich.

„Wenn Du Dich und den Feind kennst, brauchst Du den Ausgang von hundert Schlachten nicht zu fürchten. Wenn Du Dich selbst kennst, doch nicht den Feind, wirst Du für jeden Sieg, den Du erringst, eine Niederlage erleiden. Wenn Du weder den Feind noch Dich selbst kennst, wirst Du in jeder Schlacht unterliegen."

Sun Tsu, Die Kunst des Krieges, um 500 v. Chr.

ÜBERGANG ZUM JIC

Das JIC ging aus der Stabsabteilung J2 des Kommandos Strategische Aufklärung hervor, die bereits mit zentralen Koordinierungskompetenzen innerhalb des Militärischen Nachrichtenwesens ausgestattet war. Im Jahr 2020 wurde das JIC ablauforganisatorisch aufgestellt. Der Erprobungsbetrieb begann im Mai desselben Jahres. Die Initial Operational Capability (IOC) wurde zwei Monate später hergestellt. Mit Einnahme der Arbeitsgliederung CIR 2.0 erfolgte im Sommer 2021 die truppendienstliche Unterstellung unter die Abteilung Operation. Mit Einnahme der gebilligten Organi-

Auftrag des JIC –
Das Joint Intelligence Center

- steuert den Teilbereich Nachrichtenmanagement in den Streitkräften und erstellt auf Basis der Teillagen der Dimensionen eine streitkräftegemeinsame, bewertete Militärische Nachrichtenlage in aufgabenteiliger Kooperation mit ressortübergreifenden Partnern,
- steuert in der Funktion des National Collection Managers den Teilbereich Joint Intelligence, Surveillance and Reconnaissance in den Streitkräften,
- koordiniert im Auftrag des Bundesministeriums der Verteidigung die Zusammenarbeit und den Informationsaustausch des Militärischen Nachrichtenwesens über Schnittstellen mit den nationalen Akteuren des Systems Militärisches Nachrichtenwesen und internationalen Partnern.

◀ Ein Lagebild kann unmöglich von einer Einzelperson in kurzer Zeit erfasst, geschweige denn bewertet werden.
Foto: Bundeswehr/Yvonne Albert

sationsstruktur zum 1. Oktober 2022 wurde dann die volle Einsatzfähigkeit, die Full Operational Capability (FOC), erreicht.

Das JIC ist das zentrale Element der Leistungserbringung des Militärischen Nachrichtenwesens auf der operativen Führungsebene. Im Auftrag des Bundesministeriums der Verteidigung (BMVg) nimmt das JIC Kernaufgaben des Militärischen Nachrichtenwesens wahr. Es steuert unter fachlicher Führung des BMVg die Teilbereiche Nachrichtenmanagement und Joint Intelligence, Surveillance and Reconnaissance (JISR) in den Streitkräften und koordiniert die Zusammenarbeit und den Informationsaustausch des Militärischen Nachrichtenwesens mit den nationalen Akteuren des Systems Militärisches Nachrichtenwesen sowie mit internationalen Partnern. Zudem erstellt das JIC die streitkräftegemeinsame, bewertete Militärische Nachrichtenlage. Mit dem JIC sind die Steuerungsbefugnisse Nachrichtenmanagement und JISR innerhalb der Bundeswehr erstmals einer einzigen zentralen Stelle übertragen

„Mit dem Worte Nachrichten bezeichnen wir die ganze Kenntnis, welche man von dem Feinde und seinem Lande hat, also die Grundlage aller eigenen Ideen und Handlungen."

Carl von Clausewitz, Vom Kriege, Erstes Buch, Sechstes Kapitel: Nachrichten im Kriege, 1832

◀ Zur Deckung der Informationsbedarfe bezieht das JIC sämtliche Ebenen innerhalb der Bundeswehr sowie nationale und internationale Partner ein. Foto: Bundeswehr/Yvonne Albert

worden, sodass hier die Kräfte und Mittel des Militärischen Nachrichtenwesens aller militärischen Organisationsbereiche der Bundeswehr streitkräfteweit und „komplementär" mit Partnern in diesem System zusammenarbeiten, eben „joint".

Um Planungen und Entscheidungen auf allen Führungsebenen ebenso gezielt wie auch fundiert vorbereiten zu können, herrscht im Militärischen Nachrichtenwesen ein stetiger Informationsbedarf. Informationsbedarfsforderungen, die von den militärischen Organisationsbereichen, der operativen Führungsebene (Einsatzführungskommando der Bundeswehr, Nationaler Territorialer Befehlshaber) sowie nationalen Partnern ausgehen, erfahren im JIC eine Priorisierung. Weiterhin werden dort die Informationsbedarfsforderungen zusammengeführt, aufbereitet und zur Beantwortung an die zuständigen Stellen innerhalb und außerhalb der Bundeswehr weitergeleitet.

Durch die Bereitstellung von Teillagen bringen die Leitkommandos des Militärischen Nachrichtenwesens auf der taktischen Ebene ihre spezifische Expertise in das Nachrichtenwesen ein, ebenso wie die Führungskommandos der operativen Ebene. Auf dieser Grundlage wird die streitkräftegemeinsame, bewertete Militärische Nachrichtenlage durch das JIC erstellt. Diese wird bedarfsgerecht auf die militärischen Führungsebenen zugeschnitten. Übergeordnetes Ziel ist, dass jeder Bedarfsträger die Informationen erhält, die er zur Erfüllung seines Auftrages benötigt.

Das JIC umfasst den Anteil „Intelligence Requirements Management & Collection Management" (IRM & CM), der die oben genannte Steuerungsfunktionen wahrnimmt. Hierzu gehört auch das „National Watch Center" (NWC), welches eine dauerhafte (24/7) Ansprechbarkeit für das System Militärisches Nachrichtenwesen gewährleistet und darüber hinaus

Das **System Militärisches Nachrichtenwesen** ist das um ressortinterne, ressortübergreifende und internationale Schnittstellen erweiterte **Militärische Nachrichtenwesen**. Im Letzteren agieren

- das **Bundesministerium der Verteidigung** auf der **militärisch-strategischen**,
- das **Joint Intelligence Center**, das **Einsatzführungskommando der Bundeswehr** und der **Nationale Territoriale Befehlshabe**r auf der **operativen**, und
- die **Leitkommandos Militärisches Nachrichtenwesen** auf der **taktischen Ebene**.

den nationalen Beitrag zum „NATO Allied Command Operations Indications and Warning Construct" leistet, einer Art Frühwarnorganisation des Bündnisses. Mit dem Anteil „Production" stellt das JIC die Lagebearbeitung und Analyse sicher.

Die Erstellung des Lagebildes liegt in der Hand der Fachkräfte. Nach Regionen gegliedert werden die durch Aufklärungssensoren gewonnenen Informationen im Bereich der Lagebearbeitung aufbereitet, analysiert und miteinander verknüpft. Sie ergeben so nach und nach ein immer umfassenderes Gesamtbild – bestehend aus geographischen und kulturellen Gegebenheiten, ausgewerteten Daten zu den Potentialen von Streitkräften oder anderen bewaffneten Akteuren und erkannten Stimmungstendenzen – mit dem Ziel der Bereitstellung von ebenengerechten Informationen an den Bedarfsträger. Für eine korrekte Einordnung ist eine fehlerlose Analyse wesentlich.

Das **JIC** steuert das Militärische Nachrichtenwesen (MilNW), ist das operative Zentrum des MilNW, stellt so die Integrität des MilNW sicher und ist zudem Ausdruck der streitkräftegemeinsamen Identität des MilNW.

Zur Deckung der Informationsbedarfe bezieht das JIC sämtliche Ebenen innerhalb der Bundeswehr sowie nationale und internationale Partner ein. Diese Form der Kooperation hat sich insbesondere bei der Planung und Koordination von Auslandseinsätzen oder einsatzgleichen Verpflichtungen bewährt und wird dies auch im Rahmen der Landes- und Bündnisverteidigung tun.

ZUSAMMENFASSUNG UND AUSBLICK

Zusammenfassend stellt das JIC das zentrale Element der Leistungserbringung des Militärischen Nachrichtenwesens auf der operativen Führungsebene dar, welches die Integrität desselben sicherstellt. Gleichermaßen geht dies mit beachtlichen Herausforderungen einher. Um Informationsbedarfe auf sämtlichen Führungsebenen der Bundeswehr zu decken und das Steuern von Sensoren zu ermöglichen, sind die Arbeits- und Kommunikationsprozesse zwischen den Führungsebenen im Militärischen Nachrichtenwesen und im System Militärisches Nachrichtenwesen stets bestmöglich zu gewährleisten. Vor diesem Hintergrund gilt es, die hochwertige Aus- und Weiterbildung des eingesetzten Personals sicherzustellen, um mit der fortschreitenden Digitalisierung und Modernisierung mithalten zu können.

Im Kern geht es um den Schutz der Interessen unseres Staates, um seine Sicherheit, um die Erreichung gesetzter Ziele in Einsätzen und den Schutz der Soldatinnen und Soldaten. Das JIC erfüllt sowohl eine beratende als auch warnende Funktion, indem es weltweit aktuelle Veränderungen jederzeit mit verfolgt und somit Krisenherde frühzeitig erkennen kann.

DIENSTSTELLEN-PROFIL

INFORMATIONSTECHNIK-BATAILLON 281

Die mobilen IT-Kräfte des Informationstechnikbataillons 281 (ITBtl 281) stellen mit modernen Systemen robuste und sichere IT-Services bereit und damit die Führungsfähigkeit in Einsätzen, einsatzgleichen Verpflichtungen und Übungen sicher.

AUFGABEN

- Das ITBtl 281 stellt weltweit IT-Services als Beitrag zur Führungsfähigkeit in Einsätzen, Einsatzgleichen Verpflichtungen und Übungen mit IT-Spezialisten und modernen IT-Systemen bereit.
- Die Soldatinnen und Soldaten des ITBtl 281 verstehen sich als militärischer IT Service-Provider und ermöglichen auch unter widrigsten Bedingungen und an abgelegensten Orten unabhängige, moderne, zuverlässige und robuste IT-Services zur Führung von Einsätzen.
- Hierfür bildet das ITBtl 281 seine Soldatinnen und Soldaten von der Grundausbildung bis zur weiteren fachlichen Fortbildung umfassend sowohl militärisch als auch IT-fachlich aus.

AUFTRAG

Die Spezialistinnen und Spezialisten des ITBtl 281 sind weltweit in der Lage, eine von fester Infrastruktur unabhängige, sichere Verbindung in die Netze der Bundeswehr in Deutschland herzustellen. Sie sind befähigt, ein eigenes weitreichendes Netzwerk im Einsatzraum aufzuspannen – das Kernnetz. Davon ausgehend werden den Streitkräften Zugangspunkte – Service Delivery Points (SDP) – bereitgestellt, um eigene Führungseinrichtungen an das Netz anzuschließen. Diese Zugangspunkte sind ein Verbund unterschiedlicher, moderner Systeme, mit denen Telefonie, Datenübertragung und -verarbeitung auch an den abgelegensten Orten möglich wird. Darüber hinaus speisen die Kräfte des ITBtl 281 das Kernnetz mit speziellen, sicheren und für die Führung im Einsatz entwickelten IT-Services. Das ITBtl 281 errichtet und betreibt auch die lokalen Netze der Führungseinrichtungen des Organisationbereichs CIR und der Streitkräftebasis im Einsatz. Planung, Einsatz und das übergreifende Servicemanagement für das Einsatzgebiet erfolgt durch eine eigene Betriebsführungseinrichtung.

Die Angehörigen des Bataillons verstehen sich als militärischer IT-Service Provider, der auch unter schwierigsten Bedingungen robuste und sichere IT-Services zur Führung aller Kräfte im Einsatz bereitstellt. Hierfür bildet das ITBtl 281 seine mobilen IT-Kräfte an modernen Ausbildungsanlagen am Standort Gerolstein aus, von der Grundausbildung für den Organisationsbereich CIR über die Einsatzausbildung bis hin zur Weiterbildung an den eigenen Systemen. Hier angesiedelt ist auch das Fachausbildungszentrum für Satellitenkommunikation, in dem beispielsweise die Umschulung auf neue Systeme erfolgt.

ANSCHRIFT
Eifelkaserne,
Philipp-Reis-Straße 2,
54568 Gerolstein

DIENSTSTELLENLEITUNG
Oberstleutnant Sascha Günther

STAMMPERSONAL
~700

AUFSTELLUNG
01.07.1959

OBERSTLEUTNANT JOHANN MADER,
REFERAT IT-KOORDINIERUNG IM GESCHÄFTSBEREICH DES BUNDESMINISTERIUMS DER VERTEIDIGUNG,
ABTEILUNG OPERATION, UNTERABTEILUNG J6, KOMMANDO CIR

IT-KOORDINIERUNG IM GESCHÄFTSBEREICH DES BUNDESMINISTERIUMS DER VERTEIDIGUNG – EINE „HERKULES"-AUFGABE

Für die Beschäftigten in der Bundeswehr sind Ausstattung und Arbeit mit moderner Informationstechnik – einschließlich der geschaffenen Möglichkeiten, während der pandemiebedingten Situation aus dem Homeoffice zu arbeiten – zu einer Selbstverständlichkeit geworden. Doch nur wenige kennen den täglichen organisationsbereichsübergreifenden Aufwand, um vorhandene IT-Ressourcen zu steuern, Forderungen und Interessen der Nutzer gegenüber dem Bedarfsdecker zu vertreten, Erkenntnisse aus Nutzung und Betrieb zur Umsetzung zu bringen und damit die Weiterentwicklung des IT-Systems der Bundeswehr zu lenken. Diese Aufgaben übernimmt die IT-Koordinierung für den Geschäftsbereich des Bundesministeriums der Verteidigung (BMVg).

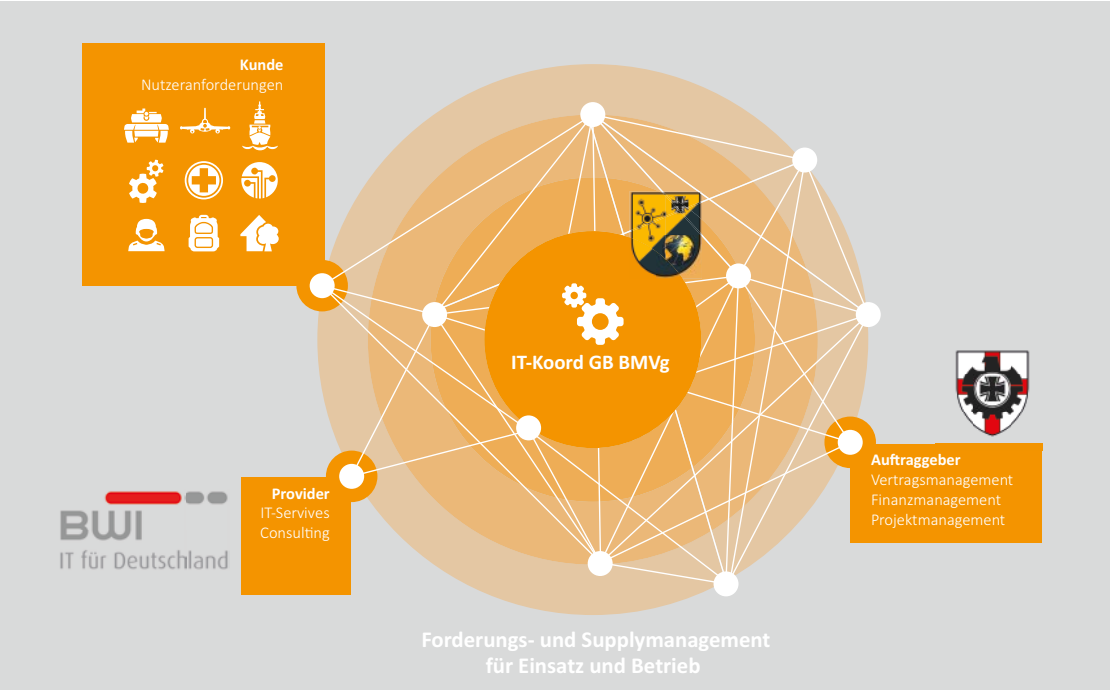
DAS REFERAT IT-KOORDINIERUNG FÜR DEN GESCHÄFTSBEREICH BUNDESMINISTERIUM DER VERTEIDIGUNG

Das Referat IT-Koordinierung wurde erstmals im Jahr 2017 als ein Koordinations- und Steuerelement des zentralen Supplymanagements für das IT-System der Bundeswehr in der Abteilung Einsatz des Kommandos Informationstechnik der Bundeswehr (KdoITBw) etabliert. Die Aufstellung erfolgte somit knapp zehn Jahre nach Unterzeichnung des Hauptvertrages für das IT-Projekt HERKULES auf Basis eines ministeriellen Erlasses. Zielsetzung war, ein besseres und zentrales Forderungsmanagement aus dem IT-Betrieb und den damit verbundenen IT-Leistungen der Bundeswehr Informationstechnik GmbH (BWI) für die Dienststellen der Streitkräfte im In- und Ausland zu erreichen.

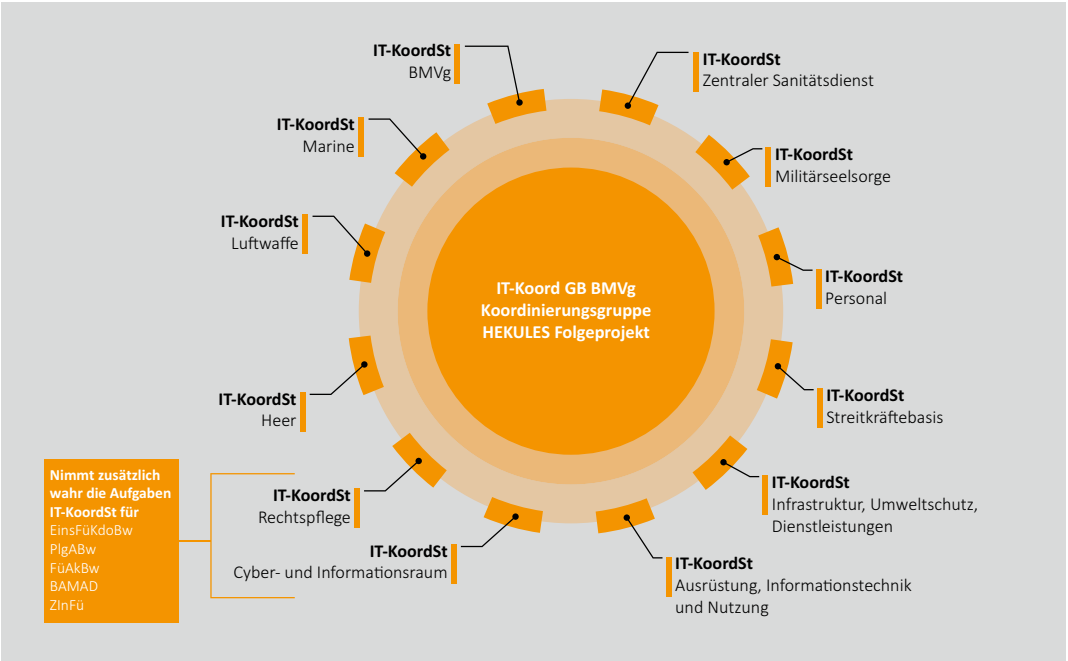
Durch die IT-Koordinierung wurde ein Bindeglied zwischen den IT-Koordinierungsstellen der Teilstreitkräfte und Organisationsbereiche („Kunde"), dem Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAAINBw) als Bedarfsdecker im Sinne des „Auftraggebers" und der BWI als „Provider" oder Auftragnehmer geschaffen.

Das Referat IT-Koordinierung ist dabei im direkten Auftrag der Abteilung Cyber- und Informationstechnik des BMVg (BMVg CIT) tätig, die auch die Fachaufsicht über das HERKULES-Folgeprojekt innehat.

Im permanenten Spannungsfeld zwischen der Forderung nach moderner IT, nutzer- und bedarfsgerechten Applikationen, Software und Services sowie der Möglichkeit von finan-



▶ IT-Koordinierung im Geschäftsbereich des Bundesministeriums der Verteidigung als Bindeglied.
Grafik: Bundeswehr/PIZ CIR



◀ Zusammenarbeitsbeziehungen IT-Koordinierung mit den Teilstreitkräften/Organisationsbereichen.
Grafik: Bundeswehr/PIZ CIR

zierbaren, sicheren und betrieblich stabilen Lösungen ist die IT-Koordinierung somit als „Spinne im Netz" tätig. Das Netzwerk wird insbesondere in regelmäßig mit allen IT-Koordinierungsstellen der Organisationsbereiche stattfindenden Sitzungen der Koordinierungsgruppe für das HERKULES-Folgeprojekt zur Bereitstellung von IT-Services ausgebaut.

Im Zuge der Neustrukturierung „CIR 2.0" wurde die IT-Koordinierung im August 2021 dem Kommando Cyber- und Informationsraum (CIR) zugeordnet und dort in die Referatsgruppe Supplymanagement der Unterabteilung J6 und IT-Services der Bundeswehr integriert.

KERNAUFGABEN UND SCHWERPUNKTE DER IT-KOORDINIERUNG

Die Kernaufgaben der IT-Koordinierung liegen im Einführungs- und Kapazitätsmanagement für vorhandene IT-Services, in der Harmonisierung der Bedarfe an IT-Services als „Forderungsmanagement" für alle Dienststellen der Bundeswehr im In- und Ausland, in der Vertretung der Interessen aller IT-nutzenden Dienststellen gegenüber dem Bedarfsdecker sowie in der Weiterentwicklung des IT-Systems der Bundeswehr.

Den Schwerpunkt der Tätigkeiten bildet – neben zahlreichen weiteren dem Supplymanagement zugeordneten Steuerungsaufgaben – die Bearbeitung sämtlicher nutzerrelevanter Aktivitäten in Bezug auf den im Jahr 2016 geschlossenen Leistungsvertrag HERKULES-Folgeprojekt.

Mit den Verfahren der IT-Koordinierung werden also die Anforderungen und Umfänge bestehender IT-Services aller Organisationsbereiche und des Verteidigungsministeriums selbst erfasst und konsolidiert. Ergebnis ist ein für alle transparentes Lagebild über gestellte Forderungen und anerkannte Bedarfe sowie verfügbare, zugeteilte und bereitgestellte IT-Services.

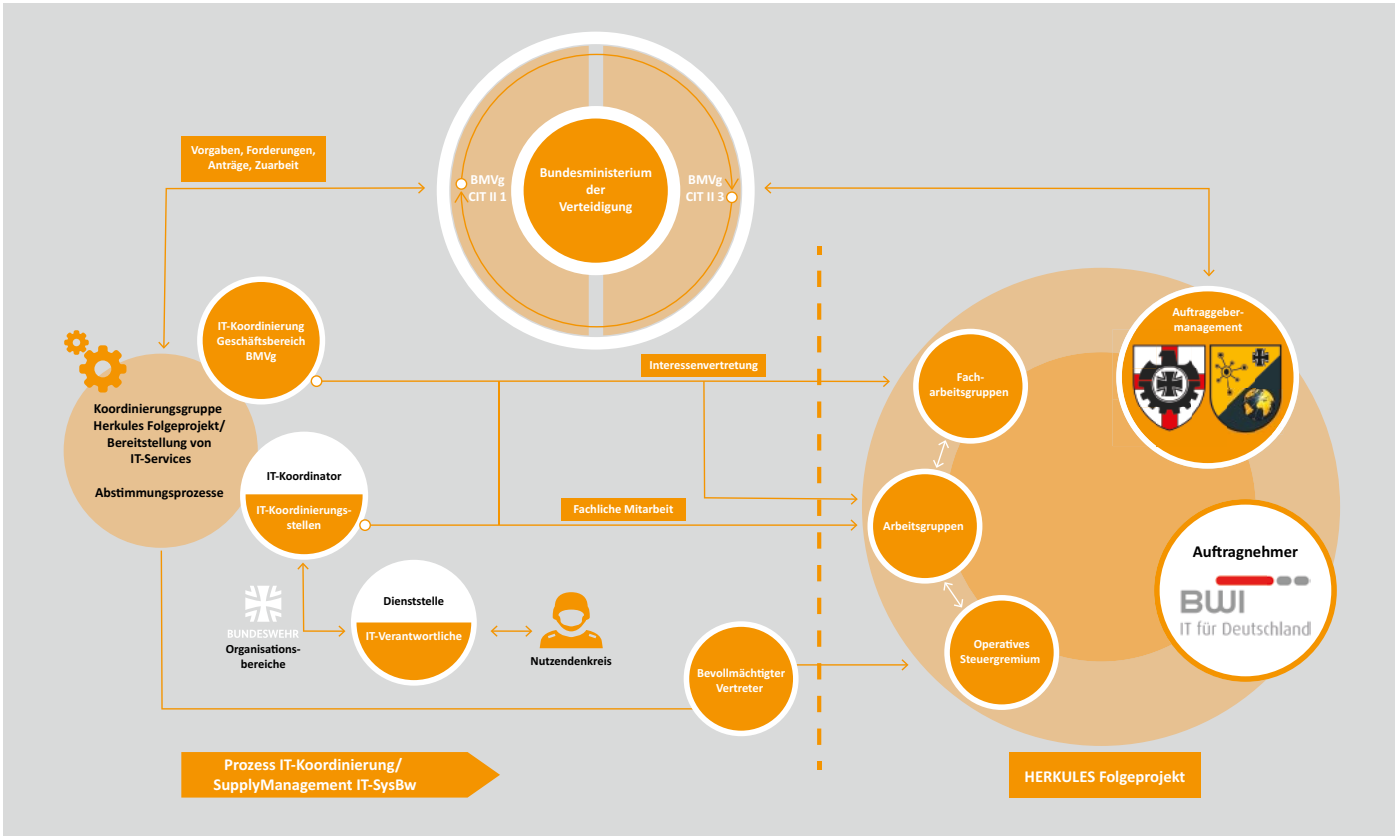
Auf dieser Grundlage ist die IT-Koordinierung in diversen Arbeits- und Facharbeitsgruppen vertreten. In diesen werden die Forderungen an IT-Services aus Nutzung und Betrieb eingebracht und deren Umsetzung begleitet. Mitglieder in diesen Gremien sind ebenfalls das hierfür federführende BAAINBw und der Auftragnehmer BWI. Formal gesehen werden die Forderungen an IT-Services durch den „Bevollmächtigten Vertreter HERKULES-Folgeprojekt für Nutzung und Betrieb in den Organisationsbereichen" im Operativen Steuerungsgremium vorgetragen, in dem das Auftraggebermanagement für das Folgeprojekt erfolgt.

Stichpunktartig sind hier einige der Aufgabenschwerpunkte der IT-Koordinierung aufgezählt:

- Durchführen des Informationsmanagements für die Koordinierungsgruppe HERKULES-Folgeprojekt.
- Erstellen und Führen der IT-Bedarfslage zur Erarbeitung bedarfsbegründender Dokumente für die Beschaffung von IT.
- Mitwirken am Anforderungs- und Portfoliomanagement im HERKULES-Folgeprojekt im dort agierenden „Integrierten Arbeitsteam".
- Steuern der Neuregelung der Versorgung der Auslandsdienststellen der Bundeswehr mit IT.
- Erstellen und Abstimmen zentraler Vorgaben/Konzepte für die Erfassung, Planung und Beauftragung von Forderungen an IT-Services im Schwerpunkt mit Bezug zum HERKULES-Folgeprojekt.
- Erstellen und Fortschreiben von Zentralrichtlinien und Regelungen für das Zusammenwirken zur Bereitstellung von IT-Services, die Ressourcensteuerung der IT-Services und die Ausplanungsvorgaben in den IT-Konzepten der Dienststellen der Bundeswehr

AUSGEWÄHLTE AUFGABEN DER IT-KOORDINIERUNG NÄHER BETRACHTET – VORBEREITUNG FÜR DIE BEREITSTELLUNG VON IT-SERVICES

Die Koordinierungsgruppe HERKULES-Folgeprojekt ist ein zentrales Gremium, das durch den „Bevollmächtigten Vertreter" geleitet und durch die IT-Koordinierung durchgeführt wird. Alle IT-Koordinierungsstellen nehmen an diesem Gremium stimmberechtigt teil und bilden damit eine gemeinsame und direkt zusammenarbeitende Fachorganisation außerhalb der



▲ Zusammenarbeitsbeziehungen IT-Koordinierung zur Bereitstellung von IT-Services (BIT-S) im Rahmen HERKULES-Folgeprojekt.
Grafik: BWI

regulären Hierarchien. Die zu behandelnden Themen werden konsolidiert, im Konsens entschieden und Positionen erarbeitet, die dann in der weiteren Gremienarbeit vertreten werden.

Diese Koordinierungsgruppe bringt Übereinstimmung in die Anforderungen an IT-Services und steuert übergreifende Umsetzungsmaßnahmen sowie Mitwirkungshandlungen. Zudem entscheidet sie Rahmenregelungen für IT-Bedarfsplanung, IT-Forderung und -Bereitstellung sowie die Bestandsführung von IT-Services.

Eine vertiefte Behandlung spezifischer Fachthemen erfolgt dann in den eigenen Arbeitsgruppen: IT-Konzepte Inhalte, Kapazitätsmanagement und IT-Nachweisführung. Diese Arbeitsgruppen erarbeiten ein gemeinsames Verständnis, stimmen Verfahren ab und arbeiten an Lösungen und Positionen für die Planung, die Steuerung von Ressourcen sowie das Assetmanagement (Betrieb, Erweiterungen, Modifikationen sowie Stilllegung von IT-Services und IT-Infrastruktur).

Der „Bevollmächtigte Vertreter HERKULES-Folgeprojekt" bringt dann die Ergebnisse der Abstimmung der Koordinierungsgruppe in das übergreifende Programmmanagement dieser „Komplexen Dienstleistung" und damit die „Kundensicht" ein.

Die Bereitstellung von Haushaltsmitteln für die Beschaffung und den Betrieb von IT erfordert belastbare bedarfsbegründende Unterlagen. Hierzu führen die IT-Verantwortlichen aller Dienststellen eigene IT-Konzepte, die durch die entsprechend zuständigen IT-Koordinierungsstellen geprüft und anerkannt werden. Die IT-Koordinierung konsolidiert den konzeptuell dokumentierten Bedarf und meldet das Ergebnis regelmäßig an die ministerielle Fachaufsicht zur Aktualisierung der „IT-Bedarfslage für ausgewählte IT-Services".

Ziel dabei ist, kontinuierlich quantitative Veränderungen der Anforderungen an den in Nutzung befindlichen IT-Service zu erfassen und zukünftige Bedarfsveränderungen ableiten zu können. Somit bilden diese Zahlen und Prognosen die Grundlage für die planerische Vorsorge und flexible Mengenanpassungen im Rahmen des Portfoliomanagements. Dies führt im Ergebnis zu einer beschleunigten und bedarfsgerechten Bereitstellung von ausgewählten IT-Services.

Die Daten der IT-Bedarfslage sind Arbeitsgrundlage für Mengenanpassungen im entsprechenden Portfoliosegment und anderer Verfahren der Beschaffung von IT. Sie „speisen" die neuen Clusterprogramme für die mittel- bis langfristige Bedarfsdeckung.

Als Beispiel für eine erfolgreiche Umsetzung der hier gewonnenen Erkenntnisse sei plakativ die Beschaffung und Bereitstellung von insgesamt 100.000 (Zweit-) Monitoren aufgeführt. Diese erfolgte durch das Sonderprogramm „Resilienz Bundeswehr" im Rahmen des Konjunkturpaketes der Bundesregierung und ist eine wesentliche Voraussetzung für eine nutzerfreundliche Anwendung der neuen Groupware der Bundeswehr für die Bürokommunikation.

Weiterhin spielt die IT-Bedarfslage eine zentrale Bedeutung für die kontinuierliche Weiterentwicklung von IT-Produkten und Services sowie für das Kapazitätsmanagement, das den Organisationsbereichen die verfügbaren Mengen an IT und IT-Services zum Abruf zuweist.

ANFORDERUNGS- UND PORTFOLIOMANAGEMENT DES HERKULES-FOLGEPROJEKTS

Die IT-Koordinierung registriert, prüft, bearbeitet und vertritt im Anforderungs- und Portfoliomanagement die funktionalen Fähigkeitsforderungen an IT und deren Services über ihre Ausplanung und Entwicklung bis hin zum Vertragsschluss mit der BWI, für den es je nach Finanzierung und Leistungsart unterschiedliche Konstrukte gibt. Dies beinhaltet den flexiblen Umgang mit einer sich stetig ändernden Anforderungslage an bestehende IT-Services und Produkte des Portfolios des HERKULES-Folgeprojekts. Ein zentrales, gemeinsam mit dem Bedarfsdecker und dem Provider geführtes Logbuch hilft hier den Überblick zu bewahren, weil die entsprechenden Anforderungen seit Jahren stetig deutlich zunehmen. Dies zeigt, dass dieser Weg als zielführend wahrgenommen wird.

Die IT-Koordinierung arbeitet hier dem IT-Portfoliomanagement im jeweiligen Segment nach dessen Vorgaben zu, initiiert und begleitet die Umsetzung der Anforderungen. Das IT-Portfoliomanagement verantwortet im Auftrag des Projektleiters die Umsetzung einer anforderungsgerechten und harmonisierten Planung von Bedarfen in neue oder auch stillzulegende IT-Services und Produkte.

KOORDINATION DER VERSORGUNG DER AUSLANDSDIENSTSTELLEN DER BUNDESWEHR MIT IT

Die Planung der IT-Services sowie der Betrieb der IT für die im Ausland befindlichen Dienststellen wurde bisher durch die entsendenden Organisationsbereiche, durch Bundeswehr-Verwaltungsstellen im Ausland oder auch durch das Auswärtige Amt selbst wahrgenommen. Diese gemischte Betriebsverantwortung und das dezentrale IT-Management führten zu einem inhomogenen und beim Nutzerkreis als nicht mehr zeitgemäß wahrgenommenen Betrieb. Über zwei Drittel der genannten Dienststellen verfügt dabei aufgrund ihres geringen Umfangs (weniger als zehn Nutzer) in der Regel nicht über eine eigene IT-Unterstützung vor Ort.

Um diesen zurzeit 488 Dienststellen – und deren teilweise dislozierten Teileinheiten in 86 Ländern auf sechs Kontinenten mit mehr als 5.560 IT-relevanten Dienstposten im Ausland – eine möglichst im gesamten IT-System der Bundeswehr einheitliche, jedoch bedarfsgerechte IT-Ausstattung mit den erforderlichen Services bereitzustellen, wurde die BWI mit einem eigenen Projekt beauftragt. Die dafür eingerichtete Projektsteuergruppe ist ebenfalls für den Anteil von BWI-Services für Einsatz/Übung im Ausland und die dafür geltenden besonderen Forderungen an Sicherheit, Resilienz und Flexibilität zuständig. Hierzu finden regelmäßig Workshops in unterschiedlichen Formaten (Auslandsdienststellen, Einsatz/Übung, Vertragsangelegenheiten) statt, in denen die IT-Koordinierung insbesondere die Forderungen der Organisationsbereiche mit Auslandsdienststellen angleicht und deren Umsetzung in IT-Services durch die BWI steuert.

Die BWI soll also als Provider eine vollumfängliche Servicebereitstellung für die Auslandsdienststellen erbringen und unterstützende, flexibel abrufbare Services für Einsatz- und Übungszwecke bereithalten. Dies wird nach derzeitiger Abschätzung bis Ende 2024 vollumfänglich realisiert sein; erste Maßnahmen wurden aber bereits in beiden Handlungsfeldern umgesetzt. So wurde beispielsweise eine sogenannte Remote-Access-Interimslösung – bestehend aus einem Laptop mit lokaler Peripherie und sicherer Kommunikationsanbindung – mit 630 Ausstattungen als ein von der BWI bereitgestellter IT-Service im Ausland etabliert, der keine Brüche zu den gewohnten Leistungen im Inland mehr aufweist.

IT-Unterstützung und IT-System Bundeswehr[1]
Mitwirkung durch die IT-Koordinierung im Geschäftsbereich BMVg

Bezeichnung/Oberbegriff Anteile IT-System Bundeswehr (vereinfacht)	Mitwirkung IT-Koordinierung im Geschäftsbereich BMVg
IT-Standards, querschnittliche Logistik, lokale Einführungsorganisation SASPF und Softwarelizenzmanagement	Im Bereich IT-Standards und beim Softwaremanagement in Bezug auf HERKULES Folgevertrag sowie Zentrales Adress- und Verzeichnismanagement und anderen HERKULES-relevanten Bereichen
Programmorganisation HERKULES, Projekte Zentrale Dienste außerhalb HERKULES	Anforderungs-, Portfolio-, IT-Service-Management, Liegenschaften, Netze (WAN, [W]LAN, Telefonie, zentrale Dienste, FileService, Rechenzentren
Führungsinformationssysteme stationär/verlegefähig	nicht-HERKULES-IT[2] – zurzeit keine Mitwirkung
Führungsinformationssysteme, Führungs- und Waffeneinsatzsysteme mobil/seegehend/spezifisch Cyber Defence-Technik und Kryptosysteme	nicht-HERKULES-IT[2] – zurzeit keine Mitwirkung
Drahtlose Kommunikationssysteme	nicht-HERKULES-IT[2] – zurzeit keine Mitwirkung
IT-Plattform-Projekte/Services Bw, Programmorganisation Kollaboration	IT-Ausstattung im HERKULES Folgeprojekt, Anteil Client Services (PC oder Notebook) mit mobiler Anbindung an das IT-System der Bundeswehr (inkl. Telearbeit), (sichere) Smartphones und Tablets, Drucker, Videokonferenzservices

1 Bundeswehrgemeinsamer Informations- und Kommunikationsverbund, der alle führungsrelevanten IT-Anteile von Einrichtungen, Plattformen und Waffensystemen miteinander vernetzt und IT-Services durch unterschiedliche IT-Service Provider bereitstellt, bestehend aus den Anteilen: Informationsübertragungssysteme, Bürokommunikationssysteme, Führungsinformationssysteme, Fachinformationssysteme, Führungs- und (Waffen-) Einsatzsysteme (IT-Anteile), IT-System Unterstützung Sanitätsdienst, gekapselte (in sich geschlossene) Systeme, externe Systeme.

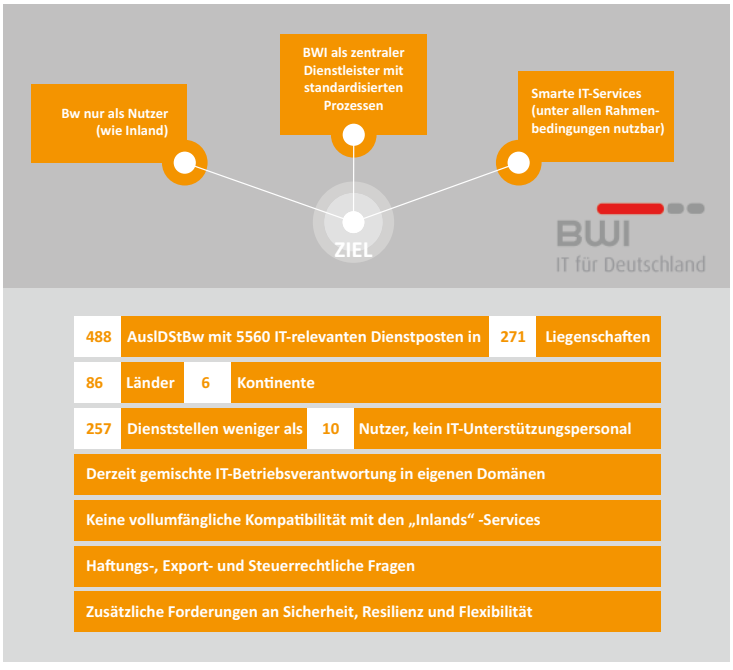
2 nicht-HERKULES-IT = IT, die nicht aus dem Leistungsvertrag HERKULES (inkl. Folgeprojekt) stammt, umgangssprachlich „grüne IT“ genannt. IT, die durch HERKULES (inkl. Folgeprojekt) bereitgestellt ist/wird, umgangssprachlich „weiße IT“ genannt.

◀ Grafik: Bundeswehr/PIZ CIR

ANWENDUNG DER VERFAHREN DER IT-KOORDINIERUNG IM KONTEXT COVID-19

Während der Corona-Pandemie haben sich die organisatorischen, planerischen und steuernden Fähigkeiten der IT-Koordinierungsorganisation als wesentliches Element des Supplymanagements für den Betrieb des IT-Systems der Bundeswehr bewährt. Die schnelle und sichere Handlungsfähigkeit in einem funktionierenden Netz mit den IT-Koordinierungsstellen, dem BAAINBw und der BWI im für die COVID-19-Steuerung eingerichteten, spezifischen und zu Beginn täglich tagenden Abstimmungsformat, unterstützte einen raschen Aufwuchs von ortsunabhängigen IT-Services und damit eine bedarfsgerechte Ausstattung der Dienststellen für ein aufgelockertes und dezentrales Arbeiten. Um auch den Inspekteur der Streitkräftebasis als „Nationalen Territorialen Befehlshaber", das Kommando Territoriale Aufgaben und die Landeskommandos für Amtshilfeleistungen im Rahmen der Pandemiebewältigung zu befähigen, wurden bundesweit IT-Pools mit 2.000 vorkonfigurierten Notebooks und gesicherter Kommunikation durch die BWI bestückt. Organisation, Verwaltung sowie Koordination der Verteilung und Bestandsüberwachung der Poolbestände erfolgen nach wie vor durch die IT-Koordinierung in Zusammenarbeit mit beauftragten Dienststellen, die für die Verteilung und Rücknahme des Geräts in der Fläche zuständig sind.

Neben der Bedarfsermittlung, Steuerung und Überwachung der Verteilung von mobiler IT zum Erhalt der Handlungsfähigkeit der Bundeswehr war die IT-Koordinierung zentraler Ansprechpartner für die BWI, das Betriebszentrum für das IT-System der Bundeswehr und die IT-Koordinierungsstellen für die Einführung und Verteilung der Software OpenVPN. OpenVPN überbrückt temporär die sichere Anbindung der Beschäftigten im Homeoffice bis zur Ausstattung mit regulär bereitgestellten Remote-Access-Geräten an die Netzwerke der BWI und des bundeswehreigenen Betriebszentrums. Die IT-Koordinierung ermittelte die Bedarfe beziehungsweise Nutzerforderungen dazu und unterstützte in enger Abstimmung mit den Organisationsbereichen, dem Betriebszentrum für das IT-System der Bundeswehr und der BWI die Planung und Durchführung der einzelnen Rollout-Wellen bis zum Zielbetrieb. Somit konnten eine pandemiegerechte Auflockerung und das sichere Arbeiten aus dem Homeoffice heraus in größtmöglichem Maße realisiert werden.



◀ Herausforderungen der Versorgung der Auslandsdienststellen der Bundeswehr mit IT.
Grafik: Bundeswehr/PIZ CIR

ZUSAMMENFASSUNG UND AUSBLICK

Die IT-Koordinierung nimmt im Schwerpunkt vorbereitende Aufgaben für die Nutzung und den Betrieb des IT-Systems der Bundeswehr zur Erfüllung von Anforderungen der Dienststellen der Bundeswehr wahr. Neben dieser Tätigkeit erfüllt sie auch unterstützende Aufgaben im Rahmen der Weiterentwicklung von IT-Services sowie der Verfahren und Werkzeuge der IT-Koordinierung selbst. Als Beispiele seien hier die Mitwirkung an der Umsetzung der „personalisierten IT-Ausstattung" und die Berücksichtigung der IT-Koordinierungsprozesse bei der Weiterentwicklung von IT-Services im Rahmen des neuen IT-Servicemanagements der Bundeswehr genannt. Sie kümmert sich auch um die Steigerung der Effektivität und Effizienz der eigenen Verfahren, indem sie ein Konzept „IT-Koordinierung der Zukunft" erstellt und abgestimmt hat. Hierdurch wurde das Fundament für die Entwicklung des eigenen Geschäftsprozesses „IT-Koordinierung/Supplymanagement" im Rahmen des Hauptprozesses IT-Management gelegt. Mit fortschreitender Weiterentwicklung des IT-Systems der Bundeswehr wird dies zukünftig zu einer weiteren Reduzierung der Schnittstellen führen; die Abstimmung wird somit beschleunigt, der Aufwand wird verringert, die Reibungsverluste werden minimiert. Dabei soll aber nicht verschwiegen werden, dass die weitere Umsetzung des Prozesses, insbesondere für bisher nicht nach den Verfahren der IT-Koordinierung behandelte IT-Projekte außerhalb des HERKULES-Folgeprojekts, durchaus initial eine „Anfangsinvestition" erfordert, die erst später Früchte tragen wird.

Die etablierten Verfahren und die Organisation der IT-Koordinierung haben sich sowohl grundsätzlich als auch in besonderen Lagen bewährt. Das Tempo der Weiterentwicklung von IT, die dadurch ständig anwachsenden Anforderungen an die IT-Koordinierung und die Absicht, vermehrt auch IT einzubeziehen, die bisher nicht dem HERKULES-Folgeprojekt zuzuordnen ist, erhöht nicht nur den Anspruch an die Organisation und die dort arbeitenden Personen, sondern auch an die Werkzeuge beziehungsweise die Qualität der zu nutzenden IT-Unterstützung. Der Umfang sowie die Komplexität der Aufgaben der IT-Koordinierungsorganisation werden dementsprechend weiter zunehmen. Die Integration der Aufgabe in die neue Struktur des Kommandos Cyber- und Informationsraum war daher ein richtiger und konsequenter Schritt: im engen Schulterschluss mit der Operationsführung im Cyber- und Informationsraum und dem Treiber der Digitalisierung der Bundeswehr kann die IT-Koordinierung ihre Rolle erfüllen.

DIENSTSTELLEN-PROFIL

INFORMATIONSTECHNIK-BATAILLON 282

Das Informationstechnikbataillon 282 leistet mit seinen IT-Spezialistinnen und -Spezialisten durch Bereitstellung von IT-Services einen elementaren Beitrag für die Führungsfähigkeit der Streitkräfte in der Bundeswehr.

AUFGABEN

- Stellt ab 2022 bis 2024 einen signifikanten Kräftebeitrag an der NATO Response Force (NRF) und leistet damit einen wesentlichen Beitrag zur Stärkung der Reaktionsfähigkeit des Bündnisses.
- Trainingszentrum Network Operations Centre – die einzige bundeswehreigene Ausbildungsstätte „Betriebsführung" in den Streitkräften.
- Stellt durch die Ausbildungsanlagen SatCom EK (Einkanal) und Teilnehmeranschalttrupp (TMA) die Ausbildung über alle Organisationbereiche in der Bundeswehr sicher.
- Bildet nach neuer Ausbildungssystematik die Offizieranwärterinnen und -anwärter des Organisationsbereichs CIR aus.

AUFTRAG

Das Informationstechnikbataillon 282 (ITBtl 282) stellt die Vernetzung von Einsatzliegenschaften und Gefechtsständen in der Landes- und Bündnisverteidigung und im erweiterten Aufgabenspektrum der Bundeswehr sicher. Mit dem mobilen Kommunikationssystem wird den anderen Organisationsbereichen ein bundeswehreigenes Providernetzwerk zur Verfügung gestellt.

Zur Vernetzung der Gefechtsstände und der Bereitstellung von Diensten werden IT-Systeme durch die hoch qualifizierten Administratoren des ITBtl 282 im Systemverbund betrieben. Diese Systeme sind Vorreiter für die Digitalisierung der Streitkräfte. Mit seinen vier leistungsstarken Einsatzkompanien sorgt das ITBtl 282 zuverlässig für die Führungsfähigkeit bei der Landes- und Bündnisverteidigung im Rahmen von NRF/VJTF, bei Auslandseinsätzen der Bundeswehr und Katastrophenhilfe im Inland.

ANSCHRIFT
Hunsrück-Kaserne,
Graf-Moltke-Straße,
56288 Kastellaun

DIENSTSTELLENLEITUNG
Oberstleutnant Anthony James Buford

STAMMPERSONAL
~700

AUFSTELLUNG
01.04.1964

OBERSTLEUTNANT KARSTEN HAUFE, LEITER NETWORK OPERATIONS CENTRE BASIS INLAND, BETRIEBSZENTRUM IT-SYSTEM BUNDESWEHR (BITS) IN RHEINBACH

DAS **NETWORK OPERATIONS CENTRE BASIS INLAND** (NOC B.I.)

Die Steuerung- und Koordinierung zur Sicherstellung aller IT-Services ist eine für die Bundeswehr essenzielle Aufgabe. Diese wird durch das Betriebszentrum Informationstechnik-System Bundeswehr (BITS) zentral wahrgenommen. Hierzu ist es gegenüber allen Providern IT-fachlich und betrieblich weisungsbefugt.

Das BITS betreibt eine integrierte IT-Service Management Umgebung (ITSME) zur Planung, Erbringung, Absicherung und Automatisierung seiner IT-Services (siehe auch Seite 90). Diese wird zukünftig auch in die Einsätze ausgerollt. Die toolgestützte Koordination von Funktionen, Prozessen und IT ermöglicht den Serviceprovidern ein durchgängiges IT-Servicemanagement für die Lieferung ihrer IT-Services.

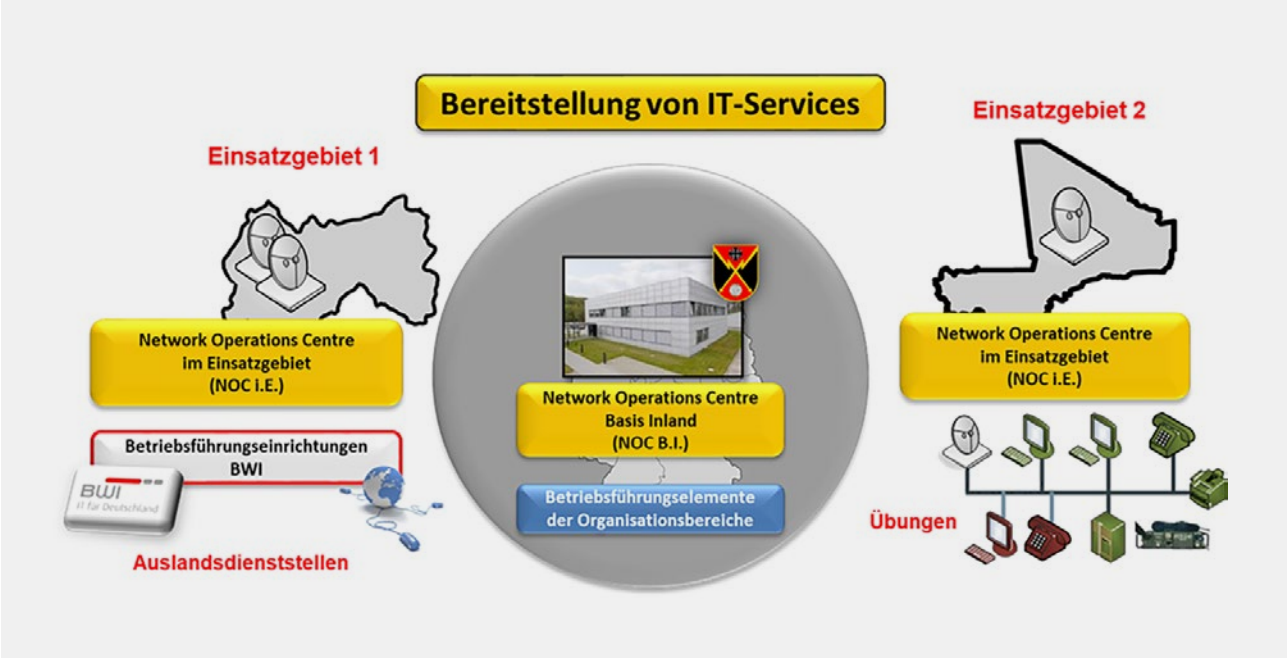
Über weitreichende, strategische Verbindungen und IP-basierte Netze werden nutzerorientierte IT-Services in nationalen und multinationalen Einsätzen der Bundeswehr geliefert. Dazu kommen Leistungen, die nicht durch das BITS bereitgestellt werden. Hierbei handelt es sich um IT-Services Dritter (z.B. SASPF), die im Einsatz oder Ausland zur Verfügung gestellt werden.

Das Network Operations Centre Basis Inland (NOC B.I.) bildet gemeinsam mit dem dort ebenfalls vorhandenen „Service Desk Einsatz/Übungen/Auslandsdienststellen" das zentrale Eingangsfenster für alle Störungen, Einschränkungen und Serviceanfragen innerhalb des IT-Systems Bundeswehr. Organisatorisch gehört es im Betriebszentrum zur Abteilung Operation. Dieser gehört auch die Betriebsführungseinrichtung des Zentrums an, die den Betrieb der gesamten Dienststelle (Informationssicherheit BITS) sicherstellt.

AUFGABEN DES NETWORK OPERATIONS CENTRE BASIS INLAND (NOC B.I.)

Das NOC B.I. koordiniert zunächst die weltweite Überwachung des IT-Systems Bundeswehr. Die Sicherstellung der Verfügbarkeit der IT-Services erfolgt dabei grundsätzlich durch verschiedene Provider. Für den Großteil der IT-Services in der Basis Inland ist dies die BWI GmbH. Teilstreitkräfte sowie die Organisationsbereiche gewährleisten zusätzlich eigene spezifische IT-Services. So stellt zum Beispiel die Luftwaffe auf der gemeinsamen Infrastruktur-Plattform HaFIS (Harmonisierung der Führungsinformationssysteme) IT-Services für die Community of Interest (COI) „Air" bereit.

Das NOC B.I. steuert aber auch alle Maßnahmen und Aktivitäten, die zur schnellen Wiederherstellung bei Störungen, Ausfällen und Problemen benötigt werden. Dies erfolgt in enger Zusammenarbeit mit den Verbänden im Einsatz sowie den Bereitstellern der IT-Services, ganz besonders der BWI. Dabei steht die schnellstmögliche Entstörung im Vordergrund, um damit die Bereitstellung der geforderten IT-Services gemäß



den abgestimmten Service Level Agreements (SLA) mit den nutzenden Organisationen und Bereichen sicherzustellen.

Schließlich fasst das NOC B.I. die Betriebszustände aller relevanten IT-Services und IT-Systeme in einer zentralen „Betriebslage IT-System Bundeswehr" zusammen. Dazu nutzt das Betriebszentrum nicht nur seine eigene Betriebslage für die ihm zugeordneten IT-Services, sondern erhält dazu die einzelnen Betriebslagen aus den Network Operations Centres im Einsatz (NOC i.E), den Betriebsführungseinrichtungen der BWI sowie den Betriebsführungseinrichtungen/-elementen der einzelnen Organisationsbereiche. Diese Betriebslagen werden durch das NOC B.I. zu einer Gesamtbetriebslage zusammengefasst. Damit erhält der Kommandeur des BITS ein umfassendes IT-Lagebild über den Betriebszustand des IT-Systems Bundeswehr, mit dem er in der Lage ist, Prioritäten hinsichtlich der Entstörung von IT-Services festzulegen. Das umfassende IT-Lagebild wird – zur operativen Bewertung für die gesamte Bundeswehr – dann der Operationszentrale des Kommandos Cyber- und Informationsraum (CIR) bereitgestellt.

Das NOC B.I. hat im Rahmen der Betriebsführung IT-System Bundeswehr eine zentrale Funktion und ist gegenüber allen Betriebsführungseinrichtungen/-elementen (z.B. NOC im Einsatz) IT-fachlich betrieblich weisungsbefugt. Die Überwachung des gesamten IT-Systems Bundeswehr sowie die zeitnahe Reaktion und Eskalation erfolgen durch das NOC B.I. im 24/7-Betrieb.

Für die Lagebilderstellung wurde dem NOC B.I. eine zentrale Rolle im Bereich der IT-Betriebslage zugewiesen. Hier werden alle operativ bedeutsamen Ausfälle mittels einer Formatvorlage durch die zuständige Betriebsorganisation (z.B. NOC Luftwaffe) an das NOC B.I. gemeldet und von dort an die Operationszentrale des Kommandos CIR übersendet.

Auch durch die Neustrukturierung im Rahmen von CIR 2.0 und der damit bevorstehenden Auflösung des Betriebszentrums und Aufstellung des Kommandos IT-Services der Bundeswehr zum 1. April 2023 wird das NOC B.I. in Struktur wie Auftrag unverändert weiterbestehen.

RAUM FÜR WEITERENTWICKLUNG

Die Zusammenführung der IT-Betriebslagen der verschiedenen IT-Serviceprovider im IT-System der Bundeswehr zu einem gemeinsamen IT-Lagebild ist derzeit nicht voll automatisiert. Daher führt das NOC B.I. die „Betriebslage IT-System Bundeswehr" zum Teil manuell zusammen. Den relevanten Entscheidern stellt es jedoch derzeit schon einen zielgerichteten Gesamtüberblick und eine solide Entscheidungsgrundlage zur Verfügung. Das gemeinsame IT-Lagebild soll zukünftig innerhalb eines durchgängigen IT-Servicemanagements automatisiert bereitgestellt werden.

Innerhalb des Betriebszentrums wird IT-Servicemanagement schon seit Jahren auf Toolbasis umgesetzt, im NOC B.I. insbesondere auch das Eventmanagement, mit dem es möglich ist, auftretende Störungen, Einschränkungen und andere Einflüsse echtzeitnah anzuzeigen, Ereignisse zusammenzufassen und Bewertungen hinsichtlich Fehlerursache und Auswirkungen vorzunehmen. Viele Services sind schon im Eventmanagement implementiert. Eine Reihe der IT-Systeme nutzt aber noch eigene und abgeschlossene Managementsysteme, die bisher über keine, beziehungsweise keine zugelassene Schnittstelle zum Eventmanagement verfügen. Deren Integration in das System ist eine gemeinsame Aufgabe für das Eventmanagement sowie für die einzelnen IT-Projekte, die gegebenenfalls Anpassungen an der jeweiligen IT-Architektur vornehmen müssen.

▲ Die Überwachung des gesamten IT-Systems Bundeswehr sowie die zeitnahe Reaktion und Eskalation erfolgen durch das NOC B.I. im 24/7-Betrieb.
Grafik: Bundeswehr/BITS

◀ Die Steuerung- und Koordinierung zur Sicherstellung aller IT-Services wird durch das Betriebszentrum IT-System Bundeswehr wahrgenommen.
Foto: Bundeswehr/Alyssa Bier

DAS ZUKÜNFTIGE GEMEINSAME IT-LAGEBILD

In der Zukunft soll mittels einer Plattform eine übergreifende und harmonisierte Darstellung der Betriebssituation für das gesamte IT-System Bundeswehr als IT-Lagebild, inklusive der IT-Sicherheitslage, zur Verfügung gestellt werden. Grundlage dafür ist der Leistungsvertrag „HERKULES-Folgevertrag" mit dem darin enthaltenen Lösungsinkrement 3 (LI 3).

So können die Auswirkungen von Störungen oder Einschränkungen noch besser bewertet, deren Ursachen erkannt und Maßnahmen zur Behebung eingeleitet werden. Darüber hinaus soll erkennbar sein, inwieweit Risiken aus Sicht der IT-Unterstützung den Einsatz gefährden könnten. Mit der Realisierung des LI 3 wird es möglich sein, ein übergreifendes und gemeinsames IT-Lagebild bereitzustellen, das damit auch für das Betriebszentrum als zentrale Betriebsführungseinrichtung nutzbar sein wird. Der Abschluss dieses Projekts ist für 2023 geplant.

Unabhängig davon wurde im November 2020 die Großbilddarstellung im NOC B.I. regeneriert und bietet mit „The Wall of BITS" eine der größten (14,51 x 1,81 Meter) innen installierten, nahtlosen Großbildwände Europas. Damit ist eine Monitorwand verfügbar, die flexibel und bedarfsgerecht Informationen über das Lagebild des IT-Systems der Bundeswehr darstellen kann.

AUSBLICK UND ZUSAMMENFASSUNG

Im Zuge der Ausgestaltung des gemeinsamen Lagebildes wird das Betriebszentrum in die Abstimmung mit den Vertretern des Kommandos CIR einbezogen und sieht sich auf dem richtigen Weg, einen effektiven und zukunftsorientierten Beitrag für das übergreifende und gemeinsame Lagebild des Cyber- und Informationsraums leisten zu können.

Das NOC B.I. hat in den vergangenen Jahren gezeigt, dass die zugewiesenen Aufgaben jederzeit sichergestellt werden konnten, vor allem auch während der Flutkatastrophe im Juli 2021, als die Liegenschaft in Rheinbach von der Flut erheblich betroffen war. In diesem Zeitraum kam es zu keinen Einschränkungen und das NOC B.I. war durchgängig einsatzbereit.

Anspruch ist und bleibt auch in Zukunft die uneingeschränkte Einsatzbereitschaft des NOC B.I., um den Betrieb des IT-Systems der Bundeswehr zu gewährleisten, Übungen speziell zur Vorbereitung auf NRF-Verpflichtungen zu unterstützen, die Führungsfähigkeit im Rahmen der Landes- und Bündnisverteidigung sicherzustellen und auf Krisen im Interessengebiet der NATO schnellstmöglich reagieren zu können.

Das Zusammenspiel von Fachkompetenz der Mitarbeiterinnen und Mitarbeiter im NOC B.I. mit dem Anspruch der bestmöglichen Nutzerunterstützung schafft hierbei das nötige Vertrauen, das die Administratorinnen und Administratoren in den Einsatzländern spüren müssen, um den Auftrag der Bundeswehr vor Ort bestmöglich erfüllen zu können. Auch deshalb werden die Auslandseinsätze schon in der Vorbereitung durch Einweisungen unterstützt und die Erfahrungsberichte der Kontingente ständig fachlich ausgewertet.

Das NOC B.I. wird auch zukünftig eine tragende Säule innerhalb des im Jahr 2023 aufzustellenden Kommandos IT-Services der Bundeswehr und damit in der Betriebsführung des IT-Systems Bundeswehr sein und sich weiterhin bewähren.

▲ Im NOC B.I. werden die Betriebszustände aller relevanten IT-Services und IT-Systeme der Bundeswehr in einer zentralen „Betriebslage IT-System Bundeswehr" zusammengefasst.
Foto: Bundeswehr/Christian Vierfuß

▼ „The Wall of BITS" ist eine der größten innen installierten, nahtlosen Großbildwände Europas.
Foto: Bundeswehr/BITS

DIENSTSTELLEN-PROFIL

INFORMATIONSTECHNIK-BATAILLON 292

Das Informationstechnikbataillon 292 stellt mit modernen IT-Systemen die nationale und internationale Führungsfähigkeit in Einsätzen und bei der Landes- und Bündnisverteidigung sicher.

AUFGABEN

- Logistische Unterstützung und Ausbildung des Bataillons.
- Sicherstellung des Betriebs der Informationstechnik bei Übungen, Einsätzen und der Landes- und Bündnisverteidigung durch die vier Einsatzkompanien.
- Durchführung der Grundausbildung der Rekrutinnen und Rekruten.

AUFTRAG

Das Informationstechnikbataillon 292 (ITBtl 292) stellt mit modernen IT-Systemen, wie zum Beispiel Satellitenkommunikation Mehrkanal (SATCOM MK), Mobiles Kommunikationssystem der Bundeswehr (Mob-KommSys Bw), verlegefähiges Netzwerk der Bundeswehr (LVNBw), Dezentrale Server Einsatzgebiet (DSE), Digitaler Richtfunk (DigRiFu), Harmonisiertes Führungs- und Informationssystem der Bundeswehr (HaFIS) und dem militärischen Mobilfunksystem Terrestrian Trunked Radio for Police (TETRAPOL) die nationale und internationale Führungsfähigkeit im Einsatz sicher.

Die Soldatinnen und Soldaten des ITBtl 292 können schon wenige Stunden nach Erreichen des Aufbauplatzes überall in der Welt verschiedene IT-Services anbieten: Telefonieren im Fest- oder Mobilfunknetz, Standard Office Produkte, E-Mail, Datenaustausch, Intra- und Internet auf Arbeitsplatz-PC und Videokonferenzen.

Darüber hinaus stellt der Verband auch IT-Services bereit, die geheim eingestufte Informationen verarbeiten können.

ANSCHRIFT
Luitpold-Kaserne
Rudolf-Diesel-Straße 1a,
89407 Dillingen a.d. Donau

DIENSTSTELLENLEITUNG
Oberstleutnant Stefan Holland

STAMMPERSONAL
~730

AUFSTELLUNG
07.10.2005

OBERSTLEUTNANT NORMAN BICHLER,
SACHGEBIETSLEITER ITSM,
BETRIEBSZENTRUM IT-SYSTEM DER BUNDESWEHR (BITS)

EIN DURCHGÄNGIGES IT-SERVICE-MANAGEMENT (AUCH) FÜR DEN EINSATZ – IMPLEMENTIERUNG EINER ITSM-UMGEBUNG FÜR MINUSMA

Aufbau des IT Centers MINUSMA in Gao, Mali, im Mai 2022.
Foto: Atos/Steffen Liebich

Für das Deutsche Einsatzkontingent MINUSMA wurde ein durchgängiges toolgestütztes IT-Service-Management etabliert. Der Artikel beleuchtet die Grundsätze des IT-Service-Managements und dessen Umsetzung in der Bundeswehr und gibt einen Einblick in die komplexe Planung eines Rollouts im Einsatz.

WAS VERSTEHT MAN UNTER IT-SERVICE-MANAGEMENT?

IT-Service-Management (ITSM) im Allgemeinen bezeichnet sämtliche Maßnahmen und Methoden, die nötig sind, um die bestmögliche Unterstützung von übergeordneten (Geschäfts-) Zielen und Werten eines Unternehmens oder einer Organisation durch IT-Kräfte zu erreichen. Es beschreibt den Wandel der Informationstechnik weg von einer Technikfixierung hin zu einer Kunden- und Serviceorientierung.

Von Bedeutung sind insbesondere die Gewährleistung und Überwachung derjenigen Services, die für den Nutzer in sichtbare IT-Dienstleistungen münden. Auf diese Weise werden Effizienz, Qualität und auch Wirtschaftlichkeit der jeweiligen IT-Kräfte kontinuierlich verbessert.

IT-Service-Management kann auf der Grundlage verschiedener Regelwerke (sog. Frameworks) praktiziert werden. In der Bundeswehr stützt es sich auf den Quasistandard „IT Infrastructure Library" (ITIL) ab. ITIL wurde in den 1980er Jahren von britischen Regierungsbehörden zur Optimierung der eigenen IT-Dienstleistungen entwickelt und unterliegt seitdem einer ständigen Anpassung: im Laufe der Jahre wurden die Prinzipien und grundlegenden Managementprozesse von ITIL (sog. Best Practices) weiterentwickelt.

Die Einführung von ITIL lässt sich als Paradigmenwechsel von technologisch getriebenen IT-Lösungen hin zu kundenorientierten Leistungen verstehen. Wurden in der Vergangenheit Kunden- beziehungsweise Nutzerbedürfnisse an den aktuellsten technischen Realisierungsmöglichkeiten gemessen, stellt ITIL die Kundenbedürfnisse in den Vordergrund und fragt, welche Technologien und Verfahren diese in geeigneter Weise erfüllen können. Die Bundeswehr praktiziert ihr Service Management derzeit nach den Prinzipien in der Version ITIL 2011 v3.

BETRIEBSFÜHRUNG ALS TEIL DES IT-SERVICE-MANAGEMENTS

In ITIL sind die Prozesse in die Phasen „Strategy", „Design", „Transition", „Operation" sowie „Continual Service Improvement" unterteilt. Während die Phasen „Strategy" und „Design" eher auf das „Big Picture", die Definition und die Erstellung neuer IT-Services, fokussieren, wird in den Phasen „Transition" sowie „Operation" die Einführung sowie der operative Betrieb von IT-Services durch die Best Practices beschrieben.

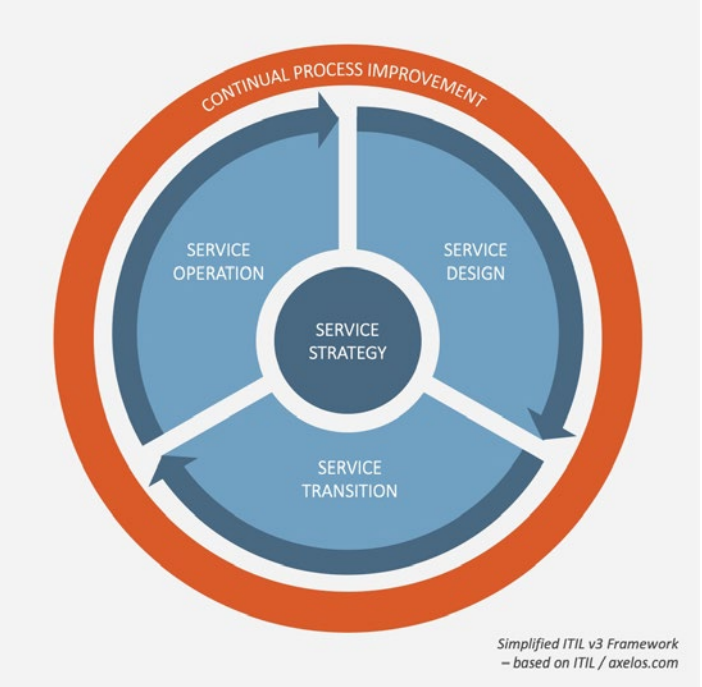
Das Ziel hierbei ist es, an den Kunden angepasste, standardisierte und wiederholbare Managementprozesse (Good

Practices) zu etablieren, die ein übergreifendes und durchgängiges IT-Service-Management ermöglichen. Dies beinhaltet unter anderem die standardisierte Bearbeitung von Störungen über Providergrenzen hinweg (Incident Management) oder Wartungsmaßnahmen (Change Management) bis hin zur Sicherstellung und Einhaltung einer Qualitäts- und Quantitätsgüte bei der vereinbarten Serviceleistung (Service Level Management).

Die Betriebsführung im IT-System der Bundeswehr konzentriert sich daher genau auf die für den Betrieb notwendigen operativen Prozesse und schafft somit Handlungssicherheit für die jeweiligen IT-Kräfte.

Hierbei trägt eine Betriebsführungseinrichtung als Organisationselement die Gesamtverantwortung für den Betrieb, das heißt, sie stellt die IT-Services des IT-Systems der Bundeswehr als Ganzes, inklusive dessen Teile in einem Einsatzgebiet, sicher.

Die Betriebsführungsorganisation steht bei jedem Provider auf mindestens drei Säulen: einem Network Operations Centre (NOC) zur Überwachung des IT-Systems im eigenen Verantwortungsbereich, einem zentralen Service Desk (SD) zur Bearbeitung und Steuerung von Service Requests (Nutzeranfragen) sowie einer Transition Cell (TC) zur Planung und Steuerung von Veränderungen am IT-System. Möglich ist die Aufnahme weiterer Elemente in die Betriebsführung, zum Beispiel einer Cyber Security Operations Cell (CSOC), die Aspekte der Informationssicherheit verantwortet.



▲ ITIL stellt die Kundenbedürfnisse in den Vordergrund und fragt, welche Technologien und Verfahren diese in geeigneter Weise erfüllen können: Die Phasen von ITIL v3.
Grafik: axelos.com

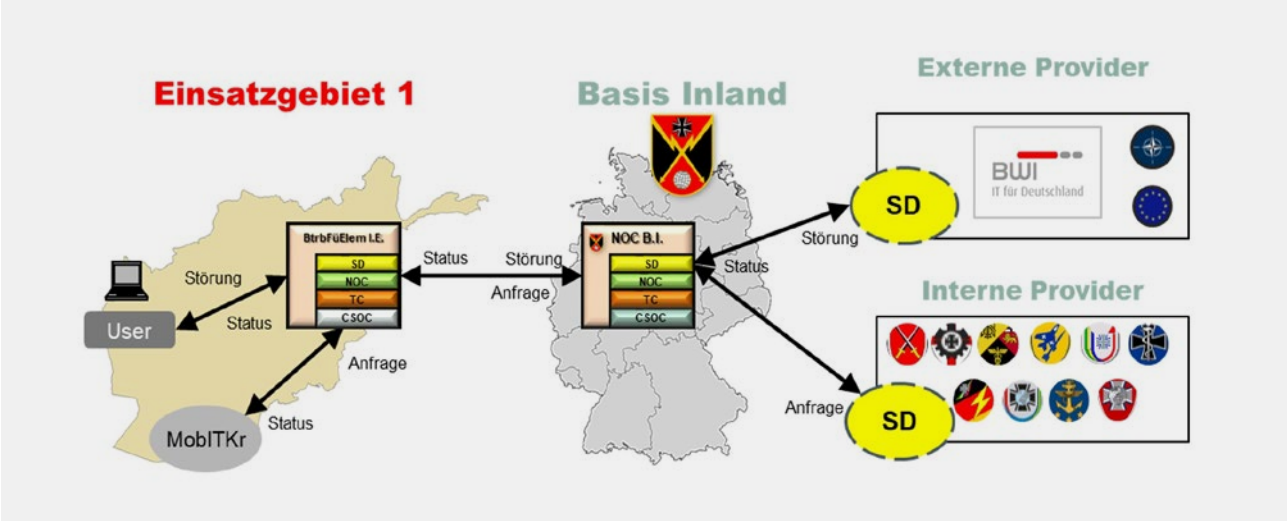
▼ Das IT Center MINUSMA: Eine mit IT-Arbeitsplätzen eingerüstete Containerlösung für alle IT-Kräfte des Einsatzkontingents zur Vereinfachung der Arbeitsprozesse.
Foto: Atos/Steffen Liebich

WIESO IT-SERVICE-MANAGEMENT UND BETRIEBSFÜHRUNG AUCH IM EINSATZ?

Der Einsatz, Betrieb und Schutz des IT-Systems stützt sich auf das IT-Service-Management der jeweils beauftragten IT-Serviceprovider ab.

Im Rahmen der Servicebereitstellung für Einsätze werden IT-Services von IT-Kräften vor Ort und zunehmend auch von Kräften der Basis Inland beziehungsweise weiterer ziviler Serviceprovider den Nutzerinnen und Nutzern zur Verfügung gestellt. Eine solche providerübergreifende Bereitstellung beispielsweise durch Einsatzkontingent, Betriebszentrum IT-System der Bundeswehr (BITS) und BWI, erfordert ein konsolidiertes und koordiniertes Vorgehen.

Die geforderte Servicequalität und -quantität kann allein über ein durchgängiges IT-Service-Management sichergestellt werden, da nur so alle Prozesse und Aktivitäten einheitlich und nach einem gemeinsamen Standard unter Einhaltung vereinbarter Parameter und Servicelevel durchgeführt und überprüft werden können. Insgesamt trägt dieses – im besten Fall harmonische – Zusammenspiel zwischen Basis Inland und Einsatz zur Entlastung der IT-Kräfte vor Ort bei.



DER ROLLOUT EINER ITSM-UMGEBUNG (ITSM-ENVIRONMENT) FÜR MINUSMA

Der Begriff IT-Service-Management Environment (ITSME) ist eine herstellerneutrale Bezeichnung für die vom BITS betriebene Managementplattform, um einen Großteil der IT-Service-Management-Prozesse abzubilden.

Der zentrale Betrieb der ITSME und die Weiterentwicklung der ITSM-Prozesse mit der entsprechenden technischen Hinterlegung obliegt der Abteilung IT-Management im BITS. Für die Betriebsführung und damit auch für den Einsatz werden die operativen Prozesse Request Fulfillment, Incident Management, Change-Management sowie Service Asset and Configuration Management betrachtet.

Die Einhaltung dieser Prozesse garantiert für den Einsatz MINUSMA den Nutzern im Einsatzland eine unterbrechungsfreie Bereitstellung der notwendigen IT-Unterstützung.

Am 1. Juni 2022 wurden mit dem IT Center MINUSMA (ITC MINUSMA) die infrastrukturellen Grundvoraussetzungen für die Einführung einer Betriebsführungseinrichtung unter Nutzung einer ITSME geschaffen. Hierzu wurde in einem enormen planerischen und logistischen Aufwand eine mit IT-Arbeitsplätzen eingerüstete Containerlösung konzipiert, in der die IT-Kräfte des Einsatzkontingents räumlich kolloziert werden, um Abläufe der Arbeitsprozesse zu vereinfachen. Zusammen mit der Anbindung des ITC MINUSMA an die ITSME bis spätestens zum Jahresende 2022 ist sichergestellt, dass das deutsche Einsatzkontingent in naher Zukunft in das harmonisierte ITSM der Streitkräfte integriert sein wird.

Im Vorfeld müssen dazu, in enger Abstimmung mit dem Einsatzkontingent, die für MINUSMA relevanten IT-Services identifiziert und die individuellen Anforderungen an jeden einzelnen IT-Service zunächst erfasst und in sogenannten IT-Service-Steckbriefen verankert werden. Ebenfalls gilt es, die Rollen und Berechtigungen der Nutzer der ITSME auf Grundlage administrativer und organisatorischer Vorgaben an die Einsatzrealität anzupassen. Insbesondere die Dislozierung des Einsatzkontingents auf die Standorte Gao, Niamey und Bamako stellt hierbei eine besondere Herausforderung dar. Nach Klärung der oben genannten Fragestellungen wird durch das BITS die ITSME entsprechend konfiguriert und anschließend remote (über Webbrowser) im Einsatzland bereitgestellt.

Mit der erfolgreichen Anbindung des Einsatzes MINUSMA in ein durchgängiges IT-Service-Management, welches bereits im Einsatz RESOLUTE SUPPORT in Afghanistan äußerst erfolgreich etabliert und bis zu seinem Redeployment genutzt wurde, wird ein weiterer wichtiger Schritt zu einer Harmonisierung der IT-Serviceerbringung der Streitkräfte abgeschlossen, um die Führungsunterstützung in den Einsatzgebieten und der Basis Inland schneller, effektiver und effizienter sicherzustellen.

▲ Durchgängige Betriebsführung von der Basis Inland bis in den Einsatz.
Grafik: Bundeswehr/BITS

Ausbildung: Neben den rein technischen und organisatorischen Planungsschritten, die zur Etablierung einer ITSME im Einsatz notwendig sind, ist die Ausbildung der betroffenen Rolleninhaber im Einsatzkontingent essenziell für eine erfolgreiche Umsetzung eines durchgängigen ITSM.
IT-Training Centre (ITTC) Lohheide: Durch die BWI bereitgestellte(s) Infrastruktur und – auf der Zeitachse – Ausbildungspersonal. Hier soll kurzfristig eine „Einsatzland-spezifische Ausbildung (ELSA) ITSM" etabliert werden und als Pflichttor vor jedem Einsatz durchlaufen werden.
Lehrgang IT-Schule der Bundeswehr: Der Lehrgang „Betriebsführung in Betriebsführungseinrichtungen/Betriebsführungselement" an der IT-Schule der Bundeswehr findet regelmäßig mehrmals jährlich statt und deckt Grundlagen der Betriebsführung sowohl theoretisch als auch mit einem generischen praktischen Anteil ab.
Übungen wie GELBER MERKUR: In Übungen wie zum Beispiel dem GELBEN MERKUR werden Abläufe der Betriebsführung unter Verwendung einer Übungs-ITSME einmal im Jahr eingeübt.

DIGITAL IN BEREITSCHAFT: VERTEIDIGUNGSEXPERTEN ERPROBEN INNOVATIVES WORKSHOP-FORMAT

Aktueller konnte ein Workshop rund um Digitalinnovationen im Verteidigungsbereich nicht sein: mit dem Angriff Russlands auf die Ukraine hat sich der Blick Deutschlands auf die Verteidigungsfähigkeit des eigenen Landes und als Bündnispartner geändert. In seiner Regierungserklärung vom 27. Februar dieses Jahres kündigte Bundeskanzler Olaf Scholz ein Sondervermögen von 100 Milliarden Euro für die Bundeswehr an – eine Trendwende nach jahrelanger Abrüstung und sinkenden Militärausgaben.

Diese aktuelle Entwicklung bildete den Hintergrund, als am 30. Juni 2022 der Verein AFCEA und IBM zu einem eintägigen Workshop in die Bonner IBM Garage for Defense einluden. Rund dreißig Digitalexperten aus Bundeswehr und Wirtschaft versammelten sich, um gemeinsam nach den Methoden der IBM Garage „Innovationen zum Anfassen" zu entwickeln.

Anhand der Frage, wie die Liegenschaft der Zukunft aussehen soll, übten sich die Teilnehmer intensiv in agilen Arbeitsweisen und Design Thinking bis hin zur Erstellung von Lösungsansätzen und Prototypen.

SCHNELLE KOMMUNIKATION UND DATENANALYSEN IN ZUKUNFT ENTSCHEIDEND

Angesichts der veränderten Weltlage waren sich die Teilnehmer der Brisanz des Themas bewusst: die Digitalisierung ist ein Schlüsselbereich bei der Weiterentwicklung der Bundeswehr, gerade auch im Hinblick auf ihre neuen Aufgaben. Schnelle Kommunikation und Datenanalysen beispielsweise können heute im Konfliktfall mit entscheidend sein, um die richtige Strategie für die jeweilige Situation zu erarbeiten. Und um die Chancen der Digitalisierung voll zu nutzen, braucht es Entwicklungsmethoden,

die Projektziele, mögliche Sicherheitsrisiken und die speziellen Anforderungen im Verteidigungsbereich miteinander in Einklang bringen.

„Rund 260.000 Menschen sind bei der Bundeswehr beschäftigt – bei dieser Größe Innovationen schnell auf den Weg zu bringen, ist naturgemäß eine komplexe Aufgabe. Doch angesichts der rasanten Veränderung des sicherheitspolitischen Umfelds müssen die Streitkräfte sowie die Sicherheits- und Verteidigungsindustrie heute schnell und flexibel auf Herausforderungen reagieren können. Diese Anforderungen bilden die Methoden des Workshops in der IBM Garage ab – sehr spannend und inspirierend, diesen Prozess live mitzuerleben", sagt Oberstleutnant i.G. Tim Frenzel vom Kommando Cyber- und Informationsraum.

AGILE ZUSAMMENARBEIT IN AKTION

Schnelles und flexibles Arbeiten, genau darauf ist das neue innovative Workshop-Format der AFCEA mit der IBM Garage for Defense ausgerichtet: Die enge räumliche Zusammenarbeit in den Bonner Räumlichkeiten verkürzt Entwurfs- und Entwicklungszeiten stark. Kontinuierliches, direktes Feedback der Kunden an die Entwicklungsteams führt dazu, eventuelle Probleme frühzeitig zu erkennen und noch im Entwurfsprozess zu beheben. Zu welchen schnellen Erfolgen die Vorgehensweise in der Praxis führt, das konnten die Innovationsbeauftragten aus Industrie, Bundeswehr und Sicherheitsbehörden an diesem Tag in Aktion erleben.

◀ Haptisches Erleben, zum Beispiel mit LEGO, unterstützt den kreativen Prozess.

▼ Das IBM Garage Modell besteht aus drei Phasen: Co-Create, Co-Execute und Co-Operate.
Foto/Grafik: IBM

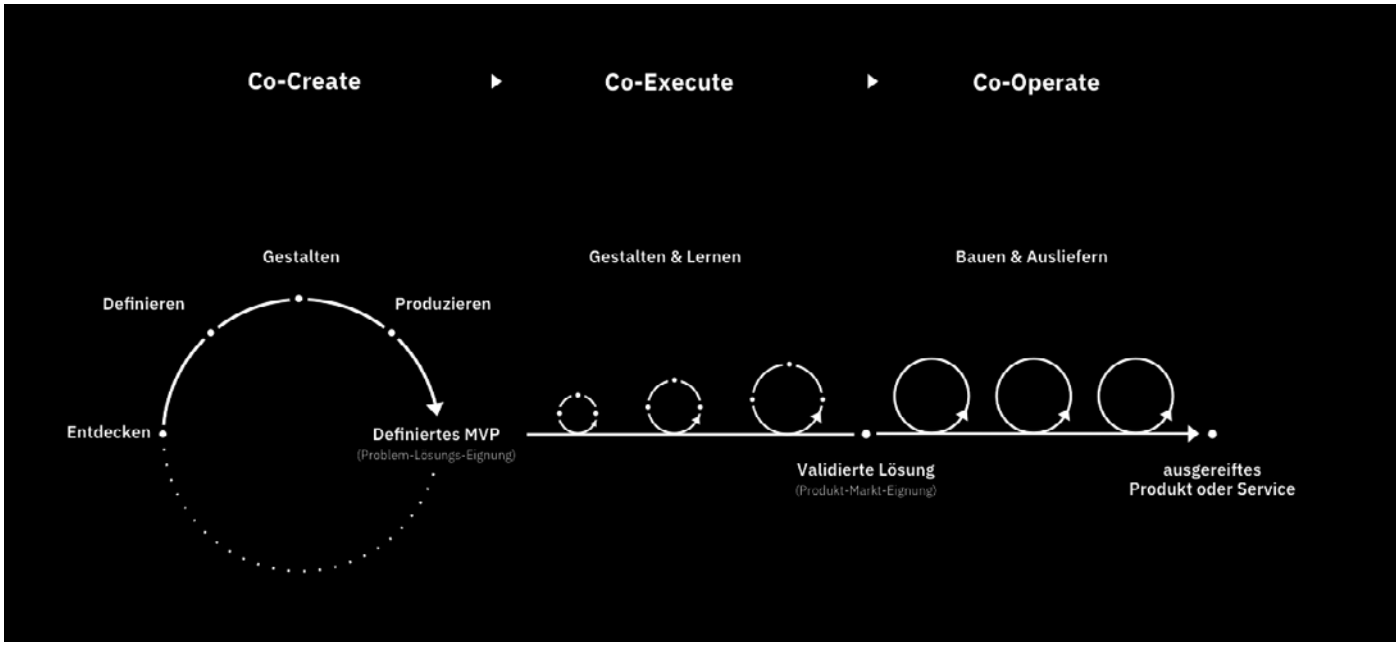
Nach der Begrüßung durch den AFCEA-Vorsitzenden Brigadegeneral Armin Fleischmann, die Beauftragte für Innovation im AFCEA-Vorstand Marianna Schwarz sowie den IBM iX Lead der IBM Garage for Defense Dr. Christian Weber ging es gleich in die Vollen: in einer kurzen Vorstellungsrunde klärten die Teilnehmer ihre Erwartungen an die Veranstaltung. Dann erläuterten die Organisatoren das Vorgehen, das an das dreiphasige Innovationsmodell der IBM Garage angelehnt war: Co-Create, Co-Execute und Co-Operate. Daraufhin wurden die gemischten Workshop-Teams eingeteilt.

In der ersten Session entwickelten die Teilnehmer zunächst Personas rund um die Thematik Liegenschaft der Zukunft. Im anschließenden Workshop ging es aufbauend auf den Analyse-Ergebnissen um die Ideenfindung zur Frage, wie die Soldatinnen und Soldaten zukünftig zusammenleben und arbeiten sollten und welche Art digitaler Lösungen dabei eine Rolle spielen könnten. Im dritten Workshop entwickelten die Teams dann bereits Konzepte, wie sich die digitalen Innovationen ganz konkret auf den Weg bringen lassen. Am späteren Nachmittag kamen dann alle Teilnehmer zusammen, um die Ergebnisse vorzustellen und zu diskutieren.

DIREKTER VERGLEICH MIT LIZA

Besonders reizvoll für die Teilnehmer war der Umstand, dass sie die Ergebnisse des Workshops mit denjenigen der BWI innoX Innovationskampagne von 2020 vergleichen konnten. Diese wurden von Tobias Orthey von der BWI GmbH vorgestellt. Auch im Rahmen des BWI-Projekts ging es unter anderem um den Themenkomplex Liegenschaften. Im Bereich technische Gebäudeausstattung hatte dort das BWI-Team die Idee zu „LiZA".

Die Grundidee: wenn alle Daten der Bundeswehr Büro- und Gebäudetechnologien konsequent miteinander vernetzt werden, lässt sich nicht nur der Komfort der Mitarbeitenden verbessern, sondern auch die Effizienz und Sicherheit an



▲ Teilnehmer des Workshops aus Industrie und Bundeswehr/BWI bei der Diskussion von „Big Ideas". Foto: IBM

Bundeswehrstandorten erhöhen. Dazu müsste eine zentrale Programmierschnittstelle entwickelt werden, die alle Endpunkte analog wie im Smart Home miteinander verbindet – so die Idee hinter LiZA.

Erstaunlich war für die Teilnehmer der Umstand, dass sie mit dem Garagen-Ansatz in kurzer Zeit auf ähnliche Ideen gekommen waren. Das war auch eines der Themen der abschließenden Feedback-Runde, in der die Teilnehmer ihre Erfahrungen und Ideen zum gerade durchlaufenen Workshop-Format teilten. Besonders positiv vermerkten sie, dass das Format sehr stark zur aktiven Teilnahme motiviert, unterschiedliches Wissen und Können zusammenbringt und in kurzer Zeit zu sehr praktischen, realitätsnahen Lösungsansätzen führt.

WICHTIGE ÜBUNG FÜR DIE ZUKUNFT

Das Feedback spiegelt auch das Konzept der IBM Garage for Defense wider: „Mit unserem Vorgehensmodell wollen wir die richtigen Spezialistinnen und Spezialisten, angewandte Technologie und neue Formen der Zusammenarbeit zusammenführen, um innovativ zu werden. Unser Motto ist es, die Geschwindigkeit eines Startups mit der Kraft einer großen Organisation zu vereinen, um die digitale Transformation der Streitkräfte in Deutschland und Europa voranzubringen", so Christian Weber. „In der Garagen-Methodik sind alle Schritte integriert, die dafür notwendig sind – von der ersten Idee über die skalierte Implementierung bis hin zum erforderlichen Kulturwandel. Dies konnten wir in den Grundzügen für die Teilnehmer heute erlebbar machen."

Maßgeblich vorangetrieben wurde der Workshop von den Mitveranstaltern der AFCEA Bonn e.V.. „Die AFCEA verfolgt als Verein das Ziel, seinen Mitgliedern und der interessierten Öffentlichkeit ein Forum moderner Informations- und Kommunikationstechnologie zu bieten. In diesem innovativen Workshop-Format konnten die Teilnehmer gemeinsam ihre Vorstellungskraft entfesseln und einen Eindruck davon gewinnen, wie schnell Innovationen auch im Verteidigungsbereich vorangetrieben werden können", sagte Marianna Schwarz, Beauftragte für Innovation im Vorstand des AFCEA Bonn. Der Verein umfasst über 1.000 Mitglieder und mehr als 100 Firmen, zu denen neben den Großen der IT- und Kommunikationsbranche eine Vielzahl mittelständischer und kleinerer Unternehmen vornehmlich aus der Region Bonn-Köln-Koblenz gehören.

Vorsitzender des AFCEA ist Brigadegeneral Armin Fleischmann, der ebenfalls am Workshop teilnahm. „Die jüngsten Entwicklungen der weltweiten Sicherheitslage zeigen, wie schnell sich heute die Verhältnisse ändern können und wie wichtig es ist, flexibel auf neue Ereignisse reagieren zu können. Dafür ist dieses Workshop-Format eine interessante und wichtige Übung gewesen, von der wir in Zukunft profitieren können."

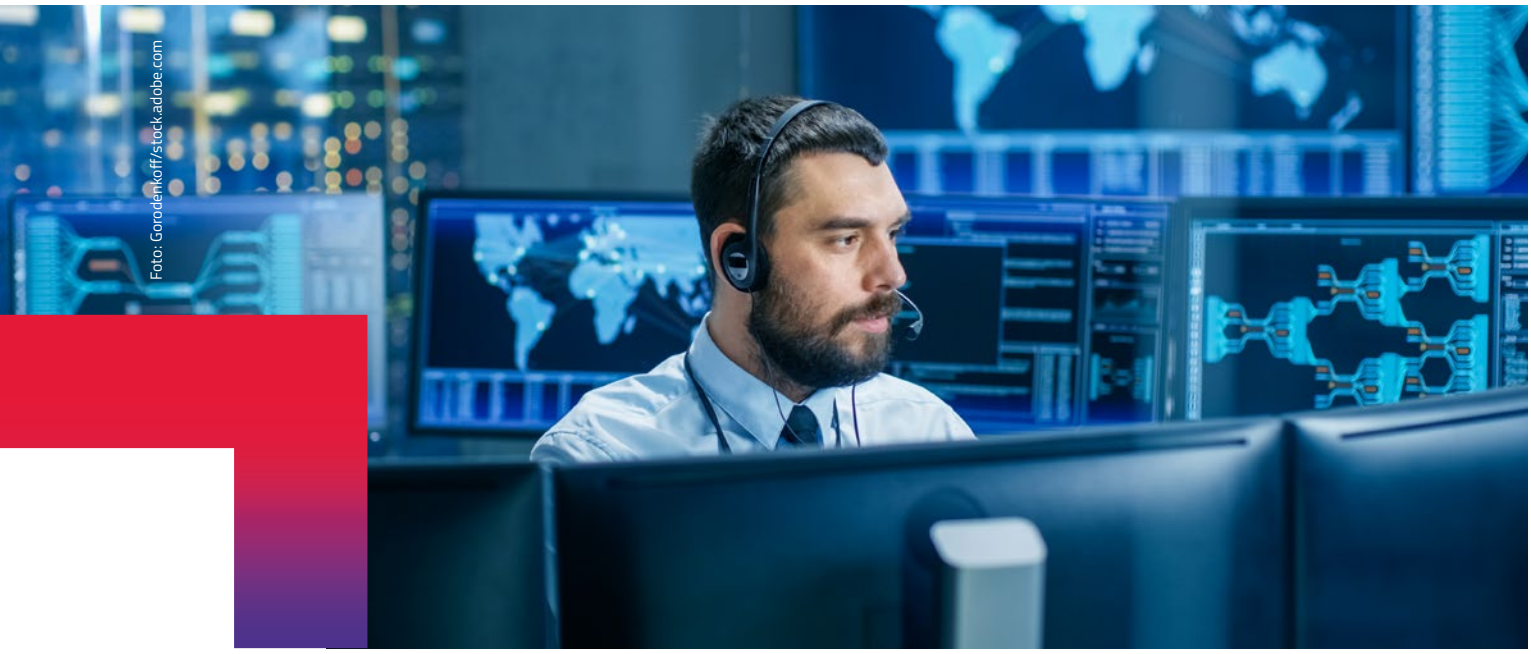


Foto: Gorodenkoff/stock.adobe.com

CGI – Wir machen Digitalisierung

CGI Deutschland B.V. & Co. KG ist die unabhängige deutsche Tochter von CGI Inc., einem der weltweit größten Unternehmen für IT- und Geschäftsprozess-Dienstleistungen. In Deutschland sind 4.500 Mitarbeitende in 27 Städten beschäftigt – davon etwa 700 im Bereich Defence, Intelligence und Space mit Schwerpunkt in Köln. Viele von uns sind ehemalige Angehörige der Streitkräfte.

Seit über 46 Jahren unterstützen wir die Bundeswehr mit umfassenden IT-Lösungen und Beratungsdienstleistungen, im Grundbetrieb wie in Übungen und Einsätzen.

Wir sind dankbar für das Vertrauen, das unsere Kunden in uns setzen: Das **Har**monisierte **F**ührungs- und **I**nformationssystem der **S**treitkräfte (**HaFIS**) / **G**erman **M**ission **N**etwork (**GMN**), das **i**ntegrierte **M**arine-**E**insatz-**R**ettungs**z**entrum (**iMERZ**) oder auch das Europäische Satellitennavigationssystem GALILEO mit dem **P**ublic **R**egulated **S**ervice (**PRS**) zählen zu einer Auswahl erfolgreicher Projekte in unterschiedlichen Dimensionen.

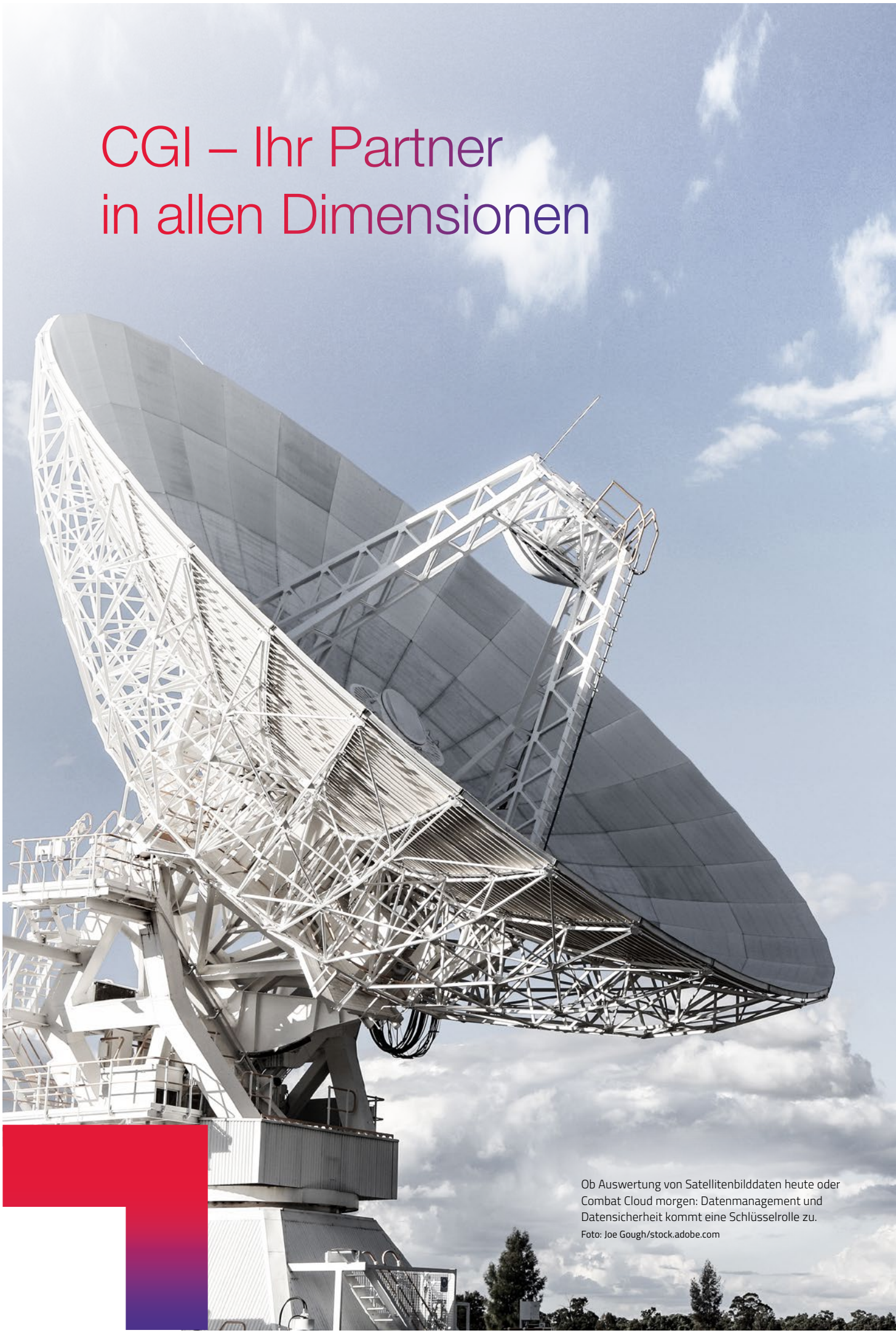
Ob auf NATO-Ebene, mit dem **D**ocument **H**andling **S**ystem (**DHS**), oder im Nationalen mit dem **Dok**umenten-**M**anagement-System der **B**undes**w**ehr (**DokMBw**), die Leistungen unserer Entwicklerteams sind weltweit bekannt und in der Nutzung. Auch im zivilen Sektor finden sich unsere einzigartigen Lösungen wie das **Lobbyregister des Deutschen Bundestags** oder auch das redaktionelle **C**ontent-**M**anagement-**S**ystem (**CMS**) dira!, welches unter anderem in **öffentlich rechtlichen Rundfunkanstalten** zu finden ist.

Die Spannweite unserer Kunden umfasst neben **NATO**, **Bundeswehr** und dem **B**undes**m**inisterium der **V**erteidigun**g** (**BMVg**) auch Kunden wie den **Deutschen Bundestag**, Inhouse-Gesellschaften der Bundeswehr wie die **H**eeres**i**nstandsetzungs**l**ogistik (**HIL**) oder die **BWI**, das **D**eutsche Zentrum für **L**uft- und **R**aumfahrt (**DLR**), die **E**uropean **S**pace **A**gency (**ESA**), die **V**ereinten **N**ationen (**VN**) oder die EU-Kommission.

Von IT-Beratung über Systemintegration und Softwareentwicklung bis hin zum Outsourcing arbeiten wir gemeinsam mit der Bundeswehr daran, ihre Führungsfähigkeit zukunftsfähig zu gestalten, die Stabs- und Verwaltungsarbeit zu digitalisieren und schutzbedürftige Daten sicher zu verarbeiten.

www.cgi.com

CGI – Ihr Partner in allen Dimensionen



Ob Auswertung von Satellitenbilddaten heute oder Combat Cloud morgen: Datenmanagement und Datensicherheit kommt eine Schlüsselrolle zu.
Foto: Joe Gough/stock.adobe.com

„Die Elemente, die zu bestimmten Dimensionen gehören, wollen wir wieder enger zusammenführen. Wir wollen mehr geschlossene Verbände aus dem Stand heraus verfügbar machen“

General Eberhard Zorn, Generalinspekteur der Bundeswehr

Die Bedrohungsszenarien haben sich über die Jahre stetig weiterentwickelt. Ob Aufklärung, Kommunikation oder Lageerfassung inklusive Simulationen – die Bedeutung von Informationsüberlegenheit nimmt stetig zu. Damit rückt die Dimension Weltraum zunehmend in das Blickfeld von Streitkräften. Wir unterstützen die Streitkräfte hier bereits beim Empfang und bei der Auswertung von Satellitenbilddaten für die strategische Aufklärung, aber auch mit Software für die Informationssammlung im Militärischen Nachrichtenwesen. Im Rahmen von nationalen und internationalen Raumfahrtmissionen liefern wir zudem moderne Lösungen und Know-how für sicherheitskritische Anwendungen; darunter auch militärisch relevante Missionen wie GALILEO/PRS, Heinrich-Hertz-Mission und zukünftige SatCom-Konstellationen im niederen Erdorbit.

Datenmanagement und Datensicherheit

Die technologischen Entwicklungen im Weltraum und die Rolle von zukünftigen Satellitensystemen eröffnen ungeahnte Möglichkeiten. Die Wichtigkeit dieser Dimension lässt sich unlängst in den kriegerischen Auseinandersetzungen erfahren. Um auch in Zukunft mit unseren Streitkräften handlungsfähig zu bleiben, dürfen wir den Weltraum nicht ignorieren. Schon heute ist die Sicherheit von Daten aus dem Weltraum von höchster Relevanz zur Beurteilung von Lagen.

Mit Blick aus dem Weltraum schauen wir auf all die darunterliegenden Dimensionen, die untereinander vernetzt kommunizieren müssen. In jeder dieser Dimensionen findet sich unsere Expertise. Bereits heute sind das Datenmanagement und die Datensicherheit Kernelemente aktueller Missionen und Operationen. Wir verfügen durch intelligente Vernetzung über die Expertise in der IT und Sicherheit. In vertrauensvoller Zusammenarbeit mit industriellen Partnern und Behörden nehmen wir an Initiativen in den Bereichen Multi-Domain Netzwerk, im elektronischen Dokumentenmanagement und Cyber Security teil. Gemeinsam mit unseren Kunden planen und beteiligen wir uns an den zukünftigen Operationen für die Future Combat Cloud und an einer sicheren Datennetzstruktur.

Systemintegration und Entwicklung mit der Perspektive der Nutzer

Die kommenden Jahre werden in den unterschiedlichen Dimensionen mit teilweise schon bekannten Großvorhaben die Fähigkeiten unserer Streitkräfte und ihrer Partner signifikant steigern. Wir werden in diesen spannenden Projekten als vertrauenswürdiger Partner bereitstehen und unsere Expertise aus der Vielzahl von erfolgreichen Systemintegrations- und Entwicklungsprojekten in die Technologievorhaben der Zukunft einbringen. Besonders die Erfahrungen im Bereich von komplexen, zum Teil weltraumgestützten Netzwerken und der Softwareentwicklung für die unterschiedlichen Teilkomponenten in Großgerät zeugen von der zielgerichteten Herangehensweise unserer Mitarbeiter. Dieses gelebte Selbstverständnis resultiert nicht zuletzt aus einer Vielzahl ehemaliger Angehöriger der Streitkräfte in unseren Reihen, die mit eigenen Erfahrungen an Systemen als frühere Anwender, aber auch mit dem früheren Blick aus der Truppe heraus, bestmögliche Grundlagen für die Kameradinnen und Kameraden im Einsatz generieren.

Die Zukunft des Gefechtsfeldes liegt nicht in einer Dimension allein. Der Blick „von oben“ kann helfen, die Bedarfe an zukünftige Technologien und die durchgängige Konnektivität aller Teilsysteme schon heute vor- und mitzudenken. Unser Team von CGI steht bereit, um dimensionsübergreifend zu unterstützen – vom Weltraum bis zum abgesessenen Soldaten im Feld!

Trusted Advisor der NATO

Tasker Tracker Enterprise, TT+, DHS, AMN Enterprise Portal – wer einmal in einem NATO Command gearbeitet hat, kennt sie. Doch wussten Sie, dass diese Tools von uns stammen?

Im Jahr 2007 führte die NATO unser, auf Basis von Microsoft SharePoint entwickeltes, Document Handling System (DHS) ein. Von Mons über Izmir bis Norfolk: An etwa 30 Standorten löste es die lokalen File Services ab und wurde für über 45.000 Nutzer zum neuen Standard für fachgerechte Dokumentenhandhabung – standortübergreifend und bis zum Geheimhaltungsgrad „NATO Secret“.

Neues Level für die gesamte IKM-Landschaft

Zur elektronischen Aufgabenverwaltung nutzt die NATO ihre Software Tasker Tracker (TT+). Auch hier unterstützten wir schon früh bei der Implementierung und Weiterentwicklung.

Aufgrund unserer Erfahrung dürfen wir nun seit 2022 die Modernisierung des kompletten Information and Knowledge Managements (IKM) der NATO begleiten. So heben wir gemeinsam, neben Tasker Tracker und dem Dokumentenmanagement, auch das NATO-Intranet auf die nächste Stufe. Hilfreich ist dabei, dass viele von unseren Experten bei den Streitkräften gedient haben und damit die Nutzerperspektive in die Entwicklung einbringen können.

Von DHS zu DokMBw

Wir glauben daher begründet von uns sagen zu können: Wir sind Experten für die Digitalisierung der Stabs- und Verwaltungsarbeit – bei der NATO, aber auch bei der Bundeswehr.

Denn das von uns für die NATO entwickelte Document Handling System haben wir zusammen mit der Bundeswehr für ihre Zwecke weiterentwickelt: zum Dokumentenmanagementsystem der Bundeswehr (DokMBw). Es befindet sich aktuell in der zweiten Ausbaustufe und soll im Zielzustand allen bis zu 200.000 Nutzenden der Bundeswehr die Stabs- und Verwaltungsarbeit erleichtern. Die User profitieren dabei von den Erfahrungen, die wir bei der NATO sammeln konnten: Ein Manager nannte es einmal „eine lange Kette von Synergieeffekten“, ganz im Sinne von „Smart Defence“.

End-to-End Services

Die Softwareentwicklung ist dabei nur ein Teil dessen, wie wir uns einbringen. Zusätzlich unterstützen wir mit Projektmanagement, der Analyse von Anforderungen, mit Training des Personals und schließlich mit Support im laufenden Betrieb, auch als Managed Service. Und das nötigenfalls auch im Einsatz, wie zum Beispiel in Afghanistan und KFOR.

Wir von CGI sind stolz darauf, das militärische und zivile Personal in den NATO Commands bei der Stabs- und Verwaltungsarbeit zu entlasten – als *der* langjährige Partner der NATO im Bereich Information and Knowledge Management.

▲ Neben Tasker Tracker und dem Dokumentenmanagement zählt beispielsweise auch das Intranet zu den Projekten von CGI innerhalb der NATO.
Foto: Pixel-Shot/stock.adobe.com

CGI als Enabler für die Deutsche Marine

Wir bei CGI decken mit unserem Portfolio wesentliche Anteile in der Dimension See ab. Betrachten wir die Einheiten der Marine, so fällt schnell auf: Neben den schiffbaulichen Komponenten macht die Integration administrativer, operativer sowie medizinischer Anteile ca. 75% eines Kriegsschiffes aus. Hier unterstützen wir als CGI die Hauptauftragnehmer aus einer Hand bei der zuverlässigen Führung der Unterauftragnehmer, um ein schnittstellenübergreifendes und bruchfreies Zusammenwirken aller Teilsysteme zu gewährleisten.

Enabler während des gesamten Lebenszyklus eines Systems

Dank vielschichtiger Erfahrungen und einem immerwährenden Austausch in nationalen und internationalen Projekten gelingt es uns, zukunftsfähige und somit nachhaltige Lösungen zu entwickeln, die den anspruchsvollen Einsatzszenarien der Deutschen Marine entsprechen und die Handlungsfähigkeit deutscher Soldatinnen und Soldaten aufrechterhalten. Unser Unternehmen hat sich im Bereich der Marinetechnik als Systemhaus, als „One-Stop-Shop“, etabliert. Der Fokus liegt auf den Bereichen Domainübergänge, Einsatzsysteme, aber auch medizinische Netzwerke. Die Elemente der administrativen, operativen und medizinischen Anwendung werden durch uns zusammengeführt und verbinden sich so zu einem funktionsfähigen Gesamtsystem. Hierfür harmonisieren wir die unterschiedlichsten Produkte verschiedener renommierter Hersteller und auch kleinerer Unternehmen und steuern so, als Unterauftragnehmer des Generalunternehmers, alle Phasen des Lebenszyklus der Teilelemente seines Bereiches. Von der Designphase über Zulassungs- und Zertifizierungsverfahren bis hin zum Betrieb, inklusive Ausbildungsanforderungen betreuten wir seine Projekte einschließlich des Obsoleszenzmanagements. Dieses Selbstverständnis, mit Blick auf die notwendigen Maßnahmen zur zielgerichteten Nutzung, leitet sich auch durch die Vielzahl von ehemaligen Soldatinnen und Soldaten innerhalb des Unternehmens ab, die stets nicht nur mit Blick auf die Erfüllung von Verträgen arbeitet, sondern die soldatischen Nutzenden im Fokus haben.

Belastbare Konzepte von Anfang an

In unseren Lösungsansätzen setzen wir auf Anwendungen, die auch in vielen Jahren noch „State-of-the-Art“ sind und somit den Anforderungen des Gefechtes der Zukunft entsprechen. Hierfür beteiligen wir uns regelmäßig an Zukunftsstudien, in die wir den Input unseres stetig wachsenden Netzwerks an Suppliern einfließen lassen und somit als High-Level-Domain-Consultant unsere Erfahrungen schon heute in zukünftige Projekte einsteuern. Ein signifikanter Unterschied zu vielen anderen Unternehmen zeigt sich nicht nur durch den bereits beschriebenen ganzheitlichen End-to-End-Ansatz, sondern auch in der Fähigkeit, Architekturen bereits während der Designphase vorzertifizieren zu lassen und somit bereits bei Angebotsabgabe mit einem belastbaren Konzept anzutreten. Nicht zuletzt die Zufriedenheitswerte der Kunden mit unserem Unternehmen beziffern unsere Leistungsfähigkeit und erklären das Vertrauen, das in unser Unternehmen gesetzt wird.

„Schwimmendes Krankenhaus“: integriert von CGI

Eines unserer aktuellen Projekte im Bereich der Deutschen Marine ist die Integration des Marine-Einsatz-Rettungszentrums (MERZ) als integriertes Zentrum (iMERZ) auf den Einsatzgruppenversorgern. Aber auch in den Bereichen Kommunikation, Combat Management System, Command and Control Information System oder in dem komplexen Umfeld des Nachrichtenwesens finden sich in diversen deutschen Projekten und Systemen Architekturen aus unserem Hause. Es gilt vielleicht ein universeller Grundsatz, der auf CGI zutrifft: Nur weil nicht CGI draufsteht, heißt das nicht, dass CGI nicht drin ist.

▶ Im Bereich Marinetechnik führen wir die Elemente der administrativen, operativen und medizinischen Anwendung zusammen und verbinden sie zu einem funktionsfähigen Gesamtsystem.
Foto: Nikonaft/Shutterstock.com

CGI Deutschland – Spezialist für Softwareentwicklung auch in sicheren Umgebungen

Software im Verteidigungsbereich muss oftmals besonderen Sicherheitsanforderungen genügen. Beispielsweise sollen Datenbankeinträge zu krisen- und kriegsrelevanten Fähigkeiten oder Algorithmen zur Entscheidungsvorbereitung nicht zum Ziel von Angreifern werden.

Bereits während der Entwicklung von Software kommt es daher darauf an, diese vor unbefugtem Zugriff zu schützen. Wie aber kann das gelingen?

Bei der Softwareentwicklung selbst ist der Einsatz von aktuellen Methoden wie SAFe und DevSecOps die Basis, um schon im Code-Design die Robustheit der Software gegenüber potentiellen Angreifern herzustellen – Stichwort „Security by Design“.

Eine eigene Entwicklungsumgebung für VS-NfD

Zusätzlich ist eine geschützte, Grundschutz konforme Umgebung der entscheidende Vorteil, um auch während der Entwicklung ein höchstes Maß an Sicherheit zu gewährleisten. Ein abgeschirmtes Netz mit eigenen Servern und Software, eigenen APC – und natürlich sicherheitsüberprüftes Personal – ermöglichen die Softwareentwicklung mit der maximal möglichen Sicherheit.

Wir verfügen über ein solches sicheres Netz: Das German Secure Network (GSN) wurde von uns eigens für die Arbeit mit schutzbedürftigen Daten entwickelt. Es ermöglicht nicht nur eine nach neusten Methoden mit dem Bedarfsträger entwickelte sichere und robuste Software, sondern auch die Entwicklungsumgebung nach höchsten Standards – alles aus einem Unternehmen.

Langjährige Erfahrung im öffentlichen und Verteidigungssektor

Insgesamt verfügen wir über mehr als 46 Jahre Erfahrung in der Softwareentwicklung mit öffentlichen Auftraggebern. Wir als CGI arbeiten in Deutschland seit Jahren erfolgreich in integrierten agilen Entwicklungsteams mit den Kunden zusammen. So entstanden in den letzten Jahren Software-Systeme wie beispielsweise das Lobby-Register des Deutschen Bundestages oder das Sendekontrollsystem dira! im öffentlich-rechtlichen Rundfunk des WDR, NDR und der BBC.

Im Defence-Bereich nutzen wir ebenfalls seit Jahren obige Methoden und Umgebungen, um das Dokumentenmanagement mit eAkte und eVorgang der Bundeswehr (DokMBw) und das Dokumentenmanagement der NATO (DHS/EDMS, TaskerTracker) auf Basis unseres Produktes eGov360 stetig in enger Abstimmung mit den Bedarfsträgern weiterzuentwickeln. Die meisten Organisationsbereiche der Bundeswehr nutzen schon heute beispielsweise zur Planung ihrer Übungs- und Ausbildungsvorhaben, zur Planung der Ressourcen der Truppenübungsplätze oder der Gefechtsübungszentren Software von CGI. Auch die Luftwaffe greift für die Steuerung und Dokumentation des Zulassungsprozesses von Luftfahrzeugen auf unsere Anwendungen zurück.

Daher freut es uns umso mehr, nun zusätzlich auch über den BWI-Rahmenvertrag Software-Engineering der Bundeswehr dieses Know-how als Spezialist für robuste Software-Entwicklung in sicheren Umgebungen – vollständig aus einer Hand – zur Verfügung stellen zu können.

Informationssicherheit: Schutz im laufenden Betrieb

Ist die Software entwickelt und implementiert, wollen sich Organisationen auch im laufenden Betrieb vor Angriffen aus dem Cyber- und Informationsraum schützen. CGI kann mit Security-Spezialisten, Security Operations Centers und Beratung dabei unterstützen. So hat beispielsweise die Weltklimakonferenz 2021 in Glasgow auf unser Cybersecurity- und Social-Media-Monitoring gesetzt: Gemeinsam konnten wir eine störungsfreie Konferenz sicherstellen.

Automatisierung und Cloudnutzung: Die Führungsfähigkeit von morgen beginnt mit dem Paradigmenwechsel von heute

Landes- und Bündnisverteidigung (LV/BV) stellt die Bundeswehr vor neue (alte) Herausforderungen. Doch die Umgebung, in der das Gefecht der Zukunft gedacht werden muss, hat sich seit der Ausrichtung auf die Fähigkeiten des Internationalen Krisenmanagements (IKM) verändert. Der Digitalisierungsgrad der Systeme ist merkbar angewachsen und besonders im Bereich der Verlegefähigkeit von Führungsinformationssystemen haben sich neue Anforderungen herauskristallisiert.

Dezentral statt zentral

Waren Rechenzentren im Umfeld von IKM noch stationär als Containerlösungen eine gute Nutzungsvariante, so zeichnet sich nun ein Bild vieler **hochmobiler** Fähigkeitsplattformen, die unabhängig von einem Basiscamp ihren Aufträgen **in der Breite** eines Gefechtsfeldes nachkommen müssen. Die Vorbereitungszeit für die Verlegung in den Einsatz wird im Rahmen LV/BV meist **kürzer** sein als es bei IKM der Fall war. Mit der Einführung von Battle Management Systemen nehmen die **Datenmengen** zu und müssen technisch verarbeitet werden.

Ausrollen fast „per Knopfdruck“

Für die hinter den Führungsinformationssystemen liegende IT heißt das: Sie kann nicht monatelang konfiguriert werden, sondern ist im besten Fall nahezu „per Knopfdruck“ ausgerollt. Die gesteigerte Rechenkapazität muss auf kleinstem Raum, in einem Luft- oder Landfahrzeug oder einer schwimmenden Einheit, Platz finden. Die bisherigen Anforderungen an Informationssicherheit und Interoperabilität gelten natürlich weiter und müssen berücksichtigt werden.

Wie lässt sich also die Führungsfähigkeit im Szenario von LV/BV im Zeitalter der Digitalisierung gewährleisten? Durch Automatisierung und Virtualisierung.

- Virtualisierung schafft die gleiche technologische Basis. Hardware-agnostisch kann eine neue Ebene zwischen Hardware und Software „vermitteln“ – unabhängig von der Plattform und Hypervisor-agnostisch, also unabhängig davon, ob die Virtualisierung über beispielsweise Microsoft oder VMWare umgesetzt wird. Damit sind alle Fahr- und Flugzeuge sowie Gefechtsstände etc. leicht miteinander vernetzbar. Durch Virtualisierung wird außerdem eine um ein vielfaches höhere Rechenleistung erzielt.

- Ein zertifizierter Ausrollprozess ermöglicht, dass jedes System, das den Prozess durchlaufen hat, direkt die Genehmigung zur Nutzung bekommt. So kann neue IT schneller in die Nutzung gehen. Dabei ist die Informationssicherheit gemäß dem Prinzip „Security by Design“ von Anfang an mitgedacht und im höchstmöglichen Maß gewährleistet.

Diese Grundsätze lassen sich innerhalb von landbasierten Operationen, aber auch in den anderen Dimensionen anwenden. Auch die Vernetzung im Bündnis ist damit zukunftsfähig möglich, Stichwort Federated Mission Networking und Multi Domain Combat Cloud.

Virtualisierung statt Software-Inseln. Automatisierung statt manueller Konfiguration. Cloudnutzung statt großer Rechenzentren. Es braucht den Paradigmenwechsel. So kann die Bundeswehr der Digitalisierung nicht nur begegnen, sondern ihre Chancen zu ihrem Vorteil nutzen. Weiter in die Zukunft gedacht, bieten Virtualisierung und Cloudnutzung zudem Vorteile beim qualitativ und quantitativ benötigten Personaleinsatz und bei der Kosteneffizienz.

Wir von CGI fühlen uns, nicht zuletzt wegen vieler ehemaliger Soldatinnen und Soldaten unter den Mitarbeitenden, der Bundeswehr und ihrem Auftrag verbunden. Es ist uns ein Anliegen, unsere Kenntnisse und Erfahrungen im Themenfeld der Führungsfähigkeit und Softwareentwicklung – national mit den verschiedenen Teilstreitkräften, z.B. im Projekt GMN/HaFIS, und international mit der NATO, z.B. mit der Modernisierung der Information and Knowledge Management Tools – im Sinne der Zukunftsfähigkeit der Streitkräfte einzubringen und zur Führungsfähigkeit von morgen beizutragen.

▲ Schneller, kleiner, interoperabel und sicher: Die Digitalisierung birgt bedeutende Chancen im LV/BV-Kontext.

◀ Software von CGI ist beim Dokumentenmanagement von Bundeswehr und NATO im Einsatz, ebenso wie beim Deutschen Bundestag.

Fotos: Gorodenkoff/stock.adobe.com

Wir sprachen mit **Dr. Pascal van Overloop**,

Industry Advisor Defense & Intelligence der Microsoft Deutschland GmbH

Dr. van Overloop, wo sehen Sie die derzeitigen und künftigen Herausforderungen des Kommandobereichs Cyber- und Informationsraum (CIR)?

Wir beobachten seit Jahren für unsere Kunden im Segment Defense & Intelligence eine sich verschärfende Bedrohungslage, die zugleich komplexer wird. Dies wird noch verstärkt durch zivile Technologien, die als Wirkmittel eingesetzt werden. Wir sehen aber auch die Besonderheiten des öffentlichen Beschaffungswesens und die zunehmende Interaktion zwischen Verbündeten und Partnern.

Heutige Streitkräfte sind zudem mit verschiedensten internen Herausforderungen konfrontiert: Fähigkeiten zur Führungsunterstützung bleiben hinter den Anforderungen moderner Einsatzbedingungen zurück – Zeit für Entscheidungszyklen reicht bei Verwendung bisheriger Technologien und Prozesse nicht mehr aus – Material und Infrastruktur veraltet – Verfahren zur Entwicklung und Beschaffung neuer Fähigkeiten sind zu langsam und starr – effektive Zusammenarbeit zwischen Partnern im Verteidigungsbereich wird immer schwieriger.

Für das KdoCIR wie auch für die gesamte Bundeswehr gilt, dass man bei der Digitalisierung mitsamt Cyber- und Data Security vorankommen, die Standardisierung, Interoperabilität und Kooperation – sowohl joint, combined als auch zivil-militärisch – verbessern, die Einsatzbereitschaft bei effizientem Ressourceneinsatz steigern und zugleich Material und Infrastruktur modernisieren muss.

Wie kann dabei Microsoft unterstützen?

Wir sehen uns als Technologiepartner bei der Bewältigung der Kernaufträge des KdoCIR wie der Aufklärung in allen Dimensionen, dem Betrieb und Schutz des ITSysBw, Unterstützungsleistungen wie der Bereitstellung von Geoinformationen und Ausbildung bis hin zur Digitalisierung, der Verbesserung der Effizienz oder des Wissensmanagements als globalen Querschnittsthemen.

Unsere möglichen Beiträge sind ebenso breit gefächert. Sie reichen von der Verbesserung der Situational Awareness und Data-driven Decision Support über Edge & Cloud Computing bis hin zur Anwendung von Mixed Reality, Künstlicher Intelligenz und DevSecOps.

Können Sie das näher erläutern und konkrete Beispiele nennen?

Aktuelles und zugleich brisantestes Beispiel ist aus unserer Sicht der Angriffskrieg Russlands auf die Ukraine. Hier konnten wir in der Ukraine dank einer rechtzeitigen Migration der staatlichen Rechenzentren in die Microsoft Public Cloud z.B. umfassende Threat Intelligence für Computernetze und Kritische Infrastruktur betreiben. Dies hilft uns bei der ständigen Verbesserung der Endpoint Protection zur täglichen Abwehr von Angriffen auf die weltweit vorhandenen Systeme, die mit Microsoft-Technologie betrieben werden. So konnten wir selbst in dieser kriegerischen Auseinandersetzung bisher unbekannter Ausprägung nicht nur den Betrieb der Netze aufrechterhalten, sondern auch Angriffe attribuieren und den Kampf gegen Propaganda und Fake News aktiv unterstützen.

Ähnliches gilt für den Betrieb der „NATO Defense Cloud“, die auf Basis unserer Technologien läuft. Dies beinhaltet auch Cybersecurity auf höchstem Niveau und die sogenannte „NATO Software Factory“, eine Umgebung für DevSecOps, also die agile Softwareentwicklung. Dabei können auf einer besonders geschützten Plattform Teil- und Zwischenversionen stetig getestet und zugleich das Know-how von Qualitätssicherung, IT-Betrieb und Endnutzern einbezogen werden. Dies klingt zunächst sehr technisch, beinhaltet aber auch tiefgreifende prozessuale und kulturelle Veränderungen. Mit deren Hilfe können moderne IT-Anwendungen entsprechend des State-of-the-Art schneller entwickelt, zuverlässig betrieben und bei Bedarf flexibel angepasst werden. Zudem können damit standardisierte Bausteine übernommen werden, was die Interoperabilität verbessert und redundanten Aufwand vermeidet.

Über Software hinaus haben wir mithilfe unserer Partner aber auch weitere Beweise für unsere Leistungsfähigkeit im militärischen Umfeld geliefert. Ich denke da an unsere Lösungen für verlegefähige oder mobile Netze oder den Einsatz der HoloLens bei der Instandsetzung von Panzern und Flugzeugen.

Was wollen Sie damit erreichen?

Unsere Mission bei Microsoft ist es, jede Person und jedes Unternehmen auf dem Planeten zu befähigen, mehr zu erreichen. Zusammen mit unseren Kunden im Bereich Defense & Intelligence wollen wir eine resiliente und effektive digitale Transformation erreichen.

Unser Hilfsmittel dafür ist die technische, prozessuale und kulturelle Adaption datengetriebener Technologien. Wichtig ist aus unserer Sicht dabei ein verantwortungsvolles Handeln. Dies umfasst den effizienten und nachhaltigen Umgang mit Ressourcen, Energie, Daten und Mensch.

Letztlich wollen wir damit als zentraler Partner die Bundeswehr in der digitalen Transformation erfolgreich machen.

Das Interview führte Matthias Wunsch

DIENSTSTELLEN-PROFIL

INFORMATIONSTECHNIK-BATAILLON 293

Das Informationstechnikbataillon 293 stellt durch Einsatz und Betrieb seiner mobilen Kräfte und Mittel des IT-Systems der Bundeswehr vorrangig die anteilige Informationsversorgung der Bundeswehr im Einsatzgebiet sicher.

AUFGABEN

- IT-Profis managen verlegefähige und mobile Anteile des IT-Systems der Bundeswehr.
- Bereitstellung von IT-Services – weltweit und 24/7.
- Beherrschen allgemeiner Aufgaben in Landoperationen der Streitkräfte.
- Beitrag zur Sicherstellung der Führungsfähigkeit der Streitkräfte.

AUFTRAG

Weitreichende Satellitenverbindungen, lokale Netzwerke oder Nutzerbetreuung sind nur einige Aufgaben des Informationstechnikbataillons 293, die zur Gewährleistung der Auftragserfüllung der Bundeswehr beitragen. Mittels der verschiedenen modernen Systeme und Servertechniken, aber auch via verschlüsselten mobilen Kommunikationsmitteln werden Sprache und Daten verarbeitet, übertragen und gemanagt. So kann das Bataillon die Führungsfähigkeit in verschiedenen Einsatzszenarien garantieren und einen erheblichen Beitrag zur vernetzten Operationsführung leisten.

Weitere Aufträge sind die Aus- und Weiterbildung. Die Soldatinnen und Soldaten werden auf Einsätze und Übungen vorbereitet. Militärische Grundfertigkeiten, wie beispielsweise die Patrouille zu Fuß, der geleitete Feuerkampf sowie die Erstversorgung von Verwundeten, müssen beherrscht werden.

Auch die Schießausbildung ist ein wichtiger Bestandteil des Soldatenberufs. Deshalb müssen auch IT-Kräfte an der Waffe ausgebildet sein, um sich und ihre Kameradinnen und Kameraden im Ernstfall verteidigen zu können. Verschiedene Schießtrainings werden jährlich durchlaufen, um in Übung zu bleiben.

ANSCHRIFT
Werdenfelser Kaserne,
Weilheimer Straße 60,
82418 Murnau am Staffelsee

DIENSTSTELLENLEITUNG
Oberstleutnant Stefan Eisinger

STAMMPERSONAL
~650

AUFSTELLUNG
01.04.1958

OBERSTLEUTNANT REINHARD LANG, REFERENT,
ABTEILUNG OPERATION, UNTERABTEILUNG J6 UND IT-SYSTEM BUNDESWEHR,
KOMMANDO CIR

ITC MINUSMA

Mit dem verlegefähigen Rechenzentrum „Information Technology Center“ (ITC) betritt die Bundeswehr Neuland: erstmals wurde ein Gefechtsstand von und ausschließlich für IT-Kräfte entwickelt. Die Bereitstellung von IT-Services und die damit verbundenen Herausforderungen lassen sich an keinem Beispiel besser darstellen.

PROJEKTBESCHREIBUNG

Ein Gesamtsystem für die Bereitstellung von IT-Services im Einsatz – geschützt, modular, verlegefähig. Mit dieser grob formulierten Idee und einer DIN-A4-Skizze des zukünftigen Rechenzentrums begann 2017 das Projekt: mit dem Information Technology Center, oder kurz ITC, wird erstmals ein Gefechtsstand exklusiv für die Bereitstellung von IT-Services entwickelt – damit geht eine durchgängige Orientierung an den Bedürfnissen der IT-Kräfte einher.

Bereits bei der Vorstellung der Projektzeitlinien wird die Dynamik und das rasante Tempo der Transformation im Bereich der Informationstechnik sichtbar. Während die ursprüngliche Bedarfsforderung nach dem geschützten Rechenzentrum 2017 noch durch das Führungsunterstützungskommando der Bundeswehr formuliert wurde, erfolgte nach dem Projektstart im Juni 2020 die Ausplanung sowie Projektbegleitung vor allem durch das Kommando Informationstechnik der Bundeswehr. Die Unterabteilung J6 und IT-Services Bundeswehr des Kommandos Cyber- und Informationsraum (CIR) läutete im Juli 2022 die Nutzungsphase ein.

Passend zum vorliegenden Sonderheft spannt das Information Technology Center also den zeitlichen Bogen – von den Anfängen des Organisationsbereichs Cyber- und Informationsraum bis zur Einnahme der neuen Struktur CIR 2.0.

Bei der Beschreibung des Vorhabens wird klar: zwischen dem Projektstart und der Nutzungsphase liegen gerade einmal zwei Jahre. Um diese – besonders für ein IT-Projekt – ambitionierte Zeitlinie umzusetzen, wird zur Realisierung auf ein sogenanntes „Rollout-Projekt" gesetzt. Der Fähigkeitsträger selbst wird extra gerüstet, bei den IT-Systemen wird auf bereits im Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAAINBw) bestehende Projekte zurückgegriffen. Der Projektumfang des ITC beinhaltet neben Design, Produktion und Systemintegration auch den Transport nach und den Aufbau in Mali selbst.

◂ ▲ Hitze und sintflutartiger Regen – Sandstürme und Gewitter: der Einsatzort des ITC MINUSMA in Gao, Mali, stellt besondere Anforderungen an den Schutz der sensiblen IT-Systeme vor den extremen klimatischen Bedingungen.

Fotos: Bundeswehr/Patrik Bransmöller (Sandsturm), Bundeswehr/Marc Tessensohn (Gewitter)




PROJEKTUMFANG

Auch wenn das Ganze mehr ist als die Summe seiner Teile, der Projektumfang ITC MINUSMA lässt sich in zwei wesentliche Elemente aufteilen: die „geschützte Hülle" und die darin verbaute Informationstechnik.

GESCHÜTZTE HÜLLE

Aufgabe der sogenannten „Hülle" ist grundsätzlich der Schutz von Personal und Material, sei es vor Beschuss, klimatischen Bedingungen, Abstrahlungen oder unbefugtem Zugang. Auch wenn das ITC auf den ersten Blick wie ein ortsfestes Gebäude aussieht, handelt es sich um eine modulare Containerbauweise, womit das System verlegefähig bleibt und weltweit eingesetzt werden kann. Neben einem ballistischen Schutz verfügt das Konstrukt zusätzlich über eine elektromagnetische Abschirmung, um einen ungewollten Abfluss von Informationen zu verhindern.

In Summe umfasst das Gesamtprojekt 41 Container in einer Standardgröße. Davon stellen 31 Container den Kern des Rechenzentrums dar, wovon wiederum 20 für den eigentlichen Betrieb genutzt werden. Die verbleibenden Container entfallen auf den gesondert geschützten Eingangsbereich sowie den Flur, der als Verbindungselement der Einzelräume, aber auch als ad hoc-Besprechungsraum dient. Neben dem Herzstück des ITC, den „Data Centers" oder Serverräumen und den darin integrierten IT-Systemen, bietet der Fähigkeitsträger unter anderem auch ein Network Operations Center (NOC) zur zentralen Überwachung des gesamten Systems sowie mehrere Arbeitsplatzcontainer in Standard- und Sonderkonfiguration. Insgesamt stellt das ITC eine Kapazität von bis zu 45 voll ausgestatteten und klimatisierten Arbeitsplätzen zur Verfügung.

Dabei wird durchgehend auf dem aktuellen Stand der Technik gerüstet: Neben einem modularen Aufbau der Arbeitsplätze selbst sind Smartboards und moderne Schließsysteme verbaut. Komplettiert wird die Ausstattung unter anderem mit Waffenhalterungen und Staumöglichkeiten für die persönliche Ausrüstung.

Ergänzt wird das Rechenzentrum um klimatisierte Peripherie: fünf Lagercontainer bieten Kapazität für empfindliche IT-Geräte, für handwerkliche Arbeiten steht zudem ein voll ausgestatteter Werkstattcontainer zur Verfügung. Die verbleibenden vier Container bilden eine Stromzone, durch die das ITC auch ohne zusätzliche Infrastruktur mit Energie versorgt werden kann.

IT-SYSTEME

Die Bundeswehr setzt bei der Bereitstellung von IT-Services im Regelfall auf einen Systemverbund. Wie sich ein Orchester aus einzelnen Instrumenten zusammensetzt, ergänzen sich auch hier mehrere spezialisierte Einzelsysteme zu einem großen Ganzen. Diese wurden speziell für den verlegefähigen Einsatz entwickelt und können bei Bedarf auch außerhalb fester Infrastruktur betrieben werden. Dazu sind die eigentlichen IT-Komponenten in sogenannte Betriebs-, Transport- und Lagerbehälter eingebaut, die unter anderem mit integrierten Klimaanlagen und unterbrechungsfreier Stromversorgungen ausgestattet sind.

Für das ITC wird zwar auf diese IT-Systeme zurückgegriffen, dabei wurden sie jedoch deutlich verschlankt. Die Hülle selbst stellt den Grundbedarf an Stromversorgung, Klimatisierung und den Schutz vor Umwelteinflüssen sicher. Damit konnte die eigentliche Ausstattung auf das Wesentliche beschränkt werden: komprimiert auf sechs Container sind alle erforderlichen IT-Systeme und diverse Informationssicherheitstechnik vorhanden. Das ITC stellt selbst einen Systemverbund dar, quasi ein Schmelztiegel für bereits eingeführte Systeme.

Im Gegensatz zur Hülle wirken diese Data Center vergleichsweise unspektakulär: in mehreren Serverschränken summen Lüfter, Statuslampen blinken dazu im Rhythmus und doch können von hier bis zu 1.000 Nutzer in bis zu drei Sicherheitsdomänen angebunden und mit IT-Services versorgt werden. Auch ist eine auf die spezielle Anwendung und den Einsatz angepasste Konfiguration möglich, um den jeweiligen Anforderungen gerecht zu werden.

◀ Jeder Container ist eine Einzel- und Maßanfertigung (oben li).

◀ Der Flur stellt die Verbindung zwischen den Funktionscontainern sicher (oben re).

◀ Ein Bürocontainer – vom Konzept zur Realisierung: In der Designphase erfolgt die Detailplanung aller Räume, 3D-Modell gerendert, um ein besseres Raumgefühl zu erzeugen. Später konnte das Modell auch mittels einer 3D-Brille interaktiv erlebt werden (unten li + re).
Fotos/Grafik: ATOS/Andreas Kaschube

BEREITSTELLUNG VON IT-SERVICES (BIT-S)

ZIELSETZUNG

Die Bereitstellung von IT-Services ist kein Selbstzweck – Schwerpunkt stellt die Führungsfähigkeit dar. Das umfasst vor allem die sichere Kommunikation zur übergeordneten Führung, aber auch zu den unterstellten Truppenteilen und Bereichen.

Zusätzlich wird damit für viele Bereiche der Bundeswehr die Basis für die grundlegende Arbeitsfähigkeit gelegt. Ohne die IT-Services wie Telefonie, Intranet, Internet, E-Mail, Druck- und Fileservice wären Arbeitsabläufe kaum denkbar – vor allem Führungs- und Stabselemente stützen sich auf die moderne Datenverarbeitung ab; fast alle Systeme und Prozesse werden durch die Informationstechnik zumindest unterstützt. Besonders im Einsatz ist eine durchgängige, zuverlässige und vor allem sichere Bereitstellung der IT-Services unabdingbar – im Ernstfall muss man sich auf eine sichere Verbindung verlassen können.

DER BETRIEB

IT-Services werden dabei fast ausschließlich von einem aus mehreren Einzelsystemen bestehenden Systemverbund bereitgestellt. Diese Zusammenstellung verschiedener Fähigkeiten ermöglicht eine gewisse Modularität und Skalierbarkeit, legt aber auch den Grundstein für die Spezialisierung in der Ausbildung des Fachpersonals.

Für den Nutzer meist unsichtbar, erstrecken sich die Mechanismen der Services in der Regel systemübergreifend über mehrere IT-Systeme. Damit werden auch einfach wirkende Vorgänge und Systematiken schnell sehr komplex, für die Koordination ist ein übergreifendes Systemverständnis erforderlich.

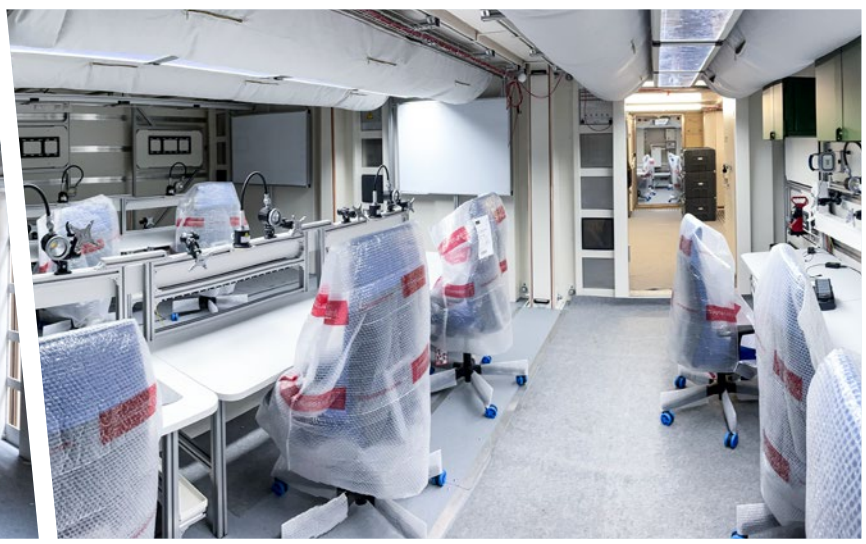
Um dieses Gesamtsystem zu beherrschen sind mehrere Elemente notwendig. Um auf die Analogie des Orchesters zurückzukommen: Wie Musiker auf ihren Instrumenten spielen, so bedienen Administratoren ihre IT-Systeme – in beiden Fällen sind Spezialisten erforderlich, um das jeweilige Arbeitsgerät adäquat bedienen zu können. Ein Trommler greift eben eher selten zur Trompete.

Das gleiche trifft auch auf die IT-Kräfte der Bundeswehr zu: auf der anderen Seite hat jedes IT-System seinen Spezialisten, der es zur Wirkung bringt. Hier gilt „Tiefe vor Breite", grundsätzlich muss jeder Administrator sein System autark bedienen können. Dabei ist die hohe Verantwortung des Einzelnen nicht zu unterschätzen: mit einem falschen Klick oder einem falschen Befehl kann nicht nur das eigene, isolierte System, sondern vielleicht sogar der gesamte Systemverbund wortwörtlich stillgelegt werden. Entsprechend sind Maßnahmen bedacht und kontrolliert anzugehen, womit das Element der „Betriebsführung" zum Tragen kommt.

DIE BETRIEBSFÜHRUNG

Während im Betrieb die Administration der Einzelsysteme erfolgt, wird das Gesamtensemble über die Betriebsführung dirigiert. Neben der Leitung des systemübergreifenden Zusammenwirkens werden auf Grundlage der Information Technology Infrastructure Library (ITIL) diverse Prozesse und Arbeitsabläufe definiert, Ressourcen verwaltet und das Gesamtsystem überwacht.

Dabei ist auch hier der hohen Komplexität der Systeme und der Abhängigkeiten untereinander Rechnung zu tragen. Selbst ein einfacher Vorgang wie die



▼ Blick in die Schaltzentrale: in den Serverschränken der Data Center (li) werden später die IT-Systeme eingerüstet. Das Network Operations Center, kurz: NOC, ist das größte Element des ITC. Von hier werden später das Gesamtsystem überwacht und Einzelmaßnahmen gesteuert.
Fotos: Fa. ATOS/Andreas Kaschube (li); Bundeswehr/Reinhard Lang (re)

Erstellung eines neuen Nutzers erfordert die Mitarbeit fast aller Bereiche. Dabei sind nicht nur die betrieblichen Vorgaben umzusetzen, auch die Auflagen der militärischen Sicherheit, der Informationssicherheit und des Datenschutzes sind zu berücksichtigen. Neben der Gesamtleitung sind deswegen auch hier Spezialisierungen erforderlich: jeder Themenkomplex hat seinen eigenen Dirigenten: während der Incident Manager die systemübergreifende Koordination bei Störungen und Ausfällen übernimmt, kümmert sich der Change Manager beispielsweise um jegliche Änderung im System.

Eine zentrale Rolle übernimmt das Network Operations Center (NOC): von hier aus werden die Systeme rund um die Uhr überwacht und Maßnahmen initiiert, denn auch ein kurzer Systemausfall kann erhebliche Konsequenzen nach sich ziehen.

INFORMATIONSSICHERHEIT

Die rasante Entwicklung der Informationstechnik zieht auch immer performantere Systeme und Services nach sich – beispielsweise in der Übertragungstechnik, aber auch in der Datenverarbeitung. Sowohl im privaten, beruflichen als auch militärischen Bereich hat sich die Informationstechnik etabliert und eine immer stärkere, zentrale Position und eine gewisse Omnipräsenz eingenommen – ohne Informationstechnik geht meistens nichts mehr. Das zeigt sich unter anderem in Konzepten wie dem Network Centric Warfare, der Vernetzten Operationsführung sowie anhand der Aufstellung eigener Strukturelemente oder dem Organisationsbereich CIR.

Mit dem Aufstieg der Informationstechnik und ihrer stetig wachsenden Bedeutung steigt nicht nur die Komplexität und Leistungsfähigkeit der Systeme, sondern auch das Risiko. Während einerseits die Bedrohungsvektoren in Anzahl und Umfang wachsen, kann ein ausgefallener IT-Service gleichzeitig erhebliche Konsequenzen nach sich ziehen. Die Dimension „Cyber" etabliert sich zunehmend zu einem Schauplatz für Konflikte aller Art.

Um diesen Risiken zu begegnen, wird auf das Werkzeug der „Informationssicherheit" gesetzt. Dazu werden technische und betriebliche, aber auch umfangreiche organisatorische Maßnahmen etabliert. Neben eigenen Sicherheitskomponenten, Betriebsvorgaben oder Awareness-Veranstaltungen werden dazu auch neue Strukturen geschaffen: innerhalb des Kommandos CIR wurde dazu eigens die Funktion des Chief Information Security Officer der Bundeswehr eingerichtet, der die Gesamtverantwortung für die Informationssicherheit der Bundeswehr innehat.

SCHLUSSWORT

Das Information Technology Center wurde orientiert an der Aufgabe „Bereitstellung von IT-Services" konzipiert und entwickelt. Das Gesamtsystem führt die IT-Systeme in einer geschützten Hülle zusammen. Die Kombination der Elemente Betrieb und Betriebsführung gewährleistet eine professionelle, zielgerichtete und nachhaltige Serviceleistung.

Aufbau und Ausstattung sind an den heutigen Anforderungen ausgerichtet und bieten die erforderliche Grundlage, um die mannigfaltigen, komplexen Aufgaben des Gesamtprozesses zu erfüllen.

Obwohl es sich mit dem ITC um eine „Sofortinitiative im Einsatz" und damit einen Sonderfall im Rüstungsprozess handelt, zeigt es doch deutlich die Richtung für die Weiterentwicklung und die Möglichkeiten der Informationstechnik in der Bundeswehr. Das Information Technology Center ist erst der Anfang einer Geschichte, die mit anderen Projekten weiter erzählt werden wird. Gleichzeitig unterstreicht das ITC die aktuelle Rolle der Informationstechnik in den Streitkräften: nicht mehr im Hintergrund, abseits, sondern mittendrin.

▼ Ansicht des Gesamtkomplexes. Das ITC besteht aus insgesamt 41 Einzelcontainern und beinhaltet die gesamte IT-Infrastruktur zur Anbindung und Versorgung von bis zu 1.000 Nutzern.
Foto: Fa. ATOS/Steffen Liebich

DR. JÖRN BECKER, HEAD OF PUBLIC SECTOR & DEFENCE;
HUBERT GEML, SALES DIRECTOR DEFENCE,
ATOS DEUTSCHLAND

DIGITALE LÖSUNGEN UND SERVICES VON ATOS:

EIN BEITRAG ZUR STEIGERUNG DER EINSATZFÄHIGKEIT DER STREITKRÄFTE IM DIGITALEN ZEITALTER

Die Sicherheitslage hat sich seit Ende Februar 2022 drastisch für unsere Gesellschaft verändert. Die jüngsten Ereignisse im Osten Europas sowie daraus resultierende politische und gesellschaftliche Debatten und Maßnahmen machen deutlich, wie unverzichtbar wehrhafte Streitkräfte zur Abwehr von militärischen Bedrohungen und zur Wahrung geopolitischer Interessen sind. Wahrzunehmen ist, dass mit Eintreten der neuen Situation reflexartig Forderungen nach schnell verfügbaren Produkten, wie Waffen und Fahrzeuge, an die Verteidigungsindustrie artikuliert und zeitgleich einfachere Vergabeverfahren in Aussicht gestellt werden. Im digitalen Zeitalter dürfen jedoch die Aktivitäten im Cyber- und Informationsraum sowie die Einsatzunterstützung durch IT nicht unberücksichtigt bleiben. Wenn auch diese Aktivitäten nicht deutlich sichtbar sind, können sie doch maßgeblich den militärischen Erfolg beeinflussen.

ATOS LÖSUNGSANGEBOT FÜR DIE EINSATZBEREITSCHAFT DER STREITKRÄFTE UND SICHERHEITSBEHÖRDEN

Als ein weltweit führender Anbieter für die digitale Transformation und lokaler Systemintegrator berät Atos Streitkräfte und Sicherheitsbehörden ganzheitlich zur Digitalisierung. Das Engagement von Atos liegt verstärkt auf den Herausforderungen und Lösungsmöglichkeiten im Sinne von militärisch nutzbaren digitalen Plattformen, Infrastrukturen sowie der Integration und Bereitstellung nutzbringender Services. Atos widmet sich u.a. der Problemstellung, wie relevante IT-Services in einem hoch dynamischen Umfeld mit schmalen Bandbreiten über Sicherheits- und Informationsdomänen hinweg ihre Ziele finden und dem Nutzer Mehrwerte liefern. Atos hat sich das Ziel gesetzt die Bundeswehr und ihre Partner bei ihren Digitalisierungsvorhaben bestmöglich zu unterstützen, um Souveränität im digitalen Operations- und Informationsraum zu erreichen und aufrecht zu erhalten. Dazu bietet Atos mit seinen Produkten und qualifizierten Projektteams ein umfassendes Lösungsangebot für militärische Einsätze und deren spezifische Anforderungen.

▶ Dr. Jörn Becker, Head of Public Sector & Defence (l.) und Hubert Geml, Sales Director Defence (r.).
Fotos: Atos

ATOS DIGITAL BATTLESPACE PLATFORM LÖST WESENTLICHE HERAUSFORDERUNGEN ZUR ERZEUGUNG EINES „SHARED SERVICE AND INFORMATION SPACE“

Ein wesentlicher und kritischer Erfolgsfaktor wird die Anbindung der taktischen Ebene in den Systemverbund auf operationeller und strategischer Ebene sein – ein viel diskutierter Punkt der letzten Jahre. Atos bietet dazu eine in Deutschland entwickelte Digital Battlespace Platform an. Diese umfasst u.a. eine einzigartige und dezentralisierte sowie D-LBO-konforme Service Middleware – das Trusted Service Mesh (TSM) zur dynamischen Orchestrierung, Bereitstellung und Vernetzung von Services. Mit der Implementierung eines Trusted Service Mesh werden Anforderungen an eine hohe Mobilität, geringe und sich verändernde Bandbreiten, Domänen abgestufter Sicherheit im gesamten Informationsraum der Streitkräfte am Boden sowie Resilienz in der Luft und auf See erfüllt. Die offene Architektur ermöglicht die unkomplizierte Aufnahme und Einbindung neuer, auch proprietärer Softwarelösungen und damit die Erzeugung neuer Fähigkeiten. Selbst der Einsatz in Verbindung mit gealterten Funkgeräten wurde erfolgreich erprobt. Die Software

ist verfügbar und macht langjährige Entwicklungen obsolet. Neben dem Trusted Service Mesh umfasst die Digital Battlespace Platform die in Deutschland entwickelten Produkte Atos Synergy zur Ermöglichung einer übergreifenden vernetzten Zusammenarbeit (Unified Collaboration und Tactical Teaming) und Atos Swarm Control für die Missionsplanung und Durchführung von z.B. Aufklärungsoperationen durch KI-gestützte unbemannte Plattformen.

STATIONÄRE UND VERLEGEFÄHIGE IT-SYSTEME TRAGEN ZUR VERBESSERUNG DER AUFKLÄRUNGS- UND FÜHRUNGSFÄHIGKEIT BEI

Atos kennt die besonderen Herausforderungen und die realistischen Möglichkeiten der Umsetzung bei mobilen, verlegefähigen und stationären IT-Systemen, u.a. durch unsere Erfahrung als Auftragnehmer in wichtigen Vorhaben der Bundeswehr, wie z.B. der Harmonisierung und Migration der Führungsinformationssysteme (HaFIS), dem German Mission Network (GMN), dem IT-Zentrum für den MINUSMA-Einsatz sowie diverse Fachverfahren und -dienste auf Basis dieser Plattformen. Unter Berücksichtigung von Cloud-Architekturprinzipien hat Atos in den letzten Jahren wesentliche IT-Infrastruktur- und Plattform-Dienste sowohl für den stationären als auch den verlegefähigen Betrieb entwickelt und erfolgreich in die Nutzung gebracht. Funktionale IT-Services der Bundeswehr, NATO und EU wurden bereits integriert und haben sich in der Nutzung bewährt. Die Harmonisierung der Führungsinformationssysteme (HaFIS/GMN) ist auf einem sehr guten Weg und wird von Atos gemeinsam mit Partnern sukzessive durch neue Projekte quantitativ und qualitativ erweitert. Damit kommt es zu einer immer besseren Interoperabilität im Einklang mit den Anforderungen des NATO Federated Mission Networking (FMN). Für die Ausprägung im Bereich von stationären Infrastrukturen bis hin zu Gefechtsständen im Einsatz gibt es bereits praxiserprobte Lösungen in der Nutzung. Diese lassen sich für den speziellen Bedarf auf verschiedenen Führungsebenen wie Division, Brigade oder Bataillon maßgeschneidert anpassen und skalieren.

ATOS LIEFERT KOMPLETTLÖSUNGEN WIE DAS WELTRAUMLAGEZENTRUM

Ein weiteres gutes Beispiel für die Bereitstellung komplexer Lösungen ist das Weltraumlagezentrum zur Verstärkung der Fähigkeiten Deutschlands zum Schutz seiner Infrastruktur in der Domäne Weltraum. Atos, als zuverlässiger Partner der Bundeswehr, wurde mit der Entwicklung und Implementierung des Weltraumlagezentrums beauftragt, um künftig ein umfassendes Weltraumlagebild (Space Situation Awareness) zu erstellen und so die Handlungsfähigkeit sicherzustellen.

ATOS SCHÜTZT DEN CYBER- UND INFORMATIONSRAUM

Um sich gegen Bedrohungen im Cyberraum proaktiv zu schützen, Angriffe zu erkennen und abzuwehren sowie relevante Aktivitäten und Zustände überwachen zu können, vertrauen Organisationen weltweit auf Atos-Lösungen, die in Europa entwickelt und hergestellt werden. Diese umfassen neben Technologiekomponenten für missionskritische Systeme auch Lösungen zur Erhöhung der Resilienz, Ermöglichung der Bedrohungserkennung und -abwehr. Die Hochleistungsrechner (High Performance Computer) von Atos liefern echtzeitnahe Analysen und Auswertungen großer und komplexer Datenmengen zur Entscheidungsunterstützung. Atos ist durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifizierter IT-Sicherheitsdienstleister für die Bereiche Informationssicherheitsberatung, Informationssicherheitsrevision, Penetrationstests sowie Trustcenter. Damit ist Atos in der Lage, seine Kunden durch Risikoanalysen, Informationssicherheitskonzepte, Audits und Revisionen und Trustcenter-Services auf Basis anerkannter Standards und hoher Güte zu unterstützen. Ferner unterstützt Atos Kunden hinsichtlich der Etablierung, Aufrechterhaltung und Wirksamkeitsprüfung von Informationssicherheitsmaßnahmen mithilfe maßgeschneiderter Lösungen, übergreifender und spezifischer Penetrationstests sowie der Realisierung von Managementsystemen. Atos ist Partner der Allianz für Cyber-Sicherheit. Die Atos-Experten verfügen über eine Vielzahl national und international anerkannter Zertifizierungen.

ATOS TREIBT INNOVATIONEN FÜR DAS DIGITALE ZEITALTER VORAN

Atos ist einer der weltweit führenden Digitalisierungsdienstleister mit starker Ausprägung in Deutschland und Europa. Erfahrene Experten mit tiefem Know-how und langjähriger Erfahrung in Defence, Intelligence, Cybersecurity und IT bilden eines der leistungsfähigsten Teams zur Lösungsbereitstellung im Bereich „Verteidigung" in Deutschland. Atos wächst kontinuierlich und sucht bundesweit hochmotivierte Talente zur Verstärkung der Teams, die Interesse haben, innovative und anspruchsvolle Projekte weiter voranzutreiben. Sehr gerne stellt Atos ehemalige Soldatinnen und Soldaten bzw. Mitarbeiterinnen und Mitarbeiter der Bundeswehr in vielfältigen Funktionen ein.

MAJOR HEIKO ZOPPKE, ABTEILUNG OPERATION, KOMMANDO CIR,
SEIT 20.08.2021 VERBINDUNGSPERSON DES KOMMANDOS CIR IM NATIONALEN CYBER-ABWEHRZENTRUM

RESSORTÜBERGREIFENDE ZUSAMMENARBEIT FÜR DIE CYBERSICHERHEIT DEUTSCHLANDS

Das Kommando CIR im Nationalen Cyber-Abwehrzentrum

Das Nationale Cyber-Abwehrzentrum (Cyber-AZ) leistet seit über zehn Jahren einen Beitrag zur gesamtstaatlichen Cybersicherheit Deutschlands. Durch den im Cyber-AZ stattfindenden, unmittelbaren Informationsaustausch deutscher Behörden und dem daraus resultierenden gemeinsamen Cyber-Sicherheitslagebild wird die Handlungsfähigkeit der Bundesregierung entscheidend unterstützt. Auch das Kommando Cyber- und Informationsraum (CIR) beteiligt sich mit Personal und im Rahmen des stetigen Informationsaustauschs aktiv am Cyber-AZ.

Cyberangriffe wurden schon vor Jahren durch die Bundesregierung als große Gefahr eingestuft. Die stetig steigende Anzahl von vielfältigsten kriminellen Vorfällen im Cyberraum und die damit verbundene wachsende Betroffenheit von Personen und Institutionen sowie die zunehmenden Schäden bestätigen diese Einschätzung. Eine der derzeit akutesten Gefahren geht in diesem Zusammenhang von Ransomware-Angriffen krimineller Gruppierungen aus.

Als Reaktion beschloss die Bundesregierung bereits im Jahr 2011 die Einrichtung einer Kooperations-, Kommunikations- und Koordinationsplattform der relevanten (Sicherheits-)Behörden. Der damalige Bundesinnenminister Dr. Hans-Peter Friedrich eröffnete im Juni 2011 das Cyber-AZ mit den Zielen, den Informationsaustausch zu beschleunigen und die Koordinierung bei der Abwehr von Cyberangriffen zu stärken. Weiterhin war es Absicht, durch ein gemeinsames, aktuelles und umfassendes Cyber-Sicherheitslagebild einen unverzichtbaren Beitrag zur Handlungsfähigkeit der Bundesregierung zu leisten. Das Cyber-AZ soll jedoch nicht in bestehende Zuständigkeiten eingreifen. Maßnahmen werden nach wie vor durch diejenigen Behörden durchgeführt, in deren Zuständigkeitsbereich diese fallen.

Die Abläufe innerhalb des Cyber-AZ werden von einem dreiköpfigen Koordinatorenteam gesteuert. Die Positionen des Koordinators und seiner zwei Stellvertreter sind durch Personal von unterschiedlichen Kernbehörden besetzt. Eine Rotation unter den Behörden erfolgt in der Regel alle zwei Jahre. Derzeit wird die Funktion eines der beiden stellvertretenden Koordinatoren durch einen Angehörigen des Kommandos CIR wahrgenommen. Alle am Cyber-AZ beteiligten Behörden stellen mindestens eine Verbindungsperson ab, die ihre jeweilige Behörde vertritt und als Schnittstelle zu dieser fungiert. Vervollständigt wird das Cyber-AZ durch eine Geschäftsstelle, deren Personal die Abwicklung des administrativen Geschäftsbetriebs des Cyber-AZ sicherstellt.

Als **Ransomware** werden Schadprogramme bezeichnet, die den Zugriff auf Dateien und Systeme einschränken oder verhindern und diese Ressourcen nur gegen Zahlung eines Lösegeldes (engl. ransom) wieder freigeben. Es handelt sich dabei um einen Angriff auf das Sicherheitsziel der Verfügbarkeit und einer Form digitaler Erpressung.

◀ Verbindungsperson Major Zoppke (re) im Gespräch mit einem Mitarbeiter der Geschäftsstelle.
Foto: Bundeswehr/Stefan Uj

NATIONALES CYBER-ABWEHRZENTRUM

Neu aufgestellt wurde in diesem Jahr das Lageteam des Cyber-AZ, das maßgeblich den Prozess der täglichen Lagebearbeitung und Berichterstattung übernommen hat. Hierzu gehören unter anderem die Sichtung und Auswertung aller eingehenden Lageprodukte (Berichte, Zusammenfassungen, Bewertungen etc.) der Behörden. Auch in diesen beiden Teilbereichen ist – beziehungsweise wird zukünftig – Personal aus dem Kommando CIR eingesetzt.

VIELE BEHÖRDEN – EIN ZIEL

Das Cyber-AZ ist keine eigenständige Behörde. Es ist vielmehr eine Plattform, an der sich Behörden aus verschiedenen Ministerien beteiligen. Derzeit sind folgende Kernbehörden im Cyber-AZ vertreten:

- Bundesamt für den Militärischen Abschirmdienst (BAMAD)
- Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK)
- Bundesamt für Verfassungsschutz (BfV)
- Bundeskriminalamt (BKA)
- Bundesnachrichtendienst (BND)
- Bundespolizei (BPOL)
- Bundesamt für Sicherheit in der Informationstechnik (BSI)
- Kommando Cyber- und Informationsraum (KdoCIR)

Zudem gibt es weitere Einrichtungen, die sich an der Kooperationsplattform beteiligen:

- Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)
- Zollkriminalamt (ZKA)
- Cyberabwehr Bayern (CAB)
- Hessen CyberCompetenceCenter (H3C)
- Justiz (Generalstaatsanwaltschaft Bamberg, Staatsanwaltschaft Köln)

VERBINDUNGSPERSON IM CYBER-AZ – EIN ERFAHRUNGSBERICHT

„Verbindungsperson im Nationalen Cyber-Abwehrzentrum" – Unter diesem Dienstposten konnte ich mir recht wenig vorstellen, als mir mein zuständiger Personalführer mitteilte, dass ich nach 24 Jahren in der Luftwaffe auf genau diesen Dienstposten im Organisationsbereich CIR versetzt werden sollte. Mir war durchaus bewusst, dass es ein Nationales Cyber-Abwehrzentrum gibt, aber wie dieses strukturiert ist, welche Behörden sich daran beteiligen und wie meine zukünftige Rolle dort konkret aussehen sollte, war mir im Vorfeld jedoch nicht klar.

Als Verbindungsperson vertrete ich meine Dienststelle im Cyber-AZ und trage dazu bei, dass das Kommando CIR seinen Teil zur gesamtstaatlichen Cybersicherheit leistet. Ich tausche mich regelmäßig mit den zuständigen Bereichen im Kommando aus und bringe aktuelle Sachverhalte und Erkenntnisse mit Bezug zum Cyberraum in das Cyber-AZ ein. Andersherum werden natürlich auch neueste Informationen der Behörden des Cyber-AZ an das Kommando CIR übermittelt. Eine Aufgabe, die Kommunikationsfähigkeit, Kompromissbereitschaft und Fingerspitzengefühl, besonders im Umgang mit den Besonderheiten der jeweiligen Behörden, erfordert. Da das Cyber-AZ keine eigene Behörde ist, sondern als Plattform agiert, gibt es keine Weisungsbefugnis für die Koordinatoren. Doch aufgrund der großen Professionalität der teilnehmenden Behörden ist dies nicht zwingend notwendig. Natürlich gibt es hin und wieder Diskussionsbedarf und unterschiedliche Meinungen über das weitere Vorgehen in einem Sachverhalt. Doch grundsätzlich ziehen alle Behörden an einem Strang und haben das gleiche Ziel vor Augen.

DER ALLTAG IM CYBER-AZ

Mein Arbeitsalltag als Verbindungsperson des Kommandos CIR ist zum einen geprägt von regelmäßigen Besprechungen. Zum anderen verlangen aktuelle und akute Sachverhalte mit Bezug zum Cyberraum auch Flexibilität im Arbeitsablauf.

◀ Informationsaustausch auf dem Weg zur täglichen Lagebesprechung.

▶ Die Bundespolizei – Eine der acht Kernbehörden des Cyber-AZ.
Fotos: Bundeswehr/Stefan Uj

Der tägliche Austausch mit den Vertretern der weiteren Behörden des Cyber-AZ erfordert die Auswertung von aktuellen Informationen zu Sachverhalten mit Bezug zum Cyberraum; doch im Gegensatz zu meinen vorherigen Verwendungen in der Luftwaffe sind es hier nicht überwiegend E-Mails, die gelesen und ausgewertet werden müssen, sondern Berichte oder Artikel, die mich über unterschiedlichste Quellen erreichen. Liegt bei dem Sachverhalt ein gesamtstaatliches Interesse vor? Gibt es Sachverhalte, die gegebenenfalls Relevanz für die Bundeswehr haben oder umgekehrt Informationen aus der Bundeswehr, die hilfreich für Behörden des Cyber-AZ sein können? Werden hier neue Vorgehensweisen von Kriminellen im Cyberraum beschrieben? Sollte etwas davon zutreffen, wird diese Thematik in die tägliche Lagebesprechung eingebracht. Visualisiert in einem gemeinsamen IT-System wird die Sachlage allen Angehörigen des Cyber-AZ vorgestellt. In diesem Rahmen entscheiden wir gemeinsam über die weitere Vorgehensweise. Können die Behörden den Sachverhalt mit zusätzlichen Informationen anreichern? Müssen Behörden außerhalb des Cyber-AZ über den Vorgang informiert werden? Oder ist der Vorgang so brisant, dass unmittelbar die zuständigen Ministerien informiert werden müssen?

Neben der täglichen Lagebesprechung findet auch eine wöchentliche Besprechung des Cyber-AZ statt. In der Plenumssitzung „Operative Fallbearbeitung" findet ein Austausch über Sachstände zu konkreten Fällen statt, mit denen sich das Cyber-AZ in Form von Unterarbeitsgruppen aktuell beschäftigt.

Weiterhin führen die Vertreter der Behörden regelmäßige Besprechungen durch, in denen die Erstellung der „Cyber-Sicherheitslage Deutschland" (CSLD) abgestimmt wird. Die CSLD ist ein wöchentliches Lageprodukt, mit dem das Cyber-AZ die verantwortlichen Ministerien zum Beispiel über aktuelle Vorkommnisse, potentielle Gefahren und Aktivitäten von Kriminellen im Cyberraum informiert. Neben dem regelmäßigen Lageprodukt kommt es auch immer wieder vor, dass akute Begebenheiten eine sofortige Einschätzung des Cyber-AZ erfordern. Hierzu wird dann eine „Anlassbezogene CSLD" herausgegeben. Dies setzt natürlich die Teilnahme an spontanen Besprechungen und Abstimmungen voraus. Mit Beginn des Angriffskrieges Russlands auf die Ukraine erstellte das Cyber-AZ zudem eine tägliche Sonderberichterstattung über aktuelle Sachverhalte, Vorkommnisse und Entwicklung im Cyberraum mit Bezug zu dem Krieg.

Da ich als Verbindungsperson aus dem Kommando CIR vor Ort in der Liegenschaft des BSI in Bonn eingesetzt bin, nimmt der regelmäßige Austausch mit der „militärischen Heimat" eine wichtige Rolle ein. Neben den Besprechungen innerhalb des Cyber-AZ tausche ich mich auch täglich mit meinem „Mutterhaus" aus. Dazu führt die Unterabteilung J3 des Kommandos CIR einen standardisierten Informationsaustausch der relevanten Fachbereiche durch. Neben der Verbindungsperson und weiteren Analysten nehmen hier auch Vertreter des Chief Information Security Officer der Bundeswehr (CISOBw) und der Unterabteilung J2, die für das Militärische Nachrichtenwesen in der Dimension CIR zuständig ist, teil. Die Verbindung zwischen Cyber-AZ und Fachleuten des Kommandos CIR ist somit durchgehend gewährleistet. Sie führen die Gefährdungs- beziehungsweise Betroffenheitsbewertung für den Geschäftsbereich des Bundesministeriums der Verteidigung durch. Weiterhin leisten die Expertinnen und Experten des Kommandos durch das Einbringen ihrer eigenen Fachkenntnis und durch gesonderte Bewertungen einen ganz wesentlichen Beitrag zur gesamtstaatlichen Cyber-Sicherheit.

Eine weitere Aufgabe des „Verbinders" aus dem Kommando CIR ist die Leitung der „Arbeitsgruppe (AG) Übungen". Diese AG soll das Cyber-AZ auf mögliche Krisen optimal vorbereiten. Besonders herausfordernd ist dabei das mit allen Behörden abgestimmte, regelmäßige Einüben von Prozessen im Cyber-AZ. Die Vor- und Nachbereitung nimmt dafür den Großteil der Tätigkeiten innerhalb der „AG Übungen" ein. Neben internen Alarmierungs- oder Planübungen beabsichtigt das Cyber-AZ, zukünftig auch verstärkt an externen Übungen teilzunehmen. Die Teilnahme an der nächsten „Länder- und Ressortübergreifenden Krisenmanagementübung" (LÜKEX) ist fest eingeplant. Das Cyber-AZ beteiligt sich bereits an den vorbereitenden Maßnahmen zur Teilnahme an der Übung.

DIENSTSTELLEN-PROFIL

INFORMATIONSTECHNIK-BATAILLON 381

Das Informationstechnikbataillon 381 stellt mit modernen IT-Systemen die nationale und internationale Führungsfähigkeit der Bundeswehr im Einsatz sicher.

AUFGABEN

- Beitrag zur Sicherstellung der Führungsfähigkeit der Streitkräfte durch fachliche Ausbildung und Inübunghaltung an den bereitzustellenden IT-Systemen.
- Bietet mit dem Betrieb der Ausbildungsanlagen für Satellitenkommunikation Ausbildungsmöglichkeiten für alle Organisationsbereiche in der Bundeswehr.
- Bildet nach neuer Ausbildungssystematik Offiziersanwärterinnen und -anwärter des Organisationsbereichs CIR und des Heeres aus.
- Lehrgangsgebundene Ausbildung von angehendem Nachwuchs der Unteroffiziere (mit Portepee) zur Befähigung in der Führung ihrer IT-technischen Teileinheit für den Kommandobereich.

AUFTRAG

Das Informationstechnikbataillon 381 (ITBtl 381) stellt IT-Services zur Verarbeitung und Übertragung von Informationen in und für die Einsätze der Bundeswehr bereit und managt deren Bereitstellung orientiert an internationalen Standards. Hierzu werden unter anderem Satellitenkommunikation, Netzwerktechnik, Servertechnik, verschlüsselte mobile Kommunikationsmittel oder digitaler Richtfunk eingesetzt.

Darüber hinaus leistet der Verband mit seinen IT-Services unverzichtbare Beiträge zu Übungsvorhaben der Streitkräfte. Hier unterstützt er mit leistungsfähigen IT-Systemen, betrieben durch hochspezialisierte Soldatinnen und Soldaten bei Bedarf auf Anforderung.

Die dabei gewonnenen Erkenntnisse werden zur kontinuierlichen Verbesserung und Weiterbildung des Personals und Materials genutzt. Dazu teilt das ITBtl 381 das erworbene Know-how mit anderen interessierten Verbänden, sodass dieses in die Weiterentwicklung der IT-Kräfte CIR einfließen kann.

Die Angehörigen des Bataillons sind als militärische IT-Kräfte auch für die Wahrnehmung von allgemein-militärischen Aufgaben und Tätigkeiten befähigt. Dies wird durch entsprechende Ausbildungen und Übungen ständig sichergestellt. So werden im Rahmen der sogenannten „Einsatzlandunspezifischen Ausbildung" (ELUSA) die Soldatinnen und Soldaten auf mögliche Einsätze vorbereitet. Zu den militärischen Grundfertigkeiten gehören z.B. Maßnahmen zur Eigensicherung, das Führen des Feuerkampfes sowie die Erstversorgung von Verwundeten.

ANSCHRIFT
Kurmark-Kaserne,
Beeskower Chaussee 15A,
15859 Storkow (Mark)

DIENSTSTELLENLEITUNG
Oberstleutnant Marc Tachlinski

STAMMPERSONAL
~700

AUFSTELLUNG
01.07.2006

GENERALMAJOR DR. MICHAEL HEINZ FÄRBER,
ABTEILUNGSLEITER PLANUNG CIR UND DIGITALISIERUNG BUNDESWEHR, KOMMANDO CIR
UND SEIT APRIL 2021 ZUNÄCHST AUF ZWEI JAHRE GEWÄHLTER VORSITZENDER
DES LENKUNGSAUSSCHUSSES IM PESCO-PROJEKT CIDCC

OBERSTLEUTNANT I.G. CHRISTOF OPOLONY,
PROJEKTKOORDINATOR DES PESCO-PROJEKTES CIDCC,
ABTEILUNG PLANUNG CIR UND DIGITALISIERUNG BUNDESWEHR, KOMMANDO CIR

MULTINATIONALES PESCO-PROJEKT DER EUROPÄISCHEN UNION

CIDCC: EIN BEITRAG ZUR PLANUNGS- UND FÜHRUNGSFÄHIGKEIT FÜR ZUKÜNFTIGE CIR-OPERATIONEN DER EU

Gemeinsam mit Frankreich, den Niederlanden und Ungarn wird derzeit das „Cyber and Information Domain Coordination Centre" (CIDCC) für die Europäische Union im Bereich der militärischen Missions- und Operationsführung entwickelt und aufgebaut. Deutschland brachte diese Idee Ende 2019 in die entsprechenden EU-Gremien ein und hat die Leitung des Projektes übernommen. Mit der Ausarbeitung, der Planung und ersten Umsetzung ist das Kommando Cyber- und Informationsraum (CIR) beauftragt. Eine der vorrangigen Aufgaben des CIDCC wird der Abgleich von Lagebildern aus dem Cyber- und Informationsraum für Missionen und Operationen der EU sein.

▲ Der multinationale Ansatz eines CIDCC wird derzeit im Organisationsbereich CIR verantwortet und vorbereitet.
Foto: Bundeswehr/Martina Pump

Im Jahr 2017 stellte die EU einen militärischen Planungs- und Durchführungsstab „Military Planning and Conduct Capability" (MPCC) innerhalb des seit 2001 existierenden Militärstabs in Brüssel auf. Er gewährleistet erstmalig in der EU eine stehende Führungsstruktur auf militärstrategischer Ebene außerhalb der Einsatzgebiete. Dieser Stab ist für die operative Planung und Durchführung militärischer Missionen verantwortlich, ohne dass ihm zunächst Exekutivbefugnisse übertragen wurden. Die Aufsicht über die Arbeit des MPCC hat weiterhin das Politische und Sicherheitspolitische Komitee (PSK), das für die Gemeinsame Außen- und Sicherheitspolitik der EU (GASP) und die Gemeinsame Sicherheits- und Verteidigungspolitik (GSVP) zuständig ist. Im November 2018 wurden dem MPCC ergänzend Exekutivbefugnisse übertragen, welche die Planung und Durchführung von militärischen Operationen in der Größenordnung einer EU-Battlegroup umfassen.

DER DEUTSCHE VORSCHLAG FÜR EIN CIDCC

Anknüpfend an diese Fähigkeit schlug Deutschland bereits 2019 mit Blick auf die EU-Ratspräsidentschaft im Jahr 2020 vor, ein CIDCC als gemeinsames europäisches Projekt zu etablieren und perspektivisch für das MPCC bereitzustellen. In der Folge wurde der Vorschlag, dies im Rahmen von Permanent Structured Cooperation (PESCO) zu realisieren, von der EU angenommen. Die gegenwärtigen Mitglieder der hierzu eingerichteten Koordinierungsstelle sind Deutschland, Frankreich, die Niederlande und Ungarn, die an der Erstbefähigung des CIDCC durch das PESCO-Projekt mitwirken.

Im September 2021 verabschiedete der EU-Militärausschuss die „EU Military Vision and Strategy on Cyberspace as a Domain of Operations", in der folgerichtig die Einrichtung eines „standing and centralized EU military cyber coordination element" gefordert wird.

Dieser multinationale Ansatz eines CIDCC wird derzeit im Organisationsbereich Cyber- und Informationsraum (CIR) verantwortet und vorbereitet. Das Projektbüro des CIDCC ist im Kommando CIR in Bonn angesiedelt. Gegenwärtig erhält das deutsche Projektbüro anteilig Unterstützung durch einen französischen und einen niederländischen Verbindungsoffizier sowie einen ungarischen Projektpartner. Mittelfristig soll das CIDCC, nach dem Ende der Aufstellungsphase, als ständige multinationale Fähigkeit dem MPCC zur Verfügung stehen. Bis dahin sind noch verschiedene Herausforderungen zu bewältigen, die insbesondere im Bereich ganzheitlicher Analysefähigkeiten und den unterstützenden IT-Lösungen liegen.

HYBRIDE BEDROHUNGEN AUS UND IM CYBER- UND INFORMATIONSRAUM ERKENNEN

Die Europäische Union tritt als internationaler Akteur auf und nimmt mit ihren Mitgliedsstaaten die Verantwortung im Bereich der GSVP wahr. In diesem Bereich kann die EU mit zivilen, polizeilichen und militärischen Instrumenten verschiedene Aufgaben in den Segmenten Krisenprävention, Krisenmanagement und Krisennachsorge übernehmen. 2003 startete die EU ihre erste militärische Mission in Mazedonien. Zu Beginn des Jahres 2022 waren sieben militärische Missionen und Operationen und elf zivile Missionen der EU aktiv. Zu den in Deutschland bekanntesten militärischen Missionen zählt die EU Training Mission in Mali (EUTM Mali).

In den unterschiedlichen Missions- und Operationsgebieten der EU nimmt der Cyber- und Informationsraum eine immer größer werdende Rolle für die beteiligten militärischen Kräfte ein. Zusätzlich müssen in diesem Raum gegnerische Akteure, die mit geringen Ressourcen zum Beispiel eine gezielte Streuung von Propaganda und Desinformation gegen eine EU-Mission, Aktionen im elektromagnetischen Spektrum oder Cyberattacken gegen Kommunikationsnetzwerke der EU-Einheiten durchführen, rasch erkannt und abgewehrt werden.

ZUKÜNFTIGE AUFGABEN DES CIDCC

Das Tätigkeitsspektrum des CIDCC soll zunächst die Analyse von CIR-typischen Lageinformationen bei EU-Missionen und -Operationen sowie deren Bewertung umfassen. Eine zentrale Aufgabe wird hierbei die Zusammenführung und Fusionierung von Daten und Information aus dem Cyber- und Informationsraum sein. Eine besondere Herausforderung des multinationalen Ansatzes ist es, dass die beitragenden Nationen sowohl hinsichtlich bestehender Strukturen, als auch verfügbarer Quellen und Sensoren sehr unterschiedlich aufgestellt sind. Vor diesem Hintergrund werden in Bezug auf die verwendeten Analyseprozesse, die etablierten IT-Lösungen wie auch bei den Elementen für ein Lagebild sowohl heterogene als auch komplementäre Beiträge der Nationen erwartet. Durch die hier notwendige Harmonisierung wird auch ein Rückfluss in die nationalen Fähigkeiten erwartet.

PESCO

Im Dezember 2017 starteten 25 Mitgliedsstaaten der EU eine „Ständige Strukturierte Zusammenarbeit" im Bereich der Sicherheits- und Verteidigungspolitik, besser bekannt unter der englischen Abkürzung „PESCO" (Permanent Structured Cooperation). Die Gründung der PESCO gilt als Meilenstein in der Entwicklung der GSVP und der Zusammenarbeit verschiedener Mitgliedsstaaten der EU im Verteidigungsbereich. Die beteiligten Länder können dort in gemeinsame Projekte investieren oder ihre operative Einsatzbereitschaft verbessern.

Mit Stand Februar 2022 existieren 60 verschiedene PESCO-Projekte. Weiterführende Informationen zu PESCO finden Sie u.a. bei der Europäischen Verteidigungsagentur.

Die Analyseergebnisse sollen kontinuierlich in den militärischen Planungs- und Führungsprozess von EU-Operationen und -Missionen eingebracht werden. Neben anderen sicherheitsrelevanten und insbesondere militärischen Nutzerkreisen im Rahmen der GSVP werden Verteidigungspolitiker innerhalb der EU und auch die EU-Kommission von dieser Arbeit des CIDCC profitieren. Um eine konkrete Projektarbeit mit den militärischen EU-Partnern aufnehmen beziehungsweise weiterführen zu können, beabsichtigt das CIDCC daher den Sitz seines Projektbüros im Jahr 2023 von Bonn nach Brüssel zu verlegen.

LANGFRISTIGES ZIEL: RESILIENZ IM CYBER- UND INFORMATIONSRAUM FÜR DIE GANZE EU

Die Zusammenarbeit des CIDCC mit den EU-Partnern soll sich langfristig nicht auf Analysen und Lagebeiträge beschränken, sondern helfen, eine auch im zivilen Bereich der EU bestehende Fähigkeitslücke im Cyber- und Informationsraum zu schließen. Auf diese Weise können übergreifende, multinational wirksame Effekte erzielt werden, die vor allem eine verbesserte Resilienz der EU in dieser fünften Dimension erzeugen. So werden zum einen vorhandene militärische Kommunikationsstrukturen zwischen den verschiedenen EU-Partnern bei den jeweiligen Missionen und Operationen gestärkt, und zum anderen die strategische Autonomie der EU im Cyber- und Informationsraum nachhaltig ausgebaut. Das CIDCC soll mit seiner Arbeit die EU langfristig unterstützen und so zum Anspruch der EU als Bereitsteller von Sicherheit kontinuierlich beitragen.

◄ Das Tätigkeitsspektrum des CIDCC soll zunächst die Analyse von CIR-typischen Lageinformationen bei EU-Missionen und -Operationen sowie deren Bewertung umfassen.
Foto: Bundeswehr/Andrea Bienert

DIENSTSTELLEN-PROFIL

INFORMATIONSTECHNIK-BATAILLON 383

Informationen effektiv verarbeiten, übertragen und managen.

AUFGABEN

- IT-Anbindung für Auslandseinsätze.
- Vorbereitende und weiterführende Qualifizierung von IT-Administratoren im Erfurt Education Training Center for IT.
- Fernmeldezug für militärische Evakuierungsoperationen in Wesel.

AUFTRAG

Das Informationstechnikbataillon 383 (ITBtl 383) stellt mit mobiler Digitaltechnik, vielfältigen Kommunikationsmitteln und hoch qualifiziertem Personal die IT-Anbindung für die Auslandseinsätze der Bundeswehr bereit. Darüber hinaus leistet das Bataillon einen unverzichtbaren Beitrag zu Übungsvorhaben der Streitkräfte. Die Soldatinnen und Soldaten des Verbandes verarbeiten, übertragen und managen mit leistungsfähigen Systemen Informationen. Dazu verwenden sie zum Beispiel Satellitenkommunikation, Netzwerktechnik, Servertechnik, verschlüsselte mobile Kommunikationsmittel oder digitalen Richtfunk.

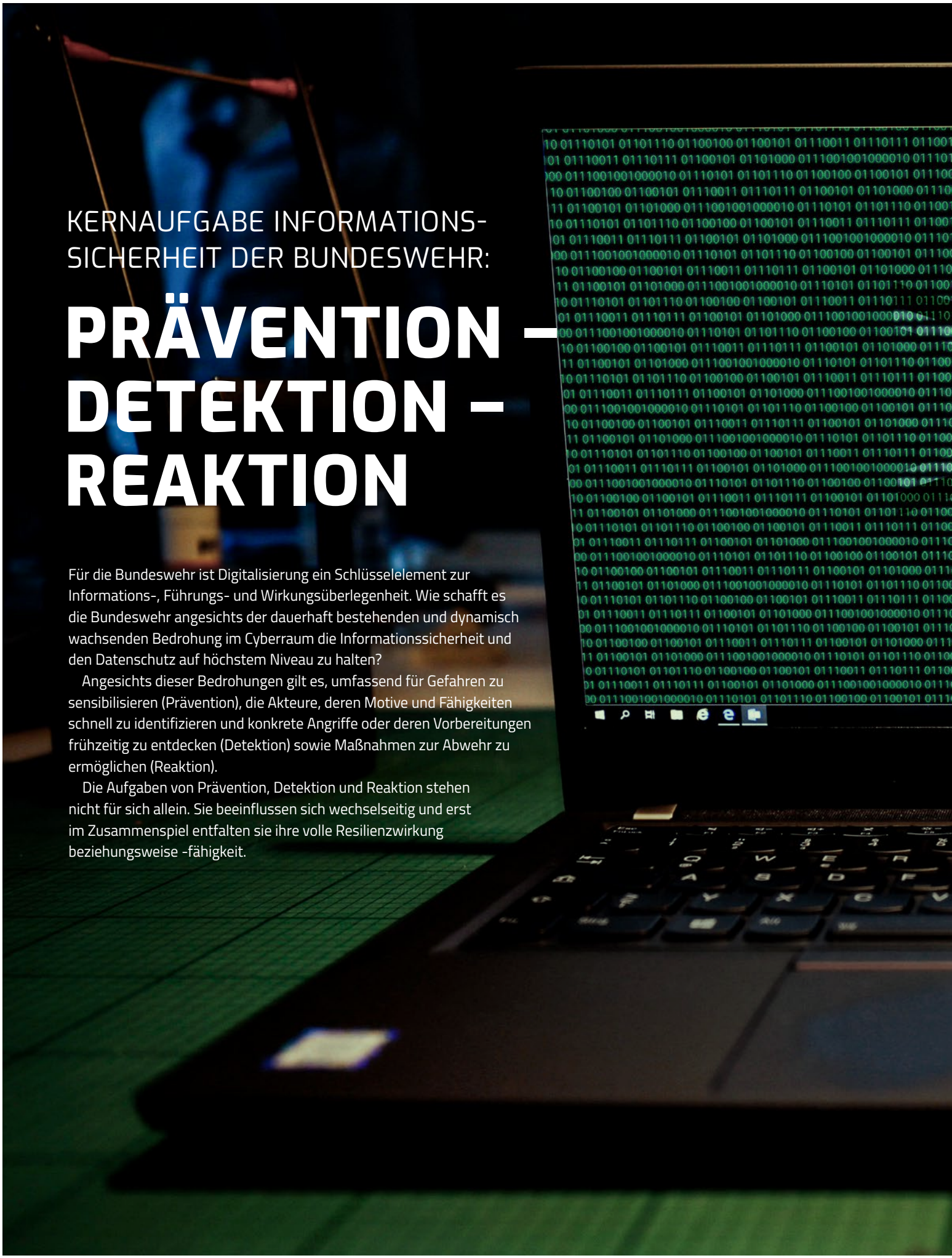
Des Weiteren ist das ITBtl 383 mit dem Fernmeldezug für militärische Evakuierungsoperationen in Wesel mit in die nationale Krisenvorsorge eingebunden. Zum Schutz deutscher Staatsangehöriger werden hier dauerhaft weltweit einsatzbereite IT-Spezialistinnen und -Spezialisten bereitgehalten, um im Notfall schnell regieren zu können.

ANSCHRIFT
Henne-Kaserne,
Nissaer Weg 10,
99099 Erfurt

DIENSTSTELLENLEITUNG
Oberstleutnant Thomas Czada

STAMMPERSONAL
~750

AUFSTELLUNG
01.04.2004



KERNAUFGABE INFORMATIONS-SICHERHEIT DER BUNDESWEHR:

PRÄVENTION – DETEKTION – REAKTION

Für die Bundeswehr ist Digitalisierung ein Schlüsselelement zur Informations-, Führungs- und Wirkungsüberlegenheit. Wie schafft es die Bundeswehr angesichts der dauerhaft bestehenden und dynamisch wachsenden Bedrohung im Cyberraum die Informationssicherheit und den Datenschutz auf höchstem Niveau zu halten?

Angesichts dieser Bedrohungen gilt es, umfassend für Gefahren zu sensibilisieren (Prävention), die Akteure, deren Motive und Fähigkeiten schnell zu identifizieren und konkrete Angriffe oder deren Vorbereitungen frühzeitig zu entdecken (Detektion) sowie Maßnahmen zur Abwehr zu ermöglichen (Reaktion).

Die Aufgaben von Prävention, Detektion und Reaktion stehen nicht für sich allein. Sie beeinflussen sich wechselseitig und erst im Zusammenspiel entfalten sie ihre volle Resilienzwirkung beziehungsweise -fähigkeit.

GENERALMAJOR JÜRGEN SETZER,
STELLVERTRETER INSPEKTEUR CIR UND CHIEF INFORMATION SECURITY OFFICER
DER BUNDESWEHR (CISOBW)

24/7 UNTER FEUER

In heutigen Konfliktszenarien setzen Angreifer auf eine Kombination aus klassischen Militäreinsätzen, Propaganda in den Medien und sozialen Netzwerken sowie direkte Computerangriffe. Das Vorgehen von scheinbar unsichtbaren Gegnern in „hybrider Kriegsführung" ist allgegenwärtig. Wie antwortet die Bundeswehr erfolgreich und resilient auf Cyberangriffe?

Eine intakte Führungsfähigkeit ist von zentraler Bedeutung für eine verteidigungsfähige Bundeswehr. Die Informationssicherheit ist daher heute eine der wesentlichen Voraussetzungen für die Einsatzbereitschaft und den Einsatz. Ohne die gesicherte Verfügbarkeit, die Integrität und die Vertraulichkeit von Daten können wir heute unseren Auftrag weder im Grundbetrieb noch im Einsatz erfüllen. Deshalb kommt dem Schutz unserer Informationen bei deren Bearbeitung, Übertragung und Speicherung eine entscheidende Bedeutung zu.

DER KAMPF GEGEN (STAATLICHE) HACKER UND KRIMINELLE IM CYBERRAUM

Am Freitag, den 13. Februar 2009, traf ein Computerwurm auch mehrere hundert Rechner der Bundeswehr und legte wichtige Kommunikationsmittel lahm. Die Angreifer sind bis heute nicht bekannt. Seitdem haben Akteurinnen und Akteure im Cyberraum weiter aufgerüstet. Angriffe aus dem Ausland mit Erpresserschadsoftware, sogenannter Ransomware, auf Unternehmen, Krankenhäuser und staatliche Einrichtungen in Deutschland haben bereits 2021 ein bedrohliches Ausmaß angenommen.

2022 steigerte sich diese Bedrohung aus dem Cyberraum auf ein noch nicht gekanntes Potential sowohl gegen Wirtschaft, staatliche Einrichtungen und kritische Infrastrukturen in Deutschland. Immer wieder wird versucht, zum Beispiel durch „Distributed Denial of Services" (DDoS)-Angriffe, die Verfügbarkeit von Informations- und Kommunikationsplattformen zu stören. Zumeist ist nicht eindeutig zu erkennen, wer die Angreifenden sind. Wird zum Beispiel eine IP-Adresse aus einem bestimmten Adressraum eines Landes genutzt, bedeutet dies noch nicht, dass der Angriff diesem Land oder einer bestimmten Personengruppe zugeschrieben werden kann.

ANGREIFER BLEIBEN MEIST IM VERBORGENEN – DIE SCHWIERIGKEIT EINER ATTRIBUTION

Bereits mit niedrigschwelligen Cyberangriffen können Gegnerinnen und Gegner unerkannt spürbare Wirkung erzielen. Bei sogenannten DDoS-Angriffen nutzen Angreifende angemietete Botnetze, meist aus dem Darknet, deren Geräte weltweit verteilt sind. Wenn es kein „Bekennerschreiben" im Netz gibt, ist eine Zuordnung zu einem bestimmten Angreifer kaum möglich.

Ein Botnet ist ein Netzwerk infizierter Computer, das aus der Ferne gesteuert und dazu verwendet werden kann, Spam zu senden, Malware zu verbreiten oder DDoS-Angriffe durchzuführen – alles ohne die Zustimmung der Gerätebesitzer.

Das statistische Nachhalten erkannter Pings, Port-Scans oder einzelner E-Mails, beispielsweise einer Schadsoftwarewelle, liefert zwar sehr große Informationsmengen, die statistische Aussagen zulassen, jedoch keine Bewertung hinsichtlich konkreter Gefährdungen oder Angreifer. Von hoher Relevanz sind dagegen potenziell schädliche Ereignisse innerhalb der Netze der Bundeswehr, also auf Servern und am Arbeitsplatz-PC erkannte Schadsoftware oder schadhafte Ereignisse, die durch die kaskadierten Schutzmaßnahmen nicht erkannt wurden. Hier kann man durch weitergehende Analysen gegebenenfalls die Techniken, Taktiken und Prozeduren (TTP) mit denen von bekannten Mustern vergleichen und so auf bestimmte Angreiferinnen und Angreifer schließen.

Unabhängig davon, ob es sich um Ereignisse an den Firewalls, auf den Arbeitsplatzrechnern oder im Netzwerk handelt: ob und wie einzelne Ereignisse zu „einem" Angriff zusammengehören, lässt sich überhaupt nur in wenigen Ausnahmefällen bei konkretem Verdacht mit sehr hohem Aufwand, etwa durch IT-forensische Untersuchungen, feststellen. Die Zuordnung und eine konkrete Attribution jedes Einzelfalles ist also schlichtweg nicht möglich und letztlich zum Festlegen geeigneter Schutzmaßnahmen für unsere Systeme grundsätzlich auch nicht relevant. Große Phishingangriffe können zum Beispiel sehr gut durch technische Anpassung geblockt werden. Spear-Phishingangriffe, also zielgerichtete und auf das Opfer präparierte Köder, sind durch präventive Awareness-Schulungen besser zu erkennen und abzuwehren.

KONTINUIERLICHE VERBESSERUNG DURCH EIN FUNKTIONIERENDES INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

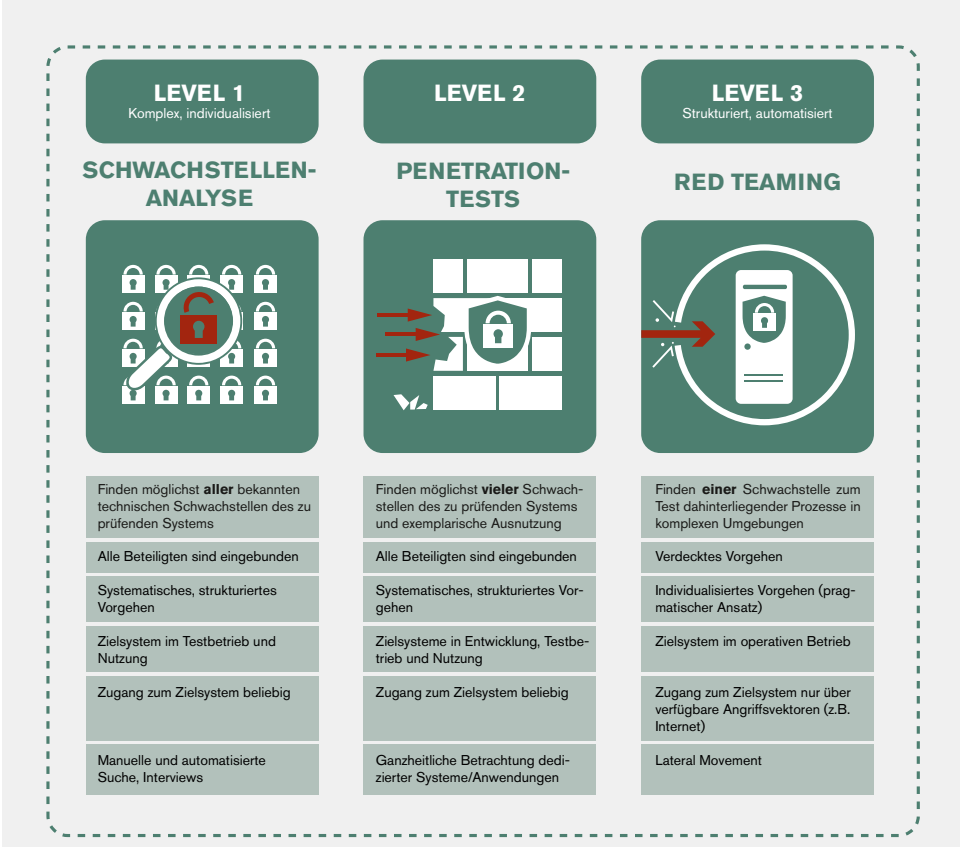
Die Bundeswehr hat sich auf Szenarien im Cyberraum bestmöglich vorbereitet. Dazu sind unterschiedliche Vorkehrungen getroffen. Dies sind zum einen technische Maßnahmen und zum anderen etablierte Prozesse, die die gesamte Kette von Detektion, Reaktion und Prävention umfassen.

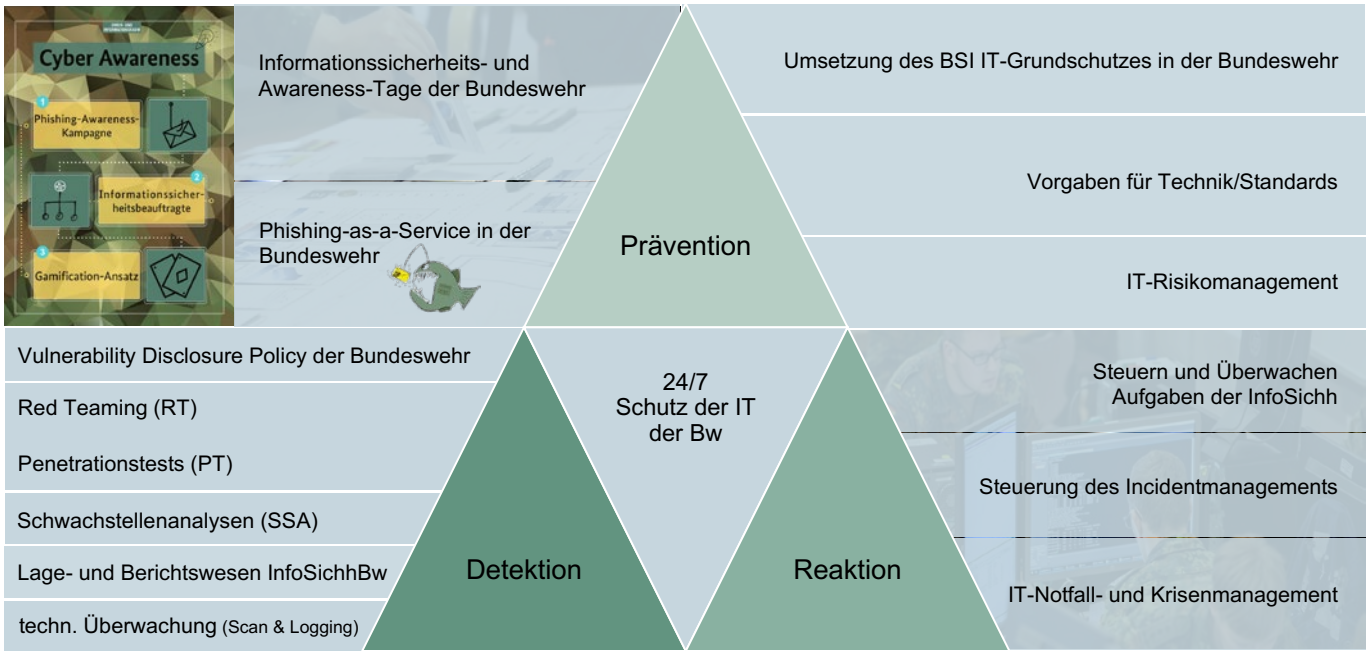
Aber die Angreifer entwickeln ständig ihre Techniken weiter. Alle Nutzerinnen und Nutzer von IT stehen daher täglich vor der Herausforderung, sich nicht von den sich ständig ändernden Taktiken der Angreifer überraschen zu lassen.

Seit 2017 ist dem Stellvertreter Inspekteur Cyber- und Informationsraum (CIR) auch das Amt des „Chief Information Officer der Bundeswehr" (CISOBw) übertragen, welche ich beide im April 2018 übernommen habe. Als Angehöriger des Kommandos CIR in Bonn bin ich daher für die Informationssicherheit in der gesamten Bundeswehr verantwortlich. Als CISOBw ist mir das Zentrum für Cyber-Sicherheit der Bundeswehr in Euskirchen fachlich und seit dem 1.10.2022 auch truppendienstlich unterstellt. Es ist die zentrale Dienststelle zur Gewährleistung eines umfassenden Schutzes der IT-Systeme und -Services der Bundeswehr. Mit seinem Computer Emergency Response Teams (CERT) gewährleistet das Zentrum schnelle und flexible Reaktionen auf Angriffe gegen die IT der Bundeswehr im In- und Ausland und in den Einsätzen.

◀ Die Bundeswehr hat sich auf Szenarien im Cyberraum bestmöglich vorbereitet.
Foto: Bundeswehr/Stefan Uj

▼ Maßnahmen zur Cybersicherheit.
Grafik: Bundeswehr/PIZ CIR





DETEKTION VON EREIGNISSEN UND SICHERHEITSVORKOMMNISSEN

Innerhalb der Netze der Bundeswehr, also zwischen den Netzübergängen in andere Netze, zum Beispiel in und aus dem Internet, auf Servern und auf Arbeitsplätzen, wird der Netzwerkverkehr kontinuierlich auf ungewöhnlichen Datenverkehr, zum Beispiel bei Schadsoftware in E-Mails oder außergewöhnlichen Abfluss von Datenmengen in das Internet, überwacht. Netzwerksensoren erfassen alle Ereignisse und werden im Rahmen eines „Security Information and Event Management" durch Analystinnen und Analysten des Lage- und Überwachungszentrums (LÜZ) im Cyber Security Operations Center der Bundeswehr (CSOCBw) 24/7 ausgewertet und bearbeitet. Das LÜZ ist die zentrale Stelle zur Bearbeitung von Informationssicherheitsvorkommnissen in der Bundeswehr. Von hier aus werden alle wichtigen Stellen für die Behandlung und Eindämmung von sicherheitsrelevanten Vorfällen koordiniert und überwacht.

Die Wirksamkeit umgesetzter Maßnahmen zur Cyber-Sicherheit werden in der Bundeswehr auch regelmäßig durch Sicherheitsinspektionen, Schwachstellenanalysen, Penetrationstests und Red Teaming überprüft, auch unabhängig von besonderen Lagen.

REAKTION

Das CSOCBw im Zentrum für Cyber-Sicherheit der Bundeswehr bearbeitet alle sicherheitsrelevanten Vorkommnisse als zentrale Stelle für den gesamten Geschäftsbereich des BMVg auf operativer Ebene. So kann der Chief Information Security Officer der Bundeswehr die Informationssicherheit mit all ihren komplexen Herausforderungen erfolgreich steuern, überwachen und bedarfsorientiert mit dem IT-Notfallmanagement und IT-Krisenmanagement auf Vorfälle, die strategische Auswirkungen erreichen können, reagieren.

PRÄVENTION

Technik und Prozesse sind aber nichts ohne die Wachsamkeit der Soldatinnen und Soldaten sowie zivilen Mitarbeiterinnen und Mitarbeiter. Ihre Aufmerksamkeit ist entscheidend, ebenso wie die schnelle und richtige Reaktion. Cyberangriffe werden immer komplexer und können nicht immer durch technische Vorkehrungen erkannt und gefiltert werden. Angriffsvektoren nutzen häufig ausgeklügelte Techniken und Taktiken. Es kommt auf jede Soldatin oder zivile Mitarbeiterin und jeden Soldaten oder zivilen Mitarbeiter an. Sie sind, bildlich gesprochen, die letzte Verteidigungslinie – „The last Line of Defense".

Zudem werden in der Bundeswehr die IT-Grundschutzmaßnahmen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) durch Vorgaben und Richtlinien umgesetzt. Durch regelmäßige fachliche Informations- und Awareness-Veranstaltungen bleiben die IT-Nutzenden auf dem aktuellen Stand.

FAZIT

Die Bundeswehr hat ein umfangreiches Informationssicherheitssystem eingerichtet, das kontinuierlich optimiert und an die jeweils aktuelle Bedrohungslage angepasst wird. Dieses System umfasst nicht nur technische (Hard- und Software), sondern auch organisatorische (Rollen und Rechte) und personelle (Ausbildung, Sensibilisierung) Maßnahmen. Damit sind wir jederzeit auf eine Verschärfung der Sicherheitslage vorbereitet und unsere mobilen Computer Emergency Response Teams sind rund um die Uhr verfügbar, um bei akuten Notfällen eingreifen zu können. Wir sind hier gut aufgestellt, aber um dieses Niveau zu halten, müssen wir uns ständig weiterentwickeln.

▲ Schutz der Bundeswehr-IT durch Detektion, Reaktion und Prävention.
Grafik: Bundeswehr/Opper

DIENSTSTELLEN-PROFIL

DIENSTÄLTESTER DEUTSCHER OFFIZIER/ DEUTSCHER ANTEIL 1ST NATO SIGNAL BATTALION

Schulter an Schulter mit Soldatinnen und Soldaten aus elf Nationen leisten wir unseren Beitrag zur Aufrechterhaltung der Führungsfähigkeit der NATO.

AUFGABEN

- Kernauftrag ist die Durchführung aller im nationalen Bereich anfallenden truppendienstlichen Aufgaben, um den Commander 1st NSB und Dienstältesten Deutschen Offizier dabei zu unterstützen, die personelle und materielle Einsatzbereitschaft des Deutschen Anteils 1st NSB sicherzustellen.
- Unterstützung des Einsatzauftrags des 1st NSB auf Basis einer Absichtserklärung (Memorandum of Understanding) zwischen SHAPE und BMVg von 2002.
- Sicherstellen truppendienstlicher Führung und Einsatzfähigkeit in allen nationalen Angelegenheiten (Personalwesen, Versorgung, personelle Einsatzbereitschaft).

AUFTRAG

Die Dienststelle Dienstältester Deutscher Offizier (DDO)/Deutscher Anteil (DtA) 1st NSB Wesel versorgt truppendienstlich den deutschen Anteil des 1st NATO Signal Battalions (1st NSB) und fungiert mit einem nationalen Stab als Host Nation Support oder auch National Support Element. Der Dienststellenleiter ist gleichzeitig Commander 1st NSB, der operativ durch die NATO Communication and Information Systems Group in Mons, Belgien, geführt wird. Das 1st NATO Signal Battalion ist multinational aufgestellt: rund 450 Soldatinnen und Soldaten aus elf Nationen leisten hier ihren Dienst. Ihr Auftrag: Sicherstellung der Führungsfähigkeit der NATO bei Einsätzen und Übungen mittels Informationstechnik. Zusätzlich garantiert das Bataillon bei Übungen im europäischen Raum die Kommunikationsfähigkeit der NATO-Hauptquartiere. Zum NATO-Verband gehören neben dem multinationalen Stab eine Instandsetzungs- und Versorgungskompanie (M&S Coy) sowie sechs schnell verlegbare Kommunikationsmodule – Deployable Communications and Information Systems Module, kurz DCM. Im Prinzip erledigen die DCMs auf NATO-Ebene den gleichen Job wie die Kompanien der IT-Bataillone im Organisationsbereich CIR: Sicherstellen der Führungsfähigkeit mit Hilfe von IT. In einem wesentlichen Aspekt unterscheiden sie sich jedoch: technisch setzen sie auf andere Geräte. Alle DCM sind während des Grundbetriebes in ihren Heimatländern stationiert, eines in Großbritannien, Dänemark und Kroatien sowie drei in Wesel. Dort befindet sich auch der Bataillonsstab des 1st NSB sowie die Versorgungskompanie.

ANSCHRIFT
Schill-Kaserne,
Bocholter Str. 6,
46487 Wesel

DIENSTSTELLENLEITUNG
Oberstleutnant Michael Paul

STAMMPERSONAL
~250

AUFSTELLUNG
1960

INNOVATIONSKRAFT IN DER VERTEIDIGUNG

Moderne Verteidigungslösungen sind innovationsgetrieben – und vor allem digitalisiert

Seit Jahrtausenden reicht bloße Muskelkraft zur Verteidigung nicht aus. Vom Schild über Festungswälle zu heutigen Zero-Trust-Ansätzen in der IT hat sich viel getan. Und eines fällt besonders auf: Entwicklungszeiten verkürzen sich kontinuierlich. Das bedeutet für das Militär, dass eigene Entwicklungen kaum mit dem aktuellen Stand, den die Wirtschaft hervorbringt, mithalten kann.

Ein gutes Beispiel hierfür ist der Krieg zwischen Russland und Ukraine. In diesem setzt die Ukraine auf Drohnen und Open-Source-Software vom offenen Markt. So handelt es sich bei der Aerorozvidka genannten Spezialeinheit der ukrainischen Armee um eine Luftaufklärungseinheit, die entfernte Ziele erkennt, identifiziert und beobachtet. Das hilft dabei, Ressourcen der ukrainischen Armee bestmöglich einzusetzen, indem genau ermittelt wird, wo Wirkmittel abgefeuert werden sollen. Diese Technologie hat eine Erfolgsquote von nahezu 100%. Das illustriert eindrucksvoll, wie eine digitalisierte Truppe mit hochentwickelten Koordinations- und Einsatzführungssystemen einen viel größeren Gegner abwehren kann.

Durch den Einbezug von Innovationen der Wirtschaft in die Verteidigung werden Streitkräfte einerseits besser auf die Vielfalt der Aufgaben – sowohl auf die physischen als auch die in der Cybersphäre – vorbereitet. Andererseits sind sie auch besser dafür gerüstet, mit der steigenden Bedrohungslage auf der ganzen Welt zurechtzukommen.

DREI TREIBENDE KRÄFTE DER INNOVATION

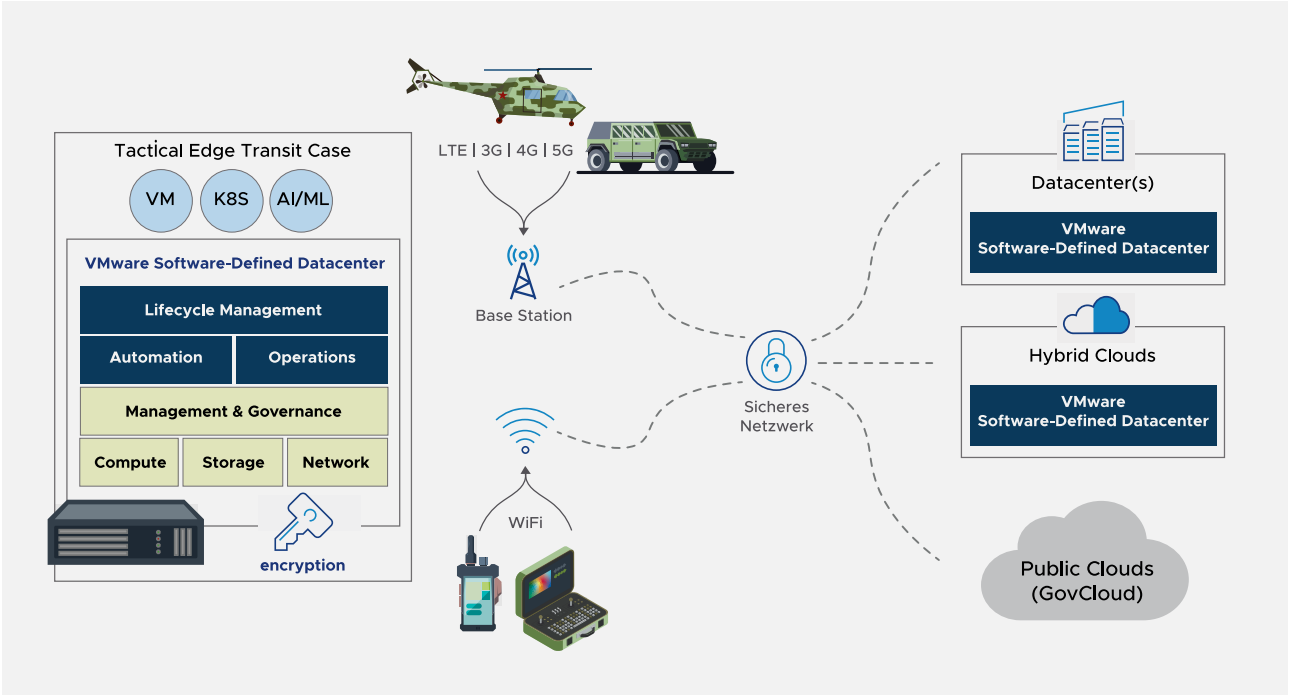
Freie Marktwirtschaft sowie Demokratisierung bringen mit sich, dass einige der fortschrittlichsten Technologien der Allgemeinheit zur Verfügung stehen. Darum können militärische Organisationen davon lernen, wie die Gesellschaft moderne Technologien einsetzt. Wie, wo und wann nutzen die Bürger welche Technologie zu welchem Zweck? Wie werden Informationen ausgetauscht? Die Antworten auf diese Fragen bringen den technologiegetriebenen Fortschritt des Militärs voran. Drei wichtige Faktoren sind dabei für unsere Zeit kennzeichnend:

- Zum einen lösten die Forschungs- und Entwicklungskapazitäten der privaten Unternehmen die staatlichen ab. Die klügsten Köpfe der Welt arbeiten heute in Technologieunternehmen angespornt vom intensiven Marktwettbewerb. Schließlich will kein Konzern von der Konkurrenz abgehängt werden. Deshalb bringen jetzt in erster Linie private Unternehmen bahnbrechende Durchbrüche hervor.

▲ Cybersicherheit steht bei jeder Operation an oberster Stelle.
Foto: iStock.com/Anya Berkut

▶ Ein mobiles, taktisches System im Außeneinsatz.
Foto: VMware

▼ Mobile, taktische Systeme erreichen durch ein sicheres Netzwerk und Software fast grenzenloses Potenzial und statten digitalisierte Truppen für den Einsatz bestmöglich aus.
Grafik: VMware



- Zum anderen wird das Innovationstempo so rasant, dass militärische Organisationen, die nicht die Technologien vom Markt nutzen, sehr schnell ins Hintertreffen geraten. Die freie Wirtschaft präsentiert in kurzen Abständen sinnvolle Verbesserungen.
- Und zu guter Letzt besteht Druck, von den Innovationen der privaten Unternehmen zu lernen, da es der Feind und andere potenzielle Bedrohungen mit allergrößter Wahrscheinlichkeit ebenfalls tun. Das Militär darf unter keinen Umständen das Risiko eingehen, den Anschluss zu verpassen.

RELEVANTE LÖSUNGEN FÜR DAS MILITÄR

Von welchen Software-Produkten der freien Wirtschaft kann das deutsche Militär im Speziellen profitieren? Und welche Vorteile bringen diese mit sich? Beispielsweise kommt die Plattform des Software-Unternehmens VMware auf mobiler, taktischer Hardware zum Einsatz. Die Plattform erfüllt alle wichtigen Aufgaben und bietet dabei folgende Vorteile:

- **Reduktion von Größe und Gewicht:** Intelligente Software automatisiert Rechen-, Speicher- und Netzwerkfunktionen, sodass zusätzliche Hardware am Einsatzort überflüssig wird.
- **Hohes Maß an Sicherheit:** Die Verschlüsselung von Daten und die Installation von Firewalls garantieren einen umfassenden Sicherheitsstandard.
- **Leichte Verwaltbarkeit:** Möglichkeiten zur Anpassung, umfängliche Kontrolloptionen und eine einheitliche Benutzeroberfläche ermöglichen Nutzern ein intuitives Software-Management.
- **Zuverlässige Konnektivität:** Die Plattform von VMware bietet einen sicheren, optimierten Datenaustausch zwischen allen Speicherorten, indem sie die gesendeten Daten komprimiert und filtert. Dies funktioniert selbst in Umgebungen mit geringer/keiner Bandbreite (DDIL).
- **Automatische Problembehebung:** Alle Software-Prozesse, die während eines Einsatzes laufen, können vom Militär überwacht werden. Außerdem behebt Künstliche Intelligenz (KI) Fehler selbstständig, damit alle Systeme im Außeneinsatz stets flüssig laufen.
- **Intelligenter Ressourceneinsatz:** Dank KI und maschinellem Lernen (ML) kann die maximale Rechenleistung der Hardware am Einsatzort abgerufen werden. Dadurch stellt sogar weniger performante Hardware Datenmodelle ohne Auslagerung von Rechenprozessen über das Internet dar.
- **Apps für jede Mission:** Mithilfe von VMware TanzuTM Labs werden Soldaten selbst zu Entwicklern des Militärs, die schnell, agil und sicher neue nutzerfreundliche Missionsanwendungen erstellen. Auch bestehende Programme können sie leicht aktualisieren.

SMARTES MANAGEMENT DER F-35-STAFFEL

Die F-35-Staffel der United States Air Force (USAF) nahm die Unterstützung von VMware TanzuTM Labs in Anspruch, um Verbesserungen des Logistikprozesses schnell und agil umzusetzen. Davor war es ein sehr langwieriger Prozess, einen wöchentlichen Flug- und Wartungsplan für eine F-35-Staffel zu erstellen. Um diesen Vorgang zu beschleunigen, untersuchte die USAF mit Hilfe des TanzuTM Labs Teams, wie der Zeitaufwand für diesen Prozess von Stunden auf Minuten reduziert werden kann. Auf Grundlage der Erkenntnisse konnte die USAF die Anzahl der manuellen Schritte reduzieren und Routine-Aufgaben automatisieren. Das erspart viel Zeit und sorgt für eine optimale Einteilung.

INNOVATION MIT GEZIELTEN SCHRITTEN

Neue Technologien einzuführen ist jedoch nur eine Seite der Medaille. Um zukunftssicher zu sein, müssen militärische Organisationen Szenarien schaffen, die es ermöglichen, Innovationen zu erproben. Denn unter realen Bedingungen müssen Streitkräfte diese reibungslos und erfolgsbringend einsetzen können. Deswegen ist es wichtig, bei der Digitalisierung des Militärs nicht von technologischer Revolution zu sprechen, sondern von einer Evolution. Militärische Organisationen und Regierungen sollten die Umsetzung von Innovationen und digitaler Transformation nicht kopflos überstützen, sondern vielmehr in gründlich durchdachten und geplanten Schritten vorgehen. Erst wenn das Militär neue Technologien modular einführt, um sie von Grund auf zu verstehen und sinnvoll einzusetzen, wird Innovation greifbar und ihr Erfolg messbar.

Wenn Sie sich über Möglichkeiten der Digitalisierung Ihrer Einheit informieren wollen, schreiben Sie an: bundeswehr@VMware.com.

GENERALMAJOR JÜRGEN SETZER,
STELLVERTRETER INSPEKTEUR CIR UND CHIEF INFORMATION SECURITY OFFICER
DER BUNDESWEHR (CISOBW)

PROFESSIONALISIERUNG DES EIGENEN HANDELNS IN DER INFORMATIONSSICHERHEIT

Anwendung einer Vulnerability Disclosure Policy im Behördenumfeld

Oft bleiben Schwachstellen in der Informationstechnik und deren Anwendungen lange unentdeckt – bis sie durch Cyberkriminelle oder andere Akteure im Cyberraum ausgenutzt werden: für kriminelle Zwecke, Spionage und Sabotage. Die Bundeswehr hat sich in den letzten fünf Jahren weiterentwickelt und hat mit der Vulnerability Disclosure Policy (VDP) eine bisher einzigartige sowie ungewöhnliche Lösung im Behördenumfeld geschaffen, um unentdeckte Schwachstellen zu identifizieren.

Trotz sorgfältiger Implementierung der IT, professioneller Konfiguration und umfangreicher Tests können dennoch Schwachstellen vorhanden sein. Zur Überprüfung der Wirksamkeit dieser Schutzvorkehrungen werden regelmäßig Sicherheitsinspektionen und Auditings, Schwachstellenanalysen und Penetration Testing durchgeführt. Auch Red Teaming wird eingesetzt. Das Hacken der eigenen Systeme soll blinde Flecke aufdecken.

Seit Oktober 2020 richte ich mich als Chief Information Security Officer der Bundeswehr (CISOBw) darüber hinaus an alle externen IT-Sicherheitsforscherinnen und -forscher, also die gutgesinnten Hacker, die mit ihrer Expertise Schwachstellen an Systemen der Bundeswehr entdecken und melden. Das „Hacken" von IT-Systemen ist grundsätzlich strafrechtlich relevant. Mit der Vulnerability Disclosure Policy der Bundeswehr (VDPBw) wurden die rechtlichen Rahmenbedingungen für die IT-Sicherheitsforschenden geschaffen. Sie erlaubt den IT-Sicherheitsforschenden, Schwachstellen in den Bundeswehr-Systemen zu suchen, sie zu identifizieren und auch mitzuteilen, bevor Angreiferinnen und Angreifer diese missbrauchen können. Dabei kommt es nicht zum Konflikt mit dem Strafgesetzbuch. Eine Strafbarkeit entfällt somit. Diese Experten und Expertinnen verfolgen eine gute Absicht und leisten einen Beitrag zu unserer aller Sicherheit und somit dem Gemeinwohl. Hierbei steht der gemeinsame Sicherheitsgedanke des Internets im Vordergrund.

▼ Besonders verdiente IT-Sicherheitsforschende werden mit dem VDPBw-Coin ausgezeichnet.
Foto: Bundeswehr/Stefan Uj

KEIN FREITICKET ZUM HACKING

Durch die VDPBw wird ein straffreier Rechtsrahmen der Schwachstellensuche durch externe IT-Sicherheitsforschende in IT-Systemen der Bundeswehr beschrieben. Alle IT-Sicherheitsforschende, die sich an diese Regeln halten, sind von einer Strafverfolgung ausgeschlossen. Zu diesen veröffentlichten Regeln gehört zum Beispiel, dass die entdeckte Schwachstelle oder das Problem nicht ausgenutzt sowie Informationen darüber nicht ohne die Zustimmung der Bundeswehr an dritte Personen oder Institutionen weitergegeben werden dürfen.

BISHER EINMALIG IM DEUTSCHEN BEHÖRDENUMFELD

Der Geschäftsbereich des Bundesministeriums der Verteidigung sowie die Bundeswehr sind Vorreiter einer solchen Richtlinie von Schwachstellenmeldungen im Behördenumfeld.

Im Fokus steht die Sicherheit des eigenen IT-Systems. Böswilligen Hackern soll es schwerer gemacht werden, in Bundeswehr-Netzwerke einzudringen oder andere Schäden anzurichten. Dank der Unterstützung der Meldenden und ihrer ausführlichen Dokumentationen ist das Sicherheitsniveau der Bundeswehr-IT verbessert worden.

UNSEREN DANK UND RESPEKT ZEIGEN WIR AUCH ÖFFENTLICH

Die hohe Anzahl an Meldungen zeigt, dass der durch die Bundeswehr ausgelobte nicht monetäre Anreiz wirksam ist. Besonders verdiente IT-Sicherheitsforschende werden mit dem VDPBw-Coin ausgezeichnet. Eine Grundvoraussetzung dafür ist, mindestens drei qualifizierte IT-Schwachstellen bei der Bundeswehr gemeldet zu haben.

Die Bundeswehr hat mit der VDPBw einen vorsichtigen Einstieg in dieses Instrument der Schwachstellenmeldungen gewählt. Zwar sind wir bislang alleiniger Vorreiter im Behördenumfeld, aber andere wollen nachziehen. So kann gemeinsam das gesamtstaatliche Sicherheitsniveau verbessert werden.

Großer Dank und Respekt geht an alle IT-Sicherheitsforschenden, die dazu beitragen, die IT-Systeme der Bundeswehr sicherer zu machen. Diesen Dank machen wir öffentlich mit dem individuellen Eintrag und der Namensnennung auf einer Dankesseite auf bundeswehr.de. Warum das ein zusätzlicher Anreiz sein kann? Welcher Hacker kann schon legal von sich behaupten, dass er die Bundeswehr gehackt hat und mit seiner Hilfe dort eine Schwachstelle gefunden und das Internet ein wenig sicherer gemacht wurde?

Die Anwendung der VDPBw kann deshalb – als Ergänzung zu den durch bundeswehreigene Kräfte durchgeführten Untersuchungen – Informationen zu unbekannten Schwachstellen und Sicherheitslücken in den Systemen der Bundeswehr liefern. Sie trägt dazu bei, jene Schwachstellen und Lücken zu schließen und so das Risiko eines erfolgreichen Angriffs gegen die Bundeswehr-Informationstechnik zu vermindern. Als Chief Information Security Officer der Bundeswehr der gesamten deutschen Streitkräfte setze ich auf das Wissen und die Hilfe der Cyber-Community für ein sichereres Internet in Deutschland und Europa.

GENERALMAJOR JÜRGEN SETZER,
STELLVERTRETER INSPEKTEUR CIR UND
CHIEF INFORMATION SECURITY OFFICER
DER BUNDESWEHR (CISOBW)

WEITERENTWICKLUNG EINER AKTIVEN AWARENESS-STRATEGIE ZUM SCHUTZ DER IT DER BUNDESWEHR

Täglich leisten knapp eine Viertelmillion Angehörige der Bundeswehr ihren Dienst: im Grundbetrieb und im Einsatz, an zirka 1.500 Standorten im In- und Ausland. Wie schafft es das Team um den Chief Information Officer der Bundeswehr (CISOBw), alle Bundeswehrangehörigen für die Gefahren des Cyberraums so zu sensibilisieren, dass sie sich diesen dienstlich wie privat erfolgreich entgegenstellen können?

Cyberangriffe werden täglich komplexer und können nicht immer durch technische Vorkehrungen erkannt und gefiltert werden. Die Aufmerksamkeit unserer Soldatinnen und Soldaten sowie zivilen Mitarbeiterinnen und Mitarbeiter ist entscheidend, verbunden mit ihrer schnellen und angemessenen Reaktionsfähigkeit. Jeder/jede einzelne an seinem/ihrem Arbeitsplatz leistet damit einen aktiven Beitrag zur „digitalen Einsatzbereitschaft" der Bundeswehr, aber auch für den persönlichen Schutz in der digitalen Welt. Diese Awareness beim Umgang mit IT darf an der Kasernenschranke nicht aufhören.

„Denken ist die schwerste Arbeit, die es gibt. Das ist wahrscheinlich auch der Grund, warum sich so wenig Leute damit beschäftigen."

Henry Ford

Angreifer nutzen häufig ausgeklügelte Phishing-E-Mails, speziell auf die Nutzenden zugeschnitten. Ohne weiteres Nachdenken wird ein beworbener Link geklickt, der Zugang zum Internet hergestellt und ungeprüfte Anhänge aus unbekannten Quellen landen auf dem Rechner. Diese Anhänge werden oft nicht nur heruntergeladen, sondern im Hintergrund direkt ausgeführt und installiert – eine „Serviceleistung", die vielen Userinnen und Usern nicht einmal auffällt und die schon gar nicht erwünscht ist. Im Umkehrschluss bedeutet das: es kommt auf jeden Mitarbeitenden an. Die Bundeswehrangehörigen sind, bildlich gesprochen, „The last Line of Defense" – die letzte Verteidigungslinie.

NACHHALTIGE AUFMERKSAMKEIT ERZEUGEN

Alle Dienststellen in der Bundeswehr sind angehalten, eine jährliche Auffrischung zur Informationssicherheit für ihre IT-Nutzenden durchzuführen und diese für aktuelle Gefahren fortlaufend zu sensibilisieren. PowerPoint ist üblicherweise das Standardwerkzeug von Präsentationen in der Bundeswehr – auch in der Informationssicherheit. Die Zuhörerschaft nimmt die Inhalte jedoch oft nur passiv wahr, weil sie die Folien entweder nicht verstehen oder keine Relevanz für sich erkennen. Wissen permanent auf die gleiche Weise oder in abstrakter Form zu vermitteln, führt zu Ineffizienz. Cyber-Awareness muss zu einem eingeübten ständigen Verhaltensmuster werden. Wie das Anlegen des Sicherheitsgurtes in einem Kraftfahrzeug vor Fahrtbeginn, sollte vor dem Öffnen einer E-Mail oder eines Anhanges ein „Kontrollblick" genauso selbstverständlich sein – hierzu genügt

▲ Cyberangriffe werden täglich komplexer und können nicht immer durch technische Vorkehrungen erkannt und gefiltert werden.

◀ Mit Gamification-Angeboten zur Informationssicherheit spielerisch die Cyber-Awareness trainieren.
Foto: Bundeswehr/Rana Sarah Wolf

oft schon die Ansicht der genauen Absenderadresse oder des Betreffs: Ergibt dieser Sinn? Ist mir der Absendende bekannt? Erscheint die Schreibweise der E-Mail-Adresse logisch? Ist der Provider bekannt? All diese Prüffragen sind durch einen kurzen, aber kritischen „Kontrollblick" schnell zu beantworten. Nichts schützt unsere Informationen und IT so gut, wie aufmerksame Mitarbeitende – auch und vor allem im Homeoffice.

Wie kann man Menschen für Themen der Informationssicherheit gewinnen, sie zum Mitmachen motivieren und nachhaltig sensibilisieren? Dies ist besonders in Zeiten von Telearbeit und Homeoffice eine fordernde Aufgabe. Immerhin soll die Sensibilisierung die Mitarbeitenden im besten Fall zu einer positiven und langanhaltenden Verhaltensänderung führen. Es ist deshalb besonders wichtig, alle Angehörigen der Bundeswehr in der Cyber-Awareness zu schulen und sie hierzu an ihrem jeweiligen Arbeitsplatz abzuholen.

▶ IT-Sicherheitsbeauftragte haben verschiedene Möglichkeiten, die Cyber-Awareness der Mitarbeitenden zu verbessern.
Grafik: Bundeswehr/PIZ CIR

WENIGER POWERPOINT – MEHR GAMIFICATION UND SIMULATION

Spielerisches Lernen mit Spaß erhöht die Aufnahmebereitschaft und ist je nach Inhalt, Lerntyp und Lernziel eine empfehlenswerte Methode, um die Lernmotivation zu steigern und Abwechslung zu fördern. Jeder Informationssicherheitsbeauftragte einer Dienststelle kann dabei auf Produkte eines Gamification-Angebots sowie die Beratung zum individuellen Einsatz zurückgreifen. Unter der Federführung des Zentrums für Cyber-Sicherheit der Bundeswehr (ZCSBw) wird das Portfolio ständig erweitert. Die Materialien reichen vom einfachen methodischen Memory-Lernspiel bis zum komplexen strategischen Planspiel.

SIMULATION VON CYBERANGRIFFEN: PHISHING-AS-A-SERVICE IN DER BUNDESWEHR

Train as you fight! – ein überlebenswichtiger Grundsatz aller einsatzbereiten Streitkräfte. Die Bundeswehr trainiert den Ernstfall eines Cyberangriffs mit der Simulation des „Phishing-as-a-Service". Hierbei versuchen fiktive Cyberangreifende die IT einer zuvor festgelegten Dienststelle der Bundeswehr anzugreifen, zu hacken und so Daten zu erbeuten, was im schlimmsten Fall die Einsatzbereitschaft oder Führungsfähigkeit der Bundeswehr beeinträchtigt.

Phishing ist eine Social-Engineering Technik und versucht mit gefälschten E-Mails oder Webseiten den Internetnutzenden zur Preisgabe von vertraulichen Informationen, wie Kennwörter oder Bankdaten, zu ködern.

Bei der Durchführung dieser Simulation werden reale Cyber-Bedrohungslagen über einen Zeitraum von sechs bis acht Wochen durchgespielt. Wie bei einem Truppenübungsplatzaufenthalt werden alle Teilnehmenden auf die Erkennung von Cyberangriffen und folgerichtiges Handeln trainiert. Einziger Unterschied: der Kreis der Teilnehmenden befindet sich weiterhin im Realbetrieb und weiß nichts von seiner aktiven „Übungsplatzteilnahme". Komplette Dienststellen können so umfassend und ressourcensparend einer Schulung unterzogen und Informationssicherheitsprozesse auf Wirksamkeit überprüft werden.

Die wesentlichen Lerneffekte dabei sind, IT-gestützte Angriffe wie Phishing-E-Mails, aktiv und rechtzeitig zu erkennen und die Anwendung der Prozesse der Informationssicherheit einzuüben.

Die Informationssicherheitsbeauftragten in den Dienststellen der Bundeswehr haben mit derartigen Maßnahmen ein probates Mittel zur Verfügung, um beispielsweise zum Schutz vor Social-Engineering vor Ort bedarfsorientiert zu sensibilisieren und das Gefahrenbewusstsein ihrer Mitarbeitenden zu schärfen. Der steigenden Gefahr vor zukünftigen (Cyber-)Angriffen kann hierdurch im Dienst und im heimischen Umfeld entgegengewirkt werden.

Mit der Weiterentwicklung einer aktiven Awareness-Strategie hat die Bundeswehr einen ressourcensparenden, nachhaltigen Weg gefunden, eine große Anzahl von Mitarbeitenden effektiv zu sensibilisieren und sich auf zukünftige (Angriffs-)Szenarien im Cyberraum bestmöglich vorzubereiten.

Beim Social-Engineering werden menschliche Eigenschaften wie Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autorität ausgenutzt, um Personen geschickt zu manipulieren. Cyber-Kriminelle und Angreifer verleiten das Opfer auf diese Weise beispielsweise dazu, vertrauliche Informationen preiszugeben, Sicherheitsfunktionen auszuhebeln, Überweisungen zu tätigen oder Schadsoftware auf dem privaten Gerät oder einem Computer im Firmennetzwerk zu installieren.

DIENSTSTELLEN-PROFIL

ZENTRUM FÜR CYBER-SICHERHEIT DER BUNDESWEHR

Gebündelte Fähigkeiten zur Cyberverteidigung

AUFGABEN

- Das ZCSBw betreibt das Cyber Security Operation Centre der Bundeswehr mit dem Computer Emergency Response Team der Bundeswehr zur Gewährleistung des zentralen informationssicherheitstechnischen Schutzes und der Überwachung der IT der Bundeswehr.
- Stellt Fähigkeiten mit zentralen IT-Diensten, Dienstleistungen und Ansprechstellen für das Kryptowesen, zur Versorgung der Bundeswehr mit fremden und eigenen Kryptomitteln sowie für die Public Key Infrastructure (PKI) als zertifikatsbasierten digitalen Authentifizierungs-, Verschlüsselungs- und Signaturdienst bereit.
- Nimmt mit der Deutschen militärischen Security Accreditation Authority, auf Basis einer Ressortvereinbarung mit dem Bundesministerium des Innern, die Aufgaben der Nationalen Security Accreditation Authority für alle IT-Systeme im Geschäftsbereich des BMVg wahr.

AUFTRAG

Das Zentrum für Cyber-Sicherheit der Bundeswehr (ZCSBw) ist die zentrale Dienststelle zur Gewährleistung eines umfassenden Schutzes der IT-Systeme und -Services der Bundeswehr. Dabei stellt das Zentrum die Kernexpertise für die Absicherung der Informationstechnik und den darin verarbeiteten Informationen bereit. Mit seinen Incident Response Teams gewährleistet das Zentrum schnelle und flexible Reaktionen auf Angriffe gegen die IT der Bundeswehr im In- und Ausland und in den Einsätzen. Es wirkt bei externen, nationalen wie internationalen Partnern sowie multi- oder supranationalen Organisationen wie der NATO und EU mit.

ANSCHRIFT
Generalmajor-Freiherr-von-Gersdorff-Kaserne,
Kommerner Straße 188,
53879 Euskirchen

DIENSTSTELLENLEITUNG
Oberst Tim Zahn

STAMMPERSONAL
~590

AUFSTELLUNG
01.04.2017

OBERSTLEUTNANT CHRISTOPH KÜHN,
DEZERNATSLEITER „CYBER-BEDROHUNG & RISIKOANALYSE“,
ABTEILUNG CYBER SECURITY OPERATIONS CENTRE
DER BUNDESWEHR (CSOCBW) DES ZENTRUMS FÜR
CYBER-SICHERHEIT DER BUNDESWEHR (ZCSBW), EUSKIRCHEN

OBERSTLEUTNANT MARKUS MAYBAUM, SENIOR LIASON OFFICER,
NATO CYBERSPACE OPERATIONS CENTRE (CYOC),
SUPREME HEADQUARTER ALLIED POWERS EUROPE (SHAPE), BELGIEN

Bestens gewappnet für die Landes- und Bündnisverteidigung im Cyberraum: **Das Cyber Security Operations Centre der Bundeswehr**

Die deutsche Außen- und Sicherheitspolitik erlebte im ersten Quartal 2022 eine Zäsur. Seit dem Beginn des Angriffskriegs Russlands gegen die Ukraine ist klar, dass konventionelle militärische Konflikte in Europa keinesfalls der Vergangenheit angehören. Diese Zeitenwende hat vielen in der westlichen Welt eine überwunden geglaubte geopolitische Realität vor Augen geführt. Im Cyber- und Informationsraum kam diese Entwicklung weniger überraschend. Seit Jahren beobachten wir einen fortschreitenden Trend zu immer gezielteren und technisch ausgereiften Cyberangriffen auf IT-Systeme staatlicher Organisationen, kritischer Infrastrukturen, der Industrie und der Wissenschaft. Dies beschränkt sich nicht nur auf Deutschland, sondern betrifft unsere europäischen und transatlantischen Partner gleichermaßen. Auch die Bundeswehr ist ein attraktives Ziel für Angriffe aus dem Cyberraum.

Die Bundeswehr hat zum Schutz ihrer IT-Systeme das Zentrum für Cyber-Sicherheit der Bundeswehr (ZCSBw) im Organisationsbereich Cyber- und Informationsraum (CIR) aufgestellt, das seinen Hauptstandort in Euskirchen hat. Zum ZCSBw gehört auch die Abteilung Cyber Security Operations Centre der Bundeswehr (CSOCBw) als operativer Nukleus mit der Aufgabe, durch präventive und reaktive Maßnahmen die Cybersicherheit aller in der Bundeswehr eingesetzten IT-Systeme zu gewährleisten.

HERAUSFORDERUNGEN DES CYBER- UND INFORMATIONSRAUMS

Zur Abgrenzung der Aussagen sei an dieser Stelle erwähnt, dass sich dieser Artikel mit dem Schutz der IT-Systeme befasst. Andere Aspekte der Dimension CIR, wie zum Beispiel das Elektromagnetische Spektrum oder strategische Kommunikation, werden nicht betrachtet. Der CIR hat im Vergleich zu den Dimensionen Land, Luft, Wasser und Weltraum die besondere Eigenschaft, dass feindliche Kräfte mit ihren „Waffensystemen“ beliebige Entfernungen praktisch ohne Zeitverzug überwinden können. Grundsätzlich müssen die Akteure nicht am Ort der Wirkung anwesend sein, sondern nutzen Weitverkehrsnetze, häufig das Internet, um Ergebnisse am Zielort oder auch meh-

reren Orten gleichzeitig zu erwirken. Die Angriffe sind dabei jedoch nicht vollständig unsichtbar, sondern können durch Veränderungen im Datengefüge festgestellt werden. Hierzu bedarf es einer genauen Beobachtung und des Vergleichs des Soll- mit dem Ist-Zustand. Aufgrund der schnellen Überwindung von Entfernungen ist eine stetige Bedrohungslage der IT der Bundeswehr gegeben. In Analogie zu realen Einsätzen kann die Gefechtssituation im CIR als asymmetrisch bezeichnet werden. Auch im Cyberraum kann sich ein einzelner Gegner mit einer guten Taktik in ein (virtuelles) Lager schleichen und dort ein (virtuelles) Wirkmittel zur Umsetzung bringen oder Informationen stehlen. Die operativen Fähigkeiten der Kräfte der Informationssicherheit müssen dieser asymmetrischen Bedrohung begegnen.

▲ Die Bundeswehr hat zum Schutz ihrer IT-Systeme das Zentrum für Cyber-Sicherheit der Bundeswehr (ZCSBw) im Organisationsbereich Cyber- und Informationsraum (CIR) aufgestellt.
Foto: Bundeswehr/Martina Pump

DAS CYBER SECURITY OPERATIONS CENTRE DER BUNDESWEHR (CSOCBW)

Strukturell ist das CSOCBw eine Abteilung des ZCSBw mit dem Kernauftrag, Informationssicherheit zu schützen und zu überwachen sowie diese wiederherzustellen, wenn sie gestört wurde. Informationssicherheit wird hierbei definiert als die Gewährleistung der Verfügbarkeit, der Vertraulichkeit und der Integrität der Informationen, meist im Zusammenhang mit ihrer Speicherung und Verarbeitung auf IT-Systemen. Während die Verfügbarkeit und die Vertraulichkeit von Informationen weitestgehend selbsterklärend sind, wird die Integrität von Informationen oftmals falsch interpretiert. Diese definiert den Schutz vor unbefugten und unzulässigen Veränderungen von Informationen und IT-Diensten und damit ihre Verlässlichkeit.

Vor dem Hintergrund einer über die letzten Jahre hinweg stets zunehmenden Gefährdung durch Spionage und Cyber-Kriminelle verwundert es nicht, dass diese Hauptaufgaben des CSOCBw de facto seit geraumer Zeit eine Dauereinsatzaufgabe ist. Diese Aufgabe muss auch im Frieden ständig er-

füllt werden und bedeutet, dass Teile des Lage- und Überwachungszentrums (LÜZ), ein Dezernat der Abteilung, ihren Dienst rund um die Uhr versehen.

Neben dieser offensichtlichen Präsenz von Personal führen aber auch andere „Mitarbeitende" der Abteilung ihre Fähigkeiten 24/7 aus. Diese sind keine Menschen, sondern Sensoren. Sie überwachen die IT-Systeme der Bundeswehr, insbesondere die Übergänge der Netzwerke und registrieren Veränderungen. Sie unterstützen dabei, bekannte Angriffsmuster zu erkennen. Hierbei gewonnene Lagedaten werden weitgehend automatisiert, bei Bedarf aber auch manuell durch die Analystinnen und Analysten ausgewertet.

Für die sachgerechte Ausbringung dieser Sensoren, deren Betrieb sowie für ständig notwendige Anpassung der Regeln für die teilautomatisierte Auswertung der Daten sind die Fachleute im Dezernat Technisches Lagebild verantwortlich.

Werden Angriffe gegen die Bundeswehr erkannt, gilt es, zügig zu handeln. Hier kommen die Spezialistinnen und Spezialisten des Dezernats Computer Emergency Response Team der Bundeswehr (CERTBw) zum Einsatz. Basierend auf Sensordaten, aber auch auf Beobachtungen und Meldungen von Fach- und Laienpersonal, können Incident Response Teams den Betroffenen helfen, die Informationssicherheit wiederherzustellen, gleichzeitig Beweise zu sichern und auszuwerten. Diese Erkenntnisse werden benötigt, um Maßnahmen zu entwickeln, ein vergleichbares Eindringen in Zukunft auszuschließen. Neben der Reaktion auf regelbasierte Auswertungen können spezialisierte Kräfte in Systemen auch nach Spuren, die auf die Anwesenheit von Eindringlingen schließen lassen, suchen. Diesen Vorgang nennt man „Cyber Threat Hunting": das Aufspüren von Cyberbedrohungen. Diese Methode gleicht der sprichwörtlichen Suche der Nadel im Heuhaufen. Sind jedoch gegnerische Kräfte, die Bedrohungslage sowie typische Taktiken des Gegners bekannt, können Abwehr und defensive Operationen passgenau darauf abgestimmt werden. Unter anderem für dieses Wissen ist im CSOCBw das Dezernat Cyber-Bedrohung und Risikoanalyse zuständig. Es liefert aber auch Risikoabschätzungen und Informationen für andere Bereiche, um Schwachstellen bewerten und schließen zu können.

Neben diesen vier operativen Dezernaten besitzt die Abteilung eine eigene Teileinheit für den Betrieb und die Konfiguration der IT-Systeme, die zur Lagefeststellung und zur Aufrechterhaltung und Wiederherstellung der Informationssicherheit genutzt werden. Dieses Dezernat gewährleistet die schnelle Reaktion auf Angriffe oder Ausfälle. Denn natürlich sind auch diese IT-Systeme gefährdet.

EINSATZ DER CSOCBW-KRÄFTE – IM FRIEDEN UND DARÜBER HINAUS

Grundsätzlich verlegen die hochspezialisierten Kräfte des CSOCBw selten an die „Front" – und das aus guten Gründen. Hochgradige Vernetzung bietet auch für CSOCBw-Kräfte die Möglichkeit, Aktionen nahezu verzugslos an IT-Systemen standortunabhängig durchzuführen, gleiches gilt im Konfliktfall auch für Einsatzkräfte in der Verteidigung. Im sogenannten Reach-Back Verfahren können IT-Betriebs- und dezentrale Informationssicherheitskräfte Fähigkeiten des CSOCBw anfordern, wenn eine Unterstützung notwendig wird. Zwar sind die Incident Response Teams mit mobiler Technik ausgestattet und damit grundsätzlich weltweit einsetzbar und können auch unter Einsatz- und Gefechtsbedingungen operieren, jedoch sind die technischen und analytischen Möglichkeiten am Heimatstandort Euskirchen für die Mehrzahl der Einsatzfälle schneller und besser verfügbar. Hierzu zählt auch der Rückgriff auf weitere Fachleute. Außerdem wird so Reisezeit eingespart und im Verteidigungsfall eine Hochwertressource einer unmittelbaren Gefährdung entzogen.

Für die Vorbereitung auf einen möglichen Verteidigungsfall ist es bereits heute sinnvoll, mögliche Eindringversuche von (potenziellen) Gegnern zu blockieren beziehungsweise gelungene Infiltrationen zu erkennen und mögliche Ankerpunkte zu entfernen. Untersuchungen zeigen eindeutig, dass die Vorbereitung eines Cyber-Angriffs wesentlich länger dauert als der Angriff selbst. Entsprechend muss das CSOCBw – durchgehend – die Zeit nutzen, seine Aufgaben zu erfüllen, in der ein Gegner seinen Angriff auf die IT der Bundeswehr vorbereiten kann. Hier sei der Vergleich zu einem realen Konflikt herangezogen. Das Ausspionieren der Lage gegnerischer Kräfte, die Planung des Einsatzes, das Annähern an die Stellungen des Gegners, das Überwinden der Umzäunung ohne Spuren, das Umgehen von Wachposten sowie das Tarnen des Verstecks

eines eingebrachten Wirkmittels dauert deutlich länger, als die Zündung desselben, wenn das Ziel in der Nähe ist. Die Abwehr und das Identifizieren von Gegnern muss also im Fokus unseres Handelns liegen.

Neben diesem stillen, asymmetrischen Kampf ist natürlich auch ein massiver Angriff auf die IT-Systeme möglich. Während die zuvor beschriebene Situation alle drei Grundwerte der Informationssicherheit gleichermaßen gefährdet, wird sich ein massiver Angriff meist nur gegen die Verfügbarkeit von Systemen richten. Der Fachbegriff hierfür ist (Distributed) Denial of Service Attack (DDOS): ein (verteilter) Angriff, um IT-Dienste

▲ Grundsätzlich verlegen die hochspezialisierten Kräfte des CSOCBw selten an die „Front" – und das aus guten Gründen.
Foto: Bundeswehr/Stefan Uj

auszuschalten. Der Allgemeinheit bekannt sind hier die Massierung von Anfragen auf einen Web-Server von vielen, durch den Angreifer gesteuerten Rechnern, sodass das Angriffsziel unter der Last zusammenbricht oder legitime Anfragen nur sehr verzögert beantwortet werden. Diese Art von Angriffen ist natürlich leicht zu entdecken. Es kann davon ausgegangen werden, dass solche Angriffe im Verteidigungsfall häufiger vorkommen als im Frieden, da sie schnell und relativ flexibel eine Schwerpunktsetzung erlauben und die angreifenden Systeme allein aufgrund ihrer Anzahl nicht ausgeschaltet werden können. Auch in der gegenwärtigen Lage wurden diese schon beobachtet. Kräfte der Informationssicherheit des CSOCBw können in einem solchen Szenario nur begrenzt unterstützen. Stattdessen muss hier durch Architekturen und Redundanzen die Projekte, IT-Betriebskräfte, aber auch kommerzielle Dienstleister bereitstellen, eine Resilienz eigener Systeme erreicht werden. Theoretisch ist es im Rahmen der bestehenden Gesetzeslage auch möglich, das System, das den verteilten Angriff steuert, durch Cyber-Operationen auszuschalten.

BÜNDNIS- UND LANDESVERTEIDIGUNG?

Als nächstes werden zwei offensichtliche Eigenschaften der Landes- und der Bündnisverteidigung betrachtet, nämlich der internationale und der nationale Kontext.

Wie in den geografischen Dimensionen dürfen wir unsere Aktionen im Cyberraum und deren Auswirkungen nicht losgelöst von der Umwelt betrachten. Gemeinsames Agieren muss koordiniert und trainiert werden. Deshalb ist es wichtig, dass ein enges Zusammenwirken mit befreundeten Staaten und Organisationen etabliert und gelebt wird. Im internationalen Zusammenhang ist dies die bi- und multinationale Zusammenarbeit, insbesondere in der EU, der NATO und dem deutschsprachigen D-A-CH-Raum. Hier sind Austauschprozesse über erkannte und bewertete Angriffsverfahren und -muster aufgebaut und über das Jahr mehrere gemeinsame Übungen verteilt. Erneut greift die Dimensionseigenschaft der Grenzenlosigkeit. Im Bündnisfall können, wenn man dies zuvor vorbereitet und geübt hat, Kräfte einer Nation schnell aus dem Reach-Back den Verteidigern an anderer Stelle zur Hilfe kommen.

Auch im nationalen Kontext sind die Zusammenarbeit und der Austausch existenziell. Hierfür gibt es mehrere Gründe. Zum einen erneut die Grenzenlosigkeit: ein durch einen fremden Staat initiierter Angriff kann im Cyberraum physikalisch von IT-Systemen im Inland ausgehen, jedoch problemlos aus dem Ausland gestartet und gesteuert werden. Durch die Asymmetrie von Aufwand und Wirkung kann eine kleine Aktivität – eventuell unbeabsichtigt durch eine Fehlkonfiguration – den massiven Ausfall von kritischer Infrastruktur und den Verlust von Leben nach sich ziehen. Man muss sich nur den Ausfall einer elektronischen Signalanlage auf einer Bahnstrecke oder die Veränderung von Datensätzen in der IT-gestützten Medizinausgabe eines Krankenhauses vorstellen. Klar sind hier der Informationsaustausch und die Zusammenarbeit der Ressorts für die innere und die äußere Sicherheit notwendig. Hierzu wurde das gemeinsame Cyber-Abwehrzentrum eingerichtet, in dem unter anderem das Innen- und das Verteidigungsministerium vertreten sind.

Die Zeiten, in denen dedizierte Kupferleitungen die Nachrichten der Streitkräfte übermitteln und verteilen, sind vorbei. Auch für die Streitkräfte ist das Internet das Medium, um Daten zu übertragen. Offenkundig ist es kein militärisch betriebenes Netzwerk und ein Angriff auf die Streitkräfte oder Regierungsorganisationen im Cyberraum wird privatwirtschaftliche Infrastruktur nutzen und stören. Auch hier ist der Vergleich zur realen Welt statthaft. Im Krieg werden Straßen, Schienen und

◀ Wo immer Personal des ZCSBw heute tätig ist, versuchen wir ein Bewusstsein zu schaffen, dass Informationssicherheit kein Hemmschuh ist.
Foto: Bundeswehr/Stefan Uj

Energieversorgung Ziele sein, um insbesondere die Logistik der gegnerischen Kräfte zu beeinflussen. Störungen des Internets und der Verkehrsinfrastruktur werden auch die private Wirtschaft und das bürgerliche Leben beeinflussen. Durch Störungen oder Zerstörungen von Sendeanlagen ist mit dem teilweisen Ausfall der mobilen, drahtlosen Datenübertragung zu rechnen. Dabei liegt es in der Natur des Cyberraums und seiner Bedeutung für Führung und Logistik, dass eine Störung sich nicht auf die Kampfzonen im Frontbereich begrenzen wird. Eine ressortübergreifende gemeinsame Lage und gemeinsame Aktionen sind notwendig und müssen verabredet und trainiert werden. Deshalb unterhält das CSOCBw bereits jetzt enge Kontakte zum CERT-Bund, zu Telekommunikationsanbietern und vielen anderen Akteuren im Cyberraum.

GIBT ES GAR KEINEN UNTERSCHIED ZWISCHEN FRIEDEN, KRISE UND VERTEIDIGUNG?

Ein erwartbarer Unterschied zwischen der heutigen Situation und der im Verteidigungsfall ist, dass im Gegensatz zu heute, wo wir meist statische und stationäre Netzwerke überwachen, in einer Operation mobile Informationsnetzwerke aufgebaut werden. Sie verbinden unterschiedliche, je nach Situation benötigte Systeme miteinander, teilweise ad-hoc. Diese Besonderheit ist ein Grund, warum die Streitkräfte eigene Informationssicherheitsorganisationen, -mittel und -kräfte haben, die sich von den zivilen Kräften unterscheiden. Wie oben dargestellt, müssen wir zum erfolgreichen Durchführen unseres Auftrags Sensoren an wichtigen Stellen im Netz haben, über Reach-Back auf die Systeme zugreifen können und das Zusammenspiel der Systeme verstehen. Dies ist in einer Gefechtssituation extrem schwierig. Um die Situation zu verbessern, baut das Dezernat Technisches Lagebild bei Übungen wie dem „Gelben Merkur" unsere Sensoriken in die mobilen Einsatznetze ein. Dies fördert die Handlungssicherheit und bringt Erkenntnisse sowohl für die Fernmelderinnen und -melder und Informationstechnikerinnen und -techniker des Betriebs als auch für unsere Analystinnen und Analysten. Bereits lange geplant, wird dieses Jahr die Verlegung von Gefechtsständen trainiert, um den mobilen Einsatz zu üben. Dabei wird die Truppe auch regelmäßig darauf aufmerksam gemacht, falls durch die operative Hektik Grundzüge der Informationssicherheit massiv und unnötig verletzt werden.

Auch die Risikobewertung ändert sich zwischen Frieden, Krise und Krieg massiv. In einer operativen Lage kann sich die Risikobereitschaft je nach Situation ändern. Auch kann es die operative Situation notwendig machen, dass Systeme, die bekanntermaßen infiltriert und unsicher sind, weiterhin betrieben werden müssen, da von deren Betrieb der Erfolg einer Operation abhängt. Das Dezernat Cyber-Bedrohung/Risikoanalyse definiert und entwickelt hierzu in Zukunft Prozesse, um es den IT- und Sicherheitsspezialisten vor Ort zu ermöglichen, schnell und lageangepasst die militärische Führung zu beraten.

Und was hat sich seit Beginn des Ukraine-Krieges Ende Februar 2022 bereits im täglichen Dienst des CSOCBw geändert? Zum einen wurden die ständigen Analysekräfte verstärkt, um der gewachsenen Gefährdung durch gezielte Angriffe Rechnung zu tragen. Des Weiteren wurden die Austauschbeziehungen zu anderen Organisationen intensiviert, um schnell von den Erfahrungen anderer zu lernen und sich gemeinsam schützen zu können. Um auf einen Angriff reagieren zu können, wurden Technikerinnen und Techniker anderer Abteilungen in Prozessen und Maßnahmen geschult, um die Incident Response Kräfte bei Bedarf zu verstärken. Diese verstärkten Teams können bei Bedarf auch im Rahmen der Amtshilfe das Bundesamt für Sicherheit in der Informationstechnik (BSI) und andere Organisationen der Informationssicherheit unterstützen.

DIE GRÖSSTE SCHWACHSTELLE

Der ganze Artikel fokussierte auf Informationstechnik, vernetzte Systeme und Prozesse. Wir dürfen aber nicht die größte Schwachstelle im System außer Acht lassen: den Menschen. Ein Auftrag des ZCSBw ist Awareness und Sensibilisierung der Nutzenden. Diese führt nicht nur das dafür aufgestellte Sachgebiet durch. Wo immer Personal des ZCSBw heute tätig ist, versuchen wir ein Bewusstsein zu schaffen, dass Informationssicherheit kein Hemmschuh ist. Sie ist eine Notwendigkeit, die, richtig angewandt, das Durchführen des Auftrags garantiert und nicht verhindert. Ein Problem dabei ist sicherlich, allen zur Erkenntnis zu verhelfen, dass wir bereits heute unterbinden müssen, dass ein Gegner ein Wirkmittel für die Zukunft in unseren Netzen vorbereitet. Denn die Gegner im Cyberraum sind für den durchschnittlichen Nutzenden unsichtbar, können aber zeitverzugslos und über weite Entfernungen hinweg agieren. Sie liegen allerdings bereits jetzt auf der Lauer, um uns auszuspionieren und unsere Schwachstellen auszunutzen. Dies betrifft alle, egal ob Nutzer, Bereitsteller oder Überwacher der IT. Bleiben wir gemeinsam wachsam und resilient.

DIENSTSTELLEN-PROFIL

ZENTRUM FÜR GEOINFORMATIONSWESEN DER BUNDESWEHR

Das Zentrum ist die zentrale Facheinrichtung des Geoinformationsdienstes der Bundeswehr (GeoInfoDBw).

AUFGABEN

- Sicherstellung der GeoInfo-Unterstützung im Verbund mit dem GeoInfo-Personal weiterer Organisationsbereiche,
- Gewinnung von Erkenntnissen über Geofaktoren und Beurteilung hinsichtlich ihrer Auswirkungen auf die Operationsführung,
- Bereitstellung aktueller und qualitätsgesicherter Geoinformationen für die Bundeswehr,
- Geowissenschaftliche Forschung als Ressortforschungseinrichtung des Bundes.

AUFTRAG

Das Zentrum für Geoinformationswesen der Bundeswehr (ZGeoBw) untersteht dem Kommando Cyber- und Informationsraum. Der Leiter des Geoinformationsdienstes der Bundeswehr, gleichzeitig Kommandeur ZGeoBw, untersteht zusätzlich fachlich der Abteilung Cyber- und Informationstechnik im BMVg. Unter dem Motto „Geoinformationen aus einer Hand" stellt der GeoInfoDBw die Unterstützung für das gesamte Aufgabenspektrum der Bundeswehr sicher. Das ZGeoBw leistet hierzu einen wichtigen Anteil: Her- und Bereitstellen von Geoinformationen, GeoInfo-Datengewinnung, -Produktion sowie -Datenmanagement. Das ZGeoBw stellt dabei unter Einbeziehung von GeoInfo-Personal in weiteren Organisationsbereichen sicher, dass der Bundeswehr aktuelle und qualitätsgesicherte Geoinformationen, beispielsweise über Geofaktoren wie Klima, Gelände, Boden und Infrastruktur, zur Verfügung stehen.

Zur Bewertung von Geofaktoren sowie der interdisziplinären Beurteilung ihrer Auswirkungen nach Raum und Zeit sind im ZGeoBw alle Wissenschaftsdisziplinen des GeoInfoDBw vertreten. Das ZGeoBw leistet als Ressortforschungseinrichtung des Bundes durch die geowissenschaftliche Forschung einen wichtigen Beitrag an der Schnittstelle zwischen Wissenschaft und Politik. Mit dieser breitgefächerten Expertise kann eine umfassende GeoInfo-Beratung zu den vielseitigen Fragestellungen der Bedarfsträger erfolgen. Die Beratung umfasst die Bereiche Landeskunde, Geopolitik, Geologie, Biologie, Ökologie sowie Positionsbestimmung, Navigation und Zeitfestlegung, Meteorologie und Ozeanographie.

ANSCHRIFT
Mercator-Kaserne,
Frauenberger Straße 250,
53879 Euskirchen

DIENSTSTELLENLEITUNG
Brigadegeneral Dipl.-Ing. Peter Webert

STAMMPERSONAL
~1.000

AUFSTELLUNG
11.03.2003

IT Bataillon 383 aus Erfurt sorgt für die IT-Anbindung bei der NATO Großübung Trident-Juncture Ende 2018 in Norwegen.
Foto: Bundeswehr/ITBtl 383

GMN und NATO DCIS Firefly – Starke Synergien für die Division 2027?

Interview mit Rainer Klotz, Senior Business Development Manager C4I & Neue Technologien, Thales Deutschland

Herr Klotz, angesichts der derzeit angespannten globalen Sicherheitslage: Was ist aus Ihrer Sicht die wichtigste Fähigkeit, die eine deutsche milCloud mitbringen muss?

Eigentlich sind es zwei Kernfähigkeiten, die unabdingbar sind. Souveränität und Interoperabilität würde ich hier nennen wollen.

Mit Blick auf die Bündnisverteidigung muss eine vollständige, möglichst native NATO-Interoperabilität die Kernfähigkeit jeder milCloud sein. Dennoch muss gleichermaßen die deutsche Souveränität in einer solchen Cloud-Lösung gewährleistet sein.

Ja, wir werden im Verteidigungsfalle nicht alleine, sondern im Bündnis agieren. Dennoch gilt es sicherzustellen, dass nationale Interessen gewahrt bleiben.

Die NATO-Mitgliedstaaten weisen unterschiedliche Ausrüstungsgrade und Fähigkeitslevel auf. Kann man trotz dieser Unterschiede im Verbund mit der notwendigen Performance funktionieren?

Sie sprechen hier einen wichtigen Punkt an. Die NATO hat diese Unterschiede bereits erkannt und deshalb mit DCIS Firefly eine auf definierte Standards basierende, also damit nativ interoperable Basis für die Bündnispartner entwickelt, welche sich auch bereits in der Umsetzung befindet. Diese Basis kann dann von den Lead Nations, zu denen prominent auch Deutschland gehört, den weniger technologisierten Bündnispartnern komplett oder in Teilen zur Verfügung gestellt werden. So stellt man eine maximale Informationsüberlegenheit aller Partner sicher.

Sie sprechen davon, dass es sich bereits in der Umsetzung befindet. Gibt es bereits eine native NATO-Lösung auf dem Markt?

Das erfolgreiche Passieren des NATO DCIS Firefly Critical Design Review (CDR) sollte nicht mehr allzu lange dauern, also würde ich hier ja sagen, da nach dem CDR nur noch kleinere Anpassungen erfolgen werden. Diese stehen einer Erstbeschaffung für Trainingszwecke am Zielsystem und dem Aufbau der souveränen deutschen Anteile in der NATO-Lösung definitiv nicht im Wege und erlauben ein schnelles Vorankommen.

Speziell um seine eigenen Ambitionen für eine geplante Division 2027 entwicklungstechnisch risikolos und auf der Zeitachse schnell mit einer dann Nato-akkreditierten Systemlösung abzudecken, ist NATO DCIS Firefly als standardisierte Basis definitiv ein Mittel der Wahl.

Sie sprechen von einer standardisierten Basis – können Sie das näher erläutern?

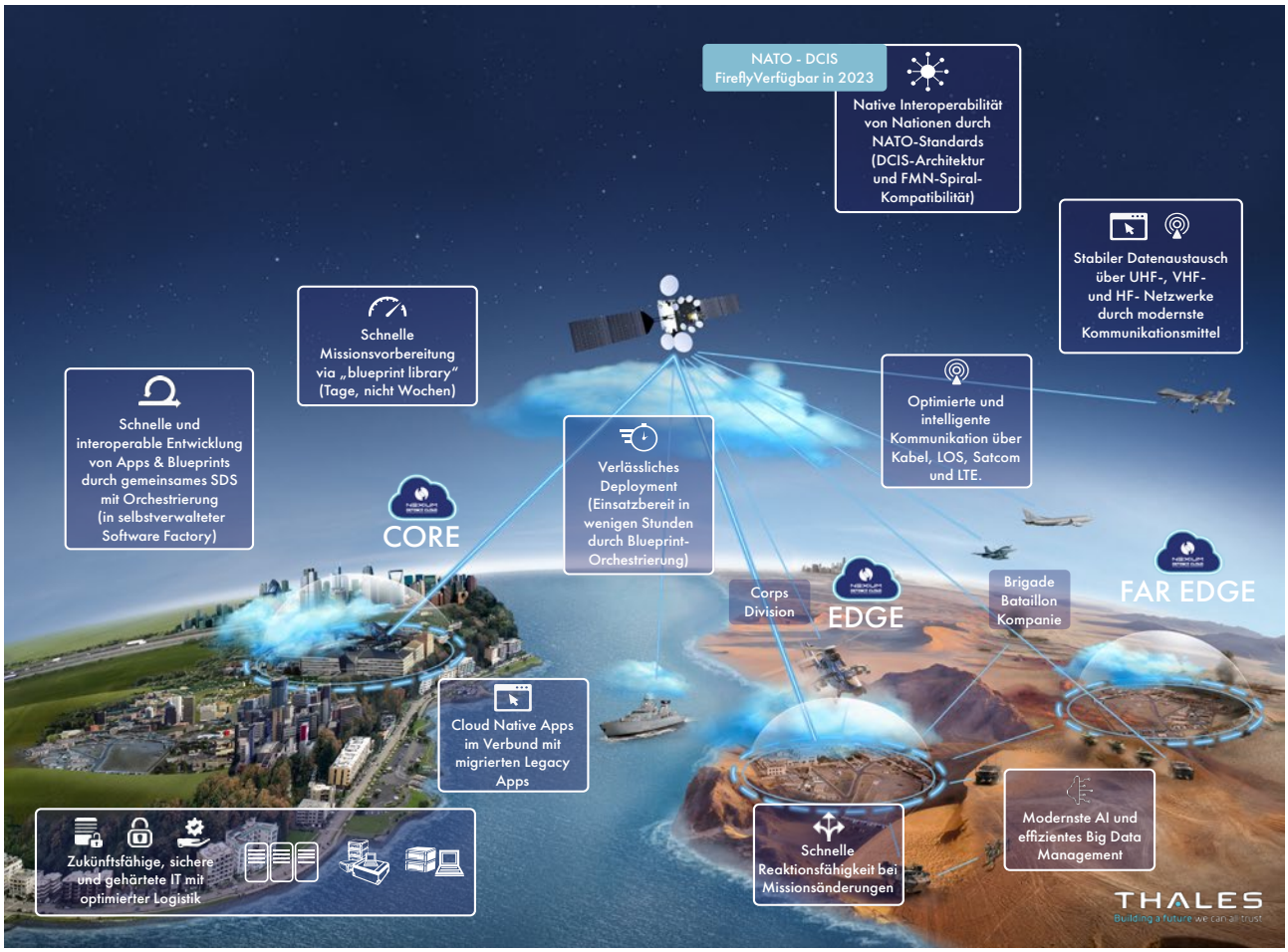
Es gibt für mich zwei Ansätze, um zu einer interoperablen Cloud-Lösung zu gelangen, jede mit architekturbedingten Vor- und Nachteilen.

Eine Lösung ist, die jeweils bestehenden Cloud-Ansätze der Nationen in einer übergeordneten Master-Cloud zu assimilieren, die dann von jeder Nation genutzt wird. Der Nachteil ist hierbei, dass die Geschwindigkeit einer solchen Lösung wahrscheinlich vom unperformantesten Anteil bestimmt wird. Die NATO setzt daher auf standardisierte Blueprints für Services, prominent würde ich hier z. B. die Verwendung des TOSCA-Standards nennen.

Diese Service Blueprints können über das NATO Software Defined Studio und dem Orchestrator der NATO im jeweiligen Land souverän, also eigenständig, aber mit 100%iger NATO-Interoperabilität erstellt werden. Das gewährleistet die dringend benötigte maximale Geschwindigkeit des Informationsaustausches in einem potentiellen Kampfeinsatz mit Partnernationen.

▶ NEXIUM Defence Cloud – Ziel ist die Informationsüberlegenheit der Partnernationen – unter nationaler Kontrolle der eingesetzten Technologie – von CORE bis FAR-EDGE über alle Domänen hinweg.
Foto/Grafik: Thales

ÜBER DEN INTERVIEW-PARTNER: Rainer Klotz, Senior Business Development Manager C4I & Neue Technologien, Thales Deutschland, ist seit den Anfängen der Service-orientierten Architekturen im Jahr 2010 mit „Einsatzunterstützender Systemverbund Aufklärung Führung Wirkung (EIS-A-F-W)" zuständig für Federated Mission Networks (FMN) und Cloud-basierende Systeme bei Thales Deutschland. U.a. war er bis 2018 zuständig für „Digitalisierung Landbasierter Operationen (D-LBO)" und bringt somit nicht nur eine große Expertise in FMN- und Interoperabilitäts-Fragen mit, sondern auch bezüglich deren Umsetzbarkeit auf den Transportmedien, wie z. B. Funk und Satcom bis in den hochmobilen Bereich.



In Deutschland gibt es bereits das Programm German MissionNetwork (GMN) zur Erlangung einer Cloud-Fähigkeit. Inwieweit passt das mit dem NATO DCIS zusammen? Was ist der Unterschied?

Von der Hardwareseite betrachtet liegt der Unterschied in der bei GMN geforderten Verbringung der IT-Komponenten in K3-beschussicheren Sheltern.

Der NATO-Ansatz in DCIS Firefly hingegen basiert auf der Verwendung von kleinen schnell verlegbaren Transportcontainern.

Außerdem hat die NATO derzeit höhere IT Performance-Anforderungen. Eine Integration der NATO DCIS Firefly IT Komponenten in K3-Shelter sehe ich als durchaus gut lösbare Aufgabe.

In der Software gilt wie bereits erwähnt Interoperabilität als höchstes Gut.

Die NATO gibt hier zwar sogenannte Spirals, also Standards, vor, dieses aber primär um sicherzustellen, dass sich nationale Umsetzungen nicht zu weit vom Kurs der NATO entfernen. Diese Spirals sind aber Standards mit ureigenen Grauzonen in der architekturellen Umsetzung. Entwicklungen angelehnt an NATO Spirals garantieren also nicht unbedingt eine „plug and play"-Fähigkeit wie oft angenommen. Es ist die architekturelle Umsetzung, die eine solche „plug and play"-Fähigkeit erzeugt. Ich bin überzeugt, dass dies aktuell nur über eine Verwendung von NATO DCIS Firefly als Basis allen weiteren Vorgehens, in einem mit der Division 2027 kompatiblen Zeithorizont, zu erreichen ist.

Können Sie dieses Vorgehen aus Ihrer Sicht beschreiben?

Aus der Helikopterperspektive betrachtet könnte folgendes Szenario zielführend sein:

1. Schnellstmögliche Beschaffung eines DCIS Firefly Trainingssystems in Hard- und Software, wie dieses derzeit von der NATO in Umsetzung ist.
2. Training des Nutzers auf diesem System hinsichtlich der Blueprinterstellung und der Orchestrierung.
3. Parallel dazu starten der Integrationsplanung von DCIS Firefly in die GMN-Shelter und Ausplanen der souverän zu erstellenden bzw. von GMN 1 auf DCIS Firefly umzusetzenden Anteile.
4. Gemeinsames Ausarbeiten und Definieren der Roadmap von der verlegbaren DCIS-Firefly-Lösung hin zu einer durchgängigen mobilen Lösung für die Division 2027.

Welches Vorgehen letztendlich auch immer gewählt wird, wir stehen als Unternehmen jederzeit bereit, unsere Partner bei ihrem Prozess hin zu einer souveränen interoperablen milCloud mit modernsten IT-Lösungen zu unterstützen. Unsere Lösungen sichern unseren Partnern dabei sowohl eine reibungslose Transformation von Legacy-Anwendungen, als auch die Integration von Next-Generation-Anwendungen zu, um eine flexible, belastbare und interoperable Infrastruktur innerhalb weniger Stunden genau dort, wo sie benötigt wird, verfügbar zu haben.

Das Interview führte Matthias Wunsch

AUTORENTEAM, REFERAT STRATEGIE,
ABTEILUNG PLANUNG CIR UND DIGITALISIERUNG DER BUNDESWEHR

VERSCHRÄNKUNG DER DIMENSIONEN – **MULTI DOMAIN OPERATIONS**

Mit der Digitalisierung wird in vielen Handlungsfeldern eine gewisse Entgrenzung geschaffen, so auch bei der Betrachtung von Dimensionen als militärisches und räumliches Ordnungsmittel. Die Idee der Verschränkung von Dimensionen entwickelt sich fortwährend und ist aktuell von dem Ausdruck „Multi Domain Operations" geprägt. Dieser Beitrag beantwortet die grundlegende Frage, ob neue Technologien Dimensionen überhaupt mehr und anders als früher verschränken und welches Potenzial technologiebasierte Ansätze bieten.

Dimensionen erlauben eine einfache Gliederung des gesamten Operationsraums in wenige handhabbare Elemente. Mit der Betrachtung nach Dimensionen folgt die Bundeswehr einer – auch in der NATO und der EU – etablierten Einteilung, in der jede Dimension durch besondere Merkmale gekennzeichnet ist. Neben die – nunmehr als „klassisch" bezeichneten – Dimensionen Land, Luft und See, treten als jüngste Dimensionen der Cyber- und Informationsraum (CIR) sowie der Weltraum hinzu. Alle Dimensionen beeinflussen mit ihren spezifischen Eigenschaften das operative Umfeld und damit auch den Einsatz militärischer Fähigkeiten. Die Operationsführung in jeder Dimension folgt der Idee des koordinierten Einsatzes militärischer Kräfte und Mittel auf taktischer Ebene unter einheitlicher Führung. Gleiches muss für die Operationsführung über Dimensionsgrenzen hinweg gelten.

Schon immer wurde Truppe im Sinne einer einheitlichen Einsatz- und Operationsführung von Streitkräften so vernetzt, dass sie im Verbund miteinander operieren kann. Dies gilt gleichermaßen für den Einsatz im nationalen wie im multinationalen Rahmen. Auf der taktischen Ebene wurden unterschiedliche Fähigkeiten stets zum Zwecke einer örtlichen Überlegenheit eingesetzt. Taktische Erfolge dienten damit in der Summe dazu, operative Effekte zu erzielen. Der zielgerichtete Ablauf einer Gesamtoperation und das gemeinsame Wirken von Fähigkeiten unterschiedlicher Dimensionen und Führungsebenen diente der Erreichung übergeordneter strategischer Ziele. Ein Beispiel hierfür ist die Luftnahunterstützung, die auf Basis eines Zusammenspiels der Dimensionen Land und Luft Erfolge erzielt und auch heute noch zum Gesamterfolg einer Operation beiträgt. Die Schaffung eines Verbundes ist damit nicht neu, wenngleich die Beschreibungen unterschiedlich sind, wie aktuelle Entwicklungen zeigen.

DIGITALISIERUNG BEWÄHRTER ANSÄTZE

Digitalisierung und technologische Entwicklungen verändern als treibende Größen moderner Streitkräfte auch die Operationsführung. Immer wieder entwickeln Streitkräfte darauf aufbauend verbesserte Konzepte zum flexibleren Zusammenwirken und einer erhöhten Interoperabilität. Die Bundeswehr sprach in diesem Zusammenhang lange Zeit vom Gefecht der verbundenen Waffen und folgend von der vernetzten Operationsführung, die als grundlegende Prinzipien auch heute nicht überholt sind. So wurde in der jüngsten Zeit, ohne nähere Beschreibung, unter anderem das „Gefecht der verbundenen Dimensionen" begrifflich weiterentwickelt oder aber man bediente sich der Bezeichnung „multidimensionale Operationen" – inklusive der englischsprachigen Übersetzung. Im militärischen Sprachgebrauch hat sich hier der Begriff Multi Domain Operations (MDO) etabliert, wobei weder international noch im Bündnis eindeutige Definitionen vorhanden sind und ein gemeinsames Verständnis noch nicht in Gänze entwickelt ist.

Wenngleich der Grundgedanke älter ist, so stehen im Zentrum der heutigen Diskussionen um MDO Überlegungen der US-amerikanischen Seite aus dem Jahr 2018. Diese fokussieren auf die Operationsführung und die Fähigkeiten von Landstreitkräften als einem Akteur im Rahmen von streitkräftegemeinsamen Operationen. Neben diesem Ansatz steht die Idee der Joint All Domain Operations (JADO), deren Ursprung in den US-amerikanischen Luftstreitkräften verortet ist und einen effizienteren Einsatz dieser über Dimensionsgrenzen hinweg beschreibt. Gedanklich setzt man sich bei MDO und JADO damit auseinander, wie einem Gegner auf Augenhöhe (peer-competitor) in allen Dimensionen begegnet werden kann. Absicht ist es, durch vielfache örtliche Überlegenheit auf Basis unmittelbarer, skalierbarer und dimensionsübergreifender Effekte, Dilemmata zu erzeugen, welche die gegnerische Entscheidungsfindung auf allen Ebenen vor große Herausforderungen stellen. Geschwindigkeit, Flexibilität, Qualität und Quantität der eigenen Operationsführung zielt darauf ab, den Gegner gezielt zu überfordern und den Erfolg der eigenen Operationsführung effizient herbeizuführen. Wenngleich die neusten Ideen zum dimensionsgemeinsamen Agieren auf den ersten Blick nicht anders erscheinen als bewährte Verfahren und auch die Literatur hierzu keine eindeutigen Antworten gibt, so steht dennoch im Zentrum der Betrachtung das Potenzial technischer und digitaler Entwicklungen, um gegen einen gleichwertigen Gegner zu bestehen.

EINFLÜSSE DER FORTSCHREITENDEN DIGITALISIERUNG AUF DIE OPERATIONSFÜHRUNG

Für den Erfolg in einer militärischen Auseinandersetzung ist eine räumliche Überlegenheit von Kräften unter Berücksichtigung der zeitlichen Verfügbarkeit ein zeitloser Grundsatz. Das Verhältnis der Faktoren Kräfte, Raum und Zeit zueinander kann dabei sehr unterschiedlich ausgeprägt sein. Ergänzt wurden diese klassischen Faktoren um den immer bedeutender gewordenen Faktor Information, der maßgeblich die Dynamik und den Ausgang von Gefechten und Operationen, bis hin zum gesamten Konflikt, bestimmt. Der Faktor Information steht auch im Kern der Betrachtung von MDO, JADO sowie weiteren dimensionsübergreifenden Ansätzen (z.B. dem britischen Begriff der Multi Domain Integration). Allen Überlegungen gemeinsam sind Lösungsansätze zur digitalen Verschränkung von Dimensionen sowie der dafür notwendigen Verbesserung der Informationsverarbeitung.

Die fortschreitende Digitalisierung und technologischen Entwicklungen verändern das militärische Denken und Handeln und beeinflussen militärische Fähigkeiten. Viele neue Technologien finden sich zuerst im Bereich der freien Wirt-

◀ Digitalisierung und technologische Entwicklungen verändern als treibende Größen moderner Streitkräfte auch die Operationsführung.
Foto: Bundeswehr/Stefan Uj

schaft oder bei Privatanwendern. Sie beeinflussen auch das sicherheitspolitische und prägen gleichzeitig das operative Umfeld. Wachsende Vernetzung vermehrt und intensiviert Wechselwirkungen zwischen vermeintlich getrennten Bereichen wie Dimensionen. Die Anpassung von Strukturen und Prozessen – im militärischen Bereich unter anderem durch die Schaffung neuer Dimensionen – war nur ein erforderlicher Anpassungsschritt, auch um dem Informationszeitalter umfassend Rechnung zu tragen. Die technologische Entgrenzung durch permanenten grenzüberschreitenden Austausch hat einen entscheidenden Einfluss auf das Zusammenspiel von Dimensionen. Besonders die jüngsten Dimensionen Cyber- und Informationsraum sowie Weltraum sind daten- und informationszentriert und bieten dem gemeinsamen Operieren vielfältige Möglichkeiten.

Streitkräfte müssen dimensionsübergreifend, schnell und flexibel Wirkung entfalten und im Einsatz bestehen können. Eine gemeinsame IT-Architektur, im Sinne eines umfassenden Informations- und Kommunikationsverbundes, ist das Kernstück einer gelungenen Verschränkung von Dimensionen. Die gemeinsame Leistungserbringung bedarf der Berücksichtigung technologischer Lösungen wie der Cloudtechnologie. Solche Lösungen bieten die Chance, technische Informationsräume kollaborativ nutzen und die Verfügbarkeit von Daten und Informationen optimieren zu können. Gleichzeitig ergeben sich hieraus Risiken, die eine weiterführende Informationssicherheit unabdingbar machen. Dies bedeutet auch die Gewährleistung einer sicheren und resilienten Übertragung sowie teilautomatisierten Verarbeitung und Bereitstellung aller für die Operationsführung erforderlichen Daten.

▲ Streitkräfte müssen dimensionsübergreifend, schnell und flexibel Wirkung entfalten und im Einsatz bestehen können.
Foto: Bundeswehr/Stefan Uj

DATENVERARBEITUNG ALS ZENTRALES ELEMENT VON MDO

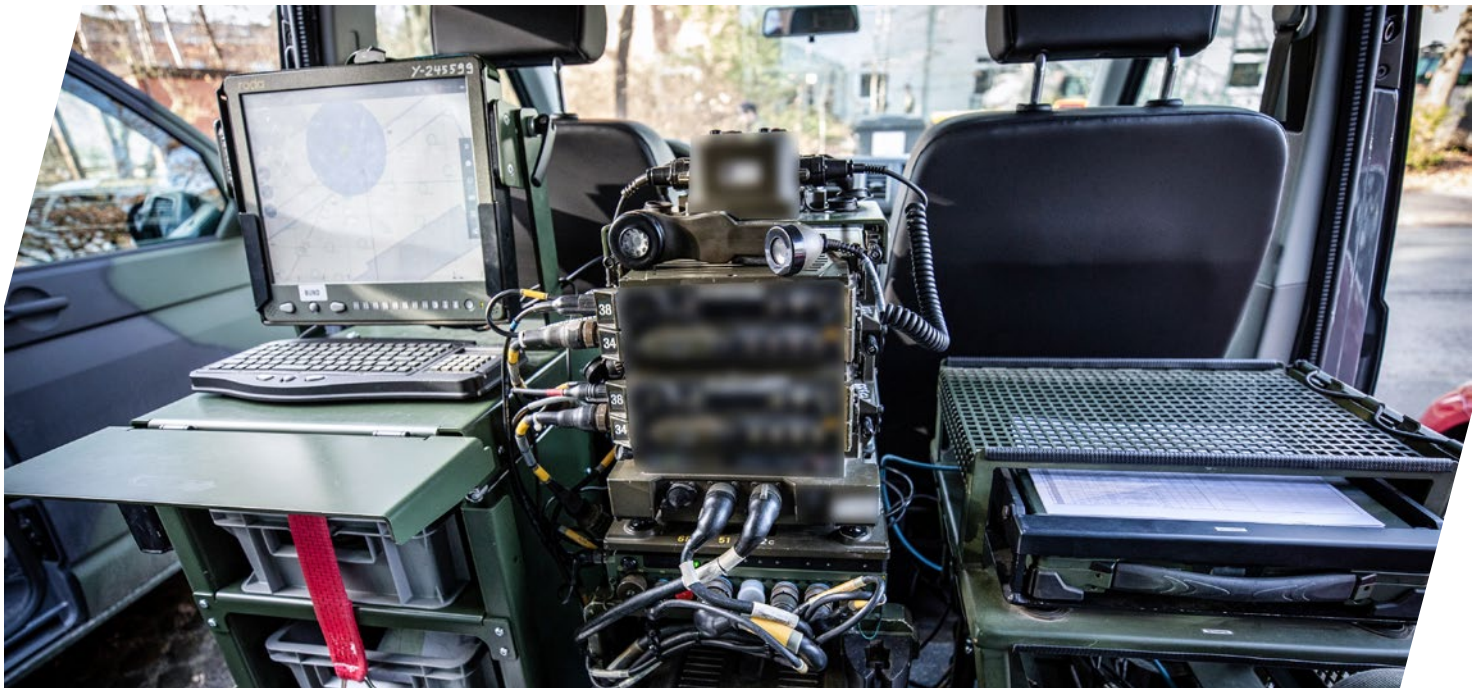
Weil Daten der Rohstoff sozialer und technologischer Entwicklungen sind und das zentrale Element für die Digitalisierung darstellen, sind sie Voraussetzung und auch eine Ressource für durchgängige militärische, IT-gestützte sowie automatisierte Prozesse. Im militärischen Bereich wird unter anderem moderne Software zur Unterstützung menschlicher Fähigkeiten im Rahmen der Auswertung von strukturierten und unstrukturierten Massendaten für die Erstellung eines gemeinsamen verifizierten Lagebildes verwendet. Dabei kommt Künstliche Intelligenz – in unterschiedlichen Ausprägungen wie Maschinelles Lernen und Deep Learning – zur Anwendung. Gleichermaßen gilt es, eine technologische Unterstützung menschlichen Handels auch auf die Optimierung der Speicherung, Validierung, Bereitstellung und Verteilung von Daten anzuwenden. Anforderungen verschiedenster Entitäten müssen stets berücksichtigt werden. Einzelne Elemente bilden auf dem Gefechtsfeld zusammengenommen eine geschlossene digitale Einheit, sowohl im Rahmen der Landes- und Bündnisverteidigung als auch im internationalen Krisenmanagement.

Die Geschwindigkeit der Entscheidungsfindung, aber auch die damit in Verbindung stehende Reaktionsschnelligkeit militärischer Akteure, erreicht insgesamt ein neues Niveau sowie eine unbekannte Dynamik.

Die zunehmende Geschwindigkeit der Informationsverbreitung, sowohl zwischen technischen Systemen als auch Menschen, verwischt Grenzen zwischen Führungsebenen und militärischen Dimensionen. Die Rolle von Staaten und Bündnissen im globalen Ringen um Macht ist auch von militärischen Handlungsoptionen abhängig. Die Annahme der permanenten Auseinandersetzung mit einem Gegner (engl. persistent competition bzw. competition continuum) ist aus strategischer Sicht entscheidender Gegenstand von MDO. Dies erfordert auf allen Ebenen die Anpassung von Fähigkeiten und Kompetenzen. Auch erwächst aus allen technologischen Entwicklungen und ihren Implikationen ein erheblicher Anpassungsdruck an die strategische Ebene, insbesondere hinsichtlich der Frage nach Verantwortlichkeiten.

Auf operativer Ebene erhöht sich das Operationstempo dadurch, dass taktische Operationen unterschiedlicher Dimensionen durch einen permanenten Datenaustausch synchronisiert angesetzt werden. Daraus erwächst ein ständiger Entscheidungsbedarf zur Priorisierung von Hochwertfähigkeiten insbesondere im Bereich der Aufklärung und Wirkung sowie deren Verbund (Sensor-to-Shooter). Komplexität und Dynamik des operativen Umfeldes münden in der Notwendigkeit, über limitierte Hochwertfähigkeiten verfügen zu müssen, die durch neue Waffen (z.B. Hyperschallwaffen) bedroht und potenziell durch aktive und passive Gegenmaßnahmen hinsichtlich ihrer Wirksamkeit eingeschränkt sind.

Auf der taktischen Ebene werden Streitkräfte durch das hohe Operationstempo, vielfältige Aufklärungsmittel des Gegners sowie ein breites Spektrum kinetischer und nichtkinetischer Wirkmittel herausgefordert. Um dem entgegenzuwirken, ist auf der taktischen Ebene im Zusammenwirken aller Dimensionen die Informationsüberlegenheit durch ein möglichst vollständiges und bewertetes Lagebild auf Grundlage einer umfassenden Datenbasis die Voraussetzung für Wirkungsüberlegenheit. Kräftedispositive, die verschiedene Fähigkeiten vereinen, sind auf der taktischen Ebene zu verorten. Der durch die Digitalisierung mögliche, nahezu verzugslose globale Informationsaustausch, die wachsende Bedeutung des Weltraums sowie die größere Reichweite verschiedenster Wirkmittel erfordern möglicherweise ein Umdenken mit Blick auf Verantwortlichkeiten auf und zwischen den Führungsebenen.



MASSGEBLICH NEUE QUALITÄT DER LEISTUNGSERBRINGUNG DER DIMENSIONEN

Die Herausforderung bei der Verschränkung von Dimensionen liegt neben der technischen Umsetzung auch in der Ausrichtung aller Beteiligten auf dasselbe operationelle Ziel. Erst wenn beides erfüllt ist, kann tatsächlich von MDO die Rede sein, einem möglichen Game Changer im Rahmen der Verbindung der realen und der digitalen Welt. Entscheidend sind die Stabilität und Resilienz einer intelligenten Vernetzung und Verknüpfung verschiedener Führungsebenen und Dimensionen, unabhängig vom beweglichen Einsatz einzelner Truppenteile, dezentralen verlegefähigen oder zentralen stationären Einrichtungen.

Die digitale Transformation ist Schlüsselelement für die Zukunftsfähigkeit der Streitkräfte und schafft eine technische Annäherung der Dimensionen aneinander. Hier wird auch gerne der Begriff der Konvergenz (engl. convergence), also einer Art Annäherung, als Ziel formuliert. MDO ist nicht als technisches System zu verstehen, sondern als eine neue Beschreibung bewährten militärischen Handelns, das durch IT-Unterstützung einen besonderen Qualitätsgewinn erfährt. Die aus operationeller und technischer Sicht notwendige Verschränkung der Dimensionen, über unterschiedliche Führungsebenen hinweg, beginnt bereits tief auf der taktischen Ebene. Dies könnte man als neue Qualität im Vergleich zu Joint Operations, welche die operative Ebene in den Blick nehmen, begreifen. Im Kern geht es um einen schnelleren und flexibleren Rückgriff auf Fähigkeiten, die unmittelbar zum Erfolg einer Operation beitragen.

MDO suchen nach mehr als nur einer lokalen Möglichkeit, einem Gegner mit eigenen Fähigkeiten zu begegnen. Perspektivisch ist – zur weiteren Effizienzsteigerung – auch ein gesamtstaatlicher Ansatz denkbar, der nationale und multinationale sowie nicht-militärische Beiträge mit militärischen verbindet, um in einem permanenten Kräftemessen, auch unterhalb der Schwelle bewaffneter militärischer Auseinandersetzung, bestehen zu können. Im Vordergrund bleibt das Entfalten von Wirkung als bewährtes Ziel der Streitkräfte bestehen, jedoch mit erhöhter Effizienz. Eine Herausforderung bleibt das Zusammenspiel der klassischen mit den jüngsten informationszentrierten Dimensionen. Es wird darauf ankommen, die technologischen Hilfsmittel, die die Führung im Informationszeitalter unterstützen können, optimal auszunutzen. Dazu ist es erforderlich, Anpassungen von gewohnten Verfahren zuzulassen und zu erkennen, dass es wenig sinnvoll ist, lediglich auf schnellere Prozesse und kürzere Wege hinwirken zu wollen. Die digitale Verschränkung von Dimensionen ist ein wichtiger Schritt, der die Möglichkeit bietet, schneller, flexibler und adaptierbarer, in jedem Falle aber im Verbund der Dimensionen, agieren zu können.

▲ Die Herausforderung bei der Verschränkung von Dimensionen liegt neben der technischen Umsetzung auch in der Ausrichtung aller Beteiligten auf dasselbe operationelle Ziel.

◀ Erprobung des Battle Management Systems (BMS), dem neuen digitalen Führungssystem für landbasierte Operationen. Die Soldatinnen und Soldaten des Cyber- und Informationsraums sind als IT-Profis verantwortlich für die Implementierung, Testung und Weiterentwicklung der Software.
Fotos: Bundeswehr/Stefan Uj

FÜHREN UND KOMMUNIZIEREN MIT DEN SYSTEMLÖSUNGEN DER ATM

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

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

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

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

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

▲ Die ATM KommServer sind in verschiedenen Bauformen in der Bundeswehr eingeführt, u.a. als COMSEC oder Manpack-Variante.
Fotos: ATM ComputerSysteme GmbH

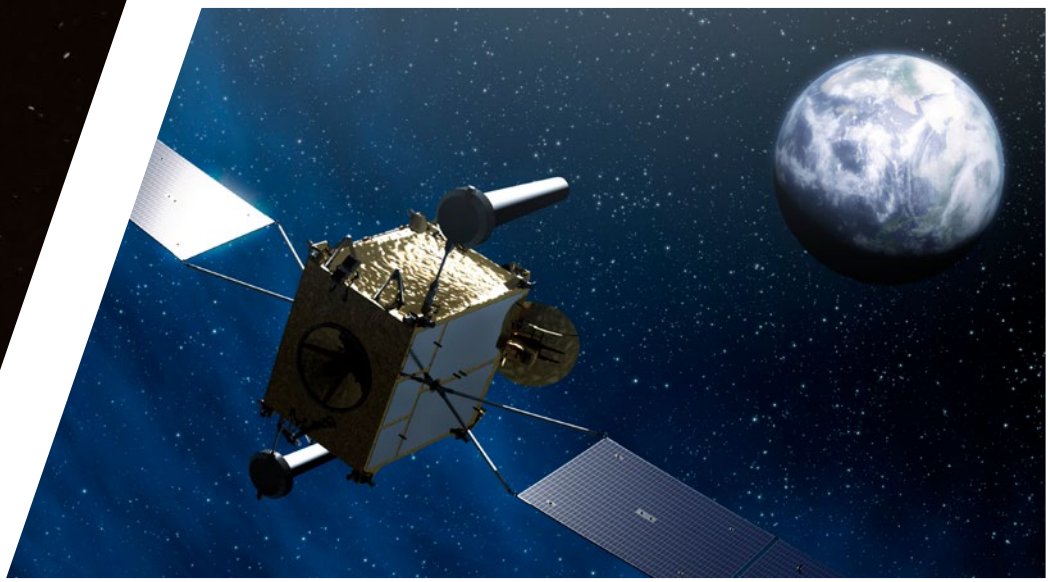
ATM Tec-Knowledge®

KONTAKT:
ATM ComputerSysteme GmbH
Tel. +49 7531 80 83
info@atm-computer.de
www.atm-computer.de

MAJOR I.G. ISABELLA SZROETER,
REFERENTIN ELEKTRONISCHER KAMPF UND MILITÄRISCHES NACHRICHTENWESEN,
REFERAT STRATEGIE, ABTEILUNG PLANUNG CIR UND DIGITALISIERUNG DER BUNDESWEHR

DIE ROLLE DES WELTRAUMS FÜR DIE DIMENSION CYBER- UND INFORMATIONSRAUM

◀ Abb.: pixabay/qimono



▼ Die Abhängigkeiten von weltraumgestützten militärischen Fähigkeiten lassen vielfältige Verschränkungen in unterschiedlichen Handlungsfeldern erahnen. Die Nutzung des Weltraums ist eine wesentliche Voraussetzung für den gezielten Einsatz moderner Streitkräfte.
Abb.: EADS Astrium

Moderne Gesellschaften sind von der freien und friedlichen Nutzung des Weltraums und weltraumbasierten Diensten und Produkten stark abhängig. Unzählbar viele Informationen werden über weltraumgestützte Verbindungen ausgetauscht. Ihre verlässliche Funktion ist ausschlaggebend für ein stabiles Bankenwesen, für die Satellitennavigation und eine ortsunabhängige mobile Kommunikation. Verlässlichkeit und Verfügbarkeit gerade der beiden letztgenannten Funktionen ist für Erhalt und Beschleunigung militärischen Handelns von großer Bedeutung.

Warum ohne eine militärische Nutzung des Weltraums schon heute Wirkungsmöglichkeiten der Bundeswehr stark eingeschränkt wären und in welchem Verhältnis der Weltraum und die Dimension Cyber- und Informationsraum (CIR) zueinander stehen, sind zentrale Fragestellungen, denen dieser Beitrag nachgeht.

WELTRAUMNUTZUNG – BEDEUTUNG FÜR DIE STREITKRÄFTE UND GRUNDLAGE MILITÄRISCHEN HANDELNS

Das militärische Ziel, Wirkung zu entfalten, zwingt Streitkräfte im Rahmen der Digitalisierung und des Technologietrends zur umfassenden Nutzung weltraumgestützter Fähigkeiten. Diese sind nicht zuletzt zentraler Schlüssel für die militärische Einsatz- und Wirkfähigkeit. Deutlich wird dies unter anderem daran, dass Streitkräfte im Grundbetrieb und in allen Szenarien vom Internationalen Krisenmanagement bis zur Landes- und Bündnisverteidigung in Operationen aller Intensitäten die Führung ihrer Kräfte über große Entfernungen sicherstellen müssen. Eine Kommunikation über Satelliten ist daher unverzichtbar. Darüber hinaus verfügen die Streitkräfte mit den weltraumgestützten Fähigkeiten zur Positionsbestimmung, Navigation und Zeitfestlegung über unerlässliche Möglichkeiten, um zum Schutz und zur Sicherheit ihrer Kräfte beizutragen. Auch trägt die satellitengestützte Aufklärung ohne hoheitliche Grenzverletzung weltweit und flexibel wesentlich zur Erstellung von Lagebildern bei, um die Truppe im Einsatz bis hinab zur taktischen Ebene zu unterstützen. Zeitgleich liefert sie Beiträge zur Krisenfrüherkennung auf strategischer Ebene. Mit ihrem signifikanten Beitrag zur Operationsführung tragen die obigen Fähigkeiten zur Wirkung bei. Die Abhängigkeiten von weltraumgestützten militärischen Fähigkeiten lassen vielfältige Verschränkungen in unterschiedlichen Handlungsfeldern erahnen. Die Nutzung des Weltraums ist eine wesentliche Voraussetzung für den gezielten Einsatz moderner Streitkräfte.

Die Bundeswehr hat mit dem Organisationsbereich CIR den zentralen militärischen Nutzer des Weltraums etabliert, der konkrete Handlungslinien zur Unterstützung von Einsätzen und Aufgaben der Bundeswehr verfolgt. In diesem Rahmen leisten weltraumgestützte Systeme einen wesentlichen Beitrag zur Informations- und Wirkungsüberlegenheit im dimensionsübergreifenden Zusammenwirken. Durch eine enge

Zusammenarbeit des Organisationsbereichs CIR mit dem in der Bundeswehr aufgestellten und im Organisationbereich Luftwaffe verorteten Weltraumkommando der Bundeswehr erfolgt eine koordinierte und auf militärische Bedarfe ausgerichtete Nutzung des Weltraums.

DER ORGANISATIONSBEREICH CYBER- UND INFORMATIONSRAUM ALS NUTZER IM WELTRAUM

Im militärischen System der Dimensionen hat der Weltraum eine besondere Bedeutung und ist eng verschränkt mit der Dimension CIR. Die Weltraumnutzung ist ohne das elektromagnetische Spektrum und die Abstützung auf den Cyberraum nicht möglich. Der Weltraum ist der physische Raum, in dem Hardware des elektromagnetischen Umfelds und des Cyberraums in Form von Satelliten und deren funktionaler Nutzlast positioniert ist. Die Bundeswehr unterscheidet zwischen Weltraumoperationen (Space Operations) und der Einsatzunterstützung aus dem Weltraum (Space Support to Operations). Beide ordnet sie der Dauereinsatzaufgabe Weltraumnutzung zu. In der Bundeswehr ist der Organisationsbereich CIR für die Einsatzunterstützung aus dem Weltraum zuständig. Dies umfasst unter anderem die Bereitstellung von Satellitenkommunikation, weltweiter Aufklärung, Positionsbestimmung, Navigation und Zeitfestlegung, Erdbeobachtung und Wetterbeobachtung als Beitrag zur Operationsführung und Entscheidungsfindung auf allen Ebenen. Das, im Organisationsbereich Luftwaffe verortete, Weltraumkommando der Bundeswehr nimmt hier eine koordinierende Rolle ein.

WELTRAUMSICHERHEIT AUS DER DIMENSION CIR HERAUS

Im Rahmen ihres Einsatzes unterliegen weltraumgestützte Fähigkeiten unterschiedlichen Bedrohungen. In militärischen Konflikten sind sie dem Wirken eines gleichwertigen Gegners im und in den Weltraum ausgesetzt. Weltraumsysteme können jedoch auch am Boden der Wirkung aus anderen Dimensionen ausgesetzt werden. Die Vektoren der Wirkmittel sind vielfältig, denn die Verwundbarkeit der Weltraumnutzung liegt im Gesamtsystem aus Raum-, Link- und Bodensegment. Wird im Rahmen eines gegnerischen Angriffs die Nutzbarkeit des Weltraums eingeschränkt, führt dies zu unmittelbaren und signifikanten Konsequenzen bis hin zum Verlust der staatlichen Ordnung. Daraus abgeleitet ist der Schutz von Weltrauminfrastrukturen, insbesondere in einem von hybridem Vorgehen bedrohten Umfeld, erforderlich. Cyberoperationen gegen jene Weltrauminfrastrukturen oder das Stören der Nutzung des elektromagnetischen Spektrums können praktikable Mittel für einen potentiellen Aggressor sein, dies auch unterhalb der Schwelle eines bewaffneten Angriffs.

Fähigkeiten des Organisationsbereichs CIR sind grundsätzlich in der Lage, gegen verschiedene Bedrohungen von Weltraumsystemen zu wirken. Vor allem reversible und nicht-kinetische Maßnahmen gegen gegnerische Raumsegmente sind hier gefordert, um der politischen Zielsetzung der Vermeidung von Weltraumschrott (Debris) zu entsprechen. Es ist, soweit möglich, von Maßnahmen abzusehen, die gegnerische Satelliten zu einer potentiellen Gefahr für die friedliche Nutzung des Weltraums werden lassen. Nach derzeitiger Vorstellung kommen Elektromagnetische Operationen und Cyberoperationen als Fähigkeiten der Dimension CIR in Betracht, um einem Gegner die Nutzung des Weltraums zu verwehren oder diese einzuschränken. Als Träger des nicht-waffensystemspezifischen Elektronischen Kampfes – und damit auch in der Zuständigkeit für Elektromagnetische Operationen – fallen nicht-kinetische Wirkfähigkeiten gegen Weltrauminfrastrukturen in die Dimensionsverantwortung des Organisationsbereichs CIR.

Nicht nur die Resilienz militärischer Weltraumfähigkeiten oder die Abwehr von Bedrohungen, sondern ganz besonders auch die Resilienz der Operation als solches hängen vom richtigen Verständnis des Weltraums und dem unmittelbaren Zusammenhang mit der Dimension CIR ab. Der Organisationsbereich CIR hat ein eindeutiges Interesse an der Sicherheit von Satelliten, von denen seine militärische Leistungserbringung abhängt. Daher ist eine widerstandsfähige Ausgestaltung der militärischen Nutzung des Weltraums von erheblicher Bedeutung, zumal davon auszugehen ist, dass Systeme zur Einsatzunterstützung aus dem Weltraum ein priorisiertes Ziel potentieller Gegner darstellen. Die Weltraumnutzung ist ohne die Dimension CIR nicht möglich. Gleichzeitig ist die Leistungserbringung des Organisationsbereichs CIR auf den Weltraum angewiesen. Weltraum und Cyber- und Informationsraum sind untrennbar miteinander verwoben.

◀ Weltraumstart SARah am 18. Juni 2022:
Die mehrstufige Trägerrakete „Falcon 9“ bringt den ersten von insgesamt drei SARah-Satelliten in seine Umlaufbahn.
Foto: SpaceX

DIENSTSTELLEN-PROFIL

SCHULE INFORMATIONSTECHNIK DER BUNDESWEHR

Die Schule Informationstechnik der Bundeswehr ist die zentrale militärische Ausbildungseinrichtung für die bundeswehrgemeinsame, trainingsgebundene, einsatz- und bedarfsorientierte Aus-, Fort- und Weiterbildung von Führungsunterstützungs- sowie des IT-Fach- und Funktionspersonals der Bundeswehr.

AUFGABEN

- Regenerationsausbildung des IT-/Führungsunterstützungs-, Fach- und Funktionspersonals (IT-Fachkräfte) der Bundeswehr.
- Militärfachliche IT-/Führungsunterstützungsaus-, -fort- und -weiterbildung für Angehörige der Bundeswehr.
- Fort- und Weiterbildung von zivilen IT-Fachkräften der Bundeswehr und militärischem Fachpersonal mit IT-lastigen Fachaufgaben.

AUFTRAG

Soldatinnen und Soldaten aller Teilstreitkräfte und Organisationsbereiche lernen an der Schule Informationstechnik der Bundeswehr (ITSBw), selbstständig komplexe Netzwerke und Kommunikationssysteme zu konfigurieren, zu administrieren und für den Einsatz zu betreiben. Das Angebot reicht von einwöchigen Grundkursen über mehrmonatige und hochspezialisierte Trainings bis hin zur staatlich anerkannten zweijährigen Berufsausbildung.

Daneben erfolgt Aus-, Fort- und Weiterbildung in organisationsbereichsspezifischen Trainings nach fachlichen Vorgaben des verantwortlichen Organisationsbereichs. Die erfolgreiche Individualausbildung der IT-Fachkräfte ist der Abholpunkt für die sich anschließende Teamausbildung, die grundsätzlich außerhalb der ITSBw erfolgt.

Die Absolventinnen und Absolventen können ihre an der Schule erworbenen Abschlüsse teilweise auch zivil zertifizieren lassen. Mit rund 6.000 Absolventinnen und Absolventen im Jahr ist die ITSBw eine der größten Schulen in der Bundeswehr.

ANSCHRIFT
General-Fellgiebel-Kaserne,
Maxhofstraße 1,
82343 Pöcking

DIENSTSTELLENLEITUNG
Brigadegeneral Rainer Simon

STAMMPERSONAL
~750

AUFSTELLUNG
24.06.1956

OBERSTLEUTNANT RÜDIGER WEBNER, DEZERNATSLEITER INFORMATIONSÜBERTRAGUNG,
BETRIEBSZENTRUM IT-SYSTEM DER BUNDESWEHR (BITS)

EINSATZUNTERSTÜTZUNG AUS DEM WELTRAUM

Betrieb des Gesamtsystemverbundes Satellitenkommunikation der Bundeswehr (SATCOMBw)

Satellitenkommunikation ist ein unerlässlicher Baustein der weitreichenden Informationsübertragung im gesamten Aufgabenspektrum der Streitkräfte. Besondere Bedeutung hat dabei die Autarkie der Bundeswehr über die Kommunikationsinfrastruktur, um sich ändernden Erfordernissen jederzeit schnell und souverän begegnen zu können.

Die Fähigkeit der Bundeswehr zur Satellitenkommunikation hat sich seit 1993 stetig weiterentwickelt. Es gab erste Miet- und Kauflösungen für den Somalia-Einsatz und Erweiterungen dieser Lösung während der Einsätze auf dem Balkan und in Afghanistan. 2009 und 2010 erfolgten die Starts der heute genutzten eigenen militärischen Satelliten COMSATBw-1 und 2 und die Übernahme der Betriebsverantwortung durch die Streitkräfte.

Die Satellitenkommunikation ist eine wesentliche Säule der weitreichenden Anbindung und Vernetzung der Streitkräfte, und zwar aufgrund der hohen Flexibilität, der sehr schnellen Aufbauzeit und der nahezu weltweiten Verfügbarkeit. Wie wichtig Satellitenverbindungen zur Reaktion auf sicherheitspolitische Herausforderungen und Naturkatastrophen sind, zeigte sich im Sommer 2021 eindrucksvoll. So mussten im Rahmen der Evakuierungsoperation in Afghanistan in kürzester Zeit sichere Sprach- und Datenverbindungen – was Vertraulichkeit, Verfügbarkeit und Integrität betrifft – zwischen dem Einsatzführungskommando der Bundeswehr in Potsdam und den Einsatzkräften in Kabul und Taschkent bereitgestellt

Die Satellitenkommunikation ist eine wesentliche Säule der weitreichenden Anbindung und Vernetzung der Streitkräfte.
Foto: Bundeswehr/Martina Pump

TESAT

15 YEARS SPACE CERTIFIED
TESAT-SPACECOM
LASER COMMUNICATIONS

STÖRFEST. ABHÖRSICHER. LEISTUNGSSTARK.

OPTISCHE KOMMUNIKATION VOM WELTMARKTFÜHRER. MADE IN GERMANY.

LCT 135 (LASER COMMUNICATION TERMINAL) – ERPROBTE TECHNOLOGIE, SOFORT EINSATZBEREIT:

- Kohärente 1.064 nm Technologie
- Monatlich 1.000 optische Links; insgesamt über 70.000
- Multi-Mission: GEO-GEO Backbone & GEO-LEO zur Anbindung von Erdbeobachtung in Echtzeit
- Seit 2008 auf NFIRE und TerraSAR
- Seit 2013 auf Alphasat
- Seit 2016 im kommerziellen Einsatz (z.B. EDRS)

Tesat-Spacecom GmbH & Co. KG
Gerberstr. 49 | 71522 Backnang | Germany | laser@tesat.de | www.tesat.de

werden. Auch der Starkregen im Juli 2021, der in Teilen von Rheinland-Pfalz und Nordrhein-Westfalen zu großflächigen und langwierigen Stromausfällen, massiven Zerstörungen und Beschädigungen der terrestrischen Telekommunikationsinfrastruktur führte, zeigte schonungslos die Anfälligkeit derselben. Allein bei der Telekom fielen im Verlauf des Unwetters 300 Mobilfunkstationen aus. Auch hier wurde erfolgreich und lange Zeit auf Satelliten zur Notfallkommunikation zurückgegriffen.

ARCHITEKTUR

Ein Satellitenkommunikationssystem besteht grundsätzlich aus mindestens einem Satelliten und zwei Bodenstationen. Eine Bodenstation, beispielsweise in Deutschland, sendet ein Signal an den Satelliten. Dieser verstärkt das ankommende schwache Signal, denn mit steigender Entfernung nimmt die Signalleistung quadratisch ab, und sendet es zu einer anderen Bodenstation, etwa in Mali, weiter. Dabei kreisen Satelliten in einem bestimmten Abstand zur Erde auf kreisförmigen oder elliptischen Bahnen, den Orbits. Es gibt zwei Ausprägungen:

Einerseits kreisen geostationäre Satelliten (Geostationary Earth Orbit, GEO) in einer Höhe von 36.000 Kilometern im Einklang mit der Erdrotation und stehen damit nahezu fest direkt über dem Äquator. Mit drei geostationären Satelliten kann die gesamte Erde mit Ausnahme der Polregionen abgedeckt werden. Die Antennen der Bodenstation müssen nur einmalig ausgerichtet werden. Nachteilig ist die große Entfernung, was zu hohen Signallaufzeiten (Latenzen) führt und hohe Sendeleistungen erfordert.

Andererseits können Satelliten auf niedrigeren Umlaufbahnen, wie Low Earth Orbit (LEO), Medium Earth Orbit (MEO) und High Elliptical Orbit (HEO), nahezu jeden Standort auf der Erdoberfläche mit wenig Sendeleistung ausleuchten. Hierfür wird jedoch eine große Anzahl an Satelliten und ein aufwendiges Management benötigt.

Die Bundeswehr verfügt über zwei eigene geostationäre Telekommunikationssatelliten COMSATBw-1 und COMSATBw-2 mit für die militärische Nutzung reservierten Satellitenfrequenzbändern (P- und X-Band). Darüber hinaus sind dauerhaft kommerzielle Kapazitäten im C- und Ku-Band auf Intelsat-Satelliten zur Abdeckung des Hauptinteressengebietes Europa, Afrika, Asien, Mittelmeer, Atlantischer und Indischer Ozean angemietet. Bei mobilen Operationen und zur Anbindung abgesetzter Kräfte wird zusätzlich auf das zivile Inmarsat- und Iridium-Satellitennetzwerk im L-Band zurückgegriffen. Diese Vielfalt reduziert Risiken wie Störungen, Ausfälle oder Schadensereignisse und erhöht Fähigkeiten wie Abdeckung, Frequenzbänder und Redundanzen. Der Regelflugbetrieb der Bundeswehrsatelliten erfolgt durch das Deutsche Zentrum für Luft- und Raumfahrt im Auftrag des Generalauftragnehmers Airbus.

▶ Nutzung geostationärer Satelliten durch die Bundeswehr.
Grafik: Bundeswehr/PIZ CIR

Zur Ankerung der breitbandigen, strategischen Satellitenfunkverbindungen betreibt das Betriebszentrum IT-System der Bundeswehr (BITS) die ortsfesten, militärischen großen Bodenstationen in Gerolstein und Kastellaun. Darüber hinaus führt das BITS die zivile Bodenstation in Weilheim betrieblich. Alle drei Erdfunkstellen sind über ein Hochgeschwindigkeits-Glasfasernetz ringförmig angebunden und bilden das Bindeglied zwischen der IT der Streitkräfte und der BWI. Das Personal der großen Bodenstationen betreibt, überwacht, steuert und entstört die Satellitenverbindungen im durchgängigen Schichtbetrieb.

Neben den ortsfesten Bodenstationen nutzt die Bundeswehr eine Vielzahl von verlegefähigen (z.B. Bodenstation mittel Multiband handelsüblich), tragbaren (z.B. PRC-117F/G) und mobilen (z.B. BGAN Explorer 727) Varianten von Bodenstationen, um die Nutzer am Einsatzort anzubinden.

Das „Herzstück" des Gesamtsystems SATCOMBw bildet das Führungs- und Kontrollelement mit der zentralen Managementinstanz im BITS in Rheinbach. Hier erfolgt die Planung, Befehlsgebung, Steuerung und Überwachung aller Funktionen, einschließlich der Telekommunikationsnutzlast. Eine speziell entwickelte Software unterstützt dabei das Personal. Für die Managementkommunikation steht ein autarkes und geschütztes Netz mit terrestrischen und satellitengestützten Übertragungsanteilen zur Verfügung.

BEREITSTELLUNGSPROZESS

Ausgehend von einer Nutzerforderung erfolgt im BITS in Rheinbach die hochkomplexe Planung, Realisierung, Überwachung und Unterstützung aller Satellitenverbindungen für Auslandseinsätze, Einsatzgleiche Verpflichtungen und Übungen zu Lande sowie auf See.

Das Einsatzspektrum einer Satellitenkommunikation ist sehr vielfältig und reicht von einzelnen Direktverbindungen zwischen zwei Stationen bis hin zu vermaschten Verbindungen bestehend aus mehreren aktiven Teilnehmern. Die Planer müssen viele Parameter unter Einhaltung verschiedener technischer, organisatorischer und regulatorischer Randbedingungen optimieren, um zum bestmöglichen und dabei oft einzig umsetzbaren Ergebnis zu gelangen. Solche Faktoren sind etwa geographische Position, Wetter, Modemtechnologie, Frequenzen, Codierung oder Leistung. In jedem Fall muss eine individuelle Netzplanung erfolgen. Denn das IT-System der Bundeswehr besteht aus einer Vielzahl miteinander vernetzter IT-Komponenten und -Systemen sowie infrastrukturellen Elementen, bereitgestellt von unterschiedlichen militärischen und zivilen Providern.

Die anschließende Realisierung erfolgt schrittweise in direkter Absprache zwischen BITS, Ankerstation sowie dem Administrationspersonal der Satellitenstation am Einsatzort und wird durch Messungen kontinuierlich überwacht. Nach einer abschließenden Abnahmemessung erfolgt die Überwachung, der First-Level-Support und etwaige einfache Störungsbeseitigungen durch das Network Operations Centre Basis Inland in Rheinbach (siehe auch Seite 86). Darüber hinaus unterstützt das BITS die Nutzer durch einen Second-Level-Support, die dauerhafte Softwarepflege und -änderung, bei der erweiterten Funktionsprüfung von Satellitenstationen sowie bei logistischen Prozessen.

Neben der durchgängigen Bereitstellung der Satellitenverbindungen für die mandatierten Auslandseinsätze werden insgesamt über 500 Nutzerforderungen im Jahr erfüllt. Zudem unterstützt das BITS die Weiterentwicklung SATCOMBw im Schulterschluss mit dem Kommando CIR, dem Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr und der Industrie.

AUSBLICK

Gegenwärtig finden umfangreiche Regenerations- und Migrationsmaßnahmen im Projekt SATCOMBw unter Aufrechterhaltung des laufenden Betriebs statt. Hierbei wird die Hardware in den verlegefähigen Bodenstationen und Ausbildungsanlagen teilweise modernisiert, die Antennenfelder der großen Bodenstationen in Gerolstein und Kastellaun erweitert sowie neue Betriebsgebäude gebaut. In den Jahren 2024 bis 2028 ist eine schrittweise Regeneration aller Bodenstationen vorgesehen.

Daneben beteiligt sich das Verteidigungsministerium an der Satellitenmission Heinrich Hertz (H2Sat). Der 2023 vorgesehene Start des deutschen Satelliten wird neben der Bereitstellung von klassischen Frequenzen zusätzlich den Einstieg in neue, zukunftsweisende Frequenzbereiche (Ka-Band) mit hohen Datenübertragungsraten für zeitkritische Informationssysteme, Bilder oder Livevideos zu mobilen Endnutzern, beispielsweise Fahrzeuge oder Schiffe, ermöglichen.

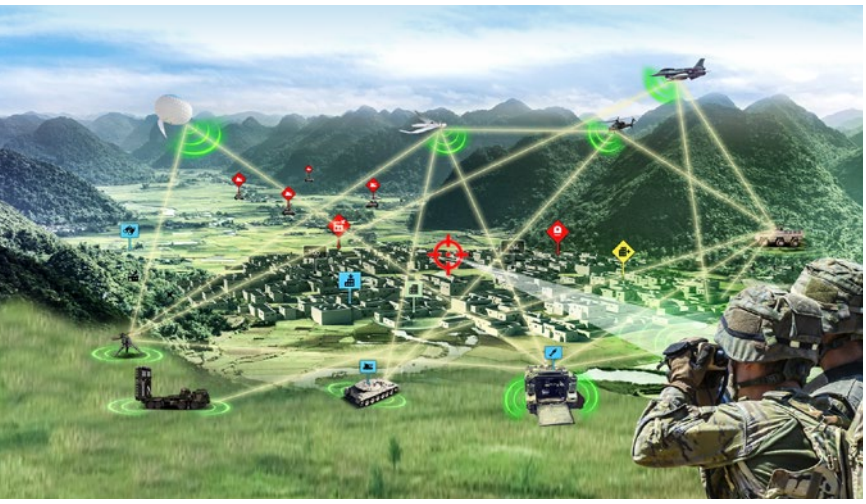
Die beiden Satelliten der Bundeswehr werden am Ende der vereinbarten vertraglichen Laufzeit von 15 Jahren voraussichtlich noch bis 2028/2029 zur Verfügung stehen. Dabei ist absehbar, dass die Technik durch Alterung schrittweise Einschränkungen mit sich bringen wird. Der Ersatz der beiden bundeswehreigenen Satelliten mit Fähigkeitsaufwuchs, unter anderem bei den Übertragungsraten, ist daher für 2028/2029 geplant. Ohne eine zeitnahe Nachfolgelösung, die am aktuellen Stand der Technik ausgerichtet ist, droht ein massiver und langfristiger Fähigkeitsverlust, zum Beispiel der Verlust der Orbit-Position. Dabei ist die Autonomie über die Führungsmittel unerlässlich.

ZUSAMMENFASSUNG

Ohne Satellitenkommunikation ist der Einsatz von Soldaten und Soldatinnen heute nicht mehr denkbar. Das BITS hat sich seit über einem Jahrzehnt der Bereitstellung von Satellitenkommunikation den Ruf eines erfahrenen, verlässlichen und kompetenten Partners für die Führungsfähigkeit der Streitkräfte erworben. Auch in Zukunft wird das BITS seinen Beitrag leisten und die digitalen Veränderungen aktiv mitgestalten.

Gegenwärtig finden umfangreiche Regenerations- und Migrationsmaßnahmen im Projekt SATCOMBw unter Aufrechterhaltung des laufenden Betriebs statt.
Foto: Bundeswehr/Martina Pump

ROBUSTE KOMMUNIKATION IN UNBEMANNTEN SYSTEMEN



Aktuelle Konflikte zeigen, dass UAV in unterschiedlichen Einsätzen große Datenmengen produzieren und für die Auswertung zur Verfügung stellen. Informationsüberlegenheit, Führungsüberlegenheit und Wirkungsüberlegenheit, die Elemente der vernetzten Operationsführung, werden dann erreicht, wenn der Prozess von der Aufnahme der Sensorinformationen durch UAV über ihre Verarbeitung für die Entscheidungsfindung bis hin zum Einsatz des idealen Wirkmittels in einer Sensor-Effektor-Kette optimal ausgeführt werden. Dazu leistet *DND-Digital* durch die Integration von Systemen und Services zur Schaffung kurzer Wirkungsketten einen wesentlichen Beitrag.

Für die Übertragung der Informationen sind moderne und sichere Kommunikationsmittel erforderlich. Hierfür bietet das Führungsfunksystem *BNET True Software Defined Radio* (SDR) eine leistungsstarke wie resiliente Plattform für UAV im Informations- und Kommunikationsverbund. Das System ermöglicht belastbare Mesh Ad-hoc Netzwerk (MANET) mit mehreren hundert Teilnehmern und stellt in diesen Netzwerken Datenraten von bis zu 100 Mbit/s zur Verfügung. In der Nano-Variante stehen die *BNET*-Funktionen auch unbemannten Systemen zur Verfügung.

Mit der einzigartigen Multi-Channel-Reception (MCR) Technologie ermöglicht das *BNET*-Führungsfunksystem den Austausch von Video-, Sprach- und Datenkommunikation im vorgegebenen Frequenzspektrum von VHF über UHF bis hinein in das S-Band. Ergänzt wird die MCR um eine dynamische Spektrumallokation (DSA) und integrierte Spektrumanalysatoren, welche das zugewiesene Spektrum permanent analysieren und nur jene Frequenzen den einzelnen Entitäten dynamisch zuweisen, die aktuell nicht gestört oder durch andere Teilnehmer belegt werden. Im intuitiven Netzwerk-Management-System (NMS) können die für die Truppenteile zur Verfügung stehenden Frequenzbereiche festgelegt werden, um die Vorgaben des Frequenzmanagements einzuhalten und Updates bzw. neue Konfigurationen „over-the-air" zu verteilen.

Neben dem softwarebasierten *BNET*-Funkgerät bietet *DND-Digital* mit dem System *FIRE WEAVER* eine marktverfügbare und D-LBO kompatible Sensor-To-Effektor Applikation. *FIRE WEAVER* verteilt Zieldaten in der notwendigen Genauigkeit zwischen Sensoren und Effektoren im Netzwerk und augmentiert diese in den Sicht- und Zielsystemen der vernetzten Elemente. Dem taktischen Führer bzw. der Feuerleitung schlägt *FIRE WEAVER* ideale Wirkmittel für die jeweiligen Ziele bereit. Die intelligenten, prädiktiven Verfahren zur Bekämpfung mobiler oder zeitkritischer Ziele unterstreichen den besonderen Mehrwert des *FIRE WEAVER* bei hoher operativer Geschwindigkeit.

Mit dem Aufbau eines Shared Information Space (SIS), welcher ausgewählte Informationen priorisiert überträgt, diese nach den verfügbaren Bandbreiten skaliert und zwischen temporär getrennten Informationsräumen synchronisiert, ist ein wesentlicher Systemrahmen gegeben, in dem einsatzbereite Anwendungen wie *FIRE WEAVER* zur Anwendung gebracht werden können.

In Verbindung mit dem leistungsstarken und resilienten *BNET*-Führungsfunksystem und taktischen UAV für die Zielaufklärung ist *FIRE WEAVER* in der Lage, einen greifbaren Fähigkeitsmehrwert zu generieren. Damit leistet *DND-Digital* einen Beitrag für die Dominanz in Multi Domain Operations und stärkt die digitale Konvergenz.

DND Digital

KONTAKT: DND-Digital
Dynamit Nobel Defence GmbH
digital@dn-defence.com
www.dn-defence.com

Fotos: DND

Weltraumstart SARah am 18. Juni 2022: Die „Stage 1" der mehrstufigen Trägerrakete „Falcon 9" kehrt fast punktgenau wieder auf die Erde zurück, nachdem sie den ersten von insgesamt drei SARah-Satelliten in seine Umlaufbahn verbracht hat.
Foto: SpaceX

OBERSTLEUTNANT KATJA BÜCHNER,
DEZERNENTIN INNOVATION & DIGITALISIERUNG,
ZENTRUM DIGITALISIERUNG DER BUNDESWEHR UND FÄHIGKEITSENTWICKLUNG CIR

PERSONAL CIR

PROFESSIONALISIEREN IN DER DIMENSION

Die Fachausbildung im Bereich Cyber/IT ist uniformträgerbereichsübergreifend.
Foto: Bundeswehr/Andreas Metka

Die Anforderungen an eine moderne Bundeswehr sind in den vergangenen Jahren deutlich gestiegen – insbesondere im Bereich Personal. Wie die Entwicklungen im sicherheitspolitischen Umfeld jüngst am Beispiel des Russland-Ukraine-Krieges sowie die rasant fortschreitende Digitalisierung zeigen, muss sich die Bundeswehr auf sehr unterschiedliche, aber sich jeweils schnell verändernde Rahmenbedingungen einstellen. Die Forderung nach Digitalisierung geht für die Bundeswehr mit großen Herausforderungen einher. Für die Lösung dieser Herausforderungen gibt es bezogen auf das Personal nur eine Antwort: Professionalisierung. Professionalisierung heißt, das fachliche Know-how der Bundeswehrangehörigen noch stärker als bisher in den Vordergrund zu stellen und zum Beispiel die Aus- und Weiterbildung des Personals so zu schärfen, dass sie passgenau auf den fachlichen Verwendungsaufbau der Bundeswehrangehörigen zugeschnitten ist. Der Grund: nur tiefgreifend professionalisiertes Personal kann in volatilen Zeiten permanenter Veränderung den mit der Digitalisierung einhergehenden Wandel aktiv gestalten.

PROFESSIONALISIERUNG DES CYBER/IT-PERSONALS

Der militärische Organisationsbereich Cyber- und Informationsraum (CIR) betritt in dieser Hinsicht neue Pfade. In Sachen Professionalisierung des Cyber/IT-Personals wird der Verwendungsaufbau in fachliche Aufgabenbereiche differenziert, so dass eine zielgerichtete Qualifikation des Personals sichergestellt werden kann. Professionalisierung berührt dabei zwei Ebenen:

1. Die Ebene des Personals CIR an sich und
2. die Ebene der Personalprozesse, die sich beispielsweise auf neue Zugangswege, Zulagen und die Ausbildung des Bereichs Cyber/IT konzentrieren.

Hierdurch werden die Angehörigen des CIR nach und nach zu „Profis" ihres jeweiligen Fachgebiets, die der gesamten Bundeswehr zur Verfügung stehen. Weil sich Personal auf diese Weise motivieren, binden und individuell (weiter)entwickeln lässt, kann dieser Prozess nachhaltig helfen, den Fachkräftebedarf langfristig zu decken.

Im Bereich Cyber/IT erfolgt zusätzlich die Unterscheidung zwischen einer Fach- und einer Führungskarriere: die Offizierinnen und Offiziere der Fachkarriere (IT-Expertinnen/IT-Experten) sind für die Erfüllung spezieller Fachaufgaben verantwortlich, während die Offizierinnen und Offiziere der Führungskarriere (IT-Management) die Einbindung der Fachaufgaben in die Operationsführung der Streitkräfte gewährleisten.

Im „Kampf um die besten Köpfe" stellt der Organisationsbereich CIR das fachliche Know-how seiner Angehörigen in den Mittelpunkt. In dieser Hinsicht wird auf die Devise „Professionalisieren in der Dimension" gesetzt. Schließlich wirken in den

▼ Durch die Bereitstellung von aufbereiteten Geoinformationen unterstützen die Angehörigen des Zentrums für Geoinformationswesen der Bundeswehr die Streitkräfte und Verbündeten.
Foto: Bundeswehr/Martina Pump

◀ Eine Soldatin vom APV-Trupp (Abstandsfähige Produktverbringung) aus dem Zentrum für Operative Kommunikation startet einen Testballon mit daran befestigter Radiosonde.
Foto: Bundeswehr/Anne Weinrich

▶ Eine Spezialistin der Elektronischen Kampfführung: die Radaraufklärerin.
Foto: Bundeswehr/Martina Pump

vier CIR-eigenen Fachlichkeiten Cyber/IT-Dienst, Militärisches Nachrichtenwesen und Elektronische Kampfführung, Operative Kommunikation und Geoinformationsdienst ausgebildete Spezialistinnen und Spezialisten dimensionsweit und dimensionsübergreifend in alle anderen Organisationsbereiche der Bundeswehr. Für alle vier Fachlichkeiten stellt „Information" das verbindende Element dar. Sie bildet den Kern allen Handelns im Organisationsbereich CIR: ob in Form der Übertragung per Satellit direkt live aus dem jeweiligen Einsatzgebiet oder aufbereitet zu einer übergreifenden Lagedarstellung.

SPEZIALISTINNEN UND SPEZIALISTEN DES CIR SIND INFORMATIONS- UND SERVICEPROVIDER FÜR DIE BUNDESWEHR

Die Digitalisierung verändert unser Leben praktisch ständig. Unser Alltag ist heute nicht nur global vernetzt, sondern digital und smart. In Sekunden buchen wir Reisen, können 24 Stunden am Tag Nachrichten in jeder Sprache der Welt abrufen oder uns per Videotelefonie überall auf dem Globus austauschen und miteinander arbeiten – mittlerweile sogar aus dem Homeoffice heraus. Neben all diesen Chancen haben sich gleichzeitig auch Risiken entwickelt. Unser Gemeinwesen, aber auch die Bundeswehr, ist mehr und mehr abhängig von einer funktionierenden IT-Infrastruktur. Jedoch haben Cyberangriffe auf Staaten und kritische Infrastrukturen, Fake News und Desinformation in den vergangenen Jahren eklatant zugenommen.

Mit der Aufstellung des Organisationsbereichs CIR im Jahr 2017 hat die Bundeswehr diesen Risiken eine konkrete Antwort entgegengesetzt. Vor dem Hintergrund bestehender und zukünftiger Anforderungen – insbesondere auch im Bereich der Landes- und Bündnisverteidigung – wurden die verschiedenen Akteure der Dimension CIR unter einem Dach versammelt. Die Zusammenführung der Anteile Digitalisierung, IT-Bereitstellung, -betrieb sowie Schutz von IT-Systemen, Aufklärung und Wirkung sowie Bereitstellung von Geoinformationen erfolgt bei den Akteuren des CIR dabei unter der Prämisse, sich im eigenen Denken und Handeln an den eigenen Fachlichkeiten auszurichten.

War beispielsweise die Fachausbildung des Personals aus dem Bereich Cyber/IT vor 2017 noch primär an den einzelnen Uniformträgerbereichen von Heer, Luftwaffe und Marine ausgerichtet, so werden diese Spezialistinnen und Spezialisten mit ihrer jeweiligen fachlichen Expertise seit 2017 schrittweise für den Kampf im Cyber- und Informationsraum uniformträgerbereichsübergreifend ausgebildet. Auf diese Weise entstehen für die Bundeswehr Synergieeffekte für das gesamte Aufgabenspektrum der Streitkräfte.

ZIELGERICHTETE PERSONALENTWICKLUNG ALS SCHLÜSSEL ZUR PROFESSIONALISIERUNG IM CIR

Fachwissen und Kompetenz sind für die Angehörigen des Organisationsbereichs CIR eine entscheidende Voraussetzung, um als Fachleute auf ihrem Gebiet für die gesamte Bundeswehr tätig sein zu können. Für die Akteure im CIR bedeutet dies, sich dienstgradunabhängig und zuweilen auch fernab der Hierarchie mit eigenem Fachwissen und eigenen Kompetenzen in die Lösung eines bestehenden Problems oder Sachverhaltes einbringen zu können. Auf diese Weise erfahren die Angehörigen des CIR individuelle Wertschätzung.

Expertise und spezialisiertes Fachwissen bauen sich allerdings erst mit der Zeit und über die Anwendung in der Praxis auf. „Lebensbegleitendes Lernen", unter der Prämisse einer stringenten, fachlich orientierten Personalentwicklung, steht deshalb im Organisationsbereich CIR an prominenter Stelle. Um dem Gedanken einer zielgerichteten Personalentwicklung als Schlüssel zur Professionalisierung gerecht werden zu können, wurden im CIR für alle vier Fachlichkeiten eigene Systematiken für den personellen Verwendungsaufbau in den einzelnen Werdegängen und der Laufbahn des Geoinformationsdienstes der Bundeswehr erstellt. Sie bilden das Herzstück zur Professionalisierung des Personals im CIR und

legen die Grundlage für den individuellen Verwendungsaufbau, der Kennzeichnung von Dienstposten in den Organisationsgrundlagen sowie der Ausbildung des Personals. In jeder dieser Werdegangssystematiken wird der Personalkörper in der Fachlichkeit in Teilbereiche, Vertiefungen und Spezialisierungen untergliedert. Hierdurch lassen sich für alle Fachtätigkeiten sogenannte qualitative Bedarfsträgerforderungen – fachliche Anforderungskriterien an das Personal – ableiten. Sie dienen als Grundlage für die Gewinnung und Bindung von Personal sowie für die Gestaltung des gezielten individuellen

Verwendungsaufbaus. Damit wird gleichzeitig die Voraussetzung geschaffen für die weitere Professionalisierung in der Fachlichkeit.

NEUE KARRIEREPFADE KÖNNEN IM CIR BESCHRITTEN WERDEN

Um sich immer wieder an schnell ändernde Lagen anpassen zu können, hat sich der Organisationsbereich CIR zum Ziel gesetzt, neue Zielgruppen zu erschließen und für deren Gewinnung innovative Zugangswege zu öffnen. Mit dem Cyber/IT Evaluation Center (CITEC) – siehe Beitrag Seite 162 – ist beispielsweise eine Einrichtung entstanden, in der sich IT-affines Personal, das bislang in anderer Funktion in der Truppe eingesetzt war, für eine Verwendung im Organisationsbereich CIR testen lassen kann.

Doch nicht nur im CITEC werden fachliche Potenziale erschlossen und Kompetenzen passgenau gefördert. Mit der Einführung einer eigenen Fachkarriere im Cyber/IT-Dienst der Bundeswehr ermöglicht der Organisationsbereich seinen Angehörigen, sich neben der klassischen Führungskarriere für einen maßgeblich fachlich geprägten Karrierepfad entscheiden zu können, um die eigene Expertise auszubauen und zu vertiefen.

DAS RICHTIGE PERSONAL MIT DER RICHTIGEN QUALIFIKATION AN DER RICHTIGEN STELLE

Um neuen Fähigkeitsforderungen – wie der Nutzung Künstlicher Intelligenz in der Führung vernetzter Operationen – mit professionell ausgebildeten Spezialistinnen und Spezialisten in der gesamten Dimension der Bundeswehr entsprechen zu können, werden die aktuellen Strukturen des CIR bis 2025 für ein „CIR 2.0“ neu ausgestaltet.

Für den Organisationsbereich CIR stellt die Konzentration auf die eigenen fachlichen Kernfähigkeiten einen entscheidenden Faktor für seine Neuausrichtung dar. Um in und aus der gesamten Dimension weiterhin professionell unterstützen zu können und mit hervorragend ausgebildeten Fachleuten für die Bundeswehr zur Verfügung zu stehen, wird die weitere Professionalisierung des Personals in der Dimension CIR vorangetrieben.

▼ Ein Soldat vom APV-Trupp (Abstandsfähige Produktverbringung) aus dem Zentrum für Operative Kommunikation bewertet die Ballonauflaststellung auf dem Monitor im Fahrzeug EAGLE.
Foto: Bundeswehr/Anne Weinrich

DIENSTSTELLEN-PROFIL

SCHULE FÜR STRATEGISCHE AUFKLÄRUNG DER BUNDESWEHR

Sie ist die zentrale Ausbildungseinrichtung für das Militärische Nachrichtenwesen einschließlich der Fernmelde- und elektronischen Aufklärung sowie für Targeting. Zu ihrem Portfolio gehören auch allgemeinmilitärische Ausbildung und Laufbahnlehrgänge.

AUFGABEN

- Ausbildung im Militärischen Nachrichtenwesen für militärisches und ziviles Personal der Bundeswehr sowie der NATO und ihrer Partnerstaaten mit dem Fokus auf Elektronische Kampfführung, Nachrichtenmanagement, Militärische Sicherheit sowie Targeting und Aufklärungssprachen.
- Allgemeinmilitärische Laufbahnausbildung der Offizieranwärterinnen und Offizieranwärter der Ausbildungs- und Verwendungsreihen Elektronische Kampfführung (EloKa), Operative Kommunikation (OpKom) sowie der Unteroffiziere und Unteroffizierinnen der EloKa, der OpKom sowie des Geoinformationsdienstes der Bundeswehr.
- Fachliche Laufbahnausbildung der Offizierinnen und Offiziere sowie Unteroffizierinnen und Unteroffiziere als auch der Beamtinnen und Beamten der EloKa.

AUFTRAG

Die Schule für Strategische Aufklärung der Bundeswehr führt jährlich etwa 100 unterschiedliche Trainingstypen mit einer Dauer von unter einer Woche bis zu einem Jahr durch. Jährlich stehen rund 4.500 Trainingsplätze zur Verfügung – Tendenz steigend.

Sie führt die lehrgangsgebundene Ausbildung für die militärischen und zivilen Angehörigen des Militärischen Nachrichtenwesens aus allen Bereichen der Bundeswehr durch. Hierzu gehört vor allem das Personal des militärischen Organisationsbereichs Cyber- und Informationsraum. Ebenso durchläuft hier das entsprechende Fachpersonal von Heer, Luftwaffe, Marine, Streitkräftebasis und Sanitätsdienst seine Basisausbildung im militärischen Nachrichtenwesen, die durch Spezial- und Vertiefungslehrgänge ergänzt wird.

Darüber hinaus werden auch internationale Lehrgänge angeboten, an denen Personal aus NATO und Partnerstaaten teilnehmen kann.

ANSCHRIFT
Stützpunkt Flensburg-Mürwik,
Mürwiker Str. 203,
24944 Flensburg

DIENSTSTELLENLEITUNG
Kapitän zur See Udo Michel

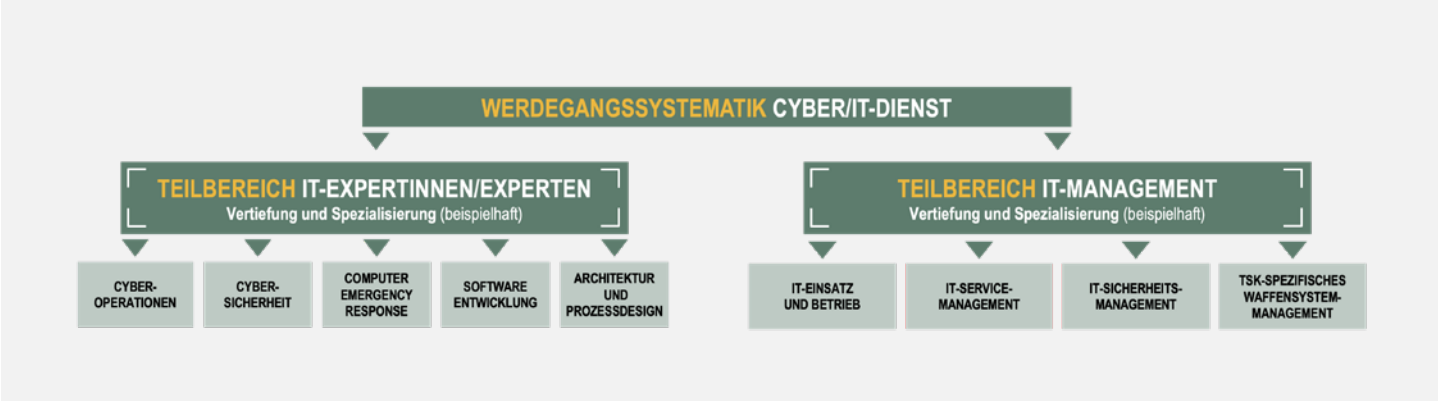
STAMMPERSONAL
~250

AUFSTELLUNG
15.01.2003

MAJOR JOHANNES VÖLPEL-SOLBACH,
REFERENT FÜR FÄHIGKEITSENTWICKLUNG
DES PERSONALS CYBER/IT-DIENST
UND PROJEKTLEITUNG CITEC,
KOMMANDO CIR

DAS CYBER / IT EVALUATION CENTER – EINE ERSTE BILANZ

Die Identifikation und Gewinnung von hochspezialisiertem Cyber/IT-Fachpersonal für die Bundeswehr ist einer der Schlüssel zur erfolgreichen Digitalisierung der Streitkräfte. Dem entgegen steht der zunehmende Druck des demographischen Wandels in Verbindung mit einem stetig steigenden Bedarf an genau diesem Fachpersonal in der Wirtschaft und in anderen Ressorts.
Dieser Herausforderung stellt sich der Organisationsbereich Cyber- und Informationsraum (CIR) mit der Etablierung des IT-fachlichen Screenings am Cyber/IT Evaluation Center (CITEC).



DER CYBER/IT-DIENST DER BUNDESWEHR – NEUE KARRIEREPFADE FÜR IT-SPEZIALISTINNEN UND IT-SPEZIALISTEN

Mit der Übernahme der Dimensionsverantwortung für den Cyber- und Informationsraum durch den Inspekteur CIR und der damit einhergehenden personellen Fähigkeitsverantwortung für den Cyber/IT-Dienst, das Militärische Nachrichtenwesen, die Operative Kommunikation und den Geoinformationsdienst erfolgte eine neue und überfällige Neubewertung der personellen Ausrichtung des IT-Bereichs der Bundeswehr. Kern war dabei herauszufinden, wie es möglich ist, die IT-Spezialistinnen und IT-Spezialisten, unabhängig von der Uniformfarbe, gemäß dem Bedarf und ihrer individuellen Fähigkeiten zielgerichtet einzusetzen und zu entwickeln, ohne die vorhandenen Bedürfnisse der Teilstreitkräfte und Organisationsbereiche zu vernachlässigen. Zur Lösung dieser Frage wurde ein streitkräftegemeinsamer Verwendungsaufbau für das militärische IT-Personal auf der Grundlage einer Werdegangssystematik für den Cyber/IT-Dienst der Bundeswehr etabliert.

Der Fokus im Verwendungsaufbau des Cyber/IT-Dienstes liegt auf der Professionalisierung des IT-Personals der Streitkräfte. Sie wird durch die Differenzierung in die fachlichen Aufgabenbereiche sowie eine damit verbundene zielgerichtete Qualifikation des Personals sichergestellt. Zusätzlich erfolgt die gezielte Unterscheidung zwischen einer Führungs- und einer Fachkarriere. Während die Offizierinnen und Offiziere der Fachkarriere (IT-Expertinnen/IT-Experten) grundsätzlich die Erfüllung spezieller Fachaufgaben verantworten, stellen die in der Führungskarriere (IT-Management) tätigen Offizierinnen und Offiziere die Einbettung der Fachaufgabe in die Operationsführung der Streitkräfte sicher.

Der Verwendungsaufbau der Offizierinnen und Offiziere des Truppendienstes Cyber/IT eröffnet damit unterschiedliche Karrierepfade, je nachdem, welche Anforderungen an die Fachlichkeit gestellt werden. Er ist somit die Grundlage für die personelle Ausrichtung auf die Chancen und Herausforderungen im Cyber- und Informationsraum und kann als möglicher Anreiz zur Erfüllung der individuellen Vorstellungen des IT-Personals dienen.

DIE ETABLIERUNG DES CITEC

Eine Fachkarriere ist jedoch ohne die Identifizierung von passendem Fachpersonal nicht realisierbar. In einer durch das Kommando CIR initiierten Untersuchung des Personalgewinnungsprozesses für IT-Fachkräfte wurde der Bedarf an einem zusätzlichen Verfahren zur Identifikation von fachlichen Kenntnissen und Fertigkeiten festgestellt. Die Idee zur Umsetzung in Form eines Cyber/IT Evaluation Centers (CITEC) wurde im Juni 2019 der Leitung des Bundesministeriums der Verteidigung vorgestellt und eine beschleunigte Umsetzung noch im selben Jahr angewiesen.

WAS IST DAS CITEC?

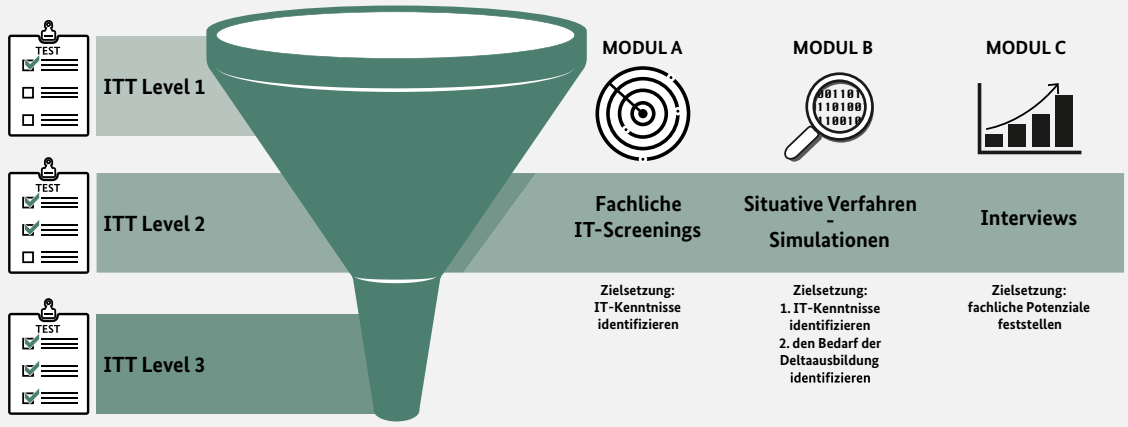
Am CITEC wird ein IT-fachliches Screening zur Identifikation notwendiger Kenntnisse und Fertigkeiten durchgeführt. Das CITEC ist ein dreistufiges modulares Testverfahren. Es ist als Gesamtprozess zu verstehen, mit dem die individuellen Fähigkeiten und verborgenen Potentiale der zu Prüfenden gemäß dem Bedarf der Bundeswehr identifiziert werden. Ziel ist dabei – neben dem durch das Bundesamt für das Personalmanagement der Bundeswehr etablierten Assessmentverfahren zur Feststellung einer Eignung für eine der militärischen Laufbahnen – ein Votum über die IT-fachlichen Fähigkeiten der Bewerbenden und die daraus ableitbaren Verwendungsmöglichkeiten zu erhalten.

Zusätzlich lassen sich individuelle Qualifizierungsbedarfe frühzeitig erkennen und somit zielgerichtet Pläne zur Schließung dieser Qualifizierungslücken entwickeln. Der Schwerpunkt der Testung am CITEC liegt auf der Eignungsfeststellung für hochspezialisierte Verwendungen aus dem Teilbereich der IT-Experten.

Die Entwicklung und fachliche Ausgestaltung wurde unter Federführung des Kommandos CIR in Zusammenarbeit mit den Fachzentren des Organisationsbereichs CIR vorangetrieben. Erst durch die Bündelung der Expertise aus Personal- und Fachabteilung ist es möglich, geeignete Fachkräfte zu identifizieren und einzustellen. Dabei fließen fachliche Erfahrungen und Bedarfe aus den Fachzentren in die Testentwicklung ein und lassen so einen stringenten Prozess und leistungsstarke Softwareprodukte für das IT-Screening entstehen.

▲ Werdegangssystematik Cyber/IT-Dienst.
Grafik: KdoCIR/GdlPers

◀ Der Cyber/IT-Dienst – Die Fähigkeit steht im Fokus, nicht die Farbe der Uniform!
Foto: Bundeswehr



DIE DREI IT-TESTLEVEL

IT-Testlevel 1 (ITT 1): Das ITT1 stellt das erste Job-Interview und das Onboarding in den Prozess des CITEC dar. Im Schwerpunkt handelt es sich um ein Werkzeug der Personalberatung und -gewinnung. In dem Interview werden den Teilnehmenden erste grobe individuelle Verwendungsmöglichkeiten, fachliche Ansprechpartner und das weitere Vorgehen im Prozess des CITEC mitgeteilt.

IT-Testlevel 2 (ITT 2): Das Herzstück des CITEC. Dieses Testlevel müssen alle Interessierten für den Cyber/IT-Dienst durchlaufen, unabhängig ob Neubewerberinnen und -bewerber oder bereits vollumfänglich ausgebildete Soldatinnen und Soldaten. In drei aufeinanderfolgenden Modulen müssen die Kandidatinnen und Kandidaten ihr Können in der gesamten Bandbreite des Cyber/IT-Dienstes unter Beweis stellen. Dabei werden im Modul A die theoretischen Fähigkeiten erfasst und bereits eine erste Einordnung in die Vertiefungen des Cyber/IT-Dienstes vorgenommen. Darauf aufbauend durchlaufen die Teilnehmenden, gemäß ihrer nachgewiesenen individuellen Fähigkeiten, die situativen Verfahren der Module B, in denen die praktischen Fähigkeiten, die in den jeweiligen Vertiefungen notwendig sind, nochmals im Detail abgerufen werden. Diese gezeigten Fähigkeiten werden durch IT-Spezialistinnen und IT-Spezialisten des Cyber/IT-Dienstes ausgewertet und in dem Jobinterview des Moduls C zusätzlich mit psychologischer Expertise für den Teilnehmenden in einen Gesamtkontext gestellt. Das aus dem Modul C resultierende fachliche Votum stellt eine Empfehlung für einen möglichen Verwendungsaufbau, aber auch für individuelle Qualifizierungsmaßnahmen dar.

IT-Testlevel 3 (ITT 3): Als schon etabliertes ITT3 steht die bekannte Cyber-Operateur-Eignungsfeststellung dem CITEC-Prozess zur Verfügung. In dieser weiteren fachlichen Testung werden die benötigten Fähigkeiten und Potentiale für Verwendungen im Zentrum für Cyber-Operationen der Bundeswehr festgestellt. Weitere fachliche Testungen befinden sich in der Planung.

▲ Das Testverfahren am CITEC.
Grafik: KdoCIR/GdlPers

▶ Beratung durch IT-Spezialisten des Cyber/IT-Dienstes.
Foto: Bundeswehr/Nicole Herzog

CITEC – MEHR ALS EIN IT-SCREENING!

Neben der IT-fachlichen Testung erfolgt eine fachlich versierte Beratung durch IT-Spezialistinnen und IT-Spezialisten. Zusätzlich wird den Teilnehmenden, aber auch den Expertinnen und Experten der Bundeswehr, eine Plattform zum fachlichen Austausch und zur Vernetzung geboten. Zukünftig wird das CITEC Anknüpfungspunkte zu akademischen und wirtschaftlichen Organisationen im Großraum München ausbauen, um so die Idee des CITEC zukunftssicher aufzustellen und auszubauen.

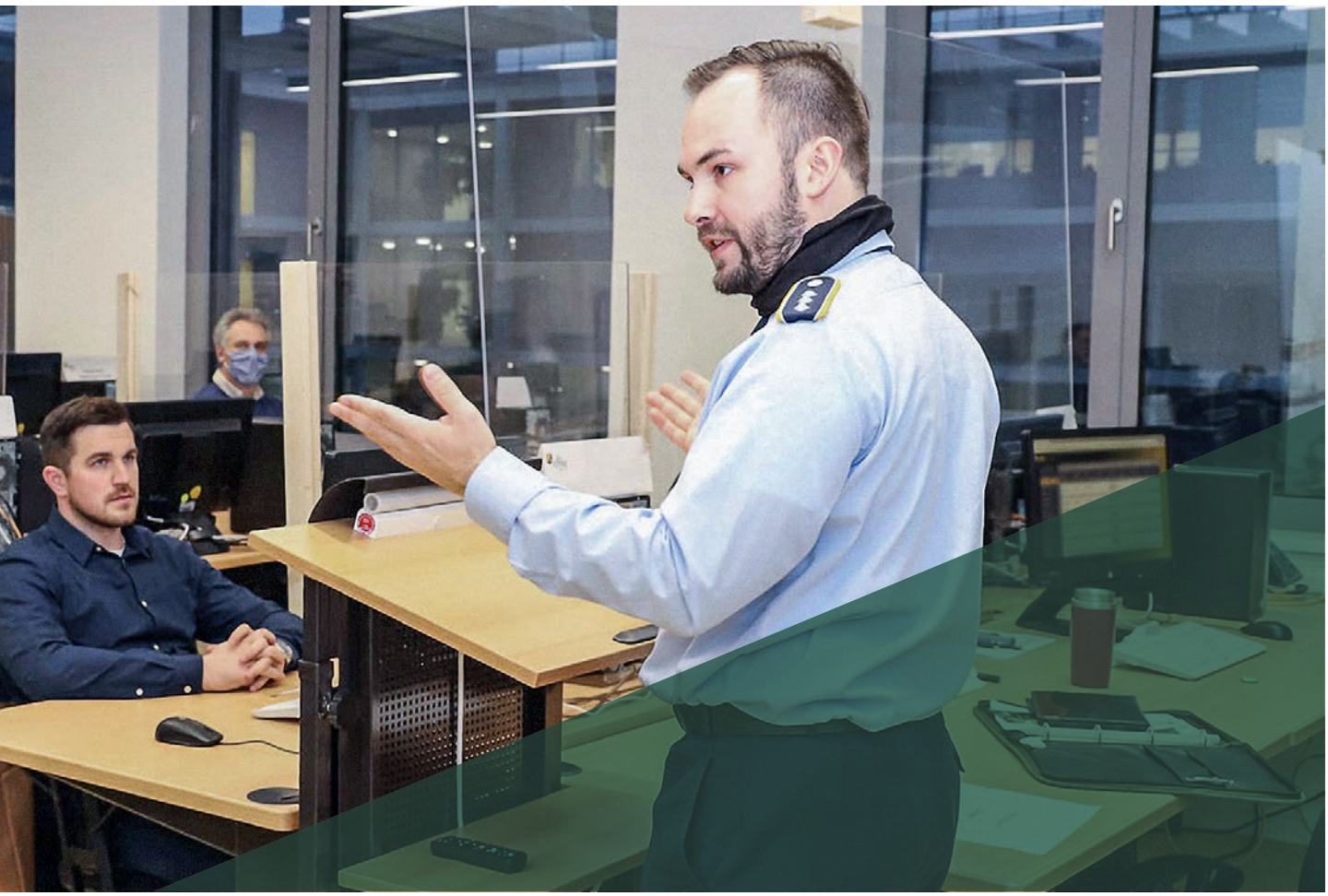
WAS WURDE ERREICHT? – DER „WAY AHEAD"!

Der erste Pilotdurchgang erfolgte im November 2019. Dafür entwickelten die Fachzentren des Organisationsbereichs CIR innerhalb von vier Monaten die ersten Testmodule und stellten die Durchführung sicher.

Im Fokus stand zunächst das Kandidatenfeld der Offizierinnen und Offiziere im Status einer Soldatin/eines Soldaten auf Zeit mit einem erfolgreich absolvierten MINT-Studium, welche sich in den letzten zwei Dienstjahren ihrer Regelverpflichtungszeit befanden und bisher nicht im Werdegang Cyber/IT-Dienst verwendet wurden. Dabei stellten sich gestandene Fallschirmjägeroffiziere, Ubootfahrer und Luftwaffensicherungsoffiziere dem IT-Screening mit dem Wunsch, einer ihrem akademischen Abschluss gerechten Verwendung nachzukommen. Im Rahmen der Phase 1 konnten so bis Ende 2021 trotz der Covid-19 bedingten Limitierungen insgesamt 45 Offizierinnen und Offiziere erfolgreich ihre Fähigkeiten für eine Verwendung im Cyber/IT-Dienst nachweisen. Zwölf Teilnehmenden konnte, abgeleitet aus den Ergebnissen des IT-Screenings, bereits ein Angebot für eine Verwendung unterbreitet werden, das, verbunden mit einer Weiterverpflichtung, zu einem Werdegangswechsel in den Cyber/IT-Dienst der Bundeswehr führte.

Mit Beginn der Phase 2, der Etablierung des CITEC, erfolgte die Ausweitung des Verfahrens auf das Kandidatenfeld der zivilen Seiteneinsteigenden. Dabei wurde erstmals bei der Einstellung von externem IT-Fachpersonal das fachliche Votum neben der formalen Qualifikation als Grundlage für eine Einstellung in den Cyber/IT-Dienst herangezogen. Diese neue Herangehensweise ermöglichte eine aus den Fähigkeiten und Potentialen abgeleitete und somit zielgerichtete Anstellung. Insgesamt konnten so innerhalb eines Jahres 13 IT-Spezialisten identifiziert und für die Bundeswehr gewonnen werden.

Neben der aktiven Seite der Bundeswehr stellt der Reservistendienst (siehe auch Seite 168) eine tragende Rolle in der Sicherstellung der Auftragserfüllung der Streitkräfte dar. Im Zuge der Professionalisierung der Bedarfsdeckung wurde zum Aufbau der Cyber-Reserve das Projekt „Speerspitze" im Zentrum für Cyber-Sicherheit der Bundeswehr ins Leben gerufen, um für die Incident Response Teams fähige IT-Fachkräfte zu identifizieren. Auch hier konnte das CITEC



seine Leistungsfähigkeit unter Beweisstellen und zunächst elf potentielle Cyber-Security Experten ausmachen und zielführend beraten.

Zum Jahreswechsel 2022 wurde mit der Testung der Absolvierenden der Bundeswehr-Universitäten die Phase 3 des Etablierungsprozesses, der auf studierende Offiziere des Cyber/IT-Dienstes abzielt, begonnen. Die formale Qualifikation eines Studiums gibt Hinweise auf eine zukünftige Verwendung. Sie ist jedoch kein Garant für eine erfolgreiche Karriere in jedem Teilbereich des Cyber/IT-Dienstes. Hier kommt es vielmehr darauf an herauszufinden, welche Qualifikationen der studierende Offizier oder die studierende Offizierin erworben hat und inwieweit diese Kenntnisse als Basis für eine Verwendung im Teilbereich des Cyber/IT-Dienstes nutzbar sind.

Durch das IT-Screening am CITEC kann dies herausgefunden werden und darauf aufbauend eine zielgerichtete Verwendungsplanung für die Offizierinnen und Offiziere erfolgen.

Ohne Etablierung des CITEC wären der Bundeswehr viele sehr gute fachliche Potentiale verborgen, und somit ungenutzt geblieben. Mit dem CITEC konnten diese jedoch erkannt werden. Darauf aufbauend wurden den getesteten Personen attraktive Angebote für den Verwendungsaufbau im Cyber/IT-Dienst gemacht.

Um die Durchführung der Testungen am CITEC sicherzustellen, wurde an der Schule Informationstechnik der Bundeswehr in Pöcking ein eigenes Organisationselement geschaffen. Hier wird nicht nur die Durchführung koordiniert, sondern von hier aus erfolgt auch die Kommunikation mit den zukünftigen IT-Spezialistinnen und IT-Spezialisten.

Zukünftig wird das CITEC eine elementare Rolle bei der Identifikation und der zielgerichteten Planung des Verwendungsaufbaus von IT-Fachkräften in der Bundeswehr einnehmen. Das CITEC ist damit ein wichtiger Baustein für die voranschreitende Professionalisierung des Personalkörpers des Cyber/IT-Dienstes der Bundeswehr. Eine Ausweitung des CITEC auf den zivilen Bereich der Bundeswehr wäre daher folgerichtig.

ZUSAMMENFASSUNG

Das Cyber/IT Evaluation Center und der neugeschaffene Cyber/IT-Dienst der Bundeswehr sind die logische Antwort des Organisationsbereichs CIR auf die Herausforderungen und Chancen im Cyber- und Informationsraum. Bereits in der frühen Pilotierungsphase des CITEC konnten dringend benötigte Fachkräfte für den Cyber/IT-Dienst gewonnen werden. Neue innovative Lösungsansätze und das Einschlagen neuer Wege sind der Garant für stetige Weiterentwicklung und somit die Grundlage, um erfolgreich nicht nur im Rennen der Digitalisierung zu bestehen, sondern auch bei der kreativen Personalgewinnung.

▼ IT-Spezialist(innen)en testen IT-Spezialist(innen)en.
Foto: Bundeswehr/Jonas Weber

Bei der Erstellung und Bewertung eines Lagebildes kommt der Beobachtung von Kommunikation eine Schlüsselrolle zu. Eine Aufgabe von enormer Komplexität. Ohne modernste IT-Lösungen ist das nicht zu leisten. Einer der wenigen Global Player in diesem Segment kommt aus Deutschland: INNOSYSTEC, der Entwickler von SCOPE, einer international führenden „Multi Source Analytics“-Software für Sicherheitsbehörden und Militär zur Erkennung und Bekämpfung von Gefahren durch Terrorismus und Kriminalität.

Zusätzlich ermöglicht SCOPE eine wirksame Nachverfolgung von Geldströmen und die Bekämpfung von Korruption. Eine ganze Reihe deutscher Sicherheitsbehörden, Militär und zahlreiche Nachrichtendienste verbündeter Staaten nutzen die INNOSYSTEC-Lösung teilweise seit 20 Jahren. SCOPE ist entsprechend ausgereift und erprobt. Zudem ist SCOPE eine rein deutsche Software, leistet also einen beträchtlichen Beitrag zur Europäischen IT-Souveränität in der „Intelligence Domäne“.

Der „Multi Source“-Ansatz von SCOPE bedeutet: Mit der Software können die unterschiedlichsten Kommunikationskanäle relevanter Gruppierungen korreliert werden: Festnetz- und Mobiltelefonie, Funk- und Satellitenkommunikation über unzählige Internet-Kommunikationskanäle inklusive Dark Net bis hin zu Social-Media-Kanälen und Messenger-Diensten.

Die Zusammenführung und Auswertung dieser Massendaten, ist mit herkömmlichen Mitteln der Datenverarbeitung nicht mehr zu bewältigen. SCOPE ist ein „Big Data Analytics Tool“. Nur mit einer solchen komplexen, extrem leistungsfähigen Lösung ist es überhaupt möglich, aus den Daten die relevanten Daten herauszufiltern und Verknüpfungen zu erkennen.

SCOPE bringt die Massendaten aus den verschiedenen Quellen bzw. Sensoren (SIGINT, OSINT, SOCMINT, usw.) zusammen (Multi Source Analytics). Anschließend werden Zusammenhänge veranschaulicht, damit die Analysten Gefahren entdecken, ehe sie sich auswirken („Datenbasierte Krisenfrüherkennung“). Auch Daten aus der Vergangenheit können von Sicherheitsbehörden und Militär mit Hilfe von SCOPE analysiert werden, um Maßnahmen für die Zukunft zu treffen oder Geschehnisse aufzuklären.

SCOPE folgt zu 100 Prozent den hohen europäischen und deutschen Datensicherheitsstandards. Außerdem hat INNOSYSTEC selbst keinerlei Zugriff auf die Daten der Kunden, stellt also lediglich das Tool SCOPE zur Verfügung. Darin liegt der entscheidende Unterschied zu anderen Anbietern, bspw. aus den USA. Peter Zerwes, Gründer und Geschäftsführer von INNOSYSTEC: „Es geht darum, sicherheitsgefährdende Ereignisse zu verhindern, und nicht darum, gläserne Menschen zu schaffen.“

SCOPE kann zudem an die jeweiligen gesetzlichen Grundlagen in anderen Ländern angepasst werden. Die Software ist hoch variabel und lässt sich problemlos an den aktuellen Bedarf der Nutzer anpassen. Camilla von Baer, CEO neben Peter Zerwes, ergänzt: „Unser Ziel ist es, mit SCOPE die Welt ein Stück sicherer zu machen.“

www.innosystec.de

MAJOR DANILA DUBRAU, KOMMANDO CIR, BEREICH INSPIZIERUNG RESERVISTENANGELEGENHEITEN

DIE CYBER-RESERVE ALS SPEZIALISIERTER TEIL DER RESERVE DES ORGANISATIONSBEREICHS CYBER- UND INFORMATIONSRAUM

Die im März 2017 gegründete Cyber-Reserve leistet, gerade mit Blick auf die „moderne" hybride Kriegsführung, einen anerkannten Beitrag zur gesamtgesellschaftlichen Sicherheitsvorsorge im Bereich Cyber- und IT-Sicherheit. Als innovatives und interdisziplinär aufgestelltes Unterstützungselement ist sie ein Transmissionsriemen aus der Gesellschaft und ermöglicht den fachlichen Erfahrungsaustausch zwischen zivilen und militärischen Cyber-Experten.

DIE ZIELE DER CYBER-RESERVE

Mit der Cyber-Reserve werden konkret drei Ziele verfolgt:

1. **Bildung eines zusätzlichen Kräfteelements im Inland, um für die Abwehr von Cyber-Angriffen weitere qualifizierte Kräfte verfügbar zu machen.*)**
2. **Bündelung von Exzellenzen und Expertinnen/Experten, um durch gemeinsames Üben eine wirkungsvolle und State-of-the-Art Cyber-Wirkkomponente auch mit internationalen Verbündeten, aufzubauen.**
3. **Förderung des Erfahrungsaustausches von eigenem Cyber/IT-Personal mit entsprechenden Spezialistinnen und Spezialisten außerhalb der Bundeswehr.**

*) Art. 35 GG i.V.m. § 63 SG. Im Spannungs- und Verteidigungsfall gff. nach § 6c WPflG.

DAS CYBER-POTENZIAL ALS KONZEPTIONELLER ANKER IN DIE GESELLSCHAFT

Der Cyber- und Informationsraum (CIR) stellt eine besondere Herausforderung für die gesamtstaatliche Sicherheitsvorsorge sowie für die Bundeswehr dar. In diesem Kontext und vor dem Hintergrund einer wachsenden Bedrohungslage im CIR wurden das weitreichende fachliche Potenzial der Reserve und ihre gesellschaftliche Vernetzung in die gesamtstrategische Überlegung mit einbezogen. Fußend auf dem „Konzept der Cyber-Reserve" wurde die Cyber-Reserve der Bundeswehr als Expertenlabel aller Akteure geschaffen, die sich aufgrund ihrer zivilberuflichen Expertise fachlich und thematisch im gesamtgesellschaftlichen Verständnis für die Bundeswehr im CIR einsetzen. Zum sogenannten Cyber-Personal gehören Personen, die im Organisationbereich CIR in den Bereichen Cyber/IT-Dienst, Geoinformationsdienst der Bundeswehr, Operative Kommunikation oder Militärisches Nachrichtenwesen eingesetzt sind.

Die Digitalisierung, einhergehend mit hybriden Formen der Konfliktaustragung und asymmetrischen Bedrohungslagen, erzeugen einen hohen Bedarf an Expertinnen und Experten zur Wahrnehmung von Aufgaben in der Dimension CIR. Basierend auf dem Prinzip der Freiwilligkeit bietet die Cyber-Reserve neben der Möglichkeit der Mitarbeit als hoch qualifizierte Reservistin und Reservist auch die Chance, sich über bürgerschaftliches Engagement und auch in zivilrechtlichen Vertragsverhältnissen einzubringen. Dabei stehen folgende Zielgruppen im Fokus der Personalgewinnung für die Cyber-Reserve:

1. Ehemalige Angehörige der Bundeswehr mit militärischer und/oder ziviler Fachexpertise mit einschlägigen, für die Cyber-Reserve nutzbaren Verwendungen und Kenntnissen.
2. Expertinnen und Experten aus Wirtschaft, Industrie, Wissenschaft und Öffentlichem Dienst.

3. Multiplikatorinnen und Multiplikatoren und Interessierte:
   a) Freiwillige, die sich außerhalb der Reserve engagieren wollen (bürgerschaftliches Engagement von Expertinnen und Experten, Fachkräften, Studierenden, Angehörigen von Vereinen und Verbänden, etc.),
   b) Seiteneinstieg von gedienten sowie ungedienten Interessentinnen und Interessenten mit einschlägigem fachlichem Hintergrund.

Das Konzept der Cyber-Reserve geht damit über den bisherigen Reservistendienst hinaus und öffnet ihn für einen größeren Personenkreis und neue Zielgruppen. Nur so kann die benötigte Expertise in einem sehr dynamischen Bereich für die Bundeswehr erhalten, erweitert und gefördert werden.

WEITERENTWICKLUNG DER RESERVE IM ORGANISATIONSBEREICH CIR IM KONTEXT „STRATEGIE DER RESERVE“ UND DER LANDES- UND BÜNDNISVERTEIDIGUNG

Die im Oktober 2019 durch die Bundesministerin der Verteidigung erlassene „Strategie der Reserve“ ist das Fundament für die weitere Arbeit zum Thema Reserve. Die „Weisung der Reservistenarbeit in den Jahren 2020-2022“ des Stellvertreters des Generalinspekteurs und Beauftragten für Reservistenangelegenheiten der Bundeswehr dient dabei der konsequenten Umsetzung der sicherheitspolitischen Grundlagendokumente sowie der darauf aufbauenden Strategie der Reserve und dem Vorantreiben der Weiterentwicklung der Reserve. Als verbindliche Richtschnur definiert sie Schwerpunkte, Zielvorgaben und Zuständigkeiten.

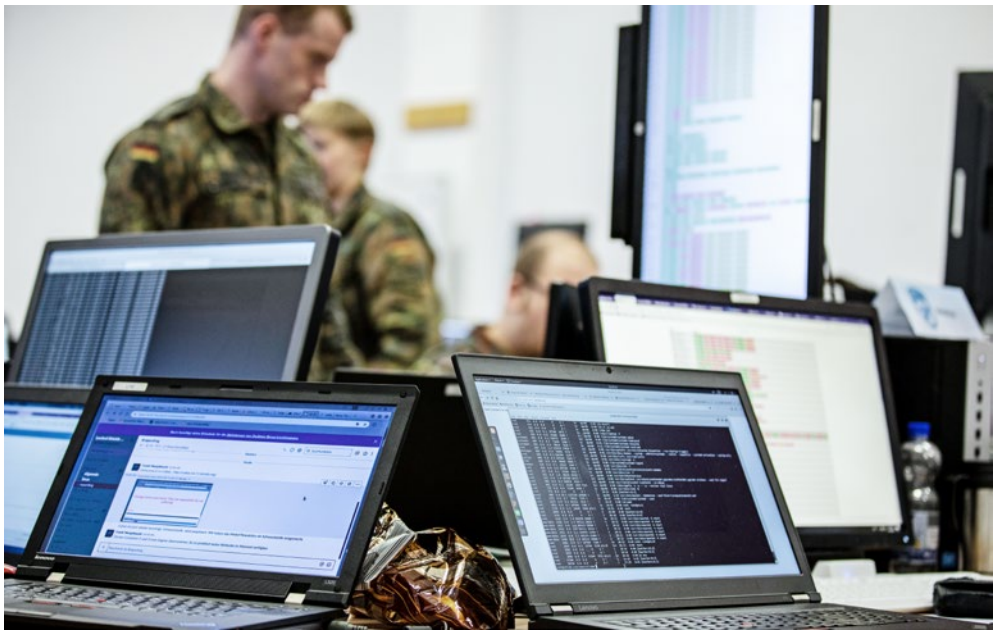
Die Neuausrichtung der Reserve verfolgt drei Etappenziele, die in ihrer Ausrichtung auf das Jahr 2032 und darüber hinaus abzielen.

Für die Umsetzung richtete das Kommando CIR Anfang 2021 eine Projektgruppe mit Vertreterinnen und Vertretern verschiedener Fachbereiche ein. Diese sollen die Reserve des Organisationsbereichs CIR schrittweise und unter Berücksichtigung der Besonderheiten der Cyber-Reserve, ausgerichtet auf das Aufgabenspektrum der Landes- und Bündnisverteidigung, aufstellen und befähigen. Strukturell sind in etlichen Verbänden des Organisationsbereichs Reserveelemente meist in Kompaniestärke ausgebracht, die personell sukzessiv im Rahmen der Grundbeorderung befüllt werden. Dieses Personal ist für Fachaufgaben vorgesehen. Hinzu kommen querschnittliche Aufgaben, wie beispielsweise Logistik und Personalmanagement.

In einem nächsten Schritt werden nun konkrete Möglichkeiten zur Entwicklung der Reserve bis zum Jahr 2025 erarbeitet. Die Maßnahmen sollen einen unmittelbaren Mehrwert für die Reserve darstellen und die aktive Truppe entlasten. Das Kommando CIR beabsichtigt dazu, bei dem Ergänzungstruppenteil – dem nichtaktiven Truppenteil – in einem Informationstechnik-Bataillon eine „Pilot-Kompanie“ aufzustellen. Diese soll mit Material „off-the-shelf“, also marktverfügbarem Material, schnell, kostengünstig und erlebbar ausgestattet werden.

◀ Die Ziele der Cyber-Reserve.
Grafik: Bundeswehr/KdoCIR

▼ Die durch die Bundesministerin der Verteidigung erlassene „Strategie der Reserve“ ist das Fundament für die weitere Arbeit zum Thema Reserve.
Foto: Bundeswehr/Stefan Uj



◀ Bei der NATO-Übung Locked Shields wehren militärische und zivile IT-Fachleute in Echtzeit Angriffe auf simulierte Computernetzwerke und IT-Systeme kritischer Infrastruktur ab.
Foto: Bundeswehr/Martina Pump

▶ Zukünftig sind weitere Projekte zur zielgerichteten Identifikation von hochspezialisiertem IT-Fachpersonal geplant.
Foto: Bundeswehr/Broschinsky

DIE GRUNDBEORDERUNG ALS KERNSTÜCK DER STRATEGIE DER RESERVE

In der Vergangenheit deckte die Beorderung in der Truppen*- und Personalreserve* den Ergänzungsumfang* nicht vollständig ab. Zudem ließ sich die militärfachliche Ausbildung der Reservistinnen und Reservisten nur bedingt abschließen. Als Antwort auf eine einsatzbereite Reserve in voll ausgestatteten Strukturen wurde die Grundbeorderung als zentrales Kernelement der Strategie der Reserve eingeführt. Seit Oktober 2021 werden alle wehrdienstfähig aus dem aktiven Dienst ausscheidenden Soldatinnen und Soldaten der Bundeswehr für einen Zeitraum von sechs Jahren in ein Beorderungsverhältnis eingeplant. Die Altersgrenze für die Beorderung liegt bei 57 Jahren. Die Ausscheidenden werden gemäß dem Bedarf der Streitkräfte auf einen Dienstposten beordert, auf dem sie ihre im aktiven Dienst erworbenen Fähigkeiten möglichst effektiv und heimatnah einbringen können. Zunächst handelt es sich bei der Beorderung um eine Einplanung auf einen bestimmten Dienstposten im Ergänzungsumfang der Bundeswehr, die Priorität liegt auf Dienstposten der Verstärkungsreserve*. Heranziehungen außerhalb eines Bereitschafts-, Spannungs- oder Verteidigungsfalls unterliegen weiterhin dem Prinzip der Freiwilligkeit.

Im Organisationsbereich CIR konnten die vorbereitenden Maßnahmen zur planmäßigen Einführung der Grundbeorderung umgesetzt werden, sodass hier mittlerweile 80 Soldatinnen und Soldaten (Stand April 2022) grundbeordert sind. Die Grundbeorderung hat den Weg in die Reihen der Soldatinnen und Soldaten gefunden. Die Zahl der „Neuzugänge" wächst von Tag zu Tag stetig an und schafft somit die personelle Grundlage für einen zügigen Aufwuchs der Reserve in einem möglichen Bereitschafts-, Spannungs- oder Verteidigungsfall.

***Truppenreserve:** Dient der Unterstützung der aktiven Truppe als integraler Bestandteil in allen Organisationsbereichen. Die Organisationsbereiche können diese Reserve auch als Ergänzungstruppenteile zum Aufbau oder zur Verstärkung bestimmter Fähigkeiten aufstellen.

***Personalreserve:** Gesamtheit aller Beorderten auf nicht strukturgebundene Beorderungsmöglichkeiten in den Organisationsbereichen. Sie dient der planerischen Vorsorge zur Kompensation fehlenden Personals oder zur Deckung eines temporär erhöhten Bedarfs zum Erhalt oder Steigerung der personellen Einsatzbereitschaft.

***Verstärkungsreserve:** Gesamtheit aller Beorderten auf strukturgebundene Dienstposten. Die Verstärkungsreserve wird zur Herstellung der vollen Einsatzbereitschaft der Dienststellen im Geschäftsbereich BMVg und zur Erweiterung bestehender oder zum Aufbau neuer Fähigkeiten benötigt.

***Ergänzungsumfang:** Summe aus Verstärkungsreserve und Personalreserve, alle Beorderungsmöglichkeiten für Reservisten im Frieden.

SPEERSPITZE DER CYBER-RESERVE UND ZIELGENAUE AUSLESE

Das Verteidigungsministerium misst der Cyber-Reserve in künftigen Konflikten eine hohe Bedeutung bei. Der Organisationsbereich CIR ist in die gesamtstaatliche Sicherheitsvorsorge eingebunden und analysiert beispielsweise mit seinen Dienststellen bereits in Friedenszeiten die Bedrohungen aus dem Cyber- und Informationsraum. Mit seinem Zentrum für Cyber-Sicherheit der Bundeswehr (ZCSBw) – siehe auch Seite 128 – gewährleistet der Organisationsbereich CIR als Teil der Cyberverteidigung einen umfassenden Schutz der IT-Services und IT-Systeme der Bundeswehr. Im ZCSBw sind die präventiven und reaktiven Fähigkeiten zum Schutz der IT-Services und IT-Systeme der Bundeswehr abgebildet. Ein wesentlicher

reaktiver Baustein sind die Computer Emergency Response Teams der Bundeswehr (CERTBw). Diese stellen die zweite Stufe der Cyber-Abwehrmaßnahmen dar, nachdem mittels der Sensorik, der Erstanalyse und dem Risikomanagement andere Bereiche ein Informationssicherheitsvorkommnis entdeckt und als besonders gefährlich eingestuft haben. Fokussiert auf die Bereiche Security Incident Response und Computerforensik leisten sie einen Beitrag zur Verteidigung der IT-Systeme und zur Eindämmung von Gefahren im Cyber-Raum. Die Incident Response Teams gewährleisten schnelle und flexible Reaktionen auf Cyber-Angriffe gegen die Informationstechnik der Bundeswehr im In- und Ausland und in den Einsätzen. Die Kräfte des CERTBw wirken bei externen, nationalen wie internationalen Partnern sowie multi- oder supranationalen Organisationen wie der NATO und EU mit.

Das hoch spezialisierte Personal dieser Teams soll zukünftig durch zivile IT-Spezialistinnen und Spezialisten mit Interesse an der Cyber-Reserve verstärkt werden. Dazu wurde 2021 ein Pilotprojekt initiiert, wobei in den IR-Teams 40 Dienstposten der Verstärkungsreserve geschaffen wurden, 24 Dienstposten davon für Seiteneinsteiger in der Laufbahn der Offiziere der Reserve. Regional verortet sollen die Teams bei den Regionalzentren in Köln, Wilhelmshaven, Ulm und Storkow (Mark) sein. Als zukünftige IT-Spezialistinnen und Spezialisten des Cyber/IT-Dienstes erfordert der jeweilige Dienstposten im Bereich der Reserveoffizierinnen und -offiziere ein vorhandenes MINT-Studium, das vornehmlich Know-how im Bereich IT-Security und IT-Forensik nachweist. Um eine adäquate fachspezifische Besetzung der Dienstposten sicherzustellen, stellen sich die potenziellen IT-Spezialistinnen und Spezialisten, nachdem sie erfolgreich das Offizierauswahlverfahren absolviert haben, dem mehrstufigen und modularen Verfahren im Cyber/IT Evaluation Center (CITEC) – siehe auch Seite 162. Seit November 2021 werden CITEC-Durchgänge auch für Reservistinnen und Reservisten durchgeführt. Ziel dieses Testverfahrens ist, die Potenziale der Teilnehmenden zu erfassen und die künftigen Reserveoffiziere gemäß ihren Fähigkeiten gezielt einzusetzen. Je nach individuellen Fähigkeiten werden die Bewerberinnen und Bewerber anschließend in der Cyber-Reserve eingesetzt. Bis März 2022 konnten so zehn aussichtsreiche Kandidaten für eine Verwendung im ZCSBw identifiziert werden. Zukünftig sind weitere Projekte zur zielgerichteten Identifikation von hochspezialisiertem IT-Fachpersonal geplant.

Der Organisationsbereich CIR ist mit dem Aufbau seiner Cyber-Reserve auf einem guten Weg. Es hat sich gezeigt, dass es notwendig ist, Reserve stets und auf allen Ebenen proaktiv mitzudenken und Ressourcen für Reservistinnen und Reservisten vorzusehen. Von der Fachlichkeit bis in die Leitungsinstanz ist gerade in einer Zeit des Umbruchs und der Neustrukturierung das aktive Einbinden und Halten von fähigen und motivierten Kräften der Reserve einer der Schlüssel für die Handlungskompetenz von morgen.

CIR: „SCHMIERÖL IM MOTOR DER AUSLANDSEINSÄTZE“

Ein Besuch bei unserem Verbindungselement im Einsatzführungskommando der Bundeswehr in Schwielowsee

Weltweit leisten Bundeswehrangehörige täglich ihren Dienst in unterschiedlichsten Funktionen und Einsatzgebieten. Major Tino Borchert vertritt den militärischen Organisationsbereich Cyber- und Informationsraum beim Einsatzführungskommando der Bundeswehr. Er leitet das Verbindungselement zum Einsatzführungskommando in Schwielowsee (Brandenburg). Als Zwei-Mann-Team ist es das „Gesicht des Kommandos CIR“ vor Ort und unter anderem für die Sicherstellung der Verbindung und des gegenseitigen Informationsaustauschs zwischen den beiden Dienststellen verantwortlich.

Herr Major Borchert, seit September 2021 sind Sie auf Ihrem, man kann sicher sagen nicht alltäglichen Dienstposten eingesetzt. Wie wurden Sie auf diese Verwendung vorbereitet beziehungsweise sind Ihre bisherigen Vorverwendungen diesbezüglich hilfreich gewesen?

In nunmehr 25 Dienstjahren durfte ich in verschiedenen Verwendungen auf unterschiedlichen Ebenen in der Bundeswehr dienen. Neben einem Drittel meiner Dienstzeit als Portepeeunteroffizier in der Infanterie diente ich zwei Drittel als Offizier in der Aufklärungstruppe und im Militärischen Nachrichtenwesen. Dementsprechend konnte ich eine Fülle an Fachkenntnissen und Erfahrungen erwerben und sammeln. Nun bin ich im Grunde wieder in einer kleinen Kampfgemeinschaft angekommen, in der ich durch einen Portepeeunteroffizier unterstützt werde. Zugegebenermaßen mit deutlich anderen und komplexeren Aufgaben. Auch die Führungsebene hat sich verändert.

Mit den Jahren entwickelte sich ferner ein weitreichendes „persönliches Netzwerk“ innerhalb der Bundeswehr, welches zum Teil bis in Dienststellen der NATO hineinreicht. Aufgrund meiner bisher kurzen Stehzeit im Kommando CIR ist dieses Netzwerk tagtäglich außerordentlich hilfreich.

Was die unmittelbare Vorbereitung auf meinen derzeitigen Dienstposten anbelangt, so konnte ich während meiner letzten Verwendung im Joint Intelligence Center unter anderem an einem zweiwöchigen Training für CIR-Personal der „Vornepräsenz der NATO in Litauen“ teilnehmen. Im Rahmen dieser erstklassigen Ausbildung konnte ich fast alle Dienststellen des Organisationsbereichs CIR kennenlernen – von A wie Auswertezentrale Elektronische Kampfführung bis Z wie Zentrum für Cyberoperationen, Zentrale Abbildende Aufklärung oder Zentrum für Softwarekompetenz. Infolgedessen verfüge ich jetzt über noch tiefergehende Vorstellungen vom Leistungsspektrum und von den Fähigkeiten dieser Dienststellen. Von diesen Einweisungen und Bildern profitiere ich regelmäßig.

Meine über drei in besonderen Auslandsverwendungen verbrachten Lebensjahre erinnern mich regelmäßig daran, „vom Einsatz her“ durch die „CIR-Brille“ zu schauen. So kann das Einbringen eines sinnvollen CIR-Beitrags in der Planung zukünftiger Einsätze der Bundeswehr gewährleistet werden.

Warum bedarf es überhaupt eines Verbindungselementes des Kommandos CIR im Einsatzführungskommando der Bundeswehr? Welche Aufgaben nehmen Sie wahr?

Die Notwendigkeit eines Verbindungselementes beim Einsatzführungskommando wurde bereits im Jahre 2015 erkannt und umgesetzt. Damals wurde ein Verbindungselement seitens des Kommandos Strategische Aufklärung in Schwielowsee implementiert. Die Aufgaben waren in dieser

Zeit im Schwerpunkt auf das Abstimmen der Arbeitsprozesse zwischen dem Kommando Strategische Aufklärung und der Abteilung J2 Militärisches Nachrichtenwesen und Geoinformationswesen der Bundeswehr im Einsatzführungskommando ausgerichtet. Kurz gesagt, ging es rein um das Militärische Nachrichtenwesen. Nach der Einnahme der Arbeitsgliederung CIR 2.0 im August 2021, wurde das Verbindungselement mit neuen Aufgaben hinterlegt. Nun geht es um deutlich mehr. Ab sofort steht die Beratungsleistung in der Einsatzplanung und -führung zu Fähigkeiten und Unterstützungsmöglichkeiten des Organisationsbereichs CIR im Vordergrund. Des Weiteren unterstützt unser Team bei der Koordinierung des CIR-Beitrages mit Blick auf die Einsätze. Dass das Verbindungselement die Ansprechstelle zu allen Aspekten der Dimension CIR ist, versteht sich von selbst. Besonders wenn deutsche Staatsangehörige bei Krisen im Ausland evakuiert werden sollen, ist ein -Element im Einsatzführungskommando vor Ort wertvoll. Vorabinformationen, für zum Beispiel die Operationszentrale im Kommando CIR, können somit unverzüglich übermittelt werden, ohne den Stab des Einsatzführungskommandos damit unnötig zu belasten, dienen aber insbesondere dazu, dem Kommando CIR frühzeitig die eigene Planung zur Unterstützung von Operationen zu ermöglichen.

Haben Sie den Eindruck, dass die Bedeutung der Dimension CIR beim Einsatzführungskommando erkannt wird?

Ein ganz klares Ja! Auch schon vor der Aufstellung des Organisationsbereichs CIR. Das Einsatzführungskommando selbst bezeichnet seine Abteilung J3/5 als „operativen Motor". Man könnte auch sagen, in diesem „Maschinenraum" werden die Einsätze und Missionen der Bundeswehr im Auftrag des Befehlshabers geplant und geführt. Folglich stellt aus meiner Sicht der Beitrag des Organisationsbereichs CIR dann gewissermaßen den Schmierstoff dar. Fehlt ein „CIR-Schmierstoff", zum Beispiel das IT-System Bundeswehr, dann läuft der „operative Motor" nicht mehr richtig rund oder erleidet gar den gefürchteten „Kolbenfresser". Dies betrifft dann auch die Einsatzgebiete.

Wie schaffen Sie es, die große Bandbreite der verschiedenen Fähigkeiten der Dimension CIR in ihrer Komplexität abzubilden sowie einzubringen?

Da ich bisher hauptsächlich im Bereich Militärisches Nachrichtenwesen „unterwegs" gewesen bin, ist dies in der Tat eine große Herausforderung für mich. Schließlich ist dieser Bereich nur eine der verschiedenen Facetten des CIR. Nicht nur deshalb wird unser Verbindungselement frühestens im Oktober 2022 durch einen weiteren Stabsoffizier ergänzt. Dieser Spezialist wird sich im Schwerpunkt in die Handlungsfelder Führungsfähigkeit und IT-System Bundeswehr einbringen.

Darüber hinaus hilft mir die Verbindung zu den mir bereits bekannten Protagonisten der verschiedenen Dienststellen des Organisationsbereichs CIR, die mir noch von der bereits beschriebenen zweiwöchigen Ausbildung bekannt sind. Wenn es darum geht, einen wertvollen CIR-Beitrag in der

◄ Major Tino Borchert ist Angehöriger des Grundsatzreferates der Abteilung Operation im Kommando CIR und Leiter des Verbindungselementes beim Einsatzführungskommando der Bundeswehr.

▼ Major Tino Borchert (re.) und Hauptfeldwebel Markus Wagner (li.) vor dem Dienstgebäude Befehlshaber Einsatzführungskommando.
Foto: Bundeswehr/Marc Tessensohn

▲ Beim „Vulnerable Point-Check" suchen Soldaten des Bataillons Elektronische Kampfführung 931 das Gelände nach behelfsmäßigen Sprengvorrichtungen ab. Hauptwaffensystem ist der Transportpanzer FUCHS CG-20+. Die Abkürzung CG steht für Counter-Improvised Explosive Device (IED) Gerät, den Störsender zur Störung von funkgesteuerten IED.
Foto: Bundeswehr/Stefan Uj

Einsatzplanung aktiv einzubringen, kann dies hier im Einsatzführungskommando im Rahmen von Arbeitsgesprächen mit Personal des Referates „Joint Effects" im Vorfeld abgestimmt werden. Aus meiner Sicht sind dann die Chancen einer Realisierung am größten. Im besagten Referat dienen Spezialisten für die Bereiche Zielplanung, Wirken im elektromagnetischen Spektrum, Operative Kommunikation sowie Cyberoperationen.

Wie halten Sie Verbindung mit dem „Mutterhaus" in Bonn?

Ich hatte mir vorgenommen, meine Dienststelle in Bonn mindestens alle vier Monate aufzusuchen. Das gelingt natürlich – aus verschiedenen Gründen – nicht immer. Daher erfolgt der Informationsaustausch hauptsächlich per Telefon sowie über eine wöchentliche Videoschalte. Und wann immer sich Reisen meiner Bonner Vorgesetzten ins Bundesministerium der Verteidigung nach Berlin mit einem Besuch in Schwielowsee verbinden lassen, wird diese Möglichkeit zum persönlichen Austausch genutzt. Nicht nur aufgrund der Entfernung hat sich dieses Verfahren bewährt. Denn das persönliche Gespräch ist durch nichts zu ersetzen. Auch ist für uns der enge und unkomplizierte Kontakt zur Operationszentrale im Kommando CIR sehr hilfreich.

Sie sagten, dass Sie schon einmal im Einsatzführungskommando in anderer Rolle eingesetzt waren. Wo sehen Sie Gemeinsamkeiten, wo Unterschiede und wie bewerten Sie Ihre zukünftige Rolle?

Aus meiner Sicht können viele Angehörige beider Dienststellen noch immer nicht zuordnen, zu welcher Dienststelle das Verbindungselement eigentlich gehört. Wir sind Angehörige des Kommandos CIR, dienen aber am Dienstort Schwielowsee.

Seinerzeit war ich als Offizier im Militärischen Nachrichtenwesen für die Feldnachrichtenkräfte in den Einsätzen verantwortlich. Als Gemeinsamkeit zu meiner derzeitigen Verwendung möchte ich die „unmittelbare Auswirkung" im Einsatzgebiet hervorheben. Allerdings ist diese jetzt komplexer, da es deutlich mehr Fähigkeiten betrifft. Wie gesagt: Jedes Einbringen von Fähigkeiten wirkt sich unmittelbar bei den Kontingentangehörigen im Einsatz aus; ihr Wegfall natürlich auch!

Bedeutendster Unterschied ist sicherlich jetzt der Umfang der Ressourcen, die in ihrer Art und Fachlichkeit verschiedener nicht sein können. Musste ich mich damals „nur" mit Informationsgewinnung durch Feldnachrichtenkräfte auskennen, so bin ich jetzt auch besser mit beispielsweise operativer Kommunikation, abbildender Aufklärung oder gar Cybersicherheit vertraut. Derzeit kann ich noch nicht abschätzen, wie der Krieg in der Ukraine meine Rolle und Aufgabe verändern wird. Eines ist aus meiner Sicht jedoch gewiss, der Organisationsbereich CIR mit seinem Verbindungselement in Schwielowsee wird seine Relevanz nicht nur im Einsatzführungskommando behalten.

Vielen Dank für das Gespräch!

Das Interview führte PIZ CIR

DR. MATTHIAS WITT, GESCHÄFTSFÜHRER WIMCOM GMBH

B2M – Business-to-Military

Spätestens mit der Entscheidung der signifikanten Erhöhung des Verteidigungsetats machen sich wehrtechnische Unternehmen auch Gedanken über den Zukauf von Unternehmen, die in das eigene Portfolio passen. **Was sind die Besonderheiten von M&A im Military Business**?

Grundsätzlich sind Umsatzsteigerungen im Military Business sowohl mit dem eigenen Produkt- und Serviceportfolio möglich, als auch durch den gezielten Zukauf von wehrtechnischen Unternehmen (Mergers & Acquisitions). Selbstverständlich gilt der Fall auch umgekehrt: Infolge einer guten „Historie" und attraktiver Möglichkeiten zur Umsatzsteigerung, kann das eigene Unternehmen auch zum „Target" werden.

M&A IN MILITARY BUSINESS

Im Rahmen der Bewertung des Unternehmens (Due Diligence) geht es wie bei „zivilen" Unternehmen auch darum, den Geschäftszweck des Unternehmens, das Angebot, Kundenstrukturen, Marktbesonderheiten, die eigene Positionierung, Wettbewerb, etc., zu verstehen. Bedeutende Unterschiede liegen aber bspw. in der Marktbearbeitung. Die Beziehung zum Kunden (BMVg/Bundeswehr) kann nur sehr langfristig entwickelt werden, eine kurzfristige Übergabe von einem Key Account Manager zum anderen gelingt meistens nicht. Darüber hinaus sind die vergaberechtlichen Auflagen, die vertragsrechtlichen Besonderheiten und die preisrechtlichen Vorgaben als Branchenfremder kaum bewertbar. Deshalb ist es besonders vorteilhaft, sich von Experten beraten zu lassen, die das Geschäft wirklich bewerten können und sich insbesondere mit Preis- und Margenbildung bei öffentlichen Aufträgen genau so auskennen wie mit der Vemeidung von vertrags- und preisrechtlichen Risiken.

INVESTITIONSPRÜFUNG DURCH BMWK

Das Bundeswirtschaftsministerium prüft grundsätzlich bei Investitionen aus Drittländern, ob Sicherheitsinteressen betroffen sind. Bedingt durch die vom Bundeskanzler ausgerufene sog. „Zeitenwende", verbunden mit der NATO-Verpflichtung im Rahmen von BV/LV, wird hier genauer geprüft, ob das Leistungsportfolio des zu verkaufenden Unternehmens systemrelevant ist. Die Sicherheitsinteressen der Bundesrepublik Deutschland stehen dabei weiter vorne als in den Jahrzehnten davor. Handelt es sich um den Erwerb eines inländischen Unternehmens im Bereich der Rüstung und Wehrtechnik durch einen ausländischen Investor, kommt das sektorspezifische Prüfverfahren zur Anwendung. Es ist davon auszugehen, dass das Verfahren mindestens zwei, eher aber sechs Monate dauert.

STRATEGIC FIT!?

Neben den o.g. Faktoren ist jedoch die Prüfung auf den „strategic fit" elementar. Dies bedeutet, dass das bisherige Produkt- und Serviceportfolio auf sinnvolle Weise ergänzt wird. Darüber hinaus ist zu prüfen, ob ein geografischer Vorteil durch den Kauf/Verkauf erwächst, weil bisher nicht berücksichtigte Marktanteile in anderen Ländern/Regionen durch die neue Aufstellung bearbeitet werden können. Ein Zukauf ist zunächst immer eine Investition, welche die Marge reduziert. Deshalb ist es so wichtig, dass vorher identifizierte Synergien – bspw. „Shared services", Zusammenlegung von Vertriebsstrukturen, etc. – von Beginn an gehoben werden.

WIMCOM
The Military Business Company

Foto: WIMCOM

KONTAKT:
WIMCOM GmbH
Hermann-Geisen-Straße 70
56203 Höhr-Grenzhausen
Ansprechpartner: Dr. Matthias Witt
Tel.: 02624 94343 10
m.witt@wimcom.de
www.wimcom.de

BRIGADEGENERAL RAINER SIMON, KOMMANDEUR DER
SCHULE INFORMATIONSTECHNIK DER BUNDESWEHR, PÖCKING

Konzeptionelle Grundgedanken und aktuelle Entwicklungen rund um modernes Lernen im Organisationsbereich CIR

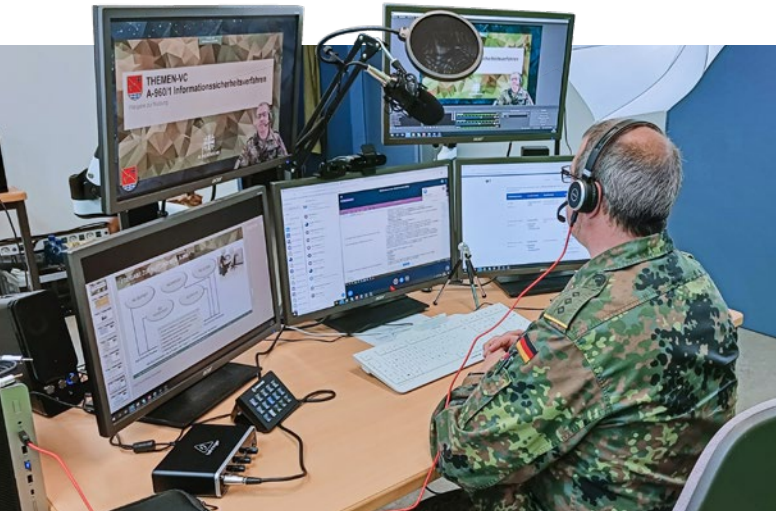
Die Gewinnung und Ausbildung des zukünftigen Nachwuchses aus der „Generation Z" zu handlungsfähigen, einsatzbereiten Soldatinnen und Soldaten stellt neben den besonderen Anforderungen des dynamischen und komplexen Cyber- und Informationsraums (CIR) hohe, zum Teil neue Anforderungen an die Ausbildung. Diesen Herausforderungen gilt es zu begegnen, etwa durch eine moderne und adaptive Lehre, eingebettet in ein leistungsfähiges und agiles Ausbildungssystem, das auf die Änderungen im CIR zeitgerecht reagieren kann. Eine Lehre, die die Möglichkeiten moderner Technologien ausschöpft und individuell auf die Lehrgangsteilnehmenden eingeht.

KONZEPTIONELLE GRUNDGEDANKEN – AUSGANGSLAGE

Das Personal ist seit jeher der wichtigste Aktivposten jeder Organisation, ohne den jede Technik und jede Ausrüstung, alle Prozesse und Verfahren ihre Wirkung nicht entfalten können. Dies gilt auch für die Bundeswehr und damit auch für den Organisationsbereich CIR. Der aktuelle und zukünftige Nachwuchs wird dabei in erster Linie aus der sogenannten „Generation Z" gewonnen, die aus den Geburtsjahrgängen 1997 bis 2012 besteht. Diese Generation der „digital natives" ist von Geburt an in einer Welt mit modernen Medien aufgewachsen und nicht erst später damit konfrontiert worden. Außerdem ist sie die Generation, die inmitten des sogenannten „Fachkräftemangels" und damit in einem deutlich veränderten Ausbildungs- und Arbeitsmarkt ihr Arbeitsleben beginnt. Im Vergleich zu vorhergehenden Generationen ist die Forderung nach flexiblen und individuellen Rahmenbedingungen in der Arbeitswelt bei der Generation Z deutlicher ausgeprägt, um einem gewachsenen gesellschaftlichem Wert nach Betonung des Individuums, den unterschiedlichen Anforderungen von Familie, Beruf, persönlichen Interessen und deren Weiterentwicklung gerecht zu werden. Daher muss gerade im technikaffinen Organisationsbereich CIR die Ausbildung an diese geänderten Voraussetzungen angepasst werden, um dem weiterhin gültigen Ziel gerecht zu werden, charakterlich gefestigte, handlungsfähige Soldatinnen und Soldaten für die gesamte Bundeswehr zu erziehen und auszubilden, die im Grundbetrieb, im Einsatz und in der Landes- und Bündnisverteidigung (LV/BV) bestehen können. Außerdem liegt es auf der Hand, dass der für die Digitalisierung in den Streitkräften verantwortliche Organisationsbereich CIR auch Motor, Treiber und Innovator für moderne Ausbildungstechnologie und damit verbunden für Methodik und Didaktik werden kann. Die Schule für Informationstechnik der Bundeswehr (ITSBw) ist dabei bereits heute Vorreiter und Weichensteller.

VERÄNDERTE LERNUMGEBUNG, MODERNE METHODIK

Aus der zunehmenden Bedeutung des CIR folgt auf absehbare Zeit auch ein wachsender Bedarf in Qualität und Quantität an Ausbildung für den CIR. Um diesen decken zu können, bedarf es vor allem einer modernen Lehre. Bindeglied zwischen Lehrendem und Lernendem ist dabei die Methodik und Didaktik, die sich genauso wie die Inhalte an die Möglichkeiten moderner Technologien und an veränderte Rahmenbedingungen anpassen müssen. Eine „Lernkultur 4.0" ist das Ziel, wir müssen Lernräume schaffen, in denen unsere Soldatinnen und Soldaten ein Umfeld für konstruktive Lernerfahrungen erleben können, in denen Raum für vielfältige, differenzierte Lernsituationen möglich ist und in dem sich Lernende Kompetenzen in unterschiedlichen Wissensdomänen weitgehend selbständig aneignen können. Modernes Lernen im Sinne eines adaptiven, individuell steuerbaren, flexiblen und digitalen Lernens ist dabei Chance und Herausforderung zugleich. Es bieten sich enorme Möglichkeiten, um dem jeweiligen Wissenstand und den Bedürfnissen der einzelnen Person gerecht zu werden, indem der individuell passende Anknüpfungspunkt bereitgestellt und zum jeweils passenden Zeitpunkt abgerufen wird. Gleichzeitig ändert sich die Ausbildersicht weg von einer Lerngruppe mit einem gemeinsamen Abholpunkt hin zu einer Gruppe von Individuen mit vielen unterschiedlichen Abholpunkten. Der Ausbildende ist damit viel weniger als bisher



„Sender“ von Informationen, sondern viel mehr Lernbegleiter oder Coach der Lernenden auf ihrem jeweils individuellen Weg. Das erfordert von Ausbildenden nicht nur fachliche Kompetenz, Empathie und Flexibilität, sondern auch eine solide Basis an Wissen und Fähigkeiten im Bereich Methodik und Didaktik, da die Tätigkeit des Lehrens deutlich weniger vorausplanbar ist. Im Gegenzug steigt auf der Seite des bisherigen „Empfängers“ die Eigenverantwortung eines jeden Lernenden, sich die jeweils erforderlichen Ausbildungsinhalte zum selbst gewählten Zeitpunkt eigenverantwortlich zu erarbeiten – auch wenn das Ausbildungspersonal just in dem Moment nicht unmittelbar verfügbar ist.

Die Flexibilisierung der Ausbildung bedeutet aber nicht, dass das klassische Präsenzlernen seine Bedeutung verloren hat. Ganz im Gegenteil, das übergeordnete Ziel, der an Grundbetrieb, Einsatz und LV/BV ausgerichtete Kompetenzerwerb, erfordert auch weiterhin das Lernen am Gerät, am System, unter einsatznahen Bedingungen. Das Erleben von Kameradschaft, gegenseitiges Kennenlernen und Vertrauen sind essentielle Bestandteile unserer militärischen Führungs- und Ausbildungskultur und bleiben unverzichtbarer Bestandteil der Ausbildung und Erziehung. An der IT-Schule der Bundeswehr wird deswegen kontinuierlich weiter der Ansatz des „Blended Learnings“ verfolgt – dort, wo es möglich ist, wird flexibel mit den unterschiedlichen Formen des E-Learnings wie Virtual Classrooms oder im Lernmanagementsystem gearbeitet. Gleichzeitig wird an den Stellen, an denen die Ausbildung vor Ort in Präsenz den höheren Lernerfolg verspricht, auch weiterhin so ausgebildet. Neben anderen Faktoren war die COVID-19-Pandemie der vergangenen zwei Jahre ein starker Katalysator, der an der IT-Schule in kurzer Zeit große Fortschritte insbesondere im Hinblick auf ortsunabhängiges Lernen und der dafür erforderlichen geänderten Lehrmethoden ermöglicht oder wohl eher erzwungen hat. Dieses Momentum gilt es nun zu nutzen, um das künftige Ausbildungszentrum CIR zu einem Centre of Excellence für moderne Methodik, Didaktik und Ausbildungstechnik werden zu lassen, von dem alle Fähigkeiten CIR und vor allem alle Ausbildungseinrichtungen der Bundeswehr über die Grenzen des Organisationsbereichs hinaus profitieren können.

Unverzichtbares Medium für flexibles Lernen ist dabei eine digitale Ausbildungsumgebung, die möglichst jederzeit und bedarfsgerecht Zugriff auf die Lerninhalte gewährt, gleichzeitig aber den besonderen Schutzbedürfnissen militärischer Lerninhalte gerecht wird. Das Ausbildungsnetz der IT-Schule wird bereits jetzt in den Informationsräumen „Offen“ und „VS – Nur für den Dienstgebrauch“ an vielen Ausbildungseinrichtungen der Bundeswehr erfolgreich genutzt und wird auch die Basis der Ausbildung im Ausbildungszentrum CIR bilden. Dabei ist die Erweiterung auf den Informationsraum „Geheim“ beziehungsweise „NATO SECRET“ bereits projektiert, in Zukunft können also auch entsprechend eingestufte Inhalte verbreitet und bereitgestellt werden. Wichtig ist in diesem Zusammenhang auch die Erstellung der Lehrmittel in der Lernumgebung. Um dem oben aufgezeigten Verständnis von Lernkultur gerecht werden zu können, müssen die Anforderungen an sie deutlich über das bisher gewohnte Maß von Ausbildungsunterlagen und Skripten hinausgehen und erfordern multimediale Kompetenzen. Die Konzeptionierung und Erstellung kann nicht allein durch das Lehrpersonal erfolgen, sondern erfordert eine „digitale Lehrmittelwerkstatt“ mit entsprechenden Fähigkeiten und Ressourcen. Erste vielversprechende Ansätze dazu sind an der IT-Schule bereits abgebildet. Über ein reines Lernmanagementsystem hinaus bietet das Ausbildungsnetz bereits heute virtuelle Ausbildungsumgebungen, bisher vor allem im Bereich der IT-Ausbildung. Fernziel ist es dabei, jedes Gerät in Form eines „digitalen Zwillings“ in das virtuelle Gesamtsystem einzubinden. Damit bieten sich nicht nur Möglichkeiten zur Ausbildung, sondern auch zur Erprobung von Konfigurations-Baselines der Systeme oder zur Bearbeitung komplexer Lagen, beispiels-

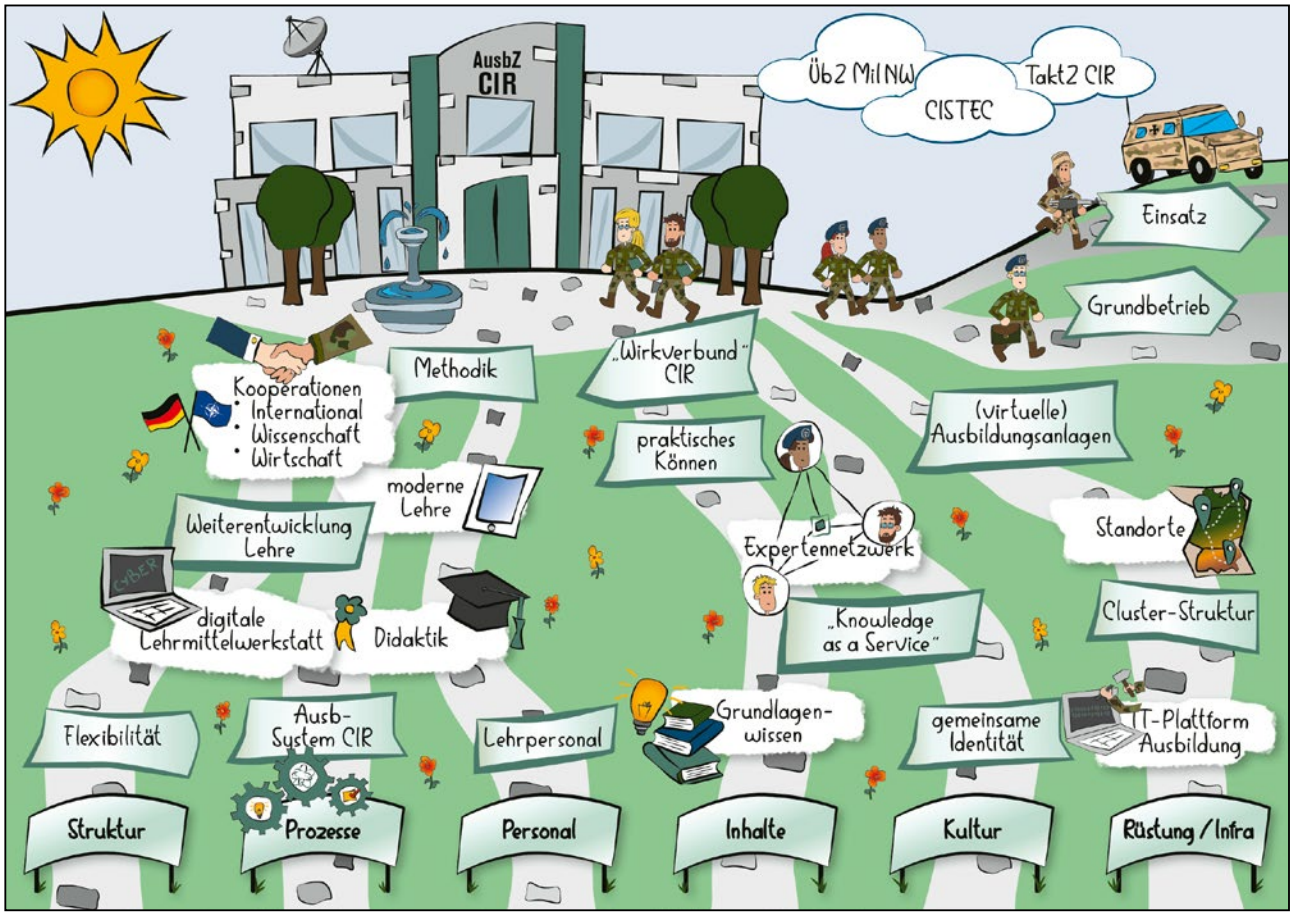
▲ Modernes Lernen im Sinne eines adaptiven, individuell steuerbaren, flexiblen und digitalen Lernens ist dabei Chance und Herausforderung zugleich.
Fotos: Bundeswehr/ITSBw

weise unter Cyberbedrohung. Die Erstellung der „digitalen Zwillinge" lässt sich dabei nur in enger Zusammenarbeit des Ausbildungszentrums mit dem Zentrum für Digitalisierung der Bundeswehr und der Einbringung dieser Forderung in den Rüstungsprozess realisieren, muss aber nach unseren Vorstellungen inhärenter Bestandteil aller Projekte werden. Neben der stetigen Weiterentwicklung von Methodik und Didaktik müssen auch die Inhalte der Ausbildung permanent weiterentwickelt werden. Änderungen im taktisch/operativen Bereich oder technische Neuerungen sind zeitgerecht in der Ausbildung abzubilden. Außerdem erfordert es gerade die Schnelllebigkeit der Technologien des CIR, dass das Ausbildungssystem bei Trends und Neuerungen „vor die Welle" kommt. Wir müssen eine Angebotssituation schaffen, zukünftig erforderliche Ausbildungsinhalte proaktiv erkennen und erarbeiten und nicht erst über die notwendige Ausbildung beginnen nachzudenken, wenn die Lösung mittels eines Produkts oder Service formal im Zuge etwa des Rüstungsprozesses bereitgestellt wird. Dazu gilt es, das Ausbildungszentrum CIR sowohl innerhalb der Bundeswehr als auch außerhalb mit Industrie und Forschung zu vernetzen und Kooperationen zu bilden.

AUSBILDUNGSLANDSCHAFT/ AUSBILDUNGSSYSTEM CIR 2.0

Der wesentliche Träger des Ausbildungssystems CIR wird das Ausbildungszentrum CIR. In diesem werden nicht nur die Ausbildungseinrichtungen Schule für Strategische Aufklärung der Bundeswehr und Schule für Informationstechnik der Bundeswehr zusammengeführt, sondern auch wesentliche Teile des Ausbildungsmanagements aus den beiden ehemaligen „Zwei-Sterne-Kommandos" und dem Kommando CIR. Neben dieser zentralen Ausbildungseinrichtung werden im Zentrum Cyber-Operationen, Zentrum für Geoinformationswesen der Bundeswehr und Zentrum für Operative Kommunikation der Bundeswehr aufgrund ihrer jeweiligen Besonderheiten weiterhin wesentliche Teile der Ausbildung in ihren jeweiligen Fähigkeiten durchgeführt werden. Außerdem wird die Grundausbildung für den Organisationsbereich in den etablierten Einheiten verbleiben. Natürlich wird auch zukünftig die Ausbildung in der Truppe ein wesentlicher Pfeiler des Ausbildungssystems CIR sein. Weitere Handlungsfelder müssen erschlossen werden, beispielsweise die Kooperation mit Bildungspartnern und der Industrie und die Qualitätssicherung von Maßnahmen der zivil anerkannten Weiterbildung.

Die genannten strukturellen Veränderungen bedeuten allerdings nicht, dass hunderte von Soldatinnen und Soldaten, Mitarbeiterinnen und Mitarbeitern ihren Dienstort verlieren. Alle bisherigen Standorte der Ausbildungslandschaft werden beibehalten und wo doch Aufgaben oder Dienstposten räumlich verlagert werden müssen, werden hierzu auf der Zeitachse sicherlich sachgerechte Lösungen gefunden werden. Ziel dieser Neuordnung der Ausbildungslandschaft ist es, Schnittstellen zwischen den Hierarchieebenen und Fähigkeiten CIR zu reduzieren und Entscheidungswege zu verkürzen, um das Ausbildungssystem agiler an die schnelllebigen Erfordernisse „unseres" CIR anpassen zu können. Führung aus einer Hand ist



hierfür sicherlich ein treffendes Schlagwort. Besonders die Zusammenlegung des Ausbildungsmanagements und die Harmonisierung der Lehrgangslandschaft mit Augenmaß bieten hier viel Optimierungspotential. Von den Grundlagen wie Lernziel- oder Kompetenzdefinitionen bis zum Qualitätsmanagement kommen hier alle Bestandteile fähigkeitsübergreifend zusammen. Entwicklungen aus dem Rüstungsprozess, Planungen anderer Organisationsbereiche und Erfahrungen aus Grundbetrieb, Übung oder Einsatz werden zentral aufgenommen und bewertet. Somit bietet sich die Möglichkeit, notwendige Änderungen der Ausbildung übergreifend zu adressieren, etwa in der lehrgangsgebundenen Individualausbildung oder in der Truppenausbildung – oder auch in beidem!

Ein weiterer innovativer Ansatz, der für das Ausbildungszentrum CIR intensiv geprüft wird, besteht in der Trennung von Lehre und truppendienstlicher Führung. Ziel ist es dem Lehrpersonal zu ermöglichen, sich auf die immer anspruchsvolleren Inhalte der Lehre zu konzentrieren, indem es weitestgehend von administrativen Tätigkeiten entlastet wird. Dies würde, zumindest für die militärfachlichen Trainings, nicht weniger als die Abkehr vom bekannten Modell der Inspektionen mit Hörsaalleitern bedeuten, in denen Betreuung, Administration und Lehre vom selben Personal geleistet werden muss. Die bisher in diesen Strukturen wahrgenommen Aufgaben der Planung und Organisation würden in ein zentrales Ressourcenmanagement einerseits und in eine Anzahl an Betreuungsstellen, analog zum bereits bisher in der zivil anerkannten Weiterbildung der Portepeeunteroffiziere, überführt. Die truppendienstliche Betreuung der Trainingsteilnehmenden würde in einem erforderlichen Mindestmaß durch diese Betreuungsstellen, bestehend aus Disziplinarvorgesetzten und Innendienstpersonal, sichergestellt, darüber hinaus organisierten sie sich anhand des Dienstplans weitestgehend selbst. Das Lehrpersonal, nunmehr ausschließlich Fachlehrer, könnte sich somit auf Durchführung, aber auch Weiterentwicklung der Lehre konzentrieren.

MEHRWERT CIR IN DER AUSBILDUNG

Die Zusammenfassung des Managements der lehrgangsgebundenen Individualausbildung als ein Bestandteil des Ausbildungsmanagements bietet eine gute Grundlage, um in weiteren Schritten über alle Fähigkeiten CIR hinweg die Inhalte oder gar Trainingstypen zu harmonisieren und neue, fähigkeitsübergreifende Trainings zu entwickeln sowie ein übergreifendes, gemeinsames Verständnis CIR zu fördern. Insgesamt liegen in dieser fähigkeitsübergreifenden Betrachtung die Chancen, einerseits die knappen Ausbildungsressourcen effektiver und effizienter zu nutzen und andererseits den Mehrwert eines wirklich gemeinsam gedachten und gelebten CIR zu erreichen. Daher wird auch die Ausbildung der Dimension CIR als Ganzes einen prominenten Anteil im Trainingsangebot in der Zukunft einnehmen. Über die letztendliche, bereits konzeptionell angelegte Abbildung der Aus-, Fort und Weiterbildung in einer flexiblen und (Einsatz-)realitätsnahen Lern-, Übungs- und

◀ Ausblick auf das zukünftige Ausbildungszentrum CIR, das im April 2024 aufgestellt wird.
Grafik: Bundeswehr/ITSBw

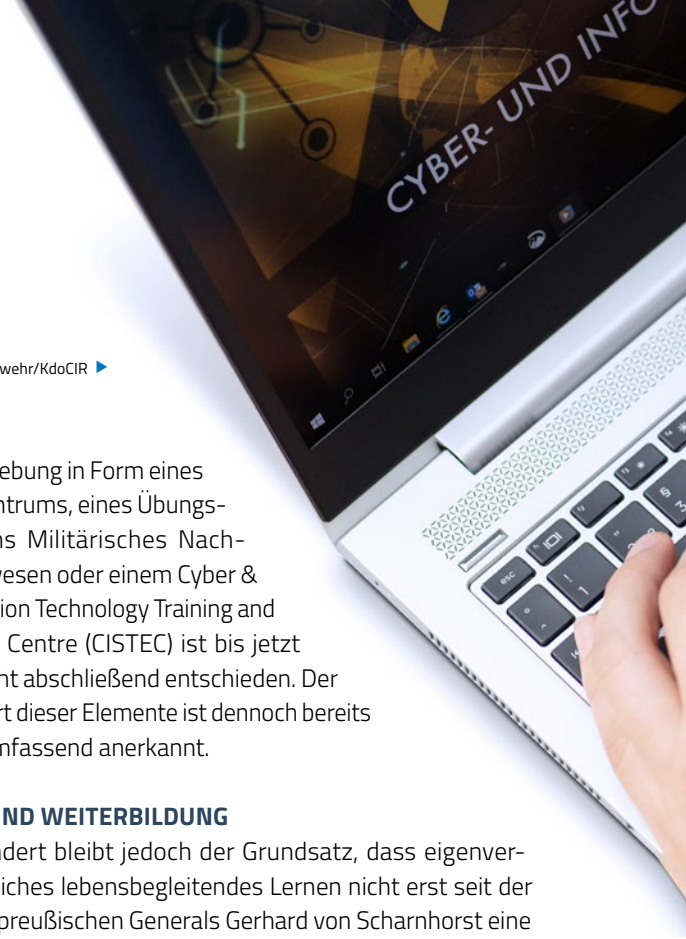


Foto: Bundeswehr/KdoCIR ▶

Testumgebung in Form eines Taktikzentrums, eines Übungszentrums Militärisches Nachrichtenwesen oder einem Cyber & Information Technology Training and Exercise Centre (CISTEC) ist bis jetzt noch nicht abschließend entschieden. Der Mehrwert dieser Elemente ist dennoch bereits heute umfassend anerkannt.

FORT- UND WEITERBILDUNG

Unverändert bleibt jedoch der Grundsatz, dass eigenverantwortliches lebensbegleitendes Lernen nicht erst seit der Zeit des preußischen Generals Gerhard von Scharnhorst eine elementare Anforderung des Soldatenberufs ist. Insbesondere in der Dimension und im Organisationsbereich CIR hat dies, aufgrund der Schnelllebigkeit und der Komplexität des CIR und der mit ihm verbundenen Technologien und sozioökonomischen Wirkmechanismen, eine noch größere Bedeutung gewonnen. Kenntnisse und Fertigkeiten veralten schneller und die Dimension selbst verändert sich nahezu täglich – anders als die althergebrachten, physischen Dimensionen Land, Luft und See. Aus diesen Gründen muss in Zukunft auf allen Ebenen der Fort- und Weiterbildung mehr Raum gewährt und das Angebot an Maßnahmen ausgeweitet werden. Dazu könnte auf die oben bereits erwähnten, vergleichsweise kompakten Trainingsmodule zurückgegriffen werden. Denkbar ist, die Weiterbildung (innerhalb und außerhalb der Bundeswehr) in eine Systematik zu fassen, etwa Qualifikationen – wie bereits heute in Einzelfällen – mit einem „Verfallsdatum" zu versehen und regelmäßige Weiterbildungen über Anreize attraktiver zu gestalten.

HERAUSFORDERUNGEN

Da wie eingangs erwähnt die „Ressource Mensch" in jeder Organisation erfolgskritisch ist, stellt die Verfügbarkeit von motivierten und qualifizierten Mitarbeitern die größte Herausforderung dar, um die beschriebenen Strukturen und Prozesse mit Leben zu füllen. Mit dieser Herausforderung ist das Ausbildungssystem CIR nicht allein, sowohl innerhalb der Bundeswehr als auch gesamtgesellschaftlich muss in Zukunft „mehr" und „besser" mit immer „weniger" erreicht werden. Der Schlüssel zum Erfolg des Ausbildungssystems CIR liegt daher vor allem darin, das Neue, das – vielleicht – Visionäre mit dem Machbaren zusammenzubringen. Unabhängig davon sind eine leistungsfähige, starke, mit ausreichend Ressourcen hinterlegte Ausbildungsorganisation und moderne Lernkultur die entscheidenden Grundpfeiler für einsatzbereite und einsatzfähige Streitkräfte.

Unser Ziel ist es,
unser CIR-Verständnis
zu fördern und zu leben.

Sehr geehrte Leserin, sehr geehrter Leser,

in unserem Sonderheft „CIR 2.0 – Von der Idee zur Dimension" haben wir Ihnen die ganze Bandbreite der Aufgaben unseres Organisationsbereichs dargestellt. Sie konnten sich davon überzeugen, welche Fülle von spannenden und relevanten Fähigkeiten wir unter dem Dach des Cyber- und Informationsraums der Bundeswehr betrachten und darstellen.

Wir verstehen uns als Enabler der klassischen Teilstreitkräfte. Gleichzeitig planen und führen wir jedoch auch eigenständig CIR-Operationen, die das gesamte Spektrum von Aufklärung, Wirkung, Betrieb und Schutz abdecken. Darüber hinaus gewährleisten wir in unserer Rolle als „Treiber der Digitalisierung der Bundeswehr", dass alle Bereiche unserer Streitkräfte von den Vorteilen der Digitalisierung profitieren und diese auch adäquat umsetzen und nutzen können.

Wie wichtig die Fähigkeiten aus unserem Organisationsbereich CIR sind, zeigt sich im Angriffskrieg Russlands gegen die Ukraine; sei es bei der Aufklärung militärischer Potentiale, dem Betrieb und Schutz von IT-Systemen, den Effekten und Wirkungen im CIR oder sei es bei der Unterstützung mit Geoinformationen. Zudem tritt durch die Geschehnisse zutage, wie mangelhafte Führungsfähigkeit die Operationsführung von Streitkräften beeinträchtigt. Vor diesem Hintergrund ist die Führungsfähigkeit neben der persönlichen Ausstattung eines jeden Soldaten das zweithöchst priorisierte Handlungsfeld unserer Ministerin sowie des Generalinspekteurs, insbesondere bei der Materialbeschaffung im Zuge des mit 100 Milliarden Euro bezifferten Sondervermögens. Mit dieser Investition wird die Bundeswehr und natürlich auch der Organisationsbereich CIR bestmöglich für die Herausforderungen der Landes- und Bündnisverteidigung vorbereitet. Dabei wird auch unserer Bedeutung im Rahmen der gesamtstaatlichen Sicherheitsvorsorge Rechnung getragen.

Die aktuellen Entwicklungen offenbaren darüber hinaus, wie wichtig es ist, sich neuen Gegebenheiten anzupassen, sich auch in der Organisation flexibel weiterzuentwickeln. Wir legen mit CIR 2.0 dafür die notwendigen Grundlagen. Wir verschlanken unsere Strukturen und optimieren unsere Prozesse, um zukünftig noch schneller und effektiver agieren zu können. Die vollständige Umsetzung von CIR 2.0 und damit der Abschluss unserer Neuausrichtung ist bis 2025 geplant. Einen Meilenstein stellt dabei die Aufstellung des Zentrums Digitalisierung der Bundeswehr im Oktober 2022 dar.

Die Neuausrichtung unseres Organisationsbereichs wird es uns ermöglichen, noch fokussierter in unseren beiden Markenkernen zu agieren. Wir werden unsere Fähigkeiten zum Planen und Führen von CIR-Operationen aus einer Hand insbesondere im Kontext der Bündnis- und Landesverteidigung ausbauen. Als Treiber der Digitalisierung der Bundeswehr werden wir hierfür im eigenen Organisationsbereich sowie darüber hinaus für die gesamten Streitkräfte die konzeptionellen und planerischen

◀ Übergabe der Führung über den Organisationsbereich Cyber- und Informationsraum am 25. September 2020 in Bonn an Vizeadmiral Dr. Thomas Daum.

▶ Ansprache bei der Verleihung von Ehrenkreuzen in Silber und Gold an Soldatinnen und Soldaten für herausragende Leistungen, darunter auch die Rettung von Leben.

Fotos: Bundeswehr/Stefan Uj

Voraussetzungen schaffen. Wir werden zudem die Nutzung der Dimension Weltraum für unsere CIR-Fähigkeiten eng begleiten. Dies werden wir national wie international eng in unsere bestehenden Kooperationen einbetten.

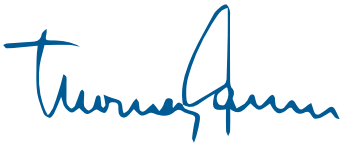
Ein Leuchtturmprojekt der internationalen Kooperation wird dabei das PESCO-Projekt der EU, das „Cyber and Information Domain Coordination Centre" (CIDCC), sein. Aber auch in der NATO sowie in bestehenden und neuen bilateralen Kooperationen werden wir gemeinsam mit Alliierten und Partnern auf die Zeitenwende in der europäischen Sicherheitspolitik und neue Bedrohungen reagieren. Im nationalen Bereich werden wir ebenfalls im Lichte der geänderten Lage in Europa unsere bestehenden Kooperationen vor allem im Bereich der Cybersicherheit intensivieren, um die Verteidigung Deutschlands im Cyber- und Informationsraum noch effektiver zu gestalten.

Zu guter Letzt ist ein diverser Personalkörper von entscheidender Bedeutung für eine erfolgreiche Aufstellung für die Zukunft. Ich habe diesen Aspekt bereits in meinem einleitenden Vorwort hervorgehoben und will es an dieser Stelle noch einmal aufgreifen: der Mensch steht für uns im Mittelpunkt. Um dem Fachkräftemangel im hartumkämpften Markt für IT-Personal zu begegnen, wurde durch das Kommando CIR das Cyber/IT Evaluation Center (CITEC) etabliert. Damit versuchen wir fachlich versiertes und sehr gut ausgebildetes Bestandspersonal zu identifizieren und mit unterschiedlichsten Maßnahmen an uns zu binden.

Unser Ziel ist es, unser CIR-Verständnis zu fördern und zu leben. Wir wollen offen für Veränderungen sein und diese als Chance verstehen. Wir stellen Bestehendes infrage, bauen Überbürokratisierung im militärischen Führungsprozess ebenso wie mangelhafte Fehlerkultur zugunsten von Geschwindigkeit und Agilität, wo immer möglich, ab.

Als Organisationsbereich Cyber- und Informationsraum gibt es uns nun bereits seit fünf Jahren. Damit stehen wir aber gerade einmal am Anfang unserer Geschichte. Wir haben seit unserer Aufstellung bereits Vieles auf den Weg gebracht und aufgebaut. Wir haben unsere Struktur in der kurzen Zeit unseres Bestehens hinterfragt, um unser Handeln noch einmal zu optimieren, stets mit dem Ziel, unsere Aufgaben effektiv und effizient bewältigen und umsetzen zu können. Ich bin daher ganz sicher, dass wir unsere bisherige Erfolgsgeschichte – wie skizziert – gemeinsam weiterschreiben, um auch in Zukunft Deutschland im Cyber- und Informationsraum bestmöglich zu verteidigen.

Ihr



Dr. Thomas Daum
Vizeadmiral

▲ Besuch des Basiscamps auf dem Truppenübungsplatz in Baumholder, wo das IT Bataillon 281 aus Gerolstein sich für die VJTF vorbereitet.
Foto: Bundeswehr/Stefan Uj

DIENSTSTELLEN-PROFIL

ZENTRUM DIGITALISIERUNG DER BUNDESWEHR UND FÄHIGKEITSENTWICKLUNG CYBER- UND INFORMATIONSRAUM

Unter einem Dach werden die Verantwortung für die Fähigkeitsentwicklung im CIR, die planerischen Aufgaben für das Teilportfolio Cyber/IT und damit die Aufgabe als wesentlicher „Treiber der Digitalisierung der Bundeswehr" gebündelt.

AUFGABEN

- Verantwortet die Erstellung der konzeptionellen Grundlagen sowohl für die Fähigkeitsentwicklung CIR als auch die Digitalisierung der Bundeswehr.
- Entwickelt die Fähigkeiten des OrgBer CIR weiter und unterstützt kontinuierlich den Aufbau der Digitalisierungsplattform Bundeswehr.
- Entwickelt selbstständig oder in Kooperationen Anwendungssoftware für den Geschäftsbereich BMVg.
- Stellt eine durchgängige Qualitätssicherung, die entsprechende Nachweisführung und die nationale Abnahme für IT-Systeme sicher.

AUFTRAG

Das Zentrum Digitalisierung der Bundeswehr (ZDigBw) ist direkt dem Kommando CIR unterstellt. Es wurde mit dem Ziel der Verbesserung der Aufgabenwahrnehmung „Fähigkeitsentwicklung CIR", des „Bedarfsträgers für das Teilportfolio Cyber/IT" sowie der Rolle „Treiber der Digitalisierung der Bundeswehr" aufgestellt. Als der Kompetenzträger für Digitalisierungsaufgaben des Organisationsbereichs CIR (OrgBer CIR) verantwortet das ZDigBw dimensionsspezifisch die Entwicklung der Fähigkeiten der Bundeswehr sowie die planerischen Aufgaben im Teilportfolio Cyber/IT einschließlich eines Innovationsmanagements und stellt die zugehörige Methodenkompetenz zur Verfügung. Es nimmt die bundeswehrgemeinsame Fähigkeitsentwicklung und die Koordinierung für das Militärische Nachrichtenwesen, die Elektronische Kampfführung, die Operative Kommunikation, das Geoinformationswesen der Bundeswehr sowie die Informationssicherheit wahr. Das Zentrum stellt eigene Fähigkeiten zur Softwareentwicklung und für Integrationsleistungen von IT-Services in das IT-System der Bundeswehr bereit. Gleichzeitig werden Fähigkeiten zur Freigabe zur Nutzung von IT-Services, zu deren Qualitätssicherung und zur technischen Bereitstellung von Plattformen für Experimente und Erprobung vorgehalten. Dabei vertritt das ZDigBw den OrgBer CIR in nationalen und multinationalen Gremien im Aufgaben- und Verantwortungsbereich in enger Abstimmung mit dem Kommando CIR (Abt PlgCIR/DigBw) und stellt eine ganzheitliche Expertise im Bereich Künstliche Intelligenz bereit.

ANSCHRIFT
Godesberger Allee 115-121,
53175 Bonn

DIENSTSTELLENLEITUNG
Oberst i.G. Michael Volkmer

STAMMPERSONAL
~780

AUFSTELLUNG
01.10.2022

IMPRESSUM

HERAUSGEBER
cpm Communication Presse Marketing GmbH
Saime-Genc-Ring 22 | D-53121 Bonn
Tel. +49 (0)228/9268597-10 | info@cpm-verlag.de
www.cpm-verlag.de
Amtsgericht Bonn | Handelsregister Nr: HRB 24687
Geschäftsführer: **Tobias Ehlke**
Prokurist: **Tom Specht**
Assist. der Geschäftsführung: **Ursula Willig-Marnett**

REDAKTION
Chefredakteur: **Rainer Krug** *(RK)*
CvD u. Stellv. Chefredakteur: **Matthias Wunsch** *(MW)*
Hauptstadt Korrespondent: **Christian Wolf** *(CW)*
Lektorat: **Frauke Wendt**

ANSCHRIFT REDAKTION
Saime-Genc-Ring 22 | D-53121 Bonn
Tel. +49 (0)228/9268597-10
redaktion@cpm-verlag.de

VERTRIEB UND ANZEIGENVERWALTUNG
Leiter Vertrieb: **Christian Lauterer**
Kundenbetreuung: **Liza Wirges**

LAYOUT
Norman Greis

PRODUKTIONSMANAGEMENT / VERSAND
Berk-Druck GmbH – Medienproduktion
Oderstraße 5-7 | D-53879 Euskirchen

Wir danken dem Hauptsponsor CGI für seine Unterstützung bei dieser Ausgabe.

Ein ganz besonderer Dank gilt Martina Pump, der Projektleiterin für diese Ausgabe aus dem PIZ CIR. Vielen Dank für die stets verlässliche und zielführende Zusammenarbeit!

INSERENTENVERZEICHNIS

THE MILITARY PUBLISHERS

cpm DEFENCE NETWORK

IHR VERTRAUEN IST UNSERE MOTIVATION

Partnerschaft für Sichtbarkeit und Reichweite

cpm SILVER PARTNER 2022

HIL

LITEF

AIRBUS

STEEP THIS WAY UP

SCANIA

RUAG

ND SATCOM

cpm GOLD PARTNER 2022

SAAB

MBDA MISSILE SYSTEMS

ESG DEFENCE + PUBLIC SECURITY

DND Dynamit Nobel Defence

cpm BRONZE PARTNER 2022

BOEING

HENSOLDT Detect and Protect.

<CONDOK>

KMW A COMPANY OF KNDS

AEROMARITIME

DIEHL Defence

RENK

ELT ELETTRONICA GROUP

38W Cases of Success

Metrohm

GENERAL DYNAMICS European Land Systems

www.cpm-verlag.de

thalesgroup.com

THALES

Building a future we can all trust

Helping you harness the extraordinary power of technology to **build a future we can all trust**

Search: Thalesgroup