wt wehr technik Spezial 2020

SEIT 1968 wt-wehrtechnik

G 4949
52. Jahrgang
ISSN 0043-2172

3 Jahre Organisationsbereich CIR

Kompetenz in einer neuen Dimension

Throughout the world!

Mönch Publications

Spanish
Published quarterly

English
Published monthly

English
(Special Issue)

English
Published bi-monthly

Arabic
Published bi-monthly

German
Published bi-monthly

Italian
Published monthly

Mönch Verlagsgesellschaft mbH

Christine-Demmer-Str. 7
53474 Bad Neuenahr-Ahrweiler
Germany
Tel.: +49-2641 / 3703-0
Fax: +49-2641 / 3703-199
E-Mail: marketing@moench-group.com
www.monch.com

Grußworte

Fähigkeiten

Personal

Kooperation

Blick in die Zukunft

Inserentenverzeichnis

Mönch Verlagsgesellschaft mbH

Christine-Demmer-Straße 7
53474 Bad Neuenahr-Ahrweiler
Germany

Tel.: +49(0)2641 3703-0
Fax: +49(0)2641 3703-199
E-Mail: wehrtechnik@moench-group.com
www.monch.com

Geschäftsführende Gesellschafter und Herausgeber:
Volker Schwichtenberg
Uta Schwichtenberg (Rechtsanwältin)
Stv. Verlagsleitung: Christa André
Mit-Herausgeber: Christian Lauterer
Gestaltung: Frank Stommel
Titelbild: Bundeswehr / Andreas Wiemer
Dokumentation: Ernst Schlegel

Erscheinung: April 2020

Druck: DCM Druck Center Meckenheim GmbH
Werner-von-Siemens-Straße 13, 53340 Meckenheim

Irrtum vorbehalten. Minderungsansprüche wegen Unvollständigkeit oder Fehlerhaftigkeit sind ausgeschlossen. »wehrtechnik« erscheint mit sechs Ausgaben jährlich und kostet im Jahresabonnement ab 2015 € 75,- (Inland) bzw. € 80,- (Ausland) inkl. Portokosten (Luftpostzuschlag € 40,-); Einzelheft € 14,50 zuzüglich Versandkosten.
Vertrieb: Mönch Verlagsgesellschaft mbH
Christine-Demmer-Straße 7 - 53474 Bad Neuenahr-Ahrweiler

Drei Jahre CIR, eine Standortbestimmung

(Foto: Bundeswehr / Martina Pump)

Liebe Leserinnen und Leser,

Kinder lernen in ihren allerersten Lebensjahren am meisten. Krabbeln, laufen, immer eigenständiger zu handeln. Dieses Heft erscheint zum dritten Geburtstag unseres Organisationsbereichs Cyber- und Informationsraum (CIR). Auch wir haben in unseren ersten Jahren eine steile Entwicklungskurve hingelegt. Anfang 2016 waren wir nicht viel mehr als eine Idee. Im April 2017 nahm dann zuerst das Führungskommando des neuen Bereichs mit zunächst rund 260 Angehörigen den Dienst auf. Drei Jahre später blicken wir auf einen bundesweit aufgestellten Organisationsbereich mit rund 14.500 Frauen und Männern, der die Verantwortung für die neue „fünfte Dimension", den Cyber- und Informationsraum, ganzheitlich aus einer Hand wahrnimmt.

Ein Einsatz der Bundeswehr, der ohne von uns bereitgestellte Fähigkeiten auskommt, ist mittlerweile undenkbar. Unser Personal leistet seinen Beitrag in den Auslandseinsätzen, sowohl vor Ort als auch aus dem Reach Back in der Heimat. Als einziger militärischer Organisationsbereich nehmen wir dabei zwei unterschiedliche Rollen wahr. Wir waren, sind und bleiben in unserem Selbstverständnis „Enabler" für die deutschen Streitkräfte. Zugleich sind wir jedoch auch zu eigenständigen und streitkräftegemeinsamen Operationen in der Lage. Die „Wirkung" als Wesenskern dieser letztgenannten Rolle erzielen die klassischen Teilstreitkräfte in der Regel als kinetischen Effekt. Wir hingegen nutzen die neue militärische Dimension, um durch den Cyberraum, das Elektromagnetische Spektrum oder das Informationsumfeld unsere Wirkung zu erzielen. Hierzu halten wir die Fähigkeiten Cyberoperationen, Elektronischer Kampf und Operative Kommunikation vor.

Zu all diesen Aspekten finden Sie in diesem Heft Beiträge, die darstellen, wie wir uns seit unserer Aufstellung entwickelt haben und welche aktuellen Fragestellungen uns jeweils beschäftigen.

In diesen Tagen, kurz vor Erscheinen des Hefts, sieht sich das ganze Land einer nie dagewesenen Herausforderung gegenüber – hier in der Heimat. Das Coronavirus fordert uns alle in einem beispiellosen Ausmaß. Einerseits ist buchstäblich jeder gefordert, die Ausbreitung zu verlangsamen und andererseits muss auch die Bundeswehr dazu beitragen, die Handlungsfähigkeit des Staates sicherzustellen. Auch der Organisationsbereich CIR leistet hierzu natürlich seinen Beitrag. So haben unsere Softwareentwickler innerhalb weniger Tage eine Online-Interessenten-Datenbank programmiert, um die Registrierung und Identifizierung von Reservistinnen und Reservisten im Sanitätsdienst der Bundeswehr zu vereinfachen. Daneben haben wir in kürzester Zeit ein virtuelles Dashboard für das Corona-Lagezentrum im BMVg entwickelt. Dies sind nur zwei kleine Beispiele, wie wir im Organisationsbereich Cyber- und Informationsraum unseren Beitrag zur Bewältigung dieser Krise leisten – schnell und lösungsorientiert. Es geht nur gemeinsam – CIR steht bereit!

Wenn ich dennoch wieder auf unseren dritten Geburtstag blicke, stelle ich fest:

Die Aufstellung des Cyber- und Informationsraums als eigenen militärischen Organisationsbereich neben Heer, Luftwaffe, Marine, SKB und Sanitätsdienst hat sich als richtig erwiesen. Das zeigt sich für mich in der inzwischen unumstrittenen Tatsache, dass sich die wahrscheinlichen Konflikte der Zukunft hauptsächlich in dieser Dimension abspielen werden. Schützenpanzer, Kriegsschiffe und Kampfflugzeuge werden zur glaubwürdigen Abschreckung weiter unentbehrlich sein. Jedoch werden Konflikte im Informationszeitalter primär mit anderen Mitteln ausgetragen – meist unterhalb der Gewaltschwelle und meist nicht rein militärisch. Hybridität heißt das Stichwort. Auch das ist eine Facette der gestiegenen Bedeutung der Landes- und Bündnisverteidigung. Ohne die Details vorwegzunehmen ist klar, dass einer Bedrohung, die auf die Gesamtheit von Staat und Gesellschaft abzielt, nur gesamtstaatlich begegnet werden kann. Wir im Organisationsbereich Cyber- und Informationsraum leisten dazu einen entscheidenden Beitrag. Im Nationalen Cyber-Abwehrzentrum (Cyber-AZ) tragen wir zur Cyber-Sicherheitslage Deutschlands unser CIR-Lagebild bei, das im Gemeinsamen Lagezentrum im Kommando CIR erstellt wird. Das ressortübergreifende Zusammenführen aller relevanten Lagebilder ist ein entscheidender Schritt, denn nur mit einem effektiven Informationsaustausch kann die Abwehr hybrider Bedrohungen gelingen. Gleichzeitig ist dies aber auch nur der erste Schritt. Alle Beteiligten wissen, dass zum Aufbau einer reaktionsfähigen operativen Institution noch ein weiter Weg vor uns liegt.

Auch über das Nationale Cyber-AZ hinaus ist die Zusammenarbeit zwischen Gesellschaft, Politik, Wirtschaft, Wissenschaft und Militär eine wichtige Voraussetzung, um hybriden Bedrohungen rund um Informationen zu begegnen. Das gilt national wie international. Deswegen legen wir großes Augenmerk darauf, mit den maßgeblichen Akteuren aus all diesen Bereichen eng zusammenzuarbeiten. Hierauf geht der Artikel „Nationale und internationale Zusammenarbeit im Cyber- und Informationsraum" ausführlich ein.

Ein zweites Thema, das mir neben der gesamtstaatlichen Cyber-Sicherheit sehr am Herzen liegt, ist die Digitalisierung der Bundeswehr. Wir im Organisationsbereich Cyber- und Informationsraum verstehen uns als Garant der erfolgreichen Digitalisierung der Bundeswehr. Unser Leistungsspektrum reicht dabei von pragmatischen Einzellösungen bis hin

zur Gesamtstruktur der IT-Landschaft. Beispielsweise entwickeln unsere Expertinnen und Experten im Zentrum für Softwarekompetenz selbst Software oder passen marktverfügbare Produkte an die Bedürfnisse der Truppe an. Dies beschreibt der Beitrag aus der jüngsten Dienststelle unseres Organisationsbereichs „Innovativ, agil und zukunftsgerichtet: Die Softwarekompetenz der Bundeswehr“ sehr anschaulich. Im Kommando CIR laufen derweil die großen Fäden zusammen: Wie kann sichergestellt werden, dass einzelne IT-Beschaffungsvorhaben zu einem funktionierenden Gesamtsystem integriert werden können? Etwa bei der Digitalisierung Landbasierter Operationen, um nur ein prominentes Beispiel zu nennen. Das funktioniert nur durch Planung aus einer Hand. Damit setzen wir auch international Maßstäbe. Die Einzelheiten beschreibt der Beitrag „Zielbildung, Digitalisierung und Fähigkeitsentwicklung im Kommando Cyber- und Informationsraum“.

Mit der fortschreitenden Digitalisierung der Bundeswehr hat sich auch eine Abhängigkeit entwickelt, die uns zugleich verwundbar macht. Daher ist die Informationssicherheit conditio sine qua non – ohne sie ist alles nichts. Gerade im militärischen Kontext sind Verfügbarkeit, Vertraulichkeit und Integrität von Informationen essenziell. Wie der Beitrag „Informationssicherheit für die Bundeswehr“ erläutert, setzen wir in diesem Bereich auf Zertifizierung und Kontrolle, auf einen guten Austausch in der breitgefächerten Informationssicherheitsorganisation der Bundeswehr und auf die konstant hoch zu haltende Awareness unserer Mitarbeiterinnen und Mitarbeiter.

Unser Organisationsbereich ist jetzt drei Jahre alt. Unsere volle Einsatzbereitschaft werden wir planmäßig im Jahr 2022 erreichen. Bereits in der „Krabbelphase“, kurz nach unserer Aufstellung, kündigten sich große Aufgaben an. Ein vor uns liegendes Mammutprojekt ist unsere Teilhabe an der nächsten deutsch geführten NATO-Speerspitze im Jahr 2023. Hierauf geht der Artikel „VJTF 2023: Der Beitrag CIR zur Landes- und Bündnisverteidigung“ näher ein.

Alle Vorhaben sind jedoch auf tönernen Füßen gebaut, wenn wir eines außer Acht lassen: die Frauen und Männer, die in Uniform und in Zivilkleidung bei uns dienen. Sie sind unser höchstes Gut. Bei der Gewinnung unseres Nachwuchses und der Bindung der bereits bei uns tätigen Fachkräfte gehen wir daher innovative Wege. Wir haben eine Fachkarriere für IT-Offiziere geschaffen, wir berücksichtigen non-formale Qualifikationen künftig stärker als zuvor, wir modularisieren die Ausbildung des IT-Personals und wir nutzen das Potenzial der Cyber-Reserve. Zu diesen Themen empfehle ich Ihnen die Artikel „Fachkarriere, Zulagen, fachliches Recruiting: Die Bundeswehr geht neue Wege im Wettbewerb um die besten Köpfe“ und „Die Cyber-Reserve der Bundeswehr – Eine erste Bilanz“ in diesem Heft.

Volle Einsatzbereitschaft nach Plan in 2022 heißt jedoch nicht, dass dann die organisatorischen Strukturen des Organisationsbereichs einen dauerhaften Zielzustand erreicht haben. Vielmehr gibt es bereits heute eine Vielzahl von Faktoren, die eine Weiterentwicklung unabdingbar machen.

Wir dürfen uns nicht auf Erreichtem ausruhen!

Mit den bisherigen Erfahrungen seit der Aufstellung des Organisationsbereichs CIR, mit einer zunehmenden Auftragslage in der Fähigkeitsentwicklung CIR, den Herausforderungen der Digitalisierung sowie auch der Ausrichtung am Fähigkeitsprofil der Bundeswehr wurde schnell deutlich, dass das Gesamtportfolio an Aufträgen bei unveränderter Ressourcenlage nur mit erheblichen Anstrengungen zu erfüllen sein wird. Hinzu kommt die Entwicklung der Wiederausrichtung der Bundeswehr auf Landes- bzw. Bündnisverteidigung mit den damit verbundenen Überlegungen zur Operationsfähigkeit in hybriden, teilweise gesamtstaatlichen Krisenszenarien sowie zur nationalen Führungsorganisation bei gleichzeitiger Erfordernis der Sicherstellung der laufenden Einsätze.

Vor diesem Hintergrund hatte ich bereits im Frühjahr 2019 die Durchführung einer umfassenden Strukturanalyse angewiesen. Sie soll ergeben, wie unter den genannten Rahmenbedingungen die Zielstruktur des Organisationsbereichs CIR mit dem Ziel der Erhöhung der Effektivität in der Auftragserfüllung aussehen müsste.

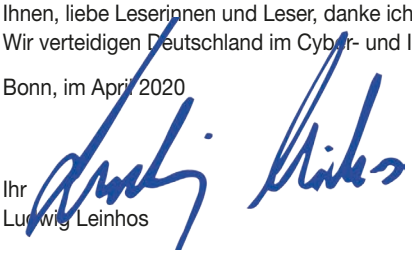
Ich bin mir sicher, auf Grundlage der zu erarbeitenden Ergebnisse den Organisationsbereich CIR auch für die Zukunft gut gerüstet aufzustellen.

Auch wenn noch viel Arbeit vor uns liegt - nach den vergangenen drei Jahren bin ich sehr stolz auf das bis hierhin Erreichte. Ich danke den Frauen und Männern meines Organisationsbereichs für die in dieser herausfordernden Zeit geleistete Arbeit!

Ich freue mich, allen Interessierten in diesem Heft einen aktuellen Einblick in unsere Arbeit bieten zu können. Dafür danke ich an dieser Stelle explizit den Autoren, die in vielen Stunden neben ihrer eigentlichen Tätigkeit großes Engagement bewiesen haben.

Ihnen, liebe Leserinnen und Leser, danke ich für Ihr Interesse!
Wir verteidigen Deutschland im Cyber- und Informationsraum!

Bonn, im April 2020



Ihr
Ludwig Leinhos

Der Organisationsbereich Cyber- und Informationsraum – Beitrag und Bekenntnis der Bundeswehr zu Herausforderungen der Digitalisierung

Grußwort von Dr. Reinhard Brandl MdB, CDU/CSU, Mitglied im Verteidigungs- und im Haushaltsausschuss des Deutschen Bundestages

In der Bundeswehr ist seit der Zeit ihrer Gründung der Schutz der eigenen Kommunikation sowie das Aufklären und Stören von gegnerischer Kommunikation fester Bestandteil des Fähigkeitsspektrums „Elektronische Kampfführung". In den vergangenen 60 Jahren haben sich die technischen Rahmenbedingungen und die Bedeutung dieser Fähigkeiten grundlegend verändert. Elektronische Kommunikationsmittel werden nicht nur zur Verständigung zwischen Truppenteilen oder zur Steuerung von konventionellen Waffensystemen eingesetzt, sondern sind zu einem Faktor zwischenstaatlicher Konflikte geworden.

Die fortschreitende Digitalisierung durchdringt alle Lebensbereiche und verändert das gesellschaftliche, wirtschaftliche und politische Leben. Für die Zukunftsfähigkeit des Geschäftsbereichs des Bundesministeriums der Verteidigung (BMVg) ist die Digitalisierung ebenso richtungsweisend, wie für alle anderen Ressorts. Mit der „Strategischen Leitlinie Digitalisierung" und der „Umsetzungsstrategie Digitale Bundeswehr" wurden die notwendigen konzeptionellen Voraussetzungen geschaffen, um die digitale Transformation zielgerichtet anzustoßen und umzusetzen. Am 5. Oktober 2016 wurde im Bundesministerium der Verteidigung die Abteilung Cyber- und Informationstechnik mit Grundbefähigung aufgestellt (CIT). Im April 2017 erfolgte mit der Aufstellung des neuen Organisationsbereichs für den Cyber und Informationsraum (CIR) eine sichtbare Antwort auf die Fragen zu den Auswirkungen der zunehmenden Digitalisierung.

Herausforderungen im Cyberraum gemeinsam bewältigen

Nicht nur die Bundeswehr bietet mittlerweile als voll digitalisierte Großorganisation zahllose mögliche Angriffspunkte und ist täglich mehr oder weniger professionellen Attacken ausgesetzt. Bereits eine kleine unentdeckte Schwachstelle kann es einem Angreifer ermöglichen, maximalen Schaden anzurichten: von kleinsten Eindringversuchen über gezielte Lähmungsangriffe (Denial of Service); von Erpressungen durch Verschlüsselungstrojaner bis zur organisierten Desinformation via Social Media. Entgegen der konventionellen Bedrohung lassen sich durch Kombination beliebiger dieser Methoden als Mittel hybrider Kriegsführung sehr viel schnellere und umfassendere Effekte erzielen. Dabei bleiben sie regelmäßig unterhalb der Schwelle kriegerischer Auseinandersetzungen.

Die Abwehr von Cyber-Angriffen ist eine gesamtstaatliche Aufgabe, denn auch die Art der Bedrohung verwischt die Grenzen zwischen innerer und äußerer Sicherheit. Beispielsweise ist zum Zeitpunkt eines Cyber-Vorfalls oder -Angriffs oft nicht bekannt, wer mit welcher Motivation der Urheber ist. Bei einem weitreichenden Angriff auf kritische Infrastrukturen in Deutschland kann sogar der Verteidigungsfall ausgerufen werden. Hierbei gilt es einen nahtlosen Übergang der Fähigkeiten in allen erforderlichen Bereichen zu gewährleisten und das Zusammenspiel sicherzustellen. Die drei Aufgabenschwerpunkte Cyber-Abwehr (Bundesministerium des Innern), Cyber-Verteidigung (BMVg) und Cyber-Außenpolitik (Auswärtiges Amt) funktionieren nur erfolgreich, wenn eine operative Zusammenarbeit dieser drei Bereiche möglich ist. Für diese Fälle und für eigene Auslandseinsätze bzw. Missionen muss die Bundeswehr

(Foto: Autor)

geeignete defensive als auch offensive Fähigkeiten vorhalten und massiv ausbauen. Um es klar zu sagen: Im Ernstfall geht es schließlich nicht nur um die Fähigkeit „hack back" sondern auch um „hack first", da mögliche Angreifer von Fähigkeiten und Ressourcen im Cyberraum abhängig sind. Ein solcher Einsatz der Bundeswehr unterliegt dabei denselben rechtlichen Voraussetzungen wie jeder andere Einsatz deutscher Streitkräfte. In Friedenszeiten ist es die vorrangige Aufgabe der Bundeswehr, sich selbst vor Cyber-Angriffen zu schützen.

Cybersicherheit als besondere Aufgabe

Damit die vorhandenen sowie die noch zu entwickelnden Ressourcen und Fähigkeiten koordiniert und effektiv zum Einsatz gebracht werden können, wurde das Kommando CIR aufgestellt. Die entsprechenden Truppenteile wurden dazu von der Streitkräftebasis dem Kommando CIR unterstellt. Nach nunmehr drei Jahren der Indienststellung kann ein positives Fazit gezogen werden. Die Einrichtung des Organisationsbereiches CIR kann als voller Erfolg mit hohem Mehrwert für die Streitkräfte gewertet werden. Dem Bundestag wurde im Februar 2020 der Zweite Sachstandsbericht des BMVg zum Cyber- und Informationsraum

vorgelegt, der einen Überblick zur aktuellen Bedrohungslage sowie Aussagen zum geplanten Mittelansatz für Investitionen enthält.

Das Weißbuch 2016 benennt zudem für das Kommando CIR die Handlungsfelder, die kontinuierlich ausgebaut und weiterentwickelt werden. Im Kommando CIR wurde bereits ein eigenes Lagezentrum für die Dimension Cyber- und Informationsraum etabliert. Durch die Fusion existierender Lagen aus allen Bereichen von Relevanz für die Dimension Cyber- und Informationsraum wird ein valides Lagebild als Basis für Handlungsoptionen generiert. Mit Erkenntnissen aus dem Bereich des Militärischen Nachrichtenwesens sowie offen zugänglichen Informationen aus sozialen Netzwerken können zudem Rückschlüsse auf eine zunehmende hybride Bedrohung oder einen koordinierten Cyberangriff gezogen werden. Die so gewonnenen Analysen werden der Bundeswehr und anderen Behörden zur Verfügung gestellt.

Dazu wird Spitzenpersonal gebraucht, das durch neue Cyber-Karrierepfade und Personalgewinnungsstrategien gewonnen wird. Mit der Einrichtung des Forschungsinstituts CODE (Cyber Defence) entwickelt sich an der Universität München eines der größten europäischen Zentren für Spitzenforschung im Bereich Cybersicherheit. Seit 2018 werden in einem neuen Masterstudiengang IT-Sicherheitsspezialisten für die Bundeswehr und Kooperationspartner ausgebildet.

Bundeswehreigene Cyber-Fähigkeiten werden ausgebaut, zusammengeführt und abgesichert. Eigene IT-Projekte werden gezielt vorangetrieben – hier ist das Programm Digitalisierung Landbasierter Operationen (D-LBO) ein bekanntes Beispiel.

Möglichkeiten für die Zukunft sichern

Die Chancen der Digitalisierung werden also genutzt, jedoch nicht ohne die dadurch neu entstandenen Bedrohungen und Risiken außer Acht zu lassen. Deutschland und die Bundeswehr müssen sich dabei auf beiden Seiten umfassend zukunftsfähig aufstellen. Unsere zunehmend vernetzte Gesellschaft ist in hohem Maße auf die Verfügbarkeit, Integrität und Vertraulichkeit ihrer Informations- und Kommunikationsinfrastruktur angewiesen. Gemeinsam muss laufend überprüft werden, welche Chancen wir nutzen wollen, welche Bedrohungen wir verhindern wollen und welche Risiken damit jeweils verbunden sind.

Im Mai 2020 werden wir uns im Deutschen Bundestag im Rahmen einer Öffentlichen Anhörung mit verfassungs- und völkerrechtlichen Fragen im militärischen Cyber- und Informationsraum beschäftigen. Dabei wird es auch um die Zurechenbarkeit von Cyberangriffen sowie die entsprechende Anpassung nationaler und internationaler Normen gehen. Es liegt nicht in unserem Interesse, dass der Cyberraum sich mehr und mehr zu einem Feld entwickelt, auf dem zwischenstaatliche Konflikte ausgetragen werden. Gleichzeitig vertreten wir in der CDU/CSU-Bundestagsfraktion die Ansicht, dass dies uns nicht von der Verantwortung entbindet, die Bundeswehr für den Ernstfall auszurüsten und die politische sowie militärische Handlungsfähigkeit für jede mögliche Situation zu erhalten. Dies zum Schutz Deutschlands, seiner Bürgerinnen und Bürger und auch seiner digitalen Souveränität.

Gemeinsam die sichere Digitalisierung gestalten

Grußwort von Arne Schönbohm, Präsident des Bundesamts für Sicherheit in der Informationstechnik (BSI)

Die Schadsoftware „Emotet“ hat uns in den letzten Monaten erneut schmerzhaft vor Augen geführt, welche Auswirkungen es haben kann, wenn man die Vorteile der Digitalisierung genießt, ohne die dafür unabdingbar notwendige Informationssicherheit zu gewährleisten. Stadtverwaltungen, Behörden, Krankenhäuser und Universitäten wurden teilweise lahmgelegt, Unternehmen mussten zeitweise den Betrieb einstellen. Die Folgen waren für jeden von uns spürbar: Waren und Dienstleistungen konnten nicht mehr angeboten und verkauft werden, Krankenhäuser mussten die Patientenannahme ablehnen. Stadtverwaltungen waren nicht mehr arbeitsfähig und schlossen ihre Bürgerbüros. Bürgerinnen und Bürger konnten keine Ausweise und Führerscheine beantragen, keine Autos anmelden und keine Sperrmüllabfuhr bestellen. Sogar Hochzeiten mussten verschoben werden.

Und wie würde die Lage wohl erst aussehen, wenn wir tatsächlich in einer voll digitalisierten Welt lebten?

Als die Cyber-Sicherheitsbehörde des Bundes setzt das Bundesamt für Sicherheit in der Informationstechnik (BSI) sich dafür ein, dass „Security by Design“ und „Security by Default“ als Grundregeln der Informationstechnik etabliert werden. Durch Informationsangebote, technische Anforderungen und Standards schaffen wir Rahmenbedingungen, um ein sicheres und selbstbestimmtes Handeln von Wirtschaft und Gesellschaft in der digitalen Welt zu ermöglichen. Wir zeigen auf, wie Informationssicherheit als neues Qualitätsmerkmal „Made in Germany“ in der Digitalisierung funktionieren kann.

Wer die Digitalisierung nutzen will, kann nicht nur A, sondern muss auch B sagen. Genauso selbstverständlich wie wir uns im Auto anschnallen oder zuhause die Tür abschließen, so müssen wir auch in der digitalen Welt angemessene Sicherheitsvorkehrungen ergreifen.

Dies kann und wird dem BSI nicht im Alleingang gelingen. Daher sind wir besonders froh, mit dem Organisationsbereich Cyber- und Informationsraum (CIR) der Bundeswehr einen starken und kompetenten Partner an unserer Seite zu haben, mit dem wir nicht nur im

(Foto: BSI / B23)

Nationalen Cyber-Abwehrzentrum partnerschaftlich und zielorientiert zusammenarbeiten. Ich gratuliere dem Kommando CIR und insbesondere Generalleutnant Ludwig Leinhos zum dritten Jubiläum und bin fest davon überzeugt, dass wir noch viele gemeinsame Jahre lang die Informationssicherheit in Deutschland erhöhen werden.

Die Gefährdungslage im Cyberraum und ihre behördenübergreifende Bewältigung

Grußwort von Holger Münch, Präsident des Bundeskriminalamtes (BKA)

Die Nutzung digitaler Informations- und Kommunikationstechnologien ist Grundlage des modernen gesellschaftlichen und wirtschaftlichen Lebens. Mit der zunehmenden Digitalisierung und fortschreitenden Entwicklungen wie das Internet der Dinge, Industrie 4.0, Smart Home oder Automotive IT erweitert sich das Spektrum für Cyberangriffe kontinuierlich. Dies zeigt sich nicht nur in den stetig steigenden Fallzahlen der Cyberkriminalität, sondern auch in dem signifikanten Anstieg der Vielfalt von Schadsoftware. Diebstahl digitaler Identitäten, massenhafte Fernsteuerung von Computern durch Botnetze, DDoS-Angriffe, digitale Erpressungen durch den Einsatz von Ransomware und der Einsatz von „Mobile Malware“ verdeutlichen beispielhaft, dass sich Cyberangriffe zu einem Massenphänomen entwickelt haben, durch das erhebliche Schäden verursacht werden. Auch die Qualität der beobachteten Cyberangriffe hat durch den technischen Fortschritt und durch eine

zunehmende Professionalisierung von Angriffsvektoren in den vergangenen Jahren deutlich zugenommen.

Die Underground Economy stellt zudem eine große Bandbreite an illegalen Angeboten in Form von Dienstleistungen zur Verfügung – wir sprechen hier von „Cybercrime-as-a-Service“, welche auch Tätern ohne eigene technische Kenntnisse und mit geringem Aufwand die Durchführung jeder Art von Cybercrime ermöglichen oder zumindest erleichtern.

Deutschland ist aufgrund seines hohen technischen Entwicklungsstands und Know-hows ein besonders attraktives Ziel für Cyberkriminelle. In diesem Kontext ergeben sich auch Gefahrenpotentiale und Auswirkungen durch Cyberangriffe auf sogenannte Kritische Infrastrukturen. Der reibungslose Betrieb dieser „zentralen Nervensysteme“ sichert die Funktionalität und fundamentale Prozesse moderner Gesellschaften. Angriffe auf Kritische Infrastrukturen stellen daher eine existentielle Bedrohung für die Sicherheit und das Funktionieren des Staates dar.

Schließlich ist die Gefährdungslage im Cyberraum gleichermaßen durch politisch motivierte Cybercrime geprägt. Darunter fallen sowohl Diebstahls- oder Betrugsdelikte zur Finanzierung extremistischer bzw. terroristischer Strukturen unter Nutzung von Informations- und Kommunikationstechnologien als auch die Inanspruchnahme der Underground Economy zum Vertrieb illegaler Waren oder zum Erwerb terrorismusrelevanter Güter. Ebenso gewinnen Propagandadelikte, das Verbreiten von Anleitungen für Straftaten, zum Beispiel zum Bauen von Bomben, Radikalisierungsbestrebungen und Sabotage über diese Medien zunehmend an Bedeutung. Malware, DDoS-Attacken oder sogenannte „Defacements“ können genutzt werden, um derartige Handlungen zu fördern oder umzusetzen.

Im Bereich der Cyberspionage dient die eingesetzte und oftmals modular aufgebaute Schadsoftware in erster Linie der Datenausspähung. Auch besteht die Möglichkeit des Einsatzes von Schadsoftware zu Sabotagezwecken.

(Foto: BKA)

Angriffe staatlicher Akteure erfolgen zumeist in Form von „Advanced Persistent Threats“. Dabei versuchen die Angreifer, dauerhaften Zugriff zu einem Netzwerk zu erlangen und diesen in der Folge auf weitere Systeme auszuweiten. Sie sind eine ernstzunehmende und weiter zunehmende Bedrohung für die Wirtschaft sowie öffentliche und nicht-öffentliche Stellen und Institutionen, insbesondere der Kritischen Infrastrukturen.

Dieser Bedrohungslage ist mit einem ganzheitlichen Ansatz aller für die Cybersicherheit und -bekämpfung verantwortlichen Stellen auf nationaler und internationaler Ebene zu begegnen. Ein umfassender und wirksamer Schutz des Cyberraums kann nur durch den koordinierten Einsatz unter Einbeziehung aller Sicherheitsbehörden des Bundes und der Länder erzielt werden. Daher ist das im Jahr 2011 eingerichtete Nationale Cyber-Abwehrzentrum (Cyber-AZ) eine tragende Säule der deutschen Cyber-Sicherheitsstrategie.

Das Cyber-AZ ermöglicht als Informations-, Koordinations- und Kooperationsplattform die enge Zusammenarbeit zwischen dem Kommando Cyber- und Informationsraum, dem Bundeskriminalamt, dem Bundesamt für Sicherheit in der Informationstechnik, dem Bundesamt für Verfassungsschutz, dem Bundesnachrichtendienst, dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, dem Bundespolizeipräsidium, dem Militärischen Abschirmdienst und dem Zollkriminalamt.

Nur auf Basis dieses ressortübergreifenden Ansatzes, der die verschiedenen Gefährdungen im Cyberraum wie Spionage, Ausspähen von Daten, Terrorismus und Cybercrime zusammenführt, kann im Cyber-AZ die Abwehr hybrider Bedrohungen durch koordinierte Maßnahmen gelingen.

Für das Cyber-AZ an der Nahtstelle zwischen ziviler Gefahrenabwehr und Strafverfolgung auf der einen Seite und militärischer Verteidigung auf der anderen Seite, stellt sich zunächst die Herausforderung, ein umfassendes Cybersicherheitslagebild unter Berücksichtigung aller verfügbaren Informationen zu erstellen. Das Kommando Cyber- und Informationsraum spielt hier eine wesentliche Rolle, denn erst durch Erkenntnisse zu militärischen Cybersicherheitsszenarien wird das Cybersicherheitslagebild Deutschlands komplettiert. Die Betrachtung von Cyberszenarien im Lagebereich des Cyber-AZ unter Einbeziehung ziviler, polizeilicher, nachrichtendienstlicher und militärischer Informationen gewährleistet somit eine umfassende Bewertung der Bedrohungslage, von der im Ergebnis alle beteiligten Sicherheitsbehörden profitieren. Nur ein derart umfassendes Lagebild ermöglicht die zielgerichtete Strategiebildung und unterstützt im Einzelfall auch die behördenübergreifende Bewältigung von Cybervorfällen. Dem Cyber-AZ kommt in diesen Fällen die Aufgabe zu, einen kontinuierlichen Informationsaustausch und gemeinsame Risikoanalysen und -bewertungen sicherzustellen sowie, in Ableitung daraus, konkrete Handlungsempfehlungen zu erarbeiten und die operativen Aktivitäten der beteiligten Einrichtungen zu koordinieren.

Die tragende Rolle des Kommandos Cyber- und Informationsraum der Bundeswehr im Cyber-AZ wird nicht zuletzt dadurch deutlich, dass es einen Stellvertreter für den Koordinator des Cyber-AZ und Personal für die Geschäftsstelle stellt sowie die Leitung der Arbeitsgruppe „Übungen“ übernommen hat. Die enge Zusammenarbeit zwischen dem Kommando Cyber- und Informationsraum und dem Bundeskriminalamt besteht aber nicht nur im Cyber-AZ. Künftig können Kommando Cyber- und Informationsraum und Bundeskriminalamt auch durch die Intensivierung der Zusammenarbeit in den Bereichen der Wissensvermittlung sowie Aus- und Fortbildung voneinander profitieren.

Im dargestellten Kontext der hybriden Bedrohungslage und der sich daraus abzuleitenden polizeilichen Aufgabenstellungen im Cyberraum weiß das Bundeskriminalamt mit dem Kommando Cyber- und Informationsraum einen geschätzten und wichtigen strategischen Partner an seiner Seite.

Grußwort von Benedikt Zimmer, Staatssekretär im Bundesministerium der Verteidigung

Sehr geehrte Leserinnen und Leser,

Informations- und Kommunikationstechnologie ist allgegenwärtig und bringt Veränderungen in allen Arbeits- und Lebensbereichen mit sich. Komplexe Großorganisationen, wie es auch die Bundeswehr ist, stellt dies auf unterschiedlichsten Führungsebenen, Anwendungsbereichen und Handlungslinien vor besondere Herausforderungen – von der Digitalisierung der Verwaltung über Awareness-Schulungen für die Mitarbeiterinnen und Mitarbeiter bis hin zum Betrieb und Schutz vernetzter Führungs- und Waffensysteme.

Der Cyber- und Informationsraum (CIR) als Dimension ist die Antwort der Bundeswehr, um dieses Spektrum angemessen und militärisch effektiv zu adressieren. Rund 14.500 zivile und militärische Angehörige des Organisationsbereichs CIR stellen umfassende Fähigkeiten für den Betrieb und den Schutz der Systeme und Netze der Bundeswehr sowie zur Aufklärung und Wirkung in dieser Dimension bereit. Sie liefern Geoinformationen, bereiten diese auf und tragen auch dadurch wesentlich zur gesamtstaatlichen Cyber-Sicherheitsarchitektur bei.

In der täglichen Arbeit gilt es, den technologischen Fortschritt in allen Bereichen des Geschäftsbereichs BMVg umfassend nutzbar zu machen – von der Gewährleistung der Durchsetzungsfähigkeit der Streitkräfte auf dem Gefechtsfeld bis hin zur Vereinbarkeit von Familie und Beruf zum Wohle aller Mitarbeiterinnen und Mitarbeiter.

Im Rahmen des HERKULES Folgeprojekts mit einem Finanzvolumen von rund 1 Mrd. Euro pro Jahr erhalten alle Angehörigen des Geschäftsbereiches BMVg Zugang zu den zentralen Diensten der Bundeswehr. Dies erfolgt maßgeblich über private Cloud-Services im eigenen Rechenzentrumsverbund und zugehörige Weitverkehrsnetze bis in die Einsatzgebiete. Durch eine mobile IT-Ausstattung werden moderne und dadurch attraktive Arbeitsumgebungen bereitgestellt. Für die elektronische Verwaltungsarbeit und Kollaboration werden mit dem Kommando CIR die Weichen für ein erfolgreiches Umsetzen der beiden Verwaltungsprojekte Dokumentenmanagementsystem der Bundeswehr und bundeswehrgemeinsame Kollaborationsplattform (Groupware Bw) für ca. 190.000 Nutzerinnen und Nutzer gestellt. Damit hält eine zeitgemäße, moderne Kommunikation und Kollaboration sowie die elektronische Aktenführung Einzug in den Geschäftsbereich des BMVg.

Daten fallen natürlich nicht nur im Rahmen der Bürokommunikation an. Unter dem Motto „Geoinformationen aus einer Hand“ sorgt der Geoinformationsdienst der Bundeswehr für die Verfügbarkeit aktueller und qualitätsgesicherter Geoinformationen. Dabei arbeiten 18 geowissenschaftliche Disziplinen in einem weltweit einzigartigen interdisziplinären Ansatz Hand in Hand, um die sogenannte „GeoInfo-Unterstützung“ als eine der Kernfähigkeiten der Bundeswehr und als Grundlage für das Operieren in allen Dimensionen aus dem Cyber- und Informationsraum heraus sicherzustellen.

Informationen zur Krisenfrüherkennung und zur Unterstützung der Einsätze werden durch zahlreiche Fähigkeiten im Bereich der Strategischen Aufklärung beispielsweise mit der „Satellitengestützten Abbildenden Aufklärung“ oder der „Fernmelde- und Elektronischen Aufklärung“ gewonnen, analysiert und den Entscheidungsträgern zur Verfügung gestellt.

Bei immer weiter fortschreitenden Digitalisierung und der zunehmenden Vernetzung spielt die Cybersicherheit eine elementare Rolle. Hierfür ist im Zentrum für Cyber-Sicherheit der Bundeswehr das Cyber Security Operation Centre als zentrales Kernelement für das Führen der Cybersicherheitslage und die Bearbeitung von Cybersicherheits-Vorfällen etabliert worden. Dort sind die Fähigkeiten zur technischen Überwachung der Systeme und Netze der Bundeswehr und zur Aggregation und Bewertung der lagerelevanten Daten gebündelt.

Um den Besonderheiten und Anforderungen der Streitkräfte auch im Bereich der Softwareprodukte sowie den schnellen Innovationszyklen Rechnung zu tragen, werden im Zentrum für Softwarekompetenz der Bundeswehr Produkte mit besonderem Augenmerk auf die besonderen Belange der Bundeswehr analysiert, weiterentwickelt und zertifiziert.

Die vorgenannten Beispiele sind nur ein kleiner Ausschnitt des Leistungsspektrums des Cyber- und Informationsraums und der täglichen Arbeit. Sie unterstreichen aber eindrucksvoll die Bedeutung des noch jungen Organisationsbereiches für die Bundeswehr. Ich wünsche allen Mitarbeiterinnen und Mitarbeitern des Cyber- und Informationsraumes, dass Sie diese spannende und wichtige Aufgabe auch weiterhin mit hoher Motivation und Freude voranbringen. Ihnen, liebe Leserinnen und Leser, wünsche ich eine gute Lektüre!

(Foto: Bundeswehr / Jane Schmidt)

Grußwort von Dr. Peter Tauber, Parlamentarischer Staatssekretär im Bundesministerium der Verteidigung

Sehr geehrte Leserinnen und Leser,

Digitalisierung ist kein Megatrend der Zukunft, Digitalisierung verändert die Welt jetzt und hier. Eine immer durchdringendere Vernetzung ermöglicht den weltweiten, nahezu ungehinderten Informationsfluss zwischen allgegenwärtigen Endgeräten als auch von Mensch zu Mensch. Grundlegende Leistungen wie die der Energie- oder Wasserversorgung sind ohne Abstützung auf das Internet nicht mehr denkbar. Diese fundamentalen Änderungen betreffen auch die Streitkräfte. Digitalisierung eröffnet neue Möglichkeiten und Chancen. Das „digitalisierte" Gefechtsfeld der Zukunft zeichnet sich durch eine hohe Transparenz, aber auch einen hohen Komplexitätsgrad in Bezug auf Informationsdichte aus. Die Aus- und Bewertung der Vielzahl vorhandener und ständig neu bildender Informationen ist essentiell, um auf dieser Basis einen Informationsvorsprung und damit letztendlich Wirküberlegenheit in allen militärischen Dimensionen zu generieren.

Wir sind mitten in der dafür notwendigen Digitalisierung der Bundeswehr. Zahlreiche Digitalisierungsaktivitäten und -fähigkeiten werden bereits umgesetzt. Damit stellen wir die Durchsetzungsfähigkeit der Streitkräfte auf dem Gefechtsfeld sicher. Darüber hinaus optimieren wir das unterstützende Verwaltungshandeln in der Bundeswehr.

Der Bereich Cyber- und Informationsraum (CIR) wirkt dabei als Schrittmacher. Vor drei Jahren hat der operative Aufbau des Cyber- und Informationsraumes mit der Aufstellung des Kommando CIR und der Bündelung und Erweiterung der Cyber-Fähigkeiten der Bundeswehr begonnen. Drei Jahre sind mit Hinblick auf die heutigen Produktzyklen in der Informations- und Kommunikationstechnologie eine sehr lange Zeit und bieten Platz für mehrere Produktgenerationen - aus Sicht einer Organisation der Größe und Komplexität der Bundeswehr ist es aber dennoch ein kurzes Zeitfenster. Umso beeindruckender ist, was in dieser Zeit im Cyber- und Informationsraum bereits geschaffen wurde!

Insbesondere zeigt sich aber auch, wie wichtig und richtig diese Strukturentscheidung war: Die Bedrohungslage im Cyber- und Informationsraum ist von einer hohen Komplexität und Dynamik geprägt, zunehmend werden Cyberoperationen von verschiedensten Akteuren zur Durchsetzung von politischen, wirtschaftlichen oder kriminellen Zielen genutzt. Rein präventive Maßnahmen sind zur Gewährleistung eines ausreichenden Schutzniveaus im Cyber- und Informationsraum nicht mehr ausreichend; ausgefeilte Angriffe können geraume Zeit „unter dem Radar" bleiben, durch Angriffe auf die komplexen, globalen Versorgungsketten eingebrachte Schläfer-Funktionalitäten oder Hintertüren können sich bereits heute unbemerkt in unseren Systemen befinden. Dies erfordert eine kontinuierliche Überwachung unserer Netze und Systeme, neue Analyseverfahren sowie Fähigkeiten, jederzeit schnell reagieren und im Cyber- und Informationsraum wirken zu können. Hierzu verfügt die Bundeswehr mit dem Organisationsbereich CIR unter anderem über Fähigkeiten, um dem Gegner die Nutzung des Cyberraumes zu erschweren oder völlig zu verwehren. Dabei erfolgen Cyberoperationen, wie alle Einsätze der Streitkräfte, im Rahmen des geltenden Rechts.

Initial ist oft schwer feststellbar, ob technische Probleme, kriminelle Cyberaktivitäten oder ein staatlich gesteuerter Cyberangriff vorliegen. Somit kann auch die Feststellung der Zuständigkeit diffizil sein. Bei der Geschwindigkeit und Komplexität des Cyber- und Informationsraumes müssen daher vorhandene Informationen zentral zusammengeführt und analysiert werden – ein gesamtstaatliches Handeln ist hier unabdingbar: Cybersicherheit ist nicht nur eine technische Fragestellung, sondern insbesondere auch eine sicherheitspolitische Herausforderung! Dies erfordert eine enge ressortübergreifende Koordination der Maßnahmen zur Cyber-Abwehr, Cyber-Verteidigung und der Cyber-Außenpolitik.

(Foto: Bundeswehr / Sebastian Wilke)

Für die Cyber-Abwehr, den zivilen Maßnahmen zum Schutz von Informationen und IT-Systemen, zur Bekämpfung und Strafverfolgung von Cyberkriminalität und die Spionageabwehr im Cyberraum, zeichnet sich das Innenministerium verantwortlich. Deutsche Cybersicherheitsinteressen werden in internationalen Organisationen wie die VN oder OSZE, in der EU und NATO durch das Auswärtige Amt im Rahmen der Cyber-Außenpolitik vertreten. Schwerpunkte hierbei sind die Einigung auf Normen für verantwortliches Staatenverhalten und die Entwicklung von vertrauensbildenden Maßnahmen für mehr Cybersicherheit. Das dritte Element schließlich, die Cyber-Verteidigung, ist die Aufgabe der Bundeswehr. Diese umfasst die Fähigkeiten zur Aufklärung und Wirkung im Cyber- und Informationsraum, zur Abwehr von Cyberangriffen, zum Schutz eigener Informationen und der IT-, Waffen- und Wirksysteme.

Dieser Dreiklang aus Cyber-Abwehr, Cyber-Verteidigung und Cyber-Außenpolitik erfordert eine behördenübergreifende Orchestrierung der Zusammenarbeit. Schlüsselelement dieser Zusammenarbeit und der gesamtstaatlichen Cyber-Sicherheitsarchitektur ist das Nationale Cyber-Abwehrzentrum (Cyber-AZ). Dort sind alle relevanten Ressorts und Behörden des Bundes vertreten, um die vorhandenen Informationen nach dem Prinzip „Need-to-Share“ zusammenzuführen, zu bewerten und als Entscheidungsgrundlage zur Verfügung zu stellen. Das konsolidierte Lagebild CIR-Bundeswehr liefert hierfür einen substantiellen Beitrag - mit der aktiven Mitarbeit im Cyber-AZ trägt die Bundeswehr zum nationalen Gesamtcyberlagebild bei, das eine Entscheidungsgrundlage für koordinierte Abwehrmaßnahmen oder für eine Attribuierung sein kann. Darüber hinaus unterstützt sie im Rahmen der verfassungsrechtlichen Möglichkeiten auf Antrag mittels Amtshilfe bei der zivilen Cyber-Abwehr der Innenbehörden.

Wächst ein Cybervorfall zur Krise heran, sind ressortgemeinsame politische Bewertung, Mittel der Außenpolitik und koordinierte technische Bearbeitung gleichermaßen wichtig. Im Rahmen der Weiterentwicklung des Cyber-AZ auf Grundlage der Vorgaben der Cyber-Sicherheitsstrategie für Deutschland 2016 gilt es, die Fähigkeiten der Bundeswehr optimal in die gesamtstaatliche Cyber-Sicherheitsarchitektur einzubringen. Der Aufwuchs des Organisationsbereichs CIR bis zur vollen Zielbefähigung 2022 ist hierbei von besonderer Bedeutung. Hierfür wünsche ich den Soldatinnen und Soldaten sowie den zivilen Mitarbeiterinnen und Mitarbeitern des Cyber- und Informationsraum weiterhin ein gutes Gelingen und Ihnen liebe Leserinnen und Leser, eine spannende Lektüre der Entwicklungen und Fortschritte im Organisationsbereich CIR!

Zwischen Innovation und Souveränität

Grußwort von Dirk Backofen, Vorstandsvorsitzender des Cyber Security Cluster Bonn e.V. und Leiter Telekom Security, T-Systems International GmbH

Herausforderungen, wo man nur schaut. Je mehr Bits und Bytes Raum in unserem Leben einnehmen, desto komplexer wird die Aufgabe sie zu schützen. In einer analogen Welt waren Bedrohungen in der Regel sichtbar und Teil unseres unmittelbaren Umfelds. Heute ist jeder von uns potentielles Ziel von digitalen Gefahren, wie etwa dem kriminellen Emotet-Ökosystem. Und diese sind in der Regel nicht regional, oft noch nicht einmal national, sondern international. Auch das sind Globalisierungs-Effekte, digitale. Sie sind nicht leicht wahrzunehmen und schwer einzuschätzen, weil sie aus einem anderen Blickwinkel betrachtet werden müssen. Und das sind wir noch nicht gewohnt.

Große Unternehmen und Institutionen sind seit Jahrzehnten darauf trainiert immer mal wieder einen Schritt zurück zu treten und das ganz große Bild zu betrachten. Allen anderen muss in besonderem Maße geholfen werden, weil ihnen der Blick für Details noch fehlt. Und hier kommen Kompetenz-Cluster ins Spiel. Dort bündeln wesentliche Akteure all ihre Kompetenz und Exzellenz. Sie sorgen für einen vollständigen Überblick. Sie wissen, wie sich beispielsweise Innovationen auswirken können und erkennen zukünftige Bedarfe. So können sie eine wertvolle Quelle für andere Netzwerke oder Entscheider sein und Ausgangspunkt weiterer Initiativen.

Das Cyber Security Cluster Bonn ist ein gutes Beispiel dafür. Der aktuelle Bericht des Weisenrats für Cyber-Sicherheit, der von diesem Kompetenz-Cluster getrieben wird, belegt dies. Er kann politischen Entscheidern zukünftig als Leitfaden dienen, macht Trends und Entwicklungen deutlich und gibt Impulse über Handlungs-Empfehlungen.

In Brüssel diskutiert man seit geraumer Zeit die Notwendigkeit einer solchen digitalen Sicherheitsunion für Europa. Die Idee sieht quasi einen runden Tisch von Akteuren aus Wirtschaft, Forschung, staatlicher Organe und Politik vor. Klingt bekannt, so ist das Cyber Security Cluster in Bonn ja auch im Prinzip aufgestellt. Die europäische Perspektive ist allerdings eine leicht andere. So drängt sich dort gerade besonders ein Wort in den Vordergrund. Es schickt sich an, Digitalisierung als Modebegriff abzulösen: Souveränität.

Nach anderen Regionen der Welt hat zuletzt Russland ein Gesetz verabschiedet, dass ein „souveränes Internet“ ermöglichen soll. Sprich, damit soll der inländische Datenverkehr über staatlich kontrollierte Knotenpunkte geleitet werden. Das ermöglicht Russland, sich im Verteidigungsfall vom Internet abzukoppeln. Natürlich fragt man sich in Europa, ob und wie dieser globalen Entwicklung Folge geleistet werden sollte. Besser und enger zusammen zu arbeiten beim Thema digitale Sicherheit ist auf jeden Fall schon einmal ein wichtiger Schritt. Der Schutz kritischer Infrastrukturen – das zeigen viele Beispiele der vergangenen Jahre – ist ein ebenso wichtiges Ziel.

Mit ihrem Netz von Sensoren erfasst die Deutsche Telekom AG im Schnitt mehr als 42 Millionen Angriffsversuche pro Tag. In der Spitze übertrifft die Zahl dieser Versuche regelmäßig sogar die 60 Millionen Marke. Diese Werte haben sich im vergangenen Jahr sprunghaft entwickelt. Die Zahlen an sich mögen schon beeindruckend sein, die Evolution der Angriffsarten ist es leider auch. Nimmt man aktuelle Schad-Software unter die Lupe, so muss man leider sagen, dass die „Gegenseite“ höchst professionell geworden ist. Bleibt man beim Beispiel Emotet, so

(Foto: Cyber Security Cluster Bonn)

entscheidet das Grundmodul bereits, welches Schicksal dem infizierten Opfer widerfahren soll. Ist wenig zu holen oder befindet sich das infizierte System in einem wirtschaftlich wenig interessanten Land, so wird ein Spamversand-Modul nachgeladen. Andere können Systeme analysieren, Daten stehlen, sie verschlüsseln und den Besitzer erpressen. Diese modulare Flexibilität macht Emotet zu einer Gefahr für Individuen, Behörden und Unternehmen gleichermaßen.

Gerade die zeigten sich im vergangenen Jahr anfällig. Der Ruf nach Schutz wird immer lauter. Jetzt kann man sagen, dass deren Mitarbeiter lediglich öfter geschult werden müssten. Es ist ein Moment der Unaufmerksamkeit, der ausreicht, um das falsche Dokument zu öffnen. Die folgende Infektion verläuft, als hätte man einen Dominostein in einer langen Reihe umgestoßen. Sensibilisiert man seine Mitarbeiter und warnt sie vor den Folgen, so steigt der Grad der Aufmerksamkeit. Systemische Schwächen bleiben aber bestehen. Und deshalb haben wir uns als Telekom in diesem Jahr das Ziel gesetzt, gerade mittelständische und kleinere Unternehmen besser schützen zu können. Wir machen neue Angebote, verbessern unsere Produkte im Hinblick auf den Bedarf kleinerer Kunden.

So werden wir einen Beitrag leisten, damit das allgemeine Sicherheitsniveau insgesamt besser wird – in allen unseren Rollen. Als Unternehmen, genauso wie als Partner im Cyber Security Cluster Bonn.

Das Gemeinsame Lagezentrum CIR in Bonn kann dank agiler Entwicklungsmethoden fortwährend an aktuelle Entwicklungen angepasst werden. (Foto: Bundeswehr / Martina Pump)

Oberstleutnant i.G.
Thomas Erlenbruch

Das Gemeinsame Lagezentrum CIR
Eine gemeinsame Lage CIR für die Bundeswehr und darüber hinaus

Die Grundlage für Schutz und Wirkung im Cyber- und Informationsraum bildet ein fundiertes Lagebild. Das Gemeinsame Lagezentrum Cyber- und Informationsraum (GLZ CIR) erstellt dieses, indem es die große Menge an relevanten Daten zusammenführt, aus- und bewertet. Mit agilen Methoden entwickelt, nutzt es dazu Big-Data-Verfahren und Künstliche Intelligenz. Seine Produkte stellt das GLZ CIR maßgeschneidert den Bedarfsträgern in und außerhalb der Bundeswehr zur Verfügung.

Realisierung des GLZ CIR

Das GLZ CIR hatte im Dezember 2018 eine Anfangsbefähigung erreicht, mit der umfangreiche Informationen zusammengefasst und analysiert sowie Lageberichte erstellt werden können. Die – verglichen mit klassischen Projekten – sehr kurze Entwicklungszeit war nur möglich, weil das GLZ CIR mit agilen Methoden der Softwareentwicklung und in einer sehr engen Zusammenarbeit zwischen Kommando CIR, BAAINBw, der BWI und zivilen Firmen realisiert wird. Dazu wird die in der Softwareentwicklung als Standardprozess verwendete Methode Scrum angewendet. Die Entwickler der verschiedenen Auftragnehmer arbeiten während der Entwicklung eng mit dem Fachpersonal des GLZ CIR zusammen: Konkrete Anforderungen an das System werden in gemeinsamen Besprechungen konkretisiert, verschiedene Realisierungsmöglichkeiten von Teilfunktionalitäten getestet und Fehlentwicklungen bereits in der Testphase der Software korrigiert. Das System wird also inkrementell erstellt – im vier-Wochen-Rhythmus wird im GLZ CIR ein neues Release installiert. So ließ sich das System zum einen ausgesprochen schnell realisieren, zum anderen können Funktionalitäten kontinuierlich erweitert werden. Neben dem unmittelbaren Bedarf eines Lagezentrums nach Aufstellung des neuen Organisationsbereichs CIR erfordert auch die hochdynamische Entwicklung im Bereich KI und Digitalisierung insgesamt die agile Implementierung.

Die Erstellung des Lagebildes CIR

Der Cyber- und Informationsraum ist weltumspannend und kann im Hinblick auf die Interessen der Bundeswehr kaum eingegrenzt werden. Das Analysepersonal und die zur Verfügung stehende Analysezeit hingegen sind begrenzt; selbst die automatisierte Unterstützung lässt keine weltumspannende Auswertung der Informationen zu. Um dieser Herausforderung zu begegnen, werden in einer morgendlichen Konferenz Analysethemen festgelegt. Hierzu werden aktuelle Ereignisse im Interessenbereich der Bundeswehr und mit möglichen Auswirkungen auf die gesamtstaatliche Sicherheitsvorsorge im Cyber- und Informationsraum vorgestellt und entschieden, welche davon weiter untersucht werden sollen und ob sie in den vierzehntägigen Lagebericht CIR einfließen oder als Sofortberichte verfasst werden.

Der CIR ist durch die Wechselbeziehung verschiedener Elemente geprägt, die in dauerhaften oder zeitweisen Beziehungen ortsunabhängig miteinander interagieren. Um dem Rechnung zu tragen, wird im GLZ CIR in der Analyse ein netzwerkfokussierter Ansatz genutzt, der eine regional nicht begrenzte Betrachtung des weltweit aufgespannten CIR ermöglicht.

Die Analyse des CIR beruht auf der Suche von Informationen in den vorliegenden strukturierten und unstrukturierten Daten. Strukturierte Daten, also Daten mit einer gleichartigen und festgelegten Struktur wie beispielsweise automatische Fehlermeldungen von IT-Systemen werden in vordefinierten Tabellen in das System übernommen und können automatisiert in eine Datenbank eingelesen und dort gespeichert werden. Unstrukturierte Daten, also in Freitextform gespeicherte Informationen, sind etwa Artikel oder Agenturmeldungen aus öffentlichen Quellen sowie Lageberichte anderer Dienststellen.

Wenn man sich an den fünf V orientiert, die Big Data definieren, dann ist die Analyse der für die Dimension Cyber- und Informationsraum relevanten Daten ein echtes Big-Data-Problem. So liegt im GLZ CIR allein aufgrund der verfügbaren öffentlichen Informationen eine enorme Menge an Daten (Volume) in großer Vielfalt der Datentypen und –quellen (Variety) und unterschiedlichster Glaubwürdigkeit (Veracity) vor. Um ein relevantes Lagebild CIR (Value) zu erstellen, aus dem Schutzmaßnahmen sowie Handlungsbedarfe und -optionen abgeleitet werden können, müssen die Daten schnell ausgewertet und weiterverarbeitet werden (Velocity). Dies erfolgt mit dem Big–Data-Ansatz als einem grundlegenden Bestandteil der Architektur des GLZ CIR.

Der erste Schritt in der Analyse ist dabei eine qualifizierte Suche in den vorhandenen Daten. Dabei geht das Analysepersonal genauso vor, wie bei der Suche nach Informationen im Internet mit einer Suchmaschine, etwa Google oder Bing. Es kann die vorhandenen Daten nach einzelnen Schlagwörtern oder nach verschiedenen Begriffen, die durch logische Operanden miteinander verknüpft werden, durchsuchen. Die Dokumente, in denen die gesuchten Schlagwörter oder Begriffe enthalten sind, werden einer Bibliothek zugeordnet. Sie bildet die Grundlage der weiteren Analyseschritte.

In den Dokumenten werden relevante Objekte und deren semantische Beziehungen identifiziert und extrahiert, zum Beispiel die Beziehung „stationiert in“ zwischen den Objekten „KdoCIR“ und „Bonn“. Theoretisch kann die Bibliothek von einem Analysten ohne weitere technische Unterstützung ausgewertet werden, indem die Objekte und deren Beziehungen von Hand identifiziert und graphisch dargestellt werden, was allerdings bei der vorliegenden Informationsfülle nicht praktikabel ist. Stattdessen werden auch hier Big-Data-Methoden und Verfahren der Künstlichen Intelligenz eingesetzt, die auf leistungsfähiger IT ausgeführt werden. Nur so lassen sich die Herausforderungen der Auswahl relevanter Daten und deren sinnvolle Aufbereitung zeitgerecht bewältigen.

Der Einsatz Künstlicher Intelligenz (KI) in der Analyse

KI ist bereits bei vielfältigen Aktivitäten in den Alltag integriert, etwa beim Spiel gegen einen Schachcomputer, der Nutzung von Sprachübersetzerprogrammen oder digitalen Sprachassistenten wie Alexa oder autonom fahrenden Autos. Für den Begriff KI gibt es noch keine abschließende Definition. Es wird in der Literatur aber zwischen zwei Ausprägungen unterschieden: schwacher und starker KI. Schwache KI fokussiert sich auf die Lösung eines konkreten Anwendungsproblems. Innerhalb ihrer Anforderungen ist die KI in der Lage, sich selbst zu optimieren, erlangt allerdings kein tieferes Verständnis für die Problemlösung. Die starke KI dagegen hat das Ziel, dem Menschen vergleichbare intellektuelle Fähigkeiten zu erlangen oder sie gar zu übertreffen. Solch eine KI ist noch nicht entwickelt.

Im Analyseprozess im GLZ CIR übernimmt schwache KI Aufgaben, die aufgrund ihrer Masse durch Analystinnen und Analysten nicht leistbar sind. Der Analyseprozess beginnt mit der Übersetzung fremdsprachiger

Die Analystinnen und Analysten setzen bei der Auswertung der Daten auch auf Künstliche Intelligenz.
(Foto: Bundeswehr / Martina Pump)

Informationen, für die leistungsfähige maschinelle Übersetzungstools angewendet werden, die sowohl die Übersetzung der Datengrundlage als auch die Aufbereitung der Lage in Englisch und in Deutsch gewährleisten. Dazu wird eine Commercial-off-the-shelf Software eingesetzt, die mittels eines KI-Verfahrens, der Neuronal-Machine-Translation (NMT), Texte automatisch übersetzt. Dieses KI-Verfahren liefert bessere Übersetzungsergebnisse als die bisher übliche phrasenbasierte statistische Übersetzung.

Im nächsten Analyseschritt werden die oben bereits erwähnten Objekte in den Daten der Bibliothek automatisiert identifiziert und daraus extrahiert. Dazu wird ein weiteres KI-Verfahren, das Natural-Language-Processing (NLP), eingesetzt. NLP basiert auf Techniken der Computerlinguistik, die KI Texte analog zur menschlichen Vorgehensweise auflöst. NLP beginnt zunächst mit der morphologischen Analyse, bei der Wörter im Text auf Grundformen zurückgeführt werden, gefolgt von der syntaktischen Analyse, bei der Subjekt, Objekt, Prädikat, Artikel usw. identifiziert werden und schließt mit Verfahren der Begriffserkennung ab. Grundlage ist der Stanford Core NLP, eine Entwicklung der Stanford University, der für den besonderen Bedarf des GLZ CIR angepasst wird. Aus den extrahierten Objekten und ihren Beziehungen zueinander werden nun automatisiert die Beziehungsnetzwerke erstellt, deren Knoten und Kanten mit qualitativen und quantitativen Informationen hinterlegt sind. Eine qualitative Information ist in diesem Fall die Art einer Beziehung zwischen zwei Knoten (freundschaftlich oder feindlich). Eine quantitative Information ist dann die Häufigkeit, mit der diese Beziehung in den untersuchten Quellen erwähnt wird. Auf den Beziehungsnetzwerken können mathematische und statistische Analysen (zum Beispiel kürzester Pfad, wichtigster Knoten) durchgeführt werden, um Bedrohungen oder Veränderungen im Cyber- und Informationsraum festzustellen.

Für weitere, tiefer gehende Analysen mit dem Ziel der Vorhersage möglicher Cyber-Bedrohungen, wird zukünftig Random-Forest-Generation, ein KI-Verfahren zur Analyse großer Datenmengen, eingesetzt werden. Dieses Verfahren erweitert die aus der Datenanalyse bekannte Methode der Entscheidungsbäume hin zur Erzeugung vieler Entscheidungsbäume (ein Wald). Random-Forest-Generation kann bei großen Datensätzen mit unterschiedlichen Eingangswerten eingesetzt werden, erkennt in den Daten vernachlässigbare Einflüsse und produziert aus der scheinbar unübersichtlichen Datenflut verständliche und nachvollziehbare Ergebnisse.

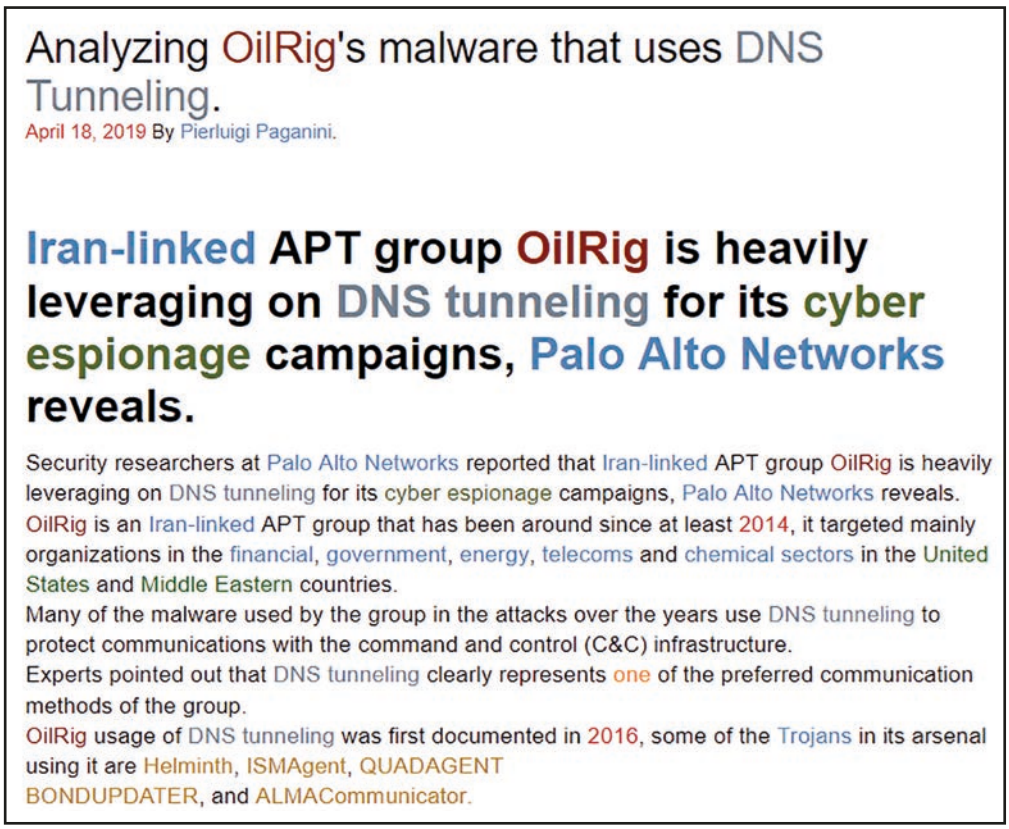
Mit der dargestellten Analysemethodik, der mathematische Aufbereitung der Daten und der komplexen Netzwerkanalyse können strukturierte Aussagen über mögliche Zusammenhänge getroffen werden. Diese werden für verschiedene Adressaten in unterschiedlichen Berichtsformen, die im Folgenden dargestellt werden, aufbereitet.

Berichte des GLZ CIR

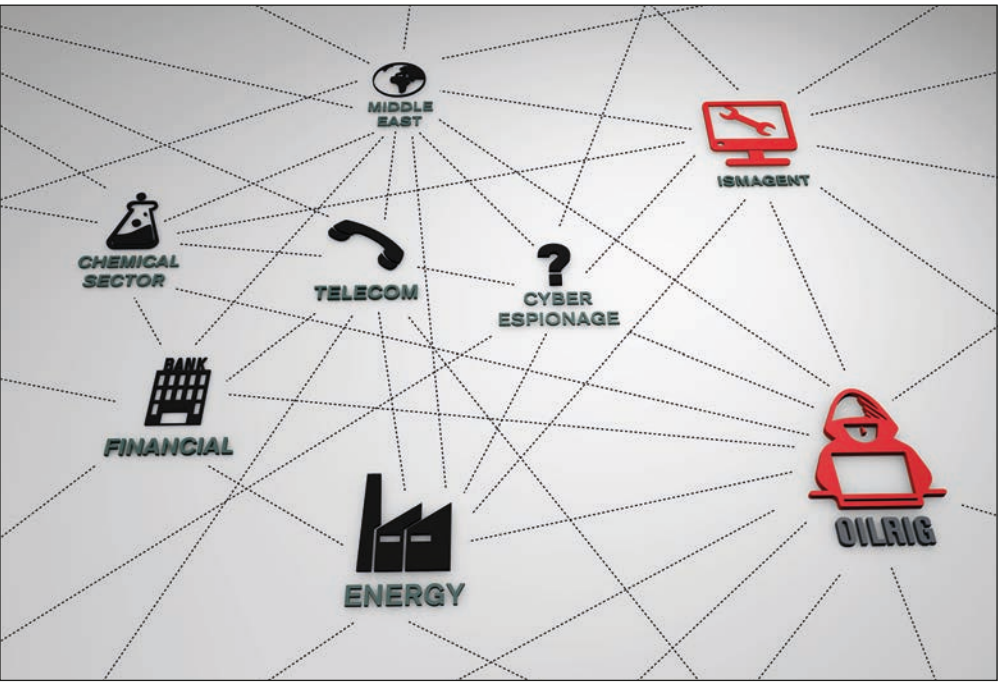
Das Produktportfolio des GLZ CIR besteht aus Sofortberichten, dem regelmäßigen Lagebericht CIR, der IT-Lage und der Einsatzlage CIR.

Sofortberichte werden bei Vorkommnissen erstellt, die unmittelbaren Handlungsbedarf zur Sicherung der Informations- und Kommunikationstechnik der Bundeswehr erfordern. Sie werden als Dokument unmittelbar an die potentiell betroffenen Dienststellen übermittelt.

Der Lagebericht CIR wird regelmäßig erstellt und deckt den Informationsbedarf, der sich aus den ständigen Aufträgen und den Einsätzen der Bundeswehr ergibt. Für den Lagebericht CIR erstellt das Analysepersonal Teilbeiträge zu den im Berichtszeitraum untersuchten Themengebieten. Dabei handelt es sich zum Beispiel um Informationen über Störungen des IT-Systems der Bundeswehr oder über Kampagnen im Internet zur Verbreitung von Computerviren, die auch die IT-Systeme der Bundeswehr bedrohen könnten. Die Teilbeiträge fassen das Analyseergebnis für den Adressatenkreis zusammen, bewerten es im Hinblick auf die Auswirkungen auf die Aufträge der Bundeswehr und enden mit einer Empfehlung zum weiteren Vorgehen. Ein Redakteur führt die Teilbeiträge zu einem Produkt zusammen und überarbeitet sie hinsichtlich sprachlicher und stilistischer Konsistenz. Derzeit wird der Lagebericht CIR in Textform, unterstützt durch Tabellen, Graphiken, Graphen und Geo-Informationen als Dokument an ausgewählte Bedarfsträger sowohl innerhalb der Bundeswehr als auch ressortübergreifend übermittelt, die sie bei Bedarf weiter verteilen können. Der Lagebericht wird als ePaper auf einer Webseite zur Ansicht und zusätzlich zum Download bereitgestellt, um die Informationen noch bedarfsgerechter und interaktiver, mit Weblinks auf Bezugsdokumente, Karten und vertiefende Informationen, anbieten zu können. Die Informationen des Lageberichts CIR, die ressortübergreifende Relevanz haben, werden auch dem nationalen Cyber-Abwehrzentrum zur Verfügung gestellt. Die dort eingesetzte Verbindungsperson des GLZ CIR bringt diese in die Gesamtlage ein und leistet damit einen Beitrag zur gesamtstaatlichen Sicherheitsvorsorge.



◁ ***Im Text wurden mittels Künstlicher Intelligenz (Natural-Language-Processing) Objekte erkannt und unterschiedlichen Gruppierungen zugeordnet, zum Beispiel OilRig gehört zur Gruppierung Hackergruppe (rot dargestellt) und ISMAgent gehört zur Gruppierung Malware (gelb dargestellt). (Abbildung: Bundeswehr / KdoCIR)***



◁ ***Das auf Basis von NLP erstellte Beziehungsnetzwerk zeigt, dass die Hackergruppe „OilRig“ die Malware „ISMAgent“ nutzt und Cyber-Spionage betreibt. Dabei liegt der Schwerpunkt auf den Finanz- und Energiesektoren. (Abbildung: Bundeswehr / KdoCIR)***

Mit der IT-Lage wird über den Sachstand, Anomalien, Auffälligkeiten und relevante Ereignisse im Betrieb der IT der Bundeswehr berichtet. Außerdem werden relevante Vorfälle in den Bereichen Informationssicherheit und Cyberraum mit Bundeswehrbezug vorgestellt. Sie ist auch die Plattform, mit der anlassbezogene Informationen von den jeweiligen IT-Fachbereichen der Bundeswehr sowie des nationalen Cyber-Abwehrzentrums dargestellt werden. Die IT-Lage wird in Textform, unterstützt durch Tabellen, Graphiken, Graphen und Geo-Informationen aufbereitet. Kern ist ein technischer Graph, der die Abhängigkeiten im IT-System der Bundeswehr aufzeigt. Die IT-Lage wird wöchentlich dem Chief Information Security Officer der Bundeswehr (Stellvertreter Inspekteur CIR) vorgetragen. Dazu werden die einzelnen Themen im Hinblick auf ihre Auswirkung auf das IT-System der Bundeswehr bewertet, erforderlicher Handlungsbedarf aufgezeigt und Handlungsempfehlungen vorgeschlagen. Die IT-Lage ist darüber hinaus Teil des Lageberichts CIR und der Einsatzlage CIR.

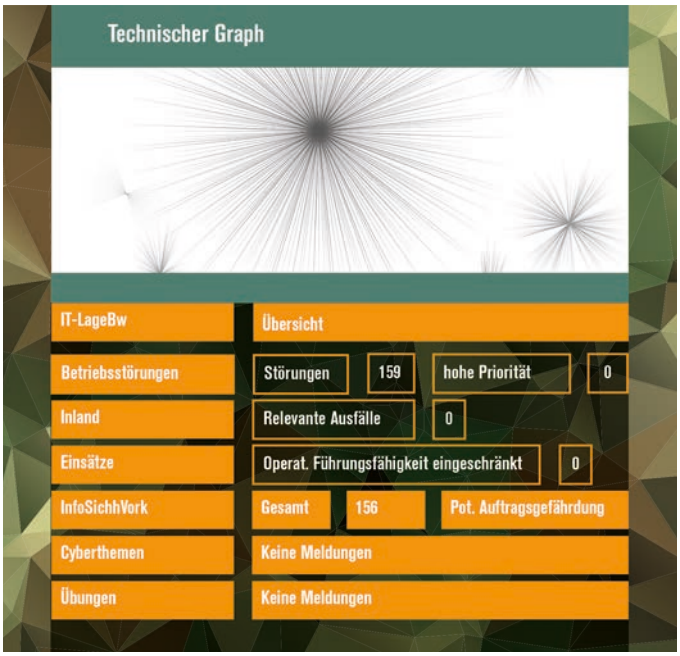
Monatlich wird im GLZ CIR die Einsatzlage CIR zur Information des Inspekteurs CIR und der Führung des Kommandos CIR über den Sachstand im militärischen Organisationsbereich CIR und der Lage im Verantwortungs- und Interessenbereich des Inspekteurs durchgeführt. Neben Informationen aus den Lageberichten und IT-Lagen der vergangenen Wochen wird der Inspekteur über aktuelle Einsätze und Übungen und die Beteiligung von Truppenteilen des Organisationsbereichs daran informiert. Die Beteiligungen werden bewertet, Handlungsempfehlungen vorgeschlagen und Entscheidungen des Inspekteurs herbeigeführt.

Zusammenfassung und Ausblick

Die Bundesregierung stellt in der nationalen KI-Strategie fest, dass der zukünftige Einsatz von KI-basierten Technologien und Systemen Auswirkungen auf die Streitkräfte haben wird und damit ein wichtiges Thema für die Zukunftsentwicklung der Bundeswehr ist. Aus Sicht des Kommandos CIR sind intelligente und automatisierte Systeme die Basis zukünftiger Führungs- und Informationsüberlegenheit. Die Menge der zur Verfügung stehenden Informationen kann weder vom Umfang noch in einer akzeptablen Zeit durch Analystinnen und Analysten ausgewertet werden. Somit ist der Einsatz automatisierter Verfahren unerlässlich. Durch die Ablösung analoger Prozessschritte sowie die Einführung neuer digitaler Arbeitsabläufe schafft es das GLZ CIR, die Chancen der Digitalisierung gewinnbringend zu nutzen. Erst der Einsatz von KI und Big Data ermöglicht die zeitgerechte Bereitstellung eines aktuellen und ebenengerechten Lagebildes CIR zur Information der Bundeswehr selbst, sowie ressortübergreifend anderer Behörden. Darüber hinaus wirkt das Lagebild auch zum Schutz eingesetzter Kräfte mit. Dabei ist sichergestellt, dass der Mensch weiterhin die Kontrolle über die Verfahren der KI behält und die Ergebnisse interpretieren und kontrollieren kann. Die Mitarbeiter werden so ausgebildet, dass sie die Funktionsweise der KI verstehen und diese auch trainieren können. Um die ständige Weiterentwicklung und Anpassung an aktuelle Herausforderungen sicherzustellen, wird die Unterstützung von Industrie und Wissenschaft beim Einsatz der KI-Systeme des GLZ CIR dauerhaft erforderlich sein.

Das GLZ CIR ist in einer ersten Ausbaustufe realisiert, dabei hat sich die agile Entwicklung bewährt. Es kann damit als Katalysator für die Beschleunigung softwareintensiver Projekte in der Bundeswehr dienen. Das GLZ CIR wurde von vornherein so entwickelt, dass es den Nukleus für die Bewältigung zukünftiger Herausforderungen im Cyber- und Informationsraum bilden und dynamisch sowie im Einklang mit den ressortübergreifenden Aktivitäten adaptiert werden kann. Diese Adaptionsfähigkeit wird auch bei den zukünftigen Ausbaustufen unverändert berücksichtigt und umgesetzt werden.

Das Dashboard im Gemeinsamen Lagezentrum CIR zeigt die IT-Lage der Bundeswehr. (Abbildung symbolisch: Bundeswehr / KdoCIR)



Oberstleutnant i.G. Thomas Erlenbruch *verantwortet im Gemeinsamen Lagezentrum CIR die Analyseunterstützung.*

Militärisches und ziviles Personal unterschiedlichster Spezialisierungen und Erfahrungsstufen arbeitet in Teams zusammen. (Foto: Bundeswehr / Martina Pump)

Oberst
Peter Hillermann
und Oberst i.G.
Hartmut Bock

Innovativ, agil und zukunftsgerichtet: Die Softwarekompetenz der Bundeswehr

Von der Vernetzung auf dem Gefechtsfeld bis zur Verarbeitung von „Big Data" – Digitalisierung birgt enormes Potenzial für die Streitkräfte. Dabei ist das Innovationstempo in der Informationstechnik enorm. Um dem gerecht zu werden, verfügt die Bundeswehr mit dem Zentrum für Softwarekompetenz über eigene Fähigkeiten zur Entwicklung und Integration von Software-Anwendungen für die Truppe. Das Zentrum leistet damit einen wichtigen Beitrag zur Digitalisierung der Bundeswehr.

Die jüngste Dienststelle

Das Zentrum für Softwarekompetenz der Bundeswehr (ZSwKBw) wurde am 1. April 2019 als jüngste Dienststelle im Organisationsbereich Cyber- und Informationsraum (CIR) in Euskirchen in Dienst gestellt. Hierzu wurden sowohl bereits vorhandene Kompetenzen für das weite Themenfeld Software zusammengefasst als auch durch personellen Aufwuchs neue geschaffen. Die Bündelung der durch die Vielzahl unterschiedlicher, sehr spezieller individueller Fähigkeiten und Kenntnisse entstehenden Softwarekompetenz unter einheitlicher Führung ist vor dem Hintergrund des Auftrages zur Harmonisierung der Softwarelandschaft der Bundeswehr eine logische und zwingende Herangehensweise.

Dabei können sich die Expertinnen und Experten nicht allein auf Software beschränken. Erst die Integration von Applikationen zu vollständigen, verfügbaren IT-Services schafft einen Mehrwert für die Truppe. Um dies zu erreichen, wird eine Vielzahl von unterschiedlichsten Methoden- und Fachkompetenzen benötigt. Das Zentrum verfügt über Fachleute, die Software sowohl aus technischer Sicht, aber insbesondere auch aus Sicht der Anwender analysieren und so marktverfügbare Softwareprodukte auf einen operativen Nutzen für die Bundeswehr hin untersuchen können. Während der Entwicklung und Einführung von bundeswehreigenen Softwareprodukten begleiten weitere Spezialistinnen und Spezialisten diese Prozesse durch qualitätssichernde Maßnahmen, um die Funktion auch im komplexen IT-System der Bundeswehr zu gewährleisten.

Häufig bieten marktverfügbare Produkte nur einen Teil der Funktionalitäten, die Streitkräfte für ihren besonderen Auftrag benötigen. Dann integriert ein Teil der Software-Entwicklerinnen und -Entwickler die fehlenden Funktionen in die bereits vorhandenen Softwareprodukte, damit diese den besonderen Anforderungen der Truppe genügen. In einigen Fällen kann nicht auf fertige Softwareprodukte zurückgegriffen werden. Eine Entwicklung durch die Industrie ist zum Beispiel aus Gründen des Geheimschutzes nicht denkbar oder die Produkte sind so speziell, dass es für die Industrie nicht wirtschaftlich wäre, diese zu entwickeln. Hier kommt ein weiterer Teil der Entwickler zum Einsatz, die dann betroffene Software-Komponenten selbst programmieren.

Warum Softwarekompetenz?

Die raschen Innovationszyklen im Bereich der Informationstechnologie erfordern ein Überdenken der Wege zur Beschaffung und Einführung von Neuerungen. Diese auch in der Industrie erkennbare Tendenz wurde bereits in der abschließenden Empfehlung zur Aufstellung des Organisationsbereiches CIR erkannt und wird mit der Verantwortung dieses Bereiches für die gesamte IT in der Bundeswehr verfolgt. Das Zentrum für Softwarekompetenz der Bundeswehr setzt hier an einem von immens hohem Innovationstempo betroffenen Teilbereich der IT an, denn gerade der Softwaremarkt wächst, selbst für die Verhältnisse der IT, rasant.

Dabei ist Softwarekompetenz nicht als Konkurrenz zu bestehenden und bewährten Rüstungsprozessen zu verstehen. Vielmehr unterstützt Softwarekompetenz diese Prozesse aktiv und verbessert die Fähigkeit der Entscheider, in softwarebestimmten Technologiefeldern in verschiedenen Integrationstiefen auf Augenhöhe mit der Industrie zu agieren. Zusätzlich kann diese neue Fähigkeit schnell prototypische (Teil-)Lösungen erzeugen, die sich verkürzend auf die Zeitspanne zwischen dem Identifizieren und dem Schließen einer Fähigkeitslücke auswirken.

Was ist Softwarekompetenz?

Kernfähigkeiten im Zentrum für Softwarekompetenz der Bundeswehr sind die Entwicklung und Integration von Softwareprodukten. Entwicklung bezieht sich dabei im Wesentlichen auf die Fähigkeit, Softwareprodukte selbst herstellen zu können. Diese oder marktverfügbare Produkte werden bei der Integration an besondere Bedürfnisse des Operateurs bzw. Nutzers angepasst (Softwareintegration) sowie in Systemumgebungen eingebunden (Systemintegration).

Übergreifend wird zusätzlich die Fähigkeit zur Zertifizierung von Software geschaffen. Diese baut auf den bereits vorhandenen, wehrtechnischen Kompetenzen zur Durchführung von Abnahmen und qualitätssichernden Maßnahmen im bereits eingeführten Prozessmodell und der integrierten Nachweisführung auf. Hierbei werden verschiedenartige Test- und Referenzanlagen sowie Demonstratoren genutzt. Künftig soll dies ein – zunächst ressortinternes – Gütesiegel ermöglichen. Dieses Gütesiegel soll bestätigen, dass Softwareprodukte den besonderen Anforderungen der Bundeswehr entsprechen. Bereits jetzt wacht ein hauseigenes Qualitätsmanagement über die Einhaltung aller qualitätsbestimmenden Vorgaben innerhalb des Zentrums für Softwarekompetenz.

Im Bereich Software-Innovationen arbeitet das Verbindungselement Partnerschaftsmanagement im Cyber Innovation Hub in Berlin eng mit dem Zentrum für Softwarekompetenz zusammen. Der Cyber Innovation Hub ist ein wichtiger Kristallisationspunkt für Innovationen im Bereich ausgewählter Software-Projekte mit Potential für die Bundeswehr. Hier werden innovative Start-Up-Ideen mit Projekten und auch direkt mit potentiellen Nutzerinnen und Nutzern zusammengebracht. So können insbesondere disruptive Technologien gemeinsam mit den zukünftigen Operateuren zielführend und schnell auf ihre Anwendbarkeit in der Truppe untersucht und bewertet werden. Durch die Vorbewertung steht erfolgsversprechende, innovative Software schneller für die Überführung in einen planmäßigen und zügigen Rüstungsprozess zur Verfügung.

Eine Vielzahl weiterer Fähigkeiten trägt zur Gesamtidee „Softwarekompetenz aus einer Hand“ bei. Dazu zählen die technische Sicht auf die Architektur, ein dem Prozessmodell folgendes Konfigurationsmanagement sowie Fähigkeiten zur Bereitstellung und Kopplung experimenteller Simulationsumgebungen und Netzwerke bis hin zu einem Software-Wissensmanagement. Viele solcher erforderlichen Bausteine werden zentral zusammengefasst, um effizient Prozesse zum Erkennen, Beschaffen und Einführen von Software flexibel zu unterstützen. Auch Spezialisierungen, wie zum Beispiel die Qualitätssicherung von Sondersoftwareprodukten im Herkules Folgeprojekt oder die tiefe Integration von Software in bereits bestehende Plattformen für landbasierte Operationen vervollständigen die vorhandene Leistungsfähigkeit des Zentrums.

Neben dem „klassischen“ Prozessmodell zur Entwicklung von Softwareystemen, V-Modell XT, werden im Zentrum für Softwarekompetenz auch moderne Industriestandards, unter anderem in der agilen Softwareentwicklung (zum Beispiel die Methode Scrum) oder im Rapid Prototyping (beispeilsweise die Methode Spiral Development) angewendet. Insbesondere die Methode Scrum ermöglicht durch regelmäßige Einbindung des Nutzenden und kurze Sprint-Zyklen eine schrittweise, schnelle Bereitstellung des Produkts, so wie es gefordert ist. Dabei

In der agilen Softwareentwicklung nutzen die Teams unter anderem die Methode Scrum. (Foto: Bundeswehr / KdoITBw)

Das Zentrum für Softwarekompetenz unterstützt maßgeblich die NATO-Interoperabilitätsübung CWIX. (Foto: NATO)

sind Anpassung und Umsetzung einzelner Forderungen im laufenden Software-Entwicklungsprozess durchaus möglich. Dies hat sich auch bereits beim Aufbau des Gemeinsamen Lagezentrums CIR (GLZ CIR) bewährt (siehe auch der Beitrag zum GLZ CIR auf Seite 12).

Wie organisiert sich Softwarekompetenz?

Die Fähigkeiten zur Beratung und Unterstützung, zur Softwareentwicklung und -anpassung, zur Systemintegration und Zertifizierung sowie zur Bereitstellung moderner Software für die Bundeswehr sind in vier Fachabteilungen zusammengefasst. Doch das Ziel, Innovationen schneller für die Streitkräfte verfügbar und wirksam zu machen, erfordert manchmal eine Abkehr von starren Strukturen einer in der Bundeswehr üblichen, stark hierarchischen Stabs-Linienorganisation, die andererseits wiederum in der Gesamtschau einer militärischen Organisationsstruktur erforderlich ist.

Daher sind die Prozesse im Zentrum für Softwarekompetenz so gestaltet, dass die an eine Matrixorganisation angelehnte Fachaufgabe mit modernen Methoden und Prozessen bearbeitet werden kann, während sich das Zentrum selbst hierarchisch passgenau in die Gesamtorganisation eingliedert. Nur so ist die erforderliche Adaptionsfähigkeit bei gleichzeitiger Unabhängigkeit von Hierarchien gegeben, um sich schnell und flexibel in den unterschiedlichen Organisationsformen der Programme und Projekte mit unterschiedlichen Partnern aus Rüstung, Forschung und Industrie einzubringen. Insbesondere diese Matrixorganisation, die die Berücksichtigung aller Aspekte einer Problemstellung mit einem einheitlichen Qualitätsstandard sicherstellt, erzielt den besonderen Mehrwert des Zentrums für die Bundeswehr. Die überwiegend militärischen, aber auch zivilen Dienstposten im Zentrum für Softwarekompetenz wurden dabei in allen Laufbahnen sowohl als Aufbauverwendungen wie auch als Folgeverwendungen ausgeplant, so dass sich junge, frische Impulse im Bereich neuer Technologien mit operativer Erfahrungen im Einsatz von Software verbinden. Diese Diversität wird durch die intensive Nutzung neuer Personalgewinnungskonzepte konsequent vertieft. So werden Seiten- und Quereinsteiger genauso wie erfahrenes Personal aus der Cyber-Reserve in alle Laufbahnen integriert. Gerade dieser Personal-Mix mit unterschiedlichen Erfahrungshorizonten aus Schule, Truppe, Forschung, Industrie und Wirtschaft erzeugt – vor dem Hintergrund der bisherigen Erfahrungen – die erhofften Synergien zur Verbesserung des Erkennens, Beschaffens und Einführens neuer Technologien.

Softwarekompetenz in der Praxis

Das Zentrum für Softwarekompetenz hat nicht bei null begonnen. Es wurde auf bereits bestehende, vielfältige und tiefgreifende Expertise und Fähigkeiten aufgebaut, die bis dato über alle Bereiche der Bundeswehr verteilt waren. Das Zentrum für Softwarekompetenz erzeugt als noch junge Dienststelle bereits jetzt einen erheblichen Teil der beabsichtigten Wirkung. So war die schnelle Auswahlentscheidung für ein Battle Management System (BMS) für die Very High Readiness Joint Task Force Land 2023 (VJTF(L) 2023) nur unter Rückgriff auf die Fähigkeiten des neuen Zentrums möglich. Auch die für das künftige German Mission Network (GMN) erforderliche deutsche Teilhabe am NATO-Interoperabilitätsprogramm Federated Mission Networking (FMN) wird zu wesentlichen Teilen durch das Zentrum für Softwarekompetenz unterstützt. Gerade die Überprüfung der Einhaltung von NATO-Vorgaben des FMN bei der jährlichen internationalen Übung CWIX wäre für die deutschen Streitkräfte ohne das ZSwKBw und seine Fähigkeiten nicht umsetzbar (zu FMN siehe auch der Artikel „Zielbildung, Digitalisierung und Fähigkeitsentwicklung“ auf Seite 68). Vor dem Hintergrund einer wachsenden Bedeutung der Landes- und Bündnisverteidigung ist es gelungen, die selbst entwickelte IT-Anwendung „Alarmwesen Bundeswehr“ in die Nutzung zu überführen und der Bundeswehr, speziell dem federführenden Kommando Streitkräftebasis, zur Verfügung zu stellen.

Mit der ebenfalls selbst entwickelten Webanwendung „Internet Reconnaissance“ konnte ein Monitoringsystem zur Massendatenverarbeitung für das Zentrum Counter-IED, verantwortlich für die Erkennung und Abwehr von Angriffen mit behelfsmäßigen Spreng- und Brandvorrichtungen (Improvised Explosive Device - IED) bereitgestellt werden. Durch Anpassung an die spezifischen Bedarfe des CIR kann die Anwendung außerdem im Gemeinsamen Lagezentrum im Kommando CIR genutzt werden.

Der „Mission Enabling Service Bw“, der im Projekt Harmonisierung der Führungsinformationssysteme (HaFIS) und dem Führungsinformationssystem des Heeres (FüInfoSys Heer) verfügbar ist, dient der Unterstützung der Einsatz- und Operationsführung auf der strategischen, operativen und taktischen Ebene. Dieser Service bietet enormes Potential für Erweiterungen über standardisierte Programmierschnittstellen (ein sogenanntes Application Programming Interface (API). Hier konnte das Zentrum für Softwarekompetenz die Möglichkeit der Einbindung von zivilen See- und Luftlagen, von Sensoren in Form von Minifunkgeräten oder die Anbindung eines Sharepoint-Servers implementieren und so die Zukunfts- und Ausbaufähigkeit dieses Service für die gesamte Bundeswehr nachweisen.

Bei der Großübung des Ausbildungs- und Übungszentrums Luftbeweglichkeit in Celle stellte die zum Zentrum für Softwarekompetenz gehörende Simulationszentrale der Bundeswehr mehr als 170 Arbeitsplätze mit dem Simulationssystem Virtual Battle Space 3 zur Verfügung und ermöglichte so die Übung in einer hochmodernen, effizienten und wirtschaftlichen virtuellen Umgebung.

Bereits diese Beispiele, die nur einen Ausschnitt der durch das Zentrum bisher bereitgestellten Leistungen abbilden, zeigen, wie sich durch die Aufstellung des Zentrums und das Zusammenfassen von Kompetenzen unter einer Führung die erhofften Synergien schnell entwickelt haben und die Modernisierung von Software vorangeschritten ist.

Wie geht es weiter?

Ein erster Schritt ist getan: Durch das Zusammenwirken unterschiedlicher Fach- und Methodenkompetenzen im neuen Zentrum für Softwarekompetenz der Bundeswehr, und mit dem engagierten und hoch spezialisierten Personal verfügt der Organisationsbereich CIR bereits heute über die Expertise und die Fähigkeit zur schnellen Erschließung neuer Software-Technologien. Hierbei kommt der fachlichen und rüstungstechnischen Beratungsexpertise bei Planung, Architektur und Integration

Die Matrixorganisation ermöglicht die notwendige Flexibilität bei der Projektarbeit. (Foto: Bundeswehr / ZSwKBw / PIZ CIR)

von Softwareprodukten durch das Zentrum für Softwarekompetenz entscheidende Bedeutung zu.

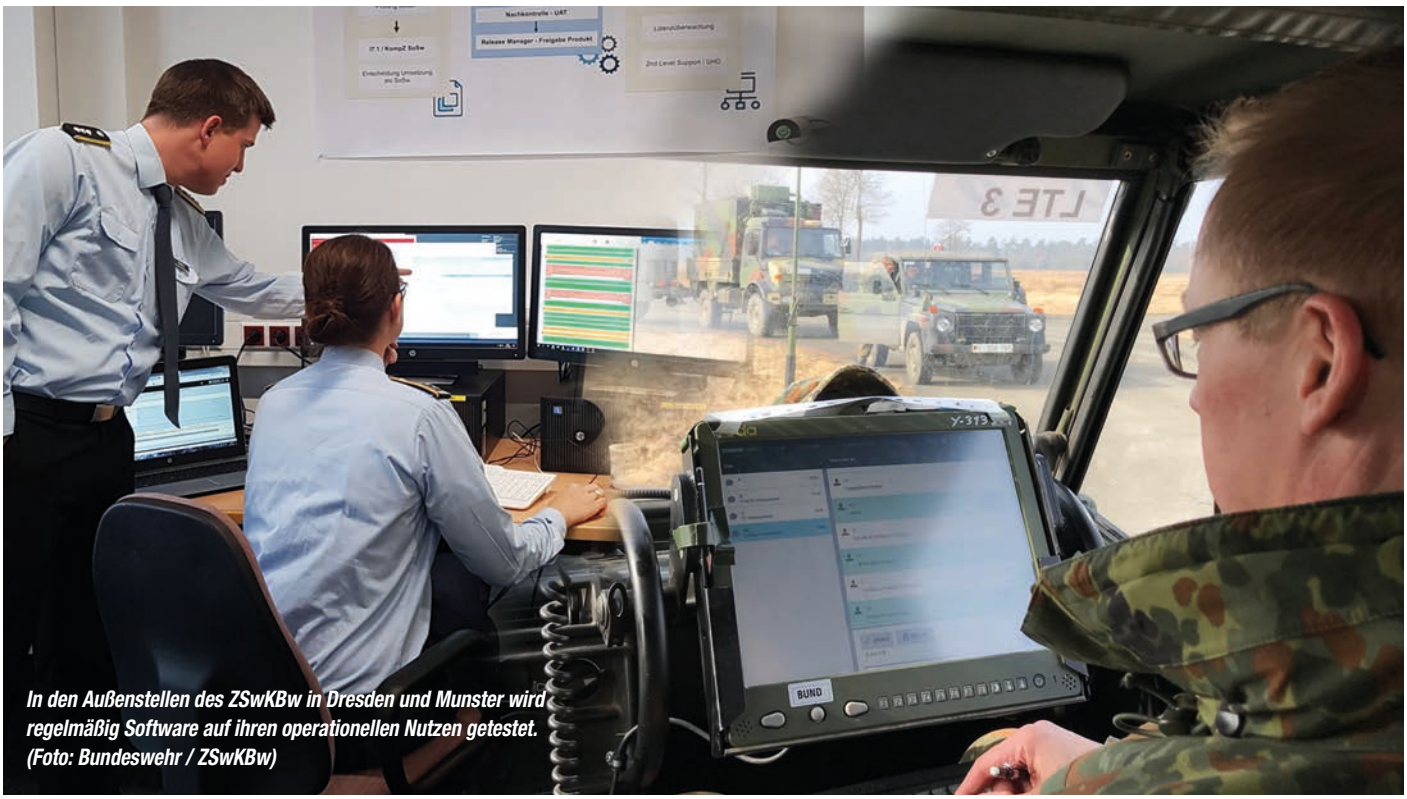
Aber die Entwicklung geht weiter: Mit der modernen, ständig innovativen IT-Welt Schritt zu halten und in vielen Bereichen eigenständig voranzugehen, besteht eine ständige Herausforderung für das Zentrum für Softwarekompetenz. Waren bisher IT-Architekturen überwiegend starr und standardisiert, so reden wir heute von Micro-Services, die als klar definierte Bausteine universell und resilient in verschiedenen Projekten genutzt werden können und müssen. Dies gewährleistet technische Interoperabilität aller Komponenten, ermöglicht technisch die Zusammenarbeit sowohl zwischen den Teilstreitkräften als auch mit internationalen Partnern und kann gleichzeitig sogar Kosten sparen.

War die traditionelle Serviceentwicklung und Servicebereitstellung mitunter von Trägheit und Langfristigkeit geprägt, so stehen heute inkrementelle, skalierbare und flexible Methoden im Vordergrund (beispielsweise Scrum). Sie gilt es nach dem Prinzip Best Practice anzuwenden und auszugestalten. Im Kern geht es um den Aufbau erweiterter Fähigkeiten im querschnittlichen Bereich der „Nutzer-Applikationen und Community of Interest- Services“. Deshalb wird das ZSwKBw hierzu zusätzlich zu den bisherigen Fähigkeiten im einsatzorientierten Anteil des IT-Systems der Bundeswehr seine Kompetenzen für Entwicklung und Integration von mobilen Apps, einschließlich „dismounted services“ (für abgesessene Soldatinnen und Soldaten im Gelände) ausbauen.

Die komplexeste Aufgabe für die Zukunft ist die operationelle Nutzung und fachlich-technische Weiterentwicklung von Künstlicher Intelligenz (KI), eine auch in der Bundeswehr unaufhaltsame Technologie. Hierbei kommt dem ZSwKBw eine wichtige Rolle zu, da KI neue Denkansätze erlaubt und mehr ist als die permanente Verbesserung von Applikationen/Software und IT-Services. Vielversprechende Anwendungsfelder ausgewählter Teilbereiche im Führungs-, Aufklärungs-, Wirkungs- und Unterstützungs-Verbund sind zu identifizieren und zu bewerten. Für die Bundeswehr gilt es herauszufinden, wie KI operativ und operationell sinnvoll genutzt werden kann und an welcher Stelle Arbeitsprozesse erleichtert werden können. Gerade in der komplexen Welt von Big Data, also der Notwendigkeit zur Verarbeitung und insbesondere Auswertung von organisationseigenen Massendaten, gewinnt künstliche Intelligenz eine immer größere Bedeutung. Rasant wachsende Datenmengen, -quellen und -strukturen sowie ein intransparentes und fragmentiertes „Ownership“ von Daten erschweren Lageauswertung und Lagebeurteilung. Durch den Einsatz künstlicher Intelligenz können auch in dieser, durch den Menschen zum Teil nicht mehr zu bewältigenden Informationsflut wichtige Erkenntnisse extrahiert und für eine gemeinsame Lagebeurteilung aufbereitet werden, um so die strategische und operative Steuerung zu verbessern. Neben der Unterstützung von Führungs- und Entscheidungsprozessen kann diese Analyse von Big Data auch zur Weiterentwicklung von Cyber Ranges im Organisationsbereich CIR beitragen. In unterschiedlichen Vorhaben trägt ZSwKBw bereits jetzt zu den Voraussetzungen für die künftig bessere Verarbeitung von Big Data bei, zum Beispiel durch die Entwicklung von Schnittstellen, um unterschiedliche Datenquellen für IT-Services zur Lageführung- und -bearbeitung aufzubereiten und in Lagezentren verfügbar zu machen. Auch im engem Schulterschluss mit wissenschaftlichen Instituten, wie zum Beispiel der Fraunhofer Gesellschaft, aber auch im Austausch mit anderen Innovationsträgern (z.B. CIHBw, BWI, BITKOM) werden in diesem Themenfeld auch kurzfristig Synergien wirksam gemacht. Mit den bereits vorhandenen, aber insbesondere noch auf- und auszubauenden Kompetenzen leistet das Zentrum für Softwarekompetenz einen entscheidenden Beitrag zur Umsetzung der fortschreitenden Digitalisierung und damit für die Erfüllung des Einsatzauftrages der Bundeswehr.

Der Organisationsbereich CIR ist durch das Zentrum für Softwarekompetenz der Bundeswehr deutlich agiler geworden und hat seine Fähigkeiten zukunftsweisend ausgerichtet und erweitert. Auf Entwicklungen in der „IT-Welt“ oder im Cyberraum nicht nur zu reagieren, sondern diese zu antizipieren und neue Herausforderungen, insbesondere auch unter Nutzung disruptiver Software-Technologien proaktiv und flexibel zu gestalten, ist ein wichtiger Schritt in die Zukunft. **wt**

Oberst Peter Hillermann *ist Kommandeur des ZSwKBw und*
Oberst i.G. Hartmut Bock *ist Abteilungsleiter I,*
Innovations- und Qualitätsmanagement im ZSwKBw.



In den Außenstellen des ZSwKBw in Dresden und Munster wird regelmäßig Software auf ihren operationellen Nutzen getestet. (Foto: Bundeswehr / ZSwKBw)

Generalmajor Jürgen Setzer ist als Chief Information Security Officer verantwortlich für die Informationssicherheit in der Bundeswehr (hier bei der NATO-Cyber Defence-Übung LOCKED SHIELDS). (Foto: Bundeswehr / Martina Pump)

Generalmajor Jürgen Setzer

Informationssicherheit für die Bundeswehr

Die Informationssicherheit ist für die Bundeswehr ein hohes Gut. Sie muss vor allem technisch gewährleistet sein, aber auch der „Faktor Mensch" spielt eine wesentliche Rolle. Dem Chief Information Security Officer der Bundeswehr steht hierfür ein breites Instrumentarium zur Verfügung, das das gesamte Spektrum abgedeckt: Von der Prüfung eines Systems noch bevor es in die Nutzung geht, über die großflächige Überwachung und die schnelle „Erste Hilfe" bis zur Sensibilisierung der Bundeswehrangehörigen mit innovativen Methoden.
Verfügbar, integer und vertraulich sollen die Daten der Bundeswehr sein. Dieser Dreiklang der Informationssicherheit ist für die Bundeswehr von grundlegender Bedeutung. Dies gilt umso mehr, je schneller die Transformation zu einer digitalisierten Bundeswehr voranschreitet und für die Auftragserfüllung immer entscheidender wird. Um Ziele, wie zum Beispiel eine Erhöhung der Durchsetzungsfähigkeit der Streitkräfte auf dem digitalisierten Gefechtsfeld oder eine Optimierung im Bereich der Verwaltung zu erreichen, bedarf es daher umfassender und nachhaltiger Gewährleistungsmaßnahmen aus der Informationssicherheit. Im folgenden Beitrag wird aufgezeigt, über welche unterschiedlichen Bereiche und welche Mittel die Bundeswehr zur Umsetzung und Überprüfung dieser Maßnahmen verfügt.

Kommando Cyber- und Informationsraum

Chief Information Security Officer der Bundeswehr (CISOBw)

In vielen Bereichen der Wirtschaft ist die Rolle des Chief Information Security Officer als Gesamtverantwortlicher für die Informationssicherheit schon lange fester Bestandteil einer modernen Unternehmensstruktur. Mit Aufstellung des Kommandos Cyber- und Informationsraum im April 2017 wurde die elementare Rolle des Chief Information Security Officer in der Bundeswehr (CISOBw) als Weiterentwicklung des damaligen IT-Sicherheitsbeauftragten der Bundeswehr implementiert und dem stellvertretenden Inspekteur des Organisationsbereiches CIR übertragen.

Die Funktion des CISOBw umfasst im Schwerpunkt die Überwachung der Informationssicherheit in der Bundeswehr. Er verantwortet zudem das IT-Risikomanagement der Bundeswehr, führt die Informationssicherheitslage für die IT in der Bundeswehr (auch für die embedded IT - also IT-Systeme welche beispielsweise in Maschinen implementiert sind und spezielle Anwendungen abarbeiten) und nimmt die militärischen Interessen zur Informationssicherheit sowohl ressortübergreifend als auch international wahr.

Um diese vielfältigen Aufgaben wahrnehmen zu können, wurden im Kommando CIR zwei Referate in der Referatsgruppe Sicherheitsmanagement als zentrale Steuerungs- und Überwachungselemente eingerichtet und dem Referatsgruppenleiter die Aufgabe des stellvertretenden CISOBw übertragen.

Eine wesentliche Rolle des CISOBw ist die Steuerung der gesamten Informationssicherheitsorganisation der Bundeswehr und hier insbesondere des Zentrums für Cyber-Sicherheit der Bundeswehr (ZCSBw) sowie der Einsatz von Computer Emergency Response Teams der Bundeswehr (CERTBw), der Penetration Test Teams des ZCSBw, sowie der Red Teams des Zentrums Cyber-Operationen. Für den Bereich der Rüstungsprojekte wird der CISOBw unterstützt durch den CISO Rüstung im Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAAINBw). Dieser ist die zentrale Ansprechstelle für die Informationssicherheit in den Projekten des BAAINBw, er koordiniert die dafür notwendigen Maßnahmen projektübergreifend und stellt die diesbezügliche Lage zur Informationssicherheit dem CISOBw zur Verfügung.

Der zunehmende Einsatz und die Digitalisierung von Gebäude- und Liegenschaftstechnik mit einer breiten Masse an handelsüblicher, vernetzter Sensor- und Steuerungstechnik stellen zunehmend eine

Im CSOCBw wird der Netzwerktraffic mit speziellen Tools überwacht (Symbolbild). (Foto: unsplash.com / Chesser)

Bei der NATO-Übung LOCKED SHIELDS erringen die IT-Forensik-Teams der Bundeswehr regelmäßig sehr gute Platzierungen. (Foto: Bundeswehr / Martina Pump)

Herausforderung für die Informationssicherheit dar. Wie der CISO Rüstung wird hier zukünftig ein CISO Infrastruktur den CISOBw durch die Anpassung von Infrastrukturprozessen, dem Einbringen von Forderungen zur Informationssicherheit und bei der Lage zum Sachstand unterstützen.

Zentrum für Cyber-Sicherheit der Bundeswehr (ZCSBw)

Cyber Security Operations Center der Bundeswehr (CSOCBw)

Das CSOCBw ist die Abteilung des ZCSBw, welche die IT-Systeme der Bundeswehr überwacht und auf IT - Sicherheitsvorkommnisse reagiert.

CERTBw - Analysieren, Unterstützen, Eingrenzen

Die Computer Emergency Response Teams der Bundeswehr (CERTBw) des CSOCBw haben zwei Hauptaufgaben. Zum einen stellen sie die sogenannten „Incident Response" Fähigkeiten bereit, mit denen eine ständige weltweite Reaktionsfähigkeit der Bundeswehr auf Informationssicherheitsvorkommnisse, wie etwa Cyber-Angriffe, gewährleistet wird. Zum anderen stellen die CERTBw die IT-Forensik als Fähigkeit der Bundeswehr bereit.

Incident Response-Fähigkeiten: Die Incident Response-Fähigkeiten werden durch mobile Incident Response-Teams sichergestellt. Diese agieren weltweit, überall wo sich Anschlüsse an das IT-Netz der Bundeswehr befinden. Aufgrund hoher Flexibilität und zeitnaher Verfügbarkeit kann somit auch kurzfristig auf Informationssicherheitsvorkommnisse reagiert werden.

Aufgabe eines Incident Response-Teams, das je nach Auftrag aus drei bis vier Personen besteht, ist es, bei einem schwerwiegenden oder technisch anspruchsvollen Informationssicherheitsvorkommnis im IT-System der Bundeswehr:

- das Ausmaß festzustellen,
- die Auswirkungen einzudämmen,
- die Angriffswege und ausgenutzten Schwachstellen zu identifizieren
- digitale Spuren auf Endgeräten und im Netzwerkverkehr zu erkennen
- bei der Wiederherstellung der Informationssicherheit zu unterstützen
- Beweise zu sichern.

Um diesen Auftrag zu erfüllen, steht dem Personal auch im mobilen Einsatz eine umfassende technische Ausrüstung, teilweise mit spezieller Soft- und Hardware, zur Verfügung. Die Mitglieder der Incident Response-Teams sind durch zahlreiche Spezialausbildungen bestens geschult.

Forensik: Im Sachgebiet Forensik werden spezialisierte Fähigkeiten vorgehalten, um zwei Kernaufträge zu erfüllen. Einerseits untersuchen die Spezialistinnen und Spezialisten Informationssicherheitsvorkommnisse. Zum anderen führen sie IT-forensische Untersuchungen bei disziplinarer und, in Amtshilfe, auch strafrechtlicher Ermittlungen durch.

Ist bei einem Informationssicherheitsvorkommnis eine tiefgehende technische Analyse nötig, übergibt das Incident Response-Team die von ihm gesicherten Daten und Hardware an das Sachgebiet Forensik. Hier erfolgt die technische, oft zeitlich sehr aufwendige Analyse. Dabei ist zu beachten, dass alle Ergebnisse gerichtsverwertbar erbracht werden müssen und eine Veränderung der Beweise verhindert werden muss.

Die umfassende digitale Spurensuche beinhaltet sowohl die Analyse, Auswertung und technische Bewertung von Datenträgern und Speichermedien als auch des Kommunikationsverhaltens der Systeme. Es ist wichtig, dass IT-forensische Standards eingehalten und Beweismittel und

Planspiele zeigen dem Nutzenden nicht nur Möglichkeiten der Cyber-Abwehr, sondern ermöglichen ihm und ihr auch, Angriffswerkzeuge und potentielle Angriffspfade kennenzulernen.
(Foto: Bundeswehr / Rana Sarah Wolf)

Arbeitsschritte lückenlos dokumentiert werden. Der abschließende, qualifizierte und objektive Untersuchungsbericht erläutert alle gewonnenen fallrelevanten technischen Erkenntnisse gerichtsverwertbar.

Das Sachgebiet bietet auch fachliche Beratung bei strafrechtlichen und disziplinarrechtlichen Verfahren, insbesondere in Hinblick auf gerichtsverwertbare informationstechnische Datensicherung, -wiederherstellung oder -analyse an und führt diese auch im Rahmen der Amtshilfe durch.

LÜZ - Überwachen, Handeln, Informieren

Das „Lage- und Überwachungszentrum“ (LÜZ) ist ein weiterer Teil des CSOCBw und leistet mit seinen präventiven und reaktiven Aufgaben einen Kernbeitrag zum Erreichen von Cyber- und Informationssicherheit. Das LÜZ erbringt diese Leistung rund um die Uhr, an 365 Tagen im Jahr und ist erste Ansprechstelle für alle Informationssicherheitsbeauftragten der Bundeswehr.

Überwachen: Das LÜZ überwacht die Abstellung der Sicherheitsmängel, die durch die verschiedenen präventiven Maßnahmen des ZCSBw zur Erhöhung des Schutzes der Informationstechnik der Bundeswehr erkannt worden sind und liefert das technische Informationssicherheitslagebild für den CISOBw.

Darüber hinaus wertet das LÜZ rund um die Uhr die Meldungen der Sicherheits-Sensorik des CSOCBw aus, analysiert diese Daten und koordiniert die Bekämpfung von erkannten Angriffen, bis das CERTBw die weitere Bearbeitung übernimmt.

Handeln: Das LÜZ übernimmt das Incident-Management zu erkannten Informationssicherheitsvorkommnissen in erster Verantwortung. Dazu koordiniert das LÜZ die strukturierte Bearbeitung von durch Sensormessungen oder durch Meldungen von IT-Sicherheitspersonal festgestellten Vorkommnissen in Zusammenarbeit mit den Betriebsverantwortlichen und dem CISOBw. Falls erforderlich, findet eine weitere Abstimmung mit dem Gemeinsamen Lagezentrum im Kommando CIR, dem nationalen IT-Lagezentrum im Bundesamt für Sicherheit in der Informationstechnik (BSI) und dem Nationalen Cyber-Abwehrzentrum (Cyber-AZ) statt. Dies dient der Aufrechterhaltung und Wiederherstellung der Informationssicherheit in der Bundeswehr und ist durch die Einbindung des BSI und des Cyber-AZ auch Teil der gesamtstaatlichen Sicherheitsvorsorge.

Informieren: Der CISOBw verantwortet alle Maßnahmen zur Erreichung von Cyber- und Informationssicherheit für die Bundeswehr. Hierzu erfasst das LÜZ alle militärisch relevanten präventiven und reaktiven technischen Informationssicherheitserkenntnisse, setzt diese in ebenen- und zielgruppengerechte Auswertungen um und stellt sie ihm in entscheidungsunterstützender und operativ nutzbarer Form als technisches Informationssicherheitslagebild bereit.

Weiterhin betreibt das LÜZ das Fachinformationssystem „Meldeportal @ller relevanten Vorgänge zur Informationssicherheit“ (M@RVIN), welches die Organisationsbereichsübergreifende Koordinations- und Kooperationsplattform für alle Informationssicherheitsvorkommnisse ist.

Diese Aufgaben unterstreichen die zentrale Rolle des LÜZ für die Aufgabenwahrnehmung des CSOCBw und des CISOBw.

Schwachstellen, Risiken und Schlussfolgerungen für sichere Systeme

Die Angehörigen der Abteilung Überprüfung und Unterstützung im ZCSBw inspizieren alle Dienststellen der Bundeswehr regelmäßig bezüglich der Informationssicherheit, einige sind aber auch Expertinnen und Experten für Schwachstellen in IT-Systemen. Sie führen zwei verschiedene Untersuchungen durch: Schwachstellenanalysen und Penetrationstests.

Die Schwachstellenanalyse der Bundeswehr: Bei der technischen Schwachstellenanalyse werden IT-Systeme der Bundeswehr auf das Vorhandensein bekannter technischer Schwachstellen und Fehlkonfigurationen überprüft. Hierbei werden auf der einen Seite übergreifende Aspekte, wie zum Beispiel die Architektur des Systems oder die Definition von Patch Management Prozessen und auf der anderen Seite die Konfiguration der einzelnen Komponenten und Dienste geprüft. Die hierfür zu Grunde gelegten Vorgaben stammen aus verschiedensten Quellen. Nationale Vorgaben der Bundeswehr und des Bundesamts für Sicherheit in der Informationstechnik kommen hierbei genauso zum Einsatz wie internationale Vorgaben der EU und der NATO oder aber auch Vorgaben der Hersteller und allgemein anerkannte „best practices“.

Eine Schwachstellenanalyse kann bereits während der Akkreditierung von IT-Projekten durch die zuständige Akkreditierungsbehörde der Bundeswehr (Deutsche militärische Security Accreditation Authority) beim Zentrum für Cyber-Sicherheit der Bundeswehr angefordert werden. Aber auch die Informationssicherheitsbeauftragten der Organisationsbereiche sowie der CISOBw können eine Schwachstellenanalyse initiieren. Sie kann für einzelne Dienststellen oder bestimmte IT-Systeme vorgesehen werden.

Als Produkt der Schwachstellenanalyse wird ein Abschlussbericht erstellt. Dieser beschreibt den Umfang der Prüfung, die gefundenen Schwachstellen und die daraus resultierenden Risiken. Abschließend wird dem Auftraggeber zu jeder Feststellung eine Empfehlung ausgesprochen, wie mit den aufgedeckten Schwachstellen weiter zu verfahren ist, um die Sicherheit des Systems zu steigern.

Das Personal der Schwachstellenanalyse durchläuft eine hochspezifische technische Ausbildung und muss ständig fortgebildet werden, um auf dem aktuellen Stand der Technik zu sein. Die hierfür notwendige Ausbildung wird sowohl durch eigenes Personal wie auch durch zivile Bildungsträger durchgeführt.

Die Penetrationstests: Die Schwachstellenanalyse zeigt technische Schwachstellen in IT-Systemen auf. Das Zentrum für Cyber-Sicherheit der Bundeswehr in Rheinbach führt jedoch noch tiefer gehende Analysen durch: Penetrationstests.

Im Dezernat Penetrationstests des ZCSBw arbeiten hochspezialisierte IT-Expertinnen und IT-Experten daran, die Resilienz kritischer IT-Systeme der Bundeswehr gegen Cyber-Angriffe zu prüfen, um dadurch die Cyber-Sicherheit der Bundeswehr in ihrer Gesamtheit zu erhöhen. Penetrationstests sind tiefgehende technische Analysen, bei denen mit speziellen Prüfwerkzeugen realistische Cyber-Angriffe gegen kritische Komponenten oder auch gegen ganze Systeme simuliert werden. Während bei der Schwachstellenanalyse möglichst alle technischen Schwachstellen eines Systems aufgezeigt werden sollen, geht es bei einem Penetrationstest insbesondere darum, die Ausnutzbarkeit vorhandener Schwachstellen aufzuzeigen.

Grundsätzlich werden Penetrationstests im sogenannten „White-Box“ Ansatz durchgeführt. Über den gesamten Penetrationstest hinweg ist eine enge Zusammenarbeit zwischen dem Penetrationsteam und der systemverantwortlichen Nutzerin oder dem systemverantwortlichen Nutzer für eine erfolgreiche Durchführung unabdingbar. Nach dem Abschluss eines Penetrationstests werden die gewonnenen Erkenntnisse genutzt, um auf das geprüfte System zugeschnittene Handlungsempfehlungen zu erstellen und somit die Cyber-Sicherheit des Systems dauerhaft zu erhöhen. Durch die dabei vorgenommene Risikobewertung stehen dem jeweiligen Systemverantwortlichen wesentliche Informationen sowohl für kurzfristige Verbesserungen als auch für zukünftige Planungen zur Verfügung.

Im derzeitigen Fokus von Penetrationstests in der Bundeswehr stehen Waffen- und Sondersysteme, bedingt durch die immer weiter voranschreitende Digitalisierung. Darüber hinaus werden auch Führungsinformationssysteme, kritische IT-Projekte, IT-Services und Anwendungen untersucht. Die Spezialistinnen und Spezialisten für Penetrationstests sind zudem in der Lage, Firmware, Codes und nicht IP-basierte Protokolle zu analysieren.

Zukünftig ist Penetration Testing bereits in der Rüstungsphase vorgesehen, um kritische Schwachstellen bereits in der Entwicklung zu erkennen und deren Behebung noch vor der Überführung in die Nutzung zu ermöglichen.

Mit der Brille eines Angreifers - Das Red Teaming

Regelmäßig werden im Betrieb befindliche IT-Systeme der Bundeswehr auf ihre Sicherheit mit dem sogenannten Red Teaming überprüft. Mit der Brille eines Angreifers stellt man sich der Frage: Wo könnten „wir“ größtmöglichen Schaden anrichten? Wo ist die IT der Bundeswehr am verwundbarsten? Ist das Ziel ausgemacht, versuchen die „hauseigenen“ Spezialisten im Zentrum Cyber- Operationen, im laufenden Betrieb „den besten Weg hinein“ zu finden. Sie stehen dabei einem realen Verteidiger gegenüber. Diese Angriffssituationen sind realitätsnah verdeckt und können sich über einen langen Zeitraum erstrecken. Sie sind besonders geeignet, blinde Flecken in der Sicherheitsarchitektur zu finden.

Mit Hilfe dieser Cyber-Sicherheitsmaßnahme ist es möglich auf „Champions-League-Niveau“ die vorhandene Angriffshürde für einen wirklichen Angreifer realistisch zu beurteilen. Zudem werden wertvolle Erkenntnisse über den Reifegrad der IT-Infrastruktur sowie die Prozesse innerhalb der Organisation gewonnen.

Abgrenzung zwischen Red Teaming, Penetrationstests und Schwachstellenanalyse

In der unten stehenden Tabelle werden Red Teaming, Penetrationstests und Schwachstellenanalyse gegenübergestellt. Das ZCSBw führt ausschließlich Penetrationstests und Schwachstellenanalysen durch. Red Teaming ist eine Fähigkeit des Zentrums Cyber-Operationen.

Schutz und Prävention

Information Security Awareness (InfoSec Awareness): Eine der besten Sicherheitsmaßnahmen sind gut ausgebildete und sensibilisierte Nutzerinnen und Nutzer. Angreifer nutzen verschiedene menschliche Eigenschaften, wie zum Beispiel Angst oder Neugier, als Schwachstelle aus, um beispielsweise mittels „Phishing“ Zugang zu einem Computer zu bekommen. Vom infiltrierten Computer aus versuchen die Angreifer in das Netzwerk einzudringen und sich dann weiter in Richtung des eigentlichen Ziels vorzuarbeiten.

Informationssicherheitsbeauftragte in jeder Dienststelle: Um einem Angreifer den Zugriff auf die IT der Bundeswehr zu erschweren, werden Vorgaben bezüglich der Konfiguration von Computern und Netzwerkkomponenten sowie Vorschriften für die Nutzer zum Umgang mit ihrer IT gemacht. Zur Erhöhung der Wachsamkeit gegen solche Angriffe ist eine regelmäßig wiederkehrende Sensibilisierung des Nutzers im Umgang

Komplex, individualisiert	Level 3	Level 2	Level 1	Strukturiert automatisiert
	Red Teaming	Penetrationstests	Schwachstellenanalyse	
	Finden einer Schwachstelle zum Test dahinterliegender Prozesse in komplexen Umgebungen (Netze, Verbund, ...)	Finden möglichst vieler Schwachstellen des zu prüfenden Systems und exemplarische Ausnutzung	Finden möglichst aller bekannten technischen Schwachstellen des zu prüfenden Systems	
	Verdecktes Vorgehen	Alle Beteiligten sind eingebunden	Alle Beteiligten sind eingebunden	
	Individualisiertes Vorgehen (pragmatischer Ansatz)	Systematisches, strukturiertes Vorgehen	Systematisches, strukturiertes Vorgehen	
	Zielsystem im operativen Betrieb	Zielsysteme in Entwicklung, Testbetrieb und Nutzung	Zielsysteme in Testbetrieb und Nutzung, (Re-)Akkreditierung	
	Zugang zum Zielsystem nur über verfügbare Angriffsvektoren (z.B. Internet)	Zugang zum Zielsystem beliebig	Zugang zum Zielsystem beliebig	
	Schrittweise Bewegung im Netzwerk, um unbeobachtet zu bleiben (Lateral Movement)	Ganzheitliche Betrachtung dedizierter Systeme/Anwendungen	Manuelle und automatisierte Suchen, Interviews	

Abgrenzung zwischen Red Teaming, Penetrationstests und Schwachstellenanalyse.
(Grafik: Bundeswehr / ZCSBw / PIZ CIR)

mit IT notwendig. Hierfür verfügt jede Dienststelle der Bundeswehr über einen Informationssicherheitsbeauftragten.

Aufgabe der Expertinnen und Experten für Sensibilisierung im ZCSBw ist es, diese Beauftragten beispielsweise dadurch zu unterstützen, indem sie Inhalte der regelmäßigen Sensibilisierung weiterentwickeln und medial aufbereiten. Dabei darf dem Nutzer auch Wissenswertes für den privaten Gebrauch vermittelt und so das Interesse für das Thema Informationssicherheit gesteigert werden. Das Maßnahmenpaket ist vielfältig: So sollen die Dienststellen beispielsweise einmal jährlich einen Information Security Awareness Tag durchführen, um ihre Angehörigen über die sich ständig ändernden Gefahren des Cyber-Raums und neue Angriffsmöglichkeiten zu informieren. Dazu sollen die Informationssicherheitsbeauftragten mit den Angehörigen ihrer Dienststellen in ein aktives Gespräch eintreten.

Einen Ansatz, um PowerPoint-Präsentationen als einziges Präsentationsmittel zu überwinden und Sicherheitsthemen attraktiver darzustellen, stellt das Konzept „Gamification“ dar, bei dem die Vermittlung von Wissen mit Hilfe spieltypischer Elemente erreicht werden soll. Das Portfolio reicht hier von einfachen Spielkarten bis hin zu Planspielen, in denen Cyber-Angriffs- und -Abwehr-Szenarien durchspielt werden. Diese Gamification-Produkte, aber auch neue Poster, Flyer und themenspezifische Präsentationen, werden in Zusammenarbeit mit der Arbeitsgruppe InfoSecAwareness des Kommandos CIR erarbeitet. Dort sind Angehörige der Bundeswehr, des Bundesministeriums der Verteidigung (BMVg) und der BWI vertreten.

Die BWI ist der zentrale Dienstleister der Bundeswehr für Informations- und Kommunikationstechnik. Die Arbeitsgruppe versteht sich selbst als Think Tank für neue Awareness-Produkte, die den Informationssicherheitsbeauftragten der Bundeswehr in einem Downloadportal zur Verfügung gestellt werden.

Aktive Bewusstseinsschärfung durch Phishing-Kampagnen: Regelmäßig sind Mitarbeiterinnen und Mitarbeiter im Geschäftsbereich BMVg Ziel von Phishing-Mails – dies ist aktuell eines der größten Einfallstore für Schadsoftware. Es sind nicht nur finanzielle Schäden möglich, sondern auch die Gefährdung von Leib und Leben der Soldatinnen und Soldaten im Einsatz. Die Gefahr entsteht insbesondere dann, wenn die erforderliche Achtsamkeit fehlt und die Phishing-Mail als solche nicht erkannt und entsprechend gehandelt wird.

Eine Achtsamkeit bei den IT-Nutzenden flacht normalerweise ohne Wiederholung der Schulung nach wenigen Tagen und Wochen wieder ab. Eigene Erlebnisse und besonders die eigene Betroffenheit von einem IT-Sicherheitsvorkommnis schaffen bleibende Eindrücke. Bei der Bundeswehr wird dies „einsatznah ausbilden“ genannt.

Daher führt der CISOBw unter anderem eine auf Dauer angelegte Phishing-Awareness-Kampagne durch. So werden die IT-Nutzenden im Umgang mit Mails von unbekannten Absendern aktiv sensibilisiert. Den Personen und dem IT-System in der Bundeswehr wird dabei kein Schaden zugefügt.

Ziel solcher Kampagnen ist es, durch Versenden von fingierten Phishing-E-Mails das Bewusstsein über Gefahren aus dem Cyber- und Informationsraum und die Bedrohung durch Phishing und Spear-Phishing zu steigern und dabei die IT-Nutzenden auf allen Führungsebenen zu erreichen.

Durch die Reflexion des eigenen Verhaltens und Hinweise auf das mögliche Erkennen solcher „gefährlichen E-Mails“ soll eine nachhaltige Verhaltensänderung und Stärkung des Verantwortungsgefühls der Bundeswehrangehörigen im Umgang mit E-Mails und deren Anhängen erreicht werden.

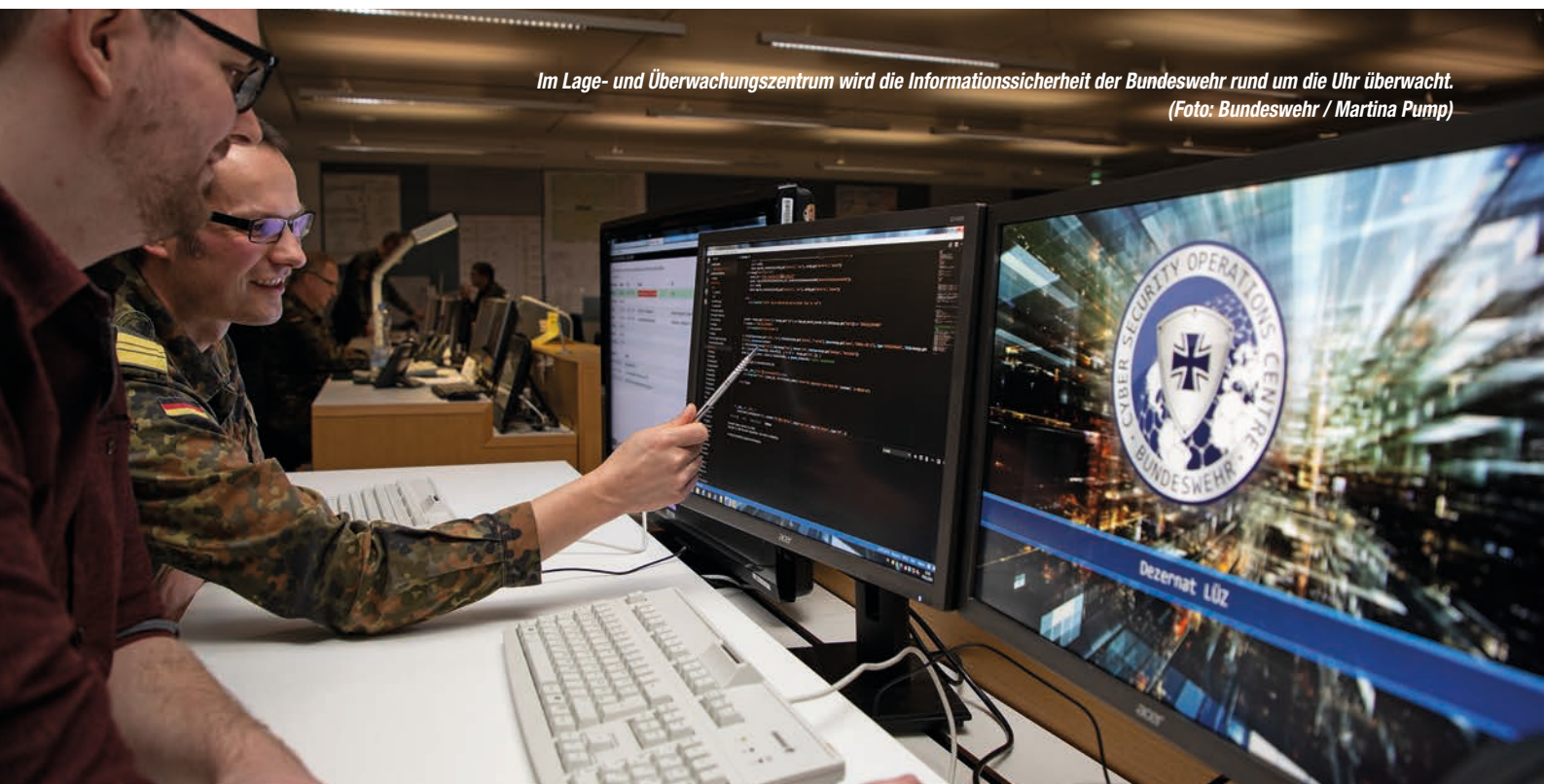
Fazit

Die Informationssicherheitsorganisation der Bundeswehr mit dem CISOBw an der Spitze verfügt mit den Informationssicherheitsbeauftragten in den Dienststellen und Projekten als dezentrale Elemente sowie mit dem ZCSBw als zentralem Element über eine umfangreiche und innovative Struktur. Damit ist sie gut aufgestellt, um die Sicherheit in der IT der Bundeswehr zu überwachen, technische und organisatorische Schwachstellen zu erkennen und sie durch die jeweils Verantwortlichen wirksam abstellen zu lassen.

Damit der Schutz vor dem Hintergrund der wachsenden Bedrohungen im Cyber-Raum wirksam bleibt, tragen alle Angehörigen der Bundeswehr in ihrer jeweiligen Funktion – egal ob als IT-Nutzende, Administratoren, Truppenführerinnen oder Projektleitende – mit ihrer Sensibilisierung dazu bei.

wt

Generalmajor Jürgen Setzer *ist Stellvertreter Inspekteur CIR und Chief Information Security Officer der Bundeswehr.*



Im Lage- und Überwachungszentrum wird die Informationssicherheit der Bundeswehr rund um die Uhr überwacht. (Foto: Bundeswehr / Martina Pump)

Blick in das Network Operation Center (NOC) des Betriebszentrums IT-System der Bundeswehr (BITS) in Rheinbach. (Foto: Bundeswehr / Martina Pump)

Generalmajor Dr. Michael Färber

Das IT-System der Bundeswehr
Einheitlich trotz verschiedener Provider?

Staat, Wirtschaft und Gesellschaft werden in unserer zunehmend vernetzten und digitalisierten Welt tagtäglich abhängiger vom Cyber-Raum und damit in der Folge verwundbarer für entsprechende Angriffe. Diese Erkenntnis führte vor drei Jahren dazu, in der Bundeswehr einen neuen militärischen Organisationsbereich Cyber- und Informationsraum (OrgBer CIR) aufzustellen. Gleichwohl, allein die Aufstellung des OrgBer CIR beantwortet selbstverständlich nicht automatisch alle Fragen, die im Kontext Cyber und IT für die Bundeswehr offen und drängend sind.

Überblick

- Wie reagiert die Bundeswehr auf die zunehmende Digitalisierung?
- Wie kann die Bundeswehr bei Einsätzen im Ausland, fernab von ortsfesten, meist unterirdischen Netzwerkleitungen, sich selbst schützen?
- Modernste Netzwerktechnik, immer schnellere Datenübertragung im GBit/s-Bereich und hochverfügbarer Datenzugriff: Alles selbstverständliche „IT-Services“ für die heutige Gesellschaft. Doch wie schaffen es die Streitkräfte der Bundesrepublik Deutschland, ebenfalls „up to date“ zu bleiben und moderne IT-Standards des 21. Jahrhunderts zum eigenen militärischen Vorteil zu nutzen?

Alle diese Fragen müssen unverändert beantwortet werden. Der OrgBer CIR und darin unser Kommando Informationstechnik der Bundeswehr (KdoITBw) spielen dabei eine zentrale Rolle. Dieser Artikel soll einen kurzen Einblick in unsere aktuellen und zukünftigen Handlungsfelder im KdoITBw geben.

Das KdoITBw wurde im Jahr 2013 zunächst als Führungsunterstützungskommando der Bundeswehr in Bonn aufgestellt und ist seit 2017 Bestandteil des neuen OrgBer CIR – bei gleichzeitiger Umbenennung in seinen aktuellen Namen. Wir im Kommando tragen die alleinige Verantwortung, IT-Services – also Dienstleistungen im Bereich der Informationstechnik – in Form von definierten Fähigkeiten für die Bundeswehr bereitzustellen, egal wann immer und wo immer sie diese benötigt. Gleichzeitig liefern wir unseren Beitrag zu den Antworten auf die oben skizzierten Fragen.
Unsere Kernaufgabe im KdoITBw lässt sich in vier funktionale Bausteine einteilen:

- IT-Services für militärische Dienststellen im In- und Ausland – also das weltweite Sicherstellen der Führungsfähigkeit in militärischen Dienststellen, bei einsatzgleichen Verpflichtungen und bei Dauereinsatzaufgaben.
- IT-Services für weitreichende Anbindung und Vernetzung – ermöglichen die Verlängerung des IT-Systems der Bundeswehr (IT-SysBw) vom Heimatland bis an den jeweiligen Einsatzort im Ausland.
- IT-Services für stationäre und verlegefähige Einrichtungen – bilden das Sicherstellen der Vernetzung innerhalb der Einsatzgebiete und von verschiedenen Einsatzgebieten untereinander ab.
- IT-Services für mobile Elemente – diese umfassen das Sicherstellen der Anbindung und die Vernetzung mobiler und hochbeweglicher, auch abgesessener Kräfte im Einsatzgebiet vor Ort.

Zur Erfüllung dieser Aufgaben verfügen wir im KdoITBw für Einsatz, Betrieb und Schutz des IT-SysBw über das Betriebszentrum IT-System

Ein IT-Feldwebel baut während der Mission Resolute Support in Mazar-e Sharif / Afghanistan eine Satellitenanlage auf. (Foto: Bundeswehr / Andrea Bienert)

der Bundeswehr (BITS) in Rheinbach sowie das Zentrum für Cyber-Sicherheit der Bundeswehr (ZCSBw) in Euskirchen, über aktuell sechs Informationstechnikbataillone (IT-Bataillone) für die verlegefähigen Anteile des IT-SysBw sowie die Schule für Informationstechnik der Bundeswehr, die die IT-fachliche Ausbildung für die gesamte Bundeswehr gewährleistet (hierzu siehe auch der Beitrag auf Seite 53). Im April 2019 wurde zusätzlich das Zentrum für Softwarekompetenz der Bundeswehr dem Leistungsportfolio des KdoITBw neu hinzugefügt. Es ist als zentraler Kompetenzträger für die operationelle Nutzung und Weiterentwicklung von Software in der Bundeswehr verantwortlich (siehe auch den Beitrag zum Zentrum für Softwarekompetenz der Bundeswehr auf Seite 16).

Wie werden mit diesen Dienststellen die genannten vier funktionalen Bausteine sichergestellt?

Unsere übergreifende Hauptaufgabe im KdoITBw ist die zuverlässige und hochverfügbare Bereitstellung von IT-Services, an jedem Ort der Welt und zu jeder Zeit (24/7)

Dazu übernehmen wir im KdoITBw in unserer Rolle als „zentraler Supply-Manager IT-SysBw“ die Planung, den Einsatz sowie Betrieb und Schutz des IT-SysBw. Aus dem BITS heraus wird dafür die zentrale Betriebssteuerung gewährleistet. Gleichzeitig wird dort auch das IT-Lagebild gesamtheitlich erstellt, überwacht und bewertet. Die Aufgaben zum Schutz des IT-SysBw werden im engen Zusammenspiel mit dem Chief Information Security Officer der Bundeswehr durch das ZCSBw wahrgenommen (siehe auch den Beitrag über die Informationssicherheit auf Seite 21).

Im militärischen Sinn wird ein IT-Service über die benötigte Funktionalität und über die Bereitstellung der für die Leistungserbringung notwendigen Ressourcen in einem IT-Servicekatalog definiert. Zur Unterstützung aller Führungs- und Geschäftsprozesse des Verteidigungsressorts wird auf personelle, organisatorische, infrastrukturelle und materielle Elemente des IT-SysBw zurückgegriffen. Das IT-SysBw bildet somit den bundeswehrgemeinsamen Informations- und Kommunikationsverbund, der wiederum IT-Services durch unterschiedliche IT-Serviceprovider bereitstellt.

Das Kommando Informationstechnik der Bundeswehr ist in Bonn auf der Hardthöhe beheimatet. (Foto: Bundeswehr / KdoITBw)

Das Portfolio der durch die Bundeswehr selbst bereitgestellten Fähigkeiten wird durch die Fähigkeiten ziviler beziehungsweise gewerblicher IT-Serviceprovider in Quantität und Qualität jeweils bedarfsgerecht ergänzt. Zusätzlich können auch Fähigkeiten von Partnernationen und Bündnissen (NATO) sowie anderen zivilen und staatlichen Organisationen integriert werden. Dadurch wird sichergestellt, dass die geforderte Leistungserbringung serviceorientiert durch die Streitkräfte erbracht werden kann. Serviceorientierung bedeutet dabei die Fokussierung auf die Leistungserbringung für die Nutzenden durch die betriebliche Bereitstellung von IT-Services und damit auf das Ziel, den Nutzenden IT-Services auf Basis der geforderten Funktionalitäten in der durch ihn geforderten Qualität und Quantität zur Verfügung zu stellen.

Vom militärischen Nutzer („Demander“) werden grundsätzlich keine Systeme gefordert, sondern Fähigkeiten

Konkret bedeutet das, dass eine vom Nutzer oder der Nutzerin geforderte Fähigkeit, der „Demand“, beispielsweise die Fähigkeit, verschlüsselte eMails „von A nach B“ versenden zu können, technisch durch unseren Kommandobereich realisiert und dem Nutzer über definierte Schnittstellen, wie etwa einen Computer, bereitgestellt wird. Dabei werden die an das Kommando gestellten Forderungen aus allen Bereichen nicht in Form einer „Einkaufsliste“ mit Benennung der gewünschten Produkte an uns herangetragen. Vielmehr kommt es darauf an, dass jeder und jede Nutzende vorab möglichst genau die Funktionalitäten und Fähigkeiten definiert, die für seinen oder ihren Auftrag erforderlich sind. Die „Übersetzung“ dieser Forderungen in technische Systeme oder zumeist komplexe Verbünde technischer Systeme ist die Aufgabe des „Suppliers“, also unserer Expertinnen und Experten im KdoITBw und unserem nachgeordneten Kommandobereich.

Bei Einsätzen der Bundeswehr im Ausland tritt das Einsatzführungskommando der Bundeswehr (EinsFüKdoBw) in Potsdam als zentraler „Demander“ auf. Das bedeutet, dass es die Aufgabe hat, die Vielzahl an operativ begründeten oder konzeptionell abgeleiteten Bedarfsforderungen der verschiedenen Nutzenden zu sammeln und zu

bündeln. Die Überführung dieses gebündelten „Demands“ in ein Konzept zur Bereitstellung der benötigten IT-Services geschieht danach in einem iterativ zu durchlaufenden Prozess zwischen EinsFüKdoBw und uns im KdoITBw.

Diese Vorgehensweise, der „Demand-Supply-Prozess“, hat sich in den letzten Jahren bewährt und ist inzwischen eingespielt. Nur so kann es überhaupt gelingen, die Führungsfähigkeit der Bundeswehr in Einsätzen und bei Übungen sowie von militärischen Dienststellen im In- und Ausland durch die Bereitstellung von IT-Services sicherzustellen.

Die Bundeswehr speichert ihre Daten nicht lokal auf dem Desktop

In verschiedenen Rechenzentren, die als das Herz der Bundeswehr-IT bezeichnet werden können, werden sämtliche Daten und IT-Services der Bundeswehr jederzeit abrufbar vorgehalten. Diese Rechenzentren werden durch die BWI und die Streitkräfte an unterschiedlichen Standorten innerhalb Deutschlands betrieben.

Die von der BWI betriebenen Rechenzentren befinden sich an den Standorten Wilhelmshaven, Strausberg, Köln-Wahn und Bonn. Militärische Rechenzentren werden an den Standorten Mechernich und Gelsdorf betrieben.

Da diese „alte IT-Infrastruktur“ historisch und daher technisch heterogen gewachsen ist, muss sie modernisiert sowie der Betrieb und das Management zukunftsfähig ausgerichtet werden. Dieser neue Rechenzentrumsverbund wird, so die Zielvorstellung, ein logischer, skalierbarer und modular erweiterbarer Verbund von Rechenzentren in mindestens zwei georedundanten Regionen sein. Zusätzlich wird ein Disaster Backup Centre (DBC) eingerichtet. Das DBC wird sämtliche Datensicherungen aufnehmen, um auch bei Ausfall aller stationären Rechenzentren einen Datenverlust zu vermeiden. Die Rechenzentren des genannten Verbundes und das DBC bilden dann den „stationären Anteil“ in der Basis Inland des IT-SysBw.

Ziel von Bundeswehr und BWI ist die Angleichung an zivile Standards

In diesem System soll die BWI zukünftig befähigt werden, gemeinsam mit der Bundeswehr alle IT-Services (darunter auch einsatzrelevante IT-Services) für den Geschäftsbereich des Bundesministeriums der Verteidigung (BMVg) als zentraler Provider zu unterstützen und Leistungen im Verbund mit der Bundeswehr gemeinsam zu realisieren. So wird etwa die Steuerung der vorgenannten stationären Anteile durch unser ausgebildetes IT-Fach- und Funktionspersonal der Bundeswehr gemeinsam mit der BWI in einem kooperativen Betriebsmodell

Auslandseinsatz KFOR:
Die BWI verantwortet den technischen Betrieb des IT-Netzes für die Bundeswehr in Pristina / Kosovo.
(Foto: Bundeswehr / Marc Tessensohn)

sichergestellt werden. Konkret heißt das, dass das Personal der zivil geführten BWI gemeinsam mit Soldatinnen und Soldaten für den Betrieb und die Steuerung eines gemeinsamen, durchgängigen IT-Systems der Bundeswehr verantwortlich sein wird. Dabei wird der sachgerechten „Durchmischung“ des zivilen und des militärischen Personals innerhalb der Betriebsführungseinrichtungen eine wesentliche Bedeutung als Erfolgsfaktor für den Rechenzentrumsverbund des Geschäftsbereiches BMVg zukommen.

Dass dieser Weg überhaupt beschritten werden kann, ist nur möglich, weil bereits zu Zeiten des Führungsunterstützungskommandos der Bundeswehr, aber auch später in Verantwortung des KdoITBw das Ziel verfolgt wurde und wird, militärische IT-Prozesse und Verfahren an zivile Standards und etablierte Verfahren anzugleichen.

Als gutes Beispiel dafür kann das IT-Service Management angeführt werden. Der damit beschriebene Betrieb und die Steuerung des IT-SysBw orientieren sich eng am (zivilen) Rahmenwerk der „Information Technology Infrastructure Library“, – kurz (ITIL). ITIL ist eine Sammlung vordefinierter Prozesse, Funktionen und Rollen, wie sie typischerweise in jeder IT-Infrastruktur mittlerer und großer Unternehmen angewendet werden. Diese haben sich, teilweise mit moderaten Anpassungen, als geeignet auch für die Anwendung in der Bundeswehr erwiesen. Erst ihre konsequente Umsetzung ermöglicht es uns nun, zivile Provider quasi bruchfrei an unser System anzubinden und mit der BWI sogar eine noch intensivere Vernetzung der IT-Services zu realisieren.

Klar ist dabei aber auch: Das oben beschriebene Kooperationsmodell kann nur dann erfolgreich sein, wenn die jeweils vereinbarte Servicequalität durchgehend gewährleistet wird. Ziel muss es also sein, eine messbare Leistungssteigerung der Bereitstellung von IT-Services durch die Streitkräfte und die BWI im Grundbetrieb und Einsatz, immer unter Gewährleistung der Informationssicherheit, zu realisieren.

Künftig wird ein erweiterbarer Rechenzentrumverbund die Daten der Bundeswehr beherbergen.
(Foto: Bundeswehr / Stephan Ink)

Die Informationstechnikbataillone sind unsere mobilen Einsatzkräfte – weltweit

Neben dem dargestellten „stationären Anteil“ bilden die sechs IT-Bataillone den zweiten,

BWI GmbH

Die BWI GmbH ist eine 100-prozentige Bundesgesellschaft und zählt mit 44 Standorten zu den Top-10 der IT-Service-Unternehmen in Deutschland.

Als langjähriger IT-Partner der Bundeswehr unterstützt sie die Streitkräfte bei ihrer digitalen Transformation und betreibt weite Teile des IT-Systems der Bundeswehr. Die BWI ist IT-Systemhaus und Digitalisierungspartner der Bundeswehr und IT-Dienstleistungszentrum des Bundes.

Ende 2006 als öffentlich-private Partnerschaft zwischen Siemens, IBM und der Bundeswehr gestartet, ist der IT-Dienstleister seit Ende 2016 ein privatwirtschaftliches Unternehmen mit dem Bund als alleinigem Gesellschafter.

(Grafik: Bundeswehr / KdoITBw)

„verlegefähigen Anteil" unserer Struktur. Die technische Führungsfähigkeit in den Einsätzen sicherzustellen ist ein zentrales, bestimmendes Element in der Gesamtkonzeption, ohne das andere mobile und stationäre militärische Kräfte nicht in der Lage wären, einen Einsatz über weite Entfernungen zu steuern oder zu koordinieren. Der Einsatz von mobilen IT-Kräften ist deshalb eine zentrale Kernkompetenz der Bundeswehr.

Mit ihren mobilen und verlegefähigen IT-Systemen bilden unsere IT-Bataillone diese Kernkompetenz ab. Mit fachlich hochqualifizierten Soldatinnen und Soldaten sowie leistungsfähigen IT-Systemen verfügen diese Bataillone unter anderem über Fähigkeiten in den Bereichen Satellitenkommunikation, Netzwerktechnik, Servertechnik, verschlüsselte mobile Kommunikation, digitaler Richtfunk und zunehmend auch im Bereich der Datenverarbeitung, als der Bereitstellung von Software. Gerade bei einer entsprechenden Gefährdungslage im Einsatzgebiet können nur noch diese Soldatinnen und Soldaten die IT-Aufgaben übernehmen, externe zivile IT-Dienstleister jedoch nicht. Dennoch soll die BWI zukünftig auch in ausgewählten Stabilisierungseinsätzen – genau wie im Inland – die Streitkräfte noch stärker unterstützen und damit dabei helfen, dringend benötigte mobile IT-Kräfte für operative Aufgaben in der Landes- und Bündnisverteidigung verfügbar zu machen.

Die BWI – der hauseigene IT-Unterstützer des KdoITBw – verlegt in die Hauptstadt des Kosovo

Ende 2017 wurde die Entscheidung getroffen, erstmalig die BWI beim Neuaufbau eines Netzes im Einsatz einzubinden. Hintergrund für diese Maßnahme war die politische Entscheidung, den Einsatzstandort Prizren im Kosovo zu schließen und das deutsche Einsatzkontingent KFOR in die Einsatzliegenschaft Pristina zu verlegen. Dies machte umfangreiche IT-Umstrukturierungsmaßnahmen notwendig; so musste beispielsweise das gesamte IT-Netz in Prizren zurückgebaut werden, am neuen Standort Pristina stand dagegen kein übernahmefähiges militärisches Netz zur Verfügung.

In dieser Situation kam es im November 2017 zu ersten Abstimmungsbesprechungen zwischen unserem KdoITBw und der BWI. Wegen der vorgegebenen Zeitlinien für den Umzug des Einsatzkontingentes musste jedoch die gesamte Technik bereits ein Jahr später funktionsfähig in Pristina stehen – ein harter Zeitplan für ein Pilotprojekt!

Bei der Umsetzung traten schnell eine Reihe von besonderen Herausforderungen auf, die technischer, IT-sicherheitstechnischer aber zum Beispiel auch arbeits- und exportrechtlicher Art waren. Trotzdem konnte der Zeitplan aufgrund des durchgehend hohen Engagements aller Beteiligten eingehalten werden, so dass die BWI nunmehr seit Oktober 2018 den technischen Betrieb des IT-Netzes für die Bundeswehr im Auslandseinsatz KFOR übernommen hat. Ein Meilenstein auf dem Weg zu einer noch engeren Verbindung der beiden „Welten" Bundeswehr und BWI.

Die erarbeitete technische Lösung sieht eine Anbindung des Einsatzkontingentes analog zu einer Liegenschaft in Deutschland vor. Das bedeutet, dass alle Serverdienste aus Rechenzentren in Deutschland betrieben und als Service im Einsatzkontingent genutzt werden. Das IT-System der Bundeswehr wird somit „einfach" von Deutschland aus in das Einsatzland verlängert.

Durch diese geschickte Lösung wurde es möglich, bislang für die Datenübertragung und die Datenverarbeitung genutzte militärische Systeme in erheblichem Umfang zurückzubauen und somit wieder für andere militärische Verpflichtungen nutzbar zu machen.

Gleichzeitig gelang es, den militärischen IT-Personalansatz im Einsatzland auf ein operativ notweniges Minimum zu reduzieren. Da es sich bei unserem IT-Personal um hoch qualifizierte IT-Spezialistinnen und IT-Spezialisten handelt, konnte durch die Unterstützung der BWI somit auch ein echter personeller Mehrwert und eine spürbare Entlastung für unsere IT-Bataillone geschaffen werden.

Natürlich kann die Lösung im KFOR-Einsatz nicht einfach auf andere Einsatzgebiete übertragen werden, da stets die jeweiligen Gegebenheiten in den unterschiedlichen Einsatzgebieten zu berücksichtigen sind. Abhängig von der Sicherheitslage und den operativen Anforderungen wird es in vielen Einsatzgebieten notwendig sein, die Aufgabenwahrnehmung vor Ort bei der Bundeswehr zu belassen und lediglich auf unterstützende Leistungen der BWI zurückzugreifen.

Gleichwohl gilt: Diesem gelungenen Pilotprojekt können und müssen weitere folgen, in denen die BWI die Bundeswehr an verschiedenen Punkten der IT-Servicebereitstellung noch intensiver unterstützt.

Die Übernahme von weiteren Funktionen in Einsatzliegenschaften durch die BWI ist dabei immer nur eine denkbare Option. Der Schwerpunkt liegt unverändert auf der Entlastung unserer militärischen IT-Kräfte im Einsatz aus Deutschland heraus und der Unterstützung bei der Konzeption, Planung und Konfiguration von IT-Systemen. Dies alles geschieht immer vor dem Hintergrund, unsere militärischen IT-Spezialistinnen und IT-Spezialisten dort einzusetzen, wo ihr Einsatz notwendig ist, und die Expertise der BWI immer dort zu nutzen, wo es möglich ist!

Zusammenfassung

Diese wenigen, nur schlaglichtartig beleuchteten Facetten unserer Arbeit im KdoITBw und dem nachgeordneten Kommandobereich machen – so denke ich – deutlich, dass hier jeden Tag erneut daran gearbeitet wird, der gesamten Bundeswehr immer diejenigen IT-Services zur Verfügung zu stellen, die sie braucht, um unseren gemeinsamen Auftrag der Teilhabe an Einsätzen sowie im Rahmen der Landes-/Bündnisverteidigung zu erfüllen.

Dabei immer die bestmögliche Qualität und Quantität zu liefern und gleichzeitig stetig an der Verbesserung von Effizienz und Effektivität zu arbeiten, gleicht ein wenig der so oft bemühten „Operation am offenen Herzen".

Dass der „Patient IT-SysBw" aber nicht nur überlebt, sondern sich einer immer besseren und stabileren Gesundheit erfreut, unterstreicht die Expertise und das Engagement unserer vielen hochqualifizierten Spezialistinnen und Spezialisten im Kommandobereich nachhaltig!

Wenn es uns gelingt, diese Leistung auch in der Zukunft mit noch stärkeren Partnern an unserer Seite fortzuführen, wird es uns auch gelingen, dass „eine IT-System der Bundeswehr" nachhaltig und erfolgreich zu implementieren und damit unserem Motto im KdoITBw auch weiterhin gerecht zu werden:

Unser.Auftrag.Verbindet.

wt

Generalmajor Dr. Michael Färber *ist der Kommandeur des Kommandos Informationstechnik der Bundeswehr.*

Das Kommando Strategische Aufklärung hat seinen Sitz in Gelsdorf bei Bonn. (Foto: Bundeswehr / KdoStratAufkl)

Generalmajor Axel Binder

Aufklärung im Cyber- und Informationsraum

Die Leistungen des Militärischen Nachrichtenwesens sind ein substanzieller Beitrag zur Bewältigung aller, auch asymmetrischer und hybrider Bedrohungslagen. Es gilt, militärische Lageentwicklungen in festgelegten Interessenräumen zu beobachten und mit einem fundierten Lagebild und abgeleiteten Empfehlungen Entscheidungen vorzubereiten. Hier ist das Kommando Strategische Aufklärung der bewährte zentrale Dienstleister der Bundeswehr, der sein Portfolio mit neuen Fähigkeiten und Strukturen weiter ausbaut.

Lagefeststellung im Wandel der sicherheitspolitischen Rahmenbedingungen

Bereits nach den ersten Signalen zu Beginn dieser Dekade, aber spätestens nach den Ereignissen in der Ukraine und der Annexion der Krim begannen die NATO-Bündnisnationen über erforderliche Fähigkeiten nachzudenken, um der Befürchtung von militärischen Auseinandersetzungen im neu entfachten Ost-West-Konflikt zu begegnen. Ein Fokus sicherheitspolitischer Vorsorge wurde deshalb zusätzlich zum internationalen Krisenmanagement auf die Befähigung zur Verteidigung der territorialen Integrität des eigenen und des Bündnisgebietes gelenkt. In der Konsequenz verstärkte die NATO unter anderem ihre dauerhafte Präsenz in den osteuropäischen Mitgliedsstaaten. Das Weißbuch zur Sicherheitspolitik von 2016 bringt zudem die Absicht zum Ausdruck, einen aktiven Beitrag zur internationalen Sicherheitsvorsorge und Konfliktverhütung zu leisten. Die Befähigung zur umfassenden Krisenfrüherkennung ist für beide gleichrangigen Aufgaben eine entscheidende Voraussetzung. Das Kommando Strategische Aufklärung gehört zum CIR und trägt mit seiner spezifischen Expertise streitkräftegemeinsam dazu bei, weltweit militärische Krisen zu erkennen und deren Entwicklung zu beschreiben. Die verlässliche, schnelle und kontinuierliche Versorgung mit aktuellen und zuverlässigen Informationen als grundlegender Beitrag zur Vorbereitung von Entscheidungen wird, in Anbetracht der veränderten sicherheitspolitischen Ausgangslage, zur bestimmenden Ausgangsgröße für eine nationale Krisenreaktion – auch im Rahmen der kollektiven Sicherheit von NATO und EU.

Es muss also künftig darum gehen, auf der Grundlage einer stets abrufbaren nationalen Beurteilung der militärischen Lageentwicklung „Rot“ – mithin potenzieller militärischer Opponenten – einen nachvollziehbaren und belastbaren Beitrag für den militärischen Ratschlag des Generalinspekteurs der Bundeswehr bei krisenhaften Entwicklungen liefern zu können. Das Militärische Nachrichtenwesen (MilNW) sammelt dazu in jeglicher Form relevante Informationen, zu Land, zu See, in der Luft und im Weltraum sowie im Cyber- und Informationsraum. Das Kommando Strategische Aufklärung verantwortet diesen streitkräftegemeinsamen Prozess im Auftrag des Inspekteurs CIR und entsprechend der strategischen Vorgaben des Bundesministeriums der Verteidigung.

Das militärische Nachrichtenwesen insgesamt sieht sich dabei dem Erfordernis gegenüber, die auf Stabilisierungseinsätze optimierten Strukturen auf die Landes- und Bündnisverteidigung auszurichten. Allen Szenarien muss es dabei gerecht werden.

Insbesondere mit den rasanten Entwicklungen in der Dimension Cyber- und Informationsraum sieht sich das MilNW konfrontiert. Die Digitalisierung der Fernmelde- und Telekommunikationstechnik bestimmt die Dynamik. Noch nie waren die Möglichkeiten zur (auch weltweiten) Kommunikation so schnell und einfach wie heute. Das Internet und die zunehmende Vernetzung von Individuen, Organisationen, Staaten und Dingen machen vieles im täglichen Leben einfacher. Anderes wird aber

auch schwerer, beispielsweise den Wahrheitsgehalt von ad-hoc und in nahezu Echtzeit verbreiteten Informationen festzustellen. Gleichzeitig sind Staat, Gesellschaft und Wirtschaft von verlässlichen IT- und Telekommunikationssystemen abhängig und damit verwundbar geworden. Dies trifft natürlich auch auf die Streitkräfte zu. Die Bedrohungen aus dem Cyber- und Informationsraum, der neben der bisher gewohnten räumlichen Einteilung der Dimensionen nach Land, Luft, See und Weltraum eine neue, im ersten Moment nicht sicht- oder greifbare, gleichwohl aber „übergreifende“ Dimension darstellt, gefährden unsere Sicherheit und erfordern eine Anpassung der Gefahrenabwehr – gesamtstaatlich, aber insbesondere auch im Hinblick auf die Aktions- und Reaktionsfähigkeit der Streitkräfte im Rahmen ihres verfassungsmäßigen Auftrags. Mit der Aufstellung des Organisationsbereichs Cyber- und Informationsraum im Jahre 2017 ist hierzu ein entscheidender, in die Zukunft gerichteter Schritt zur Begegnung der vielfältigen Herausforderungen in dieser Dimension getan. Das Kommando Strategische Aufklärung ist eine wichtige Säule im Kampf gegen diese neuen Bedrohungen. Mit seinen Möglichkeiten zur weltweiten und weitreichenden Aufklärung verfügt es im kompletten CIR-Spektrum über moderne und zukunftsweisende militärische Fähigkeiten, die in unseren Streitkräften einzigartig sind. Die Verbände und Dienststellen sind deutschlandweit stationiert und spiegeln die Komplexität und Vielschichtigkeit der Aufgaben wider.

Das Kommando Strategische Aufklärung

Das Kommando Strategische Aufklärung ist zu einem Synonym für die erfolgreiche streitkräftegemeinsame Zusammenführung von Wissen und Kompetenz geworden. In der Aufgabenwahrnehmung für die gesamten Streitkräfte stellt es allen militärischen Bedarfsträgern unter anderem tagesaktuell zusammengeführte Informationen und Nachrichten bereit, die maßgeblich zur Entscheidungsfindung auf allen Ebenen der Bundeswehr beitragen. Der Kernauftrag des Kommandos bleibt dabei, die ständige Unterstützung der Streitkräfte in den Einsätzen sicherzustellen und maßgeblich zu ihrem Schutz beizutragen. Das Kommando entsendet aber auch eigene hochspezialisierte Kräfte direkt in die jeweiligen Einsatzgebiete. Gleichzeitig leistet es mit den fast 5.000 zivilen und militärischen Angehörigen einen maßgeblichen Beitrag aus Deutschland heraus. Täglich unterstützen über 1.700 Angehörige des Kommandobereichs die Einsatzkontingente der Bundeswehr direkt aus Standorten in Deutschland im Rahmen von Daueraufgaben zur Einsatzunterstützung.

Das Kommando Strategische Aufklärung ist die zentrale Dienststelle des Militärischen Nachrichtenwesens innerhalb der Bundeswehr. Es bündelt eine Vielzahl von eigenen Sensoren und koordiniert die Aufklärungsfähigkeiten von Heer, Luftwaffe, Marine und CIR. Nach der Umgliederung im Zuge der Neuausrichtung der Bundeswehr wurden 2013 im Kommando Strategische Aufklärung die Prozesse Nachrichtenmanagement und Aufklärung auf Streitkräfteebene zusammengeführt. Damit wurden auch Schnittstellen zu anderen Ressorts, zu Bündnispartnern, zur NATO und zur EU verringert und optimiert. Im System des Militärischen Nachrichtenwesens hat das Kommando Strategische Aufklärung die koordinierende Rolle übernommen. Das zentrale Element hierfür ist die Gruppe J2 Informationsbedarfs- und Aufklärungsmanagement (englisch kurz IRMCM). Sie ist die zentrale Drehscheibe für das Militärische Nachrichtenwesen in der Bundeswehr. Sie steuert den Einsatz der Aufklärung und der Zusammenführung die Ergebnisse der Sensoren. Dabei kann sie auf die Sensorik und die jeweiligen Aufklärungsmittel der Teilstreitkräfte Heer, Luftwaffe und Marine sowie aller anderen militärischen Organisationsbereiche zurückgreifen.

CIR und Marine überwachen gemeinsam mit den Flottendienstbooten das elektromagnetische Spektrum von See. (Foto: Bundeswehr / PIZ Marine)

80 Prozent der Antworten auf die Fragen militärischer Führer finden sich im Internet, in Bibliotheken, in Fernsehen und Radio. (Grafik: Bundeswehr / KdoCIR)

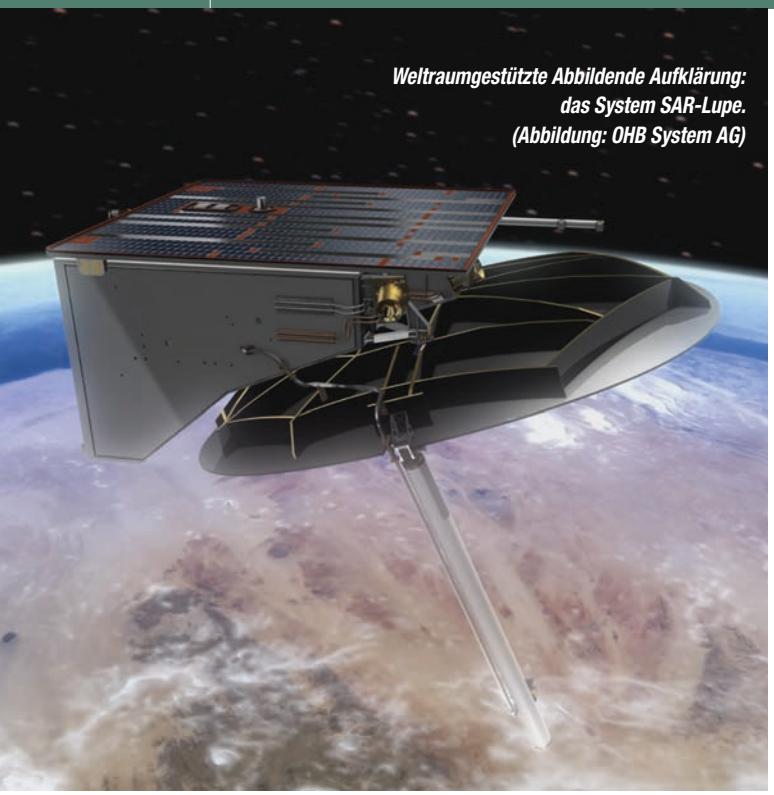
Das Kommando Strategische Aufklärung übernimmt als „Single Point of Contact“ das Nachrichtenmanagement für das System Militärisches Nachrichtwesen. Es erstellt eine fusionierte militärische Nachrichtenlage für alle Einsatzgebiete, Krisengebiete und für Länder im besonderen Interesse, und stellt diese für alle Bedarfsträger, vom Bundesministerium der Verteidigung bis zum taktischen militärischen Führer im Einsatzgebiet zur Verfügung. Es sorgt dafür, dass aktuelle Informationen zeitgerecht genau dorthin gelangen, wo sie gebraucht werden. Dabei koordiniert es den Informations- und Aufklärungsbedarf der Bundeswehr.

Ab Frühjahr 2020 wird im Auftrag des Generalinspekteurs der Bundeswehr im Kommando Strategische Aufklärung ein Joint Intelligence Centre aufgebaut, welches über noch weitergehende Steuerungskompetenzen verfügen wird.

OSINT - Aufklärung in offenen Quellen

Die Aufklärung in öffentlich und offen zugänglichen Quellen (Open Source Intelligence) ist die jüngste Aufklärungsdisziplin der Bundeswehr. OSINT ist die Antwort auf die ständig zunehmende Fülle an Daten und Informationen in und aus offenen und öffentlich zugänglichen Quellen. Über 5 Milliarden Internetnutzer tragen jede Sekunde mit etwa 24.000 GB zum digitalen Datenbestand des Web 4.0 bei. (Quelle: Kepios Pte. Ltd. (“Kepios”), We Are Social Ltd. (“We Are Social”) and Hootsuite Inc.(Hrsgb.): DIGITAL 2019 - Essential insights into how people around the world use the internet, mobile devices, social media, and e-commerce (abgerufen am 05.02.2020). https://wearesocial.com/global-digital-report-2019)

Somit sorgen etwa fünfzig Prozent der gesamten Weltbevölkerung dafür, dass in den kommenden Jahren aus 33 Milliarden TB (2018) über 175 Milliarden TB (2025) Daten werden. Diese sehr abstrakten Zahlen haben ganz konkrete Auswirkungen für die Bundeswehr: Denn der Zuwachs findet auch in geografischen Räumen statt, die für die Bundeswehr von Interesse sind. Neben Informationen zu diesen Räumen sind es aber auch die Metadaten, die Informationen über die digitale Sphäre selbst, die vor dem Hintergrund von Digitalisierung und Cyber-Operationen an Bedeutung gewinnen. Bisher wurden alle diese Daten trotz ihrer Relevanz nur vereinzelt und unsystematisch berücksichtigt. Achtzig Prozent der Antworten auf die Fragen militärischer Führer finden sich im Internet, in Bibliotheken, in Fernsehen und Radio. Dies gilt nicht nur für die Gewinnung von Grundlagendaten, sondern insbesondere auch für die Krisen- und Einsatzgebiete im Fokus des Militärischen Nachrichtenwesens. Nur ein koordiniertes und systematisches Vorgehen führt im Umgang mit dieser Datenflut zum Ziel. Die OSINT-Landschaft ist vielfältig und herausfordernd. Schnelligkeit und Sicherheit im Handeln erfordern Expertise in vielen verschiedenen Teilbereichen. Hinter OSINT verbirgt sich deutlich mehr als eine Abfrage in Internet-Suchmaschinen oder unstrukturiertem Auswerten von anderen offen zugänglichen Quellen. Das zielgerichtet hierzu ausgebildete militärische und zivile Personal arbeitet im Team zusammen. Mit der Etablierung dieser Fähigkeit als militärische Aufklärungsdisziplin, die konsequent über alle Planungskategorien hinweg aufgebaut wird, ist ein qualitativer Entwicklungssprung zu erwarten. Eine Qualitäts- und Leistungssteigerung, die darauf abzielt, dem rapiden Wandel der Informations- und Kommunikationstechnik Rechnung zu tragen. So leistet OSINT einen wertvollen Beitrag im komplementären Ansatz der Aufklärungsdisziplinen des Militärischen Nachrichtenwesens. Im OrgBer CIR wird erstmals in den Streitkräften eine zentrale Verantwortlichkeit für diese jüngste Aufklärungsdisziplin verankert. Die operative Anfangsbefähigung zur Bereitstellung von Aufklärungsergebnissen OSINT wird bis 2024 erreicht werden.



Weltraumgestützte Abbildende Aufklärung: das System SAR-Lupe. (Abbildung: OHB System AG)

Auswertezentrale Elektronische Kampfführung

Als einer der eigenen Träger der Aufklärung ist die Auswertezentrale Elektronische Kampfführung dem Kommando Strategische Aufklärung unmittelbar nachgeordnet. Die militärischen und zivilen Expertinnen und Experten der Auswertezentrale analysieren Inhalte der signalerfassenden Kommunikationsaufklärung und der elektronischen Aufklärung. Sie steuern die Erfassung durch die vier Bataillone für die Elektronische Kampfführung (EloKa), fassen die Sensorergebnisse zusammen, korrelieren sie und stellen die daraus gewonnenen Informationen dem Militärischen Nachrichtenwesen zur Verfügung. Mit den ortsfesten Anlagen und mobilen Komponenten der Bataillone sowie in Zusammenarbeit mit Heer, Luftwaffe und Marine steht der Auswertezentrale ein breites Spektrum der signalerfassenden Aufklärung zur Verfügung. Das ermöglicht ihr eine Aufklärung weltweit, weiträumig und bis hin zur Begleitung der Truppe im Einsatz. Zusätzlich kann sie sich auf die wissenschaftliche Analyse der Zentralen Untersuchungsstelle der Bundeswehr für Technische Aufklärung als dem Bindeglied zwischen technisch-wissenschaftlicher Arbeit und praktischer Umsetzung durch die EloKa-Bataillone abstützen.

Zentrale Abbildende Aufklärung

Seit 2008 steht dem Kommando das Satelliten-System SAR-Lupe (Synthetic Aperture Radar) mit fünf Satelliten zur Verfügung. Damit besitzt die Bundeswehr einen satellitengestützten Sensor auf der Basis moderner Radartechnik, der ohne geographische und hoheitsrechtliche Beschränkungen, allwetterfähig und tageszeitunabhängig Bildmaterial aus Regionen von Interesse liefern kann. Die Zentrale Abbildende Aufklärung, die direkt dem Kommando Strategische Aufklärung unterstellt ist, ist das Auge im All. Sie steuert den Einsatz der Aufklärungssatelliten der Bundeswehr und wertet die gewonnenen Satellitenbilder aus. Hier bearbeiten militärische und zivile Expertinnen und Experten Satellitenbilder für militärische Aufklärungszwecke. Neben dem eigenen SAR-Lupe-System kann die Bundeswehr in Kooperation mit Frankreich das Aufklärungssystem HELIOS II mitnutzen. Außerdem wertet die Zentrale Abbildende Aufklärung Satellitenbilder von kommerziellen Systemen oder Material anderer Quellen, wie zum Beispiel dem Satellitenzentrum der Europäischen Union in Torrejón de Ardoz (Spanien) aus.

Zentrum Cyber-Operationen

Durch die rasante Entwicklung der Telekommunikations- und Informationstechnik verbessern sich nicht nur die eigenen Kommunikationstechniken, sondern es bieten sich auch neue Möglichkeiten für die Aufklärung. Bereits seit 2007 befasst sich das Kommando Strategische Aufklärung mit den Aspekten von Cyberoperationen, vormals Computer-Netzwerkoperationen (CNO) genannt. Die vormalige Gruppe CNO wurde mit Aufstellung des neuen Organisationsbereiches Cyber- und Informationsraum in das Zentrum Cyber-Operationen überführt und mit erweiterten Fähigkeiten ausgestattet. Gleichzeitig wuchs die Personalstärke auf, was sich in den nächsten Jahren fortsetzen wird. 2018 wurde das Zentrum aus dem Kommandostab des Kommandos Strategische Aufklärung herausgelöst und als eigenständige Dienststelle unterstellt. Ziel der Aufstellung und des Aufwuchses ist die signifikante Stärkung der Fähigkeit Cyberoperationen, um zum einen im Bereich der Aufklärung erweiterte Beiträge zu einem gemeinsamen Lagebild im Cyber- und Informationsraum und somit zur Warn- und Schutzfunktion des Militärischen Nachrichtenwesens leisten zu können. Das Zentrum baut ein Cyberoperationen-Lagebild auf, auf dessen Basis unter anderem Handlungsoptionen für das Wirken durch Cyberoperationen entwickelt werden. Die Aufklärung durch Cyberoperationen muss dabei mit den anderen Sensoren, insbesondere der Operativen Kommunikation und des Elektronischen Kampfes, koordiniert werden.

Zum anderen werden die Fähigkeiten zum Planen, Vorbereiten, Führen und Durchführen von militärischen Computernetzwerkoperationen aus ortsfesten Einrichtungen und mit mobilen Systemen ausgebaut. Die Cyberoperations-Kräfte können sowohl bei der Landes- und Bündnisverteidigung als auch in mandatierten Einsätzen eingesetzt werden.

Mobile Kräfte des Elektronischen Kampfes: Funk- und Fernmeldeaufklärung im Einsatzgebiet. (Foto: Bundeswehr / KdoStratAufkl)

Zentrum Operative Kommunikation der Bundeswehr

Mit dem Zentrum Operative Kommunikation der Bundeswehr (ZOpKomBw) erschließt sich dem Militärischen Nachrichtenwesen das Informationsumfeld nicht mehr nur zur Informationsgewinnung, sondern auch als Handlungs- und Wirkungsraum. Das Informationsumfeld bildet zusammen mit dem Elektromagnetischen Umfeld und dem Cyber-Raum die Dimension Cyber- und Informationsraum. Basierend auf einer bereits seit Aufstellung des Kommandos Strategische Aufklärung bestehenden engen Zusammenarbeit unterstützen die Soldaten und zivilen Mitarbeiter des Zentrums in Mayen mit Expertise und Kräften auch das Militärische Nachrichtenwesen bei der Deckung des Informationsbedarfs der Streitkräfte. Im Rahmen der nationalen Krisen- und Risikovorsorge wird die „Lage im Informationsumfeld“ erarbeitet und täglich die Meinungs- und Wahrnehmungslage von Menschen in Krisen- und Konfliktregionen erfasst, analysiert und bewertet. Damit leistet das Zentrum Operative Kommunikation einen Beitrag zum Gesamtlagebild der Bundeswehr. Darüber hinaus unterstützt das Zentrum auch die Operationsführung eigener sowie multinationaler Streitkräfte in den Einsatzgebieten der Bundeswehr durch Expertise im Planungsprozess und in der Durchführung. In den Einsätzen ermöglichen die Angehörigen des Zentrums eine situationsangepasste und die jeweiligen kulturellen Gegebenheiten berücksichtigende Information und Kommunikation mit eigenen Kräften, Mitteln und Methoden Im Rahmen einer Wirkungskontrolle werden die entsprechenden Ergebnisse gemessen und wissenschaftlich ausgewertet.

Entwicklung zum Aufklärungs- und Wirkungskommando und zu einem streitkräftegemeinsamen Nachrichtenzentrum

Mit Blick auf die neue Struktur hat sich das Kommando Strategische Aufklärung von einem Fähigkeitskommando zu einem Aufklärungs- und Wirkungskommando weiterentwickelt. Dieser Schritt ist die Antwort auf neue Risiken und Gefahren für die Sicherheit unseres Landes und eine wesentliche Voraussetzung für den Erfolg von Missionen und Einsätzen der Bundeswehr, die sich aus der zunehmenden Bedeutung des Cyber- und

Das Personal des Zentrums Cyber-Operationen wächst weiter auf. (Foto: Bundeswehr)

Informationsraumes sowie den hierein wirkenden hybriden und asymmetrischen Bedrohungslagen ergeben. Für militärisches Entscheiden und Handeln in hybriden Bedrohungslagen bis hin zu unmittelbaren militärischen Handlungen ist es unerlässlich, Aufklärung und Wirkung im Cyber- und Informationsraum ebenengerecht in den Planungs- und Entscheidungsprozess einzubeziehen. Dazu leistet das Kommando Strategische Aufklärung als Aufklärungs- und Wirkungskommando seinen entscheidenden Beitrag nicht mehr „nur“ im Bereich der Nachrichtenlage, sondern zunehmend mit neuen Wirkfähigkeiten im Verbund aus Cyberoperationen, Operativer Kommunikation und Elektronischem Kampf auch im operationellen Bereich.

In der Domäne Aufklärung wurde unter einem „J2“ unter anderem die Fähigkeit Nachrichtenmanagement und damit auch die Aufklärungssteuerung gestärkt. Damit konsolidiert das Kommando Strategische Aufklärung die bewährte zentrale Funktion im System Militärisches Nachrichtenwesen und passt die inhaltliche Tiefe und Breite der militärischen Nachrichtenlage den sicherheitspolitischen Herausforderungen an. Ziel ist es, den Informationsbedarf der Bedarfsträger noch effektiver zu decken und die verfügbare Sensorik dafür effizient einzusetzen.

Darüber hinaus gilt es, den Ausbau der Kooperationen zu NATO, EU und bilateralen Partnern zu gestalten und bedarfsgerecht zu intensivieren. Das Aufgabenspektrum erstreckt sich dabei von der Krisenfrüherkennung im Rahmen einer Warn-, Schutz- und Informationsfunktion für die Streitkräfte bis hin zu konkreter Zielaufklärung im Einsatz. Als wesentliche Neuerung wird sich das Kommando mit der Aufstellung eines Joint Intelligence Centre darauf vorbereiten, eine zentrale Aufgabe für die Bundeswehr zu übernehmen. Entscheidend für den aufgezeigten weiteren Weg zum Aufklärungs- und Wirkungskommando im Organisationsbereich CIR und die streitkräftegemeinsame Funktion als Joint Intelligence Centre sind das Gewinnen von geeignetem Personal, der Einsatz Künstlicher Intelligenz zur Analyse von „Big Data“, die Anpassung der Ausbildung, das Sicherstellen des Zulaufs der bereits projektierten Sensorik und Einsatzmittel sowie eine fortlaufende Anpassung der eigenen Fähigkeiten an die Herausforderungen, denen es mit der zunehmenden Digitalisierung auch militärisch zu begegnen gilt.

wt

***Generalmajor Axel Binder** ist der Kommandeur des Kommandos Strategische Aufklärung.*

Der Störpanzer HUMMEL leistet mit elektronischen Gegenmaßnahmen einen wichtigen Beitrag zum Schutz der Truppe im Einsatz. (Foto: Bundeswehr / Lars Koch)

Kapitän zur See
Ronald Hoffmann

Das Kommando Strategische Aufklärung wirkt!

Das Kommando Strategische Aufklärung wandelt sich grundlegend. Zum ersten Mal sind im Kommando die Fähigkeiten zur Aufklärung und Wirkung im Cyber- und Informationsraum in einer Hand zusammengefasst. Dies war vor dem Hintergrund der rasanten Veränderungen auf dem Gefechtsfeld dringend notwendig. Als Aufklärungs- und Wirkkommando eröffnen sich damit ganz andere und zum Teil neue Handlungsoptionen für die Planung und Führung von militärischen Operationen.

Aufklärung und Wirkung aus einer Hand

Die aktuellen Krisen und Konfliktherde der Welt belegen, dass der Cyber- und Informationsraum bereits heute ein entscheidender Operationsraum ist. Dies wird auch künftig so sein.

Es handelt sich um eine Entwicklung von gleicher umwälzender Tragweite wie die Motorisierung der Landstreitkräfte, die Etablierung der Luftkriegsführung, der U-Boote, der Panzerwaffe sowie der Atombombe. Die strukturell fehlende Fähigkeit der Bundeswehr im Cyber- und Informationsraum zu operieren, war in der Vergangenheit eine große Fähigkeitslücke. Die Aufstellung des militärischen Organisationsbereichs Cyber- und Informationsraum (CIR) und die damit verbundenen Erteilung eines neuen Auftrages an das Kommando Strategische Aufklärung (KdoStratAufkl) stellt gemäß Weisung des Bundesministeriums der Verteidigung (BMVg) den wesentlichen Beitrag zur Schließung dieser Fähigkeitslücke dar.

Das Kommando Strategische Aufklärung wurde somit vom Fähigkeitskommando für das Militärische Nachrichtenwesen zu einem operationellen Kommando für Aufklärung und Wirkung. Unter dem Dach des Kommandos Cyber- und Informationsraum betreibt es Aufklärung in allen Dimensionen. Es ist zudem befähigt, in der Dimension Cyber- und Informationsraum selbstständig oder unterstützend bei anderen Operationen zu wirken.

Das KdoStratAufkl ist damit zukünftig das Manöverelement im Schwerpunkt im Cyber- und Informationsraum. Deshalb ist seit April 2018 die ehemalige Abteilung „Einsatz“ in die Joint-Bereiche J2 “Militärisches Nachrichtenwesen“ und J3 “Ausbildung, Übung, Planung und Führung“ aufgegliedert worden, um Aufklärung und Wirkung auch operationell sicherzustellen.

Militärische Nachrichtenlagen für alle Dimensionen

Der J2-Bereich KdoStratAufkl kann auf eine lange Erfahrung in der Erstellung der militärischen Nachrichtenlage zurückgreifen. Dabei wurden und werden die militärischen Lagen aus allen Dimensionen zu einem einheitlichen militärischen Lagebild fusioniert. Für die Landes- und Bündnisverteidigung ist hierbei zunehmend wichtig geworden, ressortübergreifend und international zu kooperieren. Zudem ist auch dem Bereich der offenen Informationsgewinnung mehr Gewicht beizumessen als bislang. Diese Herausforderungen wurden entsprechend in der neuen Struktur berücksichtigt. Gleichzeitig musste während des Umbaus auch die kontinuierliche Informationsversorgung der Bundeswehr durch den Bereich J2 auf allen Ebenen und in allen Dimensionen, besonders jedoch in der Unterstützung der Soldatinnen und Soldaten in den Einsätzen der Bundeswehr sichergestellt werden.

Erst eine fusionierte militärische Nachrichtenlage ermöglicht die Planung von selbstständigen oder unterstützenden Wirkungsoperationen im Cyber- und Informationsraum. Damit ist die einheitliche militärische Nachrichtenlage die Voraussetzung für einen souveränen Beitrag der Bundesrepublik Deutschland zur Landes- und Bündnisverteidigung, zu internationalem Krisenmanagement und zur nationalen Krisenvorsorge.

Wirkung im Cyber- und Informationsraum

Wirkung wird im militärischen Sinne oftmals noch ausschließlich mit dem letalen Einsatz eines Wirkmittels verbunden, wie zum Beispiel der Artillerieeinsatz durch eine Panzerhaubitze oder der Abwurf einer Bombe durch einen Kampfjet. Die Domäne Wirkung verfügt aber auch über einen nicht-letalen Aspekt. Dieser nicht-letale Beitrag wird durch die alten und zum Teil neu unterstellten Fähigkeiten des Kommandos Strategische Aufklärung geleistet. Hier liegt nun exemplarisch auch das Besondere an der Befähigung des Kommandos Strategische Aufklärung zum Aufklärungs- und Wirkkommando: Zum ersten Mal in der Geschichte der Bundeswehr sind die Möglichkeiten des Wirkens im Elektromagnetischen Spektrum, im Informationsumfeld und im Cyber-Raum unter einem Dach vereinigt. Damit wird besonders dem geänderten Schutzbedürfnis der Bundesrepublik Deutschland im Cyber- und Informationsraum Rechnung getragen.

Mit der Unterstellung des Zentrums Operative Kommunikation der Bundeswehr (ZOpKomBw) und dem Aufbau des Zentrums Cyber-Operationen (ZCO) hat sich das (Wirkungs-)Portfolio des Kommandos Strategische Aufklärung wesentlich, zu der bereits vorhandenen Fähigkeit elektronischer Kampf (EloKa), erweitert. Die verschiedenen Manöverelemente der Wirkung des KdoStratAufkl erzielen ihren Mehrwert jedoch nur, wenn sie im Verbund eingesetzt werden. Zu den Wirkfähigkeiten im Einzelnen:

Wirken im Informationsumfeld

Die Kommunikationsprofis des Zentrums Operative Kommunikation der Bundeswehr unterstützen die Operationsführung eigener und multinationaler Streitkräfte in den verschiedenen Einsatzgebieten der Bundeswehr. Ähnlich einer zivilen Medienanstalt analysieren sie die Situation der Bevölkerung in den Einsatzgebieten und wirken unter anderem mit Print-, Audio-, Video- und weiteren Medienprodukten zum Beispiel über das Internet auf freigegebene Zielgruppen ein. Im Rahmen der Direktkommunikation werden geplant und zielgerichtet Gespräche mit der Bevölkerung vor Ort genutzt, um beabsichtigte Wirkungen durch Informationsaktivitäten zu erzielen. Dazu verfügen diese Kräfte über ein weitreichendes Verständnis der Kommunikationsziele und sind mit den kulturellen Gegebenheiten vor Ort sowie den spezifischen Kommunikationsgewohnheiten der Zielgruppe vertraut. Im Rahmen einer Wirkungskontrolle werden die Ergebnisse gemessen und wissenschaftlich ausgewertet.

So verfügt das Kommando Strategische Aufklärung über die Fähigkeit, das Informationsumfeld als militärischen Handlungsraum zu erschließen. Zu den zugeordneten Unterstützungsaufgaben des ZOpKomBw gehören die Truppeninformation mit Hörfunk (Radio Andernach), die Truppenbetreuung mit TV-Produkten (BwTV) und die Einsatzdokumentation in Film und Bild. Diese wird abgebildet durch die Soldatinnen und Soldaten der Einsatzkameratrupps (EKT), welche Lageinformationen für die politische und militärische Führung liefern.

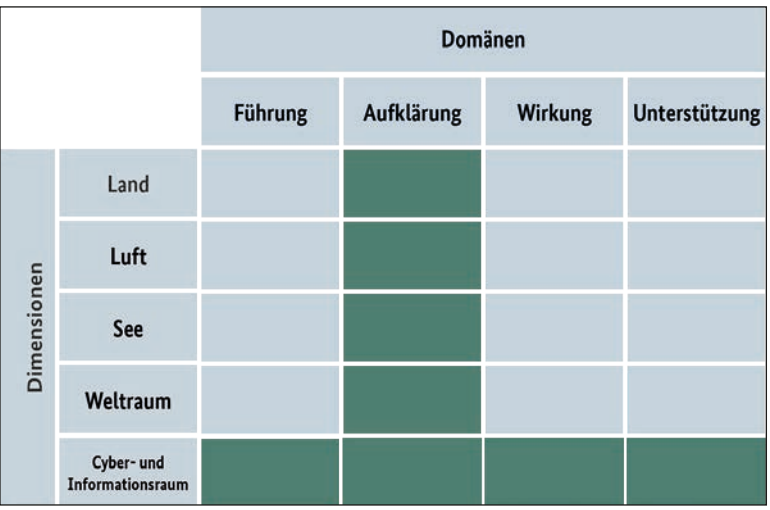
Die Kräfte der Operativen Kommunikation wirken im Einsatz zum Beispiel mit Video-Produkten auf freigegebene Zielgruppen, etwa die lokale Bevölkerung. (Foto: Bundeswehr / ZOpKomBw)

Wirken im elektromagnetischen Umfeld

Integraler Bestandteil jeder Operationsführung ist die Nutzung des elektromagnetischen Spektrums als hauptsächlichem Übertragungsweg im Cyber- und Informationsraum. Aus der Erfassung und Auswertung von Ausstrahlungen im Elektromagnetischen Spektrum resultieren Handlungsoptionen zum Einsatz von Kräften und Mitteln des elektronischen Kampfes: sowohl zum Schutz eigener Kräfte (Informationsüberlegenheit und Force Protection) als auch um Wirkung in den Systemen des Gegners zu erzielen. Die Truppe für den Elektronischen Kampf (EloKa-Truppe) besitzt Fahrzeuge und anderes Material, mit dem sie elektromagnetische Strahlung, beispielsweise Funk- oder Radarstrahlen, stören kann. So gelingt es ihr, Wirkung im Cyber- und Informationsraum zu erzielen.

Wirken im Cyber-Raum

Im Zentrum Cyber-Operationen werden die heute erforderlichen, spezifischen Fähigkeiten zur Vorbereitung und Durchführung von militärischen Operationen zur Aufklärung und Wirkung im Cyber-Raum in einer Dienststelle gebündelt. Kernauftrag des ZCO ist das Planen, Vorbereiten, Führen und Durchführen von Operationen zur Aufklärung und Wirkung sowohl im Rahmen der Landes- und Bündnisverteidigung als auch in mandatierten Einsätzen der Bundeswehr. Die Spezialisten aus Rheinbach können so – nach strengen rechtlichen Richtlinien – auch in fremden IT-Netzen wirken. Neben der Verantwortung für offensive und defensive Cyber-Operationen können Kräfte des ZCO im Rahmen einer IT-Krise die IT-Sicherheitskräfte des Kommandobereichs CIR unterstützen. Darüber hinaus werden regelmäßig Beiträge zum Schutz der eigenen IT-Systeme in neuer Qualität geliefert: Beim Red-Teaming testen die Cyber-Operateure Systeme der Bundeswehr mit der Brille des Angreifers, um die Informationssicherheit auf höchstem Niveau aufrechtzuerhalten.



◁ *Das KdoStratAufkl betreibt Aufklärung in allen Dimensionen und wirkt in der Dimension Cyber- und Informationsraum. (Grafik: Bundeswehr / KdoStratAufkl)*

Der Auftrag des KdoStratAufkl wurde um das Wirken im Cyber- und Informationsraum erweitert.
(Grafik: Bundeswehr / KdoStratAufkl)

Operationsplanung im Cyber- und Informationsraum

Seit dem 1. April 2019 verfügt das Kommando Strategische Aufklärung zudem über eine Anfangsbefähigung zum Planen und Führen von Operationen in allen drei Wirkbereichen, einzeln und zusammen, national wie international, in Unterstützung anderer Operationen oder als selbstständige Operation.

Dafür ist die J3-Abteilung des Kommandos Strategische Aufklärung um die Gruppe „Führung und Planung“ erweitert worden. Im Fokus der Planungen und Operationen steht hierbei immer zuvorderst der Schutz der Truppe in den Einsatzgebieten. Gleichzeitig beteiligt sich die Gruppe an der Entwicklung neuer Fähigkeiten im Rahmen der nationalen und internationalen Planung und Führung, insbesondere in der NATO. Im Bereich des Cyber-Raumes und des Informationsumfeldes sind dabei die Herausforderungen besonders komplex und entwickeln sich ständig weiter. Im Gegensatz zu den Dimensionen Land, Luft, Weltraum und See lässt sich hier oft nicht eindeutig klären, aus welcher Richtung eine mögliche Bedrohung kommt. Der aufzuklärende Raum ist virtuell, menschengemacht und ohne geografische Eingrenzung. Der Faktor Zeit kann im Zweifelsfalle von Monaten auf Millisekunden, den berühmten „Maus-Klick“, zusammenschrumpfen. Gerade deswegen ist eine frühzeitige und gezielte Aufklärung notwendig und wird von den anderen Aufklärungsdisziplinen des Hauses tatkräftig unterstützt, um ebenengerechte militärische Handlungs- und Wirkungsoptionen zu entwickeln und umzusetzen.

Die Planung von Operationen muss dabei so erfolgen, dass sie sich jederzeit in eine Operationsplanung der NATO oder EU im Rahmen der Landes- und Bündnisverteidigung einfügen kann. Daher erfolgt sie zwingend auf der Basis gültiger NATO-Dokumente. Hierbei sind strenge rechtliche und politische Vorgaben, national wie international, einzuhalten.

Operationsführung im Cyber- und Informationsraum

Zur Führung von Operationen bedarf es einer kontinuierlichen Lageführung, einer Operationszentrale (OPZ). Diese wächst im Bereich J3 des Kommandos Strategische Aufklärung auf. Sowohl der J2- als auch der J3-Bereich greifen dazu auch auf das erfahrene Personal im unterstellten Bereich des Kommandos Strategische Aufklärung zurück.

Das Kommando Strategische Aufklärung ist zudem bereits jetzt in der Lage, für zeitlich und regional begrenzte Operationen eine OPZ einzurichten. Sie wird dabei durch Spezialistinnen und Spezialisten aus dem unterstellten Bereich und den anderen Dimensionen Land, Luft, See und Weltraum ergänzt.

Die Bereiche J1 Personal, J4 Material und Logistik und insbesondere J6 IT-Services des Stabes Kommandos Strategische Aufklärung unterstützen diesen Auf- und Umbau zum Aufklärungs- und Wirkkommando nach Kräften.

Die einzelnen Fähigkeiten zur Aufklärung und Wirkung des Kommandos Strategische Aufklärung sind im elektromagnetischen Spektrum, dem Informationsumfeld sowie dem Cyber-Raum zu planen, zu koordinieren und vor allem zu synchronisieren. Die ersten Erfahrungen auf dem Gebiet sind richtungsweisend.

Fazit

Zusammengefasst hat das Kommando Strategische Aufklärung seine Fähigkeiten nicht nur „im laufenden Gefecht“ ausgebaut, sondern hat sich inzwischen auch als Aufklärungs- und Wirkkommando etabliert. Es ist damit befähigt, seine Verantwortung als Aufklärungs- und Wirkkommando im Cyber- und Informationsraum, aber auch in allen anderen Dimensionen, wahrzunehmen. Durch das Zusammenführen der Wirkfähigkeiten des Organisationsbereichs CIR können Handlungsoptionen für eine schlagkräftige, nicht-kinetische Wirkung entwickelt werden. Diese Rolle stetig auszubauen und weiterzuentwickeln muss der zukünftige Schwerpunkt des Kommandos sein, um den hybriden Bedrohungen der Zukunft weiter entschlossen entgegentreten zu können.

wt

Kapitän zur See Ronald Hoffmann *leitet die Abteilung J3 im Kommando Strategische Aufklärung.*

Das Cockpit des A400M ist ausgestattet mit digitalem Kartenmaterial. (Foto: Bundeswehr / Simon Otte)

Autorenteam Zentrum für Geoinformationswesen der Bundeswehr

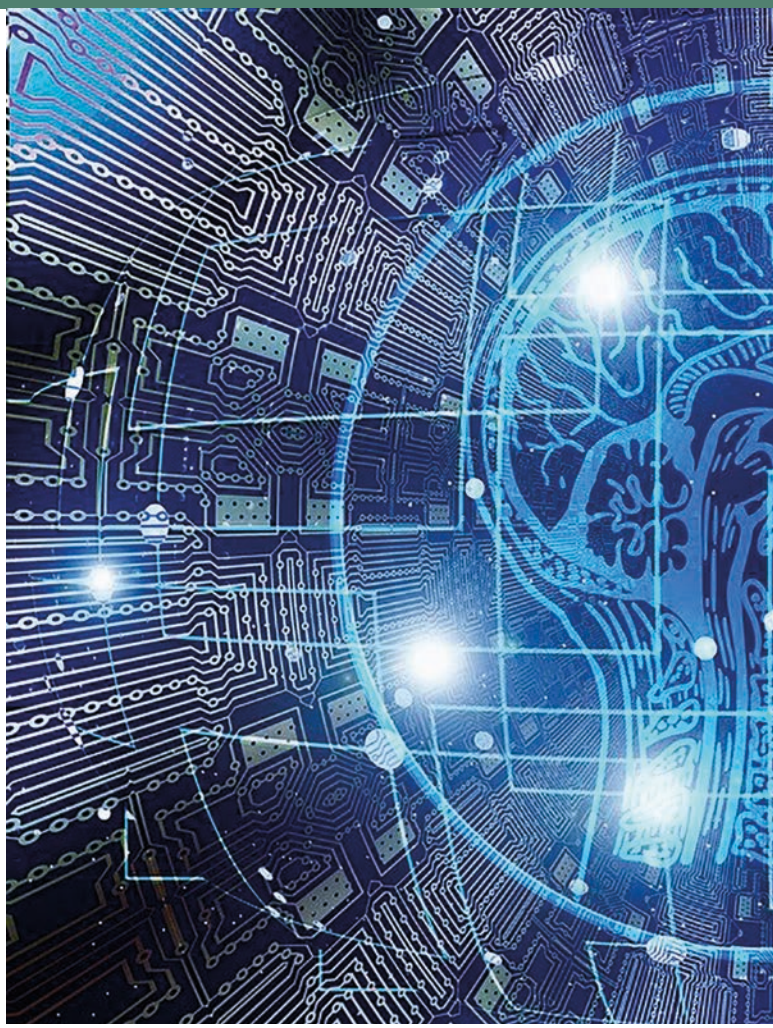
Geoinformationen für die Bundeswehr

Digitalisierung ist der Megatrend unserer Zeit, und längst leben wir in einer digitalisierten Welt. Aber weder ist es einfach, den Begriff im Hinblick auf seine Bedeutung präzise einzugrenzen, noch ist der damit verbundene Prozess endgültig abgeschlossen. Das Phänomen Digitalisierung durchdringt jedoch nahezu alle Lebensbereiche und gesellschaftlichen Sektoren. Insofern ist es nicht verwunderlich, dass auch die Digitalisierung der Geoinformationsversorgung ein Thema für die Bundeswehr ist. Vor diesem Hintergrund erörtert der Beitrag in der Einführung zunächst den Terminus „Digitalisierung". Es werden insbesondere solche Aspekte adressiert, welche für die Bereitstellung von Geoinformationen für die Bundeswehr relevant sind. Im Hauptteil des Artikels wird die Digitalisierung der Geoinformationsversorgung detaillierter vorgestellt. Es werden die bisher erreichten Erfolge und etablierte Services präsentiert, und schließlich wird sowohl auf die derzeitigen Aktivitäten als auch auf die Ziele für die Zukunft eingegangen.

Einführung

Der Begriff Digitalisierung ist omnipräsent. Mit diesem Ausdruck wird im Allgemeinen der „digitale Wandel" beschrieben, das heißt der Übergang von analogen hin zu digitalen Technologien. Eingesetzt hat der Prozess der Digitalisierung etwa mit Beginn der 1990er Jahre. Seitdem vollzieht sich eine rasante Entwicklung, die längst noch nicht abgeschlossen ist. Des Weiteren ist Digitalisierung ein Phänomen, welches viele beziehungsweise nahezu alle Lebensbereiche und Sektoren durchdringt. Sie hat bereits jetzt zu derart markanten Veränderungen geführt, dass oftmals sogar von einer „digitalen Revolution" gesprochen wird. Beispielsweise hat sich in den vergangenen Jahren durch E-Mails, WhatsApp, Facebook und so weiter die (private) Kommunikation grundlegend verändert. Der Einkauf von Waren über das Internet ist mittlerweile üblich, die Anzahl der Kunden, die diesen Service nutzen, wächst zunehmend. Des Weiteren sind heute für viele Unternehmen, Organisationen und Behörden Homepages und virtuelle Auftritte unverzichtbare Standards im täglichen Geschäftsbetrieb. Diese kleine Auswahl von digitalen Erscheinungen ist im Alltag zweifelsohne evident, aber nun dringen weitere innovative Technologien vor, wie zum Beispiel die Künstliche Intelligenz und die Robotik.

Grundsätzlich bietet die Digitalisierung auf der einen Seite ein enormes Potenzial, auf der anderen Seite ist der digitale Wandel mit ernsthaften Risiken behaftet. Hinsichtlich des letztgenannten Punktes ist die Cyber-Sicherheit gerade im Hinblick auf die wachsende Nutzung von internetbasierten Diensten sowie in Bezug auf die zunehmende Vernetzung von



Mensch und Maschine von großer Bedeutung. Es ist sogar treffender, zu sagen, dass die Cyber-Sicherheit – vor allem für Organisationen mit Sicherheitsaufgaben wie die Bundeswehr – eine notwendige Bedingung für das Arbeiten mit digitalen Services und Daten ist. Betrachtet man demgegenüber die Möglichkeiten der Digitalisierung, stellt man fest, dass die (digitalen) Daten der eigentliche Rohstoff für die Wertschöpfung sind. Aktuell zählt es zu den wirklich großen Herausforderungen, die permanent wachsenden Datenmengen effizient einzusetzen. Das Stichwort lautet Big Data. Ein anderer Aspekt ist der Datenaustausch. So erfordern sowohl der Datenverkehr als auch die Verkopplung von Technologien verbindliche Standards und Normen für die Schnittstellen, denn nur auf diese Weise kann Interoperabilität gewährleistet werden. Schließlich sei das Aufkommen der Cloud-Dienste genannt. Das sind IT-Infrastrukturen, die über das Internet verfügbar gemacht werden und zum Beispiel Speicherplatz, Rechnerleistung oder spezifische Anwendungen beziehungsweise Dienstleistungen bereitstellen.

Die Bundeswehr setzt sich ebenfalls intensiv und aktiv mit dem Thema Digitalisierung auseinander, denn die Digitalisierung ist ein maßgeblicher Faktor in Bezug auf die Informations-, Führungs- und Wirkungsüberlegenheit. Aus diesen Aktivitäten ist zum Beispiel die „Umsetzungsstrategie Digitale Bundeswehr“ hervorgegangen, welche im Juni 2019 vom Bundesministerium der Verteidigung (BMVg) erlassen wurde. Des Weiteren wurde in diesem Zuge ein Digitalrat im BMVg etabliert, um die digitale Transformation der Bundeswehr gezielt zu steuern und zu gestalten. Der Organisationsbereich Cyber- und Informationsraum versteht sich als der Treiber der Digitalisierung der Bundeswehr. Hier werden die Voraussetzungen für eine erfolgreiche Digitalisierung der Bundeswehr geschaffen.

Die Versorgung der Bundeswehr mit standardisierten Geo-Daten und -Produkten ist ein Teil der GeoInfo-Unterstützung und wird grundsätzlich durch das Zentrum für Geoinformationswesen der Bundeswehr (ZGeoBw) geleistet.

Digitale Geoinformationsversorgung

Der Terminus Geoinformation ist sehr weit gefasst und beschreibt allgemein Daten, die an eine Position (Koordinaten) gebunden sind. Anders formuliert sind Geoinformationen einfach solche Daten, die einen Raumbezug haben, das heißt ortsabhängig sind. Im Ressort des BMVg ist das ZGeoBw zuständig für die Erfassung beziehungsweise

Die Apps im GIS-Portal reichen von Viewern topographischer Karten bis hin zur Darstellung von Schutzgebietsinformationen. (Grafik: Bundeswehr / KdoCIR)

◁ ***Künstliche Intelligenz kann auch im Geoinformationswesen helfen, große Datenmengen auszuwerten. (Grafik: Pixabay)***

für die Genese von notwendigen Geoinformationen sowie für die Bereitstellung derselben. Zum Beispiel werden die Bedarfsträger in der Bundeswehr neben den bekannten weltweiten Informationen auf thematischen und topographischen Karten mit Informationen zum terrestrischen Wetter, zum Vogelschlag, zu GPS oder zum Weltraumwetter versorgt. Diese Auflistung ist keineswegs vollständig. Im ZGeoBw leisten 18 geowissenschaftliche Disziplinen jeweils ihren Beitrag, um den vielfältigen Organisationsbereichen der Bundeswehr die zur Planung und Durchführung ihrer Aufgaben erforderlichen Daten, Services und Produkte zur Verfügung zu stellen.

Zum Archetypus digitaler Technologien zählen die Informationssysteme (IS) beziehungsweise die Geoinformationssysteme (GIS). Bereits in den 1980er Jahren wurde kommerzielle GIS-Software entwickelt. Ein IS und ein GIS unterscheiden sich dahingehend, dass das Erste maßgeblich Sachdaten und das Zweite Sachdaten mit Raumbezug enthält. Die wesentlichen Funktionen eines GIS sind das Vorhalten und Verwalten von Daten sowie die Analyse und die Visualisierung dieser Daten. Prominente Beispiele für IS beziehungsweise GIS – und vielen Nutzern in der Bundeswehr bekannt – sind zum einen das Harmonisierte Führungsinformationssystem (HaFIS), welches aus den separaten Führungsinformationssystemen Streitkräfte, Luftwaffe und Militärisches Nachrichtenwesen hervorgegangen ist und als eine essentielle Komponente die Bereitstellung von Geoinformationen vorsieht.

Das System „Infanterist der Zukunft (IdZ)“ steht in der Bundeswehr querschnittlich allen infanteristisch agierenden Kräften zur Verfügung. Das Modul „Command, Control, Computers, Communication and Information (C4I)“ des IdZ bindet die Soldatinnen und Soldaten grundsätzlich an

Das Archivsystem des ZGeoBw hat eine Speicherkapazität von 5 PB (Petabyte). (Fotos: Bundeswehr / Martina Pump)

die vernetzte Operationsführung an. Die für die Zukunft geplanten Ausbaustufen des IdZ optimieren und erweitern diese Funktionalität der vernetzten Operationsführung.

Zum anderen kennen viele Bundeswehrangehörige das GIS-Portal (https://gisportal.geoinfo.svc/portal) des ZGeoBw, wo Nutzer die verschiedensten (thematischen) Karten abrufen und hilfreiche Anwendungen (Apps) starten können.

Um bedarfsgerecht Geoinformationen zusammenzustellen, können der Anwender und die Anwenderin selbst Basiskarten mit ausgewählten Inhalten kombinieren und auf diese Weise maßgeschneiderte Produkte erstellen. Ist der Nutzer zusätzlich mit den Rechten eines Publishers ausgestattet, so besteht die Möglichkeit – innerhalb gewisser Grenzen – mit Hilfe des Web-App-Builders individuelle Web-Anwendungen zu erzeugen.

Die Bundeswehr – insgesamt gesehen – verfügt so schon lange über ein bewährtes leistungsfähiges digitales System zur Geoinformationsversorgung. Dennoch ist die Digitalisierung der Geoinformationsversorgung noch nicht abgeschlossen. Denn dieser dynamische Prozess bringt hochfrequent neue Herausforderungen mit sich und veranlasst immer wieder zu neuen Zielsetzungen. So ist die Digitalisierung der Geoinformationsversorgung zum Beispiel auch im Kontext von Künstlicher Intelligenz zu diskutieren.

Wie oben ausgeführt sind die elementaren Aufgaben eines GIS das Halten und Administrieren von Daten sowie die Analyse und Präsentation dieser Daten. Möglicherweise – und mittlerweile wird dieser Sachverhalt in der öffentlichen Diskussion ernsthaft erörtert – kann die Implementierung der Künstlichen Intelligenz ein GIS um die Funktionalität „Entscheidung vorbereiten“ oder sogar „Entscheidung treffen“ erweitern. Im Rahmen der militärischen Führung sind Entscheidungen oftmals in sehr zeitkritischen Situationen zu fällen. Das Lagebild ist dabei äußerst komplex. Das heißt, der militärische Führer muss eine extrem große Menge an Daten und Informationen berücksichtigen. Die Künstliche Intelligenz kann durchaus ein nützliches Instrument sein, um diese Datenflut – man spricht von Big Data – zu kontrollieren und sie zuverlässig sowie systematisch auszuwerten (Stichwort: Echtzeitdatenanalyse). Ein anderes Moment, das im Diskurs oftmals untergeht, aber unbedingt Relevanz hat, ist das Schaffen einer entsprechenden Infrastruktur.

Das heißt, der Transfer von großen Datenvolumen erfordert zum Beispiel Breitband-Netze, die hohe Geschwindigkeiten erlauben. Die Datenübertragung muss schnell sein und Ziel ist die „Echtzeit-Datenübertragung“. Zusätzlich sind beispielsweise eine gute Netzüberdeckung, ausreichende Datenspeicher, intelligente Verfahren der Datensicherung, eine Systemunterstützung (Support), die rund um die Uhr verfügbar ist, bedeutsam. Zudem ist es wichtig, den Online-Anteil von Diensten und Produkten weiter zu steigern. Zusätzlich ist die Vernetzung von Komponenten, zum Beispiel die Kopplung von Sensoren mit GIS-Plattformen sowie die Kopplung von GIS-Plattformen mit (mobilen) Endgeräten voranzutreiben.

Folglich können die Digitalisierung im Allgemeinen und die Digitalisierung der Geoinformationsunterstützung der Bundeswehr im Besonderen keine ausschließlich nationalen Themen sein. Vielmehr muss der Austausch von Daten und Informationen zwischen der Bundeswehr und ihren Partnern sichergestellt sein. Multinationale Programme, wie das Multinational Geospatial Co-Production Program zur gemeinsamen Herstellung von Vektordaten (das sind Daten mit geometrischen Informationen für die Produktion von topographischen Karten) hoher Auflösung bezogen auf die Maßstabsbereiche 1:50.000 beziehungsweise 1:100.000 laufen bereits erfolgreich. Die Vektordaten werden nach einer gemeinsamen Spezifikation und vorgeschriebener gegenseitiger Qualitätssicherung und -kontrolle produziert und in eine internationale Datenbank, das International Geospatial Warehouse, eingestellt.

Das ZGeoBw und die National Geospatial-Intelligence Agency der Vereinigten Staaten von Amerika haben gemeinsam das TanDEM-X High Resolution Elevation Data Exchange (TREx) Programm initiiert, um durch eine Verteilung der Lasten die Kosten sowie den Aufwand zur Nutzbarmachung des globalen, homogenen Digitalen Höhenmodells zu minimieren. Viele weitere Nationen sind inzwischen am TREx-Programm beteiligt.

Zusammenfassung

Digitalisierung ist und bleibt ein Schwerpunktthema für die Bundeswehr und damit auch für die Geoinformationsversorgung der Bundeswehr. Das ZGeoBw ist in dieser Hinsicht prinzipiell gut aufgestellt. Allerdings ist es eine Daueraufgabe, dem schnellen Innovationstempo dieses Prozesses stets in adäquater Weise zu begegnen. Denn es gilt, weder den Entwicklungen hinterherzulaufen noch gar „abgehängt“ zu werden. Sowohl die Abteilung Cyber- und Informationstechnik im BMVg als auch der militärische Organisationsbereich Cyber- und Informationsraum verfolgen mit Nachdruck die ganzheitlich gestaltete Digitalisierung der Bundeswehr. In diesem Kontext ist ebenfalls die Digitalisierung der Geoinformationsversorgung eingebettet. Die Bundeswehr im Allgemeinen als auch die Geoinformationsversorgung der Bundeswehr im Besonderen sehen sich in den kommenden Jahren vor beachtlichen Aufgaben. Um diese erfolgreich meistern zu können, müssen frühzeitig Maßnahmen eingeleitet und zeitgerecht umgesetzt werden. Das ZGeoBw sieht sich grundsätzlich gut vorbereitet und in der Lage, die notwendigen Maßnahmen zu ergreifen, welche die Bundeswehr zu einer (vollständig) digitalisierten Geoinformationsversorgung befähigen.

wt

◁ ***Touchscreens mit GIS-Funktionalität werden unter anderem bei der Einweisung in das Gelände eingesetzt. (Foto: Bundeswehr / Martina Pump)***

IT-Fachkräfte sind auch in der Bundeswehr stark gefragt. (Foto: Bundeswehr / Martina Pump)

Oberstleutnant i.G. Dennis Pohl und Oberstleutnant i.G. Alexander Strelau

Fachkarriere, Zulagen, fachliches Recruiting: Die Bundeswehr geht neue Wege im „Wettbewerb um die besten Köpfe“

Behörden, Organisationen und die Wirtschaft suchen gleichermaßen nach Cyber/IT-Fachkräften. Hat die Bundeswehr im „Wettbewerb um die besten Köpfe“ überhaupt eine Chance? Die erste Reaktion ist im Allgemeinen ein Kopfschütteln. Zu verlockend erscheinen die Angebote aus der Wirtschaft. Staatliche Stellen können da in der Regel nicht mithalten. Das Kommando Cyber- und Informationsraum (CIR) hat ein Bündel an Maßnahmen geschnürt, um dieser Herausforderung zu begegnen.

Neue Herausforderungen für die Bundeswehr

„Fachkräftemangel“ ist in aller Munde. Der Bereich Cyber/IT scheint hiervon besonders betroffen zu sein – besteht er doch zu einem wesentlichen Teil aus eben solchen Experten und Spezialisten, die den Weg im Zeitalter der Digitalisierung bahnen sollen. So verwundert es nicht, dass die Hochwertressource IT-Fachkraft in Unternehmen wie Verwaltungen gleichermaßen stark nachgefragt ist.

Auch für die Bundeswehr stellt die digitale Transformation einen wesentlichen Erfolgsfaktor dar. In einer globalisierten Welt ist die sichere und freie Nutzung des Cyber- und Informationsraums elementare Voraussetzung staatlichen und privaten Handelns. Staat, Gesellschaft und Wirtschaft sind eng in diesem Raum, aber eben auch mit diesem Raum verknüpft. Den Chancen aus der Nutzung stehen immanente Risiken gegenüber. Bedrohungen im Cyber- und Informationsraum – von technischen Manipulationen bis Desinformation – sind nahezu allgegenwärtig. Im Weißbuch zur Sicherheitspolitik werden die Auswirkungen von Cyberangriffen auf Staat, Wirtschaft und Zivilleben daher als besonders eklatant bewertet. Folgerichtig ist in allen Bereichen, öffentlichen wie privatwirtschaftlichen, die Nachfrage nach qualifiziertem Personal für die Umsetzung der Digitalisierung aber auch für die Gewährleistung der erforderlichen Cyber-Sicherheit sprunghaft angestiegen. In der Folge ist die Lücke zwischen Angebot und Nachfrage für IT-Experten im Laufe von nur vier Jahren auf fast 60.000 Fachkräfte gestiegen und hat sich damit verdreifacht. Für die Bundeswehr, und damit vorrangig den Organisationsbereich Cyber- und Informationsraum, als gesamtstaatlich Verantwortlicher für die Cyberverteidigung, stellt dies eine besondere Herausforderung dar.

Bestimmendes Merkmal von Entwicklungen im Cyber- und Informationsraum sind disruptive Innovationszyklen, infolge derer die Innovationen von heute schon morgen wieder veraltet sind. Der Prozess der Digitalisierung kann so nie abgeschlossen werden: Die Akteure müssen beständig am Puls der Zeit bleiben. Übertragen auf die Cyber-Sicherheit bedeutet dies, dass die heute noch wirksamen Maßnahmen bereits morgen keinen Schutz mehr bieten können oder sogar als Schwachstelle ein Einfallstor für Angriffe auf die IT-Infrastruktur darstellen. In diesem Kontext kommt der Auswahl von Cyber/IT-Fachpersonal für die Bundeswehr herausragende Bedeutung zu: IT-Experten müssen nicht nur hochqualifiziert sein, sondern ihr Wissen und ihre Fähigkeiten stets topaktuell halten. Im Ringen um diese Fachkräfte werden den

Der klassische Offizier ist Führer, Ausbilder und Erzieher. Im Cyber/IT-Dienst steht dagegen die Fachlichkeit im Mittelpunkt. (Foto: Bundeswehr / Dana Kazda)

staatlichen Institutionen mit ihren starren Regeln und Rahmenvorgaben per se Wettbewerbsnachteile zugeschrieben. Wie soll eine vermeintlich unflexible und behäbig agierende Verwaltungsorganisation mit den modernen und auf das Individuum zugeschnittenen Angeboten der Wirtschaft konkurrieren? Dabei werden häufig auch die deutlich höheren monetären Anreize, welche Wirtschaftsunternehmen zahlen können, ins Feld geführt. Entsprechend der Nachfrage haben sich auch die Gehälter entwickelt. So stieg das Bruttogehalt eines Datenanalysten mit langjähriger Berufserfahrung („Senior") innerhalb von drei Jahren von 63.000 Euro auf 82.197 Euro und damit um mehr als 30 Prozent an. Im Ergebnis, so scheint es, haben staatliche Stellen kaum eine realistische Chance, wettbewerbsfähig zu sein.

Vor dem Hintergrund dieses Vergleichs mit der Wirtschaft wurde im Kommando CIR frühzeitig begonnen zu untersuchen, wie diesem Dilemma begegnet werden kann. In einem umfassenden Ansatz wurden drei Grundlinien der Untersuchung herausgearbeitet und in Fragestellungen formuliert:

1. Wie können die bestehenden „Karrieremöglichkeiten" im Cyber/IT-Dienst angepasst werden, um attraktiver zu werden?
2. Wie können die bestehenden Verfahren der Personalgewinnung für den Bereich Cyber/IT-Dienst unterstützt werden?
3. Wie kann das in der Bundeswehr vorhandene Potenzial noch besser ausgeschöpft werden?

Neue Karrierepfade

Von Offizieren wird erwartet, dass sie in dynamischen Situationen, mit begrenzten Informationen und unter hohem Zeitdruck Entscheidungen treffen und diese mit den ihnen zur Verfügung stehenden personellen wie materiellen Ressourcen zielgerichtet umsetzen. Offiziere führen „von vorne". Sie teilen Härten und Entbehrungen mit den ihnen anvertrauten Soldatinnen und Soldaten. Es verwundert nicht, wenn unter diesen Rahmenbedingungen ein besonderes Augenmerk auf die physische und psychische Belastbarkeit gelegt wird. Dieses Verständnis dominiert traditionell das Bild des Offiziers: Offizier in den Streitkräften ist ein Führungsberuf und folgt einer Führungskarriere. Offiziere werden in relativ kurzen Zeitabständen versetzt und regelmäßig mit neuen Aufgaben betraut. Bewusst werden sie unter Umständen sogar mit ihnen völlig neuen Aufgaben, für die sie bisweilen im Vorfeld nicht umfassend qualifiziert wurden, konfrontiert. Dadurch wird das Verständnis des Offiziers als „Generalist", der in der Lage ist, sich eigenständig in eine neue Materie einzuarbeiten, weiter geprägt. Mit einem so gestalteten Verwendungsaufbau wird dem Einzelnen die Möglichkeit eröffnet, seinen eigenen Erfahrungsschatz zu erweitern und Kompetenzen aufzubauen, um im Ergebnis Führungsaufgaben auf verschiedenen Führungsebenen mit weitreichender und umfassender Verantwortung wahrnehmen zu können.

Auch im Cyber/IT-Dienst werden militärische Führer benötigt. Zwar müssen alle Offiziere des Cyber/IT-Dienstes gleichsam fachlichen Ansprüchen genügen, um die technisch geprägten Aufgaben umfassend wahrnehmen zu können, im Mittelpunkt steht jedoch unverändert die Forderung nach hoher Führungskompetenz. Hiernach wird das Führungspersonal des Cyber/IT-Dienstes ausgewählt, geprägt und gefördert. Mit der Hervorhebung der Bedeutung der Cyber-Verteidigung in einer volatilen Umgebung und den sich hieraus ergebenden Anforderungen an das Personal rückt jedoch schnell die Frage in den Vordergrund: Ist das „klassische" Bild des Offiziers als militärischer Führer auf IT-Experten anwendbar? Es muss kritisch hinterfragt werden, ob die Fokussierung auf das militärische Führen und das hiermit verknüpfte Bild des Typus eines Offiziers der Attraktivität des Cyber/IT-Dienstes nicht abträglich ist.

Tatsächlich gelten für das Personal in der Cyber-Verteidigung andere Rahmenbedingungen zum Auf- und Ausbau seiner Kompetenzen als für den „klassischen" Offizier. Fachkräfte entwickeln ihre Cyber/IT-Fähigkeiten durch die tägliche aufgabenbezogene Beschäftigung mit der Materie weiter. Ein beständiger Wechsel zwischen Aufgaben, gegebenenfalls sogar fachfremden, wäre demgegenüber weder sachgerecht noch förderlich. So kann es sich die Bundeswehr schlichtweg nicht mehr leisten, mühsam geworbene Fachkräfte in kosten- und zeitintensiven Lehrgängen auszubilden und diese dann fachfremd einzusetzen.

Es muss auch berücksichtigt werden, dass diese Fachkräfte häufig keine an Führungsaufgaben orientierte Karriere anstreben: Sie wollen oft ausschließlich in ihrer Fachlichkeit arbeiten. Aus Sicht des Kommando CIR muss die für die große Mehrzahl der Offiziere unverändert gültige Ausrichtung auf militärische Führung nicht per se auch den IT-Expertinnen und Experten „übergestülpt" werden. Vielmehr muss die Bundeswehr diesen Fachleuten einen eigenen Karrierepfad, als Alternative zu einer Führungskarriere anbieten, um als Bundeswehr auch für die Fachkräfte attraktiv zu sein.

Das Kommando CIR nutzte daher eine Initiative des Bundesministeriums der Verteidigung zur Etablierung verschiedener Karrieremodelle, um eine Cyber/IT-Fachkarriere für die Offiziere des Truppendienstes auszuplanen. Offiziere, die in einer Fachkarriere tätig sind, arbeiten von Beginn an ausschließlich in der Fachlichkeit. Anstatt der in der Führungskarriere erforderlichen regelmäßigen Versetzungen wird auf lange Verwendungsdauer in einer Aufgabe gesetzt: Dem Expertiseaufbau

Der Cyber/IT-Dienst

Die neue Fachkarriere für Offiziere des Truppendienstes

- Attraktive Alternative zur klassischen Führungskarriere
- Lange Verwendungsdauer in der Fachaufgabe
- Rein fachliche Leitungsaufgaben
- Ausschließlich fachlicher Aufstieg bis B03 (Dienstgrad Oberst) möglich
- Finanzielle Zulageoptionen

Im Februar 2020 wurde die neue Fachkarriere etabliert. (Grafik: Bundeswehr / KdoCIR)

Experten aus der Truppe spielen bei der Rekrutierung von IT-Fachpersonal eine wichtige Rolle. (Foto: Bundeswehr / Martina Pump)

wird somit deutlich höheres Gewicht beigemessen als einem allgemeinen Kompetenzerwerb. Für diesen alternativen Karrierepfad können Personen für den Dienst in der Bundeswehr gewonnen werden, die sich nicht primär für Führungsaufgaben interessieren – oder eignen. Um Fachkräfte langfristig an die Bundeswehr zu binden, wird die Möglichkeit eines fachlich geprägten Karriereaufstiegs, bis in die Dotierungsebene B3 nach Bundesbesoldungsgesetz ermöglicht. Die mit zunehmender Dotierungsebene zwangsläufig einhergehenden Führungsaufgaben begrenzen sich auf die fachliche Leitungsfunktion. Experten leiten Experten.

Damit ergänzen sich Führungs- und Fachkarriere: Während die Offiziere der Fachkarriere die Erfüllung der Fachaufgabe verantworten, stellen die in der Führungskarriere tätigen Offiziere die Einbettung der Fachaufgabe in die Operationsführung der Streitkräfte sicher.

Neue Testverfahren

Die Einführung einer Fachkarriere im Cyber/IT-Dienst ist die Konsequenz aus der Analyse von Chancen und Risiken, welche der Cyber- und Informationsraum darstellt. Es wurde festgestellt, dass die bisherige Systematik der reinen Fokussierung auf eine Führungskarriere nicht mehr geeignet war, Fachpersonal für die Cyberverteidigung anzusprechen und gezielt einzusetzen. Eine Fachkarriere nutzt jedoch nichts, wenn keine Fachkräfte gewonnen werden. Es musste daher ergänzend der Personalgewinnungsprozess untersucht werden. Handlungsleitend war die Frage: Wie kann gewährleistet werden, dass künftige IT-Experten zwischen all den Bewerberinnen und Bewerber für den Dienst in der Bundeswehr frühzeitig identifiziert werden? Um nicht eindimensional auf Neubewerbungen zu fokussieren, wurde auch die Potentialausschöpfung des „Bestandspersonals“ der Bundeswehr untersucht. Dabei wurde geprüft, ob es ein Verfahren gibt, welches qualifizierte Cyber/IT-Fachkräfte identifiziert, die bereits in der Bundeswehr Dienst leisten, aber gar nicht als solche eingesetzt werden.

Das Recruiting der Bundeswehr setzt für die Personalgewinnung heute auf einen Mix aus verschiedenen Diagnoseverfahren. Dadurch wird eine Vielzahl an Bewerberinnen und Bewerbern in Assessmentverfahren auf ihre Eignung für eine der militärischen Laufbahnen geprüft und im optimalen Fall in die Bundeswehr eingestellt. Diese Verfahren sind etabliert und führen potentiellen Nachwuchs in großer Zahl in den Bewerbungsprozess. Die Quantität und die Eignung für eine Laufbahn sind aber nur eine Seite der Medaille. Die andere Seite ist die Frage nach den vorhandenen Qualitäten der Bewerberinnen und Bewerber – in spezifischen fachlichen Aspekten. Die Recruiter der Bundeswehr sind für die Gesamtorganisation Bundeswehr und damit für die vielfältigen Aufgaben der Bundeswehr zuständig. Sie stellen von Soldaten für die Kampftruppe über Versorgungsoffiziere bis hin zu Technikerinnen Personal für die unterschiedlichsten Aufgaben der Bundeswehr ein. Sie sind Profis für Recruiting und Personalmanagement. Wer aber bewertet die fachliche Eignung einer Bewerberin oder eines Bewerbers für eine spezifische Aufgabe, zumal in einem ausschließlich fachlich geprägten und hochspezialisierten Bereich?

Blick in die Wirtschaft

In dieser Frage gab ein Blick über den sprichwörtlichen Tellerrand den entscheidenden Hinweis. In der heutigen Arbeitsmarktlage müssen Arbeitgeber in der Wirtschaft umdenken: Nicht die Fachkräfte bewerben sich bei den Unternehmen, sondern andersherum. Potentielle Mitarbeiterinnen und Mitarbeiter entscheiden sich für ein Engagement in einem Unternehmen, wenn sie vom „Gesamtpaket“ des Angebots überzeugt sind. Das Gehalt ist dabei nur ein Faktor unter mehreren. Ein gesamtstaatliches Alleinstellungsmerkmal erfährt vermehrt in der Cyber/IT-Community Beachtung: In keiner anderen Organisation dürfen Fachkräfte offensive Cyberoperationen durchführen. Ein Pfund, mit dem der Organisationsbereich CIR wuchern kann. Förderungsmöglichkeiten, Reputation und Innovationskraft kommen ebenfalls gestiegene Bedeutung zu. Der Fachkräftemangel in Verbindung mit der hohen Spezialisierung im IT-Bereich hat dazu geführt, dass in den Wirtschaftsunternehmen die bis dahin ausschließlich in den Personalabteilungen verortete Rekrutierung nun als Gemeinschaftsaufgabe von Personalabteilung und fachlich Verantwortlichen begriffen wird. Ergänzend kommt hinzu, dass interessierte Bewerberinnen und Bewerber das Bedürfnis haben, sich bereits im Bewerbungsprozess inhaltlich über ihren zukünftigen Arbeitgeber detailliert zu informieren. Diese Informationen können aber nur authentisch durch die jeweilige Fachexpertise transportiert werden. Erst durch die Bündelung der Expertise aus Personal- und Fachabteilung kann es gelingen, geeignete Fachkräfte zu identifizieren, anzusprechen und einzustellen. Experten werben Experten.

Konsequenterweise muss die Frage der fachlichen Eignung von Bewerberinnen und Bewerbern für den Bereich Cyber/IT-Dienst im Organisationsbereich CIR verortet sein. Dies gilt auch für die Frage, wie mit bundeswehreigenem fachlich qualifiziertem Personal umgegangen werden soll. In der Forderung „Die richtige Cyber/IT-Fachkraft, zur richtigen Zeit am richtigen Platz im Cyber/IT-Dienst“ muss der Organisationsbereich CIR mehr in die Pflicht genommen und mit seinem fachlichen Votum berücksichtigt werden. Die Fachlichkeit muss der Taktgeber sein.

Diese Ableitungen mündeten in dem Entschluss des Inspekteurs Cyber- und Informationsraum, ein Cyber/IT Evaluation Center (CITEC) zu schaffen. Das CITEC soll den Rekrutierungsprozess unterstützen, indem aus fachlicher Sicht eine Bewertung zur Eignung für den Cyber/IT-Dienst ausgesprochen werden kann. In bis zu drei aufeinander aufbauenden Testlevels soll die fachliche Eignung für den Cyber/IT-Dienst überprüft werden:

- IT-Testlevel 1 (ITT 1): Dieser Level soll ortsunabhängig durchgeführt werden können. Der internetbasierte Test richtet sich an Neubewerber für den Dienst in der Bundeswehr und wird Multiple Choice Fragen umfassen. Wer diesen Test erfolgreich absolviert, wird zum nächsten Testlevel eingeladen. Allen anderen werden die Möglichkeiten für eine andere Karriere in der Bundeswehr aufgezeigt werden.
- IT-Testlevel 2 (ITT 2): Das Herzstück des CITEC. Dieses Testlevel müssen alle Interessierten für den Cyber/IT-Dienst durchlaufen, unabhängig ob Neubewerber oder bereits vollumfänglich ausgebildeter Offizier. In verschiedenen Modulen müssen die Kandidatinnen und Kandidaten ihr Können in der gesamten Bandbreite des Cyber/IT-Dienstes unter Beweis stellen. Das Ergebnis ist kein schlichtes „geeignet“ oder „nicht geeignet“. Vielmehr werden konkrete Empfehlungen zu möglichen

Vertiefungen im Cyber/IT-Dienst ausgesprochen. Mehr noch kann der Test Aussagen treffen, in welchen Bereichen Ausbildungsbedarf besteht, um eine bessere Empfehlung zu bekommen.

- IT-Testlevel 3 (ITT 3): Die Einladung zum ITT 3 erhalten diejenigen Kandidatinnen und Kandidaten, die sich aufgrund ihrer fachlichen Leistungen in den beiden vorangegangenen Testlevels möglicherweise für die Fachkarriere empfehlen können.

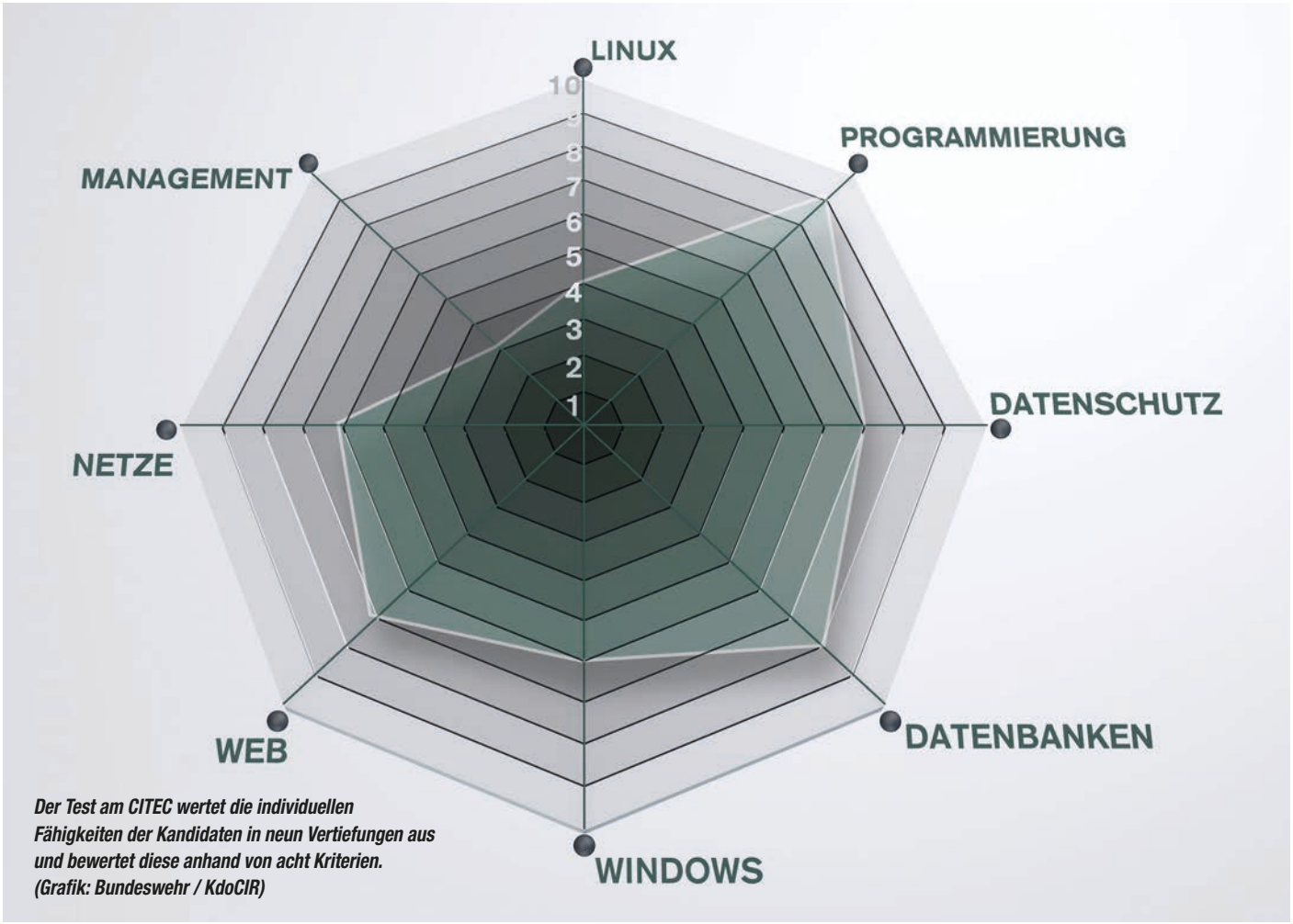
Leitungsentscheidung: beschleunigte Umsetzung

Das zunächst am „Reißbrett“ ausgeplante CITEC musste schneller als erwartet seine Feuerprobe bestehen. Nachdem die Idee im Juni 2019 der Leitung des Bundesministeriums der Verteidigung vorgestellt worden war, wurde angewiesen, das CITEC beschleunigt umzusetzen und noch in 2019 mit den Testungen zu beginnen. Hierzu wurde ad hoc ein Testentwicklungsteam zusammengezogen, welches alle Bereiche des Cyber/IT-Dienstes abdeckte. Auftrag dieses Teams war es, in vier Monaten das erste Testmodul zu entwickeln. Dieses Modul besteht aus einem Multiple-Choice-Test, der Fragen aus allen Disziplinen des Cyber/IT-Dienstes enthält. Der erste Testdurchgang erfolgte im November 2019 an der IT-Schule der Bundeswehr in Feldafing am Starnberger See (zur IT-Schule siehe auch den Beitrag auf Seite 53). Insgesamt 19 Offiziere, die außerhalb des Cyber/IT-Dienstes verwendet wurden, ein MINT-Studium absolviert hatten und kurz vor Ende ihrer Verpflichtungsdauer als Zeitsoldaten standen, stellten sich dem Modul A des ITT 2. Das Testentwicklungsteam wartete gespannt auf die Ergebnisse: War das Verfahren geeignet, um tatsächlich valide Aussagen zur fachlichen Eignung zu treffen? Für die Kandidatinnen und Kandidaten ging es um ungleich mehr: Das Bundesamt für das Personalmanagement der Bundeswehr hatte eigens erfahrene Personalführer entsandt. Diese unterbreiteten, bei fachlicher Empfehlung, konkrete Angebote für eine Dienstzeitverlängerung und einen Wechsel in den Cyber/IT-Dienst. Im Ergebnis wurde die Übernahme von 18 Kandidatinnen und Kandidaten aus fachlicher Sicht empfohlen. CITEC hat einen ersten Achtungserfolg erzielt: Für den Cyber/IT-Dienst qualifizierten Offizieren, die ansonsten die Bundeswehr verlassen hätten, konnten konkrete Angebote zum Verbleib in der Bundeswehr unterbreitet werden. 13 von ihnen haben das Angebot angenommen.

Neue Ideen: Der „way ahead“

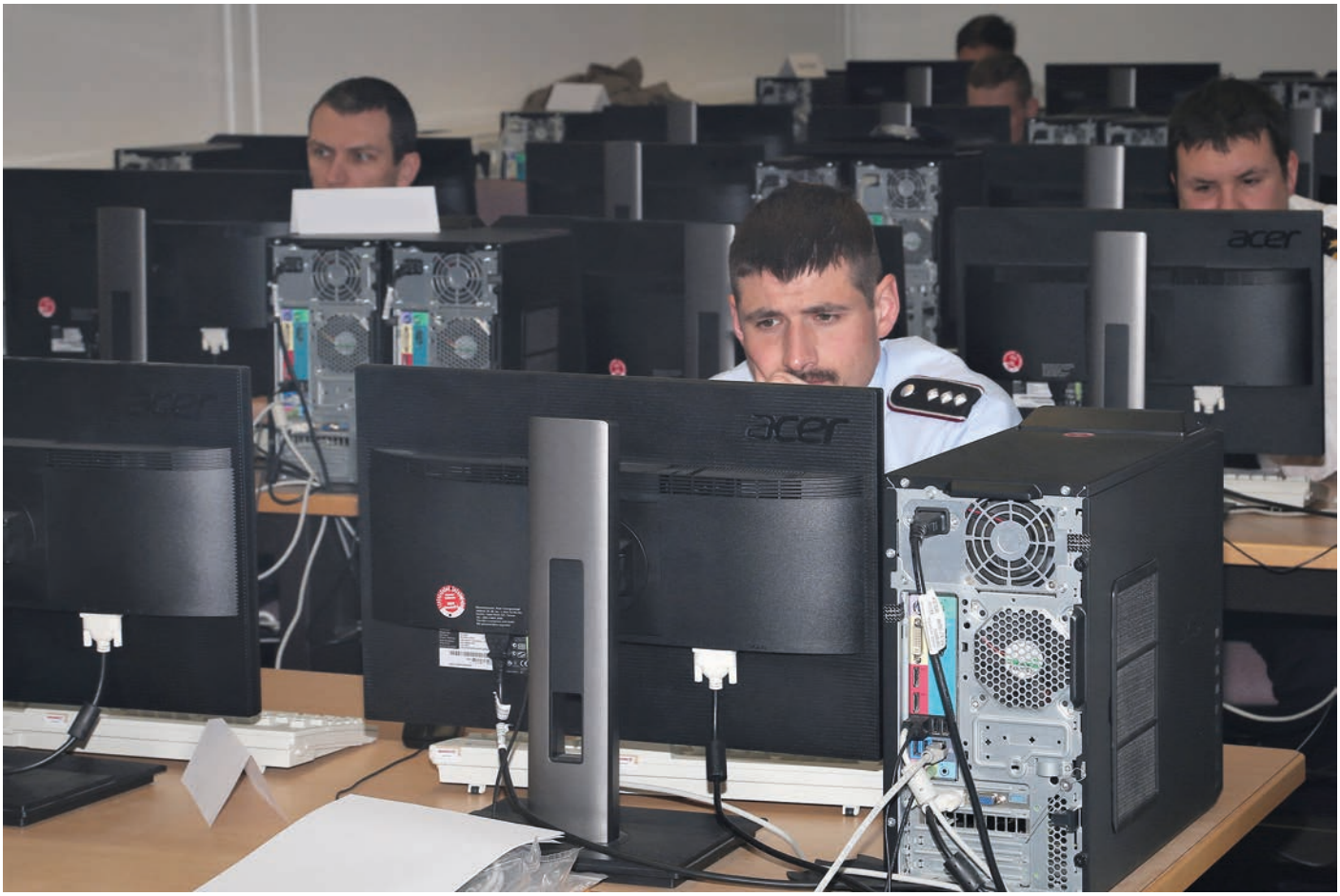
Für 2020 haben bereits mehrere Dutzend weitere Offiziere ihr Interesse an einer Testung am CITEC angemeldet. Die zweite Testung erfolgte im März; weitere folgen noch im gleichen Jahr. Parallel wird ein weiteres Testmodul für das ITT 2 entwickelt. Dieses Modul erweitert das Modul A um ein tiefergehendes IT-Screening. Es wird simulationsgestützt die zuvor festgestellten IT-Kenntnisse verifizieren und den testenden IT-Experten ermöglichen, tiefergehende fachliche Potentiale abzuschätzen. Auf dieser Basis sollen im November 2020 erstmalig Seiteneinsteiger – also Bewerber, die mit einem formalen Abschluss, beispielsweise einem Studium, mit höherem Dienstgrad in die Bundeswehr eingestellt werden wollen – fachlich getestet werden.

Ab 2021 soll zudem das ITT 1 programmiert werden und zur Verfügung stehen. Im ITT 2 sollen dann auch Bewerber, die sich gleich mit Abschluss ihrer Schul- oder Berufsausbildung bei der Bundeswehr bewerben, einem fachlichen Screening unterzogen werden können.



Der Test am CITEC wertet die individuellen Fähigkeiten der Kandidaten in neun Vertiefungen aus und bewertet diese anhand von acht Kriterien. (Grafik: Bundeswehr / KdoCIR)

Die ersten 19 Offiziere stellten sich im November 2019 dem neuen Test. (Foto: Bundeswehr / Monika Monden)



In der letzten Ausbaustufe des ITT 2 sollen nach Entwicklung von weiteren Modulen auch Kandidatinnen und Kandidaten ohne formalen Bildungsabschluss getestet werden können. Zurzeit erfolgt die Einstellung in eine Laufbahn der Bundeswehr aufgrund formaler Bildungsabschlüsse. In dem hochvolatilen Cyber/IT-Dienst sind aber vielmehr tatsächliche Fähigkeiten zur Erfüllung spezifischer Aufgaben gefragt. Es gibt unzählige Beispiele von international anerkannten IT-Experten, die nie einen formalen IT-Abschluss erzielt haben, sondern ihr Wissen in Eigenleistung erworben haben. Um auch diese „klugen Köpfe“ mit einer attraktiven Laufbahn ansprechen zu können, haben sich die Planer hinter dem CITEC als ambitioniertes Fernziel die Validierung non-formaler Kompetenzen als mögliche Voraussetzung zur Einstellung mit höherem Dienstgrad gesetzt. Der erste Schritt, eine erforderliche Anpassung der Soldatenlaufbahnverordnung, wurde bereits initiiert.

Neue monetäre Möglichkeiten

Über die Fachkarriere und das CITEC hinaus wurden in 2019 auch im Bereich der monetären Vergütung entscheidende Weichen gestellt. In das Besoldungsstrukturenmodernisierungsgesetz konnten zwei völlig neue Cyber/IT-Dienst bezogene Zulagen eingebracht werden. Die Zulage für Soldatinnen/Soldaten und Beamtinnen/Beamte in der Cyber-Verteidigung fokussiert auf das Personal, welches entweder mit Computernetzwerkoperationen betraut ist oder Maßnahmen der operativen Cyberabwehr wahrnimmt. Die Zulage für Soldatinnen/Soldaten und Beamtinnen/Beamte zur Aufrechterhaltung und Sicherstellung des IT-Betriebs der Bundeswehr richtet sich an das hochqualifizierte Personal, welches in zentralen Einrichtungen die Aufrechterhaltung und Sicherstellung des IT-Betriebs der Bundeswehr gewährleistet.

Diese Zulagen wenden sich vor allem an die fachliche Wahrnehmung von Aufgaben im Cyber/IT-Dienst. Die in Führungsverantwortung eingesetzten Soldatinnen und Soldaten im Cyber/IT-Dienst profitieren von der Neufassung einer Zulage für militärische Führungskräfte der Bundeswehr.

Schließlich wurden die bestehenden Personalbindungs- und -gewinnungszuschläge umfassend überarbeitet und modernisiert. Vorgesehen sind diese nicht nur für Einstellung und Weiterverpflichtung, sondern erstmalig auch für Berufssoldaten. Diesen kann, bei Vorliegen von attraktiven Beschäftigungsangeboten außerhalb der Bundeswehr, ein monetärer Anreiz zum Verbleib unterbreitet werden.

Insgesamt wurde ein finanzielles Maßnahmenpaket geschnürt, welches ein Engagement im Cyber/IT-Dienst auch in monetärer Hinsicht deutlich aufwertet.

Zusammenfassung

Der Cyber/IT-Dienst braucht den Vergleich mit der zivilen Wirtschaft nicht zu scheuen. Innerhalb von zwei Jahren konnten weitreichende Voraussetzungen geschaffen werden, um Fachkräfte für den Dienst in der Bundeswehr anzusprechen. Mit der Schaffung des fachlichen Werdegangs Cyber/IT und des CITEC ist der Organisationsbereich Cyber- und Informationsraum neue Wege gegangen. Der weitere Ausbau des CITEC wird dazu beitragen, die Bundeswehr in Zeiten des IT-Fachkräftemangels zukunftssicher aufzustellen und den Weg im Zeitalter der Digitalisierung zu bahnen.

wt

Oberstleutnant i.G. Dennis Pohl *ist Referatsleiter für Grundsatzfragen des Personalmanagements und* ***Oberstleutnant i.G. Alexander Strelau*** *ist Sachgebietsleiter Fähigkeitsentwicklung für die Entwicklung der Vorgaben zum personellen Verwendungsaufbau für den Cyber/IT-Dienst, beide im Kommando CIR.*

Die Cyber-Reserve nutzt das fachliche Potenzial der Reserve und ihre gesellschaftliche Vernetzung für die gesamtstaatliche Sicherheit. (Grafik: Bundeswehr / KdoCIR)

Generalmajor Jürgen Setzer

Die Cyber-Reserve der Bundeswehr – Eine erste Bilanz

Die Cyber-Reserve ist zu ihrer Aufstellung im Jahr 2017 mit großen Erwartungen gestartet. Nach Vollendung der ersten drei Jahre kann die Cyber-Reserve auf eine beachtliche Leistung zurückblicken. Über die personelle Unterstützung der aktiven Truppe hinaus leistet sie einen anerkannten Beitrag zur gesamtgesellschaftlichen Sicherheitsvorsorge im Bereich Cyber- und IT-Sicherheit. Hierzu bietet die Cyber-Reserve insbesondere Beschäftigten aus kleinen und mittleren Unternehmen interessante Perspektiven der Wissensvermittlung.

Cyber-Reserve – Geburtsstunde eines innovativen und interdisziplinären Kräfteelements

Die Gefährdungslagen im digitalen Raum haben sich in den letzten Jahren dramatisch verändert. Das Bedrohungspotenzial für die kritische Infrastruktur, wie staatliche Institutionen, Energie- und Gesundheitsversorger, Banken und Logistikbranche, wird durch die öffentlich wahrnehmbaren Cyber-Attacken für die Bevölkerung immer deutlicher erfahrbar. Solche Angriffe attackieren sensible Bereiche unseres Gemeinwesens und können für die Bürgerinnen und Bürger unseres Landes gravierende Auswirkungen haben. Manipulationen von Datensätzen und Identitätsdiebstahl bilden darüber hinaus eine nicht zu unterschätzende Qualität von Cyber-Attacken, die auch vor der Bundeswehr nicht Halt machen. Unabhängig von der Kompromittierung ziviler Stellen steht die Bundeswehr gleichfalls im Fokus digitaler Angriffe. Nicht nur der Wettlauf der eingesetzten digitalen Systeme und die Fähigkeitsentwicklung fordern die Bundeswehr und verbündete Streitkräfte, sondern auch der Facettenreichtum möglicher hybrider und asymmetrischer Bedrohungsszenare. Hier sind über digitale Angriffe hinaus insbesondere Einflussnahmen auf die öffentliche Meinung durch Fake News von entscheidender Sensibilität, wie dies der Fall der vermissten Schülerin „Lisa“ im Jahr 2016 eindrucksvoll zeigte, indem meinungsgestaltende Impulse über soziale Netzwerke nachhaltig ihre Verbreitung fanden. Auch die Bundeswehr verzeichnet solche Online-Desinformationsaktivitäten gegen sich, beispielsweise im Baltikum. Der Schlüssel zum verantwortungsvollen und angepassten staatlichen Handeln ist daher eine zeitnahe Lagebewertung im Cyber- und Informationsraum. Die Urheber solcher Angriffe sind oftmals nur schwer identifizierbar. Die Zuordnung eines digitalen Schadensfalles als krimineller Akt oder gar als Teil einer hybriden Kampagne eines ausländischen Akteurs ist meist nur unter hohem Analyseaufwand möglich. Was auf der einen Seite durch die Angreifer auf unser Gesellschaftssystem im Verborgenen läuft, kann andererseits für die Betroffenen, wie Bürger, Behörden und Unternehmen, unmittelbar als auch zeitlich weit verschleiert schwerwiegende Folgen auslösen. Wenn die Strom- als auch die Patientenversorgung in Krankenhäusern digitalen Manipulationen ausgesetzt ist, die Existenz Einzelner durch Identitätsdiebstahl und Erpressungsversuche sowie ganze Unternehmen durch online-Spionage Gefahr laufen, sensible Geschäftsgeheimnisse zu verlieren und im internationalen Wettbewerb abgehängt zu werden, ist der Staat gefordert. Auf diese Bedrohungslagen hat die Bundesregierung robust reagiert und mithin die IT-Sicherheitslandschaft neu aufgestellt. Neben staatlichen Stellen stehen auch Unternehmen der kritischen Infrastruktur in der Mitverantwortung zur Härtung der eingesetzten Computersysteme vor Cyber-Angriffen. Im Selbstverständnis einer verantwortungsvollen und gesamtstaatlichen Sicherheitsarchitektur hat die Bundesrepublik Deutschland die Bundeswehr mit der Sicherung Deutschlands vor äußeren Angriffen im Cyber- und Informationsraum beauftragt. In diesem Kontext und vor dem Hintergrund einer wachsenden Bedrohungslage wurden das weitreichende fachliche Potential der Reserve und ihre gesellschaftliche Vernetzung in die gesamtstrategische Überlegung mit einbezogen. Mit Erlass des Konzeptes für die personelle Unterstützung der „Cyber-Community“ der Bundeswehr wurde zum 2. März 2017 die Cyber-Reserve aufgestellt.

Cyber-Reserve – zwischen wachsenden Bedrohungen und knappen personellen Ressourcen

Die Cyber-Reserve ist ein innovatives und interdisziplinär aufgestelltes Unterstützungsinstrument. Sie bildet einen Transmissionsriemen in die Gesellschaft und bietet fachlichen Erfahrungsaustausch. Sie ist als Teil der Bundeswehr in die gesamtstaatliche Sicherheitsarchitektur der Bundesrepublik Deutschland eingebunden. Die Angehörigen der Cyber-Reserve leisten ihren Beitrag bei der Sicherung Deutschlands vor äußeren Angriffen im Cyber- und Informationsraum. Im Kontext dieses Kernauftrages ist eine Vielzahl an Fähigkeiten gefragt, die sich perspektivisch an der Dynamik der modernen Bedrohungsszenarien und Technologien ausrichten. Dies bezieht neben künstlicher Intelligenz etwa auch Expertisen aus der Weltraumforschung mit ein. Eine weitere Herausforderung bildet im Kontext hybrider und asymmetrischer Kampagnen die Identifizierung der ressortspezifischen Trennlinie zwischen äußerer und innerer Bedrohung. Konkret geht es hierbei um die richtige Zuordnung von „digitalen Anomalien“: Handelt es sich hierbei um von Kriminellen initiierten CyberCrime, der in die Zuständigkeit der Strafverfolgungsbehörden fällt, oder handelt es sich um konzertierte Attacken im Cyber- und Informationsraum, die durch andere Staaten oder Terrororganisationen grenzüberschreitend initiiert werden und die Bundesrepublik Deutschland sowie ihre Bündnispartner bedrohen. Letzteres Szenario fiele in die Zuständigkeit des Ressorts des Bundesministeriums der Verteidigung. Gerade die Verantwortlichen für verschleierte militärische Operationen einzukreisen und diese richtig zu identifizieren ist ein Schlüsselelement. Um mithin eine fachlich valide Zuordnung von Attacken verantwortungsvoll sicherstellen zu können, sind unterschiedliche Disziplinen notwendig, voran Polizisten und Kriminologen aus dem Bereich CyberCrime-Forensik des Bundes und der Länder. Perspektivisch sind zum Aufbau des Fähigkeitsspektrums Interdisziplinarität insbesondere CIR-spezifische Studiengänge wie IT-Forensik als auch sozial- und organisationswissenschaftliche Expertisen zur Netzwerkanalyse gesucht. Hier ist ein kontinuierlicher Expertisenaustausch erforderlich, um kritische Vorkommnisse ressortgerecht innerhalb des föderalen Systems der Bundesrepublik Deutschland richtig den verfassungsgemäßen Zuständigkeiten zuordnen zu können. Erschwerend kommt beim Aufbau einer gesamtstaatlichen Sicherheitsarchitektur – für die Ressorts Innere Sicherheit und Verteidigung als auch für die Wirtschaft – noch hinzu, dass verfügbare Expertinnen und Experten im Bereich Cyber-/IT- und Informationssicherheit auf dem Arbeitsmarkt eine kostbare Ressource darstellen. Eine Situation, die sowohl dem demografischen Wandel als auch der hohen Komplexität in der Cyber- und IT-Sicherheit in unserem Lande nachweislich geschuldet ist. Dies führt nachvollziehbar zur Verknappung vorhandener Expertinnen und Experten auf dem Arbeitsmarkt. Hierauf hat die Bundeswehr innovativ durch das Konzept Cyber-Reserve reagiert und für alle Akteure im Cyber- und Informationsraum interessante Wege zur ressortübergreifenden Kooperation und Mitarbeit von öffentlichem Dienst, Wirtschaft, Forschung und Lehre mit dem Ziel des Fähigkeitstransfers etabliert.

Ziele der Cyber-Reserve

Die Cyber-Reserve verfolgt drei konkrete Ziele:

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 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.

Das Prinzip Cyber-Reserve

Der Bundeswehr und speziell dem neu aufgestellten Organisationsbereich Cyber- und Informationsraum ist bewusst, dass die neuen digitalen Veränderungen und asymmetrischen Bedrohungslagen sowie hybriden Formen der Konfliktaustragung einen hohen Experten-Bedarf mit sich bringen, jedoch die eigenen Ressourcen nicht ausreichen. Erschwerend kommt hinzu, dass der Personalbedarf durch die sich rasch verändernden Szenarien künftig noch weniger vorausschauend planbar

Hauptfeldwebel d.R. Georgi Steffenhagen, B.Sc., entwickelt im Referat Reservisten des Kommando CIR hausinterne Softwarelösungen. (Foto: Bundeswehr / Holger Bartnitzki)

Oberstabsgefreiter d.R. Markus Reiser, B.A., bei der Datenaufnahme und -pflege der Interessendatenbank beim Inspizienten für Reservistenangelegenheiten. (Foto: Bundeswehr / Holger Bartnitzki)

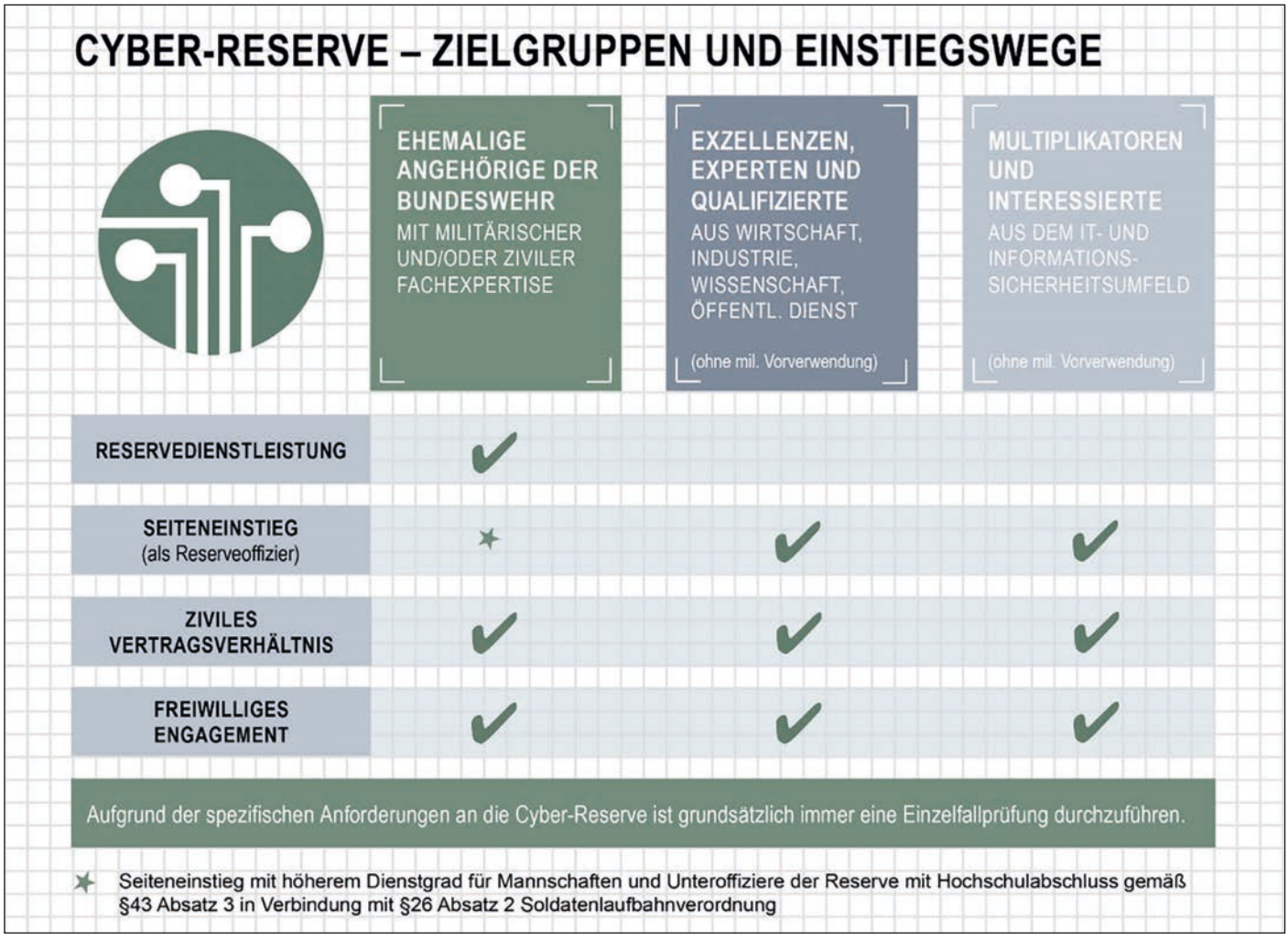
wird. Dies stellt eine besondere Herausforderung für die Bundeswehr dar. Ein strategischer Lösungsansatz bildet hierbei die Cyber-Reserve.

Die Cyber-Reserve steht daher nicht nur hoch qualifizierten Reservistinnen und Reservisten offen, sondern bietet auch Interessierten, die bisher noch keine Berührung zur Bundeswehr hatten, verschiedene Möglichkeiten der Mitarbeit an. Ausgehend vom Grundsatz der Freiwilligkeit bietet die Cyber-Reserve neben der Mitarbeit im Status Soldat als Reservistendienst Leistender auch weitere Formen der Mitarbeit an. Über zivile Vertragsverhältnisse hinaus bis hin zum bürgerschaftlichen Engagement hat sich die Bundeswehr auch für Mitmenschen geöffnet, die sich konkret für die Bundeswehr und somit für unsere Gesellschaft und unseren Staat einsetzen möchten. Dies auch, wenn diese Engagierten nicht in einem Wehrdienstverhältnis tätig werden können oder wollen.

Zielgruppenmanagement – Das Cyber-Potential als konzeptioneller Anker in die Gesellschaft

Konkret stehen folgende Zielgruppen im Fokus der Personalgewinnung für die Cyber-Reserve:

1. Ehemalige Angehörige der Bundeswehr mit militärischer und/oder ziviler Fachexpertise.
   Ausscheidende Berufs- und Zeitsoldatinnen bzw. Berufs- und Zeitsoldaten, freiwillig Wehrdienstleistende sowie Zivilbeschäftigte (mit und ohne Studium, jedoch mit einschlägigen, für die Cyber-Reserve nutzbaren Verwendungen und Kenntnissen).
   Personen, die über spezialisierte Ausbildungen oder herausragende Fähigkeiten, Fertigkeiten und Kompetenzen in einschlägigen Bereichen oder Funktionen verfügen.
2. Exzellenzen, Expertinnen und Experten aus Wirtschaft, Industrie, Wissenschaft und Öffentlichem Dienst.
   Dazu gehören beispielsweise Vorstände, Geschäftsführerinnen und Geschäftsführer, Leitende Angestellte, Wissenschaftlerinnen und Wissenschaftler oder Führungskräfte mit entsprechendem herausragendem Know-how, die aktiv ihr Fachwissen der Bundeswehr zur Verfügung stellen. Diese Zielgruppe unterstützt durch ihr Engagement die Bundeswehr, um interessierte Mitbürgerinnen und Mitbürger für die Cyber-Reserve zu gewinnen.
3. Multiplikatoren und Interessierte.
   Diese Zielgruppe umfasst:
   a) Freiwillige, die sich außerhalb der Reserve engagieren wollen.
      Dazu zählen Fachkräfte, Experten und Führungskräfte beispielsweise aus dem „CERT“ (computer emergency response team) – Umfeld, IT- und Informationssicherheitsverantwortliche, aber auch Freiwillige, wie beispielweise Studierende, Angehörige von Nicht-Regierungsorganisationen, Vereinen und Verbänden, sonstige Talente und Freiberufler, die für vielfältigste Aufgaben im Cyber-/IT-Bereich herangezogen werden können (Beispiel: „Ethical“ Hacker, die in gemeinsamen Übungen Cyberangriffe simulieren) und die im



Die Zugangswege in die Cyber-Reserve sind vielfältig.
(Grafik: Bundeswehr / KdoCIR)

Rahmen eines ehrenamtlichen oder bürgerschaftlichen Engagements in der Bundeswehr – ohne Soldatenstatus – tätig werden.

b) Seiteneinstieg/ Direkteinstellung
Hier kommen sowohl gediente als auch ungediente Interessenten mit einschlägigem fachlichem Hintergrund außerhalb der Bundeswehr in Betracht, die über etablierte Fach-Foren, Netzwerke, Fach-Veranstaltungen oder vergleichbare Plattformen als potenzielle Cyber-Reservisten identifiziert werden und aktiv geworben werden können.

Die Cyber-Reserve als flexibles Kräftedispositiv – Kooperationsbereitschaft als Schlüssel robusten gesamtstaatlichen Handelns

Die Bundeswehr hat die Zeichen der Zeit klar erkannt. Zur Flexibilisierung und Sicherstellung der Einsatzbereitschaft bietet die Reserve den strategischen Vorteil, auch kurzfristig Fachleute nach Bedarf einsetzen zu können. Hierfür knüpft das Kommando Cyber- und Informationsraum über die Arbeitgeberverbände und Kammern ein Unterstützernetzwerk. Insbesondere mit Institutionen und Unternehmen aus dem Bereich kritischer Infrastruktur bis hin zu Großunternehmen und dem Mittelstand sind seit der Aufstellung des Kommandos Cyber- und Informationsraum Verbindungen aufgebaut worden, geeignetes Fachpersonal für die Cyber-Reserve zu finden. Das Schlüsselelement ist hierbei, und das ist die gesamtgesellschaftliche Herausforderung, die Arbeitgeberseite für diese dialogorientierte Kooperation des Fähigkeitstransfers zu gewinnen, um interessierte und qualifizierte Arbeitnehmerinnen und Arbeitnehmer für Reservistendienstleistungen freizustellen.

Die Cyber-Reserve versteht sich daher ausdrücklich nicht als Einbahnstraße. Im Selbstverständnis des Netzwerkansatzes bindet die Cyber-Reserve alle Fähigkeitsträger mit ein. Durch den Fähigkeitstransfer und das miteinander Lernen setzt die Cyber-Reserve sichtbare Akzente. Hierdurch besitzt die Bundeswehr ein zusätzliches Kräftedispositiv, das insbesondere bei besonderen Bedarfslagen auch andere Behörden bis hin zu Unternehmen der kritischen Infrastruktur mit Know-how unterstützen kann.

Aufgrund der besonderen Bedeutung für die gesamtstaatliche Sicherheitsvorsorge hat das Verteidigungsministerium der Cyber-Reserve im Herbst 2019 eine gewichtige Rolle bei künftigen Konflikten zugesprochen. Im Positionspapier „Strategie der Reserve“ ist klar definiert, dass nach dem Aussetzen der Wehrpflicht perspektivisch innovative Lösungen zur möglichst verzugslosen Einbindung von Reservistinnen und Reservisten in einer Krisensituation oder bereits im Vorfeld einer Krise gefunden werden müssen. Dieser Findungsprozess wird daher in einem gesamtstaatlichen und gesamtgesellschaftlichen Ansatz erfolgen. Ziel ist hierbei, im offenen Dialog mit allen relevanten Akteuren die Gewinnung von zivilen Cyber- und IT-Expertinnen und -Experten für einen kontinuierlichen Expertisenaustausch sicherzustellen, um die „Cyber-Community“ der Bundeswehr schlagkräftig unterstützen zu können. Somit besitzt die Cyber-Reserve für die Bundeswehr als Innovationsmotor Impulscharakter.

Dies gilt auch für den von der Bundeswehr eingeschlagenen Weg, sich weiter für Ungediente zu öffnen. Hierbei steht nicht nur der klassische IT-Spezialist im Fokus, sondern das umfassende Spektrum an Fähigkeiten. Desinformations- und Hetzkampagnen bedürfen zur Erkennung als niedrigschwellige Eskalationsformen zur Vorbereitung von Destabilisierungen von Gesellschaften professionelle Analysen. Somit ist ein breiter Expertenkreis über alle Disziplinen hinweg angesprochen.

Seit der Aufstellung des neuen Organisationsbereiches CIR haben sich bereits an die 1.000 Interessentinnen und Interessenten aus den unterschiedlichsten Disziplinen initiativ an das Kommando Cyber- und Informationsraum gewandt und über einen fachlichen Informationsaustausch hinaus auch den Schritt gewagt, sich für den Seiteneinstieg in die Offizierslaufbahn der Reserve zu bewerben. Ein ambitionierter Weg, der neben zeitlichem Engagement auch die Bereitschaft der Teilnahme an einer Offizierslaufbahn erfordert. Die ersten Freiwilligen haben das Assessment Center bestanden und befinden sich seit diesem Jahr in der Ausbildung. Bereits jetzt bringen sie ihre Expertise in die Bundeswehr ein.

GRIFFIN DAWN ist die deutsch-niederländische Cyber-Übung mit Reservisten. (Grafik: Bundeswehr / Holger Bartnitzki)

Die Renaissance der Reserveoffizier-Ausbildung – „ROA 2.0“

Mit Aussetzen der Wehrpflicht vom 1. Juli 2011 wurde die Bundeswehr von einer Wehrpflichtigenarmee zu einer Berufsarmee umstrukturiert. Somit ist heute das gesamte Engagement in der Reserve auf das Primat Freiwilligkeit aufgebaut. Die Regeneration von Reservisten aller Dienstgradgruppen speiste sich vor dem Umbau aus der Wehrpflicht und der anschließenden Beorderung. Hieraus generierten sich überwiegend die späteren Unteroffiziere und Offiziere der Reserve. Mit dem Erlass zum Aufbau der Cyber-Reserve bietet die Bundeswehr interessierten Mitbürgerinnen und Mitbürgern vielfältige Möglichkeiten, ihre Fähigkeiten in die Sicherheitsarchitektur der Bundesrepublik Deutschland freiwillig einbringen zu können. Aufgrund des hoheitlichen Auftrages der Bundeswehr gibt es jedoch Bereiche in der Cyber-Abwehr und IT-Sicherheit, in denen ausschließlich Expertinnen und Experten im Soldatenstatus Dienst leisten dürfen. Für diese Spezialisten bietet die Bundeswehr den Seiteneinstieg als Reserveoffizier in der militärfachlichen Verwendung an.

Interessierte, die über einen akademischen Abschluss verfügen, können sich bei der Bundeswehr als Seiteneinsteigerin oder Seiteneinsteiger für eine militärfachliche Verwendung mit höherem Dienstgrad bewerben. Nach Feststellung der wehrrechtlichen Verfügbarkeit – wie gesundheitliche Eignung und Unbescholtenheit – und Bestenauswahl durch das Karrierecenter durchlaufen sie mit einem vorläufig verliehenen Offizier-Dienstgrad eine verkürzte Offizierausbildung. Derzeit erstreckt sich diese Ausbildung für ungediente Bewerberinnen und Bewerber über sechs Ausbildungsmodule mit einer Gesamtzahl von 79 Ausbildungstagen und 129 Telekollegstunden, die – angepasst an die zivilberuflich bedingte Verfügbarkeit – in Kurzzeitveranstaltungen innerhalb von drei Jahren abzuschließen ist. Je nach vorgesehener Verwendung schließen sich dann weitere Fachlehrgänge an. Gleichfalls gewinnt ein weiteres Ausbildungsangebot der Reserveoffizierausbildung künftig größere Beachtung. Das Potential des klassischen Ausbildungsganges für Reserveoffizieranwärterinnen und -anwärter außerhalb des Wehrdienstes (ROA a.d.W.) wird wiederentdeckt. Hiermit spricht die Bundeswehr und voran der militärische Organisationsbereich Cyber- und Informationsraum interessierte Studierende an zivilen Hochschulen an, sich für eine vergleichbar komprimierte Offizierausbildung in der Reserve zu engagieren. Ähnlich eines Stipendiums erhalten hierdurch künftige Akademikerinnen

und Akademiker während ihres Studiums eine fundierte Zweitausbildung zur Führungskraft und durchlaufen gestrafft alle militärischen Ausbildungsstufen von der Grundausbildung über den Gruppenführer bis hin zum Zugführer. Bei geplanten Verwendungen als IT-Offizier schließt sich sodann eine fachliche Ausbildung an. Interessant für Studierende aus den Spezialgebieten ist, dass bereits an den Hochschulen vergleichbar erworbene Semesterscheine zur Verkürzung hierbei angerechnet werden können. Ein weiterer Vorteil ist: Mit der zweiten vollwertigen Ausbildung als Reserveoffizier – parallel zum zivilen Studium – bringen die Absolventen als Jungakademiker bereits nachweislich berufliche Erfahrung beim Start in das zivile Berufsleben mit. Auch eröffnet sich nach der Studienzeit die Möglichkeit, neben dem zivilen Arbeitsmarkt, die Bundeswehr als potentiellen Arbeitgeber mit dem Direkteinstieg als Wiedereinsteller wahrzunehmen. Dieses Ausbildungsangebot bietet gerade vor dem Hintergrund der Unterhaltssicherungsleistungen, die durch das Bundesamt für Personalmanagement der Bundeswehr geleistet werden, eine gegenüber dem zivilen Markt beachtliche finanzielle Perspektive, die Semesterferien fachorientiert für die eigene berufliche Entwicklung zu nutzen sowie planbare finanzielle Ressourcen für das Studium sichern zu können. Beide oben skizzierte Offiziersausbildungen vermitteln die Befähigung zum militärischen Vorgesetzten und zur Menschenführung sowie die Eignung, verantwortungsvoll hoheitliches Handeln umzusetzen. In dieser Verantwortung stehen die Reservistendienst Leistenden der Cyber-Reserve.

Stabsunteroffizier d.R. Holger Bartnitzki unterstützt den Inspizienten für Reservistenangelegenheiten und das Referat Reservisten im Kommando CIR als Medienproduktionsunteroffizier.
(Foto: Bundeswehr / KdoCIR)

Cyber-Reserve als Speerspitze internationaler Zusammenarbeit

Die hohe Dynamik von Cyber-Attacken und die multiple Verwundbarkeit international verbundener Systeme, die das Rückgrat unserer freien Demokratie in Europa und der transatlantischen Bündnispartner in der NATO bedrohen, erfordern wehrhafte Allianzen. Mit dieser Notwendigkeit im Blick hat im Herbst 2019 die erste deutsch-niederländische Cyber-Übung GRIFFIN DAWN stattgefunden. Hier lag der Schwerpunkt auf dem Kennenlernen und ersten Übungsszenarien. Im Frühsommer 2020 erfolgt die Gegenübung beider Partnerländer in Deutschland, um die bisherigen Erfahrungen in der Zusammenarbeit weiter auszuweiten. Unter hohem internationalen Interesse steht dieses Format auch anderen NATO-Partnern offen, um ein gemeinsames Üben und den Erfahrungsaustausch sicherstellen zu können.

Deutschland und die Niederlande bilden den Nukleus einer zunächst europäischen Cyber-Reserve, die Zug um Zug durch weitere interessierte Länder erweitert werden soll. Hier soll mit Blick auf die NATO durch eine eigene Vernetzung der internationalen Akteure Impulse gesetzt und das gemeinsame Lernen gefördert werden.

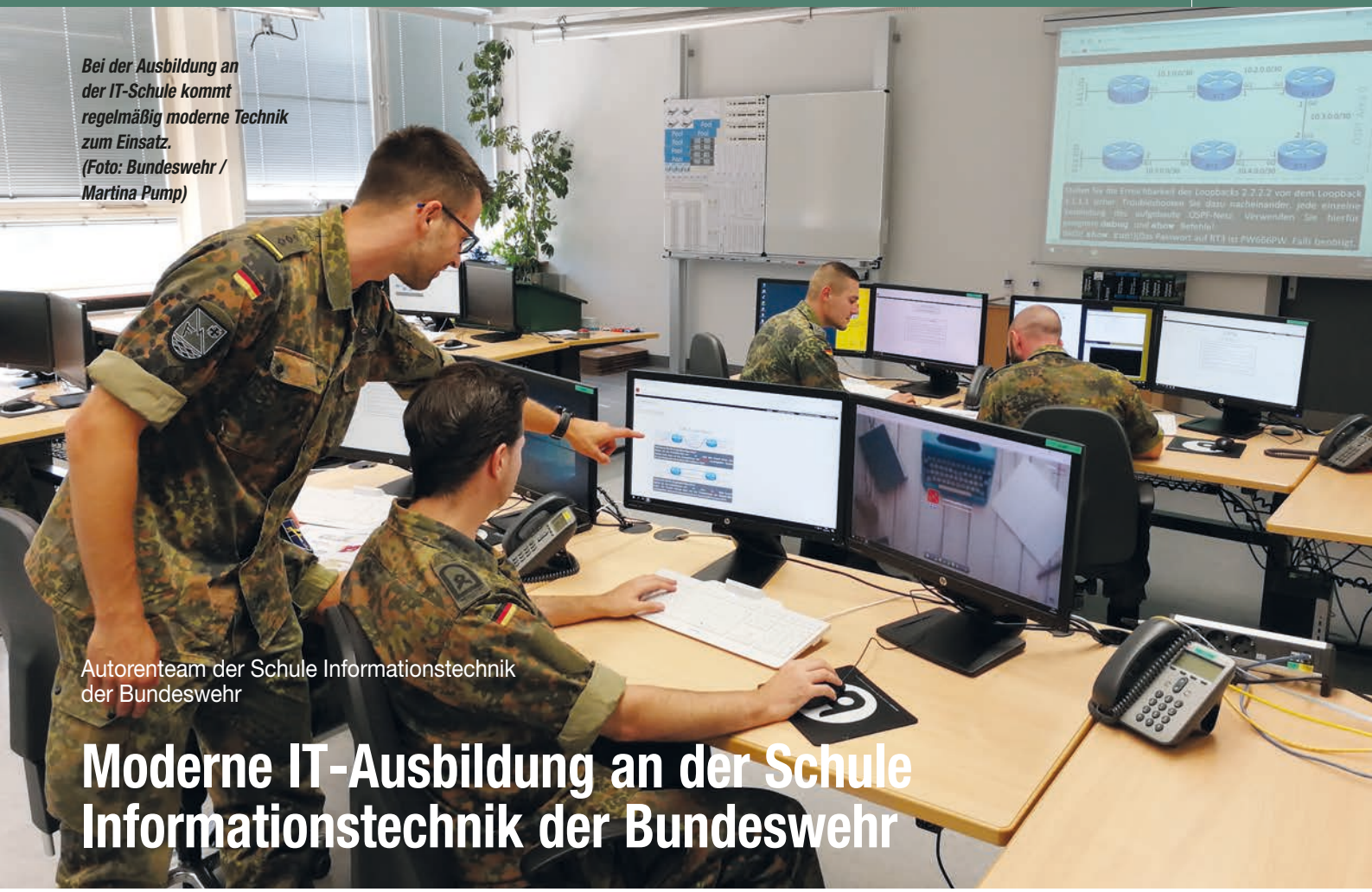
Attraktivität im gesamtgesellschaftlichen Verständnis

Der Bedarf an qualifizierten IT-Fach- und Führungskräften ist hoch, das Angebot vergleichsweise gering. Derzeit sind mehrere Ansätze im Rahmen der Attraktivitätssteigerung und Personalgewinnung in der näheren Betrachtung. Von der Anerkennung ziviler Qualifikationen, über die Einbindung von Fähigkeitsträgern ohne staatlich anerkannte Abschlüsse bis hin zur Inklusion. Auch hier befindet sich die Bundeswehr in der strukturellen Transformation, die etablierten Prozesse der Personalfindung und -gewinnung auf die neuen Bedarfslagen hin anzupassen. Das entscheidende Potential der Reserve liegt, wie das Thema IT-Sicherheit und -Forensik im Kontext kompromittierter IT-Systeme der kritischen Infrastruktur erahnen lässt, im Wissenstransfer und im Reiz, an sensiblen Aufgabestellungen der Wiederherstellung kompromittierter Netzwerke kritischer Infrastruktur mitarbeiten zu können.

Ferner besitzt die Bundeswehr ein vielfältiges Weiterbildungspotential, das sich die öffentliche Verwaltung wie auch Großunternehmen und Unternehmen des Mittelstands über die Freistellung von Belegschaftsangehörigen erschließen können. Dies betrifft insbesondere den Erfahrungsaustausch als aktiven Beitrag zur Prävention im Bereich Cyber-Sicherheit. Hierzu ist Ende 2018 eigens eine Kommunikationsplattform „Cyber-Community“ online gestellt worden. Hierüber können sich Interessierte zu Themen der Cyber- und IT-Sicherheit austauschen – gleich, ob sie Teil der Cyber-Reserve sind oder nicht (https://bundeswehr.community, community@cyberinnovationhub.de). Gleichfalls baut der Organisationsbereich Cyber- und Informationsraum perspektivisch weitere Dienstposten für die künftigen Bedarfe an Spezialisten der Cyber-Reserve auf. Dies, um einerseits das hohe Aufkommen an Interessierten zielführend kompensieren zu können und um andererseits als Organisationsbereich die strategische Flexibilität zu erhöhen, rasch auf verändernde Situationen zu reagieren und gezielt spezielle Fähigkeiten über das Cyber-Netzwerk und deren Partner aus Wirtschaft, öffentlicher Verwaltung und Forschung kurzfristig gewinnen zu können. Mithin ist das gesuchte Expertenportfolio weit gefächert: über die klassischen IT-Fachleute hinaus sind Spezialisten für künstliche Intelligenz wie auch Cyber-Rechtsexperten bis hin zu Politikwissenschaftlern und Landeskundler gefragt. Somit erhält die Bundeswehr ein Kräftedispositiv, das dem Anspruch einer State-of-the-Art Cyber-Wirkkomponente gerecht wird. Die Arbeitgeber bleiben aufgerufen, im Verständnis bürgerschaftlichen Engagements als Partner der Reserve hierbei eine aktive Rolle zu übernehmen und der Belegschaft die Mitarbeit in der Cyber-Reserve als bewussten Beitrag der Krisen- und Daseinsvorsorge zu ermöglichen. Denn ohne Arbeitgeberinnen und Arbeitgeber sind Reservistendienst-Arrangements und zivile Vertragsverhältnisse für Beschäftigte nicht realisierbar.

wt

Generalmajor Jürgen Setzer *ist Stellvertreter Inspekteur CIR und Beauftragter für Reservistenangelegenheiten des Organisationsbereichs CIR.*



Bei der Ausbildung an der IT-Schule kommt regelmäßig moderne Technik zum Einsatz. (Foto: Bundeswehr / Martina Pump)

Autorenteam der Schule Informationstechnik der Bundeswehr

Moderne IT-Ausbildung an der Schule Informationstechnik der Bundeswehr

Im Zeitalter der Digitalisierung kann die Ausbildung von IT-Personal nicht mehr als „Rucksack für 30 Jahre“ gestaltet sein. Vielmehr kommt es auf kontinuierliches und flexibles, mithin lebenslanges Lernen an. Dies ist das Ziel der Schule Informationstechnik der Bundeswehr. Gestützt auf moderne technische Methoden reformiert sie die IT-Ausbildung der Feldwebel und Offiziere durch Modularisierung.

Ausgangssituation

Zunehmende Digitalisierung ist in allen Bereichen der Gesellschaft, Wirtschaft und Verwaltung eine Chance wie auch Herausforderung. Sie beeinflusst Prozesse, Geschäftsmodelle sowie Abläufe und Organisationsformen. Die technologische Weiterentwicklung zeichnet sich dabei durch immer kürzer werdende Innovationszyklen aus. Zuvor autarke IT-Kommunikationssysteme werden zu miteinander vernetzten, zunehmend integrierten Plattformen. Komplexität, Themenbreite und -tiefe und fortlaufende Veränderung stellen dabei besondere Anforderungen an eingesetztes Personal.

Der passgenauen fachlichen Aus-, Fort- und Weiterbildung des Cyber-/IT-Fachpersonals kommt daher besondere Bedeutung zu. Die Digitalisierung zwingt neben der verstärkten Rekrutierung von Cyber-/IT-Fachpersonal zu einer flexiblen und dynamischen Ausrichtung der Cyber-/IT-Aus-, Fort- und Weiterbildung. Denn eine alles umfassende Erstausbildung erscheint unter den oben angedeuteten Rahmenbedingungen nicht mehr zielführend. Ziel muss daher sein, mit Hilfe eines durchgängig verfügbaren Angebotes eine Kultur des kontinuierlichen „lebenslangen“ Lernens zu etablieren. Erworbenes Wissen und korrespondierende Fähigkeiten werden so ständig ergänzt und nutzbar gehalten.

Zeit- und ortsunabhängiges, informelles und selbstgesteuertes Lernen müssen befördert werden. Moderne, bedarfsgerechte und flexible Ausbildung ist somit eine Grundvoraussetzung, um Führungs-, Fach- und Funktionspersonal für die zu fordernde technologische Leistungsfähigkeit moderner Streitkräfte bestmöglich zu qualifizieren.

Die Schule Informationstechnik der Bundeswehr hat sich diesem Ziel bereits seit geraumer Zeit verschrieben. Sie treibt als zentrale militärische Ausbildungseinrichtung für die bundeswehrgemeinsame, lehrgangsgebundene, einsatz- und bedarfsorientierte Aus-, Fort- und Weiterbildung von Führungsunterstützungs-, IT-Fach- und Funktionspersonal der Bundeswehr moderne Ausbildung aktiv voran. Als Grundlage für die organisationsbereichsspezifischen Lehrgänge, die nach inhaltlichen Vorgaben des Fähigkeitskommandos, der jeweiligen Teilstreitkraft oder des jeweils verantwortlichen Organisationsbereiches und des Ressort-CIO des Bundesministeriums der Verteidigung (BMVg) konzipiert sind, dient die IT-Fortbildungsverordnung des Bundes. Der Ressort-CIO BMVg ist der Chief Information Officer und zuständig für die gesamte IT-Struktur im Geschäftsbereich.

Durchschnittlich werden knapp 1.000 Lehrgangsteilnehmende pro Tag (in Spitzenzeiten bis zu 1.200), jährlich insgesamt rund 5.000 Trainingsteilnehmende in bis zu 600 Trainings und mehr als 150 verschiedenen Trainingstypen ausgebildet.

Moderne Ausbildung wird dabei an der Schule Informationstechnik der Bundeswehr in vielerlei Hinsicht aktiv gestaltet, durchgeführt und weiterentwickelt. Dies soll im Folgenden an einigen ausgewählten Beispielen verdeutlicht werden. Ein Schwerpunkt ist dabei die Neuordnung der Ausbildung der IT-Feldwebel. Darüber hinaus werden weitere neue Entwicklungen in der Trainingslandschaft und der Einsatz moderner Ausbildungstechnik an der Schule vorgestellt.

Neues Basis-Training für IT-Feldwebel

Mitte des Jahres 2020 wird in einem ersten Schritt der Ausbildungsgang der Informationstechnik-Feldwebel des Allgemeinen Fachdienstes reformiert. Soldatinnen und Soldaten der Feldwebellaufbahn im Allgemeinen Fachdienst der Bundeswehr werden in allen militärischen Organisationsbereichen eingesetzt. Sie üben Fachtätigkeiten (zum Beispiel Administration von IT-Systemen) aus, die meistens nach dem erlernten Zivilberuf zugeordnet werden.
Die Hintergründe dieser grundlegenden Umstrukturierung sind vor allem:

- der gestiegene Bedarf der Streitkräfte an IT-Feldwebeln,
- ein insgesamt „atmender Personalkörper“ mit schwankenden Bedarfszahlen,
- die bisher lange Ausbildungsdauer inklusive entstehenden Wartezeiten zwischen den verschiedenen Fachqualifikationen im Ausbildungsverlauf,
- das Beenden der unzweckmäßigen Trennung der Fachrichtungen InfoÜbertragung und InfoVerarbeitung,
- die hohe Systemlastigkeit in der Ausbildung.

Um die Grundlage für eine schrittweise weitere Modernisierung der gesamten Lehrgangslandschaft im Bereich Informationstechnik zu schaffen, fasste das Kommando Informationstechnik der Bundeswehr im Konsens mit allen Organisationsbereichen Anfang des Jahres 2018 den Entschluss, gemeinsam mit der Schule Informationstechnik der Bundeswehr zunächst die Neuordnung der Feldwebel-Ausbildung zu erarbeiten. Kern ist die Einführung eines Basis-Trainings für IT-Feldwebel.

Bisheriger Ausbildungsgang

Seit Aufstellung der Streitkräftebasis im Jahr 2000 und der damit verbundenen Harmonisierung der IT-Ausbildung in der Bundeswehr gliedert sich der Ausbildungs-werdegang der Unteroffiziere mit Portepee in folgenden Dreiklang:

- Grundqualifikation,
- Fachqualifikation,
- Dienstpostenqualifikation.

Diese Qualifikationskategorien werden beim Verwendungsaufbau für jeden Soldaten beziehungsweise jede Soldatin in dieser Reihenfolge entweder durch militärfachliche Ausbildung oder zivilberufliche Aus- und Weiterbildung realisiert. Die daraus abgeleiteten Modelle für die Ausbildungs- und Verwendungsfolge sind organisationsbereichsübergreifend harmonisiert, wobei im Anschluss an die Laufbahnausbildung (Fachqualifikation „IT-Administrator-Feldwebel“) eine Spezialisierung für die Fachrichtungen Informationsverarbeitung, Informationsübertragung und S6, die „Dienstpostenausbildung Teil 1“, erfolgt.

Daran schließt sich die spezifische Ausbildung für das jeweilige IT-System, die „Dienstpostenausbildung Teil 2“ wie zum Beispiel Satelliten-Kommunikation an, welche die militärfachliche Ausbildung abschließt.

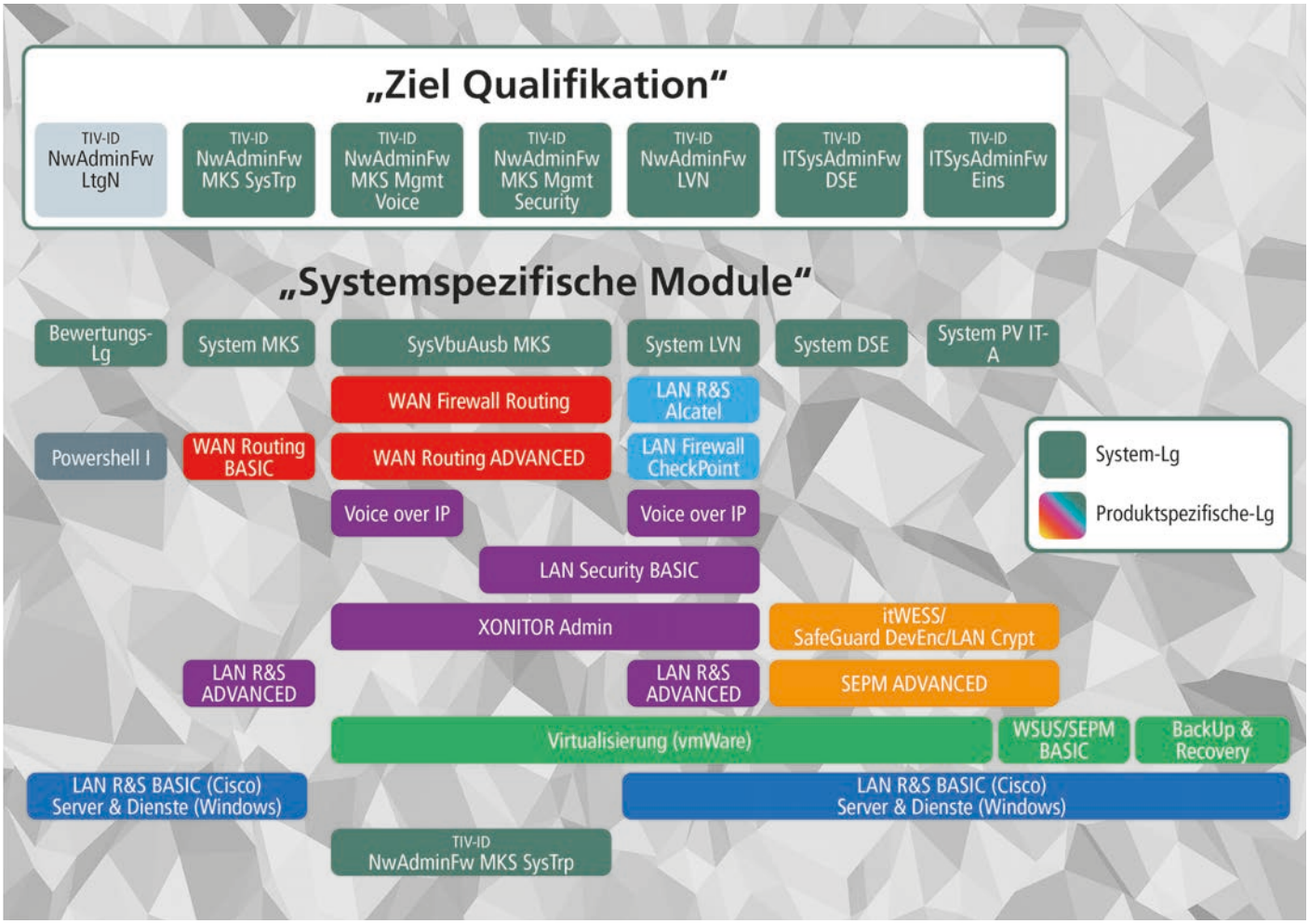
Wesentliche Chancen der Neuordnung

Bislang erfolgte die Einstellung der IT-Feldwebel bereits mit Zusage auf Dienstort und Dienstposten, aber ohne tatsächliche Kenntnis über das vorhandene Leistungsvermögen des Bewerbers beziehungsweise der Bewerberin. Durch die bisher übliche Trennung der Fachrichtungen Informationsverarbeitung und Informationsübertragung bestand zudem eine erhebliche Einschränkung in der Flexibilität hinsichtlich des zukünftigen Einsatzes des IT-Feldwebels. So eröffnet die Einführung eines gemeinsamen, einheitlichen Basis-Trainings für alle IT-Feldwebel unter anderem mehr Chancen in Bezug auf

- die Flexibilität bei sich ändernden Anforderungen der Bedarfsträger,
- die Fähigkeit, den schnellen Innovationszyklen in der Informationstechnik in Bezug auf die Abbildung in der Lehre besser Rechnung zu tragen,

Systemverbundausbildung – Abbild der Einsatzrealität in der Ausbildung.
(Foto: Bundeswehr / ITSBw)

Neue Ausbildungssystematik: produktspezifisch – flexibel – agil. (Grafik: Bundeswehr / ITSBw)



- eine Verkürzung der zeitlichen Abstände zwischen den militärfachlichen Ausbildungsanteilen,
- die Erhöhung der operativ nutzbaren Zeit für Einsätze,
- das Potential zu größerer Verwendungsbreite der Soldatinnen und Soldaten durch breitere Qualifizierung in kürzerer Zeit,
- die Steuerung auf Dienstposten nach individueller Fähigkeitsbewertung und
- die Gewährleistung größtmöglicher beruflicher Attraktivität bei höchstmöglicher Ausbildungsqualität.

Im Grundansatz rückt die Neuordnung der Ausbildung die Person gegenüber dem IT-System noch weiter in den Mittelpunkt der Betrachtung. Sie trägt nun noch mehr zur gezielten Qualifizierung des Bewerbers beziehungsweise der Bewerberin unter Berücksichtigung seiner beziehungsweise ihrer persönlichen Eignung bei.

Das Basis-Training IT-Feldwebel – Inhalte

Mit Einführung des Basis-Trainings erfolgt die Zusammenführung der Fachausbildung mit der Dienstpostenausbildung Teil 1 in einem Ausbildungsgang, der auch um zusätzliche Inhalte bedarfsgerecht erweitert wird. Damit wird der IT-Feldwebel zukünftig in seiner Grundqualifikation breiter aufgestellt sein. Auch der angestrebte „Multi-Role-Ansatz“ lässt sich leichter realisieren, da der Soldat beziehungsweise die Soldatin nun nicht mehr rein system-, sondern fähigkeitsbezogen ausgebildet wird und somit aufgrund der Reduzierung der Fachrichtungen qualifizierungsabhängig schneller dort eingesetzt werden kann, wo er tatsächlich gebraucht wird. Der so ausgebildete Feldwebel wird zum kompetenten „Erstansprechpartner IT“ auf dem Gefechtsfeld.

Das Training wird nach den Grundsätzen kompetenzorientierter Ausbildung durchgeführt und stellt somit das Handeln in den Mittelpunkt: Das exemplarische Handeln im Lernprozess entspricht den Tätigkeiten der militärischen Praxis. Das Training hat nach derzeitiger Planung einen Umfang von insgesamt 74 Ausbildungstagen. Das heißt, es besteht eine Zweiteilung in laufbahnrelevante und weitere Fachausbildung.

Im ersten Abschnitt wird mit inhaltlicher Schwerpunktsetzung auf Themengebiete der Informationsverarbeitung in den Lernfeldern „Betriebssystem“, „Netzwerktechnik“ und „Informationssicherheit“ innerhalb von circa 45 Ausbildungstagen die Voraussetzung für die Durchführung der Laufbahnprüfung als zwingende Bedingung für die Ernennung zum Feldwebel beziehungsweise Bootsmann geschaffen.

Im zweiten Abschnitt erfolgt die fachlich breite Qualifikation des zukünftigen IT-Feldwebels in den Lernfeldern „Groupware“, „IT-System der Bundeswehr“, „Grundlagen der Informations- und Kommunikationstechnik“ sowie Anteile der „Informationsübertragung“, „Führung und Einsatz“, „Logistik in der IT“ und dem Bereich „Gesetzliche Schutzaufgaben“.

In seiner Gesamtheit wird mit dem Basis-Training aktuell noch ein Abholpunkt für die weiteren Anteile der Dienstpostenausbildung Teil 2 erreicht. Vor dem Hintergrund der Ausbildungs- und Einsatzflexibilität sollen diese Anteile in eine modularisierte fähigkeitsbezogene und zivil zertifizierbare Ausbildung in der IT-Landschaft, die „Modulmatrix“, überführt werden. Zudem ist beabsichtigt, die Anteile der ortsunabhängigen Ausbildung beziehungsweise virtualisierten Ausbildung in diesem Lehrgang schrittweise zu erhöhen und einzelne Teile der Ausbildung auch auf Englisch, zum Beispiel durch den Austausch von Fachlehrern aus den USA, abzubilden.

Offizierausbildung praktisch – IT-Fachmann im scharfen Schuss.
(Foto: Bundeswehr / ITSBw)

Modularisierung der IT-Fachausbildung

In einem Workshop „Modulmatrix“ wurde im April 2019 erstmals eine zukünftige Variante der IT-Ausbildung an der Schule Informationstechnik der Bundeswehr thematisiert. Ziel war, die Ausbildung der IT-Fachkräfte in der Bundeswehr zu flexibilisieren und zukunftsorientiert zu gestalten.

Ausbildung heute / Grundidee der Modulmatrix

Die derzeit stattfindende Ausbildung ist stringent auf die vorhandenen IT-Systeme ausgerichtet. Das bedeutet, die vorhandenen Ausbildungsanlagen sowie die Ausbilder sind fest an ein System gebunden. Die Ausbildungsabschnitte unterschiedlicher Systeme ähneln sich jedoch in Teilen, wie zum Beispiel bei der Thematik Netzwerktechnik, Betriebssysteme, Virtualisierungsumgebungen sowie bei der verwendeten handelsüblichen Hardware. Dies birgt die Möglichkeit, die Ausbildung der angehenden IT-Spezialistinnen und -Spezialisten systemübergreifend weitgehend gemeinsam durchzuführen.

Grundidee und Ziel ist also, den Weg von den bisherigen monolithischen, festen Lehrgängen hin zu einem hochflexiblen modernen Ausbildungssystem zu gestalten, welches der heutigen Zielgruppe deutlich besser gerecht wird und hilft, den individuellen Lernerfolg zu optimieren. In der initialen Betrachtung stehen zunächst die Ausbildungen zum Netzwerk-Administrationsfeldwebel „Mobile Kommunikationssysteme Bundeswehr“, „Lokale Verlegefähige Netzwerke Bundeswehr“ sowie der IT System-Administrationsfeldwebel „Einsatz / Dezentrale Server-segmente Einsatz“ im Fokus.

Vorteile

Erste Synergieeffekte entstehen bereits bei der Ressourcennutzung, wie zum Beispiel bei der Auslastung der Hörsäle, der Ausbildungsanlagen sowie bei der zum Teil kostenintensiven Qualifizierung der Ausbilderinnen und Ausbilder. Auch werden die Lehrgangsteilnehmenden in ihrer Fachausbildung an die systemübergreifenden Terminologien herangeführt. Das soll die zukünftige Kommunikation zwischen den Administratorinnen und Administratoren der verschiedenen Systeme erleichtern.

Für die Truppe, den eigentlichen Bedarfsträger, ergeben sich ebenfalls Vorteile. Das Nichtbestehen eines Moduls führt nicht mehr zwangsweise zur Wiederholung ganzer Ausbildungsabschnitte, sondern nur zur Wiederholung des besagten Moduls.

Insgesamt wird die Ausbildungslandschaft dadurch deutlich flexibler. Bei verändertem Bedarf kann der IT-Feldwebel vergleichsweise schnell auf ein anderes IT-System qualifiziert werden, indem er ergänzend die für das neue System fehlenden Module absolviert. Dieser Vorteil ergibt sich auch bei der Ausbildung, bei Neubeschaffung und Regeneration von IT-Systemen oder der Einstellung von Seiteneinsteigern, die oftmals bereits über ein erhebliches Qualifkationsportfolio verfügen.

Veränderungen in der Offizierausbildung

Der Inspekteur des Heeres hat entschieden, die Ausbildung zum Offizier des Truppendienstes in der größten Teilstreitkraft der Bundeswehr, dem Heer, neu zu gestalten. Ab dem 1. Juli 2020 wird die Ausbildung der Offizieranwärterinnen und Offizieranwärter (OA) deutlich stärker auf die jeweiligen Truppengattungen der Landstreitkräfte zugeschnitten sein. So

will das Heer einen stärkeren Zusammenhalt im Heer insgesamt wie auch einen „Blick über den Tellerrand“ für alle seine Soldatinnen und Soldaten erreichen.

Diesem neuen Ausbildungskonzept des Heeres folgt der militärische Organisationsbereich Cyber- und Informationsraum (CIR) ausdrücklich, bietet es doch die Möglichkeit, allen OA des Heeres den Zugang in das Werdegangsmodell Cyber/IT zu eröffnen. Der militärische Organisationsbereich CIR wird die neue Ausbildungssystematik Heer grundsätzlich adaptieren, jedoch mit eigenen inhaltlichen Schwerpunkten versehen. Es wird eine ausgewogene Balance zwischen den Bedarfsträgerforderungen des Heeres und den Anforderungen an den Offizier im Organisationsbereich CIR erzielt. Durch die aktive Mitgestaltung der Ausbildung des Führernachwuchses erwächst die Chance, ein Stück berufliche Prägung zu erreichen und letztendlich auch das berufliche Selbstverständnis als Soldatin und IT-Spezialist zu entwickeln. Ausbildung wird damit einen wichtigen Beitrag zur Herausbildung einer eigenen „CIR-Identität“ leisten.

Beginnend mit dem neuen Offizieranwärterjahrgang 2020 hat der Organisationsbereich CIR dazu für den Bereich Kommando Informationstechnik der Bundeswehr festgelegt, dass die Grundausbildung in den IT-Bataillonen 281 in Gerolstein und 292 in Dillingen an der Donau durchgeführt wird. Danach folgt die Spezialgrundausbildung in den IT-Bataillonen 282 Kastellaun, 293 Murnau am Staffelsee, 381 Storkow und 383 Erfurt.

Im Anschluss, erstmalig ab Januar 2021, werden die Offizieranwärterinnen und Offizieranwärter an der Schule Informationstechnik der Bundeswehr den neu konzipierten Fahnenjunkerlehrgang mit Ablegen der entsprechenden Laufbahnprüfung absolvieren. Mit der Teilnahme an einem neuen Führungspraktikum, der Sprachausbildung und, je nach Studiengang, einem Grundpraktikum wird dieser Ausbildungsabschnitt abgeschlossen. An der Offizierschule des Heeres wird das neu konzipierte Modul Heeresprägung besucht, bevor die Versetzung an die Universitäten der Bundeswehr erfolgt.

Nach dem Studium wird dann an der Schule Informationstechnik der Bundeswehr mit der Teilnahme am Lehrgang für IT-Offiziere und dem überarbeiteten Lehrgang Zugführer (bisher Offizierlehrgang 3) die Offizierausbildung abgeschlossen.

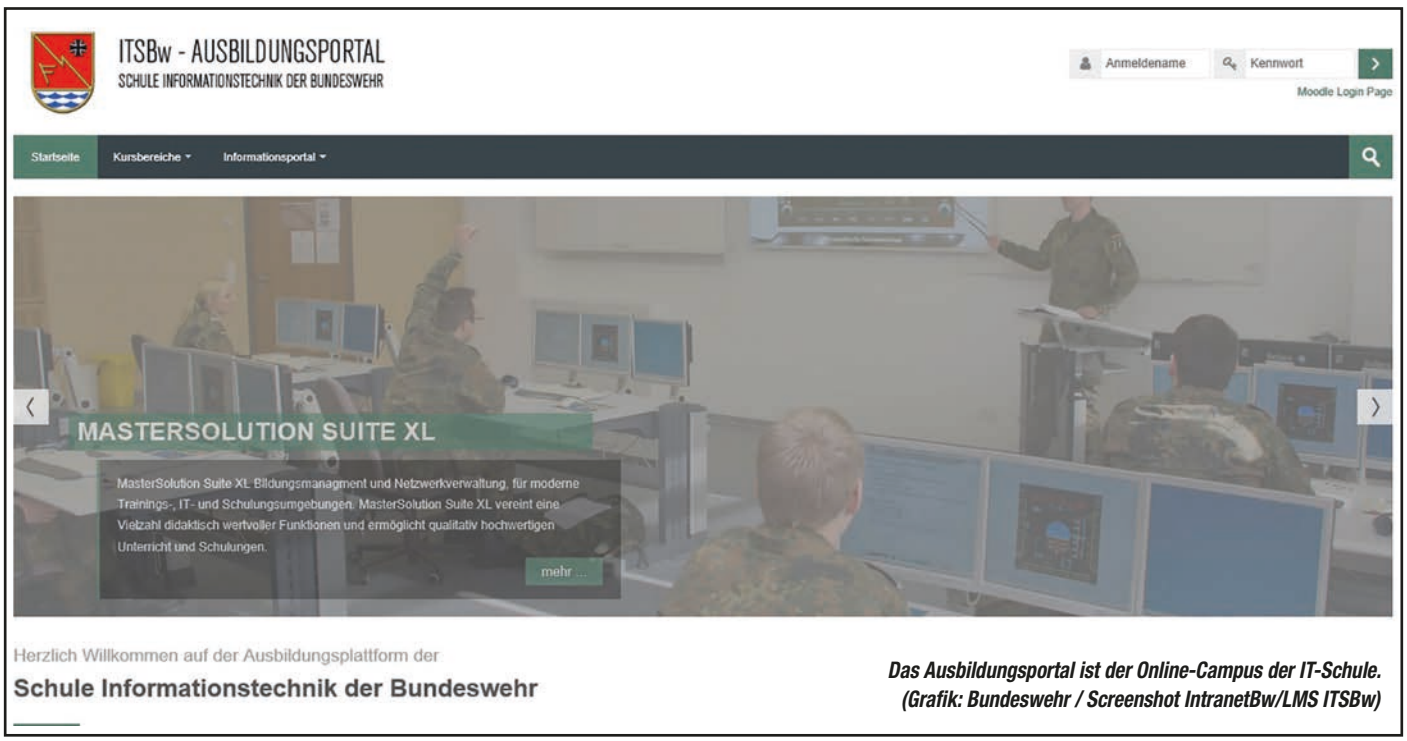
Mit den Offizieranwärterinnen und -anwärtern des Heeres wird eine neue, weiter modularisierte Ausbildungsfolge eingeführt. Aus Sicht des Organisationsbereichs CIR ist es langfristig das Ziel, auch die OA der anderen Teilstreitkräfte in dieses Ausbildungskonzept zu integrieren, um einen einheitlichen Ausbildungsstand aller IT-Offiziere der Bundeswehr zu gewährleisten.

Einsatz moderner Ausbildungstechnik

Wesentliche Grundlage für eine zukunftsfähige, effiziente und moderne Ausbildung ist eine moderne Ausbildungstechnik an der Schule Informationstechnik der Bundeswehr. Verschiedene Ausbildungseinrichtungen der Bundeswehr setzen bereits Lernmanagementsysteme ein. In enger Verbindung dazu steht die Bereitstellung von Lehr- und Lernmaterialien in einer Ausbildungsmediendatenbank. Beide Produkte wurden seit 2018 an der Schule Informationstechnik der Bundeswehr eingeführt. Die Erprobungsphase, in der die Durchführung verschiedener Lehrgänge getestet wurde, ist bereits erfolgreich abgeschlossen. 2020 schließt sich eine Konsolidierung und breite Ausfächerung der Lernmittelsysteme und -datenbanken an. Die so geschaffene, nutzerfreundliche und IT-gestützte Arbeitsumgebung ist wesentliche Voraussetzung für die weitere Einführung und Umsetzung der kompetenzorientierten Ausbildung sowie für die Realisierung virtueller Klassenzimmer und individueller Ausbildung „auf Distanz“.

Ausbildungsmediendatenbank

Das „Digital Asset Management System“ beinhaltet Lehr- und Lernunterlagen wie Präsentationen, Bilder, Grafiken, Audio- und Videodateien, verwaltet aber auch Lernprogramme und stellt diese bereit. Zusätzlich kann eine flexible und komplexe Volltextsuche genutzt werden. Primär ist die Ausbildungsmediendatenbank eine Webanwendung, die den Ausbildenden das Anlegen ihrer digitalen Portfolios erleichtert. Damit ist es möglich, digitale Inhalte, die in einem Training verwendet werden sollen, vor, während und nach der Ausbildung zur Verfügung zu stellen. Es ist nicht mehr notwendig, digitale Inhalte auf der lokalen Festplatte abzulegen. Auch externe Inhalte, beispielsweise Links zu Regelungen, können den Trainingsteilnehmenden gebündelt zur Verfügung gestellt werden.



Das Ausbildungsportal ist der Online-Campus der IT-Schule. (Grafik: Bundeswehr / Screenshot IntranetBw/LMS ITSBw)

Jeder Trainingsteilnehmende hat in vollem Umfang Zugriff auf Inhalte zu Ausbildungsthemen an einer zentralen Stelle. Alle digitalen Inhalte werden durch eine interne Funktion qualitätsgesichert bereitgestellt. Somit stehen alle Daten dem Nutzenden immer in aktueller Form zur Verfügung. Wird ein eingestellter Inhalt aktualisiert, ist diese Änderung sofort für die Nutzerin oder den Nutzer verfügbar. Ausbildende und Trainingsteilnehmende haben beispielsweise über die „integrierte Technologiegestützte Ausbildungsplattform der Bundeswehr“ (iTAPBw) oder den Intranet-Auftritt der Schule Informationstechnik der Bundeswehr verschiedene Zugriffsmöglichkeiten auf die Ausbildungsmediendatenbank. Der Login kann auch von außen erfolgen.

Durch die Registrierung und das Login auf der Webseite gibt es auch die Möglichkeit, aus allen Inhalten eigene Sammlungen zu speziellen Ausbildungsthemen zusammenzustellen.

Lernmanagementsystem

Für das Lermanagementsystem (LMS) wird die Software Moodle genutzt. Dieses LMS ist ein Kursmanagementsystem auf Open-Source-Basis. Die Software bietet umfangreiche Möglichkeiten zur Unterstützung kooperativer Lehr- und Lernmethoden. So können in virtuellen Kursräumen Arbeitsmaterialien wie Texte, Präsentationen, Links, Dateien und weiteres bereitgestellt werden. Verschiedenste Lernaktivitäten, wie zum Beispiel Foren, Aufgaben, Chat, Wiki, Tests/Prüfungen können durchgeführt werden. Die Ausbilder haben auch die Möglichkeit, den Lernfortschritt der Trainingsteilnehmenden zu überwachen. Auch hier haben alle Beteiligten zum Beispiel über die iTAPBw oder den Intranet-Auftritt der Schule Informationstechnik der Bundeswehr verschiedene Zugriffsmöglichkeiten auf das LMS. Der Login von außen ist auch hier möglich.

Das Lernmanagementsystem und die Ausbildungsmediendatenbank sind technisch miteinander verbunden. Bei der Bereitstellung der digitalen Lehr- und Lernunterlagen greift das Lernmanagementsystem auf die Ausbildungsmediendatenbank zu.

Außerdem haben auch ehemalige Trainingsteilnehmende so stets Zugriff auf aktuelle Ausbildungsdokumente über das IntranetBw. Die herkömmliche „Lehrgangs-CD“ kann damit entfallen.

Ausblick

Perspektivisch gilt es auch an der IT-Schule den Entwicklungen in der Bundeswehr, aber ganz besonders auch den Möglichkeiten im Zeitalter der Digitalisierung Rechnung zu tragen, und sowohl in der Lehre, der Methodik als auch der Ausbildungstechnologie und in den Strukturen zukunftsfähig zu sein. Stichworte wie Wissensgesellschaft, lebenslanges Lernen spielen bei den Überlegungen für eine mögliche Zukunftsentwicklung ebenso eine Rolle, wie die Notwendigkeit zur Intensivierung der Aus-, Fort und Weiterbildung über alle Aspekte des Cyber-/Informationsraums. Dies kann und muss sicherlich alle Laufbahnen und Dienstgrade, zivil und militärisch, umfassen und berücksichtigen können. Aufklären, Wirken und Handeln im CIR werden - das zeigen bereits heute die aktuellen Einsätze, aber auch die Entwicklungen weltweit - eine zentrale Rolle einnehmen. Das Wissen und die Kenntnisse über Zusammenhänge und Abhängigkeiten sowie Verfahren und Prozesse müssen gelernt und gelehrt werden. Wir sehen das perspektivisch als eine der kommenden, zentralen Aufgaben der IT-Schule.

Die oben vorgestellten neuen Ausbildungsgänge und die Nutzung moderner Ausbildungstechnik in Verbindung mit der Einführung kompetenzorientierter Ausbildung sind nur Beispiele für Handlungsfelder die es zu gestalten gilt, um als zentrale Ausbildungseinrichtung für Informationstechnik in der Bundeswehr gut gerüstet in die Zukunft zu gehen. Wir werden weiter an einem, den Ausbildungserfolg förderlichen Lernumfeld arbeiten, sei es mit veränderter Organisation, wie es unter anderem auch die NATO mit der NCI Academy vorlebt, und unter weiter intensivierter Nutzung moderner Ausbildungstechniken sowie der Schaffung leistungsstarker und bedarfsgerecht konfigurierter Wissens- und Lernmanagementsysteme. Künftig wird hierzu eines der modernsten Lehrsaalgebäude der Bundeswehr zur Verfügung stehen, um attraktive Ausbildung in einer hochwertigen und modernen Infrastruktur anbieten zu können. Ab Mitte 2020 werden Lehrgänge auf über 11.000 Quadratmeter Nutzungsfläche durchgeführt. Die unmittelbare Nähe zum netzwerktechnisch voll erschlossenen Standortübungsplatz ermöglicht darüber hinaus die optimale Balance zwischen theroretischer Ausbildung und dem praktischen Anwenden des Erlernten in einsatznahen Szenaren und Lagebildern.

Internationale Kooperation mit verschiedenen Partnerschulen ausländischer Streitkräfte, zivile Zertifizierbarkeit von Ausbildungen und Kooperationen mit nationalen Ausbildungseinrichtungen, Behörden und Industrieunternehmen sind zusätzliche Aktivitäten, die die IT-Ausbildung an der Schule Informationstechnik der Bundeswehr attraktiv und zukunftsfähig gestalten. Ganz nach dem Leitbild der Schule: „Wir bilden selbständig handlungsfähige Soldatinnen und Soldaten als IT-Spezialisten aus, die im Einsatz und Friedensdienst bestehen können. “Engagement und kreatives Denken in der Ausplanung solcher Visionen sind gut investiert und werden sicherlich zu einem Mehrwert für Bundeswehr führen.

wt

Neues Lehrsaal- und Bürogebäude der IT-Schule.
(Foto: Bundeswehr / ITSBw)

Technischer Regierungsdirektor Thomas Chladek und Oberstleutnant Peter Leffler

Nationale und internationale Zusammenarbeit im Cyber- und Informationsraum

Bereits im zweiten Jahr seines Bestehens war das Kommando CIR Gastgeber des multinationalen Cyber Commanders Forum und des International Cyber Operations Symposium in Bonn. (Foto: Bundeswehr / Martina Pump)

Der Cyber- und Informationsraum als Dimension kennt weder institutionelle noch politische Grenzen. Erfolgreiches Handeln innerhalb dieser Dimension ist nur gesamtstaatlich und grenzüberschreitend denkbar. Dieser Ansatz wird im Kommando Cyber- und Informationsraum der Bundeswehr seit seiner Aufstellung verfolgt und auch in der nationalen und internationalen Zusammenarbeit des Kommandos abgebildet.

Einleitung

In der aktuellen Cybersicherheitsstrategie für Deutschland aus dem Jahr 2016 sind den verschiedenen Ressorts der Bundesrepublik Deutschland unterschiedliche Aufgaben zugewiesen. Dem Verteidigungsressort kommt in diesem Kontext die Aufgabe der Cyber-Verteidigung zu. In Abgrenzung dazu verantwortet das Bundesministerium des Inneren die Cyber-Abwehr und das Auswärtige Amt die Cyber-Außenpolitik. Die Cybersicherheitsstrategie für Deutschland beschreibt den Bereich Cyber als Domäne ohne exakt greifbare politische oder institutionelle Grenzen. Damit sind Zuständigkeiten im Detail nicht immer eindeutig. Die nationale Sicherheitsvorsorge Deutschlands kann in diesem Bereich nur ressortübergreifend und gesamtstaatlich gedacht und muss darüber hinaus auch bi- und multinational umgesetzt werden.

Im Weißbuch 2016 wurde dieser gesamtstaatliche Ansatz aufgegriffen und die Notwendigkeit der Bündelung aller im Cyber- und Informationsraum agierenden Kräfte der Bundeswehr „unter einem Dach“ beschrieben. Diese Bündelung wurde mit der Bildung der Abteilung Cyber- und Informationstechnik im Bundesministerium für Verteidigung noch im Jahr 2016 und der Aufstellung des Organisationsbereichs Cyber- und Informationsraum der Bundeswehr im April 2017 auch strukturell umgesetzt. Die Bundeswehr verfügt seitdem über nunmehr sechs Teilstreitkräfte bzw. militärische Organisationsbereiche (Cyber- und Informationsraum, Heer, Luftwaffe, Marine, Sanitätsdienst, Streitkräftebasis).

Auch innerhalb des Kommandos Cyber- und Informationsraum wurde mit dem Referat Nationale und Internationale Zusammenarbeit, als direkt dem Chef des Stabes unterstelltes Organisationselement, der gesamtstaatliche und multinationale Ansatz strukturell hinterlegt.

Dort wird die nationale und internationale Zusammenarbeit des Organisationsbereichs Cyber- und Informationsraum koordiniert, sowie ministerielle Vorgaben und Schwerpunkte umgesetzt. Im Einzelnen bedeutet das unter anderem die Auseinandersetzung mit den Strategien im Cyber- und Informationsraum der verbündeten Nationen und relevanten internationalen Institutionen, einschließlich des multinationalen Austauschs. Ein regelmäßiges Format des multinationalen Austauschs ist das Cyber Commanders Forum. Hier treffen sich zweimal im Jahr die Kommandeure der Cyber-Streitkräfte von über 40 Nationen inner- und außerhalb Europas. Bereits im zweiten Jahr nach seiner Aufstellung durfte der Inspekteur Cyber- und Informationsraum den Vorsitz übernehmen und als Gastgeber dieser bedeutenden internationalen Veranstaltung auftreten.

Aus nationaler Sicht ist die Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik und anderen Bundesbehörden für den Organisationsbereich Cyber- und Informationsraum ebenso wichtig wie die Kooperation mit Industrieverbänden und Bildungseinrichtungen. Alle genannten Akteure sind wichtige Teile einer gesamtstaatlichen Sicherheitsvorsorge.

Wir erwarten von der Zusammenarbeit mit unseren internationalen und nationalen Partnern auch einen Austausch darüber, wie den gegenwärtigen Herausforderungen im Cyber- und Informationsraum begegnet werden könnte.

Diese sind unter anderem dadurch gekennzeichnet, dass Bedrohungen im Cyber- und Informationsraum permanent bestehen und sich im „Network Speed“ auswirken können. Anders als in den anderen Dimensionen (Luft, See, Land, Weltraum) existieren also kaum Vorwarnzeiten und die Kräfte des Cyber- und Informationsraums sind dadurch folglich immer im Einsatz. Das aus Sicht eines potentiellen Gegners unter Umständen günstige Kosten-Nutzen-Verhältnis für Angriffe im Cyber- und Informationsraum und die sich ändernde Bedeutung von politischen und institutionellen Grenzen wurde an anderer Stelle bereits

Der Inspekteur CIR, Generalleutnant Ludwig Leinhos, eröffnet in Berlin die erste gemeinsame Arbeitstagung mit dem Bitkom e.V. (Foto: Bundeswehr / Sebastian Wanninger)

Gruppenarbeit im Cyber Innovation Hub der Bundeswehr. (Foto: Bundeswehr / Sebastian Wanninger)

beschrieben. Kräfteverhältnisse zwischen Angreifer und Verteidiger, welche in klassischen Bedrohungsszenarien eine Rolle spielen, sind im Cyber- und Informationsraum deshalb nahezu bedeutungslos.

Mit dem deutschen Ansatz, alle für den Cyber- und Informationsraum relevanten Kräfte in einem Organisationsbereich zusammenzufassen, wurde bereits eine bei befreundeten Streitkräften weitläufig anerkannte Antwort auf diese Herausforderungen gefunden.

Darüber hinaus erfordert dieses andere Bedrohungsszenario im Cyber- und Informationsraum eine Anpassung von Prozessen sowie von Organisationsstrukturen und eine Neugestaltung des Arbeitsumfelds im Organisationsbereich Cyber- und Informationsraum.

Hinsichtlich der Prozesse kommt es vor allem darauf an, diese schlank und effizient zu gestalten, um den oben genannten Herausforderungen zu begegnen. Die Umsetzung der Scrum-Methode als agile Managementmethode bei Prozessen im Projekt- und Produktmanagement war bisher weniger im militärischen Kontext angesiedelt. Hier konnte viel von nationalen Partnern aus Industrie und Wissenschaft gelernt werden. Weitere Beispiele für diesen fruchtbaren zivil-militärischen Erfahrungs- und Wissensaustausch ist die gemeinsame Beantwortung der Fragestellung, wie Künstliche Intelligenz bzw. Machine Learning den militärischen Führungsprozess unterstützen können.

Diese Anpassung von Prozessen bedingt auch eine entsprechende Entwicklung eigener Organisationstrukturen. Bei der Umsetzung kollaborativer Stabsarbeit zur Vermeidung sequentiellen Arbeitens konnte ebenfalls sehr viel von den Erfahrungen nationaler und internationaler Partner gelernt werden.

Die Steigerung der Attraktivität des Arbeitsumfelds ist Voraussetzung dafür, Spitzenpersonal gewinnen und binden zu können. Hier sieht sich der Organisationsbereich Cyber- und Informationsraum nicht nur als Konkurrent zu anderen Akteuren, vielmehr ist beabsichtigt, gemeinsam Lösungswege zu finden, wie die Mangelressource „Fachpersonal“ optimal angesprochen werden kann. Mit dem Konzept der Cyber-Reserve ist es hier gelungen, Expertise aus Industrie, Wissenschaft und anderen Behörden nutzbar zu machen und im Gegenzug die eigenen Besonderheiten und die Bedürfnisse eines militärischen Organisationsbereichs in das zivile Umfeld zu transportieren (siehe hierzu den Artikel auf Seite 48).

Sowohl die tiefgreifende Kooperation mit dem Königreich der Niederlande, welche sich über das gesamte Spektrum des Cyber- und Informationsraums erstreckt, als auch die intensive Zusammenarbeit mit dem Digitalverband Bitkom e.V. sind zwei Beispiele, die aufzeigen, wie nationale und internationale Kooperationen angebahnt, ausgebaut und strukturiert werden können. Im Folgenden soll anhand dieser beiden, für den Organisationsbereich Cyber- und Informationsraum Mehrwert bringenden, Beispiele die nationale und internationale Zusammenarbeit vorgestellt werden.

Kooperationen mit weiteren nationalen Partnern, wie zum Beispiel der Telekom-Security, dem Fraunhoferinstitut FKIE, innerhalb des Cyber Security Clusters Bonn, aber auch mit befreundeten Nationen aus der Europäischen Union, der NATO und darüber hinaus runden das Bild eines erfolgreichen vernetzen und gesamtstaatlichen Handelns ab.

Beispiel 1 – Nationale Kooperation mit dem Digitalverband Bitkom e.V.

Der Weg zur Kooperation

Unter dem Dach des Bitkom e.V. sind ca. 2.700 Unternehmen der digitalen Wirtschaft organisiert. Darunter sind gut 1.000 Mittelständler, über 500 Startups und nahezu alle deutschen Global Player der Branche vertreten. Der Bitkom e.V. ist damit einer der wichtigsten Ansprechpartner für Cyber-/IT-Themen, Digitalisierung und Zukunft in Deutschland und ein idealer Kooperationspartner, um die Digitalisierung in den Streitkräften, deren Auswirkungen auf die Bundeswehr und letztlich auf die Bundesrepublik verstehen und vorantreiben zu können.

Nicht einmal ein Jahr nach Aufstellung des Kommandos Cyber- und Informationsraum wurde das erste Konzept zur Kooperation mit dem Bitkom e.V. erstellt und durch den Inspekteur Cyber- und Informationsraum gebilligt.

Mit der Unterzeichnung der Kooperationsvereinbarung zwischen Kommando Cyber- und Informationsraum und dem Bitkom e.V. im April 2019 wurden Ziele sowie gemeinsame Arbeits- und Interessensfelder abgesteckt. Bereits wenige Wochen später konnte eine erste gemeinsame Arbeitstagung mit großem Erfolg durchgeführt werden.

Ziel der Kooperation

Ziel der Kooperation ist es, in einen regelmäßigen Dialog mit der Wirtschaft zu treten, um der Dynamik der technologischen Entwicklung

mit Blick auf die Fähigkeitsentwicklung und Fähigkeitsweiterentwicklung im Cyber- und Informationsraum in der Bundeswehr Rechnung zu tragen. Hierzu soll die verstärkte und strukturierte Zusammenarbeit zwischen dem Bitkom e.V. und dem Kommando Cyber- und Informationsraum im gegenseitigen Interesse vorangetrieben werden. Dies umfasst konzeptionelle, informationstechnische sowie IT-architekturtechnische Themen wie auch Fragestellungen von Personalgewinnung und Personalqualifikation.

Strukturierung der Zusammenarbeit

Die Zusammenarbeit zwischen Kommando Cyber- und Informationsraum und dem Bitkom e.V. erfolgt in drei Arbeitsgruppen unter paritätischer Leitung durch jeweils einen Abteilungsleiter aus dem Kommando Cyber- und Informationsraum und einem Vertreter der Wirtschaft.

- Arbeitsgruppe 1 - Zusammenarbeitspotenziale unter besonderer Beachtung von Compliance
- Arbeitsgruppe 2 - Digitale Souveränität im Cyberraum
- Arbeitsgruppe 3 - Aufklärung in hybriden Szenarien.

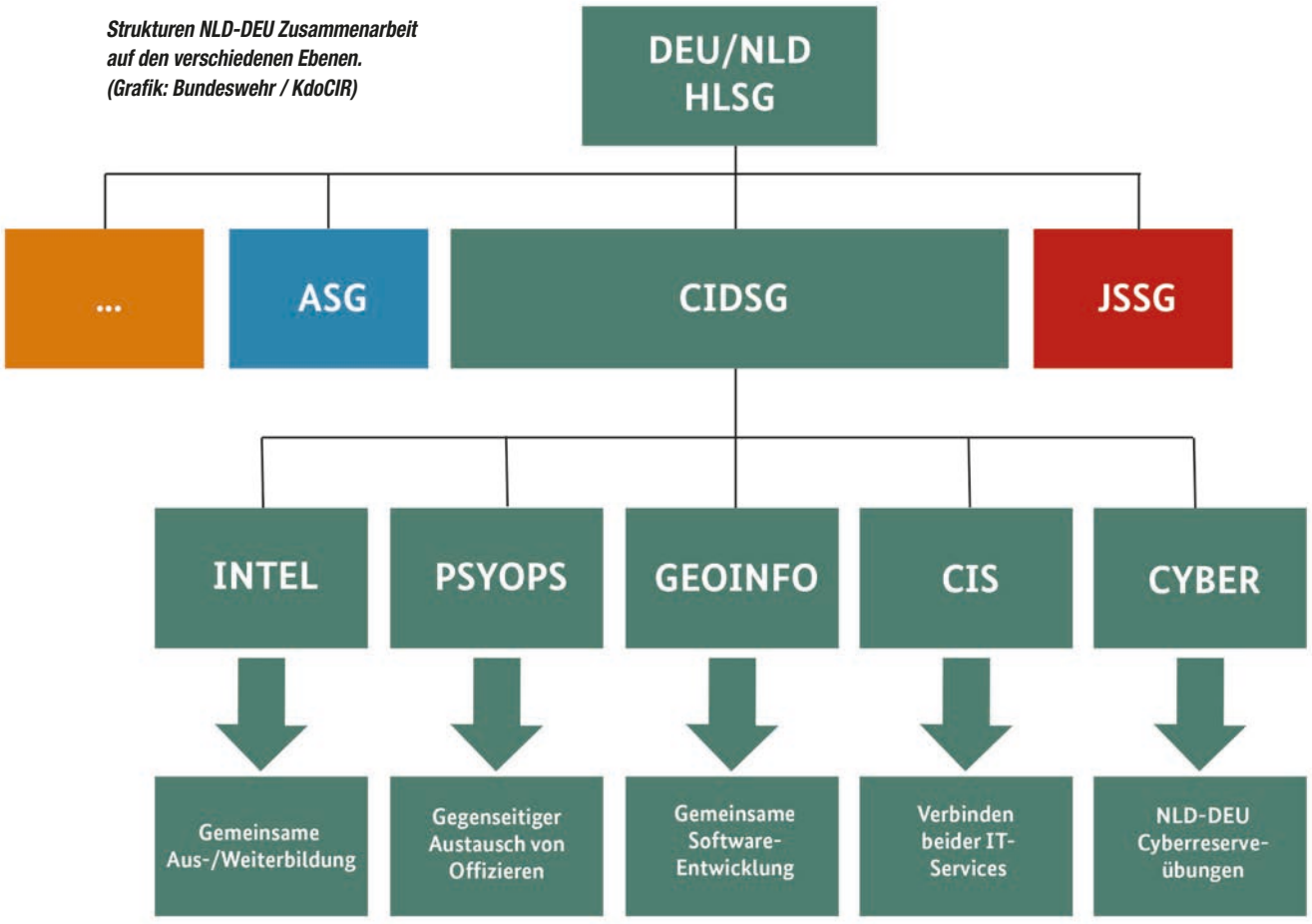
Mit Blick auf die zukünftigen Herausforderungen zur Gewinnung und Qualifizierung von Personal im Cyber- und Informationsraum verfolgt die Arbeitsgruppe 1 das Ziel, die Möglichkeiten zur Personalgewinnung, sowie Aus- und Weiterbildung zu erweitern. Hierzu werden verschiedene Gedankenmodelle untersucht, die von der kurzfristigen Einzelabstellung von Personal bis hin zu speziellen Zertifizierungsformen für Mitarbeitende und Expertinnen und Experten im Cyber- und Informationsraum reichen. Zudem ist geplant, eine gemeinsame Austauschplattform zur Zusammenarbeit auf Grundlage der bestehenden Cyber-Community Plattform zu schaffen (https://bundeswehr.community). Mittels einer derartigen Kollaborationsplattform sind unterschiedliche Zusammenarbeitsformen denkbar. So könnten beispielsweise gemeinsame Arbeitsgruppen zu spezifischen Themen in Themenportalen mit klarer Zielsetzung und zum gemeinsamen Nutzen entstehen. Denkbar ist sogar, auf dieser technologischen Grundlage einen gemeinsamen Arbeitsmarkt für Cyber-Kräfte zu etablieren.

Die Arbeitsgruppe 2 beschäftigt sich mit dem weiten Thema der digitalen Souveränität im Cyber- und Informationsraum, wobei eine abschließende Definition bislang fehlt.

„Bis zum Ende des Jahrzehnts werden weltweit voraussichtlich 50 Milliarden Menschen, Dinge, Bauteile und Prozesse über das Internet miteinander verknüpft sein. Die Vernetzung ermöglicht dabei enorme Effizienzsteigerungen mit einem Wertschöpfungspotential von etwa 700 Milliarden Euro allein für die Wirtschaft in Deutschland. Wirtschaftliche Erfolgsgeschichten lassen sich im 21. Jahrhundert nur mit proaktiven Digitalisierungsstrategien schreiben“, so der Bitkom e.V. in einem Positionspapier zum Thema Digitale Souveränität. Darin heißt es ganz konkret: „Wir verstehen unter Digitale Souveränität die Fähigkeit zur Selbstbestimmung im digitalen Raum – im Sinne eigenständiger und unabhängiger Handlungsfähigkeit. In diesem Sinne müssen ein digital souveränes Deutschland und Europa bei digitalen Schlüsseltechnologien, entsprechenden Diensten und Plattformen über eigene Fähigkeiten auf internationalem Spitzenniveau verfügen. Nicht zuletzt müssen ein digital souveränes Deutschland und Europa in der Lage sein, ihre Funktionen im Inneren zu sichern und ihre Integrität nach außen zu schützen.“

Digitale Souveränität ist untrennbar mit der Fragestellung: „Wo ist Schlüsseltechnologie notwendig?“ verbunden. Schlüsseltechnologien sind nach Bitkom e.V. Technologien und Kompetenzen:

Strukturen NLD-DEU Zusammenarbeit auf den verschiedenen Ebenen. (Grafik: Bundeswehr / KdoCIR)



HLSG – High Level Steering Group / CIDSG – Cyber Information Domain Steering Group / ASG – Army Steering Group / JSSG – Joint Support Steering Group

- Der Entwicklungs- und Produktionskompetenzen rund um IT-, Netzwerk- und Plattformsicherheit und
- Der Kompetenzen, digitale Technologien, Lösungen und Plattformen zu verstehen, zu prüfen, verantwortungsvoll einzusetzen und im Bedarfsfall so weitgehend zu veredeln und zu härten, dass sie den jeweils angestrebten Sicherheitsanforderungen entsprechen.

Die Arbeitsgruppe soll in diesem weiten und durchaus sehr theoretischen Feld der Digitalen Souveränität zunächst eine Roadmap „Souveränität im Cyber- und Informationsraum“ auf Basis einer klaren Definition von „Digitaler Souveränität“ entwickeln. In einem weiteren Schritt soll sie gemeinsam inhaltlich bestückt werden, um im Sinne eines Lagebildes erkennen zu können, wo möglicherweise Lücken bei Schlüsseltechnologien im Cyber- und Informationsraum in Deutschland vorhanden sind.

Die Arbeitsgruppe 3 „Aufklärung in hybriden Szenarien“ arbeitet vor dem Hintergrund der Bedrohung durch hybride Vorgehensweisen am gemeinsamen Verständnis zum Thema und darüber hinaus an den Möglichkeiten, diesen angemessen zu begegnen. Hybride Vorgehensweisen zielen auf die Destabilisierung von Staaten ab und nehmen dafür Wirtschaft, Gesellschaft und Militär gleichermaßen in den Fokus. Um dieser Herausforderung gesamtstaatlich wirksam zu begegnen, ist ein verlässliches gemeinsames Lagebild unerlässlich. Das Kommando CIR leistet hierzu seinen Beitrag (siehe Beitrag GLZ, Seite 12) und hat sich zum Ziel gesetzt, die Weiterentwicklung des Lagebilds Cyber- und Informationsraum voranzutreiben. Dadurch soll ein wesentlicher Beitrag zum gesamtstaatlichen Lagebild geliefert werden. In der Arbeitsgruppe ist dazu als erster Schritt die Schaffung einer gemeinsamen Plattform nebst gemeinsamer Gremienstruktur zum Informations-/ Erfahrungsaustausch angedacht. In einem weiteren Schritt sollen Ergebnisse im Bereich Forschung und Entwicklung im Kontext der Aufklärung in hybriden Szenarien ausgetauscht werden. Abgerundet wird die Arbeitsgruppenarbeit mit einer jährlich stattfindenden gemeinsamen Arbeitstagung, in welcher Ergebnisse in einem größeren Rahmen und unter Einladung von weiteren Vertretern der Bundeswehr, aus Politik und Wirtschaft präsentiert und diskutiert werden.

Beispiel 2 – Internationale Kooperation mit den Niederlanden

Die Zusammenarbeit mit dem Königreich der Niederlande findet im Wesentlichen im Rahmen der bilateralen „Cyber and Information Domain Steering Group“ statt und erstreckt sich über das gesamte Spektrum des Cyber- und Informationsraums. Mit der Bildung dieser Steering Group sind die Strukturen geschaffen, um die umfangreichen Aufträge aus der im Mai 2019 durch beide Verteidigungsministerinnen gezeichneten „Joint Declaration of Intent on the further Enhancement of bilateral Relations“ umzusetzen.

Damit ist die „Cyber and Information Domain Steering Group“ im Zusammenspiel mit den entsprechenden Steering Groups anderer militärischer Organisationsbereiche ein wichtiger Bestandteil der militärischen Kooperation beider europäischer Nachbarstaaten.

Als Beispiel für bereits erzielte Mehrwerte ist hierbei neben dem dauerhaften Personalaustausch in Form von Verbindungs- und Austauschoffizieren die umfangreiche Umsetzung gemeinsamer Ausbildungsvorhaben und Übungen zu nennen. So nimmt im Rahmen der akademischen Ausbildung beispielsweise seit Oktober 2019 als erster ausländischer Teilnehmer ein niederländischer Offizier am vierjährigen Masterstudiengang „Cyber Security“ der Universität der Bundeswehr München teil. Die Teilnahme von Angehörigen der Streitkräfte an Ausbildungsangeboten der jeweils anderen Nation, zum Beispiel in den Bereichen Operative Kommunikation oder Cybersecurity, runden diese Ausbildungskooperation ab.

Ein weiterer Aspekt dieser bilateralen Zusammenarbeit ist das Einrichten einer verschlüsselten Verbindung zwischen den niederländischen und deutschen IT- Systemen. Hierbei ist es gelungen, in einem ersten Schritt, die beiden Emailservices der Streitkräfte zu koppeln. Weitere Meilensteine in diesem Kooperationsprojekt sind die Schaffung einer gemeinsamen dokumentenbasierten Kollaborationsplattform für zwei Nutzergruppen mit insgesamt bis zu 2.000 Teilnehmern zum dritten Quartal 2020 und eine Integration dieser bilateralen Kollaborationsplattform in ein multinationales Extranet ab dem Jahr 2021.

Im Geoinformationswesen ist die niederländisch-deutsche Kooperation Takt- und Ideengeber im Rahmen entsprechender NATO Working Groups. Das Entwickeln und Testen von Softwarelösungen im Bereich der Ozeanographie und das Erstellen von Länderinformationen, beispielsweise in Form von Country Books, sind weitere Mehrwerte der niederländisch-deutschen Zusammenarbeit im Geoinformationswesen.

Beispielgebend für eine Cybersicherheitsvorsorge über nationale Grenzen hinweg, unter Einbindung von Experten aus Wissenschaft und Industrie beider Nationen, ist das gemeinsame Üben niederländischer und deutscher Cyberreservisten bei bilateralen Cyberreserveübungen. Niederländische Cyber-Reservisten sind außerdem fester Bestandteil der NATO-Übung CYBER COALITION.

Ausdruck der engen Zusammenarbeit mit den Niederlanden ist auch die Teilnahme eines niederländischen Offiziers am Masterstudiengang Cybersecurity an der Universität der Bundeswehr. (Foto: Bundeswehr / Martina Pump)

Zusammenfassung

In der Dimension Cyber- und Informationsraum existieren weder politische noch institutionelle Grenzen. Um seine in der Cybersicherheitsstrategie für Deutschland zugewiesene Aufgabe der Cyberverteidigung erfüllen zu können, muss der militärische Organisationsbereich Cyber- und Informationsraum gesamtstaatlich und grenzüberschreitend handeln. Die genannten Beispiele der Zusammenarbeit mit dem Digitalverband Bitkom e.V. und dem Königreich der Niederlande zeigen konkrete Erfolge auf diesem Weg.

wt

***Technischer Regierungsdirektor Thomas Chladek** und **Oberstleutnant Peter Leffler**,*
beide Referat Nationale Zusammenarbeit im KdoCIR.

Referat Einsatzplanung im Kommando CIR

VJTF 2023: Der Beitrag CIR zur Landes- und Bündnisverteidigung

Die Digitalisierung revolutioniert Informationsbeziehungen und Handlungsoptionen von Streitkräften. Dabei ist die Informationstechnik Mittel zur Erlangung der eigenen Führungsfähigkeit und Überlegenheit – aber auch Angriffspunkt und mögliche Schwachstelle. Eine Vielzahl von unterschiedlichen Kommunikationssystemen ist erforderlich, um die verschiedenen militärischen Anforderungen, insbesondere an die Führungsfähigkeit, durch die Bereitstellung der IT-Services zu erfüllen. Im Bereich Aufklärung und Wirkung im Einsatz sind CIR-Kräfte ein „scharfes Schwert" in den Händen der Streitkräfte. Landes- und Bündnisverteidigung ist ohne die Fähigkeiten des Organisationsbereichs Cyber- und Informationsraum (CIR) undenkbar geworden.

Landes- und Bündnisverteidigung in Zeiten der Digitalisierung

Deutschland bietet aufgrund seiner offenen, pluralistischen und international vernetzten, auf Freiheit, Rechtstaatlichkeit und Demokratie gründenden Gesellschaftsordnung zahlreiche Verwundbarkeiten durch hybride Bedrohungen. Jeder Aspekt des politischen, gesellschaftlichen, geistig-kulturellen und wirtschaftlichen Lebens kann nicht zuletzt aufgrund der anhaltenden digitalen Transformation aller Lebensbereiche zur Angriffsfläche werden. Die Bundeswehr leistet mit ihrem breiten Fähigkeitsspektrum einen verfassungsrechtlich klar umgrenzten Beitrag zum Umgang mit diesen Bedrohungen. Dies gilt umso mehr bei feindlicher hybrider Kriegsführung, die sich wesentlich auf die Sicherheit unseres Staates und auf das Bündnis auswirken kann, ohne dass ein einziger Schuss gefallen sein muss. Daraus ergeben sich für die Bundeswehr aber auch beträchtliche Herausforderungen für die eigene Landes- und Bündnisverteidigung (LV/BV).

Man stelle sich folgendes Szenar vor: Streitkräfte eines Landes setzen eine Aufklärungsdrohne ein, um gegnerische Artilleriestellungen aufzuklären. Gleichzeitig erstellen Soldaten in einer dieser Artilleriestellungen „Gruppenbilder" und stellen diese für die Angehörigen zuhause in ein soziales Netzwerk ein. Die Drohne entdeckt ein Luftabwehrsystem in diesem Stellungsraum und übermittelt die Koordinaten an die eigene Operationszentrale. Diese entscheidet, eine Bodenrakete auf das Ziel abzufeuern. Doch der Gegner ist vorbereitet - er manipuliert den Datenverkehr der Drohne, die Rakete wird mit falschen Koordinaten gefüttert und explodiert über einer unbewohnten Gegend. Zeitgleich werden Bilder von Soldaten in ihrer Artilleriestellung im Sozialen Netzwerk identifiziert und deren ebenfalls in den Bilddateien hinterlegte GPS-Daten ausgewertet. Unmittelbar danach werden diese Opfer eines Artilleriebeschusses aus über 40km Entfernung.

Die Digitalisierung im Militärischen schreitet weiter voran und verändert fast alle Prozesse - auch auf dem Gefechtsfeld. Sie stellt sich als eine tiefgreifende und unumkehrbare Entwicklung dar. Informationstechnik ist hierbei eine fest implementierte Größe, die auf vielen Ebenen militärischer Organisationsbereiche und Teilstreitkräfte nicht mehr wegzudenken ist. Die Einstiegsbarriere für Cyber-Angriffe ist zudem gering und kann unter Einsatz entsprechender Hardware und einem Internetzugang von jedem Punkt der Erde durchgeführt werden.

Die Bundeswehr wurde nach der Auflösung des Warschauer Pakts aufgrund politischer Entscheidungen von der Aufgabe der Landes- und Bündnisverteidigung hin zur Einsatzarmee für internationale Einsätze im Rahmen von multinationalen Stabilisierungsoperationen von NATO und Vereinten Nationen ausgerichtet. Nach dem Gipfel in Wales 2014 rückte für die NATO die Bündnisverteidigung wieder in den Vordergrund. Diese Entscheidung wurde bezüglich der Einsatzszenare im Rahmen der LV/BV für die Bundeswehr im Weißbuch 2016 umgesetzt. Die Bundeswehr, wie auch andere Teile der Exekutive sowie internationale oder supranationale Organisationen, wie NATO und Europäische Union (EU), sind dabei einer permanenten Bedrohung durch Angriffe aus dem Cyber- und Informationsraum ausgesetzt. Auch Informationskampagnen, insbesondere zum Beispiel durch Desinformation, Propaganda und den großflächigen Einsatz von „Bots" in Sozialen Medien, können gezielt auf Akteure der Bundeswehr sowie der NATO- oder EU-Streitkräfte zersetzend ausgerichtet sein. Die Bundeswehr hat dazu einen Militärischen Organisationsbereich aufgestellt, um in der Dimension Cyber- und Informationsraum militärisch handlungsfähig zu sein – ob in Szenarien des Internationalen Krisenmanagements, bei nationalen Operationen oder im Rahmen der LV/BV.

Eine zielgerichtete Gestaltung der Operationsführung unter Berücksichtigung dieser Phänomene und Rahmenbedingungen ist Grundvoraussetzung für Informationsüberlegenheit und damit für die eigene Führungs- und Wirkungsüberlegenheit. Im Militärischen Organisationsbereich CIR werden dafür Kräfte und Mittel der Bundeswehr in der Dimension CIR gebündelt und die Unterstützung des Einsatzführungskommandos der Bundeswehr und des Nationalen Territorialen Befehlshabers für Führungsfähigkeit, Aufklärung und Wirkung und Schutz im Einsatz durch das Kommando CIR mit seinen CIR-Kräften und – Fähigkeiten sichergestellt. Im Gemeinsamen Lagezentrum Cyber- und Informationsraum (GLZ CIR) wird dafür das relevante Wissen in der Bundeswehr korreliert und verfügbar gemacht (siehe auch der Beitrag zum GLZ CIR auf Seite 12).

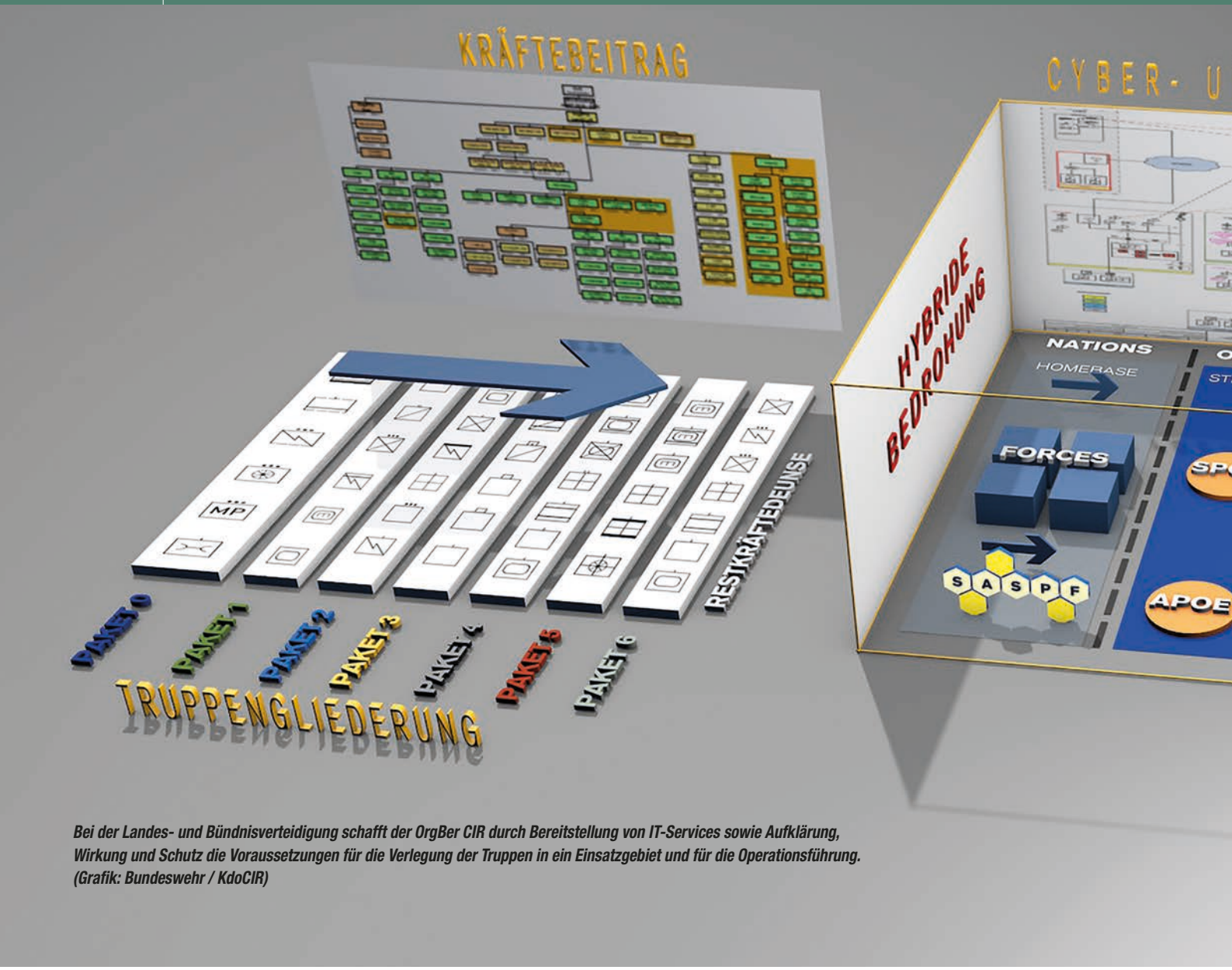
Deutschland führt 2023 erneut die NATO-Speersitze VJTF

Die NATO hat die Landes- und Bündnisverteidigung wieder in den Vordergrund gerückt. Um aber potentielle Aggressoren abzuschrecken, muss sie ihre Fähigkeit zur Verteidigung glaubhaft abbilden. Dazu dienen die NATO Response Forces (NRF) und ganz besonders die „Very High Readiness Joint Task Force" (VJTF), auch NATO-Speerspitze genannt. Deutschland stellt hierfür nicht nur Kräfte bereit, sondern übernimmt nach 2019 auch in 2023 erneut deren Führung.

Der deutsche Beitrag zur NRF ist dabei so ausgeplant, dass Aufträge im multinationalen Rahmen mit besonderem Fokus auf Operationen bis hin zu Artikel 5 des Nordatlantikvertrags (Bündnisverteidigung) innerhalb der festgelegten Einsatzbereitschaftszeiten ausgeführt werden können.

Die Einsätze der Bundeswehr sind bisher geprägt von der Teilnahme an multinationalen Stabilisierungsoperationen. Operationen der LV/BV unterscheiden sich von diesen dadurch, dass notwendige Kommunikationsverbindungen zwischen den eingesetzten Truppenteilen in der Bewegung über große Entfernungen von Beginn an funktionieren müssen.

Kräfte des Militärischen Organisationsbereichs CIR leisten dabei einen wesentlichen Beitrag zur Einsatzbereitschaft der NRF 2022 - 2024 und zur Stärkung der Reaktionsfähigkeit des Bündnisses. CIR stellt mit seinen Informationstechnikbataillonen die weitreichende Anbindung und Operationsfähigkeit der deutschen Kräfte sicher, bildet durch die Electronic



Bei der Landes- und Bündnisverteidigung schafft der OrgBer CIR durch Bereitstellung von IT-Services sowie Aufklärung, Wirkung und Schutz die Voraussetzungen für die Verlegung der Truppen in ein Einsatzgebiet und für die Operationsführung. (Grafik: Bundeswehr / KdoCIR)

Warfare Task Force das Rückgrat für die Gefechtsfeldaufklärung der Kampfverbände, des Wirkens im elektromagnetischen Spektrum sowie durch Operative Kommunikation im Informationsumfeld und ermöglicht durch hochspezialisierte Kartenbeiträge des Geoinformationsdienstes die Operationsführung der Landstreitkräfte. Der Beitrag einzigartiger CIR-Fähigkeiten zur NRF erfordert bis 2022 die Weiterentwicklung und das Vorantreiben zahlreicher Projekte aus den Bereichen IT, Aufklärung, Wirkung und Schutz. Dieser Fähigkeitsbeitrag ist als „Grundlast“ des „Unternehmens CIR“ zu verstehen.

Es gilt, die eigenen CIR-Kräfte handlungsfähig zu halten. Nicht nur durch Teilhabe am Informationsaustausch, sondern auch durch den Erhalt der Funktionsfähigkeit moderner, IT-gesteuerter Plattformen und Waffensysteme. Dem Schutz eigener Systeme kommt bei der Fähigkeitsentwicklung geschützter Führungsfahrzeuge/Transportfahrzeuge gleichfalls eine wesentliche Bedeutung zu.

Die gestiegene Bedeutung des Cyber- und Informationsraums mit seinen schnell aufeinanderfolgenden, disruptiven Innovationszyklen wird in Summe in den nächsten Jahren zu einem stetig steigenden Investitionsbedarf führen, der zur Realisierung der angestrebten Fähigkeitsentwicklung und Rüstungsprojekte durch den Haushalt gedeckt werden muss.

Fähigkeitsentwicklung CIR für die Landes- und Bündnisverteidigung

CIR-Kräfte haben einen entscheidenden Anteil am Erfolg möglicher LV/BV-Operationen in den Domänen Führungsfähigkeit, Aufklärung, Wirkung und Schutz im Einsatz. Hierzu werden zahlreiche Fähigkeiten für die VJTF 2023 weiterentwickelt.

Die für die Bundeswehr zu planenden und zu entwickelnden „militärischen Kommunikationsservices“ umfassen die Anbindung und Vernetzung der Truppe, basierend auf den derzeit verfügbaren IT-Standards. Sie erfüllen die Vorgaben des Geschäftsbereichs Bundesministerium der Verteidigung an die Informationssicherheit dieser Systeme ebenso wie die Anforderungen der NATO an die Bundeswehr im Rahmen der Bündnisverteidigung.

Hierzu gehören die Bereitstellung eines Missionsnetzwerk (Mission Net) im Einsatzgebiet, die Bereitstellung der zentralen Dienste aus dem IT-System der Bundeswehr (unter anderem SASPF, VoIP, IntranetBw, Internet), die Anbindung eines Brigadegefechtsstandes, der logistischen Basis sowie Bataillonsgefechtsständen und Gefechtsständen verstärkter Kompanien im Einsatzgebiet; insbesondere auch während eines Gefechtsstandwechsels, bei dem alle geforderten Services an zwei unabhängigen Orten bereitgestellt werden müssen.

Anhand der Rahmenbedingungen und Demands (IT-Forderungen) werden die Kommunikationsservices geplant und entwickelt. Dazu zählen exemplarisch Satellitenkommunikation, digitaler Richtfunk, mobile Kommunikationssysteme, Fähigkeiten zum Aufbau von Kernnetzen inklusive Netzknoten sowie deren Managementfunktionalitäten.

Eine Vielzahl von unterschiedlichen Kommunikationssystemen ist dabei erforderlich, um die verschiedenen militärischen Anforderungen zu erfüllen. Angepasste/standardisierte Ausstattung, Multinationale interoperable Fähigkeiten zur Integration von NATO-Partnern (Federated Mission Networking und Coalition Shared Data), vernetzte Operationsführung, weltweite Nutzbarkeit in verschiedenen Klimazonen, Redundanz zur Erhöhung der Ausfallsicherheit, Echtzeitfähigkeit, Schutz gegen Aufklärung und ein hohes Maß an Fehlertoleranz müssen jeweils abgeleitet vom beabsichtigten Verwendungszweck gegeneinander abgewogen werden.

Als Schlüsselprojekte für die Bundeswehr sind die „Satellitenkommunikation der Bundeswehr“ (SATCOMBw), die „Digitalisierung landbasierter Operationen“ (D-LBO), die Weiterentwicklung des Projekts „Standard-Anwendungs-Software-Produkt-Familien“ (SASPF) sowie die Einführung eines hochmodernen Battle Management Systems (BMS) für die VJTF-Anteile Land 2023 deutlich herauszustellen (siehe auch der Beitrag „Zielbildung, Digitalisierung und Fähigkeitsentwicklung“ auf Seite 68).

Zur Bereitstellung von weitreichenden Übertragungskapazitäten wurden über das Projekt „Satellitenkommunikation der Bundeswehr Stufe 2“ (SATCOMBw Stufe 2) bundeswehreigene geostationäre Satelliten (COMSATBw 1 und 2) in den Jahren 2009 und 2010 in Betrieb genommen. Weitere ortsfeste große Bodenstationen und mobile transportable Bodenstationen unterschiedlicher Größe und Leistungsfähigkeit werden beschafft sowie kommerzielle Satellitenübertragungskapazitäten bei zivilen Providern langfristig angemietet.

Mit dem Folgeprojekt SATCOMBw Stufe 3 sollen im Wesentlichen die mit SATCOMBw Stufe 2 bereitgestellten Fähigkeiten über das Laufzeitende dieser Satelliten hinaus sichergestellt werden. Zur Realisierung sollen neben eigenen militärischen Fähigkeiten auch internationale und bi-, bzw. multinationale Kooperationsmodelle betrachtet werden. Wesentliches Ziel ist es, die verfügbare Satellitenübertragungskapazität zur Führung und Unterstützung der Einsätze – auch im Rahmen LV/BV – zu erhöhen, um dem mittel- und langfristig ansteigenden Bedarf der Bundeswehr Rechnung zu tragen.

Im Rüstungsprogramm Digitalisierung landbasierter Operationen werden künftig IT-Services für die vernetzte Operationsführung im Bereich der mobil genutzten IT bereitgestellt. Dazu wird ein auf die Belange der Führungsfähigkeit abgestimmter und mit dem Kernnetz des IT-Systems der Bundeswehr Ebenen gerecht vernetzter Informations- und

◁ *Service Delivery Points binden die Einsatzkräfte aus dem Einsatzgebiet heraus an das Bundeswehrnetz im Inland an. (Foto: Bundeswehr / Betriebszentrum IT-System der Bundeswehr)*

Kommunikationsverbund geschaffen, der auf der untersten taktischen Ebene beim abgesessenen Soldaten beginnt und bis zur Ebene der verlegefähigen Gefechtsstände reicht.

Die prozessorientierte IT-Unterstützung wird mit dem Projekt SASPF auch für Einsätze der Landes- und Bündnisverteidigung weiterentwickelt. SASPF ist als betriebswirtschaftliche Standardsoftware Teil des IT-Systems der Bundeswehr. Es verarbeitet annähernd die Gesamtheit aller logistischen und administrativen Daten der Bundeswehr und ist heute von elementarer Bedeutung für den Grundbetrieb sowie die Unterstützung bei Einsätzen, Einsatzgleichen Verpflichtungen, Missionen und Übungen. Das Ziel von SASPF besteht darin, eine moderne, an den aktuellen Erfordernissen und Prozessen ausgerichtete IT-Unterstützung für Einsätze jedweder Art zur Verfügung zu stellen.

Die herausgehobene Bedeutung von SASPF für den Cyber- und Informationsraum und für die Digitalisierung der Bundeswehr wird besonders deutlich am Übergang der bestehenden IT-Systemlandschaft von SAP/R3 auf S4/HANA. S4/HANA ist eine SAP-Datenbank, die auf In-Memory-Technologie zur Analyse großer Datenmengen in Echtzeit beruht. Der damit verbundene weitere Ausbau der In-Memory-Technologie unterstützt die mobile und vernetzte Nutzung von Daten sowie Analyse- und Simulationsmöglichkeiten auf Basis von Informationen in Echtzeit bei laufenden Einsätzen im Rahmen der LV/BV. Neue Qualitäten der Informationsbereitstellung bei steigenden Anforderungen hinsichtlich Autarkie, Verfügbarkeit und Informationssicherheit werden mit Advanced Analytics (autonome oder halbautonome Analyseverfahren), Internet of Things, Machine Learning, Augmented Reality und insbesondere auch prädiktiven Anteilen (schwache Künstliche Intelligenz), in den kommenden Jahren durch SASPF in Einsätzen Einzug halten.

Die Verbesserung der technischen wie organisatorischen Zusammenarbeitsfähigkeit steht ebenso wie betriebliche Optimierung, Fähigkeitserhalt und Fähigkeitsausbau der vorhandenen Anwendungen zur Unterstützung der Führungsprozesse bei der LV/BV in einem besonderen Fokus. Mit dem Programm „Harmonisierung der Führungsinformationssysteme“ (HaFIS) wurde begonnen, die zahlreichen Führungsinformationssysteme der Teilstreitkräfte zusammenzuführen und eine gemeinsame Infrastruktur, Nutzerverwaltung etc. serviceorientiert unter einem „Programm“ zu etablieren. Nutzerspezifische Fachanwendungen werden zukünftig auf einer gemeinsamen Plattform (Rechenzentrumsverbund) über Rechenzentren und Cloud-Infrastruktur geliefert. Ziel ist es, den Informationsaustausch und die Unterstützung der Führungsprozesse für multinationale (combined) und teilstreitkraft-übergreifende (joint) Einsätze signifikant zu verbessern, so dass relevante operative und taktische Informationen allen Führungsebenen schnell zur Verfügung stehen.

Informationstechnik für die VJTF 2023

Für die IT der Bundeswehr bedeutet die Refokussierung auf die Landes- und Bündnisverteidigung eine Abkehr vom stationären und unbeweglichen Feldlager-Denken zurück zur hochmobilen und beweglich-gefechtsführenden Denkweise, die große Kampfverbände im Rahmen von Operationen der Verbundenen Kräfte zur Führungsfähigkeit befähigt.

Die bisherigen Szenare für die Stabilisierungseinsätze konnten bereits für das Anforderungsprofil der VJTF 2019 nicht als Blaupause herangezogen werden. Dies machte sich beispielsweise bei den Satellitentrupps „Bodenstation dynamisch Multiband“ aus dem Projekt SATCOMBw Stufe 2 (Stand 2006) bemerkbar. Sie waren aufgrund ihrer technischen Auslegung nicht für das Szenar VJTF geeignet. Als richtiger LV/BV-Lösungsansatz wurde die Nutzung der Satellitentrupps BSdynM für taktische Anbindungen in Ergänzung zu den Punkt-zu-Punkt-Verbindungen der strategischen Anbindungen identifiziert. Die prinzipielle Funktionsweise der BSdynM entspricht dem geforderten Szenar: Alle Gefechtsstände, die mit einer BSdynM angebunden sind, sind Teilnehmer in einem vollständig „vermaschten“ Netz und können damit direkt untereinander kommunizieren. Wesentlicher Vorteil ist es, dass Kommunikationsbeziehungen erst bei Bedarf nutzerorientiert aufgebaut werden. Zudem werden nicht genutzte Satellitenübertragungskapazitäten anderen Nutzern im dynamischen Netz zur Verfügung gestellt.

Für die VJTF (L) 2023 gilt es somit, das Prinzip der BSdynM auf weitere Stationstypen wie „Bodenstation mittel Multiband handelsüblich“ und „Taktische Bodenstation“ auszudehnen, um einen reduzierten Kräfteansatz von Bodenstationen und ein Höchstmaß an Flexibilität bei sich ständig ändernden Kommunikationsbeziehungen in einem hoch dynamischen Gefecht sicherzustellen.

Die IT-Kräfte des Organisationsbereichs CIR haben sich planmäßig zu hocheffektiven IT-Servicedienstleistern der Bundeswehr im Aufgabenspektrum LV/BV weiterentwickelt. Die bisherigen Erfahrungen haben gezeigt, dass militärische Handlungsfähigkeit ohne robuste, flexible und hochmoderne militärische IT nicht gegeben ist. Die erläuterten Weiterentwicklungen von SATCOMBw, D-LBO, SASPF und BMS stellen einen bedeutenden Beitrag zur Refokussierung der Bundeswehr auf LV/BV dar.

Aufklärung und Wirkung im Einsatz der VJTF

Das Kommando Strategische Aufklärung (KdoStratAufkl) stellt wesentliche Kräfte und Mittel für die Aufklärung und Wirkung im Cyber- und Informationsraum (siehe auch die Beiträge „Aufklärung“ und „Wirkung“ auf den Seiten 31 und 36). Diese Kräfte begleiten die Kampftruppe als „Augen“, „Ohren“ und mit „Herz“ zur Sicherung der Informationsüberlegenheit auf dem Gefechtsfeld. Konkret bedeutet dies, das elektromagnetische Spektrum, das Informationsumfeld mit seinen

Medien, Meinungen, Wahrnehmungen und Gerüchten bis hin zu den Netzwerken der modernen Informationstechnologie zu beobachten und im Einsatz zu nutzen.

Besondere Relevanz haben hierbei geschützte Systeme zum Stören gegnerischer Kommunikation. Diese dienen den Kräften der Elektronischen Kampfführung (EloKa) zur Durchführung von elektronischen Gegenmaßnahmen mit hoher Leistung im VHF/UHF-Bereich gegen gegnerische Kommunikations- und Datenverbindungen sowie Navigationsanlagen im Einsatzraum – hierbei soll ein Gegner soweit beeinträchtigt werden, dass dieser zeitlich befristet eigene Operationen nicht durchführen oder seine taktischen Planungen umsetzen kann. Natürlich wird auch ein potentieller Gegner den CIR für sich zu nutzen suchen. Dies in einem Konfliktfall zu verhindern, ist Auftrag des KdoStratAufkl mit seinen Fähigkeiten - es agiert so als Aufklärungs- und Wirkkommando. Mögen die Wirkkomponenten der VJTF-Kräfte für Aufklärung und Wirkung im Einsatz, unter dem Blickwinkel „Show of Forces“ betrachtet, auf den ersten Blick nicht so imposant wirken wie eine Panzerhaubitze 2000 – so können diese bei einem möglichen Gegner Funkverbindungen stören, Nachrichten und Informationen verfälschen oder eine mögliche gegnerische Propaganda entlarven.

Als Teil des deutschen Beitrags NRF 2023 stellt das KdoStratAufkl für drei Jahre (2022-2024) mit über 300 Soldatinnen und Soldaten einen umfänglichen aktiven Anteil am Kräftedispositiv im Brigadegefechtsstreifen und auf den Ebenen der Component Commands. Zusätzlich unterstützt es die Einsätze mit über 1.700 Soldatinnen und Soldaten im Rahmen von Dauereinsatzaufgaben. So können aufgrund von Einschränkungen der Kontingentgröße im Einsatzraum nicht abbildbare Fähigkeiten im „Reachback“ aus der Basis Inland heraus wahrgenommen werden.

Die Kräfte unterstützen in einer bataillonsübergreifenden EloKa-Task Force mit den Fähigkeiten der Elektronischen Kampfführung, einer Komponente Luftbildaufklärung, einer Luftlandefähigen Komponente für den elektronischen Kampf zur Nahunterstützung im Einsatz (LEKE) sowie durch Aufklärung und Wirkung im Informationsumfeld mit Kräften der Operativen Kommunikation. Zusätzliche Unterstützung wird durch Beratungsleistungen auf allen Ebenen der spezialisierten Component Commands und des Joint Force Command der NATO erbracht.

Die genannten VJTF-Kräfte unterstützen mit gezielter Aufklärung und Wirkung im Cyber- und Informationsraum und leisten dadurch einen signifikanten Beitrag zum Schutz der eigenen Kräfte. Sie decken anteilig den Informationsbedarf der Bundeswehr und tragen somit gezielt zur Lagefeststellung bei.

Das EloKa-Waffensystem HUMMEL in der Stellung.
(Foto: Bundeswehr / KdoStratAufkl)

Mit dem VJTF-Auftrag des KdoStratAufkl wird auch Neuland betreten. So wie sich das Gefechtsfeld digital gewandelt hat, müssen sich auch Mittel und Taktik ändern und beübt werden. Aus Übungen assignierter Verbände wurden Lehren gezogen, die Task Forces angepasst und für VJTF 2023 gezielt auf die Aufgaben im Kampfverband vorbereitet. Die nationalen Beraterteams CIR, die auf ihren jeweiligen Ebenen die Truppenführer vor Ort in allen CIR-Angelegenheiten unterstützen, müssen in die Operationsführung eingebunden werden. Dies gilt nicht nur für die deutschen Anteile an der VJTF, sondern im Übrigen für die NATO und EU insgesamt. Die CIR-Kräfte des KdoStratAufkl sind ein zum Teil neues und scharfes Schwert in den Händen der Streitkräfte. In der Landes- und Bündnisverteidigung sind sie ein unentbehrliches Element.

Geoinformationswesen der Bundeswehr

Der Geoinformationsdienst der Bundeswehr stellt die benötigten GeoInfo-Unterstützungsleistungen bereit. Er umfasst 18 Fachdisziplinen mit ca. 180 Produkten und Dienstleistungen, die, wo immer möglich, als Service über das IT-System der Bundeswehr bereitgestellt werden sollen.

Mit Bezug auf die LV/BV ist die „land- und seegebundene robuste Navigation unter NAVWAR- (Navigational Warfare) Bedingungen“ ein zentrales fähigkeitsstiftendes Projekt. Durch dieses Projekt soll die Ausrüstung zur Positionsbestimmung, Navigation und Zeitfestlegung querschnittlich für die Bundeswehrplattformen Land und See umgerüstet/modernisiert werden. Zur land- und seegebundenen robusten Navigation gehört auch die Berücksichtigung der Störer- und Täuscherrobustheit sowie der Schutz vor Cyber-Angriffen solcher land- und seegebundenen Plattformen. Der Schutz für alle Plattformen und Systeme (luftgebundene Systeme, Munition, Handgeräte, Rechenzentren etc.) bedarf zum Teil noch vorgeschalteter Forschung & Technologie - Maßnahmen und wird im Rahmen eigenständiger Projekte realisiert.

Fazit

Wesentliches Merkmal und relevantes Konfliktbild zukünftiger Landes- und Bündnisverteidigung sind Hybride Bedrohungen, wobei „Information“ die zentrale operationelle Handlungslinie in hybriden Vorgehensweisen ist. Damit militärisches Denken und Handeln zukünftig überhaupt erfolgreich sein kann, muss dies in allen Bereichen der Bundeswehr verstanden und verinnerlicht werden. Dieser sicherheitspolitischen Entwicklung trägt der Militärische Organisationsbereich CIR Rechnung durch die Bereitstellung von CIR-Kräften. Diese bieten für die Zukunft wirksame Antworten auf gesamtstaatliche und militärische Herausforderungen in der militärischen Dimension Cyber- und Informationsraum. Da die Bedrohungslage im Cyber- und Informationsraum sich dynamisch weiterentwickeln und technische Innovationszyklen sich mit der gleichen Dynamik weiter verkürzen werden, benötigen wir Strukturen, die dem daraus resultierenden, stetig steigenden Investitionsbedarf in den nächsten Jahren Rechnung tragen können. Der Organisationsbereich CIR ist durch die Stärkung der Steuerungsfähigkeit der IT und der Sicherstellung von Aufklärung, Wirkung und Schutz in der Dimension CIR „aus einer Hand“, insbesondere für die LV/BV der Bundesrepublik Deutschland, die folgerichtige Antwort auf diese Entwicklung. Er ist mit seinen Truppen und Kommandos der verlässliche Leistungserbringer für die Fähigkeiten im Cyber- und Informationsraum.

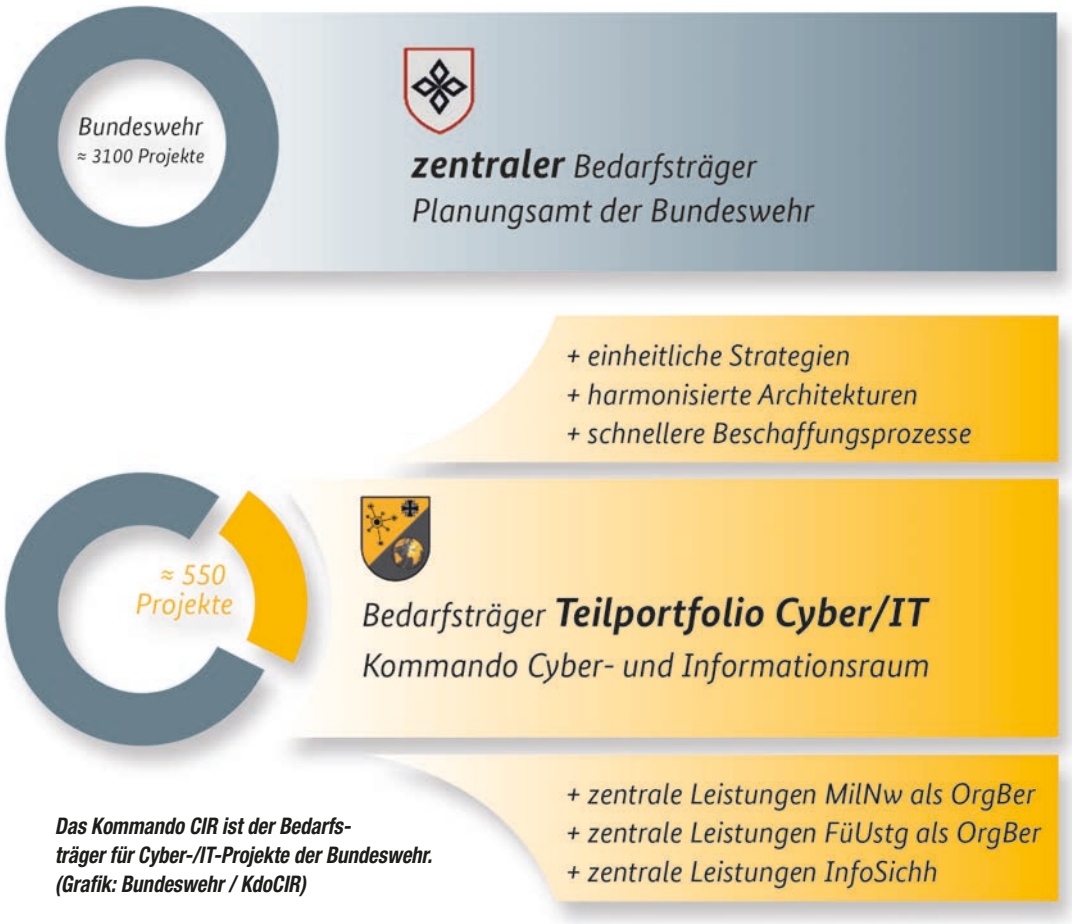
wt

---

*Das **Referat Einsatzplanung** im Kommando CIR trägt als Kräfteplaner die Verantwortung für die Beiträge des Organisationsbereichs CIR zu LV/BV.*

Brigadegeneral Armin Fleischmann

Zielbildung, Digitalisierung und Fähigkeitsentwicklung im Kommando Cyber- und Informationsraum



Das Kommando CIR ist der Bedarfsträger für Cyber-/IT-Projekte der Bundeswehr. (Grafik: Bundeswehr / KdoCIR)

Der Cyber- und Informationsraum ist der als militärischer Operationsraum erschließbare, zugleich virtuelle, physische und kognitive Raum, der aus dem Cyberraum, dem Elektromagnetischen Umfeld sowie dem Informationsumfeld besteht. Die Fähigkeit von Streitkräften, sich im Cyber- und Informationsraum zu schützen und ihn in militärischen Operationen gleichermaßen gestaltend und wirksam zu nutzen, ist in künftigen Konflikten von entscheidender Bedeutung. Hierzu ist neben dem digitalen Situationsbewusstsein das kontinuierliche konzeptionelle Durchdringen des Cyber- und Informationsraums als Operationsraum und seiner Gesetzmäßigkeiten die Kernherausforderung.

Die durchgängige Digitalisierung der Streitkräfte, der Imperativ multinationaler Interoperabilität, die schnellen Innovationszyklen der Informationstechnik sowie die einhergehende Veränderung der klassischen Konfliktdynamiken und -muster hin zu einer dauerhaft bestehenden Bedrohung im Cyber- und Informationsraum erfordern leichter adaptierbare Verfahren und besondere Kompetenzen in der ganzheitlichen Fähigkeitsentwicklung, Beschaffung und Bereitstellung von speziellen CIR-Fähigkeiten.

Dieser Beitrag beschreibt die wesentlichen Rahmenbedingungen, Vorgaben und Verfahren für die zielorientierte Zukunfts- und Fähigkeitsentwicklung im Kommando Cyber- und Informationsraum an ausgewählten Beispielen.

Eindeutige Zuständigkeiten

Die militärische Dimension Cyber- und Informationsraum ist gleichrangig zu den Dimensionen Land, Luft, See und Weltraum als Teil des militärischen Operationsraums zu betrachten. Gleichzeitig sind Land-, Luft-, See- und Weltraum- sowie Spezialoperationen ohne die Nutzung der Dimension Cyber- und Informationsraum kaum mehr vorstell- und durchführbar. Das künftige Einsatzumfeld der Bundeswehr wird sich auch auf die Verteidigung des Cyber- und Informationsraums erstrecken.

Die Bundeswehr hat diesem Umstand mit der Aufstellung des militärischen Organisationsbereichs CIR organisatorisch Rechnung getragen. Entscheidende Fähigkeiten zum Betrieb und Schutz des IT-Systems der Bundeswehr (IT-SysBw) sowie zu Aufklärung, Wirkung und Schutz im Cyber- und Informationsraum und deren Fähigkeitsentwicklung wurden unter einheitlicher Führung zusammengefasst.

Das Kommando CIR hat - neben seiner Führungsverantwortung - als einziger Bedarfsträger der Streitkräfte für das Teilportfolio Cyber/ IT eine besondere Verantwortung innerhalb des Integrierten Planungsprozesses (IPP). Das heißt, das Kommando CIR ist alleinverantwortlich für reine IT-Projekte der Bundeswehr. Der Integrierte Planungsprozess ist der bundeswehrgemeinsame Ansatz, Planung so zu gestalten, dass die vorgegebenen Ziele erreicht und die Aufgaben der Bundeswehr erfüllt werden können. Dabei gilt es, technologisch Wünschenswertes mit finanziell Machbarem zu harmonisieren. Durch diese Zentralisierung wurden unter anderem die Voraussetzungen für eine gesamtheitliche Strategie und IT-Architektur unter Einbeziehung der IT-Anteile der Plattformen geschaffen. Denn das IT-SysBw umfasst auch IT-Anteile in Waffensystemen, Sensoren, Medizingerätetechnik und Gebäudeinfrastruktur, die als integrale Bestandteile der jeweiligen Hauptplattform verbaut sind.

Neben dem Teilportfolio Cyber/IT gestaltet das Kommando CIR im Rahmen des IPP über das Planungsamt der Bundeswehr auch die Zukunfts- und Fähigkeitsentwicklung als „zentraler Dienstleister“ für die gesamte Bundeswehr in den Bereichen Operative Kommunikation, Militärisches Nachrichtenwesen, Aufklärung und Wirkung im CIR sowie GeoInfo-Unterstützung.

Fokus: Einsatz und Operateur

Das IT-SysBw steht dabei vor einer einzigartigen Herausforderung im Vergleich zu IT-Systemen in anderen Ressorts. Neben der Unterstützung von administrativen Aufgaben ist es an den Anforderungen der

militärischen Einsätze und der Operateure auszurichten. Dazu muss das IT-SysBw die IT-Services gemäß den operationellen Vorgaben und Nutzerforderungen bereitstellen. IT-Services sind Dienstleistungen, die von einem oder mehreren IT-Service-Provider(n) zur Unterstützung von Aufgaben oder Prozessen der Bundeswehr zur Verfügung gestellt werden. Ein IT-Service setzt sich immer aus organisatorischen, personellen, materiellen und infrastrukturellen Komponenten mit den dazugehörigen Prozessen zusammen.

Um mit Blick auf die Größe und Komplexität der vernetzten Systeme für die Bundeswehr die erforderlichen Fähigkeiten transparent und valide ableiten und bereitstellen zu können, wird die Methode „Architektur" zusammen mit einem durchgängigen Portfoliomanagement angewendet. Eine auf den operationellen Aktivitäten basierende Architektur ermöglicht eine detaillierte, strukturierte und vergleichende Analyse, Darstellung und Bewertung. Diese bezieht die Infrastrukturen, die Organisationen und die Systeme in ihrem Zusammenwirken mit ein. Dazu gehören operationelle Forderungen des Nutzers, Fähigkeiten, Prozesse, Systemfunktionen, Services, Informationen, Daten, technische Standards und deren Beziehungen untereinander. So können dem Operateur IT-Services bereitgestellt werden, die er tatsächlich benötigt, die keine Duplizierungen oder Insellösungen darstellen und in das Gesamtsystem integrierbar sind.

Diese Vorgehensweise ermöglicht zudem die Integration der von Verbündeten bereitgestellten Fähigkeiten und die Bereitstellung eigener Fähigkeiten in ein multinationales Umfeld. Auch eine vergleichsweise kostengünstige Weiterentwicklung, Harmonisierung und Migration von bereits bestehenden Lösungen und Fähigkeiten ist so möglich.

Digitalisierung und Innovationen

Die Digitalisierung unter Nutzung zukunftsbestimmender Technologiefelder und Innovationen unterstützt die Überlebens- und Durchsetzungsfähigkeit unserer Streitkräfte in dem oftmals hybriden Umfeld und optimiert zusätzlich das unterstützende Verwaltungshandeln. Damit trägt sie entscheidend zur Auftragserfüllung aber auch Zukunftsfähigkeit der Bundeswehr bei.

Die Digitalisierung erhöht die Transparenz des Handelns und fordert die intensive Auseinandersetzung mit neuen Arbeitsformen und –medien, zum Beispiel in Form virtueller, selbstregulierender Teams.

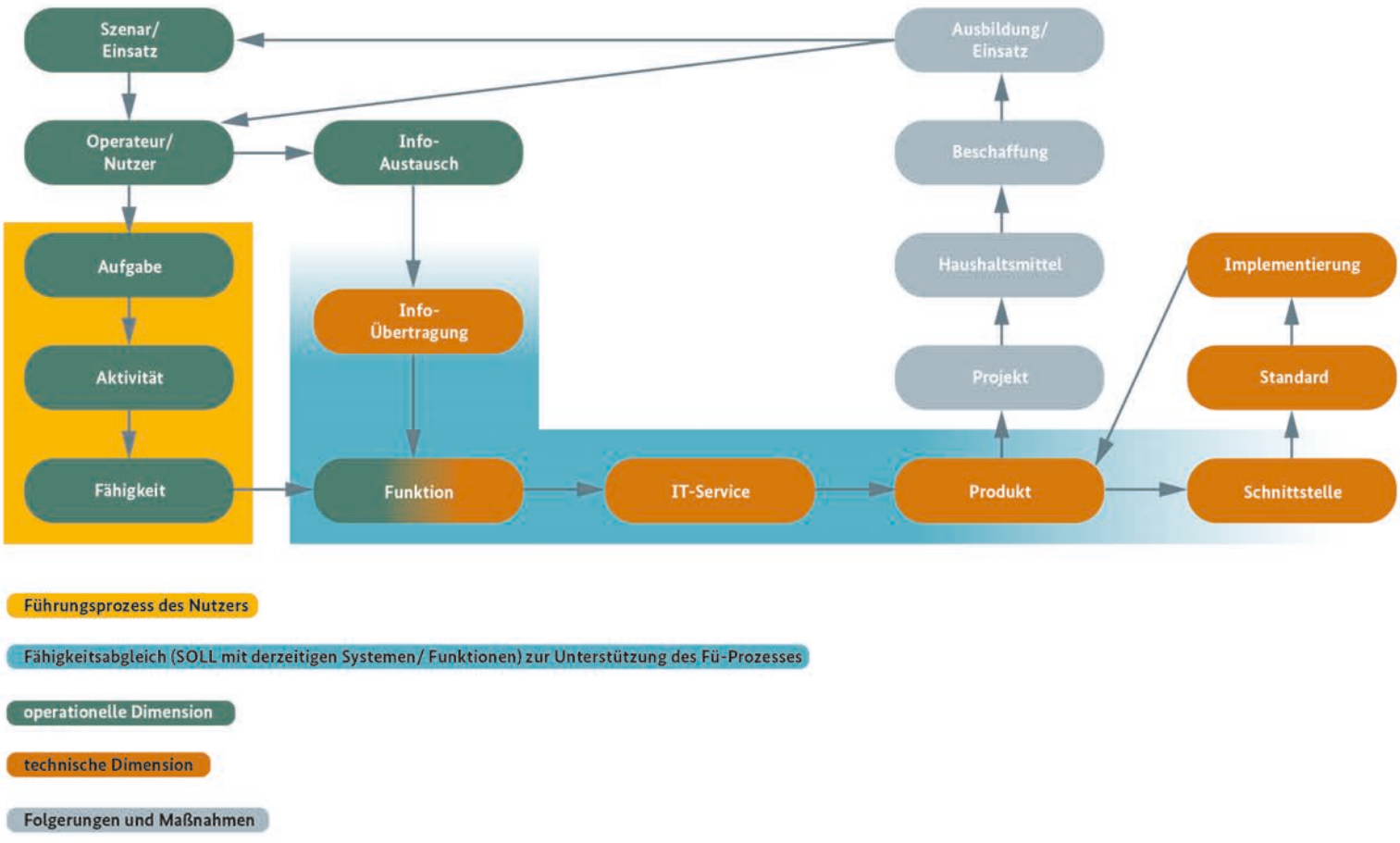
Zu Unterstützung der Digitalisierung gilt es, ein schlankes Innovationsmanagement für das Teilportfolio Cyber/IT zu etablieren. Mit dem Cyber Innovation Hub hat die Bundeswehr ein eigenes „Verbindungselement" zur Start-up-Szene, über das junge IT-Unternehmer mit der Bundeswehr in Kontakt treten können.

An der Universität der Bundeswehr in München wurde ein deutschlandweit einzigartiges Forschungszentrum für Informatik und Cybersicherheit geschaffen und bringt Menschen aus Wirtschaft, Militär und Wissenschaft zusammen. Eine weitere Errungenschaft in diesem Zusammenhang ist das Forschungsinstitut „Cyber Defense and Smart Data" – das CODE. Es forscht an innovativen und für die Bundeswehr relevanten Themen, wie beispielsweise künstliche Intelligenz, Quantencomputing und Blockchain-Technologien.

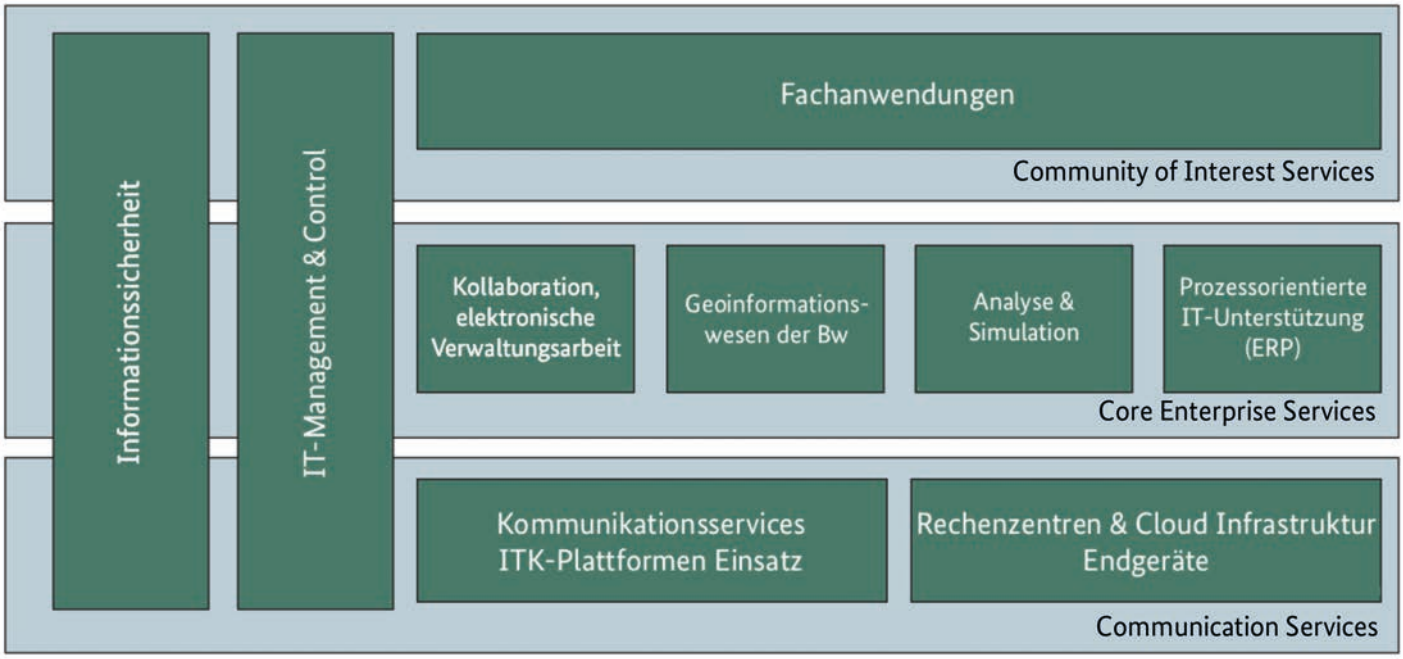
Um Innovationen und Digitalisierung in ihrem eigentlichen Sinne umzusetzen, müssen die Voraussetzungen für schnelle und flexible Realisierung, effiziente Nutzung verfügbarer Ressourcen und optimale Integration der in der Bundeswehr vorhandenen Kompetenzen geschaffen werden.

Mit der Entscheidung zur Einführung der Digitalisierungsplattform Geschäftsbereich (GB) Bundesministerium der Verteidigung (BMVg) wird dazu ein Verbund aus organisatorischen, personellen, materiellen und infrastrukturellen Elementen samt einer durchgängigen, ebenenübergreifenden Steuerungslogik zum Realisieren und Betreiben von IT-Services mit folgender Zielsetzung geschaffen:

Die Architektur des IT-SysBw basiert auf den operationellen Forderungen des Nutzers. (Grafik: Bundeswehr / KdoCIR)



Die Cluster (IT-Servicegruppen) des Teilportfolios Cyber/IT. (Grafik: BMVg Cyber und Informationstechnik - modifiziert)



- durchgängige Steuerungsfähigkeit für das Teilportfolio Cyber/IT durch einheitliche Prozesse im Zusammenwirken mit den betroffenen Elementen BMVg, Kommando CIR und Bundesamt für Ausrüstung und Informationstechnik der Bundeswehr (BAAINBw),
- flexiblere Planungs- und Beschaffungsweg für IT-Services,
- Bereitstellung wiederverwendbarer IT-Services,
- schnellere sowie effizientere Umsetzung von Projekten basierend auf bestehenden IT-Services.

In der Digitalisierungsplattform GB BMVg bündeln und managen Cluster IT-Services. Die korrespondierenden Clusterprogramme beschreiben jeweils das Zielbild und identifizieren Maßnahmen und Projekte, um die Entwicklung modular aufgebauter, effizienter und skalierbarer IT-Services im GB BMVg zu planen, umzusetzen und zu betreiben. Sie sind Grundlage für ein ganzheitliches Management des Teilportfolios Cyber/IT. Die Clusterlogik ist im BMVg und im nachgeordneten Bereich aufbau- und ablauforganisatorisch umzusetzen.

Mit der Digitalisierungsplattform GB BMVg wird die bisherige Ausrichtung der IT-Bereitstellung von einer langwierigen und geringfügig standardisierten Einzelbeschaffung von IT-Services hin zu einer standardisierten und serviceorientierten Leistungserbringung konzeptionell weiterentwickelt.

Effiziente Digitalisierung ist nur erreichbar, wenn IT-Services aus standardisierten Bausteinen in wiederholbaren und flexibel modifizierbaren Systemkonfigurationen zusammengesetzt werden. Die entwickelten Konzepte und Modelle stehen jetzt vor der Umsetzung.

Portfoliomanagement

Das Portfoliomanagement steuert und überwacht das Teilportfolio Cyber/IT. Im Fokus steht das Gesamtportfolio zur Aufgabenerfüllung der Bundeswehr und daraus abgeleitet die notwendigen IT-Services. Zielsetzung des Portfoliomanagements ist, ein aufgabengerechtes, dem Stand der Technik entsprechendes und wirtschaftliches, mit den verfügbaren Ressourcen betreibbares Angebot an IT-Services dem Nutzer zeitgerecht bereitzustellen.

Portfoliomanagement ist somit eine strategische Aufgabe. Es besteht aus zwei Ebenen. Das Fähigkeitsportfolio der Bundeswehr bestimmt auf einer übergeordneten Ebene, welche Fähigkeiten die Bundeswehr vorhalten muss. Auf der anderen Ebene sind im IT-Service Portfolio die Projekte, Produkte und Dienstleistungen zusammengefasst, die die geforderten Fähigkeiten bereitstellen. Aus der gesamtheitlichen Betrachtung beider Ebenen ergeben sich leitungsrelevante Informationen, Bewertungen sowie Handlungsempfehlungen.

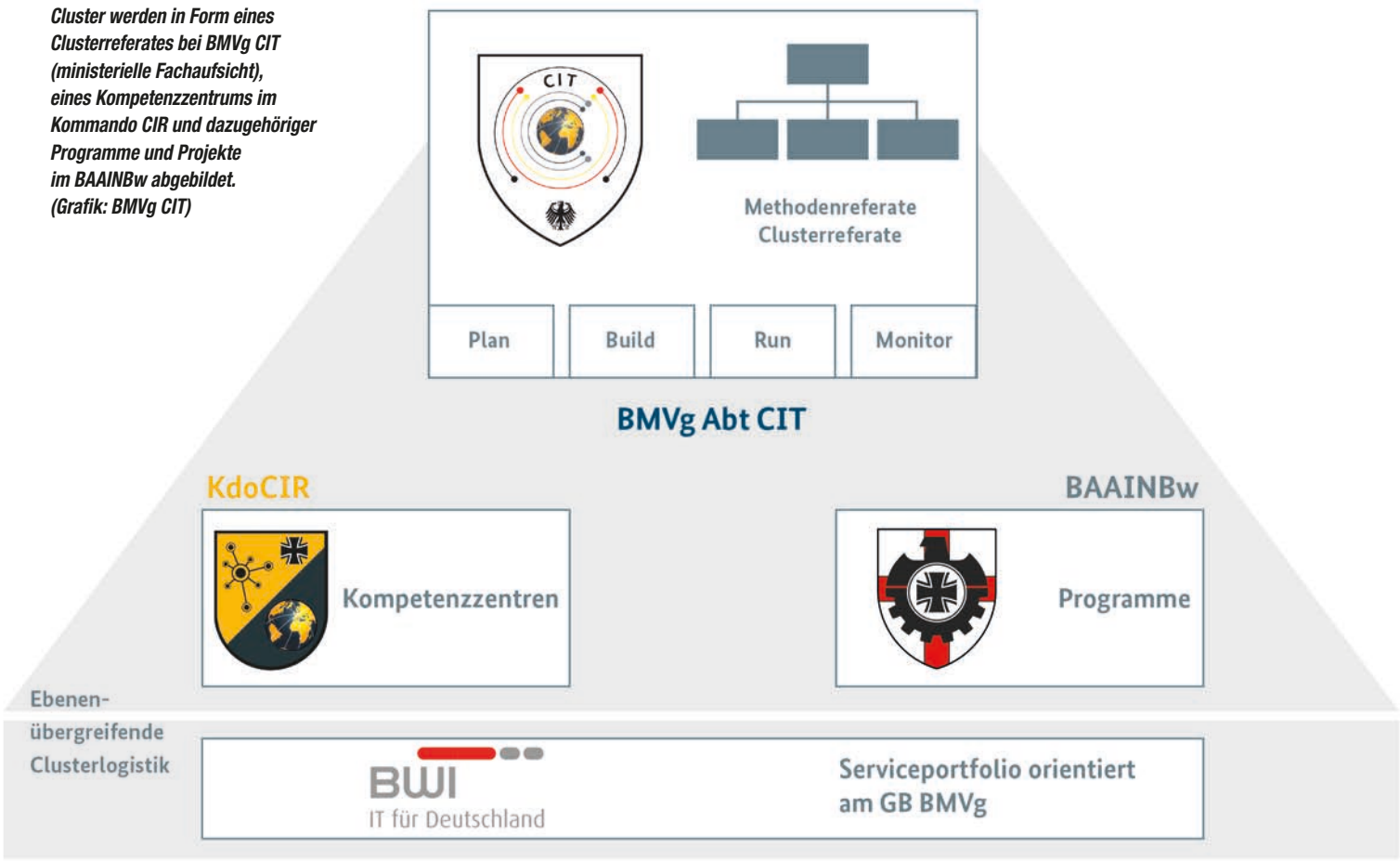
Funktionale Bausteine beschreiben Fähigkeiten und bilden die Schnittelle zu den benötigten Ressourcen wie beispielsweise Material, Personal und Infrastruktur. Im Teilportfolio Cyber/IT werden die benötigten Ressourcen als IT-Service funktionsbestimmt zusammengefasst. Damit entstehen standardisierte IT-Services, die wiederverwendbar sind und aufgabenspezifisch in IT-Service-Module zusammengefasst werden. Damit wird ein durchgängiges Ebenen gerechtes Planen und Steuern möglich. Gleichzeitig werden die Schnittstellen zum übergeordneten Integrierten Planungsprozess sowie zum Hauptprozess Rüstung und Logistik bedient.

Die Ausplanung des Bedarfes für IT-Service-Module sowie die Festlegung deren funktionaler Umfänge obliegt dem Portfoliomanagement im Kommando CIR. Die Umsetzung beziehungsweise die Aufteilung in IT-Services erfolgt durch den IT-Serviceportfoliomanager IT-SysBw im BAAINBw. Zusammen legen sie fest, welche IT-Services wiederzuverwenden und welche neu zu entwickeln sind.

Multinationale Ausrichtung – konzeptionell und technisch

Multinationale Zusammenarbeit ist ein wichtiger Bestandteil der Einsatzrealität. Insofern ist es folgerichtig, dass die Fähigkeitsentwicklung konzeptionell und technisch insbesondere auf die Interoperabilität mit NATO- und internationalen Partnern ausgerichtet wird. Daher ist das Kommando CIR an allen wesentlichen strategischen Initiativen wie Connected Forces, Framework Nations Concept, Federated Mission Networking (FMN) oder Permanent Structured Cooperation beteiligt. Dies schließt die Beteiligung an der Entwicklung oder Fortschreibung strategischer Dokumente von NATO und EU ein.

FMN steht besonders im Vordergrund. Die im Rahmen der FMN-Initiative implementierten Aktivitäten und deren Management durch die NATO dienen unter anderem der Definition von sich kontinuierlich erhöhenden Anforderungen an FMN-Konformität von IT-Systemen und machen Vorgaben bezüglich Priorisierung, Spezifizierungen, Standards, Architektur und Qualität von IT-Services. Entwicklungsschritte werden



Cluster werden in Form eines Clusterreferates bei BMVg CIT (ministerielle Fachaufsicht), eines Kompetenzzentrums im Kommando CIR und dazugehöriger Programme und Projekte im BAAINBw abgebildet. (Grafik: BMVg CIT)

jedes Jahr bei der größten Interoperabilitätsübung der NATO, der Coalition Warrior Interoperability Exploration, Experimentation, Examination and Exercise (CWIX) überprüft. Hier sind alle Möglichkeiten gegeben, Systeme unterschiedlicher Entwicklungsreife sowie NATO-Standards zu testen oder Interoperabilitätsprobleme aufzuzeigen, um anschließend die Ergebnisse in die Rüstung von IT-Services einfließen zu lassen.

Das Kommando CIR koordiniert bei der Übungsserie CWIX alle deutschen Aktivitäten und kann so diesen insbesondere für den Cyber- und Informationsraum wichtigen Aspekt der Fähigkeitsentwicklung steuernd begleiten.

Schnittstellengespräche

Das Kommando CIR trägt die streitkräfteübergreifende Verantwortung bei der Fähigkeitsentwicklung mit den Planungen für die Bereitstellungen von IT-Services für die Landes- und Bündnisverteidigung (LV/BV).

Im Jahr 2019 hat der Inspekteur CIR mit allen militärischen Organisationsbereichen Schnittstellengespräche mit dem Ziel initiiert, die Verantwortung für die Bereitstellung von IT-Services im Szenar LV/BV festzulegen. Hierbei wurde ein gemeinsames Zielbild entwickelt, das festlegt, „wer“ durch „wen“ in der LV/BV mit IT angebunden wird. Daraus leiten sich die operationellen Forderungen an den militärischen Organisationsbereich CIR zur Anbindung der anderen militärischen Organisationsbereiche sowie die Forderungen an das Teilportfolio Cyber/IT insgesamt ab. Diese sind Grundlage für Qualität und Quantität der benötigten Fähigkeiten der nächsten Dekade.

Zur notwendigen Verfeinerung des Zielbildes werden die Schnittstellengespräche fortgesetzt, um weitere Verantwortungen und Aufgaben der einzelnen militärischen Organisationsbereiche zu definieren, beispielsweise bei der Betriebsführung und dem IT-Service Management. Darüber hinaus ist es notwendig, die Bereitstellung von IT-Services innerhalb Deutschlands im Rahmen einer nationalen Führungsorganisation sowie die Rolle der BWI im Rahmen von LV/BV genauer zu untersuchen. Die BWI ist der zentraler Dienstleister der Bundeswehr für Informations- und Kommunikationstechnik.

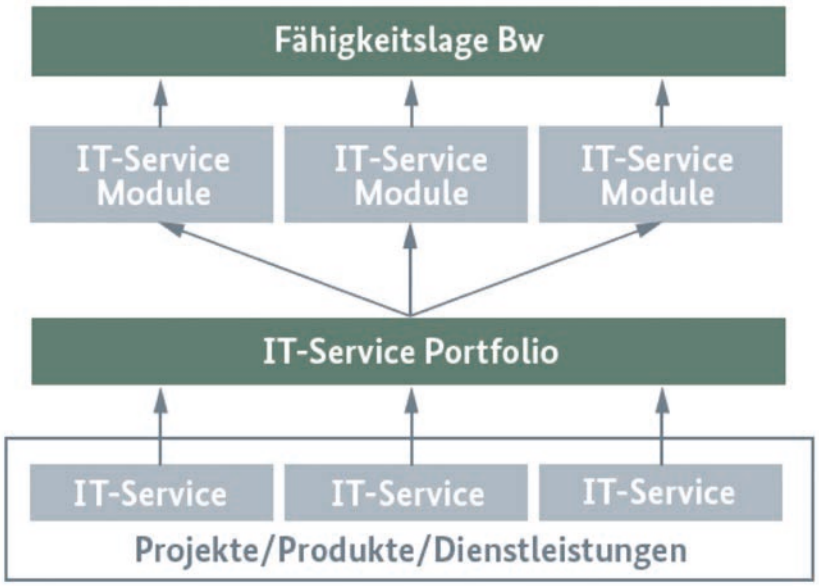
Damit dieses Zielbild ab 2027 in die Realität umgesetzt werden kann, ist ein erheblicher Planungs- und Rüstungsaufwand notwendig. Im Kommando CIR werden derzeit die IT-Bataillone der Zukunft ausgeplant. Hierbei werden technische Trends und Entwicklungen sowie die gestiegenen Anforderungen an Schutz und Mobilität im Rahmen eines Szenars hochintensiver Gefechtsführung berücksichtigt.

Neben dem erforderlichen Fachpersonal und Strukturen ist die Umsetzung wichtiger Rüstungsprojekte wie Satellitengestütztes Kommunikationssystem der Bundeswehr (SATCOMBw), German Mission Network (GMN), Digitalisierung Landbasierter Operationen (D-LBO) und Taktisches Wide Area Network (TaWAN) essenziell. Das Kommando CIR steht hierzu in der Verantwortung der Fähigkeitsentwicklung.

Fähigkeitsentwicklung Militärisches Nachrichtenwesen und Wirkung im CIR

Am Anfang der Fähigkeitsentwicklung müssen die konzeptionellen Grundlagen geschaffen werden. Dabei liefern die im Kommando CIR verantworteten Grundsatzdokumente des Militärischen Nachrichtenwesens ein einheitliches Verständnis von Führungs- und Einsatzgrundsätzen und sind damit wesentliche Voraussetzungen für die im Militärischen Nachrichtenwesen benötigte Ausstattung und deren Unterstützung durch IT-Systeme und IT-Services.

Darüber hinaus wird im Kommando CIR die deutsche Position zur Abstimmung der NATO-Doktrinen für das Militärische Nachrichtenwesen



Das IT-Service Portfoliomanagement basiert auf der Fähigkeitslage der Bundeswehr. (Grafik: BMVg Cyber und Informationstechnik - modifiziert)

Connected Forces ist eine Initiative der NATO. Ziel ist, unter anderem durch neueste Technik die Interoperabilität der NATO-Kräfte weiter zu erhöhen.

Kern des **Framework Nations Concept** (Rahmennationen-Konzept) ist eine gemeinsame strukturierte Entwicklung militärischer Fähigkeiten in europäischen Staaten. Deutschland stellt als Rahmennation unter anderem Führungseinrichtungen.

Die **Permanent Structured Cooperation**, kurz PESCO, ist die Ständige Strukturierte Zusammenarbeit der EU-Nationen, die ausgewählte Verteidigungsprojekte gemeinsam umsetzen wollen. Derzeitig hat Deutschland als vorschlagende Nation die Rolle des Projektkoordinators für das Projekt „Cyber and Information Domain Coordination Centre (CIDCC)“ inne. Das Kommando CIR stellt das Projektteam.

Das Kommando CIR ist an allen wesentlichen multinationalen Initiativen zur Zukunfts- und Fähigkeitsentwicklung beteiligt. (Grafik: Bundeswehr / KdoCIR)

im Auftrag des BMVg erarbeitet, abgestimmt und in die NATO-Gremien eingebracht. Diese gemeinsamen NATO-Verfahren und -Grundsätze haben Auswirkungen auf die gesamte Informationstechnik der Bundeswehr. Auch aus diesem Grund werden die Fähigkeiten der Bundeswehr hinsichtlich Militärischen Nachrichtenwesens und IT aus einer Hand im Kommando CIR weiterentwickelt.

Die technische Entwicklung mit ihren immer kürzeren Innovationszyklen und die Einführung neuer Technologien bieten Möglichkeiten, stellen andererseits aber auch die Aufklärungsfähigkeiten der Bundeswehr vor neue Herausforderungen. Durch die hybriden Vorgehensweisen als wahrscheinliche Form der Konfliktaustragung, ergeben sich zusätzliche Anforderungen an eigene Aufklärungsfähigkeiten. Der Bogen spannt sich hier von der klassischen Krisenfrüherkennung bis hin zu Fähigkeiten, die der konkreten Zielaufklärung im Einsatz - auch im Cyber- und Informationsraum - dienen.

Zukünftig werden daher neben den wesentlichen Säulen der weltweiten abbildenden Aufklärung, der hochfrequenten Aufklärung, den Fähigkeiten zur seegestützten signalerfassenden Aufklärung sowie - in einer komplementären Rolle - zur luftgestützten weiträumigen Überwachung und Aufklärung neue Ansätze zu betrachten sein, bei denen insbesondere die Aufklärung von netzwerkprotokollbasierter Datenübertragung im Fokus stehen wird.

Eine Bewältigung des zukünftigen Auftragsportfolios, insbesondere die Auswertung großer Datenmengen, erscheint ohne den Einsatz künstlicher Intelligenz in diesem Zusammenhang nicht realistisch. Daher treibt das Kdo CIR aktiv das Thema Künstliche Intelligenz und Big Data innerhalb der Bundeswehr voran.

Moderne Streitkräfte sind in hohem Maße auf Führungsmittel wie SATCOM und taktische Datenlinks einschließlich ziviler Funkübertragungsstandards wie Mobilfunk 4G und 5G oder WLAN angewiesen. Das geschützte System zum Stören gegnerischer Kommunikation wird deshalb als zukünftiger Träger der taktischen elektronischen Gegenmaßnahmen in der Bundeswehr neu entwickelt. Durch die deutliche Erweiterung des Frequenzbereichs und einer vollständigen Digitalisierung der Störtechnik und -prozesse wird dieses System befähigt, gegen moderne militärische und zivile Kommunikationsmittel effektiv zu wirken. Es wird dabei weiterhin den Schutz einer gepanzerten Plattform bieten, um den elektronischen Kampf von „ganz vorne“ durchzuführen. Das geschützte System zum Stören gegnerischer Kommunikation wird ab 2025 das bewährte, aber technisch veraltete System HUMMEL in den Verbänden der Elektronischen Kampfführung ablösen.

Neben technischen Entwicklungen werden im Kommando CIR auch menschliche Aspekte und dabei insbesondere die Wirkung von Propaganda betrachtet. Propaganda wird sowohl von staatlichen als auch nichtstaatlichen Akteuren eingesetzt, um Wahrnehmungs-, Willens- sowie Verhaltensänderungen herbeizuführen. Zielgruppe von Propaganda können unter anderem Soldaten der Bundeswehr sein, deren Einsatzwert gemindert werden soll. Das Kommando CIR entwickelt Fähigkeiten, um dem entgegenzuwirken. Im Mittelpunkt steht die Entwicklung der Prävention und Reaktion von beziehungsweise gegenüber Propaganda. Dazu werden auch IT-Tools getestet. Ziel ist, umsetzbare Handlungsempfehlungen geben zu können, um Effekte von Propaganda zu minimieren.

Zusammenfassung

Mit Aufstellung des Militärischen Organisationsbereichs CIR im Jahr 2017 wurde die Dimensionsverantwortung für den Cyber- und Informationsraum übertragen. Diese Verantwortung beinhaltet, den Cyber- und Informationsraum im Rahmen der gesamtstaatlichen Sicherheit sowie in militärischen Operationen zu durchdringen und militärisch zu nutzen.

Die Informationstechnik ist durch Komplexität, starke Interdependenzen von Produkten und Systemen sowie einer hohen Innovationsgeschwindigkeit geprägt. Die Bundeswehr muss die Chancen und Möglichkeiten der Digitalisierung mit aller Entschlossenheit nutzen. Vorgaben und Methoden zur Planung, Realisierung und Nutzung von IT sowie die dazugehörige Aufbau- und Ablauforganisationen sind daran ausgerichtet.

Die Digitalisierung der Streitkräfte ist für diese überlebenswichtig. Die dazu erforderliche kongruente Umsetzung der Digitalisierungsplattform

◁ ***Bei der Digitalisierung Landbasierter Operationen (D-LBO) werden Fahrzeuge, Soldaten und das Führungspersonal durch ein digitales Führungssystem miteinander verknüpft. (Foto: Bundeswehr / Marco Dorow)***

GB BMVg im Kommando CIR ermöglicht eine durchgängige Steuerungsfähigkeit für das Teilportfolio Cyber/IT durch einheitliche Prozesse im Zusammenwirken zwischen BMVg, Kommando CIR und BAAINBw. Die schnellere Umsetzung von Projekten durch effiziente Nutzung der begrenzt verfügbaren Ressourcen basierend auf bestehenden und wiederverwendbaren IT-Services und Umsetzung digitaler Innovationen führt zu einer zukunftsorientierten, agilen und wirtschaftlichen Weiterentwicklung von IT-Lösungen.

Die im Kommando CIR mit Hochdruck verfolgte multinationale Fähigkeitsentwicklung stellt eine gemeinsame Form der Einsatzvorbereitung, -planung und -durchführung dar, bei der durch vorausschauendes Handeln schnell und dauerhaft die operationelle Effektivität zur Erreichung militärischer Zielsetzungen verbessert werden kann.

Bei Schnittstellengespräche mit anderen militärischen Organisationsbereichen werden die entscheidenden Weichen für die zukünftige Qualität und Quantität der IT-Kräfte der Zukunft gestellt.

Mit dem Kommando CIR wird das Denken und Entwickeln von Fähigkeiten als Gesamtsystem von verschiedenen Elementen, die vormals eher unabhängig voneinander gesehen wurden, möglich. Dieses zeigt sich besonders deutlich in den Domänen Aufklärung und Wirkung, die zunehmend von einem ganzheitlichen Verständnis möglicher zukünftiger Einsätze vorangetrieben werden.

wt

Brigadegeneral Armin Fleischmann
ist Abteilungsleiter Planung im Kommando CIR.

SARah ist das zukünftige System der Bundeswehr zur weltweiten abbildenden Aufklärung. (Abbildung: OHB System AG)


MACH, WAS WIRKLICH ZÄHLT.
#IT
FOLGE DEINER BERUFUNG.
bundeswehr karriere.de
BUNDESWEHR