Relevanz, Attraktivität und Zukunftstüchtigkeit – Bundeswehr 4.0 ante portas

Ralph D. Thiele

Januar 2015

Zusammenfassung

‚Vernetzte Operationsführung' ist als grundlegendes Prinzip der Bundeswehr nun schon über ein Jahrzehnt konzeptionell verankert. Sie setzt in den Dimensionen Land, Luft, See, Cyber und Weltraum Vorgaben für das gesamte Handlungs- und Leistungsspektrum der Bundeswehr im Verbund von Führung, Aufklärung, Wirkung und Unterstützung. So sehr die Prinzipien der *‚Vernetzten Operationsführung'* auch das Konzeptionsgebäude der Bundeswehr durchdrungen haben, in der Truppe und bei den Fähigkeiten der Streitkräfte ist davon bisher nicht viel angekommen.

Dr. Katrin Suder, Staatssekretärin im Verteidigungsministerium, stellte beim Celler Trialog 2014 die Forderung nach einer Rüstungsindustrie 4.0. Tatsächlich werden sich im Zuge von Industrie 4.0 die Möglichkeiten und Anforderungen zur Umsetzung der Prinzipien der *‚Vernetzten Operationsführung'* revolutionär erweitern. Insbesondere zwei Namen stehen für das Potenzial von Industrie 4.0: *‚Eingebettete Systeme'* und das *‚Internet der Dinge'*. Die Bundeswehr braucht die wehrtechnische und die Sicherheitsindustrie als leistungsfähigen Partner, um das inhärente Potenzial von Industrie 4.0 unter den Bedingungen hybrider Herausforderungen und knapper Ressourcen zeitnah zu erschließen. Wer jetzt nicht entsprechend plant und zielgerichtet investiert, ist in zehn Jahren nicht mehr relevant und hat zudem enorm Geld verschwendet. Das gilt nicht zuletzt auch für die Bundeswehr selbst.

Das ISPSW

Das Institut für Strategie- Politik- Sicherheits- und Wirtschaftsberatung (ISPSW) ist ein privates, überparteiliches Forschungs- und Beratungsinstitut.

In einem immer komplexer werdenden internationalen Umfeld globalisierter Wirtschaftsprozesse, weltumspannender politischer, ökologischer und soziokultureller Veränderungen, die zugleich große Chancen, aber auch Risiken beinhalten, sind unternehmerische wie politische Entscheidungsträger heute mehr denn je auf den Rat hochqualifizierter Experten angewiesen.

Das ISPSW bietet verschiedene Dienstleistungen – einschließlich strategischer Analysen, Sicherheitsberatung, Executive Coaching und interkulturelles Führungstraining – an.

Die Publikationen des ISPSW umfassen ein breites Spektrum politischer, wirtschaftlicher, sicherheits- und verteidigungspolitischer Analysen sowie Themen im Bereich internationaler Beziehungen.

Giesebrechtstr. 9
10629 Berlin
Germany

Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06

E-Mail: info@ispsw.de
Website: http://www.ispsw.de

ANALYSE

Ausplanung am Minimum

Die Bundeswehr ist in schwerem Wasser. Berichte über Mängel ihrer Einsatzbereitschaft prägen die deutsche Medienberichterstattung. Die Mängel sind eine Folge der in den vergangenen Jahren praktizierten Ausplanung am Minimum. Das Planungsamt der Bundeswehr stellt nach Medienberichten fest, dass der zur Neuausrichtung erforderliche Ausrüstungsbedarf der Bundeswehr nicht mit finanziellen Mitteln hinterlegt ist. Eine Erhöhung der für Beschaffung und Betrieb vorgesehenen Haushaltsmittel sei unvermeidlich, zugleich eine Präzisierung der Zielvorgaben für die Bundeswehr. Die Streitkräfte werden auf Fähigkeiten verzichten, Strukturen und Materialumfänge reduzieren müssen. Der Weg in eine bessere Zukunft kann vor dem Hintergrund des enormen Potenzials von Industrie 4.0 in einer künftig konsequenteren Ausgestaltung der *‚Vernetzten Operationsführung'* liegen.

‚Vernetzte Operationsführung' ist die Führung und der Einsatz von Streitkräften auf der Grundlage eines streitkräftegemeinsamen, führungsebenenübergreifenden und interoperablen Kommunikations- und Informationsverbundes. Relevante Akteure, Truppenteile und Einrichtungen sowie Sensoren und Effektoren werden miteinander vernetzt. Dahinter steht Metcalfe[1] mit seiner Faustregel vom exponentiellen Leistungszuwachs in Kommunikationsnetzen. In den Streitkräften erlaubt dieser Verbund von Führung, Aufklärung, Wirkung und Unterstützung schnelleres, effektiveres und effizienteres militärisches Handeln im gesamten Aufgabenspektrum.

Die Nutzung des Informationsraumes ist ein Multiplikator für den Erfolg im Einsatz. Informationen lassen sich in einer besseren Qualität und höheren Aktualität als je zuvor anfordern, gewinnen, bewerten, verdichten, fusionieren, bereitstellen und für die eigene Operationsführung nutzen. Das beschleunigt Planungs- und Entscheidungsabläufe und führt zu Wirkungsüberlegenheit im Einsatz. Damit verbundene Produkte sind

- eine solide Wissensbasis;
- ein gemeinsames, umfassendes, aktuelles Lagebild;
- eine schnelle, flexible, präzise Operationsführung.

Die Möglichkeiten moderner Informations- und Kommunikationstechnologie stehen natürlich nicht nur der Bundeswehr und Ihren Verbündeten zur Verfügung. Auch andere Sicherheitsakteure könnten dieses Potenzial im Zuge hybrider Operationen gegen die Bundeswehr und ihre Verbündeten einsetzen. Die deutschen Streitkräfte sind gut beraten, ihre Befähigung zur *‚Vernetzten Operationsführung'* konsequent voranzutreiben.

Enormes Potenzial

‚Industrie 4.0' bietet hierzu geeignetes Potenzial. Unter dem Stichwort *‚Industrie 4.0'* beginnt derzeit die deutsche Industrie, sich für die Zukunft der Produktion zu rüsten. Sie steht an der Schwelle zur vierten industriellen Revolution. Nach Dampfmaschine, Fließband und Automatisierung wachsen in der beginnenden vierten Revolution – durch das Internet getrieben – reale und virtuelle Welt immer weiter zusammen. Vereinfachend kann

[1] Das Metcalfe'sche Gesetz ist eine Faustregel über das Kosten-Nutzen-Verhältnis von Kommunikationssystemen. Diese beschreibt, dass der Nutzen eines Kommunikationssystems proportional zur Anzahl der möglichen Verbindungen zwischen den Teilnehmern (also etwa dem Quadrat der Teilnehmerzahl) wächst, während die Kosten nur proportional zur Teilnehmerzahl selbst wachsen.

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

man sagen: Maschinen werden *‚intelligent'*. Sie lernen, miteinander und auch mit den Menschen zu sprechen. Sie können Prozesse optimieren, Fehler frühzeitig erkennen und somit auch weitere Fehler vermeiden.

Grundlage ist Datenaustausch in der eigenen Wertschöpfungskette, digitale Kennzeichnung der Produkte und die Nutzung von Echtzeitdaten zur Steuerung der Produktion. Bereits in den nächsten Jahren wird sich die Fähigkeit zur effizienten Analyse und Nutzung von Daten auf globalen Märkten erfolgsbestimmend ausprägen. Diese Entwicklung wird eine parallele Entwicklung mit Blick auf die Fähigkeiten von Sicherheitsakteuren einleiten.

Der *‚Comprehensive Approach'* bzw. das Konzept *‚Vernetzte Sicherheit'*, *‚Network Enabled Operations'* bzw. *‚Vernetzte Operationsführung'* waren im Feld der Außen-, Sicherheits- und Verteidigungspolitik die Antwort auf eine immer komplexer werdende Welt. *‚Industrie 4.0'* ist die Antwort der Wirtschaft auf das gleiche Phänomen. Industrieunternehmen aus Deutschland erwächst in Asien und zunehmend auch in Südamerika starke Konkurrenz, die mittelfristig deren internationale Wettbewerbspositionen gefährden kann. Unternehmen dort steigern sehr dynamisch ihre Produktivität und Innovationskraft. Zugleich beschleunigen sich die Innovationskreisläufe in vielen Technologiefeldern. Die Märkte werden volatiler. Zudem müssen deutsche Unternehmen auf weitere Herausforderungen Antworten finden: knappere Rohstoffe, steigende Energiepreise oder das zunehmende Durchschnittsalter der Beschäftigten.

Mit *‚Industrie 4.0'* wird eine Industrieproduktion anvisiert, die auf eine starke Individualisierung der Produkte zielt – sogenannte hybride Produkte, stark individualisiert, auf Grundlage einer hoch flexibilisierten (Großserien-) Produktion bei weitgehender Integration aller Akteure in Geschäfts- und Wertschöpfungsprozessen sowie bei Kopplung von Produktion und hochwertigen Dienstleitungen. Neuartige Geschäftsmodelle entstehen. Erhebliche Optimierungspotenziale in Produktion und Logistik werden erschlossen; darunter neue Dienstleistungen für Anwendungsbereiche wie Mobilität, Gesundheit und Energie. Unternehmen, die jetzt nicht mit der Schaffung der Grundlagen beginnen, spielen in zehn Jahren auf den Weltmärkten keine Rolle mehr.

Hybride Herausforderungen

Bereits die Sicherheitsentwicklungen in und um Afghanistan, in Mali, Gaza, Syrien und Irak haben erste Vorstellungen davon vermittelt, worauf sich die Weltgemeinschaft im Zuge künftiger, hybrider Auseinandersetzungen einstellen muss. Hybride Kriege sind nicht groß, eher klein. Sie sind nicht regulär, eher irregulär. Sie mischen tradierte Formen des Krieges mit asymmetrischen und hochmodernen Elementen. Sie sind blutig und grausam. Sie haben langfristig verheerende Folgen.

Ganz offensichtlich hat Russland diese Entwicklung in den letzten Jahren sehr genau beobachtet und die Lehren in praktisches Können der eigenen Politikinstrumente übersetzt. Der Westen bekam davon nichts mit. Als russische Truppen Ende Februar die ukrainische Halbinsel Krim unter ihre Kontrolle brachten, war die westliche Welt schockiert und empört. Dosierte und verdeckte militärische Aggression wird abgeschirmt und begleitet von Diplomatie, Informationskriegsführung, Propaganda, humanitären Aktionen, Cyberwar, Geheimdienstoperationen, Wirtschaftsinitiativen und innenpolitischen Repressionen. Tatsächlich war die russische Invasion von langer Hand geplant, vorbereitet und geübt. Die Methodik war sogar zuvor öffentlich angekündigt.

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

So beschrieb der damals frisch bestellte russische Generalstabschefs Walerij Gerassimow Ende Januar 2013 in seiner Rede vor der Jahresversammlung der Russischen Akademie für Militärwissenschaft seine Vorstellungen der russischen Variante *‚Vernetzter Operationsführung'*. Er erläuterte, dass sich die Grenzen zwischen Krieg und Frieden auflösen. Kriege würden nicht mehr erklärt, und sie verliefen nach einem „ungewohnten Muster". Ein prosperierender Staat könne – als Opfer einer ausländischen Intervention – in kurzer Zeit in einen Schauplatz erbitterter bewaffneter Auseinandersetzungen verwandelt werden mit Ausprägungen wie Chaos, humanitären Notlagen und Bürgerkrieg inklusive.

In der Ukraine erlebt die Welt derzeit *‚Vernetzte Operationsführung'* unter den Bedingungen des 21. Jahrhunderts. Der russische Begriff dafür ist „nichtlineare Kriegsführung". Militärische Maßnahmen seien zwar erforderlich, beschrieb Gerassimow 2013, aber sie müssten einen *„verdeckten Charakter"* haben: Dazu gehörten Angriffe auf Informationssysteme und der Einsatz von Spezialtruppen. *„Der offene Einsatz von Truppen – oftmals unter dem Deckmantel von Friedenserhaltung und Krisenbewältigung – kommt erst zu einem späten Zeitpunkt in Betracht, vor allem, um in einem Konflikt endgültig zu gewinnen"*. Entscheidend dafür seien *„Geschwindigkeit, schnelle Bewegungen, der kluge Einsatz von Fallschirmjägern und das Einkreisen feindlicher Kräfte"*.

Tiefhängende Früchte pflücken

Der NATO-Gipfel in Wales im September 2013 adressierte ausdrücklich die hybriden Herausforderungen in Krisenmanagement, Landes- und Bündnisverteidigung, denen das Bündnis im Verbund mit anderen Organisationen wie der EU und der OSZE sowie dem gesamten relevanten Portfolio an Politikinstrumenten der Mitgliedstaaten entgegentreten wird. Im NATO-Kontext wird sich Deutschland an der Aufstellung einer *„Very High Readiness Joint Task Force"* in Brigadestärke beteiligen, die als Speerspitze innerhalb von zwei Tagen verlegt werden können soll. Das deutsche Engagement in der NATO Response Force wird verstetigt. Die Bundeswehr wird im Rahmen des Framework-Konzeptes Verantwortung übernehmen. Das Deutsch-Dänisch-Polnische Korps in Stettin soll zu einem High Readiness Headquarters mit kurzer Vorwarnzeit weiterentwickelt und hierzu bereits im Jahr 2015 personell verstärkt werden. Vor diesem Hintergrund wird die Bundeswehr ihre Fähigkeiten zur Vernetzten Operationsführung nachdrücklich vorantreiben müssen. Hierzu wäre es zweckmäßig, die tiefhängenden Früchte von *‚Industrie 4.0'* alsbald zu pflücken.

Bis heute fremdelt die Bundeswehr beim Umgang mit ihren Daten, Informationen und Wissen. Sie erhebt diese nicht oder schlecht. Sie verwendet sie kaum und nur in wenigen Bereichen effizient und effektiv. Ein wichtiger Grund hierfür ist die fehlende einheitliche IT-Governance. Aufgaben, Zuständigkeiten und Verantwortlichkeiten liegen nicht in einer Hand.

Das muss sich ändern, denn die bisherige Ignoranz wird sie sich auf Dauer nicht leisten können – nicht mit Blick auf Effizienz und Effektivität, nicht mit Blick auf Kosten, nicht mit Blick auf die erforderliche Relevanz der Bundeswehr im Kontext *‚Vernetzter Sicherheit'*.

Die Bundeswehr 4.0. braucht valide Führungs- oder Geschäftsprozesse. Die Führungsfähigkeit der Streitkräfte erfordert moderne, interoperable, skalierbare und serviceorientierte IT im Informations- und Kommunikationsverbund. Dies sind unverzichtbare Grundlagen für die Befähigung zur *‚Vernetzten Operationsführung'*. In Zukunft werden viele Prozesse in Echtzeit über große Entfernungen gesteuert und koordiniert. Voraussetzung

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

dafür ist die Standardisierung und Modularisierung vieler einzelner Prozessschritte und die Programmierung von virtuell bearbeitbaren Modellen dieser Module. Mit ihrer Hilfe werden künftig betriebliche wie einsatzbezogene Prozesse geplant, gesteuert und kontrolliert. Die Kommunikation verlagert sich dabei zunehmend von der übergeordneten Software auch auf die eingebettete Intelligenz einzelner Komponenten.

Die vertikale Integration aller Prozesse – der stetige Kreislauf von der Lageübersicht, über die Einsatzplanung, das Ressourcenmanagement bis hin zum Einsatz selbst und die Einsatzauswertung – revolutioniert die Planung, Betriebs- und Einsatzführung von Streitkräften. Die Prozessebenen der Organisation – einschließlich auftragsbezogen zusammengestellter Task Forces – werden durchgängig miteinander verknüpft und können auf Grundlage der jeweils aktuellsten Prozessdaten immer wieder neu aufeinander abgestimmt werden. Dazu braucht es flexible Schnittstellenkommunikatoren. Denn die Realisierung von *‚Industrie 4.0'*-Anwendungen in den Streitkräften, *‚Big-Data-Analyse'* und *‚Internet der Dinge'* ist vom Zugriff auf eine gewaltige Datenflut abhängig. IT-Sicherheit muss als integraler Bestandteil verstanden werden. Das Thema Cybersicherheit spielt hierbei konstitutiv eine wesentliche Rolle. Die Sicherheit der Netzwerke herzustellen und zu garantieren, ist eine der größten Herausforderungen im Rahmen der zunehmenden Vernetzung.

Rechtzeitige und richtige Informationen sind die Basis für qualifizierte Entscheidungen, vom Sensor bis zur obersten politisch-militärischen Führungsebene. Die Transparenz durch Verfügbarkeit der Daten ist die Voraussetzung dafür, dass Entscheidungsträger ihrer Führungsverantwortlichkeit entsprechend bei Bedarf regulierend eingreifen können. Sobald die Daten einmal erhoben sind, müssen diese möglichst schnell dorthin gelangen können, wo sie in Führungs- und Wirkungsvorteile umgesetzt werden können. Leistungsfähige, sichere Netze sind erforderlich. Erst die Vernetzung schafft die Voraussetzung für den kontinuierlichen Austausch von Daten, aus denen automatisch situationsgerechte Prozessanpassungen abgeleitet werden.

Eine immer größere Bedeutung für die Leistungsfähigkeit dieser Netze erlangen Zug um Zug die sogenannten Cyber-Physical-Systems (CPS). Diese vernetzen die eingebetteten IKT-Systeme untereinander und mit dem Internet. CPS sind Netzwerke kleiner, mit Sensoren und Aktoren ausgestatteter Computer, die als sogenannte ‚Eingebettete Systeme' in Materialien und Gegenstände, Geräte und Maschinenteile, Waffensysteme und Sensoren etc. eingebaut und über das Internet miteinander verbunden werden. In einem derartigen ‚Internet der Dinge' verbinden sich die physische und die digitale Welt und tauschen kontinuierlich Informationen aus. Einsatz- und Logistikprozesse werden integriert. Bereits 2009 wurde von Experten im Auftrag der Bundesregierung eine „Nationale Roadmap Embedded Systems" erarbeitet. Auf dem Gebiet der (softwareintensiven) eingebetteten Systeme hat sich Deutschland bereits eine führende Stellung, insbesondere im Automobil- und Maschinenbau, erarbeitet. Diese Innovation brauchen wir auch in und für die Streitkräfte.

Das Internet und dedizierte Führungsinformationsnetze der Streitkräfte ermöglichen die ständige Koordinierung auch zwischen weltweit verteilten Standorten und über Organisationsgrenzen hinweg. Die horizontale Integration, also die Vernetzung zwischen verschiedenen Organisationen, ist Ausgangspunkt der flexiblen Gestaltung ihrer gemeinsamen Wertschöpfungsprozesse. Streitkräfte und mit ihnen kooperierende Organisationen und Unternehmen bilden künftig dynamische Netzwerke, aus denen heraus sie auftrags- und Fähigkeiten bezogen ihre Kapazitäten zu virtuellen Leistungsverbünden zusammenschließen.

Da die Bundeswehr nahezu ausschließlich im multinationalen Rahmen agiert, ist die Weiterentwicklung der Vernetzten Operationsführung eng mit den jeweiligen Institutionen in der NATO abzustimmen; darüber hinaus dann auch mit der Europäischen Union sowie mit einzelnen Partnernationen. Das Framework-Konzept gibt

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

hierfür Deutschland eine tragende Rolle. Im Kontext des Konzepts der Vernetzten Sicherheit sind darüber hinaus auch ressortübergreifende Aspekte der Vernetzung zu beachten, die zudem aus der regierungsseitig angestrebten Harmonisierung der IT aller Ressorts befeuert wird.

Mit dem German Mission Network entsteht eine solche Fähigkeit für die deutschen Streitkräfte. Es zielt auf eine Verbesserung der Führungsfähigkeit der Bundeswehr in Einsätzen. Das German Mission Network ist kompatibel zum Federated Mission Networking der NATO und soll die bisher weitgehend physikalisch getrennten, durch Schnittstellen miteinander verbundenen und national/multinational wenig interoperablen IT-Services, für Einsätze zu einem physikalisch und logisch durchgängigen System zusammenführen.

Das Federated Mission Networking der NATO setzt quasi den Standard. Es basiert auf dem ‚Afghanistan Mission Network', das erstmalig in der Geschichte des Bündnisses zentrale und durchgängig einsatzrelevante Informationen (IT-Services) verfügbar gemacht hat – eine Intensität der IT-gestützten Zusammenarbeit, die über Jahrzehnte nicht gelungen ist und allen Beteiligten hinsichtlich Kosten, Leistung und Interoperabilität aufgezeigt hat, wohin sich die Bündnismitglieder und auch weitere Kooperationspartner bewegen müssen. Mit der deutschen Initiative ‚German Mission Network' ist die Bundeswehr bereits auf dem Weg zu einer interoperablen Lösung. So werden derzeit mit dem Programm ‚*Harmonisierung der Führungsinformationssysteme'* erste diesbezügliche Fähigkeiten erworben. Eine Erweiterung des funktionalen Umfangs und der Mengengerüste ist für die Jahre 2015 – 2017 vorgesehen – mit einer sukzessiven Erweiterung in den Jahren 2017 – 2020. Dann könnte die Übernahme der Betriebsverantwortung durch das HERKULES Folgeprojekt erfolgen.

Die funktionale Leistungsbeschreibung für das Herkules Folgeprojekt wird derzeit erarbeitet.

Hier sind die Anforderungen einer Bundeswehr 4.0 definitiv zu berücksichtigen. Mit dem Übergang in das HERKULES Folgeprojekt ab 2017, den laufenden Aktivitäten zur IT-Konsolidierung des Bundes, der Verpflichtung Deutschlands im Rahmen des „Framework"-Konzeptes eine angemessene Führungsfähigkeit nach Maßgabe des Federated Mission Networking bereitzustellen sowie mit Blick auf die dringend erforderliche Verschränkung von grüner und weißer IT besteht dringender Handlungsbedarf für eine einheitliche IT-Governance. Zudem müssen Prozessorientierung und Leistungsportfolio weiterentwickelt werden, nicht zuletzt auch mit Blick auf

- Cybersicherheit,
- Informations- und Wissensmanagement,
- Vernetzte Operationsführung (insbesondere der Verbund Führung-Aufklärung-Wirkung-Unterstützung.

Mitwirkung der Industrie

Mit Blick auf die zunehmenden hybriden Konflikte an der europäische Peripherie, die Defizite bei der klassischen Landes- und Bündnisverteidigung, aber auch die steigenden Erwartungen an Deutschlands Führungsrolle im Rahmen des Framework Nation Concept braucht eine zukunftstüchtige Bundeswehr eine leistungsfähige deutsche wehrtechnische und Sicherheitsindustrie. Folgerichtig forderte Dr. Katrin Suder, Staatssekretärin im Verteidigungsministerium, beim Celler Trialog 2014 eine Rüstungsindustrie 4.0.

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

Bislang gehörte die wehrtechnische- und Sicherheitsindustrie zu den Innovationstreibern in Deutschland. Mittels *‚Industrie 4.0'* wird sie auch weiterhin wettbewerbsfähig bleiben können. Hierzu sind industrieseitig die erforderlichen Investitionsentscheidungen zu treffen, Forschungs- und Entwicklungspotenziale nachhaltig zu stärken sowie Schlüsseltechnologien im internationalen Verbund stärker auszubauen. Ergänzend brauchen regierungsseitig Beschaffung und Rüstungsexport mehr Transparenz und strategische – auch industriepolitische – Ausrichtung als bisher.

Die Großen der Sicherheitsbranche machen sich heute bereits auf den Weg zu *‚Industrie 4.0'*. Standardisierungsaktivitäten und leistungsfähige Technologieplattformen werden insbesondere durch internationale Aktivitäten realisiert. Dagegen kennen fast zwei Drittel der mittelständischen Fertiger in Deutschland, Österreich und der Schweiz den Begriff *‚Industrie 4.0'* noch nicht einmal.[2]

Aber gerade auch der Mittelstand muss schneller und effizienter auf die Bedürfnisse des Marktes eingehen können, braucht eine schnellere Umsetzung seiner Intellectual Properties in produktreife Innovation und kürzere Innovationszyklen. Dies unterstreicht die Bedeutung nationaler und regionaler Förderinstrumente. Über die Zusammenarbeit von kleineren und mittleren Unternehmungen – durchaus auch in Zusammenarbeit mit Großkonzernen, Universitäten und Forschungslabors – ist es auch auf nationaler und regionaler Ebene – staatliche finanzielle Unterstützung vorausgesetzt – durchaus möglich, die komplette Wertschöpfungskette zu bedienen.

Bislang produzierte die Rüstungsindustrie meist kostenintensive und hochleistungsfähige Systeme in geringer Stückzahl. *‚Industrie 4.0'* wird hier die Kosten senken helfen. Zugleich besteht dank neuer Technologien die Möglichkeit, künftig mehr auf „intelligente Masse" zu setzen. Der bereits begonnene Wettstreit um die Kontrolle strategisch relevanter Räume wie Luft, See, Weltraum, Cyberraum befördert diesen Trend.

Den sich ändernden militärischen Anforderungen folgend hat sich die Sicherheits- und Verteidigungsindustrie zunehmend differenziert. Im Gegensatz zu vergangenen Jahrzehnten macht die Produktion im sogenannten Konventionellen Sektor – hierzu zählen militärische Güter wie Panzer, Waffen, Flugzeuge, Schiffe und Munition – nur noch ein Drittel der Wertschöpfung aus. Der Trend geht längst in Richtung des sogenannten Erweiterten Sektors. Hier dominieren Güter und Dienstleistungen für Prävention und Einsatzmanagement, darunter insbesondere:

- Einsatzbereitschaft,
- Einsatzmobilität,
- Lagebild,
- ITK-Lösungen,
- Dienst- und Serviceleistungen,
- Überwachung, Aufklärung und Alarmierung.

Neben dem Markt für Technologieanwendungen mit militärischem Verwendungszweck entstehen ein Markt der Technologieanwendung für zivile Sicherheitsaufgaben und eine Schnittmenge mit mehrfach nutzbaren Technologien. Viele dieser Dual Use-Technologien sind zivilen Ursprungs. Durch ihren Einsatz wird die sicherheits- und verteidigungspolitisch relevante Technologiebasis breiter und globaler.

[2] So das Ergebnis einer Umfrage unter rund 1.000 Unternehmen durch das Analysehaus techconsult im Rahmen seiner Studie "Business Performance Index Mittelstand 2014".

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

Wandel von Arbeitswelt und Aufgaben

Für die Mitarbeiter und Soldaten der Bundeswehr bedeutet der mit Bundeswehr 4.0 verbundene Einsatz der neuen Technologien einen Wandel ihrer Arbeitswelt und ihrer Aufgaben. Der ist auch dringend und zwingend erforderlich. Die künftige Einsatzbereitschaft der Streitkräfte hängt nicht nur von guter Ausrüstung ab, sondern auch davon, ob es der Bundeswehr gelingt, geeignetes Personal langfristig an den Arbeitgeber Bundeswehr zu binden und neue qualifizierte Kräfte für eine Karriere in den Streitkräften oder den zivilen Bereichen zu gewinnen.

Der demografische Faktor ist dabei von entscheidender Bedeutung. Er betrifft nicht nur die Bundeswehr, sondern unsere gesamte Gesellschaft. Auch bei Polizei und Feuerwehr, bei der Not- und Katastrophenhilfe drohen die helfenden Hände auszugehen. Entsprechend steht die Bundeswehr in einem zunehmend harten Verdrängungswettbewerb um leistungsfähige Arbeitskräfte. Bereits heute kann die Bundeswehr ihren Bedarf an qualifizierten Fachkräften in wichtigen technischen Bereichen, aber auch bei der Marine und im Sanitätsdienst, nicht mehr ausreichend decken. Mit dem fortschreitenden demografischen Wandel wird sich der Wettbewerb um Fachkräfte mit Polizei und Feuerwehr sowie weiten Teilen der Wirtschaft weiter verschärfen.

Vor diesem Hintergrund bietet Bundeswehr 4.0 eine verbesserte Ausgangslage, denn

- Es wird weniger Personal benötigt.
- Es wird qualifizierteres Personal gebraucht.

Den Soldaten und zivilen Mitarbeitern kann dann bei konsequenter Innovation ein technologisch, finanziell und auch Aufgaben bezogen attraktiver Arbeitsplatz geboten werden, der zugleich auf die Vereinbarkeit von Familie und Beruf angemessen Rücksicht nimmt.

In der Bundeswehr 4.0 gewinnt in vielen Prozessen die Automatisierung weiter an Bedeutung. Intelligente Assistenzsysteme, z. T. auch Roboter zu Land, See und in der Luft übernehmen bereits heute – und künftig immer mehr – einen Teil der Arbeit. Die militärischen und zivilen Mitarbeiter nehmen immer hochwertigere – ingenieursähnliche – Aufgaben wahr. Sie haben dann überall und jederzeit Zugriff auf die für ihren Auftrag relevanten Informationen. Bei Bedarf können anwendungsspezifische Trainingsangebote aufgerufen werden, um jeden Mitarbeiter bei der Erfüllung seiner Aufgaben optimal zu fördern. Die Vereinbarkeit von Familie und Beruf wird durch eine flexible Prozessvernetzung vereinfacht. Letztere verstärkt und verbessert auch den Austausch zwischen den Mitarbeitern aus verschiedenen Organisationsbereichen.

Diese vielfältigen Entlastungen gehen mit einer hohen Reaktionsfähigkeit in der Planung des Personaleinsatzes einher. Die Einsatzplanung wird viel adäquater auf die individuelle Situation eines Mitarbeiters eingehen, seinen Rhythmus berücksichtigen und auf seine kurzfristigen Anliegen zügig reagieren können. Der Aspekt individueller Karrieren gewinnt an Bedeutung. Dies erleichtert die immer wichtiger werdende Talentgewinnung.

Bundeswehr 4.0 eröffnet der Bundeswehr breite Perspektiven für Relevanz, Attraktivität und Zukunftstüchtigkeit. Natürlich ist die Revolution eher ein evolutionärer Prozess, der nicht von heute auf morgen zu bewältigen ist. Aber das ist kein wirkliches Novum. Die Soldaten und zivilen Mitarbeiter der Bundeswehr kennen dies aus zahlreichen Reformen. Jede kleine Automatisierung, jede Einführung eines neuen, vernetzteren IT-Systems, jede moderne Ausrüstung der Soldaten kann letztlich als ein Schritt in Richtung Bundeswehr 4.0 angelegt und verstanden werden. Die Zukunft hat längst begonnen.

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

Anmerkungen: *Der Beitrag gibt die persönliche Auffassung des Autors wieder.*

Über den Autor dieses Beitrags

Oberst a.D. und Diplom-Kaufmann Ralph D. Thiele ist Vorsitzender der Politisch-Militärischen Gesellschaft e.V. (pmg), Berlin und CEO von StratByrd Consulting. In seiner militärischen Laufbahn war Herr Thiele in bedeutenden nationalen und internationalen, sicherheits- und militärpolitischen, planerischen und akademischen Verwendungen eingesetzt, darunter im Planungsstab des Verteidigungsministers, im Private Office des NATO-Oberbefehlshabers, als Chef des Stabes am NATO Defense College, als Kommandeur des Zentrums für Transformation und als Direktor Lehre an der Führungsakademie der Bundeswehr.

Eine Vielzahl von Publikationen, regelmäßige Vorträge in Europa, Amerika und Asien sowie eine intensive Forschungstätigkeit im Kontext deutscher, österreichischer und europäischer Sicherheitsforschung unterstreichen sein ausgeprägtes Kompetenzspektrum.

Ralph D. Thiele ist Mitglied im Beirat Deutscher Arbeitgeber Verband e.V., Wiesbaden und im Defence Science Board, das von Gerald Klug, Verteidigungsminister der Republik Österreich, geleitet wird.

Ralph D. Thiele

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de