Heiko Borchert (Hrsg.)

Vernetzte Sicherheit

Leitidee der Sicherheitspolitik im 21. Jahrhundert

Vernetzte Sicherheit

Herausgegeben von Ralph Thiele und Heiko Borchert

Band 1

Heiko Borchert (Hrsg.)

Vernetzte Sicherheit

Leitidee der Sicherheitspolitik im 21. Jahrhundert

Ein Gesamtverzeichnis der lieferbaren Titel der Verlagsgruppe Koehler/Mittler schicken wir Ihnen gerne zu. Sie finden uns auch im Internet unter www.koehler-mittler.de

Bibliographische Information Der Deutschen Bibliothek
Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.db.de abrufbar.

ISBN: 3-8132-0824-9

Produktion: Hans-Peter Herfs-George
Druck und Bindung:
Printed in Germany

Das Erscheinen dieses Bandes wurde von der Rheinmetall DeTecAG gefördert.

Inhalt

Dirk Böcker

Vorwort

Das gewandelte geopolitische Umfeld Deutschlands und die Dynamik der sicherheitspolitischen Herausforderungen erfordern die umfassende Neuausrichtung der deutschen Sicherheits- und Verteidigungspolitik im globalen Kontext. Die Politik hat hierzu in den vergangenen Monaten entscheidende Weichenstellungen vorgenommen.

Die Struktur und das Fähigkeitsprofil der Bundeswehr sind auf das gesamte sich aus dem politischen Auftrag ableitende Aufgabenspektrum auszurichten. Die multinationale Einbindung der Bundeswehr in die Konfliktverhütung und Krisenbewältigung im Rahmen des transatlantischen Bündnisses sowie der Vereinten Nationen und der Europäischen Union, einschliesslich des Kampfes gegen der internationalen Terrorismus, sind in diesem Zusammenhang bestimmende Eckpfeiler der Integration der Bundeswehr in die Mechanismen internationaler Sicherheit.

Die Neuausrichtung der Bundeswehr hat zum Ziel, nach Einsatzbereitschaft und Fähigkeiten differenzierte, moderne und leistungsfähige Streitkräfte bereit zu stellen, die schnell, wirksam und durchhaltefähig mit den Streitkräften anderer Nationen eingesetzt werden können. Diese Zielsetzung verlangt einen umfassenden, innovativen und bundeswehrgemeinsamen Ansatz, der Aufgaben, Strukturen, Prozesse und Mittel konsequent an den Erfordernissen des Einsatz deutscher Streitkräfte orientiert und aufeinander abstimmt.

Die Bundeswehr bündelt und integriert die hierzu erforderlichen Prozesse und Massnahmen unter dem Begriff Transformation. Das Verständnis von Transformation greift dabei sehr viel weiter als der Begriff der Weiterentwicklung und erfordert ein bundeswehrgemeinsames Handeln und Denken. Im Vordergrund werden nicht mehr die Fähigkeiten der einzelnen Organisationsbereiche stehen, sondern die Fähigkeiten der Bundeswehr als Ganzes.

Die Transformation der Bundeswehr ist ein auf Kontinuität ausgerichteter Prozess, der insbesondere die operationellen Grundsätze und Konzepte, die Organisationsstruktur sowie die Führung, die Ausbildung und nicht zuletzt die fähigkeitsorientierte Ausrüstungsplanung der Bundeswehr auf die Anforderungen zukünftiger militärischer Einsätze ausrichten wird. Die für die Bundeswehr wahrscheinlichsten Einsätze werden hierbei in den Mittelpunkt gestellt.

Die multinationale Dimension wirksamer Konfliktverhütung und Krisenbewältigung erfordert zwingend die Interoperabilität unserer Streitkräften im Bündnis und in internationalen Koalitionen. Die Integration der Bundeswehr in die multinationalen Transformationsprozesse wurde daher konsequent verfolgt und wird unter besonderer Berücksichtigung der nationalen Transformationsziele weiter intensiviert und ausgebaut.

Führungsfähigkeit und Information sind für die Einsatzführung moderner Streitkräfte von herausragendem Stellenwert. Eine hohe Effektivität und Effizienz der Einsatzführung setzt voraus, dass die beteiligten Kräfte und Führungsprozesse eng miteinander verzahnt sind und Informationen schnell, durchgängig und ebenengerecht in Führungsleistung umgesetzt wer-

den. Die bundeswehrweite Vernetzung aller Führungsebenen, einschliesslich der Sensoren und Effektoren in einen umfassenden Verbund von Aufklärungs-, Führungs-, und Wirksystemen, bildet den Träger einer vernetzten Operationsführung der Bundeswehr.

Die konzeptionellen Ansätze zu Network Centric Warfare sind Ausgangspunkt für die Umsetzung einer vernetzten Operationsführung in der Bundeswehr. Die technologischen Weiterentwicklungen und Trends eröffnen in diesem Zusammenhang neue Perspektiven. Technologische Aspekte sind für die Entwicklung einer Gesamtarchitektur der vernetzten Operationsführung von wesentlicher Bedeutung. Die Zielsetzungen der vernetzten Operationsführung können jedoch nur erreicht werden, wenn Technologie, Doktrin und Führungsprozesse in einem kohärenten Ansatz zusammengeführt und integriert werden.

Die vernetzte Operationsführung stellt kein isoliert zu betrachtendes Konzept dar, sondern ist durchgängig und konsistent in den operativen und funktionalen Konzepten der Bundeswehr abzubilden. Die zentrale Idee der vernetzten Operationsführung schafft die Grundlage für die ganzheitliche Ausformung der Planungs-, Entscheidungs-, und Führungsprozesse der Bundeswehr.

Die intellektuelle Auseinandersetzung mit den Prinzipien und konzeptionellen Ansätzen der vernetzten Operationsführung sowie die kontroverse Diskussion von Strategien ihrer Implementierung ist für die Bundeswehr von hoher Bedeutung. Ich danke dem Herausgeber und den Autoren für die exzellenten Beiträge und das besondere Engagement in dieser für die Bundeswehr zentralen Aufgabenstellung.

Ich bin sicher, dass diese Publikation weitreichendes Interesse innerhalb der Bundeswehr, der wehrtechnischen Industrie und einer interessierten Öffentlichkeit finden wird.

Hubert Feigl

Überlegungen zu Network Centric Warfare (NCW)

Die USA haben bekanntlich schon viel früher als ihre Bündnispartner damit begonnen, sich mit den Erfordernissen einer Neuorientierung der militärischen Dispositive auseinander zu setzen. Man reagierte damit auf Entwicklungen, die eventuelle Veränderungen in der Kriegführung implizierten und wollte durch antizipatorisches Handeln die unbestreitbare militärische Überlegenheit auch weiterhin sicherstellen. Ausschlaggebend dafür war die Einsicht, dass die Auswirkungen des Informationszeitalters für die Streitkräfte konzeptionell erst mangelhaft erfasst wurden. Vor allem fehlte ein den sich abzeichnenden Erfordernissen entsprechendes Operationalisierungskonzept für „Streitkräfte des Informationszeitalters".

Um diese Lücke zu schließen, wurden Mitte der neunziger Jahre die anstehenden Fragen der künftigen Orientierung und Ausgestaltung von Streitkräftedispositiven in systematischer Form behandelt und erste Schlussfolgerungen gezogen.[1] Mit dem Ziel, realisierbare Lösungsvorschläge zu erarbeiten, entwickelte sich daraus bald eine sehr ambitionierte Projekttätigkeit. Inzwischen liegen nicht mehr nur Visionen, sondern auch erweiterte Konzepte und konkret umsetzbare Lösungsvorschläge vor, wobei letztere größtenteils auch schon konkret umgesetzt wurden.

Das keinesfalls abgeschlossene Vorhaben umfasst auch heute noch zahlreiche, zum Teil sehr anspruchsvolle Evaluierungs- und Entwicklungsprogramme. Fragen der praktischen Ausgestaltung des Transformationsprozesses und seiner Fortschreibung rücken dabei zusehends in den Mittelpunkt. Nach wie vor wird großer Wert darauf gelegt, das Wirksamwerden von Lösungsansätzen ohne ausreichende Überprüfung zu vermeiden. Diesem Zweck dient die Einschaltung der oft ausgedehnten Experimentier- und Erprobungsphasen – meist schon mit intensiver Beteiligung der Streitkräfte.

Die erzielten Ergebnisse sind, was die konzeptionelle Neuorientierung anbelangt, zweifellos vielversprechend. Sie wirken meist in einem generellen Sinn fähigkeitsbestimmend und sorgen auf diese Weise für eine deutliche Modifizierung der Einsatzprofile. Die zum Teil neuen, die Kriegführung insgesamt verändernden funktionalen Zuordnungen werden seit einiger Zeit unter dem Begriff Network Centric Warfare (NCW) zusammengefasst. Im Zentrum der konzeptionellen Orientierungen stehen die vernetzte Generierung, Umsetzung und Absicherung von Fähigkeiten und der dafür erforderliche Einbezug von Netzwerken. NCW fungiert in diesem Zusammenhang als vereinheitlichende Zuordnungsstruktur, vor allem aber als konzeptionelles Grundraster für Streitkräfteoperationalisierungen.

---

[1] Hierzu grundlegend: *Joint Vision 2010* (Washington, D.C: US Joint Chiefs of Staff, 1996), <http://www.dtic.mil/jv2010/jv2010.pdf> (Zugriff: 30. Dezember 2003); *Joint Vision 2020* (Washington, D.C.: US Joint Chiefs of Staff, 2000), <http://www.dtic.mil/jointvision/jvpub2.htm> (Zugriff: 30. Dezember 2003).

US-amerikanische Praxiserfahrungen

Die Aktivitäten der zurückliegenden Jahren waren hauptsächlich darauf ausgerichtet, Orientierungsvorgaben zu erstellen. Vorausgreifende Festlegungen in Bezug auf Doktrinbildung und Entwicklung von Einsatzkonzepten sollten dabei zurückgestellt werden. Der inzwischen erarbeitete konzeptionelle Ansatz entspricht zwar schon mehr einem Operationalisierungskonzept, beinhaltet aber immer noch keine fertige Rezeptur für künftige Kriegführung.

Die ergebnisoffene Weiterführung des Evaluierungs- und Entwicklungsprozesses und das bisherige Fehlen umfassender Festlegungen dürfen jedoch nicht missverstanden werden. Es wäre sicherlich eine Fehleinschätzung, wenn man mit NCW die Vorstellung verbinden würde, es handele sich hier um ein bislang unverbindliches Konzept, dessen Festlegungen noch zur Disposition stünden, der endgültige Nachweis ihrer Brauchbarkeit vielleicht sogar noch fehle. Der mitunter geäußerte Verdacht, man würde mit NCW nur ein Glasperlenspiel betreiben, ist keinesfalls berechtigt. Gegen solche Einschätzungen spricht bereits der im Verlauf der Aktivitäten stets sehr eng gehaltene Bezug zur praktischen Umsetzung. Hinzu kommt, dass die NCW-Ansätze nicht losgelöst von Vorgängermodellen entwickelt wurden. Sie bauen vielmehr in wichtigen inhaltlichen Zuordnungen auf schon früher für richtig erachteten programmatischen Festlegungen auf, die überwiegend schon in der Praxis erprobt wurden.[2]

Den Ausschlag gibt jedoch sicherlich, dass konkret nutzbare neue Ergebnisse von großer Tragweite vorliegen – und daraus schon Sachzwänge für eine Realisierung resultieren, z.B. im Hinblick auf die Überlegenheitswahrung. In Anbetracht dieser Tatsache erscheint es gerechtfertigt, eher davon auszugehen, dass die eingeschlagenen Entwicklungsrichtungen unumkehrbar sind. Dem entspricht auch, dass man sich auf US-amerikanischer Seite schon veranlasst sah, Fakten zu schaffen: Die USA haben bereits gemäß den neuen Vorgaben gehandelt und gegen viele Widerstände aus Politik und Militär ihre Streitkräfte in weiten Bereichen entsprechend umgebaut und ausgerüstet – und, was noch wichtiger ist, die veränderten Dispositive (soweit dies ihnen angeraten erschien) unter Kriegsbedingungen einer Bewährungsprobe unterzogen. Anlass, diese Möglichkeiten zu nutzen, gaben die Kriegshandlungen der jüngeren Vergangenheit im Nahen und Mittleren Osten, bei denen die USA in teilweise neuer Form ihre High-Tech-Kriegsmittel zum Einsatz brachten.

In diesen Fällen wurde zwar von den grundsätzlich bestehenden Optionen der netzwerkzentrierten Kriegführung nur eingeschränkt und meist fokussiert auf bestimmte Anwendungssegmente Gebrauch gemacht. Dennoch genügte dies, um in Ansätzen die Vorteile der Neuorientierungen gegenüber älteren konzeptionellen Vorgaben deutlich werden zu lassen. Bestätigt hat sich vor allem, dass Informationsüberlegenheit die Kriegführung des 21. Jahrhunderts bestimmen wird. Auf dieser Grundlage können neue Operationalisierungsformen von Information in den verschiedenen Varianten der vernetzten Generierung, Umsetzung und Absicherung militärischer Fähigkeiten wirksam werden. Die Voraussetzungen dafür werden durch die netzwerkzentrierten Schwerpunktsetzungen verbundener Einsatzprofile geschaffen, die Bestandteile des NCW-Konzepts sind.

[2] Zu nennen sind in diesem Zusammenhang beispielsweise die Vorläuferkonzeptionen zu „Air-Land-Battle“ sowie die revolutionierenden Programme für weiträumige, präzise Zielbekämpfung mit Hilfe des sensorgestützten Waffeneinsatzes

Die Kriegshandlungen zeigten vor allem die Möglichkeiten des maßgeschneiderten, höchst wirksamen und schnell umsetzbaren Streitkräfteeinsatzes auf. Neue Formen des Zusammenwirkens der Teilstreitkräfte waren dafür ausschlaggebend (Jointness) und haben insbesondere den Wert eines schnellen präzisen Ineinandergreifens gefechtsrelevanter Bestandteile in den jeweiligen Bedarfsszenarien nachhaltig unterstrichen. Die enge Koordination von Aufklärungsmitteln auf dem Boden, in der Luft und im Weltraum mit den Geheimdiensten, mit den Führungs- und Kommandoebenen sowie mit den Waffensystemen und Soldaten auf dem Gefechtsfeld erwies sich dabei stets als besonders wichtig.

Im Verlauf der Kriegshandlungen kam vor allem die enorme Steigerung der Einsatzeffizienz militärischer Mittel zum Tragen, wobei insbesondere im Bereich des Waffeneinsatzes neue Maßstäbe gesetzt wurden. Besonderes Interesse erweckten in diesem Zusammenhang die offenkundig gewordenen Möglichkeiten der Abstandskriegführung (etwa beim Einsatz von Präzisionsabstandswaffen). Einschlägige Beispiele lieferten die chirurgisch präzisen Schläge aus der Luft, die in manchen Szenarien vorentscheidende Bedeutung für den Ausgang des Krieges hatten. Beeindruckend war auch die Schnelligkeit, mit der Landstreitkräfte im Zusammenwirken mit fliegenden Einsatzmitteln eine Entscheidung erzwingen können, wenn die Mittel der sensortechnischen Kriegführung greifen. Hervorzuheben ist dabei insbesondere die Rolle der Nachtkampffähigkeit. Neue Einsatzmöglichkeiten eröffneten sich insbesondere für kleine hochbewegliche Spezialeinheiten, die mit Luftunterstützung in großer räumlicher Tiefe operierten.

Bei alledem ist zu beachten, dass ein massiver High-Tech-Einsatz notwendig war, um den Erfolg sicherzustellen. Dabei konnte dem Grundsatz der Verhältnismäßigkeit des generell schädigenden oder zerstörenden Mitteleinsatzes in vielen Szenarien weitgehend entsprochen werden. Vor allem gelang der überzeugende Nachweis, dass es in vom Kampf gegen Streitkräfte dominierten Kriegsphasen gelingt, den militärischen Erfolg bei gleichzeitig sehr geringen eigenen Verlusten sicherzustellen. Allerdings rufen Leistungsschwächen, Defizite und Pannen, die bei der High-Tech-Kriegführung nie auszuschließen sind, auch immer wieder kritische Stimme auf den Plan. Mängel im Leistungsprofil können jedoch den Wert des hochtechnisierten Einsatzes der Kriegsmittel weder im Einzelfall noch allgemein in Frage stellen. Diese Einschätzung bestätigt bei objektiver Betrachtung auch der Irak-Krieg, wenngleich hier wie in anderen Fällen deutlich wurde, dass sich die Bedingungen radikal ändern können, wenn der Gegner zum verdeckten Kampf übergeht.

Konsequenzen für Europa

Bei den europäischen Partnerstaaten ist inzwischen die Überzeugung gewachsen, dass sie dem US-amerikanischen Beispiel folgen müssen. Einige dieser Staaten haben auch schon konkrete Schritte unternommen, ihre Streitkräftedispositive im Hinblick auf Erfordernisse der netzwerkzentrierten Kriegführung umzubauen.[3] Sachzwänge, so zu handeln, bestanden schon lange, denn die Kooperationsfähigkeit des Bündnisses war in Gefahr und konnte insbesondere gegenüber den USA kaum noch aufrecht erhalten werden. „Netzkompatibilität“ unter Bedin-

[3] Siehe hierzu auch den Beitrag von Burkhard Theile in diesem Band.

gungen von NCW ist sicherlich eine Grundvoraussetzung für effektives Zusammenwirken der Streitkräftedispositive der Partner, wenn das Bündnis seinen Stellenwert behalten soll. Aufgrund der Schwierigkeiten, den Erfordernissen der Führungsmacht zu entsprechen, ist jedoch aus heutiger Sicht eher mit einem begrenzten Ergebnis der europäischen Bemühungen zu rechnen.

Gleichwohl werden sich die europäischen Staaten – Deutschland eingeschlossen – dieser Herausforderung stellen müssen. Das gilt unabhängig davon, ob sie in Zukunft weiterhin auf eine enge Kooperation mit den USA setzen (was wohl wahrscheinlich ist), oder ihre Interessen stärker auf eigenständige Befähigung zur High-Tech-Kriegführung konzentrieren. Erforderlich ist in jedem Fall die Bereitschaft, gemäß den neuen Vorgaben möglichst glaubhafte Fähigkeitsprofile für die jeweiligen Dispositive zu entwickeln. Gerade die jüngsten Kriegsereignisse haben die Unzulänglichkeit der bisher vorherrschenden Verhaltensweise verdeutlicht. Die Europäer werden große Anstrengungen unternehmen müssen, dem Eindruck entgegenzuwirken, dass sie auf die militärischen Auseinandersetzungen des 21. Jahrhunderts nur mit den Streitkräften des 20. Jahrhunderts reagieren können.

Der Umbau der Dispositive auf der Basis der neuen konzeptionellen Schwerpunktsetzungen wird selbst dann nicht obsolet sein, wenn asymmetrische Bedrohungen künftig stärker hervortreten werden. Solange Streitkräfteüberlegenheit sinnvoll ins Spiel gebracht werden kann – und das ist selbst in vielen Szenarien der Terrorismusbekämpfung der Fall – wird die neue Grundkonzeption der Dispositive nicht an Wert verlieren.

NCW als konzeptionelle Klammer

Die bisher erzielten Ergebnisse und die Art ihrer Umsetzung, vor allem aber die inhaltlichen Schwerpunktsetzungen lassen auf Allgemeingültigkeit des Orientierungsrasters von NCW schließen. Netzwerkzentrierte Vorgehensweisen im Krieg würden damit in einem generellen Anwendungskontext, d.h. unabhängig vom Kriegsbild, verbindlich sein. Die in der praktischen Anwendung erbrachten Nachweise, vor allem aber die Ergebnisse, die in Kriegshandlungen erreicht werden konnten, sprechen eindeutig für diese Einschätzung. Was bereits vorliegt bzw. noch bearbeitet wird, bestätigt, dass der richtige Weg eingeschlagen wurde und dieser weiter beschritten werden muss.

Es ist mehr als wahrscheinlich, dass es in Anbetracht dieser Nachweise zu einer Konsolidierung der Entwicklungsstrategien kommt. Dafür spricht auch die inhaltliche Konsistenz des verfolgten Grundgedankens, der darauf abzielt, dem netzwerkzentrierten Prinzip des Fähigkeitsverbunds in neuen Zuordnungen zum Durchbruch zu verhelfen. Im gleichen Sinn stabilisierend wirkt die aufgrund der Unentbehrlichkeit informationsgeprägter Lösungsansätze notwendige Einbindung in ein Entwicklungsumfeld. Dieses wird von den generell trendbestimmenden Innovationen der „Informationstechnischen Revolution“ geprägt. Durch die Netzwerkzentrierung des Konzepts werden Voraussetzungen geschaffen, die es erlauben, aus diesem Bereich weitere Fähigkeitszugewinne zu beziehen, ohne dass es zu konzeptionellen „Brüchen“ kommt. Gleichzeitig bedeutet das aber ganz offensichtlich auch das Verbleiben von NCW im Mainstream der Entwicklungen, deren Nutzungsmöglichkeiten unser Zeitalter prägen. Diese Sachverhalte wirken zweifellos im Sinne einer verstetigenden Konsolidierung

des gesamten Programmansatzes, was eine dauerhafte Umorientierung der Befähigung zur Kriegführung impliziert.

Hinsichtlich der Nutzung entwicklungsbedingter Ressourcen entstehen durch die zunehmende „Informationsprägung" der High-Tech-Kriegführung – speziell auch im Hinblick auf Überlegenheitswahrung – besonders große Anforderungen. Netzwerkzentrierte Formen des Krieges verdeutlichen dies in exemplarischer Weise. Die Funktionalitäten, um die es dabei geht, werden bestimmt von Informationsüberlegenheit und ihrer konsequenten Umsetzung in vielfältigen technisch-funktionalen, verfahrens- und operationsbezogenen Zuordnungen. Die Möglichkeiten, diesen vernetzten Fähigkeitsverbund in Einsatzüberlegenheit (z.B. in Form schnell umsetzbarer Kampfkraftvorsprünge) zu überführen, sind in diesem Zusammenhang ausschlaggebend.

Die Schlüsselrolle informationsgeprägter Entwicklungen bei der Formierung konzeptioneller Dispositive darf keinesfalls außer Acht gelassen werden. Das Operationalisierungskonzept der netzwerkzentrierten Kriegführung bietet einen Bezugsrahmen, der diesen Anforderungen gerecht wird. Eine konsequente Nutzung der Möglichkeiten wird angesichts der Bedeutung der Entwicklungen und der daraus für die Umsetzung resultierenden Sachzwänge notwendig. Zum einen werden mit dem konzeptionellen Raster die Voraussetzungen dafür geschaffen, Innovationen in größtmöglichem Umfang einzubeziehen und davon Gebrauch zu machen. Zum anderen bietet das Dispositiv die Möglichkeit, die verschiedenen Entwicklungen unter einem gemeinsamen konzeptionellen Dach zusammenzufügen. Der Bezugsrahmen, der netzwerkzentrierter Kriegführung zugrunde liegt, wirkt demnach in einem erweiterten Einzugsbereich der „Informationsprägung" strukturbildend. Das Orientierungsraster von NCW ist deshalb dafür prädestiniert, konzeptionelle Lücken einer „Kriegführung des Informationszeitalters" zu schließen.

Zivile und militärische Bedeutung der Vernetzung

Netzwerkzentrierte Kriegführung bietet sehr unterschiedliche Möglichkeiten der inhaltlichen Strukturierung. Dies wird nicht zuletzt durch die Begriffswahl und die Orientierungen, die diese beinhalten, unterstrichen. Wichtige Zuordnungen ergeben sich bereits aus der Charakterisierung des konzeptionellen Dispositivs als „netzwerkzentriert", was Assoziationen mit Begriffen wie Networking oder vernetztem Denken und Handeln weckt. Diese Zuordnung darf nicht vernachlässigt werden, wenngleich die Umsetzung über Netzwerke – also die instrumentellen Aspekte des Begriffs – sicherlich im Vordergrund stehen.

Dem Wortsinn gemäß wird man NCW als „Kriegführung in, mit und gegen Netzwerke" beschreiben können. Dieses komplexe Einsatzdispositiv entspricht auch den Erfordernissen und Realisierungsmöglichkeiten, auf die das Konzept ausgerichtet ist. Bestandteile dieser Zuordnung sind natürlich auch die verschiedenen begrifflichen Assoziationen, die im Kern den „Verbundgedanken" – und damit im wesentlichen den Fähigkeitsverbund in seinen vielfältigen Konkretisierungen – betreffen. Dabei stehen instrumentellen Aspekte „systemischer" Lösungsansätze für vernetzte Fähigkeiten – auch in Form von „Netzwerken" – im Mittelpunkt.

Vernetztes Denken und Handeln werden im Zusammenhang mit Neuorientierungen sicherlich ihren Realitätsbezug behalten. Für die Verhaltens- bzw. Handlungsweisen in Kriegen

war die Berücksichtigung von Zusammenhängen und Wechselbeziehungen immer schon von ausschlaggebender Bedeutung. Nicht ganz selbstverständlich ist jedoch, dass inzwischen kriegsbedingtes Handeln aufgrund der Mittel und Verfahren, die im wesentlichen der „Informationstechnischen Revolution" zu verdanken sind, unter grundsätzlich veränderten Voraussetzungen erfolgreich gestaltet werden kann. Dieser Wandel ist fundamentaler Art. Er betrifft ein breites Spektrum von Ressourcen, die Vorteile sicherstellen können, darunter jedoch vor allem diejenigen, die sich durch ihre „Informationsprägung" auszeichnen.

Damit kommt zum Ausdruck, dass die aussichtsreichsten Nutzanwendungen aus der Aktivierung informationstechnischer Innovationen resultieren. Hervorzuheben sind in diesem Zusammenhang die grundlegenden Verbesserungen der Fähigkeitsprofile von Instrumentarien und Verfahrensweisen, wobei Leistungssteigerungen bei Beschaffung, Aufbereitung und Management großer Datenmengen eine zentrale Rolle spielen.

Die neuen Möglichkeiten, die damit für vernetzte Vorgehens- und Verfahrensweisen entstehen, sind natürlich keineswegs nur militärisch determiniert, sondern betreffen das erfolgsorientierte interaktive Handeln im Allgemeinen und die „systemischen" Umsetzungsarten dieser Nutzungsprofile im Besonderen. Von großer Bedeutung sind hier Netzwerke mit technisch-funktionaler, organisatorischer und/oder strukturierender Zuordnung. Systemlösungen für Korrelate dieser Art beinhalten wichtige synergiebedingte Optimierungsmöglichkeiten – nicht zuletzt unter Zugrundelegung des Verbundgedankens für militärisch relevante Fähigkeitsprofile (z.B. in Form aufgabenspezifischer generischer Lösungsansätze für verbundene Fähigkeitsprofile).

Systemlösungen für Netzwerkarchitekturen werden heute in vielfältigen Anwendungsbezügen sowohl zivil als auch militärisch genutzt. Dabei kommen vor allem die enormen Fortschritte auf den Gebieten Datenübertragung und -verarbeitung zum Tragen, die teilweise über weltraumgestützte Systemarchitekturen wirksam werden. Weltweit nutzbare Informations- und Datennetze eröffnen längst neue Dimensionen der Teilhabe an Informations- und Wissensressourcen oder auch an anderen informationsgeprägten Dienstleistungen.

In militärischen Anwendungen ermöglichen Netzwerke mit weiträumiger kommunikativer Funktionalität neue Formen der dezentralen Generierung, Nutzung und Absicherung von Fähigkeiten. Dabei bestehen ausgezeichnete Voraussetzungen für die Realisierung synergiebedingter Fähigkeitszuwächse bzw. Effizienzsteigerungen im Rahmen von Verbundlösungen. Weiträumig operationalisierbare Netzwerkarchitekturen eröffnen darüber hinaus die für Neukonzeptionen der Kriegführung so wichtigen Möglichkeiten, große Interaktionsräume auf der Grundlage von „Information and Asset Sharing" zu erschließen.

In entsprechend angepasster Form bestimmen vernetzte Nutzanwendungen – ebenfalls unter Einbezug von Netzwerken – auch schon längst das Geschehen im zivilen Bereich. Einschlägige Beispiele liefern die großen Wirtschaftsakteure. Sie nutzen in sehr unterschiedlichen Zuordnungen die Möglichkeiten dezentral strukturierter Verbundlösungen, um im Konkurrenzkampf bestehen zu können. Dass sie dabei oft gezielt von Informations- bzw. Wissensvorsprüngen Gebrauch machen, gehört ebenfalls zum gewohnten Erscheinungsbild. Die Verhaltens- und Verfahrensweisen dieser Akteure – auch die grundsätzlichen Funktionalitäten der ihnen zugänglichen Instrumentarien der Informationsinfrastruktur – unterscheiden sich in

weiten Bereichen nicht von denen der militärischen Bedarfsträger, wenn diese unter netzwerkzentrierten Bedingungen handeln.

Synergieeffekte durch Systemzuordnung im Verbund

Netzwerkzentrierte Kriegführung baut auf Bekanntem auf. Ihre Operationalisierungsformen sind allerdings noch mehr als andere darauf ausgerichtet, Fähigkeiten gemäß den bewährten Grundsätzen des auf Synergieeffekte abzielenden Fähigkeitsverbunds zu generieren, umzusetzen und abzusichern. „Netzwerkzentrierung" eröffnet Möglichkeiten, den Verbundgedanken auf neuer konzeptioneller Grundlage aufzugreifen und in zweckdienlichen, den Erfordernissen besser angepassten funktionalen Zuordnungen zu verwirklichen. Dies bedeutet auch, dass auf andere Weise nicht zugängliche Optimierungsmöglichkeiten (z.B. durch Systemzuordnungen im Verbund) erschlossen werden.

Der Neuformierung von Verbundlösungen auf funktionaler Grundlage sind freilich Grenzen gesetzt, wenn im jeweiligen Lösungsansatz hauptsächlich Aggregierungen von Fähigkeitsprofilen (wie etwa im Fall von Großwaffensystemen) berücksichtigt werden, die – weil vielleicht nicht „auflösbar" – nicht den Optimierungsgrundsätzen entsprechen. „Nichtauflösbarkeit" von Aggregierungen – gleichgültig ob erzwungen oder nicht – kann auch unter Gesichtspunkten der Absicherung von Fähigkeiten zu Nachteilen führen. Dies gilt vor allem für verbleibende funktional hoch aggregierte Einzelplattformen, die nicht zuletzt wegen ihrer meist beträchtlichen Wertkonzentration in vielfältiger Form Angriffe auf sich ziehen könnten. Aus diesen Gefährdungen – das Beispiel von Saturierungsangriffen mit „Billigwaffen" soll hier erwähnt werden – kann eine empfindliche Schwächung der High-Tech-Dispositive resultieren, der allenfalls mit sehr hohem Aufwand begegnet werden kann.

Die sich anbietenden Möglichkeiten einer Umformierung der Dispositive sollten konsequent genutzt werden. Dazu gehört nicht zuletzt, „funktionale Entflechtungen" (evtl. mit anschließender Neuformierung in einem geeigneten Verbund) vorzunehmen, wenn immer die Voraussetzungen dafür gegeben sind. Daneben sollten auch Optionen einer räumlichen Trennung (wenn möglich und geboten auch einer Neuvernetzung) der Bestandteile des Fähigkeitsaggregats genutzt werden.

Netzwerkgebundene Transformationen der beschriebenen Art orientieren sich an den Grundstrukturen des Sensor-Decider-Shooter-Komplexes. Besonders wichtig ist die Auftrennung und Neuorientierung der Bestandteile bei technisch-funktionalen Agglomeraten (z.B. komplexen Waffensystemen). Bei Zielbekämpfungssystemen resultiert vor allem aus der Sensor-Shooter-Entkopplung ein breites Spektrum von Systemzuordnungen. Dabei spielen räumlich getrennte Operationalisierungsmöglichkeiten der funktionalen Bestandteile in vernetzten Zuordnungen eine große Rolle, z.B. durch die Abtrennung von Zielaufklärung, Zielerfassung usw. von der Waffe bzw. der Waffenplattform. Neuformierungen, die den Zuordnungsbereich der Führung, Nachrichtengewinnung, Überwachung und Aufklärung (C4ISR) betreffen, sind Kernbestandteile effizienzsteigernder Weiterentwicklungen, die netzwerkzentrierte Streitkräftedispositive prägen.

Die Erzeugung synergiebedingter Zugewinne durch den Verbund von Fähigkeiten in vernetzten Strukturen – was meist den Verbund von Netzwerken bedeutet – wird die weitere

Entwicklung immer mehr bestimmen. Die Umformierung funktionaler Zuordnungen mit Hilfe geeigneter Netzwerkarchitekturen wird die Kriegsbilder der Zukunft nachhaltig prägen. Plattformzentrierte Kriegführung wird dabei in der Tendenz zurückgedrängt werden, netzwerkzentrierte Kriegführung dafür um so mehr hervortreten. Dabei ist die wachsende Bedeutung weiträumig operationalisierbarer Netzwerke besonders hervorzuheben. Vor allem Funktionalitäten in erweiterten räumlichen Dimensionen „auszulagern", neu zu verknüpfen und im Verbund wirksam werden zu lassen, hat erhebliche Konsequenzen, denn es ergeben sich daraus Möglichkeiten der Streitkräfteoperationalisierung und des Waffeneinsatzes in erheblich vergrößerten Interaktionsräumen, die Kernbestandteile der Abstandskriegführung darstellen.

Informationsgewinnung bestimmt Leistungsfähigkeit des Verbunds

Im Kontext wirkungsbezogener Streitkräfteoperationalisierungen werden die Fähigkeitsprofile durch drei Aspekte bestimmt. Man unterscheidet die jeweils miteinander verbundenen bzw. vernetzten Bereiche Informationsgewinnung (Systemverbund Nachrichtenwesen, Nachrichtengewinnung und Aufklärung), Führung (Battle Management, Einsatzmanagement) und Einsatz (Wirkungsverbund von Kräften, Mitteln und Verfahren). Die abzudeckenden Funktionalitäten lassen sich auch in den technologischen Konkretisierungen in segmentierter Form abbilden, woraus ein „geschichteter" Zuordnungsverbund von Netzwerken aus drei Bestandteilen entsteht.[4] Die Teilnetzwerke repräsentieren in ihren funktionalen Zuordnungen die Besonderheiten der die netzwerkzentrierte Kriegführung beherrschenden „Informationsprägung", d.h. die Generierung eines im Prinzip kontinuierlichen Informationsflusses, die schrittweise „Abarbeitung" und schließlich die Umsetzung in Form von Führungsentscheidungen und unmittelbar operationsbezogenen Maßnahmen, die eine Optimierung des Streitkräfte- und/oder Waffeneinsatzes ermöglichen. Dadurch entsteht dass eine Zuordnungsstruktur mit sequentiell abzudeckenden Aufgabenfeldern. Ausschlaggebend ist dabei die für serielle Verknüpfungen typische Abhängigkeit der Fähigkeitsentfaltung eines Zuordnungsbereichs vom Leistungsergebnis des „vorgeschalteten" Bereichs. Die jeweils vom Prinzip der „Eingangssteuerung" bestimmten Prozessabfolgen wirken in genereller Weise hierarchisch strukturierend, d.h. die Hierarchisierung kommt sowohl in der Gesamt-Netzwerkarchitektur als auch in ihren Teilnetzen zum Tragen.

Welche Möglichkeiten die Operationalisierungsformen netzwerkzentrierter Dispositive bieten, hängt darüber hinaus entscheidend von der Leistung des kommunikativen Verbunds in den verschiedenen Zuordnungen der Architektur ab.[5] Dabei ist zu berücksichtigen, dass die beschriebene modellhafte Grundstruktur in Wirklichkeit sehr viel komplexer ist und u.a. auch Rückkopplungsschleifen aufweist. Praxiserfahrungen machen insbesondre deutlich, dass dem „Eingangssegment" Informationsgewinnung eine Schlüsselrolle zukommt. Das in diesem Zuordnungsbereich erzielbare Ergebnis ist ganz offensichtlich ausschlaggebend für die Leistung in den nachfolgenden Bereichen und bestimmt damit die Leistungsfähigkeit des gesamten

[4] Im angelsächsischen Sprachgebrauch: „Sensor Grid", „Command and Control Grid", „Engagement/Shooter Grid".

[5] Siehe hierzu die Ausführungen von Martin Neujahr zur wirkungsorientierten Operationsführung in diesem Band.

Dispositivs. Deshalb werden Neuorientierungen der Kriegführung werden schwerpunktmäßig in diesem Segment ansetzen müssen. Erst ein Informationsaufkommen, das hinsichtlich Umfang, Qualität, Vollständigkeit und Schnelligkeit der Erstellung höchsten Ansprüchen genügt, wird (nach „führungsgerechter" Aufbereitung) für die angestrebten Leistungssteigerungen im Führungsverbund sorgen können. Fähigkeitszuwächse in diesem Teilbereich sind wiederum eine Voraussetzung dafür, dass die Streitkräftedispositive in optimaler eingesetzt werden können. So entscheidet sich bereits in diesem Segment, ob die Voraussetzungen für Kriegführungen unter Bedingungen von Informationsüberlegenheit (z.B. unter Prämissen überlegener Battlefield Awareness) geschaffen, umgesetzt und behauptet werden können.

Für die Möglichkeiten der Bedarfsabdeckung durch NCW ist es, im Hinblick auf die Erfordernisse unterschiedlicher Kriegsbilder erfolgsentscheidend, im Bereich der Informationsgewinnung höchste Leistungsstandards zu verwirklichen. Während sich in mehr oder weniger symmetrischen Konstellationen der Kriegführung Möglichkeiten der Leistungssteigerung in diesem Segment (vorwiegend auf High-Tech-Grundlage) abzeichnen, die sich auch durchsetzen lassen, gilt dies nicht ohne weiteres für Szenarien, in denen der Gegner – vielleicht sogar in sehr extremer Form – von asymmetrischer Kriegführung Gebrauch macht. In diesem Fall interessiert vor allem die Entwicklung von Leistungsprofilen, die den Erfordernissen militärischer Einsätze bei der Terrorismus-Bekämpfung entsprechen. Die Besonderheiten des verdeckten Kampfes, die hier im Mittelpunkt stehen, erfordern andere, mehr auf nachrichtendienstliche Aktivitäten setzende Verbundlösungen. Naturgemäß muss in solchen Bedarfsszenarien stets mit dem Verbleiben vergleichsweise großer „Aufklärungslücken" gerechnet werden, aus denen dann zwangsläufig Einsatzlimitierungen der Streitkräfte resultieren. Durch die Weiterentwicklung vernetzter Mittel und Verfahrensweisen erschließen sich freilich auch hier neue, aussichtsreiche Möglichkeiten, wie Beispiele im Afghanistan-Krieg zeigen.

Defizite, Pannen und Performance-Schwächen bei der Beschaffung relevanter Informationen sind jedoch auch in anderen Szenarien nie völlig auszuschließen. Das gilt auch für Fälle, bei denen die Voraussetzungen für massiven High-Tech-Einsatz gegeben sind. Einschlägige Beispiele liefern die immer wieder auftretenden Unzulänglichkeiten bei der Freund-/Feind-Identifizierung oder die mitunter eklatanten Fehlleistungen bei der Zielaufklärung bzw. der Erfassung von Zielen (mit negativen Folgen für die Zielbekämpfung). Hochentwickelte NCW-Dispositive bieten gleichwohl die besten Voraussetzungen für einschlägige Korrekturen. Auch dies wird, was die Zielbekämpfung anbelangt, zwar keine „fehlerfreie" Leistung gewährleisten. Dem bewährten Grundsatz des fokussierten, unnötige Schädigungen vermeidenden Waffeneinsatzes wird damit jedoch sicherlich noch besser entsprochen werden können.

Führungsunterstützung übersetzt Informationsüberlegenheit in Führungsüberlegenheit

Im NCW-Rahmen werden die Fähigkeitsprofile vor allem dann erheblich aufgewertet, wenn die Voraussetzungen für das Wirksamwerden eigener Informationsüberlegenheit gegeben sind. Falls diese Überlegenheit nicht von Anfang an besteht, wird sie „nachträglich" (mit Hilfe prioritär darauf ausgerichteter Kampfhandlungen, wie z.B. Informationsoperationen) hergestellt werden müssen. Bei der letztgenannten Zuordnung handelt es sich um eine zeitlich vor-

gezogene Kriegsphase, deren Ergebnis vorentscheidende Auswirkungen auf den weiteren Verlauf der Kampfhandlungen haben kann. Netzwerkzentrierte Kriegführung ist dadurch gekennzeichnet, dass Informationsüberlegenheit (vielleicht auch Informationsdominanz) in „Führungsüberlegenheit" transformiert wird und daraus schließlich durchschlagende Einsatzvorteile in den Bereichen Streitkräfteoperationalisierung und Waffeneinsatz erwachsen. Die Fähigkeitszugewinne, die durch den „Kampf um und mit Informationsüberlegenheit" zu erzeugen, umzusetzen und abzusichern sind, werden ebenfalls in Abhängigkeit des Kriegsbilds variieren. Die Operationalisierung netzwerkzentrierter Ansätze sorgt dabei jedoch immer für einen gewissen Ausgleich.

Ob die NCW-Fähigkeitsprofile tatsächlich hohen Ansprüchen genügen können, hängt neben dem Aspekt der Informationsüberlegenheit auch sehr stark von den Optimierungsmöglichkeiten im Segment der Führungsunterstützung ab. Dabei kommt es zunächst darauf an, den Datenstrom in „führungsgerechter Form" aufzubereiten. Dies setzt die Ausfilterung relevanter Daten und ihre „Fusion" voraus. Zwar können hier technische Mittel und Verfahren verstärkt eingesetzt werden, doch wichtige Komponenten fehlen noch immer oder weisen Defizite im Leistungsvermögen auf.[6] Das gilt vor allem für die zeit- und lagegerechte Zusammenführung des erstellten „Datenwissens" mit dem Expertenwissen der militärischen Operateure. Angesichts der Wichtigkeit dieses Funktionsbereichs, sind große Anstrengungen zu seiner verfahrensmäßigen Abdeckungen gerechtfertigt. Allerdings bleibt es ungewiss, ob der Aufwand zur Erarbeitung der technisch-funktionalen Grundlagen ausreicht, denn es ist auch weiterhin davon auszugehen, dass die Bereitstellung richtiger Informationen nicht zwangsläufig zu richtigen Entscheidungen führt.

Gleichwohl bieten NCW-Ansätze die Möglichkeit, beim Streitkräfte- und speziell auch beim Waffeneinsatz bislang nicht zugängliche Operationalisierungsvorteile zu nutzen. Militärisch relevant ist vor allem die räumliche Ausdehnung lagegerechter „Informationsteilhabe" (Shared Situational Awareness). Diese Entwicklung begünstigt insbesondere im Kontext von Abstandsfähigkeiten die vereinheitlichende Zusammenführung der ursprünglich den Teilstreitkräften individuell zugeordneten Interaktionsräume. Damit gewinnt der Aspekt einer dominanten aufgabenorientierten Zuordnung der Einsatzprofile von Streitkräften – auch mit Folgen für die Begründungszusammenhänge von Jointness – für die Kriegführung zweifellos an Bedeutung.

Schlussfolgerungen

Auch in den USA sind weiterhin große Anstrengungen erforderlich, um die schrittweise eingeleitete Transformation der Streitkräfte umzusetzen. Nach wie vor steht das „plattformorientierte Denken" im Vordergrund, und die Sachzwänge, die aus der Forderung nach mehr Jointness resultieren, werden von den Teilstreitkräften unterschiedlich beurteilt. Gleichwohl spricht vieles dafür, dass mit fortschreitender NCW-Entwicklung auch in diesen Sachbezügen die Chancen einer Durchsetzung überwiegen. Vor allem kann die kooperative, von der Art der

[6] Diesbezüglich sei auf die Entwicklungen im Bereich der Experten- und Entscheidungsunterstützungssysteme hingewiesen.

Aufgabe bestimmte Grundorientierung des Kräfte- und Mitteleinsatzes viel zur Harmonisierung partikulärer Streitkräfteinteressen beitragen.

Das Festhalten an High-Tech-Überlegenheit ist zweifellos unverzichtbar, wenngleich die Risiken der Übertechnisierung und die Gefahr, von Low-Tech-Kriegführung unterlaufen zu werden, in diesem Zusammenhang stets eine wichtige Rolle spielen. Notwendig ist nicht zuletzt auch die Orientierung des Grundkonzepts netzwerkzentrierter Kriegführung am oberen Ende des technisch Machbaren, zumal sich damit die Nutzung der an Multiplikator-Effekten reichen Ergebnispalette der „Informationstechnischen Revolution“ verbindet.

Es spricht viel dafür, dass speziell in weiter geführten Entwicklungen ein Ergebnis erreicht werden kann, das der idealtypischen Konfiguration von „Kriegführung im Informationszeitalter“ entspricht. Dies in Rechnung zu stellen, ist von grundsätzlicher Bedeutung und sollte deshalb auch für die europäischen Partnerstaaten verpflichtend sein. Das gilt zumal dann, wenn diese Staaten ihre Ambitionen im Sicherheitsbezug künftig extensiver definieren.

Burkhard Theile

Transformation: Veränderte Streitkräfte und neue Rüstungstechnik

Die Mittel, mit denen wir unseren Wohlstand schaffen, sind die gleichen, mit denen wir Krieg führen, schreiben die Zukunftsforscher Alvin und Heidi Toffler in ihrem 1995 erschienenen Buch *War and Anti-War.*[7] Seit Beginn der achtziger Jahre finden revolutionäre Prozessveränderungen in kommerziellen und administrativen Bereichen statt, wie Fertigung mit „Just in Time"-Anlieferung, papierlose Konstruktion oder weltweite Botendienste mit Zustellungszeiten von 24 Stunden. Früher war die Information über den Bestimmungsort eines Paketes mit diesem fest verbunden, heute eilt diese Information der Sendung voraus, damit der weitere Transport schon vor der Ankunft am nächsten Umschlagplatz geplant werden kann. Informationen werden als Mittel der Wertschöpfung genutzt.

In den neunziger Jahren des letzten Jahrhunderts wurden unter dem Begriff „Revolution in militärischen Angelegenheiten" (RMA) in den USA intensive Strategiedebatten geführt, deren Ergebnisse in den Leitpapieren Joint Vision 2010 und später Joint Vision 2020 zusammengefasst wurden. Danach waren für die zukünftigen Streitkräfte Fähigkeitskonzepte in vier übergeordneten Kategorien zu entwickeln: Überlegener Kräfteeinsatz (Dominant Maneuver), Wirkung im Ziel (Precision Engagement), systemisches Schutzkonzept (Full Dimensional Protection) und bedarfsorientierte Logistik (Focused Logistics).

Eine wesentliche Komponente der Sicherheitsvorsorge der westlichen Welt sind schnell einsetzbare mobile militärische Kräfte mit streitkräftegemeinsamen Einsatzkonzepten. Streitkräfte der Zukunft werden fähigkeitsorientiert aufgestellt, und die militärischen Fähigkeiten werden systemisch erzeugt. Plattformen wie Flugzeuge und Panzer werden mit Aufklärungs- und Wirkmitteln zu einem Systemverbund vernetzt, der oftmals auch als System der Systeme bezeichnet wird. Der Systemverbund wird gemäß der jeweiligen militärischen Aufgabenstellung zusammengestellt.

Die Überführung klassischer Streitkräftestrukturen in fähigkeitsorientierte vernetzte militärische Kräfte wird als Transformation bezeichnet. Die Transformation hat Auswirkungen auf Doktrin, Organisation, Training, Ausrüstung, Führung, Personal und militärische Einrichtungen sowie die Rüstungsindustrie. Der Transformationsprozess der US-amerikanischen Streitkräfte ist bereits im Gang. Die NATO folgt den USA, und so beginnen die Bündnispartner, die Bundesrepublik eingeschlossen, ebenfalls ihre Streitkräfte zu transformieren. Ziel des vorliegenden Beitrags ist es, die Auswirkungen dieses Transformationsprozesses aufzuzeigen, um damit die Voraussetzung für einen sachgerechten Umgang mit transformationsbedingten Fragestellungen schaffen.

[7] Alvin Toffler and Heidi Toffler, *War and Anti-War* (New York: Warner Books, 1995).

Auslöser der Transformation

Sicherheitspolitische Herausforderungen und technologische Möglichkeiten sind die primären Treiber der Transformation mit Folgeeffekten im politischen und wirtschaftlichen Bereich.

Sicherheitspolitische Forderungen

Das sicherheitspolitische Umfeld für die deutschen Streitkräfte ist durch die im Mai 2003 erschienenen Verteidigungspolitischen Richtlinien (VPR) beschrieben.[8] Danach sieht sich die Bundesrepublik in eine multinationale sicherheitspolitische Vorsorge eingebunden. Militärische Einsätze, abgesehen von Evakuierungsaufgaben, werden grundsätzlich nur teilstreitkräfteübergreifend im Bündnis oder mit Partnern im Rahmen von UNO, NATO oder EU stattfinden. Die multinationalen Einsätze sind ein Beitrag zu den als Petersberg-Aufgaben bezeichneten sicherheitspolitischen Zielsetzungen der EU. Weiter hat sich die Bundesrepublik verpflichtet, 6.000 Soldaten für die neu geschaffene NATO-Eingreiftruppe (NATO Response Force, NRF) zur Verfügung zu stellen. Petersberg-Aufgaben und die Verpflichtungen im Rahmen der NRF können nur durch transformierte Streitkräfte wahrgenommen werden. In der "Weisung für die Weiterentwicklung der Bundeswehr" vom Oktober 2003 präzisiert der Minister die notwendigen Maßnahmen und gibt einen Zeitplan vor.[9]

Technologische Fähigkeiten

Die verfügbaren Technologien der Kommunikations- und Informationstechnik liefern die technischen Voraussetzungen für die Streitkräftetransformation. Große Datenmengen können transportiert und bearbeitet werden. Raumgestützte Infrastrukturen für Kommunikation, Nachrichtengewinnung, Navigation und Synchronisation ermöglichen weltweite Operationen. Leistungsfähige Sensoren können über große Entfernungen Szenarien in verschiedenen Spektralbereichen abbilden. Signalerfassende Sensoren können, durch Algorithmen gestützt, funkgestützte Kommunikation über große Entfernungen sammeln und aufklären. Nachrichtengewinnung und Aufklärung sind nahezu lückenlos möglich. Softwaretechnologien für Datenbanken und numerische Modelle werden für digitale Landschaftsmodelle, Umfeldbeschreibungen und Entscheidungsunterstützung eingesetzt. Bustechnologien ermöglichen Datentransporte mit großer Anpassungsfähigkeit an die jeweilig verfügbaren Übertragungswege.

Die Vernetzung von Plattformen, Sensoren, Effektoren und der Zugriff auf Hintergrundinformationen, wie Landschaftsmodelle und logistische Daten, bilden das Rückgrat transformierter Kräfte. In den USA wird der Einsatz transformierter Kräfte als netzwerkzentrierte Kriegführung (NCW) bezeichnet, die Briten sprechen von netzwerkgestützten oder netzwerkgestärkten Fähigkeiten (Network Enabled oder Enhanced Capabilities, NEC) und die Schweden von netzwerkbasierter Verteidigung (Network Based Defense). Australien hat dafür den Begriff Network Enabled Warfare (NEW) entwickelt, die Niederlande arbeiten mit Network Centric Operations (NCO), und in der NATO spricht man entweder von Network Centric Ca-

[8] Siehe: <http://www.bmvg.de/pic/sicherheit/vpr_broschuere.pdf> (Zugriff: 29. Dezember 2003).
[9] Siehe: <http://www.bundeswehr.de/pic/pdf/Weisung.pdf> (Zugriff: 29. Dezember 2003).

pability (NCC) oder Network Enabled Collective Security (NECS). In Deutschland wird der Begriff Vernetzte Operationsführung (NetOpFü) benutzt.

Die Vernetzung ist ein geniales Verfahren zur Bearbeitung komplexer Problemstellungen. Vernetzte Systeme können in vielen Fällen hierarchische Strukturen teilweise oder ganz ersetzen. Ein klassischer Ansatz für die Lösung komplexer Probleme ist die hierarchische Strukturierung des jeweiligen Problems in überschaubare Arbeitspakete. Technisch können das Baugruppen und Einzelteile bzw. Systeme und Untersysteme sein. Gleichermaßen kennen wir die Hierarchie als Managementwerkzeug in Industrie, Verwaltung und beim Militär. Das hierarchische Verfahren ist durch sequentielle Abläufe, Informationsreduktion und hohen Zeitbedarf gekennzeichnet.

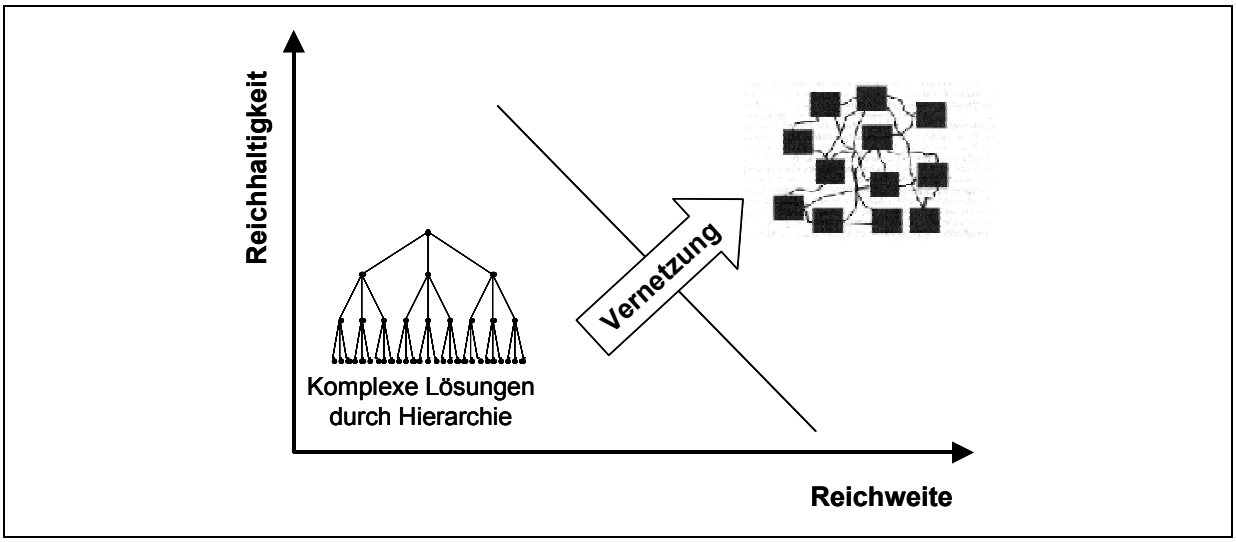

Abbildung 1: Auflösung des Reichweite-Reichhaltigkeitskompromisses durch Vernetzung

Der sequentielle Ablauf eines Vorganges im hierarchischen System ist aus dem täglichen Leben bekannt und unter der Bezeichnung Dienstweg nicht immer geschätzt. Die Hierarchie benutzt als Technik die Informationsreduktion. Die Summe des bei den Sachbearbeitern einer Firma residierenden Fachwissens ist wesentlich größer als das akkumulierte Fachwissen der oberen Führungsebene. Der Reichhaltigkeit des Fachwissens auf der Sachbearbeiterebene steht die Reichweite der Führungsebene gegenüber. Das Fachwissen auf der Führungsebene ist auf das für Führungsentscheidungen Wesentliche reduziert. In hierarchischen Systemen werden komplexe Aufgabenstellungen durch Kompromisse zwischen Reichweite und Reichhaltigkeit gelöst. Abbildung 1 verdeutlicht dies anhand einer Führungsspanne von drei Elementen. Jedes Element des hierarchischen Systems hat einen Punkt auf der Kompromisslinie. Die Sachbearbeitung oben links, die oberste Führung unten rechts, die Zwischenebenen dazwischen. Weitere Beispiele für Reichweite- und Reichhaltigkeitspaarungen sind Betriebsversammlung und Personalgespräch oder Buch und Plakat.

In einem vernetzten System braucht dieser Kompromiss nicht eingegangen zu werden. Die oberste Hierarchieebene kann auf reichhaltige Information der untersten Ebene selektiv zugreifen. Gleichermaßen können Elemente der hierarchischen Zwischenebenen direkt, d.h. ohne den aufwendigen Weg über die nächsthöheren Ebenen miteinander verkehren. Bei-

spielsweise hat in der Automobilzulieferindustrie die direkte Kommunikation zwischen Motorenherstellern und Aggregatzulieferern erhebliche Zeit- und Kostenersparnisse ermöglicht. Auch der sogenannte kleine Dienstweg in einer Hierarchie ist nichts anderes als eine Vernetzung, die zwar nicht vorgesehen, aber dennoch oftmals sehr effizient ist.

Der Nutzen der Vernetzung kann analytisch dargestellt werden. Nach einem von Metcalfe, dem Erfinder des Ethernets, formulierten Gesetz ist der Nutzen eines Netzes proportional zum Quadrat der Zahl der Knoten. Der Nutzen liegt auf der Hand, denn die Kosten eines Netzes steigen proportional zur Zahl der Knoten. Verdoppelt man die Zahl der Knoten, verdoppelt man die Kosten bei einer Vervierfachung des Nutzens. Abbildung 2 veranschaulicht diese Aussage.

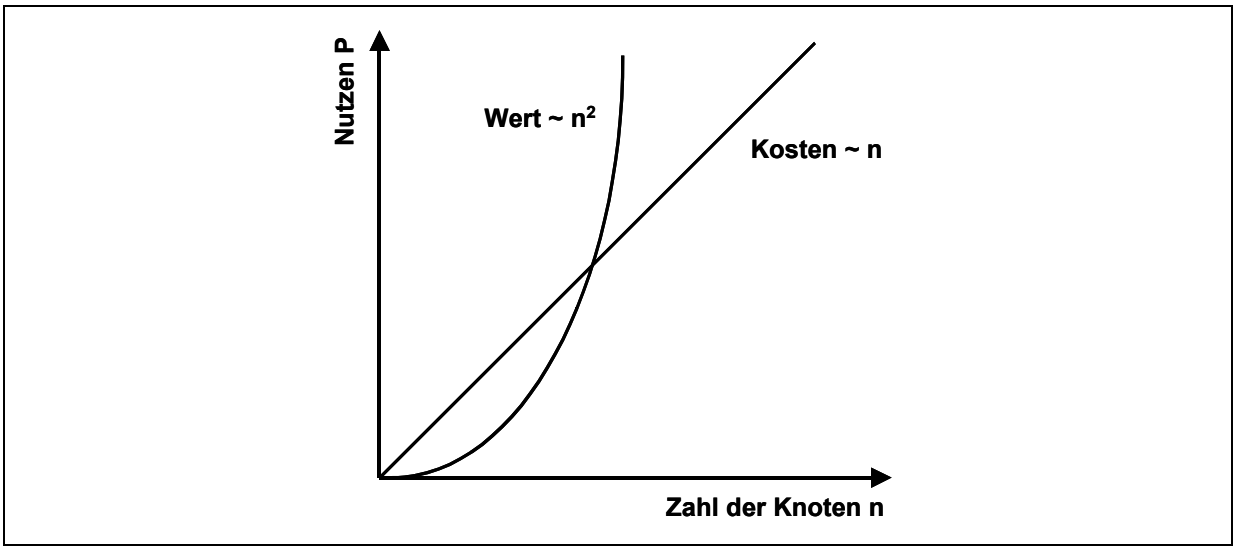

Abbildung 2: Nutzen und Kosten eines Netzes in Abhängigkeit der Knotenzahl

Als praktische militärische Anwendung betrachten wir eine vernetzte Flugabwehr. In Abbildung 3 ist schematisch dargestellt, wie miteinander kommunizierende Flugabwehrstellungen gegnerische Fluggeräte wirkungsvoll bekämpfen können. Bei unabhängig voneinander operierenden Systemen ist die Bekämpfung beider Eindringlinge nicht notwendigerweise gegeben. Die zum Systemverbund miteinander vernetzten Flugabwehrsysteme bieten mit geringerem Hardwareeinsatz einen besseren Schutz.

Das Prinzip der Transformation kann schon durch dieses vergleichsweise einfache Beispiel veranschaulicht werden. Die Fähigkeit zur Luftraumverteidigung wird durch vernetzte Sensoren und Effektoren hergestellt. Dabei können die Sensoren und die Feuereinheiten räumlich voneinander getrennt sein. Im vorliegenden Beispiel erzielt ein System von zwei vernetzten Einheiten ein besseres Ergebnis als drei unabhängig voneinander operierende Stellungen. Richtig genutzte Informationen erzeugen einen Mehrwert.

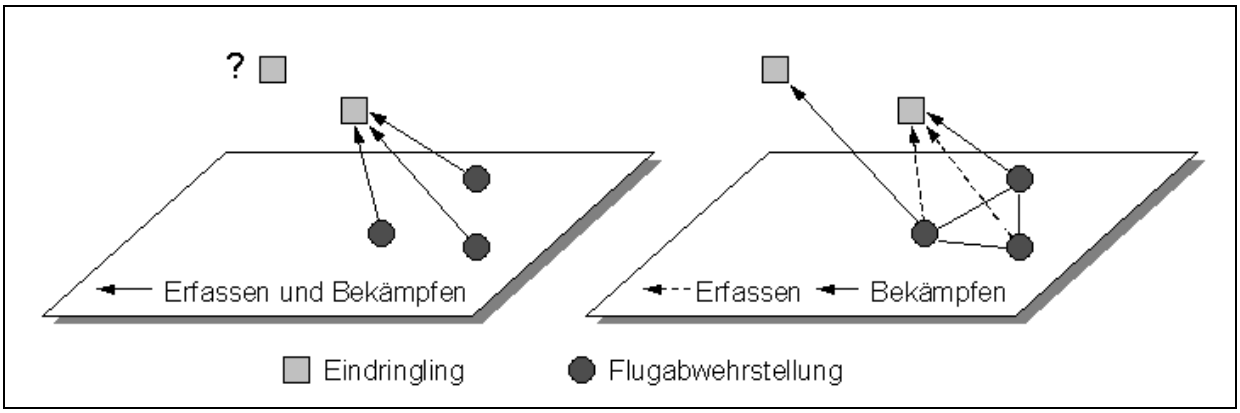

Abbildung 3: Vernetzte und nicht vernetzte Flugabwehr

Hinweis: Drei einzelne Flugabwehrstellungen (links) erfassen den näheren Eindringling und bekämpfen ihn. Im vernetzten System (rechts) werden beide Ziele durch nur zwei Stellungen bekämpft.

Politische Aspekte

Militärische Operationen werden von der Weltöffentlichkeit beobachtet und bewertet. Die öffentliche Meinung erteilt in den westlichen Ländern den Politikern das Mandat und erwartet militärische Erfolge bei minimalen, kriegerisch bedingten Zerstörungen. Der Verlust von Menschenleben ist grundsätzlich zu vermeiden, unabhängig von der Zugehörigkeit der Betroffenen zu Freund oder Feind. Das Vermeiden von Kollateralschäden setzt eine gute Lagekenntnis und eine präzise Waffenwirksamkeit voraus. Dies sind typische Eigenschaften transformierter Kräfte, wie wir im nächsten Abschnitt sehen werden. Im Umgang mit unerwarteten terroristischen oder militärischen Bedrohungen spielen schnelle und situationsgerechte militärische Gegenmassnahmen eine entscheidende Rolle. Die Transformation der Streitkräfte ist die Voraussetzung dafür, dass die verzugslose Handlungsfähigkeit hergestellt werden.

Wirtschaftliche Betrachtungen

Strikt bedarfsgesteuerte Logistik und präziser Waffeneinsatz transformierter Streitkräfte ermöglichen signifikante Einsparungen bei Material und Transport. Das einfache Beispiel der Flugabwehr hat gezeigt, wie durch Informationsmanagement Geräte eingespart werden können. Im vernetzten System leisten zwei Flugabwehrstellungen mehr als drei unvernetzt operierende. Darüber hinaus wird Munition eingespart. Die logistische Versorgung kann durch Vernetzung auf das sinnvoll Notwendige reduziert werden. Ersatzteile, Betriebs- und Kampfmittel können bedarfsgerecht vorgehalten werden, da ein logistisches „Lagebild“ existiert.

Transformation

Die Überführung eines hierarchischen Systems in ein anderes ist einfach darstellbar. Ausgangs- und Zielstruktur sind bekannt, wie wir das von Umorganisationen kennen. Die Streitkräftetransformation ist eine Überführung einer aus Teilstreitkräften, Truppengattungen, etc. aufgebauten hierarchischen militärischen Struktur in ein vernetztes System mit vorgegebenen

militärischen Fähigkeiten. Die Fähigkeitsorientierung ist ein wesentliches Paradigma der Transformation.

Wir haben den Einsatz vernetzter Strukturen in militärischen Einsätzen in Afghanistan und im Irak beobachten können. Berittene Beobachter übermittelten ihre Aufklärungsergebnisse direkt an Besatzungen von Kampfflugzeugen, und dies oftmals erst nach deren Start zum Einsatzflug. Mit kommunizierenden Knoten eines Netzwerkes können Fähigkeiten erzeugt werden, die ein hierarchisches System nicht liefern kann. Die Hierarchie ist statisch, das Netzwerk ist eine fallweise Konfiguration geeigneter Elemente zur Erzeugung aktuell gefragter Fähigkeiten. Transformation ist somit ein dynamischer Prozess. Transformierte Streitkräfte verfügen über systemisch hergestellte Fähigkeiten. Dabei können gleiche oder nahezu gleiche Fähigkeiten durch unterschiedlich zusammengesetzte Systeme erzeugt werden. Aufklärungsergebnisse können von einer Drohne, einem Kampfflugzeug oder einem Satelliten kommen. Die Bekämpfung kann durch Raketen, Artillerie oder Flugzeugeinsatz geschehen.

Es gibt viele unterschiedliche Definitionen des Begriffes Transformation. Die Transformation Planning Guidance des US-Verteidigungsministeriums erklärt den Begriff wie folgt:[10]

> Transformation ist ein Prozess, der der wechselnden Natur des militärischen Mit- und Gegeneinander durch neue Kombinationen von Konzepten, Fähigkeiten, Personen und Organisationen eine Form gibt, die die Überlegenheit unserer Nation nutzt und uns vor asymmetrischer Gefährdung schützt, um unsere strategische Position zu wahren, die dazu beiträgt, Frieden und Stabilität in der Welt zu festigen.

Die Transformation ruht auf den vier Säulen Technologie, operationelle Konzepte, institutionelle Veränderungen (z.B. Entscheidungsprozesse) und Finanzen. Sie betrifft alle Bereiche der Streitkräfte: Doktrin, Organisation, Training, Führung, Material, Personal und die Infrastruktur. Diese umfassende Transformation stellt auch die Rüstungstechnik vor neue und große Herausforderungen, denn die Leistungsfähigkeit vernetzter militärischer Systeme kann nicht durch bloße analytische Verfahren bestimmt werden, wie das bei der Konstruktion eines Fahr- oder Flugzeuges möglich ist. Das Rüstungsmaterial wird durch einen neuen Prozess der Konzeptentwicklung und Experimente (Concept Development and Experimentation, CD&E) ausgelegt, getestet und erprobt. Dieser Prozess ist komplex und setzt entsprechendes Grundverständnis seitens der wehrtechnischen Industrie voraus.

Transformierte Streitkräfte sind vernetzte teilstreitkräfteübergreifende Truppen, die in der Lage sind, schnelle entscheidende Operationen (Rapid Decisive Operations, RDO) an jedem Ort der Erde durchzuführen. Ihr übergeordnetes Handlungsprinzip ist das der wirkungsorientierten Operationen oder Effects Based Operations (EBO).[11] EBO nutzen zum Erreichen der strategischen Ziele das ganze Spektrum gegnerischer Verwundbarkeiten und Schwächen aus und verzichten nach Möglichkeit auf ein direktes Kräftemessen oder gar einen Zermürbungskrieg. EBO sind im gesamten strategischen Umfeld einsetzbar. Diese Vorgehensweise setzt

---

[10] Transformation Planning Guidance (Washington, D.C.: US Department of Defense, 2003), <http://www.oft.osd.mil/library/library_files/document_129_Transformation_Planning_Guidance_April_2003_1.pdf> (Zugriff: 15. Januar 2004).

[11] Siehe hierzu den Beitrag von Martin Neujahr in diesem Band und Edward A. Smith, *Effects-Based Operations. Applying Network Centric Warfare in Peace, Crisis, and War* (Washington, D.C.: CCRP Publications, 2003).

eine genaue Kenntnis des Gegners und der eigenen Möglichkeiten voraus. Diese Kenntnisse werden durch das Operational Net Assessment (ONA, Abbildung 4) gewonnen.

Der potentielle Gegner wird als komplexes System mit den Untersystemen Politik, Militär, Wirtschaft, Soziales, Infrastruktur und Information (Political, Military, Economic, Social, Infrastructure, Information, PMESII) analysiert. ONA bildet die Grundlage für alle Entscheidungen auf taktischer, operativer und strategischer Ebene. Die für den ONA-Prozess benötigten Daten sind in einer Datenbasis enthalten. ONA definiert Knotenpunkte (Nodes) und deren Rolle im gegnerischen System. Die ONA-Gesamtverantwortung liegt z.B. in den USA beim neu geschaffenen Standing Joint Forces Headquarters (SJFHQ), dessen Funktionsweise im nächsten Abschnitt beschrieben wird.

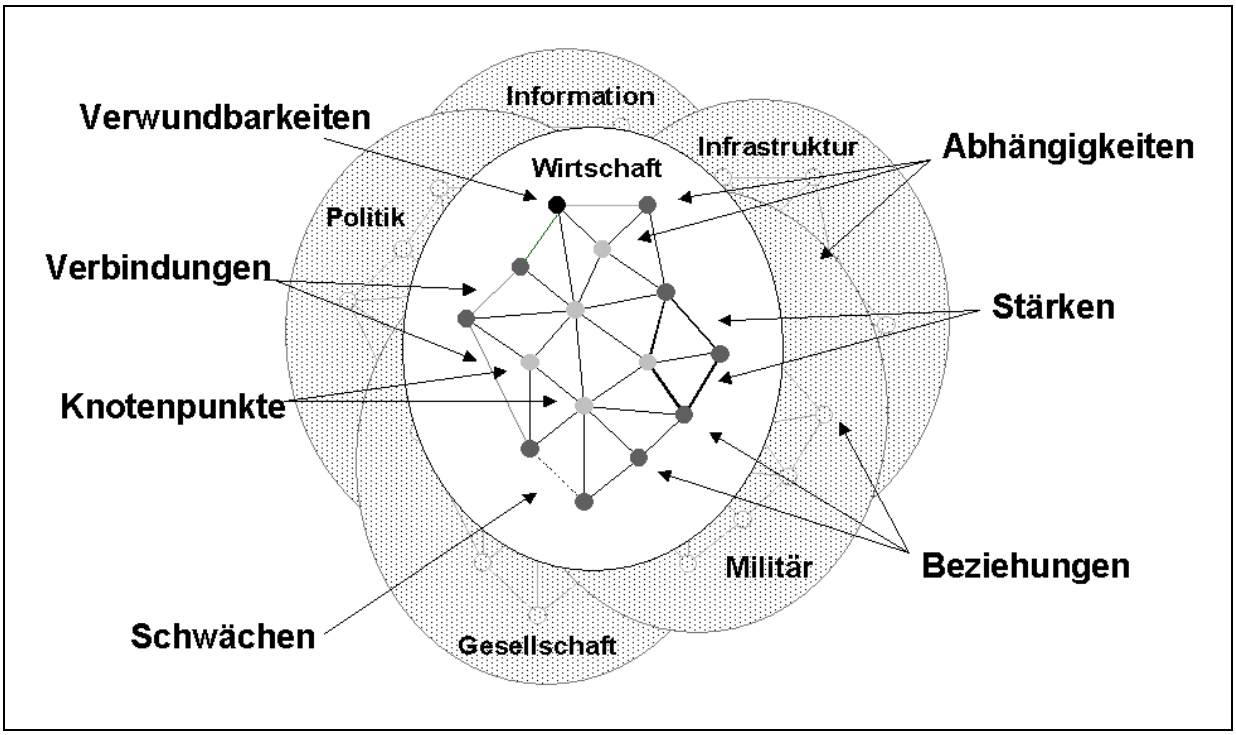

Abbildung 4: Operational Net Assessment-Analyse

Hinweis: ONA analysiert den Gegner als Systemverbund, um die wesentlichen Beziehungen, Abhängigkeiten und Verwundbarkeiten zu verstehen. Daraus werden Mittel bestimmt, um Fähigkeiten, Wahrnehmungen, Entscheidungsprozesse und Verhaltensweisen zu beeinflussen.

Der Systemansatz zur Bewertung der Stärken und Schwächen eines Gegners ist ein grundlegend neuer Ansatz der militärischen Planung (Abbildung 5). Durch den ONA-Prozess können Entscheidungen für bestes militärisches Handeln – im Sinne von EBO – vorbereitet werden. Zusammenfassend lässt sich somit sagen, dass transformierte Streitkräfte mehr sind als nur vernetzte Streitkräfte und qualitativ etwas anderes darstellen als der Kampf der verbundenen Waffen. Transformierte Kräfte nutzen Informationen und Zusammenhänge, die bei klassischen militärischen Operationen nicht zur Verfügung stehen.

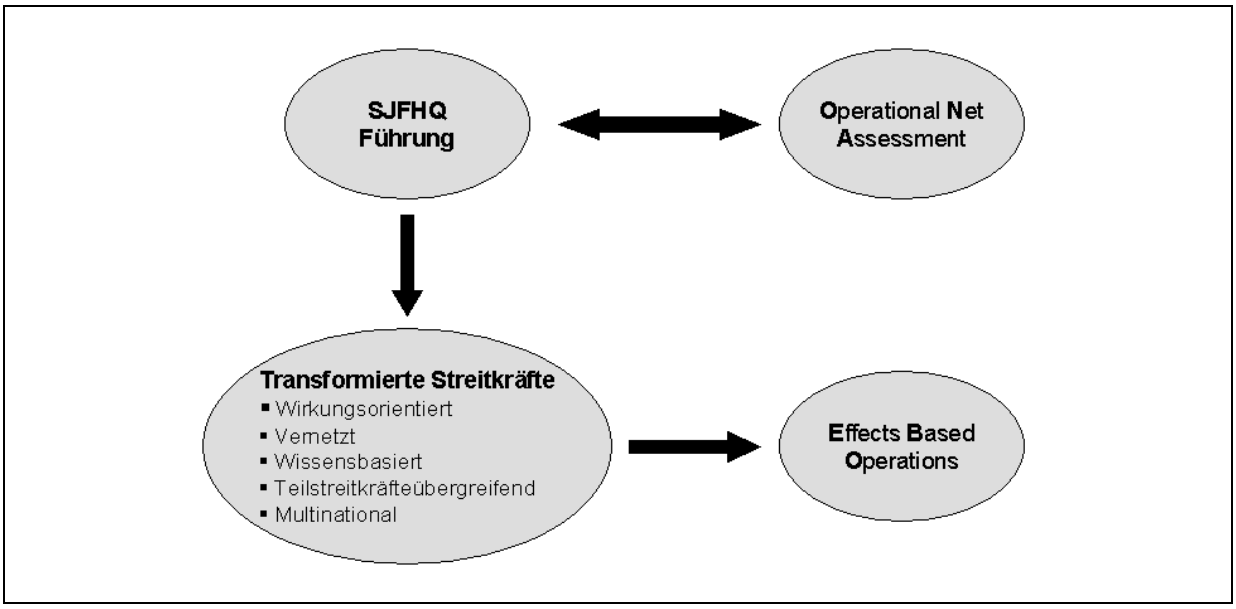

Abbildung 5: Zusammenspiel zwischen SJFHQ, ONA, transformierten Streitkräften und EBO

Transformation in den USA

Die USA sind im Transformationsprozess weit fortgeschritten. Für die Steuerung ist im Verteidigungsministerium das Office of Force Transformation eingerichtet worden, dessen Direktor direkt dem Verteidigungsminister berichtet. Die militärische Umsetzung erfolgt durch das US Joint Forces Command (USJFCOM), die rüstungstechnische Umsetzung geschieht durch die Defense Advanced Research Projects Agency (DARPA) und die Teilstreitkräfte.

Der Direktor für Streitkräftetransformation hat fünf übergeordnete Ziele festgelegt:[12]

- Transformation als Schlüsselelement der Strategie des Ministeriums und der nationalen Verteidigungsstrategie
- Grundlegende Veränderung der Streitkräfte und deren Kultur mit den Mitteln des Experimentierens, operationeller Prototypen und der Vermittlung neuer Kenntnisse und Erfahrungen
- Einführung von Network Centric Warfare (NCW) als Kriegstheorie des Informationszeitalters sowie als Organisationsprinzip für die nationale militärische Planung, teilstreitkräfteübergreifende Fähigkeitskonzepte und Systeme
- Einführung brauchbarer Regeln für Entscheidungen und Bewertung zur Anwendung im gesamten Bereich der Transformation
- Entwicklung oder Veranlassung der Entwicklung neuer militärischer Fähigkeiten zur Erweiterung der Fähigkeitsbasis und zur Risikominderung

Die US-amerikanische Streitkräftestruktur weist insgesamt neun Kommandos aus. Fünf regionale[13] und vier funktionale Befehlsbereiche. Einer dieser funktionalen Befehlsbereiche

[12] Siehe: <http://www.oft.osd.mil> (Zugriff: 16. Januar 2004).

[13] European Command (Stuttgart-Vaihingen), Pacific Command (Honolulu/Hawaii), Central Command (MacDill Air Force Base/Florida), Southern Command (Miami/Florida), Northern Command (Peterson Air Force Base/Colorado)

ist das USJFCOM in Norfolk, Virginia. Der derzeitige Befehlshaber dieses Kommandos ist Admiral Giambastiani, der in Personalunion auch das Allied Command Transformation (ACT) der NATO leitet. Das USJFCOM (Abbildung 6) mit seinen etwa 1.800 Soldaten wird als „Transformationslabor" der Streitkräfte bezeichnet.[14] Die Mission des USJFCOM ist die Maximierung der derzeitigen und zukünftigen Fähigkeiten der US-Streitkräfte. Dazu leitet es den Transformationsprozess teilstreitkräfteübergreifend mit den Mitteln der Konzeptentwicklung und des Experimentierens. Durch Aufstellung teilstreitkräftegemeinsamer Forderungen, ein teilstreitkräftegemeinsames Training und das Herstellen von Interoperabilität werden durch das USJFCOM transformierte Streitkräfte für Einsätze zur Verfügung gestellt.

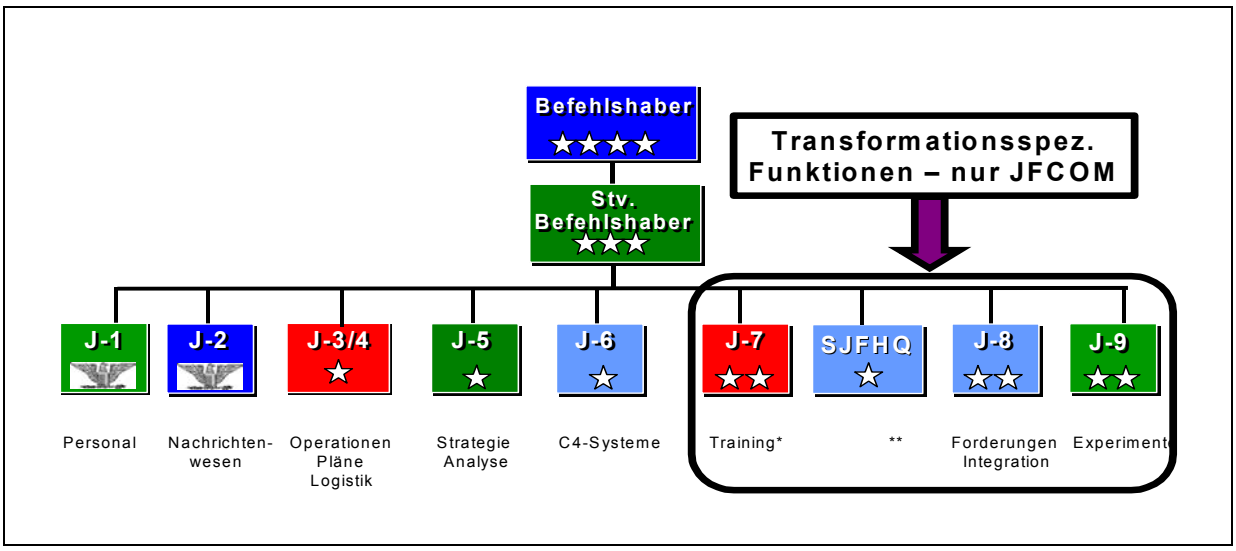

Abbildung 6: Struktur des US Joint Forces Command (USJFCOM)

Quelle: Präsentation von Adm Ed Giambastiani, Navy League Conference, Air, Land, Sea Expo, 16. April 2003.

Das USJFCOM soll die folgenden politischen Vorgaben für die Streitkräfte umsetzen:

- Reduzierte Kosten bei erhöhter Effizienz
- Global, flexibel und für verschiedene Operationen einsetzbar
- Kürzere Planungen und Durchführungen von Operationen durch verbesserte Verfahren und reduzierte Bürokratie
- Schaffen von Konzepten und Infrastruktur mit höherer Qualität (zuverlässig, flexibel, kompatibel, innovativ, mit modernster Technik), die auf den Endnutzer (Combatant Commander) abgestimmt sind
- Sicherstellen der Full Spectrum Dominance (FSD)
- Fördern neuer Ideen, die experimentell getestet werden können
- Bilden von voll kompatiblen Teilstreitkräften in eine neue JOINT-FORCE
- Betreiben eines kontinuierlichen Verbesserungsprozesses, der innovative Lösungswege fördert

[14] Siehe: <http://www.jfcom.mil> (Zugriff: 30. Dezember 2003).

Bis zum Fiskaljahr 2005 soll jeder der fünf regionalen Befehlsbereiche über ein Standing Joint Forces Headquarters (SJFHQ) verfügen. Das SJFHQ gewährleistet dem regionalen Befehlshaber eine permanente Führungsfähigkeit durch ONA und wirkungsorientiertes Planen (Effects Based Planning, EBP). Das SJFHQ stellt dem regionalen Befehlshaber umfangreiche Daten zur Verfügung, so dass er bei einer sich abzeichnenden Krise frühzeitig Maßnahmen ergreifen kann. Das Spektrum möglicher Handlungsweisen eines Befehlshabers wird dadurch wesentlich erweitert.

Das komplexe Szenario der Kriegführung mit transformierten Kräften wurde 2002 durch eine vom USJFCOM angelegte Großübung unter dem Namen Millennium Challenge 2002 (MC02) durchgespielt. Die Übung sollte zeigen, inwieweit die Streitkräfte schnelle entscheidende Operationen (RDO) durchzuführen in der Lage sind. Die Teilnehmer der Übung kamen aus den Teilstreitkräften, funktionalen und regionalen Kommandos, Organisationen des Verteidigungsministeriums und anderen staatlichen Behörden. Die Ergebnisse der Übung sind im einzelnen nicht bekannt. Über die Problemstellungen weiß man:[15]

- Festlegen der operativen Bedingungen für Rapid Decisive Operations
- Untersuchen von Konzepten wie gemeinsames relevantes operationelles Lagebild (Common Relevant Operational Picture, CROP) und gemeinsame interaktive Planung (Joint Interactive Planning, JIP)
- Festlegen teilstreitkräftegemeinsamer Führungsfunktionen und Fähigkeiten zur Nachrichtengewinnung, Überwachung und Aufklärung
- Herstellen einer umfassenden, zeitlich unbegrenzten Überlegenheit

Eine nächste Großübung soll im Jahre 2005 stattfinden. Inzwischen arbeiten die US-Teilstreitkräfte an der Transformation oder experimentieren mit Spezialeinheiten. Die US Army entwickelt das Future Combat System (FCS), das in der derzeitigen Form eine radikale Abkehr von der klassischen Heerestechnik und der Doktrin für Landstreitkräfte bedeutet. Das FCS befindet sich in der Entwicklungsphase und soll im Jahre 2010 einsatzfähig sein. Das operative Konzept ist in Abbildung 7 dargestellt und zeigt die Rolle der Teilstreitkräfte. Die schwarzen Linien kennzeichnen die Verbindungswege innerhalb des FCS, die grauen Verbindungen zeigen die teilstreitkräfteübergreifenden Kommunikationswege oder Schnittstellen zu Koalitionskräften. Die Kampftruppen sollen mit neu zu entwickelndem Gerät ausgestattet werden. Kampfkraft und Schutzfunktionen sollen durch vernetzte Sensoren und Effektoren auf hochmobilen Plattformen hergestellt werden.

[15] Für weitere Hinweise siehe: <www.jfcom.mil/about/experiments/mc02.htm> (Zugriff: 30. Dezember 2003).

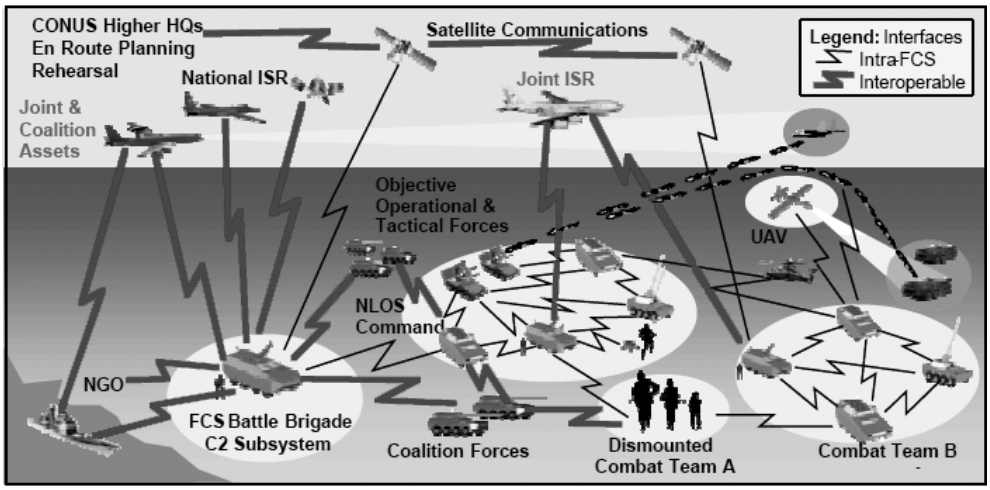

Abbildung 7: Operatives Konzept für das Future Combat System (FCS)

Quelle: Roy Minson and Steve Marion, „Future Combat Systems“, Folie 4, Präsentation an der A&D Conference, Airlington, 30. Oktober 2003 <http://www.boeing.com/defense-space/ic/fcs/bia/031104_arlington_briefings/031104_lsi.pdf> (Zugriff: 16. Januar 2004)

Die klassischen durch Panzerung hergestellten Schutzfunktionen sollen durch operative Konzepte ersetzt werden: Der Gegner muss erkannt und erfolgreich bekämpft werden, solange die eigenen Kräfte außerhalb der Reichweite seiner Waffen sind. Geht dieses Konzept nicht auf, so wird das Überleben durch weitere technologische und operative Maßnahmen gesichert. Dies setzt ein fehlerfreies Lagebild und sehr schnelle Handlungsabläufe voraus. Unabhängig davon, ob das US-amerikanische Konzept in der jetzt angedachten Form realisiert werden kann, werden die Grundelemente wie Vernetzung, Roboter und Beweglichkeit bestimmende Elemente zukünftiger Heerestechnik sein. Das FCS sieht verschiedene bemannte Fahrzeugvarianten in der 20-Tonnen-Klasse für Mannschaftstransport, Führung, Aufklärung und als Waffenträger für Kanonen und Mörser vor. Unbemannte Luftfahrzeuge und Bodenroboter werden zur Aufklärung und Nachrichtengewinnung eingesetzt. Eine andere Klasse von Bodenrobotern ist für Materialtransport und Kampfaufgaben vorgesehen. Abbildung 8 zeigt ein Beispiel eines vernetzten FCS-Systems.

Transformierte Streitkräfte müssen nach neuen Grundsätzen trainiert werden. Das US-Verteidigungsministerium hat hierzu ein spezielles Dokument veröffentlicht und darin die folgenden Zielsetzungen definiert:[16]

- Stärkung streitkräftegemeinsamer Operationen durch Einführung neuer Konzepte für die Kriegführung
- Ständige Verbesserung der Kampfbereitschaft durch Ausrichtung streitkräftegemeinsamer Ausbildung, Training und Ressourcen auf die Bedürfnisse des militärischen Befehlshabers

[16] DOD Training Transformation Implementation Plan (Washington, DC: Office of the Undersecretary of Defense for Personnel and Readiness, June 2003).

- Weiterentwicklung des streitkräftegemeinsamen Denkens bei Individuen und Institutionen
- Befähigung von Personen und Institutionen zur improvisierten Anpassung an aufkommende Krisen
- Einsatz einer Vielfalt von Mitteln zum Erreichen eines Zieles

Drei Fähigkeiten bilden die Grundlage für die Transformation des Trainings:

- Durch die streitkräftegemeinsame Fähigkeit zur Aufbereitung und Verteilung von Wissen sollen zukünftige Entscheidungsträger und Befehlshaber lernen, teilstreitkräfteübergreifend zu handeln und ein gemeinsames Verständnis der operativen Lage zu entwickeln
- Die streitkräftegemeinsame nationale Trainingseinrichtung (Joint National Training Capability), eine nationale Infrastruktur aus realen und virtuellen Trainingsmöglichkeiten, verschafft Trainings- und Übungsmöglichkeiten für globale Operationen

Durch die streitkräftegemeinsame Bewertungs- und Umsetzungsfähigkeit sollen die Beurteilung von Individuen, Organisationen und Prozessen hinsichtlich ihrer Leistungsfähigkeit ermöglicht und die gemeinsame Wissensbereitstellung entwickelt werden

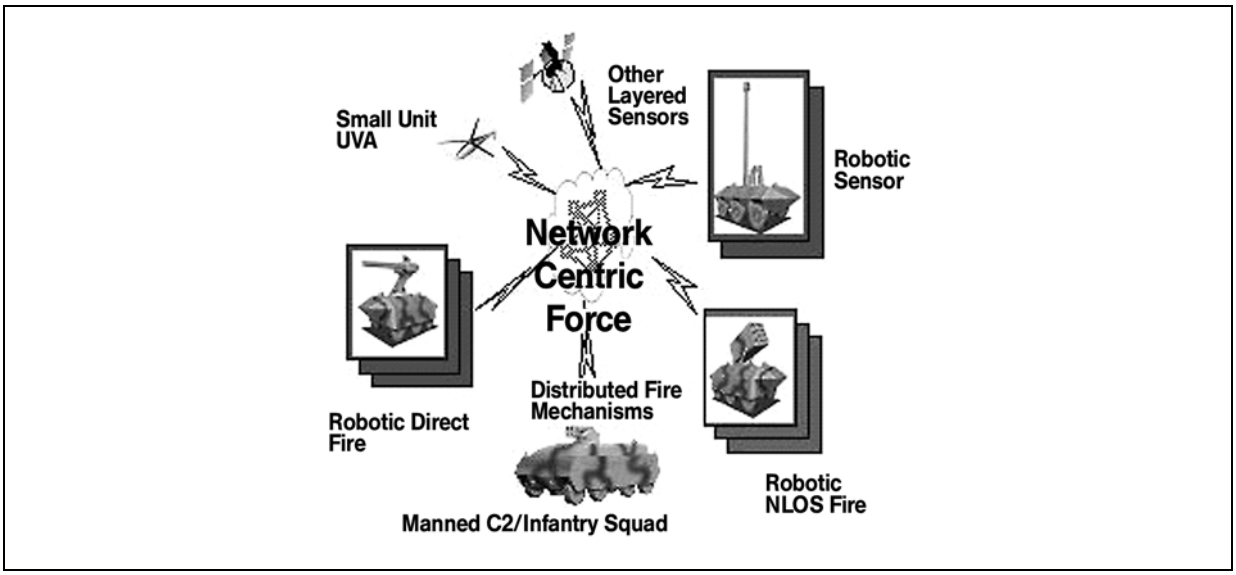

Abbildung 8: Komponenten des Future Combat Systems der US Army

Quelle: Vortrag von Dr. Allen Adler anlässlich der DARPA Industry Days vom 11. Januar 2000.

Transformation in der NATO

Die Transformation der NATO-Streitkräfte wurde durch die Teilnehmer des Prager NATO-Gipfels 2002 beschlossen.[17] Der militärische Kommandobereich unterscheidet neu zwischen dem Allied Command Transformation (ACT) und dem Allied Command Operations (ACO). Das ACO in Mons (Belgien) wird vom Supreme Allied Commander in Europa (SACEUR)

[17] Siehe: <http://www.nato.int/docu/pr/2002/p02-127e.htm> (Zugriff: 29. Dezember 2003).

geleitet und ist für die Vorbereitung und die Durchführung aller Operationen verantwortlich. Hierzu gehören auch Operationen auf NATO-Territorium, die vormals unter der Verantwortung des atlantischen Kommandobereichs (SACLANT) standen.

Das ACT (Abbildung 9) hat am 19. Juni 2003 seine Tätigkeit aufgenommen. Es liegt räumlich in unmittelbarer Nachbarschaft des USJFCOM in Norfolk, Virginia, und wird vom Supreme Allied Commander Transformation (SACT), Admiral Giambastiani, geleitet. Das ACT verantwortet die NATO-spezifische Umsetzung des Transformationsprozesses. Hierbei nimmt der Aufbau der ebenfalls in Prag beschlossenen NRF einen wesentlichen Platz ein. Das ACT ist gegenüber dem NATO-Militärausschuss für alle Empfehlungen bezüglich Transformation verantwortlich. Zur Erfüllung dieser Aufgabe untersucht das ACT Konzepte, fördert die Entwicklung von Doktrinen, führt Experimente durch und unterstützt die Erforschung und Beschaffung neuer Technologien.

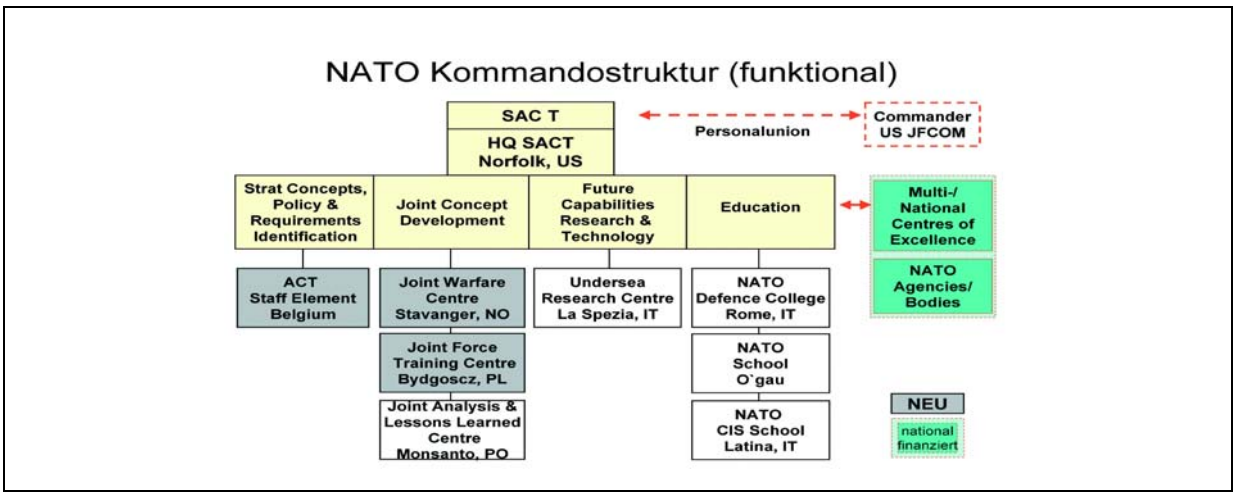

Abbildung 9: Struktur des Allied Command Transformation (ACT)
Quelle: Klaus Olshausen und Heinrich Lange, „Die neue Kommandostruktur der NATO“, *Soldat & Technik* 46:8 (August 2003), S. 8-14, hier S. 12

Transformation in Großbritannien

Als Ergebnis einer „Strategic Defence Review“ im Jahre 1998 hat Großbritannien eine gründliche Neugestaltung der Streitkräfte eingeleitet.[18] Die Briten setzen sich terminologisch und inhaltlich von den USA ab. Sie betonen den nicht-doktrinären und nicht-visionären Charakter ihrer Network Enabled Capability (NEC). NEC wird als eine sich entwickelnde Fähigkeit beschrieben, die Entscheider, Waffensysteme und Sensoren zwecks Fähigkeitssteigerung zusammenbringt. Es wird als Wegbereiter für EBO gesehen und wie folgt charakterisiert:

> NEC erlaubt Plattformen und Führungssystemen das Ausnutzen einer gemeinsamen Lagekenntnis für die gemeinsame Planung, Kommunikation von Führungsabsichten und ein nahtloses Battle-Management. Es unterstützt Überlegenheit bei Entscheidun-

[18] Das Grundlagendokument ist inzwischen vollständig überarbeitet und im Dezember 2003 neu veröffentlicht worden. Siehe: <http://www.mod.uk/linked_files/publications/whitepaper2003/volume1.pdf> (Zugriff: 29. Dezember 2003).

gen und den Einsatz schneller synchronisierter Mittel auf dem streitkräftegemeinsamen, multinationalen Gefechtsfeld.[19]

Die britischen und US-amerikanischen Ziele bezüglich der angestrebten Fähigkeiten sind ähnlich, doch der britische Weg ist evolutionär angelegt. Als technisches Rückgrat für die Vernetzungsfähigkeit haben die Briten das Kommunikationssystem Bowman beschafft, das für Daten- und Akustikübertragung eingesetzt werden kann. Beim Heer wird unter der Bezeichnung Future Rapid Effect System (FRES) eine neue Generation gepanzerter Fahrzeuge konzipiert. In etwa acht Jahren soll dieses System für globale Konfliktbewältigung einsatzfähig sein. Insgesamt sollen 1.300 Fahrzeuge beschafft werden. Der Nutzer will damit die Fähigkeit erwerben, globale, das gesamte Spektrum umfassende Operationen mit verschiedenen Waffen multinational in einem weiten Bereich zukünftiger Operationsgebiete durchführen zu können.

Transformation in Frankreich

Aus Frankreich ist bisher nicht viel zum Thema Transformation nach außen gedrungen. Die Délégation Général pour l'Armement (DGA) hat im Juni 2002 eine Pressemitteilung veröffentlicht. Darin erläutert sie ihren konzeptionellen Ansatz des „vernetzten aeroterrestrischen Kampfs" der Zukunft und stellt als erste Anwendung die „operationelle aeroterrestrische Kugel" (Boule Opérationelle Aéroterrestre, BOA) vor.[20] Hierbei handelt es sich im wesentlichen um ein Konzept vernetzter Landstreitkräfte, dessen Umsetzung sehr langfristig angelegt ist.

Transformation in Schweden

Schweden hat die derzeitige sicherheitspolitische Lage zum Anlass einer grundsätzlichen Neuausrichtung der Streitkräfte genommen. Im Jahre 2000 hat das schwedische Parlament die Transformation der Streitkräfte beschlossen. Schweden wird die Streitkräfte nach den Prinzipien der netzwerkbasierten Verteidigung (Network Based Defense, NBD) entwickeln. Dabei soll ein hohes Maß von Anpassungsfähigkeit an zukünftige Forderungen erreicht werden. Die Umwandlung geschieht gemäß einem Masterplan, der in drei Phasen eingeteilt ist.

Die erste Phase ist abgeschlossen und bestand darin, militärische Einrichtungen und Trainingszentren zu schließen sowie die Zahl des vorhandenen alten Gerätes (Legacy Systems) zu reduzieren. Auf diese Weise wurde Geld freigesetzt. Die zweite Phase ist auf Forschungsvorhaben und Demonstrator-Programme ausgerichtet. Die dritte Phase besteht in der Umsetzung und wird als kontinuierlicher Entwicklungsprozess ohne Endstufe verstanden. Auf diese Weise werden die schwedischen Streitkräfte Experimente und Training mit neuen Technologien neben der Nutzung traditioneller Rüstung betreiben.

Die Entwicklung von NBD geschieht in vier größeren Arbeitspaketen:

- Doktrin: Hier werden – ähnlich dem CD&E-Prozess der USA und der NATO – Methoden untersucht und Experimente durchgeführt

[19] MajGen R H G Fulton, „NEC Brief to Industry at RUSI", Royal United Services Institute, London, 28. November 2002.

[20] Siehe: <http://www.defense.gouv.fr/dga/fr/pdef/dp_boa2.pdf> (Zugriff: 29. Dezember 2003).

- Technologie: Schwerpunkte sind die Lage des Gefechtsfeldes und Technologien zur Unterstützung des Doktrin-Programms
- Training: Zielt darauf ab, das militärische Personal darin auszubilden, mit neuer Doktrin und Technologie bessere Fähigkeiten herzustellen und den Übergangsprozess von prozeduraler zu vernetzter Kriegsführung besser zu verstehen
- Organisation: Entwicklung von Strukturen und Prinzipien zur Zusammenstellung von streitkräftegemeinsamen Einheiten

Parallel dazu entwickelt Schweden die industriellen Fähigkeiten für Vernetzungstechnologien.

Transformation in Deutschland

Das Thema Vernetzung ist in Deutschland zögerlich in Gang gekommen. Vorreiter war das Zentrum für Analysen und Studien der Bundeswehr (ZASBw).[21] Beim NATO-Gipfel im November 2002 hat sich die Bundesregierung zur Beteiligung an der NRF entschlossen. Da es sich hierbei um eine transformierte Streitkraft handelt, musste die Bundeswehr die Transformation in Angriff nehmen.

In der im Mai 2003 erlassenen Verteidigungspolitischen Richtlinie und in der im Oktober 2003 an den Generalinspekteur erteilten Weisung hat Bundesminister Struck nun auch in Deutschland die Transformation der Streitkräfte eingeleitet. Der nächste Schritt ist eine neue Konzeption der Bundeswehr und ein neues Material- und Ausrüstungskonzept. Nach der jetzigen Planung müsste bis zum Frühjahr 2004 der zukünftige deutsche Weg bekannt sein.

Deutschland arbeitet im Rahmen des NATO CD&E-Prozesses an multinationalen Experimenten mit, und am ZASBw wird ein aus etwa 80 Personen bestehender Stab für Transformationsmanagement aufgebaut. Mitarbeiter aus der Industrie sind als Industrial Research Fellows (IRF) am ZASBw tätig und können auf diese Weise ihre Mutterhäuser über die Entwicklungen direkt informieren.

Auswirkungen auf die Industrie

Die Konsequenzen der Streitkräftetransformation für die Industrie können unter drei verschiedenen Aspekten betrachtet werden: Veränderung des militärischen Bedarfs, Neugestaltung der Zusammenarbeit zwischen Militär und Industrie und rüstungswirtschaftliche Fragen.

Bedarf transformierter Streitkräfte

Transformierte Streitkräfte müssen sowohl konzeptionell als auch materiell ohne Zeitverluste auf neuartige Herausforderungen reagieren können. Es ist nicht möglich, das Material für alle denkbaren Varianten moderner kriegerischer Auseinandersetzungen bereitzuhalten. So fordert

[21] Siehe zum aktuellen Stand: Ralph Thiele: „Innovation an der Spitze des Fortschritts", *Europäische Sicherheit* 52:11 (November 2003), S. 25-29; Holger H. Mey und Michael K.-D. Krüger, *Vernetzt zum Erfolg? „Network-Centric Warfare" – zur Bedeutung für die Bundeswehr,* ISA-Studie Nr. 9 (Frankfurt: Report Verlag, 2003), S. 47-56; *Network Centric Capabilities und der Transformationsprozess. Kompendium des Symposiums vom 4. September 2003* (Bonn: Studiengesellschaft der Deutschen Gesellschaft für Wehrtechnik, 2003).

das US-amerikanische Office of Force Transformation die Fähigkeit der Parallelentwicklung von Konzepten, Prozessen, Organisationen und Technologien. Was damit gemeint ist, wurde während des Afghanistan-Krieges am Beispiel der Predator-Drohne demonstriert, die innerhalb kürzester Zeit zu einem waffentragenden System umgerüstet und erfolgreich eingesetzt wurde. Von der Industrie wird hier die Fähigkeit zu spontanen technischen Lösungen erwartet.

Vernetzte Systeme fordern von der Industrie innovative Problemlösungen. Schutzkonzepte können beispielsweise durch Schnelligkeit, kleine Signaturen und aktiven Selbstschutz dargestellt werden. Robotertechnik und die Trennung von „Sehen“ und „Wirken“ sind weitere typische Innovationsfelder. Das Erzeugen militärischer Fähigkeiten durch einen Systemverbund ist ein neues Arbeitsgebiet, das neue Denkansätze, neue Werkzeuge und auch neue Mitarbeiterqualifikationen fordert. Militärische Fähigkeiten werden durch die Kombination von operationeller Wissensnutzung und Rüstungstechnik hergestellt. Hier eröffnen sich neue Tätigkeitsfelder mit viel Innovationspotential.

Die vollständige und aktuelle Lagedarstellung mit allen relevanten Informationen, nichtmilitärische eingeschlossen, ist eine unabdingbare Voraussetzung für den erfolgreichen Einsatz transformierter Streitkräfte. Das setzt industrielle Kompetenzen auf den folgenden Gebieten voraus:

- Sensorik
- Informationssysteme
- Datenbanken
- Informationssicherheit
- Informationsoperationen
- Numerische Modelle
- Schnittstellenengineering

Transformierte Streitkräfte benötigen eine industrielle Basis, die das Spektrum vom Systemintegrator über technologische Innovation, Informationstechnologie, Sensorik bis zur Informationsmanipulation abdeckt. Da die Transformation allerdings nur einen Teil der Streitkräfte betrifft, wird das klassische Rüstungsmaterial weiterhin benötigt und muss durch entsprechende rüstungstechnische Fähigkeiten in seinem Bestand und seiner Weiterentwicklung gesichert sein. Materialerhalt und Missionsadaptionen werden die Schwerpunktthemen für klassisches Rüstungsmaterial sein. Teilweise hat sich die Industrie schon darauf eingestellt.

Militärisch-Industrielle Zusammenarbeit

Militärische Fähigkeiten werden durch einen komplexen dynamischen Systemverbund hergestellt. Ein solcher Systemverbund kann wegen der außerordentlich großen Zahl von Variablen und Optimierungsparametern nur mit Hilfe numerischer Modelle und Simulationen ausgelegt werden. Dies nennt man Konzeptentwicklung. Die operationelle Wirkung eines solchen Systemverbundes wird dann experimentell wiederum mit Unterstützung von Simulationen und numerischen Modellen verifiziert. Diese Vorgehensweise erlaubt nicht nur die Beurteilung

militärischer Fähigkeiten, sondern ermöglicht es gleichzeitig, die Auswirkungen neuer Konzepte auf Doktrin, Organisation, Material, Führung, Personal und Infrastruktur zu bewerten. Die industrielle Leistung wird folglich nicht durch physikalisch feststellbare Spezifikationen, sondern durch „weiche“ Fähigkeitskriterien beurteilt. Wegen seines iterativen Charakters kann dieser Prozess nur in enger Zusammenarbeit zwischen Industrie und Kunden erfolgreich gestaltet werden.

Transformation ist ein kontinuierlicher Prozess. Analysen und Anpassungen des Systemverbundes liefern die jeweils erforderlichen Fähigkeiten. Fähigkeitsanpassungen werden überwiegend durch neue Architekturen, veränderte Komponenten und Software erzielt. Dies läuft auf ein verändertes Geschäftsmodell für die Industrie hinaus: Für kleine Stückzahlen ist ein hoher technischer Anspruch zu realisieren. Dies ist eine Umkehrung der Verhältnisse aus der plattformorientierten Zeit, in der Entwicklungstätigkeiten für eine Serienproduktion mit „großen“ Stückzahlen angelegt waren. Jede Firma muss hier eine Neuausrichtung ins Auge fassen und bewusst festlegen, welche Fähigkeiten in Zukunft aufrechtzuerhalten oder zu entwickeln sind.

Rüstungswirtschaft

In der durch Plattformen dominierten Zeit wurden Waffensysteme, Geräte und Komponenten als Bedarf ermittelt, spezifiziert und bei der Industrie in Auftrag gegeben. Die rüstungstechnische Gesamtleistung der Streitkräfte wurde aus der Summe der einzelnen Komponenten gebildet. Die Streitkräfteausrüstung wurde von der Basis nach oben gestaltet.

Die Herstellung militärischer Fähigkeiten durch komplexe Systeme erzeugt eine neue industrielle Aufgabe, die des Systemintegrators. Dies ist eine Funktion oberhalb des auf Plattformebene tätigen Systemherstellers. Der Systemintegrator beherrscht komplexe Systemarchitekturen und nimmt Managementfunktionen im Auftrag des Auftraggebers wahr. Ein Systemintegrator muss hinreichende Erfahrungen mit Systemen haben und wird im CD&E-Prozess eine wichtige Rolle spielen.

Wie in Abbildung 10 dargestellt, führt die Fähigkeitsorientierung zu einer von oben nach unten gerichteten Bedarfsermittlung, so wie es auch durch das Beschaffungsverfahren CPM 2001 (Customer, Product, Management) festgelegt wird. Aus einer Fähigkeitslücke werden Systemfähigkeitsforderungen und daraus schließlich funktionale Forderungen hergeleitet. Diese werden durch einen Hauptauftragnehmer in Wehrmaterial umgesetzt. Dieses Verfahren kappt die bis dato übliche direkte Verbindung eines Untersystemherstellers mit dem militärischen Kunden. Die Streitkräfte als Endkunde haben wenig bis keinen Einfluss auf die Auswahl der Unterauftragnehmer seitens des Systemverantwortlichens. Mittel- bis langfristig kann dies eine vertikale industrielle Integration zu Folge haben.

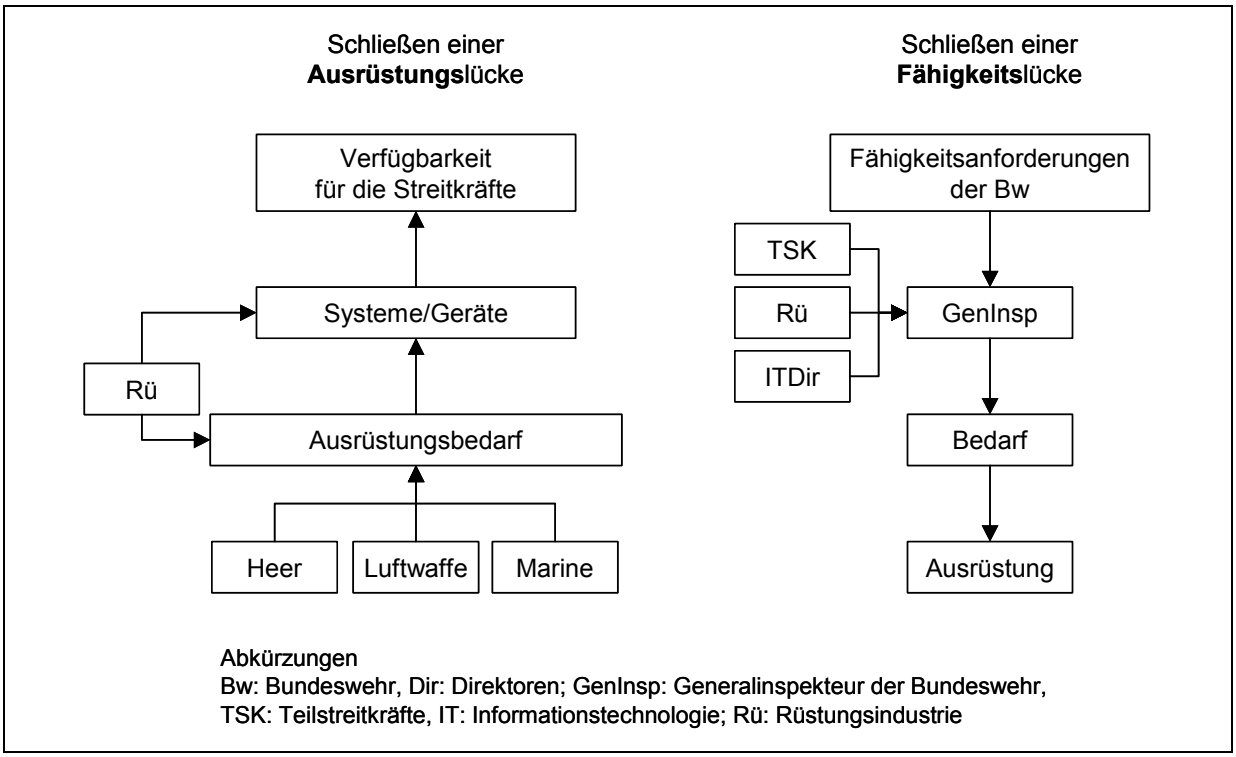

Abbildung 10: Bedarfsermittlung zum Schließen einer Ausrüstungs- bzw. Fähigkeitslücke

Zusammenfassung

Transformation setzt die heute verfügbaren technologischen und technischen Möglichkeiten für die Neugestaltung der Streitkräfte ein. Das bedeutet einen tiefen Eingriff in die durch den Kalten Krieg geprägten Streitkräftestrukturen und betrifft Doktrin, Organisation, Training, Führung, Ausrüstung, Personal und militärische Einrichtungen. Die USA entwickeln transformierte Streitkräfte und haben den Transformationsprozess auch in die NATO getragen. Andere westliche Nationen gehen eigene Wege zur Transformation ihrer Streitkräfte. Transformation betrifft auch die Industrie. Es werden neue Fähigkeiten gefragt, und die Zusammenarbeit mit den Streitkräften wird bei der Entwicklung neuartiger militärischer Ausrüstung eine andere Form annehmen. Der Systementwickler als Verantwortlicher für die Leistungserbringung wird eine herausragende Rolle spielen. Das kann rüstungswirtschaftliche Auswirkungen zur Folge haben.

Martin Neujahr

Vernetzte Operationsführung und das neue operative Umfeld: Gesteigerte Einsatzwirksamkeit durch verbesserte Führungsfähigkeit

Network Centric Warfare (NCW) und die deutsche Entsprechung der vernetzten Operationsführung (NetOpFü) sind binnen kurzer Zeit zu den wichtigsten Schlagworten geworden, wenn es um die Modernisierung von Streitkräften geht.[22] Unstrittig ist, dass ein verändertes sicherheitspolitisches Umfeld nach neuen Instrumenten verlangt, um die Sicherheit der in unseren Ländern lebenden Menschen zu gewährleisten. Die Philosophie der vernetzen Operationsführung und die Vorstellung davon, was sich hinter NetOpFü verbirgt, haben schnell Eingang in die Planung von Transformationsprozessen gefunden.

Wesentlich unklarer ist jedoch allgemein, welche Auswirkungen NetOpFü auf die Erfordernisse moderner Konfliktbewältigung hat, besonders hinsichtlich der Philosophie der „wirkungsorientierten Operationsführung“ (Effects Based Operations, EBO). Darüber hinaus ist das Wissen um die Konsequenzen der vernetzen Operationsführung für die politische und militärische Führung von Streitkräfteeinsätzen von wesentlicher Bedeutung. Erste Überlegungen zur Implementierung vernetzter Fähigkeiten zeigen, dass der daraus resultierende Wandel für die Streitkräfte grundlegender ist, als bei bloßer Einführung neuer Technologie, da es um die Definition und die Anwendung einer neuen Philosophie des Streitkräfteeinsatzes geht. Die folgenden Ausführungen sollen einen Beitrag zum Verständnis des Zusammenhangs zwischen NetOpFü, EBO und „Führung“ in einem veränderten sicherheitspolitischen und operativen Umfeld leisten sowie einige Konsequenzen für die Implementierung der Fähigkeit zur vernetzten Operationsführung aufzeigen.

Wandel des gesellschaftlichen, sicherheitspolitischen und operativen Umfelds

Wir befinden uns heute in einer globalen Übergangsphase von der Industrie- zur Informations- und Wissensgesellschaft. Die Geschwindigkeit der Veränderungsprozesse und die Vernetzung von Lebensbereichen nehmen dabei zu. Gleichzeitig birgt die voranschreitende technische Entwicklung die Gefahr des Kontroll- und Steuerungsverlustes für staatliche Organe. In diesem Prozess ist die Rolle und Position des Militärs laufend auszurichten. Bisher greifen wir allerdings weitgehend auf Strukturen und Steuerungsmechanismen der Industriegesellschaft zurück.

Neben dem gesellschaftlichen Wandel hat sich der Sicherheitsbegriff erweitert. An die Stelle klassischer militärischer Konflikte treten in zunehmenden Maße kleine und asymmetrische Kriege. Dabei ist das Handeln nicht-staatlicher Akteure meist nicht gegen militärische Ziele gerichtet, sondern auf die Erzielung eines größtmöglichen – insbesondere psychologi-

[22] Nach deutscher Interpretation kommen Streitkräfte nicht nur im Sinne klassischer Kriegführung zur Anwendung. Deswegen wurde der Begriff der vernetzten Operationsführung etabliert. Siehe hierzu auch die Ausführungen von Burkhard Theile in diesem Band.

schen – Effektes in der Gesellschaft. Dieses wirkungsorientierte Vorgehen ist weder nach Art, Raum und Zeit rational vorhersehbar.

Zusätzlich bietet die sich immer rascher entwickelnde Technologie in allen Lebensbereichen neue Möglichkeiten der Auseinandersetzung, bis hin zum Informationskrieg, d.h. zu Informationsangriffen im Informationsraum. Militärische Einsätze im erweiterten Bedrohungsspektrum zielen auf einen Gegner, der als vernetztes System zu begreifen ist und daher schwer fassbar ist.[23] Allerdings erfordern effektbasierte Angriffe eines asymmetrisch agierenden Gegners ein gesamtstaatliches Handeln, zumindest aber militärische Aktionen in Bündnissen und Koalitionen. Das operative Umfeld wird komplexer.

Das Militär wird in politisch brisanten Situationen als geeignetes Mittel zum Krisen- und Konfliktmanagement angesehen und auch eingesetzt. Einschränkende Rahmenfaktoren sind dabei die begrenzten finanziellen Mittel sowie die oft restriktiven Einsatzbestimmungen (Rules of Engagement). Jede militärische Handlung unterliegt einer hohen Visibilität und Resonanz in den Medien („CNN-Faktor"), wodurch der Handlungsrahmen limitiert wird. Selbst Terroristen wird über weltweit zugängliche Medien eine Bühne geboten, über die sie ihre Botschaften global kommunizieren können („Al-Dschasira-Faktor").

Aus dem operativen Umfeld von heute ergibt sich, dass klassische militärische Instrumentarien, also die weitere Optimierungen der plattform- und der munitionszentrierten Kriegführung sowie Reorganisationen vorhandener Strukturen weder ausreichen noch finanzierbar sind, um den neuen Herausforderungen effektiv und effizient zu begegnen. Effektivität und Effizienz würden keinesfalls proportional zu den eingesetzten Ressourcen steigen, sondern eher reduziert werden.

Die gestiegene Abhängigkeit von Wissens- und Informationsbeziehungen führt zu einer Dominanz der Information und einer Neubewertung der übrigen operativen Faktoren. Der Faktor Zeit wird dabei bestimmend gegenüber Raum und Kräften. Die Dynamik von Aktionen wird im verstärkten Maße ein paralleles statt sequentielles Handeln erfordern. Aufgrund der technischen Möglichkeiten verliert die geographisch oder physisch verstandene räumliche Dimension an Bedeutung. Gleichzeitig entstehen aber auch neue Räume für die Kriegführung, darunter der Informationsraum. Der Faktor Kräfte erhält ein neues inhaltliches Verständnis: Die Konzentration von Kräften ist obsolet, Fähigkeiten müssen gebündelt werden.

Die Neugewichtung der operativen Faktoren stellt die Fähigkeit, Informationen gewinnen und verarbeiten und hieraus eine zielgerichtete und zeitgerechte Führungsleistung erbringen zu können, in den Mittelpunkt. Allerdings ist das Erzielen der Informationsüberlegenheit nur notwendige und nicht hinreichende Bedingung, um einem anspruchsvolleren operativen Umfeld begegnen zu können. Hierzu bedarf es der Übersetzung der Informationsüberlegenheit in Entscheidungsüberlegenheit, um zu einer Handlungsüberlegenheit über den Gegner gelangen zu können.

[23] Zum Verständnis eines Gegners als komplexes System und seiner Analyse mit Hilfe des Operational Net Assessment (ONA) siehe auch die Ausführungen von Burkhard Theile in diesem Band.

Prinzipien der vernetzten Operationsführung

Die Fähigkeit zur vernetzten Operationsführung basiert auf einer umfassenden Informationsstruktur. Diese Informationsstruktur beinhaltet eine Vernetzung vom Sensor über die Entscheidungsträger bis hin zum Effektor einschließlich der Informationsbeziehungen und der technischen Infrastruktur. Das Informationsmanagementsystem verarbeitet und verteilt die Erkenntnisse bedarfsgerecht und schafft damit das geforderte Lagebewusstsein (Battlespace Awareness) bei den Entscheidungsträgern. Wird dieses Informationsmanagementsystem um menschliche Expertise und Intuition erweitert, wird schließlich ein tieferes und umfassenderes Lageverständnis (Battlespace Knowledge) erreicht. Der Geführte kann damit in jeder Situation im Sinne der übergeordneten Zielsetzung handeln. Gleichzeitig wird der Führungsprozess durch direkte Rückkopplung erneut stimuliert und beschleunigt. Das Ergebnis sind selbstsynchronisierende Streitkräfte, denen es unter Nutzung aller relevanten Informationen ermöglicht wird, auf allen Ebenen eigenständig und im Sinne des erteilten Auftrags zu handeln. Auf der Basis angepasster Command and Control (C2)-Strukturen wird die Effizienz der Streitkräfte zudem erheblich gesteigert, indem die Bewegung von Information die oftmals aufwendige Bewegung von Mensch oder Material ersetzt. Dies erlaubt ein höheres Operationstempo und eine gesteigerte Reaktionsfähigkeit bei niedrigeren Risiken und Kosten. Der aus dem Informationsvorteil resultierende Handlungsvorteil führt zu einer deutlich gesteigerten Einsatzwirksamkeit der Streitkräfte (Abbildung 11).

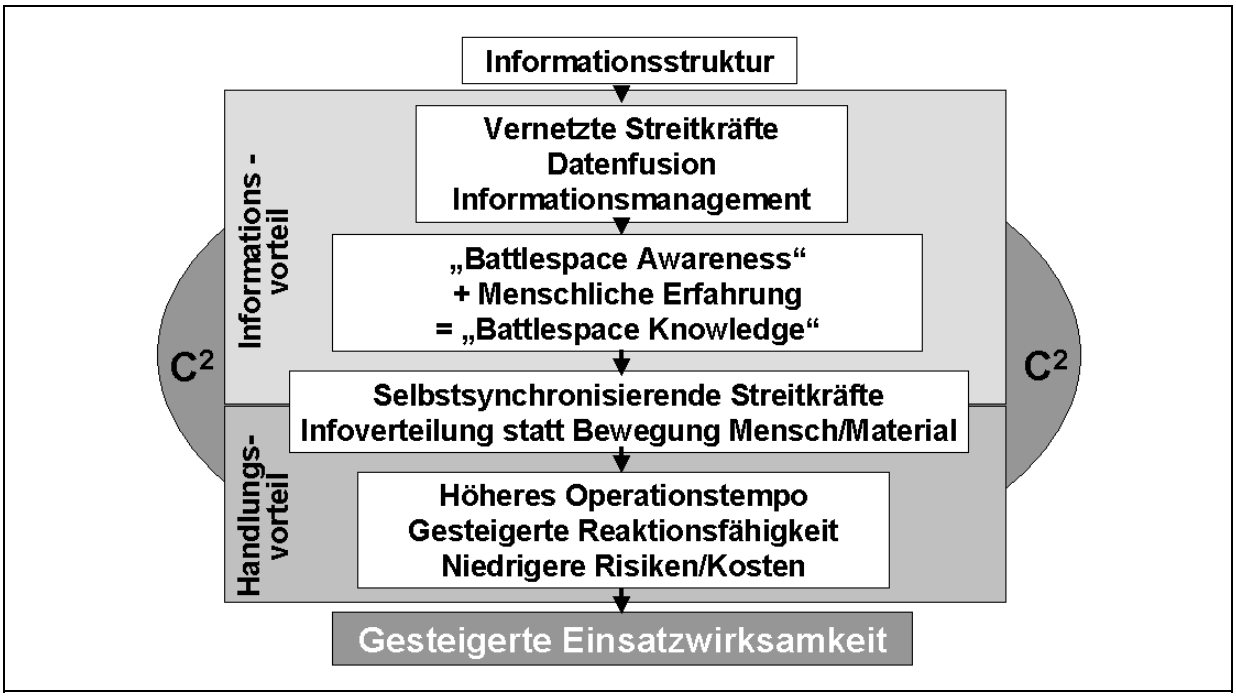

Abbildung 11: Wechselwirkungen zwischen den NetOpFü-Grundprinzipien

Die Diskussion über die Notwendigkeit vernetzter Operationsführung wird bisweilen von drei Interpretationsfehlern überlagert:

1. Die Annahme, dass es nur um Technologie geht
2. Der Gedanke, dass sich alles um Information dreht
3. Die Überzeugung, erst mit der Implementierung beginnen zu können, wenn NetOpFü als Komplettlösung verfügbar ist

NetOpFü fokussiert nicht auf Computer im Netzwerk oder Kommunikationsmittel, sondern insbesondere auf den Informationsfluss sowie die Art und den Umfang des Informationsbedarfes räumlich verteilter Kräfte. NetOpFü ist ein ganzheitlicher Ansatz, der Technologie zwar zu seiner Umsetzung benötigt, gleichzeitig aber auch Anpassungen in den Strukturen, Verfahren und im Denken aller Beteiligten erfordert. Dabei müssen die Konzeption von NetOpFü künftigen Entwicklungen angepasst und die Streitkräfte kontinuierlich weiterentwickelt werden. Es ist demnach nicht möglich, auf ein Entwicklungsende oder eine Komplettlösung zu warten, um erst dann mit der Implementierung von NetOpFü zu beginnen.

Das Wesen von Effect Based Operations (EBO)

Operationen im Informationszeitalter sind geprägt durch drei Faktoren:

- Erweitertes Spektrum sowohl hinsichtlich der Bedrohung als auch der Art eigener Einsätze wie beispielsweise Peace Support Operations
- Gestiegene Komplexität der Interdependenzen und gleichzeitige Diffusität des Einsatzraumes
- Höhere Qualität, schnellere Verfügbarkeit und damit gestiegene Bedeutung von Information

Der bereits beschrittene Weg der Anpassung von Operationen betrachtet nicht mehr die Einzelwirkung auf singuläre Ziele, sondern Effekte im System. Das diesem Gedanken zugrunde liegende Konzept wird Effect Based Operations (EBO, wirkungsorientierte Operationsführung) genannt. Aufgrund der Aktualität und Dynamik des Themenbereiches steht keine eindeutige Begriffsbestimmung für EBO zur Verfügung. Im Folgenden werden deshalb die Wirkungsdimensionen von EBO betrachtet:

> EBO sind Prozesse zur Erreichung eines vorgesehenen Ergebnisses durch synergetische Anwendung des gesamten Spektrums direkter und indirekter Effekte. Hierbei kommen diplomatische, psychologische, militärische und wirtschaftliche Instrumente zur Anwendung.

Der Fokus liegt auf den funktionalen und systematischen Effekten auch jenseits der direkten physischen Einwirkung auf die taktische, operative oder strategische Ebene. Der angestrebte Systemeffekt beinhaltet neben traditionellen militärischen „harten Zielen“ wie Infrastruktur und Führungseinrichtungen auch „weiche Ziele“, die im kognitiven Bereich liegen, wie beispielsweise der Wille zu bestimmten Handlungen oder die gegnerische Zielsetzung. Charakteristisch für EBO ist der funktionale Ansatz. So kann zum Beispiel nicht nur das Zerstören einer Brücke eine Verbindungslinie unterbrechen, sondern auch das Einfrieren von Ka-

pital zum Kauf von Gütern oder Transportmitteln. EBO bedeutet also, *„wirkungsorientiert, nicht zerstörungsorientiert“* zu operieren.

Auf das operative Umfeld (Abbildung 12) von heute bezogen bedeutet dies, dass aktuelle EBO in der Lage sein müssen, den gesamten Operationsraum zu umfassen. Hierzu sind verschiedene Bausteine notwendig, die je nach Ausprägung den Rahmen und damit die Möglichkeiten für EBO vorgeben.

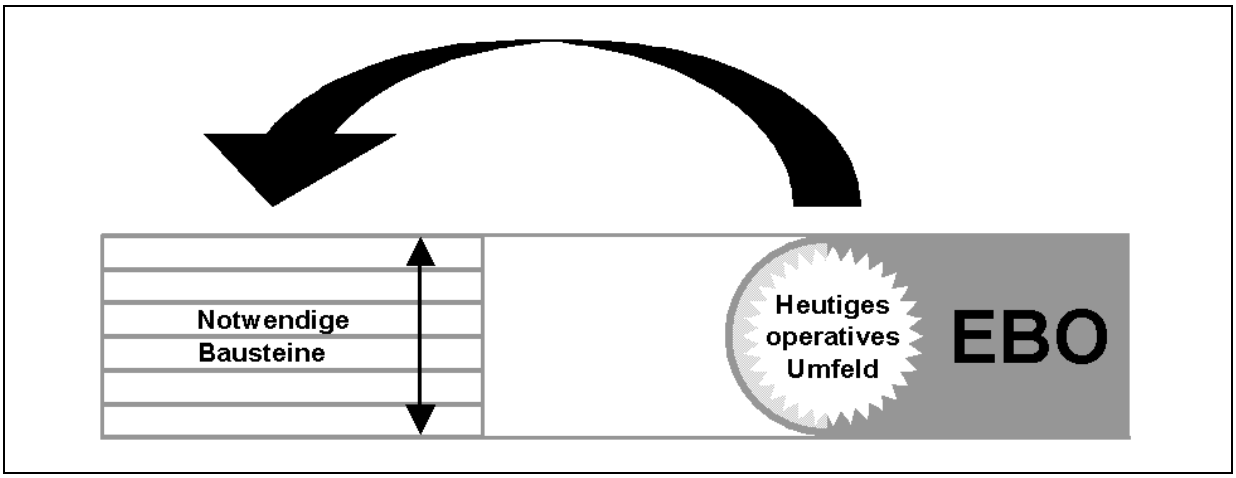

Abbildung 12: EBO im operativen Umfeld der Gegenwart

Für die weitere Analyse liegt der Betrachtungsschwerpunkt auf den militärischen Bausteinen im Rahmen einer interdisziplinären Gesamtoperation. Die Dynamik des operativen Umfeldes von morgen bedingt eine Adaption von EBO (Abbildung 13). Die Qualität der erforderlichen Bausteine muss deutlich verbessert werden, um den gewünschten Effekt auch weiterhin erzielen zu können.

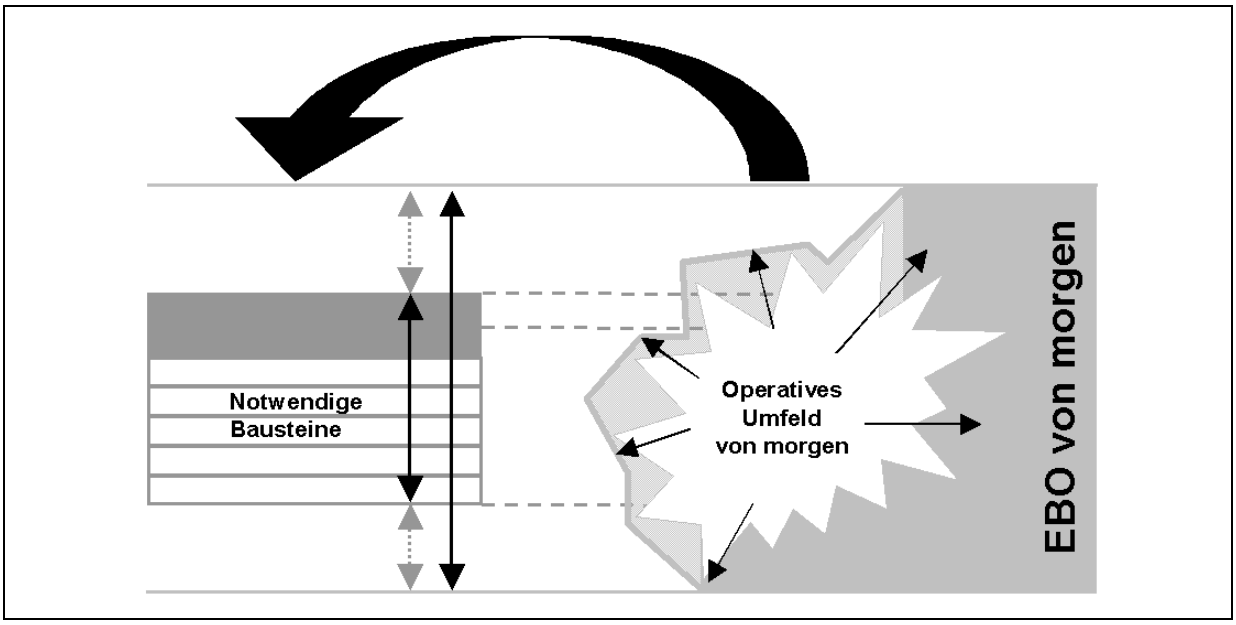

Abbildung 13: EBO im operativen Umfeld der Zukunft

Die entstehende Differenz kann zwar durch Verbesserung eines oder mehrerer Bausteine verringert werden, zur vollständigen Abdeckung des benötigten Gesamtspektrums reichen diese Maßnahmen jedoch nicht aus. Selbst die qualitative Verbesserung aller Einzelbausteine bewirkt lediglich die Bildung von „Inseln“, die in der Summe nicht geeignet sind, das gesamte, in Zukunft notwendige Spektrum abzudecken. Fehlende Beziehungen und Interaktionen innerhalb des Gesamtsystems führen zu quantitativen und qualitativen Einschränkungen. Erst eine Vernetzung der Subsysteme mittels NetOpFü ermöglicht die vollständige Abdeckung des gesamten Spektrums. Auf diese Weise besteht für einzelne Teilnehmer sogar die Möglichkeit, Bausteine zu begrenzen, zu priorisieren oder eventuell ganz aufzugeben, wenn ihre Funktionalität innerhalb des Netzes umfassend vorhanden sind (Abbildung 14).

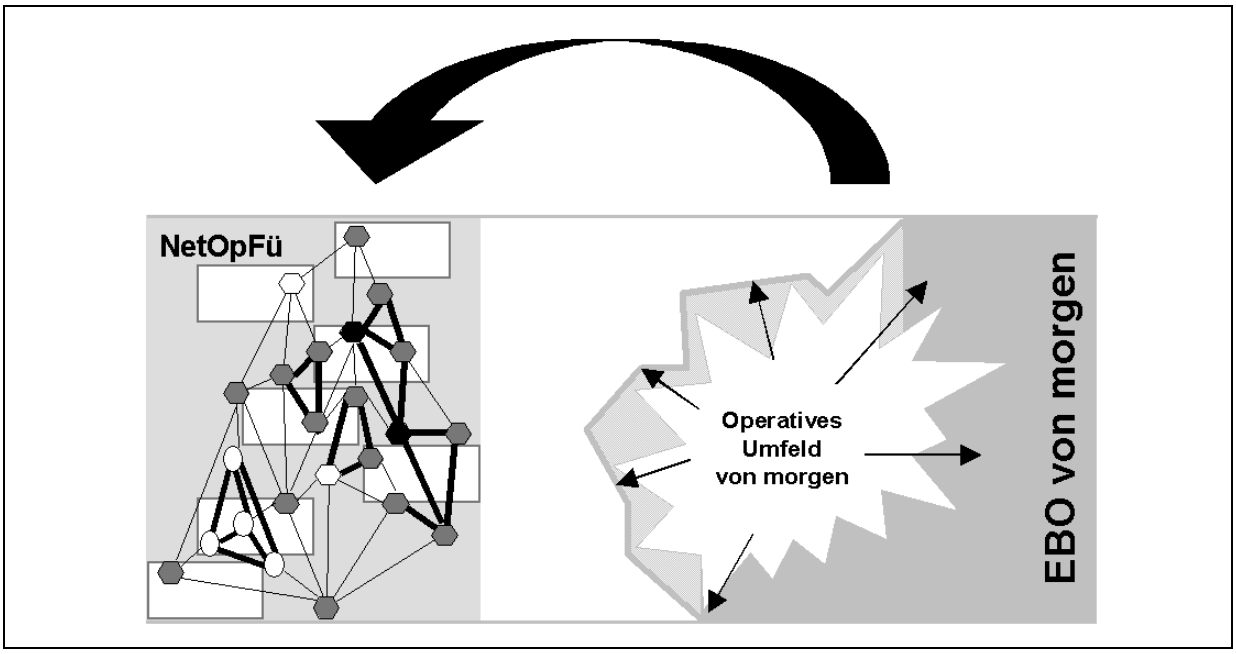

Abbildung 14: EBO und NetOpFü im operativen Umfeld der Zukunft

Möglichkeiten durch die Verknüpfung von EBO mit NetOpFü

Es wurde bereits grundsätzlich ausgeführt, wie NetOpFü den Prozess von EBO verbessert. In der Folge werden nun stichwortartig die Auswirkungen von NetOpFü auf die einzelnen militärischen Bausteine genannt. Dabei sind die folgenden Aspekte besonders hervorzuheben:

- Durch den Verbund zwischen Effektoren, Sensoren und Führungssystemen lässt sich eine signifikante Verbesserung der Verhältnisse von Kräften, Raum, Zeit und Information erzielen. Dies führt dazu, dass bei gleichem Kräfteansatz mehr Effekte bzw. gleiche Effekte durch weniger Kräfte ermöglicht werden.
- NetOpFü kann durch Vernetzung zu einer schnelleren Entscheidungsfindung bei gleichzeitig reduzierter Unschärfe der zugrunde liegenden Information beitragen. Dadurch können der Planungs- und der Entscheidungszyklus beschleunigt sowie die Entscheidungsträger entlastet werden. Beides fördert die Generierung einer Entschei-

dungsüberlegenheit zur Ausübung adäquater Wirkungen auf das System des Gegners (Wirkungsüberlegenheit).
- NetOpFü steigert die für die Dynamik des zukünftigen Operationsraumes unabdingbare Flexibilität durch die mögliche Umgehung prozeduraler Limitierungen[24] und kann somit zu dauerhafter Initiativfähigkeit beitragen.
- NetOpFü eröffnet die Möglichkeit, ohne jeglichen Qualitätsverlust dynamische Operationen unter Nutzung statischer Strukturen zu führen und begrenzt somit den benötigten Projektionsbedarf bei gleichzeitiger wirkungsorientierter Optimierung der qualitativen und quantitativen Ausgestaltung der vor Ort befindlichen Kräfte und Mittel – Just in Time.
- Die Fähigkeit zur vernetzten Operationsführung wird künftig unabdingbare Voraussetzung für streitkräftegemeinsame EBO im Rahmen von Koalitionen sein. Dies schließt auch interdisziplinäre und ressortübergreifende Beziehungen, zum Beispiel zu Polizei, Zoll und Nicht-Regierungsorganisationen ausdrücklich mit ein. NetOpFü verknüpft einzelne Kräfte zu einer Entität.
- Abgestützt auf die mittels NetOpFü ermöglichte Optimierung des Informations- und Wissensmanagements kann ein entscheidender Operationsvorteil erzielt werden. Dies generiert einen qualitativen Quantensprung für EBO in einem dynamischen Operationsraum.
- Informationen und die verknüpfende Intelligenz werden von den Plattformen auf das Netz verlagert, um geteilt werden zu können. Diese Verlagerung fördert den Aufbau koalitionsweiter kollaborativer Informationsumgebungen.[25]

Diese Analyse verdeutlicht, dass EBO im operativen Umfeld von morgen nur möglich sind, wenn sie sich der Dynamik zukünftiger Szenarien permanent anpassen können. Die durch NetOpFü erst mögliche Informationsüberlegenheit ist zwingende Voraussetzung für die Analyse gegnerischer Systeme im Rahmen von EBO, wie beispielsweise die Identifikation von Schwachstellen. Ferner wird durch NetOpFü eine signifikante Prozessbeschleunigung bewirkt, welche die Voraussetzung schafft, EBO im Rahmen eines sich diffus und dynamisch wandelnden operativen Umfeldes zeitgerecht durchzuführen. Zukünftige EBO erfahren erst durch NetOpFü die notwendige Effizienz und Effektivität durch die potenzierte Wirksamkeit von Effektoren. Unter dem Strich bleibt festzuhalten, dass NetOpFü mehr ist als die reine Weiterentwicklung oder Nutzung von bereits vorhandener Technologie. Es ist vielmehr eine neue Philosophie!

Wechselwirkungen zwischen NetOpFü und dem Aspekt „Führung“

Um die Veränderung der Ansprüche an die politische und militärische Führung analysieren zu können, werden zunächst idealtypisch Konsequenzen für die Führung in den Dimensionen

[24] Beispielsweise limitieren Luftraumordnungen (Airspace Co-ordination Order, ACO) für ein Konfliktgebiet, die für einen Tag im Voraus festgelegt werden, die Beweglichkeit eigener Kräfte.

[25] Solche Informationsumgebungen (Collaborative Information Environment, CIE) befinden sich bereits auf dem Prototypenpfad und sind Gegenstand mehrerer internationaler Experimente mit deutscher Beteiligung im Rahmen von CD&E-Projekten.

Führungsorganisation, -verfahren, -verhalten und Führungsphilosophien abgeleitet und bewertet.

Organisation

Die Aufbauorganisation muss so ausgelegt sein, dass notwendige Elemente der vernetzten Streitkräfte in die Einsatzstruktur integriert werden können. Dies bedeutet modularer Aufbau und fordert einen fähigkeits- und funktionsbezogenen Ansatz. Die hier dargestellten Vorstellungen sind grundsätzlich nicht neu, bedeuten aber unter dem Aspekt vernetzter Operationsführung eine ganz neue Qualität und Herausforderung an die Führung.

Die Führungsorganisation (Abbildung 15) muss von der Informationsstruktur getrennt werden. Die Informations- und Kommunikationsstruktur ermöglicht die hierarchienunabhängige Nutzung des virtuellen Informationsraumes. Dies führt bei konsequenter Anwendung zu Informationsüberlegenheit als Grundvoraussetzung für eine beschleunigte Operationsführung, erhöhte Transparenz sowie der Schaffung einer Wirkungsüberlegenheit.

Bei einer auf NetOpFü fokussierten Streitkraft ist die Aufbauorganisation nicht mit der Organisation des Informationsflusses kongruent. Der Informationsaustausch zwischen den Elementen der vernetzten Streitkräfte ist notwendig und anzustreben. Der Handlungsrahmen in diesem Netz wird durch den Auftrag der vorgesetzten Führungsebene vorgegeben, weil der Befehlsstrang der Führungsorganisation eindeutig festgelegt bleiben muss (Unity of Command).

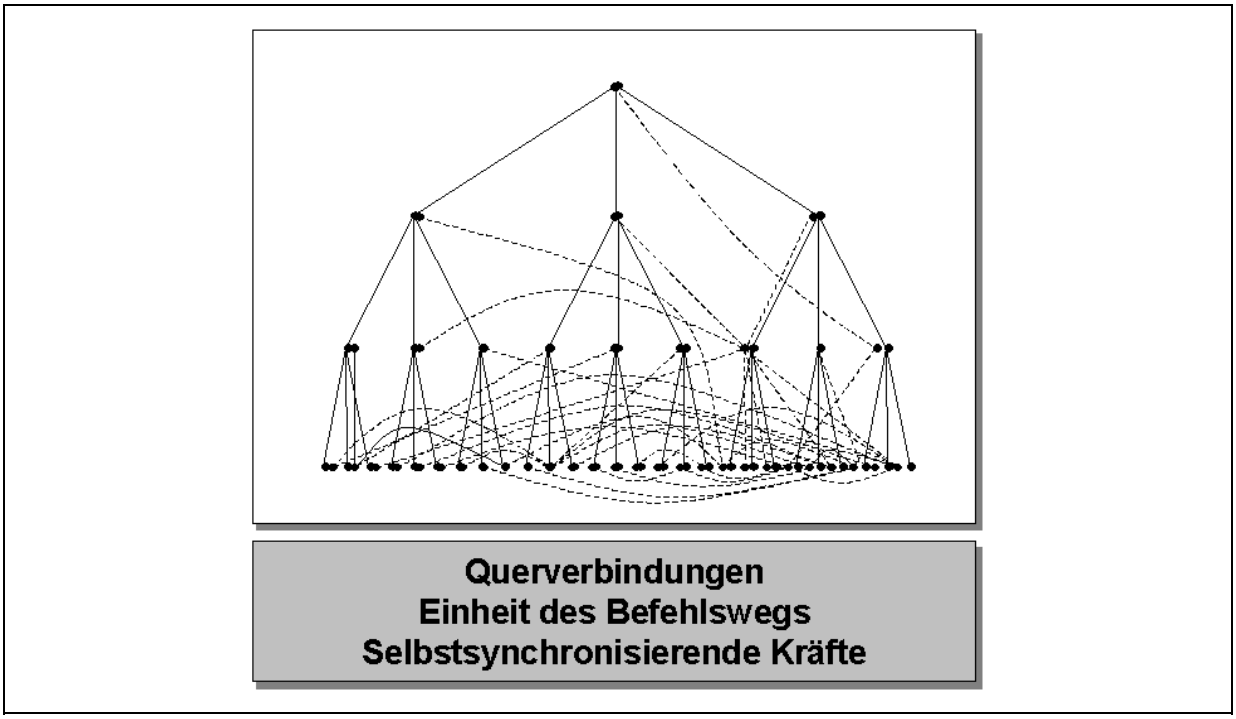

Abbildung 15: Vernetzte Führungsorganisation

Einsatzgebundene und dynamisch wechselnde Veränderungen der regulären Unterstellungsverhältnisse jenseits der Hierarchie gewinnen in diesem Umfeld an Bedeutung. Hierzu sind die jeweiligen Verantwortungsbereiche nach Raum, Zeit und Kräften im Sinne des Kon-

zepts Supporting/Supported Commander dynamisch, aber klar voneinander abzugrenzen. Synchronisation und Koordination finden zusätzlich zur Planungsebene nun in zunehmenden Maße auf der Durchführungsebene statt (bis hin zu einer Selbstsynchronisation). Insbesondere in der streitkräftegemeinsamen Betrachtung wird deutlich, dass sich die Informationssystematik der heutigen Führungsorganisation für eine netzwerkzentrierte Streitkraft als unzureichend erweist. Derzeitige Informations- und Kommunikationsbeziehungen sind weitestgehend an die Führungshierarchie gebunden. Dies verzögert unverhältnismäßig die Weitergabe von Informationen und führt zu mangelnder Transparenz.

Um das sich bietende Potential von NetOpFü nutzen zu können, gilt es daher, die bestehende Informationssystematik im Sinne des gewählten Ansatzes anzugleichen. Die frühzeitige Integration aller Organisationsbereiche und auch der Potentiale verbündeter Streitkräfte sind in diesem Zusammenhang unerlässlich. Dies bedeutet aber nicht, dass grundsätzlich bestehende Führungsorganisationen in Frage gestellt werden müssen. Entscheidend ist, dass die Verantwortungsbereiche und Querverbindungen klar geregelt sind.

Führungsverfahren

Ziel muss es sein, Führungsverfahren zu etablieren, die mit Hilfe von NetOpFü eine Beschleunigung des Führungsprozesses sicherstellen. Im Grundsatz bleibt der Führungsprozess in seiner jetzigen Form erhalten. NetOpFü steigert jedoch die auf den Führungsprozess einwirkende Informationsqualität durch konsequente Nutzung des virtuellen Informationsraumes. Im Ergebnis werden der Führungsprozess als Ganzes bzw. einzelne Phasen vor allem in der laufenden Operationsführung verkürzt. Dabei kommt es darauf an, überlegene Informationen in eine überlegene Operationsführung zu übersetzen.

Um die Komplexität, die durch die Informationsfülle und die zu erwartende Entscheidungsvielfalt bestimmt wird, zu reduzieren, sind zunächst Entscheidungshilfen für den militärischen Führer bereitzustellen, welche die Informationsvielfalt auf ein handhabbares Maß verdichten, aufbereiten und Vorschläge zur Entscheidung anbieten. Exemplarisch sei an dieser Stelle auf die Möglichkeiten moderner Instrumente und Verfahren zur Entscheidungsunterstützung sowie auf integrierte, automatisch im Hintergrund ablaufende Simulationssysteme im Sinne eines Wargaming hingewiesen. Die Führungsunterstützung ist dabei hinsichtlich ihrer Qualität so auszulegen, dass zusätzliche Potentiale erschlossen werden, die eine adäquate Bewältigung nicht vorhergesehener Lageänderungen zeitgerecht zulassen.

Die Aufbereitung und Bereitstellung der Information orientiert sich dabei an einer Kombination aus Angebot (Push) und Nachfrage (Pull). Im Einzelnen bedeutet dies, dass diejenigen Informationen zur Verfügung gestellt werden, die für die Auftragserfüllung unerlässlich sind. Darüber hinaus besteht jederzeit die Möglichkeit, zusätzliche Informationen aus dem Informationsraum abzurufen. Hierbei gilt es, den Grundsatz der ebenen- und auftrags- sowie der zeitgerechten Informationsbereitstellung zu berücksichtigen.

Die Interoperabilität von Streitkräften im erweiterten Einsatzspektrum ist mit Hilfe geeigneter technischer, prozeduraler und operationeller Verfahren sicherzustellen. Erst dadurch wird die nationale Führungs- und Bündnisfähigkeit zukunftsgerichtet ermöglicht. Wegen unvermeidbarer Überschneidungen sind in der Bewertung unter Gesichtspunkten der vernetzten

Operationsführung ein bis dato unzureichendes Informationsmanagement und ein fehlendes umfassendes Wissensmanagement als zentrale Herausforderung zu nennen.

Führungsphilosophie

Hinsichtlich der Führungsphilosophie in vernetzten Strukturen (Abbildung 16) muss erkannt werden, dass das Prinzip „Führen mit Befehl“ (Befehlstaktik) an Qualität gewinnt, da in Abhängigkeit von der Bedeutung einer Aktion bzw. eines Ereignisses ein Durchgriff von höherer Stelle auf die Durchführungsebene direkt möglich ist. Gleichwohl ist die Anwendung des Prinzips „Führen mit Befehl“ die Ausnahme, weil sie das Potential von NetOpFü nicht optimal zur Wirkung bringt. Situativ kann dieser Ansatz jedoch erforderlich sein, um weitreichende Konsequenzen einer Entscheidung direkt steuern zu können.

Nationen, die sich für die Implementierung von Fähigkeiten zur vernetzten Operationsführung entschieden haben, setzen daher zunehmend auf das Führungsprinzip „Führen mit Auftrag“ (Auftragstaktik). Die Vernetzung bietet dabei insbesondere die Möglichkeit, die Absicht der übergeordneten Führung auf allen Ebenen transparent zu gestalten. Die mit der Anwendung des Prinzips „Führen mit Auftrag“ verbundene Delegation von Aufgaben, Kompetenzen und Verantwortlichkeiten entspricht dabei in besonderer Weise den Bedürfnissen des NetOpFü-Gedankens nach weitest gehender Dezentralisierung. In diesem Sinne fördert die Vernetzung die Anwendung der Auftragstaktik. Im Vergleich zu den Streitkräften anderer Nationen verfügt die Bundeswehr schon heute über den entscheidenden Vorteil, das Führungsprinzip „Führen mit Auftrag“ als Handlungsmaxime und wesentlichen Bestandteil der Inneren Führung etabliert zu haben.

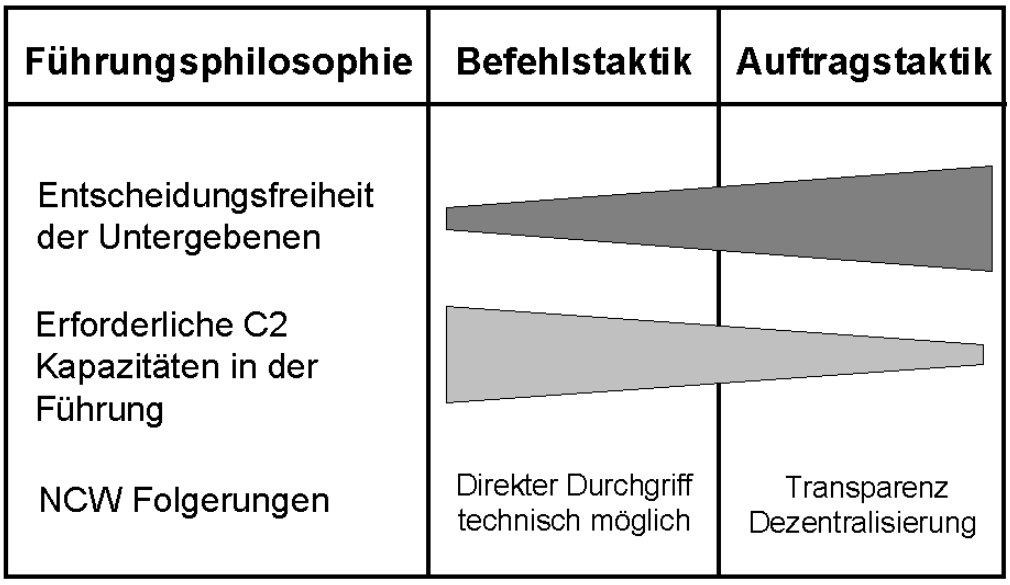

Abbildung 16: Führungsphilosophien und NCW/NetOpFü

Herausforderungen bei der Einführung netzwerkzentrischer Fähigkeiten

Netzwerkzentrierte Streitkräfte werden maßgeblich durch ihre Organisationsstrukturen sowie ihren Umgang mit Informationen bestimmt. Heute wie Morgen steht allerdings der Mensch

im Mittelpunkt des Systems Streitkräfte. Als verantwortungsvoller Entscheidungsträger, kreativer Bediener oder intelligenter Nutzer besetzt er die Knotenpunkte des grundlegenden Informations- und Handlungsnetzwerkes.

Die zu steigernde Führungsfähigkeit ergibt sich aus der Qualität des Zusammenwirkens von Mensch, Information und Organisation. Ergänzt um geeignete Sensoren und Effektoren, ergibt sich schließlich die Einsatzwirksamkeit, wie sie im Rahmen der Darstellung effektbasierter Operationen bereits beschrieben worden ist (Abbildung 17). Im Zeitalter limitierter Ressourcen scheint es darüber hinaus angebracht, NetOpFü auch an seinen Auswirkungen auf die Wirtschaftlichkeit von Streitkräften zu messen.

Im Zusammenhang mit NetOpFü sind häufig Bedenken, ja fast Ängste vor der zunehmenden Komplexität moderner Informations- und Waffensysteme festzustellen. Ein subjektiv empfundener Zuwachs von Stress sowie vielschichtige Symptome der Überforderung deuten dabei auf die Gefahr des Überschreitens der Grenze menschlicher Leistungsfähigkeit hin. Deswegen ist beim umfassenden Einsatz moderner Informationstechnologie vor allem der Mensch-Maschine-Schnittstelle besondere Aufmerksamkeit zu widmen, wobei der Mensch selbst keineswegs der limitierende Faktor ist.

Bei der Auswahl neuen Personals gilt es, die zu fordernden Schlüsselkompetenzen und Qualifikationen neu zu bewerten. Die Fokusverschiebung wird unter anderem zu einer zunehmenden Bedeutung von Innovationsbereitschaft, Lernfähigkeit und Technologieverständnis führen. Diese Kompetenzen und Qualifikationen sind auch im Rahmen der Ausbildung zu fördern. Der fortschreitende Wandel hin zu netzwerkzentrierten Streitkräften wird von einer nachhaltigen Fortentwicklung der Organisationsphilosophie und -kultur begleitet werden. Die Prinzipien Auftragstaktik und moderne Menschenführung können mit Rücksicht auf das Herausforderungsfeld Mensch bereits heute auf der Haben-Seite verbucht werden.

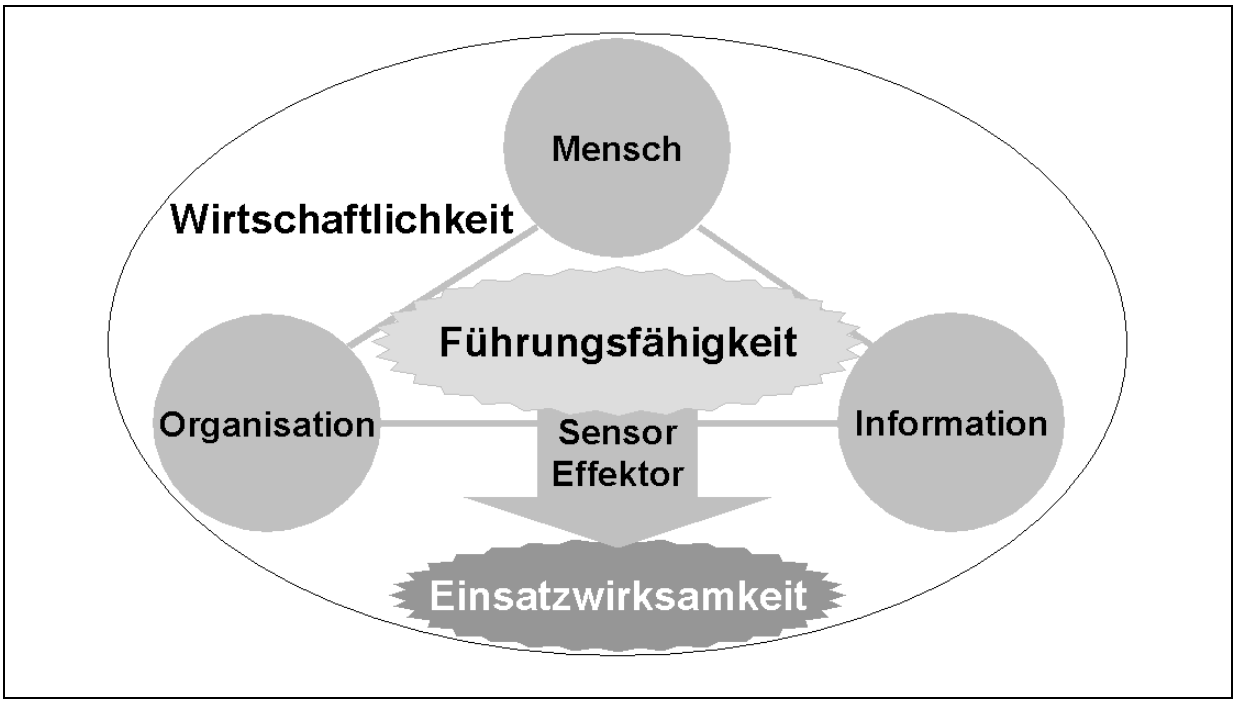

Abbildung 17: Bestimmungsfaktoren der Einsatzwirksamkeit

Neben der genannten Fortentwicklung der Organisationsphilosophie erfordert NetOpFü zukünftig möglicherweise auch eine Anpassung der Organisationsstrukturen. Obwohl das hierarchische Grundprinzip des Militärs unverändert erhalten bleiben wird, bergen umfassende Vernetzung und zunehmende Dezentralisierung die bereits erwähnten Gefahren der Verantwortungsdiffusion und des Mikromanagements in sich. Um diesem Risiko begegnen zu können, muss in einem iterativen Prozess unter enger Berücksichtigung dynamischer Netzwerkstrukturen und Informationsströme eine Anpassung eingeleitet werden. Dabei ist der Schwerpunkt im Bereich der Verfahren anzusiedeln, wodurch der Trend zur konsequenten Prozessorientierung zusätzlich verstärkt wird. Nur auf diese Weise können flexible und modulare Strukturen geschaffen werden, die für netzwerkbasierte Streitkräfte in diesem Bereich notwendig sein werden. Im Detail sind dabei ein umfassendes Informationskonzept sowie eine klare Zuweisung von Verantwortlichkeiten von entscheidender Relevanz.

Der Einsatz intelligenter Schnittstellen wird helfen, die aufkommende und unausweichliche Datenflut zu bewältigen. Die kontinuierliche Integrität und Validität aller Daten muss durch geeignete, nach innen wie außen wirksame robuste Sicherheitsstrukturen und -maßnahmen sowie angemessene Redundanzen gewährleistet werden. Dazu zählt z.B. auch die Absicherung gegen gegnerische und das Ermöglichen eigener Informationsoperationen (Information Warfare). So kann es gelingen, das Ziel einer dauerhaften Informationsüberlegenheit zu erreichen und diese in einen Wirkungsvorteil zu übersetzen. Gleichzeitig kann Informationsdominanz ein nicht-letales Wirkmittel unterhalb der Schwelle des Einsatzes bewaffneter Gewalt sein. Das Gesamtsystem netzwerkbasierter Streitkräfte muss in das streitkräftegemeinsame, multinationale und zivile Netzwerk im Rahmen eines breiten, ganzheitlichen Ansatzes eingebettet werden.[26]

Implementierung von NetOpFü

Ein gangbarer Weg zur Implementierung von NetOpFü orientiert sich analog zu den zuvor skizzierten Herausforderungsfeldern an den drei Ebenen Mitarbeitende, Organisation und Technologie.

Mitarbeitende

Auf der Ebene der Mitarbeitenden gilt es zunächst, durch eine gezielte Kommunikation und einen breiten Dialog die uneingeschränkte Aufgeschlossenheit gegenüber NetOpFü zu wecken. Es muss ein ganzheitlicher Prozess des Umdenkens auf allen Ebenen eingeleitet werden, der sowohl kognitiv als auch affektiv wirkt. Dabei ist einem Top-Down-Ansatz zu folgen. Parallel dazu muss NetOpFü in der Dokumentenhierarchie der Streitkräfte als umfassende und streitkräftegemeinsame Doktrin verankert werden. Mit dem Ziel einer schnellen Erstbefähigung muss diese Doktrin gleichzeitig die Grundlage für die Rüstungssteuerung sowie für das Controlling im Führungsprozess der Streitkräfte sein. Durch die Personalführung müssen vorhandene Fachkompetenzen besser ausgenutzt werden. Ebenso sollten Laufbahnmodelle angepasst werden, um bereits für NetOpFü qualifiziertes Personal mit erhöhter Durchläs-

[26] Siehe hierzu auch die Ausführungen von Heiko Borchert in diesem Band.

sigkeit zu fördern. Ferner sollten auch die Quoten für IT-Studiengänge innerhalb der Streitkräfte angehoben werden.[27] NetOpFü ist in alle Ausbildungsgänge zu integrieren, um die Nutzung der neuen Möglichkeiten bei den Mitarbeitern zu verankern. Auf moderne Menschenführung und Auftragstaktik kommt im NetOpFü-Umfeld eine gestiegene Bedeutung zu.

Organisation

Auf der Ebene Organisation müssen Strukturen und Verfahren angepasst werden. Eine derartige Strukturerweiterung entspräche der verbreiteten Forderung nach „Denkfabriken", die zu leistungsfähigem konzeptionellen und ganzheitlichem Denken befähigt sind und ebenfalls zu einer vermehrten taktischen, operationellen, aber auch konzeptionellen Schulung/Ausbildung des militärischen Schlüsselpersonals beitragen können. Das Zentrum für Analysen und Studien der Bundeswehr (ZASBw) kann hierzu einen bedeutenden Beitrag leisten.

Daneben wird es aber auch darum gehen, vermehrt nicht-militärische Entscheidungsträger und Multiplikatoren in die konzeptionelle Arbeit einzubinden, um zu gemeinsamen Lösungen zu kommen. Ziel ist der Aufbau eines strategischen Weiterentwicklungsnetzwerkes mit aktiver Teilhabe an nationalen und internationalen Foren, Schulungen und Übungen. Um im Vergleich zu sich ständig weiterentwickelnden Streitkräften anderer Nationen bestehen zu können, muss die Bundeswehr den Weg hin zu flexibleren und modularen Strukturen konsequent weiter gehen.

Technologie

Auf der Ebene Technologie muss zuerst ein Soll-Ist-Vergleich als Bestandsaufnahme erfolgen. Bei der weiteren technischen Realisierung ist eine anfängliche Beschränkung auf Entwicklung und Verbindung von Teilsystemen durchaus akzeptabel, wobei Insellösungen zu vermeiden sind. Hierzu sind Führungs-, Führungsinformations- und Fachinformationssysteme zu integrieren, so dass ein aktueller und konsistenter Datenbestand im Format NATO-weit abgestimmter Datenbankmodelle implementiert wird. [28]

Auch taktische Datenlinks (TDL) sollten einen Schwerpunkt zukünftiger Investitionen und Beschaffungen darstellen, da diese ein Schlüssel zum Gesamtverbund sind. Ferner sollte im Hinblick auf Wirtschaftlichkeit vorrangig eine Beschaffung handelsüblicher und bereits verfügbarer Systeme (Commercial off the Shelf, COTS) angestrebt werden. Außerdem muss die prozessorientierte Verknüpfung aller Entitäten verstärkt werden. Der Abstimmung von

[27] Da die wirkungsorientierte Operationsführung ein besseres Verständnis der gegnerischen Motive, Fähigkeiten und Verwundbarkeiten erfordert, wird auch die Bedeutung der sozial- und kulturwissenschaftlichen Lehrfächer zunehmen.

[28] Für die Integration von Führungssystemen (FüSys), Führungsinformationssystemen (FüInfoSys) und Fachinformationssystemen (FachInfoSys) werden bereits seit einigen Jahren im Rahmen der „Joint Warrior Interoperability Demonstrations (JWID)" Prototypen eingesetzt, die diese Integration leisten. Hierbei werden die Daten einzelner Inselsysteme über Translator-Boxen in ein NATO-weit akzeptiertes und damit interoperables Datenbankmodell überführt. Da die Translator-Boxen bidirektional funktionieren, können die einzelnen Inselsysteme in den konsistenten Datenbestand integriert werden. Diese Lösung macht es nicht erforderlich, die gesamte IT-Landschaft der Streitkräfte auszuwechseln, um die C2-spezifischen Fähigkeiten zur vernetzten Operationsführung zu erlangen.

Schnittstellen sowie der internationalen Standardisierung von Datenformaten kommt dabei eine entscheidende Bedeutung zu.

Wir sollten zwar schnell zu einer Erstbefähigung zu NetOpFü gelangen, doch bedeutet dieses nicht, dass wir erst anfangen können, wenn alle transformationsrelevanten Schritte umgesetzt sind. Vielmehr sollten neue Verfahren angewendet werden, die das Nebeneinander von konzeptioneller Entwicklung und gleichzeitiger Umsetzung ermöglichen, wie das in der Privatwirtschaft z.B. im Rahmen des Rapid Prototyping bereits erfolgreich praktiziert wird. Absolute Voraussetzung für erste Erfolge ist jedoch ein breites Engagement aller Beteiligter. Ferner sind – und dieses ist für die Bundeswehr bereits eingeleitet – Priorisierungsentscheidungen notwendig. Alle Investitionen, die der vernetzten Operationsführung dienen, müssen Vorrang haben; „nicht-NetOpFü-fähige" Projekte sollten keine Zukunft haben. Die Beantwortung der Frage nach der Zukunftsfähigkeit unserer Streitkräfte hängt am Ende davon ab, ob sie die dargestellten Herausforderungen meistern können. Hier geht es vor allem um die nachhaltige Befähigung zur effizienten Teilhabe an EBO und vernetzte Operationen im streitkräftegemeinsamen und multinationalen Verbund.

Zusammenfassung

Moderne Wissens- und Informationsgesellschaften sind durch ihre weitreichende und unaufhaltsam fortschreitende Vernetzung bestimmt. Sie basieren entscheidend auf der allgegenwärtigen Verfügbarkeit der Ressource Information, während die Bedeutung klassischer „Regelgrößen" wie Raum und Kräfte kontinuierlich abnimmt. Potentielle Gegner und Aggressoren werden nichts unversucht lassen, diese gesellschaftliche Entwicklung für ihre Ziele zu nutzen. Dementsprechend lässt sich derzeit eine weltweite Diversifizierung von Konflikttypen und Szenarien mit qualitativ unterschiedlichen Akteuren und steigender Asymmetrie (z.B. durch Weapons of Mass Effect, effektbasierte Waffen) beobachten. Erschwert wird deren Beherrschbarkeit durch ein Kaleidoskop an nur unzureichend kontrollierbaren und einzudämmenden Risiken wie Proliferation oder Verfügbarkeit militärischer Hochtechnologie für nichtstaatliche Akteure (z.B. durch Military off the Shelf-Technologie, MOTS).

Operationen werden künftig in einem zunehmend komplexer werdenden und diffuseren Bedrohungsspektrum erfolgen. Gefechtsfelder reichen dabei von allen multidimensionalen natürlichen Gegebenheiten bis in urbane und virtuelle Räume. Einsatzwirksamkeit und Leistungsfähigkeit von Streitkräften werden vor allem von ihrer Führungsfähigkeit abhängen. Streitkräfte müssen hierfür flexibel, anpassungs- und vor allem lernfähig sein. Die operativen Faktoren Zeit und vor allem Information gewinnen überproportional an Bedeutung; entscheidend ist im Sinne eines effizienten Wissensmanagement der zielorientierte Erkenntnisgewinn. Verkürzte Reaktionszeiten und komplexer werdende Multidimensionalität werden den Menschen bei Beibehaltung „konventioneller" Strukturen und Denk- und Entscheidungsprozesse möglicherweise überfordern sowie eine zielgerichtete Führungsleistung erheblich erschweren. Um dies zu verhindern und um durch Informationsüberlegenheit einen Gefechtsvorteil zu erlangen, sind Ideen und neue Konzepte unverzichtbar.

An dieser Stelle wird NetOpFü einen entscheidenden Beitrag leisten können. NetOpFü ist mehr als eine rein technologische Vision von der zeitverzugslosen Informationsbereitstellung

in allumfassenden Netzen. NetOpFü ist eine Führungsphilosophie, die altbekannte Stärken der Auftragstaktik mit modernsten Mitteln der Informationstechnologie synergetisch verbindet. Durch den zu erwartenden Leistungszuwachs bei der Entscheidungsfindung wird der Entscheidungsträger noch effektiver. Die Etablierung von NetOpFü als Vision zukünftiger Streitkräfte ist eine Führungsaufgabe, die bereits in Angriff genommen worden ist; die tatsächliche Implementierung und Ausgestaltung eines deutschen NetOpFü-Konzepts bedarf allerdings noch intensiver analytischer Anstrengungen und budgetärer Priorisierungsentscheidungen.

Heiko Borchert

Vernetzte Sicherheitspolitik und die Transformation des Sicherheitssektors: Weshalb neue Sicherheitsrisiken ein verändertes Sicherheitsmanagement erfordern*

Die moderne Sicherheitspolitik bewegt sich in einem Spannungsfeld. Einerseits erfordert der erfolgreiche Kampf gegen die neuen Risiken und ihre Ursachen den schnellen und koordinierten Einsatz der zur Verfügung stehenden Fähigkeiten und Mittel. Andererseits wird die Erfüllung dieser Forderung durch die bisherige Organisation der Sicherheitspolitik erschwert. Zu viele der neuen sicherheitspolitischen Aufgaben sind „institutionell heimatlos", das heißt es fehlt die klare Zuordnung von Verantwortung, Kompetenzen und Mitteln zu deren Bewältigung.[29]

Die Feststellung, dass Sicherheitspolitik heute weder ausschließlich national noch ressortspezifisch betrieben werden kann, sondern internationale und ressortübergreifende Konzeption und Koordination erfordert, ist nicht wirklich neu. Gleichwohl wurde bislang mit zu wenig Nachdruck an der Umsetzung der daraus resultierenden Konsequenzen gearbeitet. In einem umfassenden Verständnis von Sicherheit ist die Verteidigung einer von mehreren Politikbereichen und das Militär eines von mehreren Instrumenten. Militärisch relevante Konzepte und Entwicklungen müssen daher vor diesem umfassenden Hintergrund interpretiert werden. Das gilt insbesondere für das Konzept der vernetzten Operationsführung, die im Kern die richtige Antwort auf die neue Herausforderung gibt – nämlich die Vernetzung der relevanten Akteure, ihrer Mittel und ihrer Organisationen.[30]

Der vorliegende Aufsatz schlägt deshalb die gedankliche Brücke von der vernetzten Operationsführung zur vernetzten Sicherheitspolitik und stellt diese als neue Leitidee des Sicherheitsmanagements im 21. Jahrhundert vor. Zu diesem Zweck begründet der erste Abschnitt zunächst die Notwendigkeit des Übergangs zur vernetzten Sicherheitspolitik, die sich durch konsequente Prozess-, Fähigkeits-, und Wirkungsorientierung anstelle der bisherigen Ressortorientierung auszeichnet. Daran anschließend werden die Herausforderungen und die Konsequenzen der vernetzten Sicherheitspolitik mit Blick auf die Transformation des Sicherheitssektors – d.h. militärische, polizeiliche, paramilitärische Streitkräfte, Grenzschutz, Nachrichtendienste, die entsprechenden Ministerien sowie die politischen Aufsichts- und Koordinationsorgane – analysiert. Die Ausarbeitung schließt mit einigen Überlegungen zur künftigen Rolle sicherheitspolitischer Vernetzungsorgane und zum europäischen Handlungsbedarf.

---

* Leicht überarbeitete Fassung eines Beitrags, der in der Reihe „Positionspapiere zur Sicherheitspolitik" des Büros für Sicherheitspolitik des Bundesministeriums für Landesverteidigung, Wien, veröffentlicht worden ist.

29 Ashton B. Carter, „Keeping the Edge. Managing Defense for the Future", in Ashton B. Carter and John P. White (eds.), *Keeping the Edge. Managing Defense for the Future* (Cambridge, London: MIT Press, 2001), S. 2.

30 So auch: Mey/Krüger, *Vernetzt zum Erfolg?,* S. 16.

Vernetzte Sicherheitspolitik

Es sind im wesentlichen drei Entwicklungen, die den Übergang von der ressortgesteuerten zur vernetzten Sicherheitspolitik bedingen (Abbildung 18):[31]

Erstens hat die Erosion des staatlichen Gewaltmonopols bei gleichzeitiger Privatisierung der Gewalt und dem Aufstreben nichtstaatlicher Gewaltakteure in zahlreichen Regionen der Welt ein neues Konflikt- und Risikobild geschaffen. Daraus resultieren neue Gefahren für die internationale Stabilität und Sicherheit wie beispielsweise die Proliferation von Massenvernichtungswaffen oder ethnisch motivierte Kriege, die zu Massenvertreibungen führen können. Weil die Anwendung von Gewalt in diesen Regionen wirtschaftlich vorteilhaft ist, entstehen sogenannte Bürgerkriegsökonomien, die über die weltwirtschaftliche Verflechtung direkt mit den Industrieländern verknüpft sind. Das neue Risikobild schlägt somit direkt und indirekt auf die stabilen Regionen der Welt zurück und erschwert dadurch die Unterscheidung zwischen innerer und äußerer Sicherheit sowie den Einsatz der dafür bislang vorgesehenen Mittel.

Geht es, zweitens, um die Bekämpfung dieser neuen Risiken sowie ihrer Ursachen, so wird schnell klar, dass dafür in doppelter Hinsicht neue Operationstypen gefordert sind. Einerseits zeigt die jüngste Entwicklung internationaler Stabilisierungsoperationen, dass die dazu eingesetzten Kräfte neben den klassischen Kampfaufgaben vermehrt neue Schutzaufgaben übernehmen. Dadurch kommt es zu einer Vermischung von militärischen mit polizeilichen Aufgaben in einem bislang konzeptionell kaum durchdrungenen Graubereich. Andererseits wirkt die trennscharfe Unterscheidung zwischen militärischen, politischen, wirtschaftlichen und gesellschaftlichen Mitteln der Konfliktlösung zusehends dysfunktional, da alle Mittel in verschiedenen Phasen der Konfliktverhütung und -bewältigung in unterschiedlicher Weise aufeinander angewiesen sind.

In Europa erhöht, drittens, die Vertiefung und die Erweiterung der Europäischen Union (EU) den Druck zur kohärenten Politikvorbereitung und -umsetzung. Inhaltlich müssen die vielfältigen und teilweise neuen Instrumente der EU-Außen-, Sicherheits- und Verteidigungspolitik besser mit den vorhandenen Instrumenten der Außenwirtschafts- und der Entwicklungs- sowie der Justiz- und der Innenpolitik abgestimmt werden.[32] Das bleibt nicht ohne Rückwirkung auf die nationalen Planungen und Konzepte in diesen Politikbereichen sowie deren Abstimmung mit internationalen Beschlüssen.

Diese drei politischen Treiber erklären, weshalb die sicherheitspolitische Vernetzung immer wichtiger wird. Daneben gilt es aufgrund des technologischen Fortschritts einen vierten Aspekt zu berücksichtigen, der diese Vernetzung im Sinne der technischen Verknüpfung der Sicherheitsministerien und -akteure auch tatsächlich möglich macht. Die daraus resultierenden Optionen wurden in den 90er Jahren vor allem von den US-amerikanischen Streitkräften erkannt und unter dem Hinweis auf eine sich abzeichnende Revolution in Military Affairs (RMA) in neuen Konzepten umgesetzt.[33] Die Idee der vernetzten Operationsführung (auch als

[31] Basierend auf: Heiko Borchert und Reinhardt Rummel, „Von segmentierter zu vernetzter Sicherheitspolitik in der EU-25“, *Österreichische Militärische Zeitschrift* 42 (2004, i.V.)

[32] Hierzu beispielsweise: *A Secure Europe in a Better World,* 15895/03, Brüssel, 8. Dezember 2003, S. 9 <http://register.consilium.eu.int/pdf/en/03/st15/st15895.en03.pdf> (Zugriff: 20. Januar 2004).

[33] Siehe hierzu neben den Beiträgen in diesem Band auch Bill Owens with Ed Offley, *Lifting the Fog of War* (Baltimore, London; The Johns Hopkins University Press, 2001); Eliot A. Cohen, „A Revolution in War-

Network Centric Warfare, NCW, bekannt) stellt die logische Fortsetzung der vor allem auf das Ziel der Informationsüberlegenheit ausgerichteten Bemühungen dar. Ziel ist es „ [to network] sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization. “[34] Die wesentlichen Vorteile liegen in der erhöhten Transparenz hinsichtlich des Lagebildes (Battlespace Awareness), der Verkürzung der Entscheidungsprozesse, der Erhöhung des Operationstempos und der verbesserten Wirkung im Einsatz. Wie in der Folge dargestellt wird, lassen sich diese Überlegungen sinngemäß auf die Reorganisation des gesamten Sicherheitssektors übertragen.

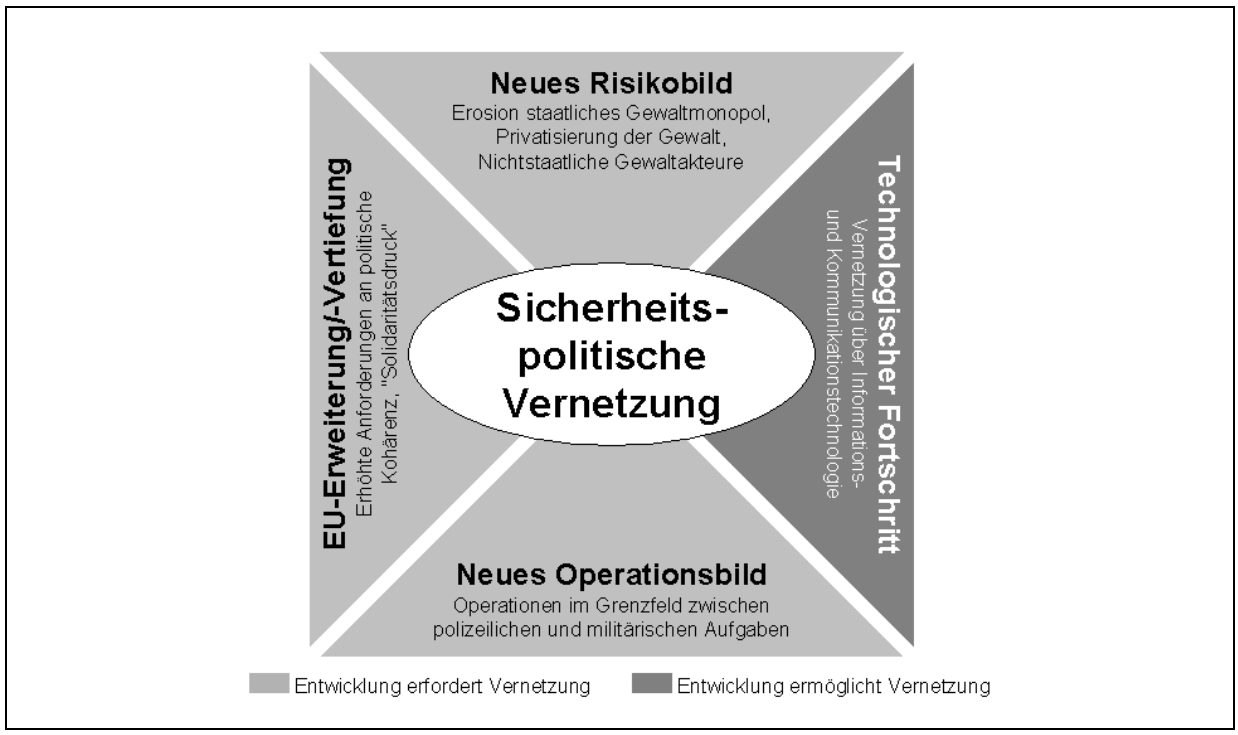

Abbildung 18: Treiber der sicherheitspolitischen Vernetzung

Die aus den eben beschriebenen Entwicklungen abgeleitete Forderung nach einer sicherheitspolitischen Vernetzung basiert auf der Einsicht, dass sicherheitsrelevante Akteure (z.B. Sicherheitskräfte, Ministerien, Industrie etc.) die aktuellen und künftigen Herausforderungen nur dann meistern können, wenn sie ihre Ziele, ihre Prozesse und Strukturen sowie ihre Fähigkeiten und Mittel bewusst miteinander vernetzen.[35] Neu an diesem Verständnis sind die Erweiterung des relevanten Akteurskreises sowie die bewusste Durchbrechung bestehender

fare,“ *Foreign Affairs* 75:2 (March/April 1996), S. 37-54; Michael O’Hanlon, *Technological Change and the Future of Warfare* (Washington, D.C.: Brookings, 2000).

[34] David S. Alberts, John J. Garstka, Frederick P. Stein, *Network Centric Warfare. Developing and Leveraging Information Superiority,* 2nd ed (Washington, D.C.: CCRP, 2000), S. 2.

[35] Ähnlich auch betriebswirtschaftliche Konzepte, die unter Netzwerkfähigkeit die Fähigkeit einer Geschäftseinheit verstehen, ihre Wettbewerbsposition durch Vernetzung zu verbessern. Siehe: Elgar Fleisch, *Das Netzwerkunternehmen. Strategien und Prozesse zur Steigerung der Wettbewerbsfähigkeit in der „Networked Economy“* (St. Gallen: Springer Verlag AG, 2001), S. 208.

Organisationsgrenzen. Sicherheitspolitische Vernetzungsfähigkeit bezieht sich demzufolge auf die

- zu berücksichtigenden Ebenen der Beschlussfassung und der Umsetzung (z.B. supranational, national und sub-national),
- einzubeziehenden bzw. zu berücksichtigenden Akteure (z.B. Staaten, Nichtregierungsorganisationen, Unternehmen, Sicherheitskräfte),
- zu erbringenden Aufgaben (z.B. Konfliktprävention, Krisenmanagement, Intervention, Friedensaufbau und -erhaltung),
- zur Auswahl stehenden Instrumente (z.B. diplomatische, wirtschaftliche, militärische, polizeiliche Mittel).

Die Forderung nach konsequenter sicherheitspolitischer Vernetzung hält Herausforderungen von neuer Komplexität bereit. Das gilt für die Reform der militärischen Streitkräfte genauso wie für die Neugestaltung der nationalen sowie der internationalen Sicherheitssektoren. In vielerlei Hinsicht ist die Reform der Sicherheitssektoren sogar die Voraussetzung, damit die militärischen Streitkräfte reibungslos mit den anderen Sicherheitskräften kooperieren können und dadurch maximale Synergiegewinne realisiert werden. „If adapting to wartime conditions is desperately difficult," so führen Williamson Murray und MacGregor Knox in ihrer Untersuchung über historische und künftige militärische Revolutionen aus, „those involved in peacetime innovation confront almost insoluble problems: it is here that the leaders of military institutions earn their pay."[36] Diese Schlussfolgerung kann nahtlos auf die Erwartungen an die politischen Entscheidungsträger übertragen werden, denn es sind in erster Linie diese, die die Grundlagen für die sicherheitspolitische Vernetzung schaffen müssen.

In der Folge geht es deshalb vor allem darum, in einer Auswahl grundlegende Konsequenzen aus dem Übergang von der segmentierten zur vernetzten Sicherheitspolitik zu erläutern und Ansätze zur Bewältigung der damit verbundenen Herausforderungen aufzuzeigen. Im Vordergrund stehen dabei fünf Themenschwerpunkte: Erstens verstärkt die sicherheitspolitische Vernetzung die gegenseitige Abhängigkeit im Normal- bzw. im Krisenfall und lenkt damit die Aufmerksamkeit auf den Zusammenhang zwischen der Kompatibilität der politischen Systeme der Koalitionspartner und der daraus resultierenden Entscheidungs- bzw. Handlungsfähigkeit. Damit verbindet sich, zweitens, die Frage, ob und wie Koalitions- bzw. Zusammenarbeitsfähigkeit im Zeitalter der Vernetzung möglich und welche Akteure dabei zu berücksichtigen sind. Drittens rückt diese Frage das Management der nationalen Sicherheitssektoren ins Zentrum der Aufmerksamkeit, denn das Vernetzungsparadigma erfordert funktionsorientierte und organisationsübergreifende anstelle ressortspezifischer Lösungsansätze. Dadurch gewinnen, viertens, sogenannte vernetzte Fähigkeiten an Bedeutung, weil sie wesentlich zur verbesserten Zusammenarbeit zwischen den Sicherheitskräften beitragen. Und zu guter Letzt ist der Blick auf die Rüstungsindustrie als Trägerin einer Vielzahl entscheidender Kompeten-

[36] Williamson Murray and MacGreogor Knox, „Thinking about revolutions in warfare", in MacGregor Knox and Williamson Murray (eds.) *The dynamics of military revolution 1300-2050* (Cambdrige: Cambridge University Press, 2001), S. 14.

zen zu richten, wobei insbesondere nach neuen Formen der Zusammenarbeit zwischen dem öffentlichen Sicherheitssektor und der Industrie zu fragen ist.

Kompatibilität der politischen Systeme

Die Befürworter der vernetzten Operationsführung argumentieren, dass der erhöhte Informationsaustausch die Qualität der Information steigert, die Aussicht auf ein gemeinsames Lagebild verbessert und damit die enge Zusammenarbeit und die teilautonome Führung (Self-Synchronization) der an einer Operation Beteiligten ermöglicht.[37] Die Realisierung dieser Vorteile steht jedoch unter einem Vorbehalt:

> (...) the operations an RMA [Revolution in Military Affairs] will make possible and necessary will not achieve their most potent form unless the interagency process can meet the demands of revolutionized military forces. (…) If operations are too fast for coordination with policymakers, then they will be ineffective, no matter how successful militarily, because they will *unfold before policy can properly shape them.* Worse, operations may present policymakers with faits accomplis and thus determine policy.[38]

Diese Feststellung lenkt die Aufmerksamkeit auf einen bislang eher vernachlässigten Punkt: die Kompatibilität der politischen Systeme der an multinationalen Operationen beteiligten Staaten. Marc Houben und Dirk Peters haben kürzlich darauf hingewiesen, dass die erfolgreiche Entsendung multinationaler Einheiten ohne Synchronisation der Entscheidungsprozesse der daran beteiligten Staaten kaum möglich ist.[39] Die Bedeutung dieses Aspekts ergibt sich im wesentlichen aus drei Punkten. Erstens werden multinationale Operationen mit Beteiligung militärischer und anderer Sicherheitskräfte künftig den standardmäßigen Rahmen internationaler Einsätze bilden. Zweitens sieht der Entwurf des EU-Verfassungsvertrags die Einführung der Prinzipien der strukturierten Zusammenarbeit im militärischen Bereich vor und erhöht damit die Komplexität der intergouvernementalen Entscheidungsfindung.[40] Drittens steht vernetzte Operationsführung in unmittelbarem Zusammenhang mit der Idee wirkungsorientierter Operationen (Effects Based Operations), wobei deren Möglichkeiten und

---

[37] Mey/Krüger, *Vernetzt zum Erfolg?,* S. 23; Alberts/Gartska/Stein, *Network Centric Warfare*, S. 87-114; Arthur K. Cebrowksi and John J. Gartska, „Network-centric warfare: its origin and future," *Proceedings* 124:1 (January 1998), S. 28-36; *Network Centric Warfare. Department of Defense Report to Congress* (Washington, D.C.: Department of Defense, 2001), S. 3.1-3.18.

[38] David Tucker, „The RMA and the Interagency: Knowledge and Speed vs. Ignorance and Sloth," *Parameters* 30:3 (Autumn 2000), S. 66-76 <http://www.carlisle.army.mil/usawc/parameters/00autumn/tucker.htm> (Zugriff: 30. Dezember 2003), S. 2, 5 (Internetversion).

[39] Marc Houben and Dirk Peters, *The Deployment of Multinational Military Formations: Taking Political Institutions into Account,* CEPS Policy Brief No 36 (Brussels: Centre for European Policy Studies, 2003), <http://shop.ceps.be/downfree.php?item_id=1038?> (Zugriff: 20. Januar 2004), S. 1.

[40] Udo Diedrichs and Mathias Jopp, „Flexible Modes of Governance: Making CFSP and ESDP Work," *The International Spectator* 38:3 (July 2003), S. 15-30, hier S. 29. Siehe zur strukturierten Zusammenarbeit im Verteidigungsbereich Art. I-40.6 und Art. III-213 des Entwurfs zum EU-Verfassungsvertrag. Zit gemäss: Entwurf eines Vertrags über eine Verfassung für Europa, CONV 850/03, Brüssel, 18. Juli 2003, <http://european-convention.eu.int/docs/Treaty/cv00850.de03.pdf> (Zugriff: 20. Januar 2004).

Grenzen vor allem in internationalen Koalitionen wesentlich durch die Kohärenz der daran teilnehmenden Partner und deren Verhalten bestimmt wird.[41]

Die Kompatibilität der politischen Systeme der an einer Operation beteiligten Staaten kann unter inhaltlichen und strukturellen Gesichtspunkten untersucht werden.

Inhaltliche Kompatibilität

In diesem Bereich sind zuerst die bekannten Unterschiede zwischen den nationalen Sicherheitskulturen anzusprechen, die sich auf die grundsätzliche Bereitschaft zum Einsatz militärischer Streitkräfte sowie die damit verbundenen Vorgaben auswirken.[42] Wenn die Annahme zutrifft, dass es über die vernetzte Operationsführung zu einer Angleichung der militärischen Doktrin auf dem Weg der Technologieintegration kommt, dann ist es entscheidend, welcher Staat bzw. welche Staatengruppe federführend ist – zumindest solange, als nationale Unterschiede in der Einschätzung sicherheitspolitisch relevanter Risiken bestehen. Javier Solanas Entwurf einer EU-Sicherheitsstrategie kann in diesem Zusammenhang als wichtiger Baustein zur Angleichung der Perzeptionen interpretiert werden, indem er die wichtigsten sicherheitspolitischen Bedrohungen (Terrorismus, Proliferation von Massenvernichtungswaffen, regionale Konflikte, gescheiterte Staaten und Organisierte Kriminalität) analysiert und Europas strategische Ziele (Stabilität und gute Regierungsführung, funktionsfähige multilaterale Ordnung, Bekämpfung alter und neuer Risiken) definiert.[43]

Die Angleichung der Perzeptionen ist jedoch ohne Koordination – oder noch besser Harmonisierung – der politischen Ambitionen nicht zu erreichen. Hier liegt gerade im Hinblick auf die Anwendung der vernetzten Operationsführung ein Knackpunkt:

> Die amerikanische RMA wird von europäischen und asiatischen Verbündeten nicht kopiert werden [können]; vielmehr gilt es, die amerikanischen Aktivitäten gerade bezüglich NCW als Maßstab zu akzeptieren, jedoch *eigene* Antworten und Herausforderungen in gesellschaftlicher, wirtschaftlicher und militärischer Hinsicht zu finden, und eigene Fähigkeiten in den Prozess einzubringen, damit regionalen Erfordernissen Rechnung getragen und die Vernetzung mit den USA im *eigenen* Sinne mitgestaltet wird.[44]

Wie diese europäischen Antworten allerdings aussehen könnten, ist bislang unklar. Die weltweite Ausrichtung und die damit verbundene Forderung nach globaler Machtprojektion, die das US-Streben nach Informationsüberlegenheit und damit auch die konsequente Ausnutzung technologischer Fortschritte im militärischen Bereich erklären, finden in Europa keine entsprechende Antwort. Richtigerweise wird daher die Diskussion über ein europäisches

---

41 Edward A. Smith, *Effects-Based Operations. Applying Network Centric Warfare in Peace, Crisis, and War* (Washington, D.C.: CCRP Publications, 2003), S. 336-346.

42 Paul Cornish and Geoffrey Edwards, „Beyond the EU/NATO dichotomy: the beginnings of a European strategic culture," *International Affairs* 77:3 (May 2001), S. 587-603. Zum Konzept der Sicherheitskultur grundlegend: Ronald L. Jepperson, Alexander Wendt, and Peter J. Katzenstein, „Norms, Identity, and Culture in Natonal Security," in Peter J. Katzenstein (ed.), *The Culture of National Security. Norms and Identity in World Politics* (New York: Columbia University Press, 1996), S. 33-75.

43 *A Secure Europe in a Better World,* S. 5-12.

44 Mey/Krüger, *Vernetzt zum Erfolg?,* S. 17. Hervorhebungen im Original.

Leitbild der vernetzten Operationsführung dazu führen müssen, dass die während langer Zeit beiseite geschobene Frage nach der Rolle und dem Stellenwert militärischer Mittel als einem Instrument der Konfliktlösung und der Stabilisierung endlich beantwortet wird. Das ist die wesentliche Voraussetzung, um die im folgenden Abschnitt diskutierte Koalitions- und Zusammenarbeitsfähigkeit gewährleisten zu können.

Strukturelle Kompatibilität

Die Aspekte der inhaltlichen Kompatibilität kommen auch in den strukturellen Elementen des politischen Systems zum Ausdruck. Dabei sind insbesondere die Wechselwirkungen zwischen der Rolle und den Kompetenzen der politischen Behörden, der Entscheidungsfindung und den rechtlichen Rahmenbedingungen zu berücksichtigen. Alexander Siedschlag hat in einer vergleichenden Länderstudie gezeigt, dass die Regierungen Deutschlands, Frankreichs, Großbritanniens, Italiens und Schwedens bei der Entscheidung über Auslandeinsätze eine deutliche Vorrangstellung einnehmen, wobei in Deutschland und Schweden Parlamentsvorbehalte bestehen. Umfangreiche innenpolitische Abstimmungsbedürfnisse sind vor allem dann erforderlich, wenn es um größere, langfristige militärische Operationen geht und ein internationales Mandat nicht vorliegt.[45] Allerdings hat sich gerade Verteidigungsminister Peter Struck anlässlich des fiktiven Einsatzszenarios zur Entsendung der NATO Response Force, das beim informellen Ministertreffen in Colorado Springs (Herbst 2003) durchgeführt wurde, über die Langsamkeit deutscher Entscheidungsprozesse beklagt und Reformen angemahnt.[46]

Der Zusammenhang zwischen den Kompetenzen von Exekutive und Legislative sowie dem Tempo der Entscheidungsfindung ist vor dem Hintergrund des Kernnutzens der Beschleunigung von entscheidender Bedeutung. Auch wenn es richtig ist, dass der Informations- und der Handlungsbedarf auf der politischen und der militärischen Führungsebene unterschiedlich ausgeprägt sind und die vernetzte Operationsführung damit auf diesen Ebenen unterschiedlich beurteilt werden muss,[47] so besteht doch die Gefahr asymmetrischer Entscheidungsprozesse. Dass diese Gefahr die Effektivität der militärischen Operationsführung und damit auch die Kohärenz einer internationalen Koalition wesentlich beeinträchtigen kann, hat das Beispiel des Kosovo-Krieges eindrücklich vor Augen geführt.[48] Ebenso zeigen Einsatzauswertungen der US-Intervention in Afghanistan, dass innerhalb eines 20minütigen Sensor

---

[45] Alexander Siedschlag, „Nationale Entscheidungsprozesse bei Streitkräfteeinsätzen im Rahmen der Petersberg-Aufgaben der EU – Deutschland, Frankreich, Großbritannien, Italien, Schweden," in Erich Reiter et. al. (Hrsg.), *Europas ferne Streitmacht: Chancen und Schwierigkeiten der Europäischen Union beim Aufbau der ESVP* (Hamburg: Mittler, 2002), S. 222-232.

[46] „Struck will Einsätze schneller billigen können," *Süddeutsche Zeitung* 10. Oktober 2003 <http://www.sueddeutsche.de/deutschland/artikel/336/19317/print.html> (Zugriff: 20. Januar 2004). Die SPD-Fraktion hat am 20. Oktober 2003 einen ersten Entwurf des neuen Parlamentsbeteiligungsgesetzes vorgelegt.

[47] Milan Vego, „Net-centric is not decisive", *Proceedings* 129:1 (January 2001), S. 52-58; Milan Vego, „Network-Centric Warfare: its promises and problems," *Allgemeine Schweizerische Militärzeitschrift* 169:6 (Juni 2003), S. 24-27.

[48] John E. Peters et. al, *European Contributions to Operation Air Fore. Implications for Transatlantic Relations* (Santa Monica: RAND, 2001), S. 25-29; Bruce R. Nardulli et. al., *Disjointed War. Military Operations in Kosovo, 1999* (Santa Monica: RAND, 2002), S. 27, 32, 44-47, 115; Benjamin S. Lambeth, *NATO's Air War for Kosovo. A Strategic and Operational Assessment* (Santa Monica: RAND, 2001), S. 120-135, 184-189; Frederic L. Borch, „Targeting After Kosovo. Has the Law Changed for Strike Planners?" *Naval War College Review* 56:2 (Spring 2003), S. 64-81.

to Shooter-Zyklus' gut 18 Minuten für den Führungs- und Entscheidungsprozess benötigt wurden.[49]

Wenn es so ist, dass das durch die vernetzte Operationsführung erhöhte Maß an Flexibilität – das u.a. aus der Beschleunigung der militärischen Entscheidungen und der Operationsführung resultiert – zusätzliche Optionen eröffnet,[50] dann ist vor dem Hintergrund der jüngsten multinationalen Erfahrungen zu erwarten, dass die politischen Entscheidungsträger unter einem erhöhten Druck stehen, die politischen Ziele des Einsatzes Militäreinsatzes zu definieren.[51] Dabei ist davon auszugehen, dass die Wahrscheinlichkeit des politischen „Durchgriffs" auf die verschiedenen militärischen Führungsebenen, die gemäss Skeptikern zu übermäßiger Zentralisierung und Kompetenzstreitigkeiten in der Befehlsgebung führen kann,[52] vor allem dann am größten ist, wenn der Einsatz militärischer Mittel innenpolitisch umstritten ist. Sind die politischen Zielsetzungen der militärischen Intervention nicht klar definiert, wird die Politik – nicht zuletzt unter dem Druck der öffentlichen Meinung bzw. mit Blick auf die Wählerunterstützung – laufend nachsteuern. Dabei muss u.a. auch der Eindruck vermittelt werden, dass die politischen Entscheidungsträger das Zepter in der Hand halten, und dies können sie durch „Mikromanagement" nachhaltig unterstreichen. Diese Hypothese lässt sich aus Martha Finnemores Untersuchung ableiten, die aufzeigt, dass sich die Gründe zur Rechtfertigung militärischer Intervention in jüngster Zeit wesentlich verändert haben. Ausschlaggebend dafür waren u.a. der abnehmende normative Wert militärischer Gewalt in der internationalen Politik und die zunehmende Verrechtlichung derselben.[53] Gerade rechtliche Aspekte spielen unter den Gesichtspunkten der vernetzten Operationsführung eine wesentliche Rolle, denn sie können – z.B. über die Ausgestaltung der Rules of Engagement – die Bewegungsfreiheit (Agilität) der militärischen Truppen einschränken oder die Entscheidungsprozesse zur Freigabe von Zielen verlangsamen. Es ist deshalb davon auszugehen, dass die Auseinandersetzung über das künftige Leitbild der Kriegführung – vernetzte Operationsführung ja oder nein und wenn ja nach US-amerikanischem oder europäischem Muster (so es letzteres denn gibt) – wesentlichen Einfluss auf die Debatte über das Gewaltverbot und die Präemption im Rahmen der Weiterentwicklung der UN-Charta ausüben wird.[54]

---

[49] Ralph Thiele, „Network Centric Warfare: Relevanz für deutsche Streitkräfte?", Präsentation für das DGAP-Expertengespräch vom 31. Januar 2003 <http://www.dgap.org/bfz/veranstaltung/Praes_Thiele_030131.ppt> (Zugriff: 20. Januar 2004).

[50] David S. Alberts and Richard E. Hayes, *Power to the Edge. Command and Control in the Information Age* (Washington, D.C.: CCRP Publications 2003), S. 143-149.

[51] So ähnlich auch: Clark Wesley K. Clark, „Iraq: What Went Wrong", *The New York Review of Books* 50:16 (23 October 2003), S. 52-54, v.a. S. 54.

[52] Siehe hierzu auch die Ausführungen von Martin Neujahr in diesem Band sowie Vego, „Network-Centric Warfare", S. 25; Pierre Forgues, *Command in a Network-Centric War* (Toronto: Canadian Forces College, 2000) <http://198.231.69.12/papers/amsc3/forgues2.doc> (Zugriff: 30. Dezember 2003).

[53] Martha Finnemore, *The Purpose of Intervention. Changing Beliefs About the Use of Force* (Ithaca, London: Cornell University Press, 2003).

[54] Siehe zum Zusammenhang zwischen Völkerrecht und High-Tech-Kriegführung auch: Thomas W. Smith, „The New Law of War: Legitimizing Hi-Tech and Infrastructural Violence," *International Studies Quarterly* 46:3 (September 2002), S. 355-374.

Koalitions- und Zusammenarbeitsfähigkeit

Die Fähigkeit zur Zusammenarbeit genießt im militärischen Bereich traditionell eine hohe Beachtung, weil sie eine wesentliche Voraussetzung der Glaubwürdigkeit internationaler Koalitionen darstellt.[55] Im Zeitalter der sicherheitspolitischen Vernetzung muss diese Fähigkeit vor dem Hintergrund zweier neuer Herausforderungen analysiert werden: den Auswirkungen des technologischen Fortschritts und der Erweiterung des relevanten Akteurskreises.

Technologie

Über die Frage, ob die Integration neuer Technologien in die militärischen Streitkräfte die multinationale Zusammenarbeit erleichtert oder erschwert, herrscht Uneinigkeit. Auf der einen Seite wird argumentiert, dass die vernetzte Operationsführung bestehende Interoperabilitätsprobleme insbesondere zwischen den transatlantischen Partnern noch vergrößern wird, weil die USA konsequent auf dieses neue Leitbild setzen, während die sich Europäer auf kein gemeinsames Konzept einigen können.[56] Aus einer kritischen, eher dem neo-realistischen Weltbild verpflichteten Analyse der internationalen Beziehungen wird darüber hinaus auf die Unverlässlichkeit zwischenstaatlicher Beziehungen verwiesen. Der heutige Freund kann der morgige Feind sein. Informationsaustausch werde daher nur sehr punktuell erfolgen, und insbesondere die USA dürften kaum bereit sein, ihren Verbündeten den vollständigen Zugang zu ihren Netzen zu gewährleisten.[57]

Auf der anderen Seite sehen Befürworter insbesondere in den neuen technologischen Möglichkeiten ein Instrument, um die Kohäsion internationaler Allianzen zu stärken. Erst das gemeinsam erarbeitete Lagebild schafft die Grundlage für gemeinsame Situationsanalysen und hilft, Misstrauen und Unsicherheit bezüglich der Informationsweitergabe zwischen den Alliierten abzubauen. Zudem profitieren Koalitionskräfte von der Einbindung in das gemeinsame Netzwerk, weil ihr Optionenspektrum durch gemeinsame Aktionen im Verbund erweitert wird. Und weil ein beachtlicher Anteil der erforderlichen Technologie nicht proprietär, sondern am Markt erhältlich ist (Commercial off the Shelf, COTS), werden der Technologietransfer und die Streitkräftetransformation vereinfacht.[58]

Eine Zwischenposition nehmen schließlich die technologiekritischen Experten ein. Aus ihrer Sicht sind die von den RMA-/NCW-Befürwortern vertretenen Positionen kaum haltbar. Daher ist es eher unwahrscheinlich, dass technologische Entwicklungen die internationalen Zusammenarbeit behindern oder diese es den USA sogar erlauben, sich aus ihren Überseestützpunkten zurückzuziehen und sich auf die „Kriegführung auf Distanz" zu verlegen.[59]

---

[55] Diese Feststellung gilt in besonderem Mass für EBO. Siehe: Smith, *Effects Based Operations*, S. 336-346.

[56] David C. Gompert, Richard L, Kugler, and Martin C. Libicki, *Mind the Gap. Promoting a Transatlantic Revolution in Military Affairs* (Washington, D.C.: National Defense University Press, 1999).

[57] Vego, „Network-Centric Warfare", S. 26; Robert Chekan, *The Future of Warfare: Clueless Coalitions?* (Toronto: Canadian Forces College, 2001) <http://198.231.69.12/papers/amsc4/chekan.doc> (Zugriff: 20. Januar 2004).

[58] William A. Owens, „The Once and Future Revolution in Military Affairs", *Joint Forces Quarterly* 31 (Summer 2002), S. 55-61, hier S. 60 <http://www.dtic.mil/doctrine/jel/jfq_pubs/1131.pdf> (Zugriff: 20. Januar 2004); Alberts/Garstka/Stein, *Network Centric Warfare,* S. 226.

[59] O'Hanlon, *Technological Change and the Future of Warfare,* S. 144-160.

Erweiterter Akteurskreis

Neben diesen technologischen Aspekten ist zu beachten, dass die Zahl der relevanten Akteure im Zeitalter der sicherheitspolitischen Vernetzung sprunghaft ansteigt. Die bisherigen Überlegungen zur Zusammenarbeit zwischen Teilstreitkräften (Jointness) bzw. zur internationalen Kooperation in gemeinsamen Verbänden (Combinedness) müssen, wie Abbildung 19 verdeutlicht, ergänzt werden. Zuerst ist der Blick von der militärischen Kooperation auf die Zusammenarbeit aller Sicherheitskräfte zu richten. Dazu zählen neben der Polizei sowie paramilitärischen Einheiten auch die Kräfte des Grenzschutzes sowie die Nachrichtendienste. Im Hinblick auf die Herausforderungen des Heimat- bzw. Bevölkerungsschutzes sind zusätzlich u.a. die Feuerwehr und die Sanität zu berücksichtigen. Darüber hinaus muss künftig zwingend auch die Schnittstelle zwischen dem öffentlichen Sektor und der Industrie berücksichtigt werden, denn diese spielt bei der Krisenvorsorge und der Krisenbewältigung eine zunehmend wichtige Rolle.[60] Gewisse Sicherheitsthemen wie beispielsweise der Schutz der kritischen Infrastruktur oder die Vorsorge gegenüber bioterroristischen Risiken sind ohne die Mitarbeit der Industrie überhaupt nicht zu bewältigen.

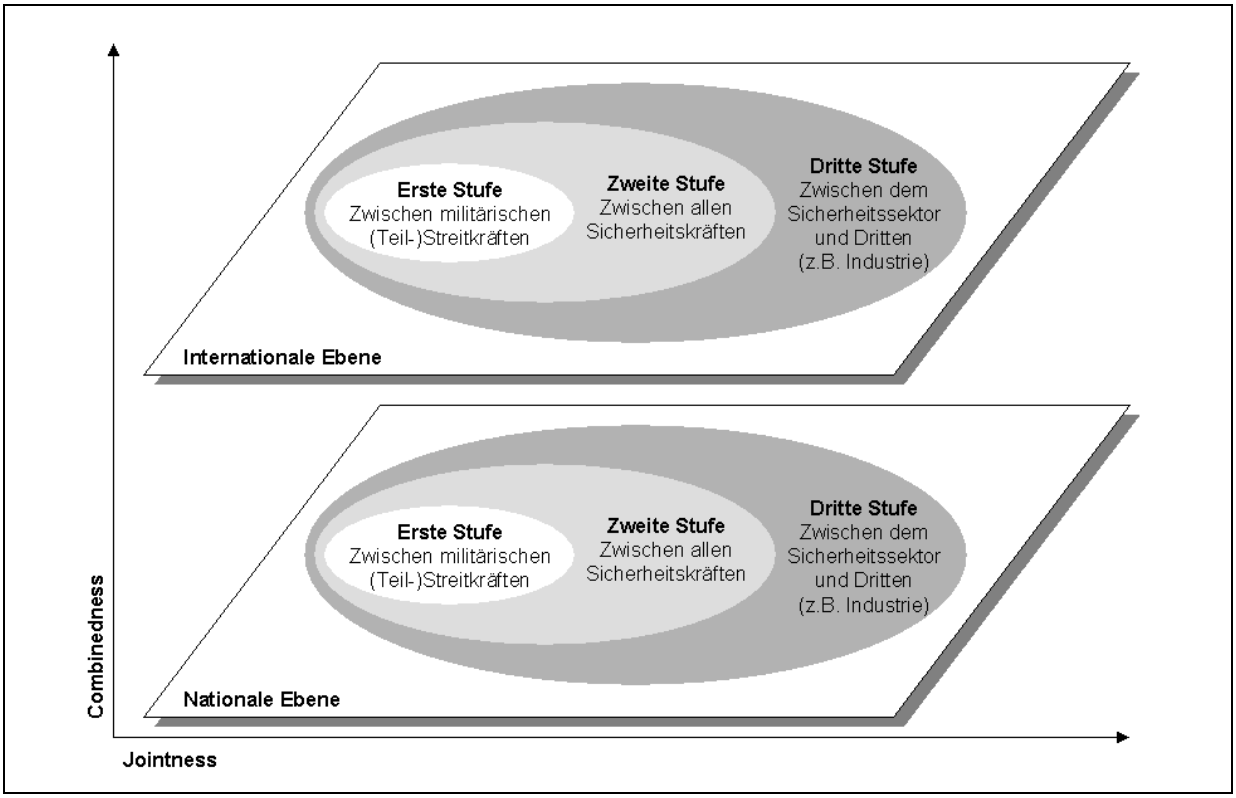

Abbildung 19: Jointness, Combinedness und sicherheitspolitische Vernetzung

Mit dieser erweiterten Betrachtung von Jointness und Combinedness steht der Sicherheitssektor jedoch vor einer „herkulischen Herausforderung". Die bisherigen Bemühungen zur Sicherstellung der Zusammenarbeitsfähigkeit beschränken sich beinahe vollständig auf

[60] So auch: Manuel W. Wik, *Network-Based Defence for Sweden – Latest Fashion or a Strategic Step Into the Future?* (Stockholm: Defence Materiel Administration, 2002), S. 25 <http://www.kkrva.se/kkrvaht_4_2002_04.pdf> (Zugriff: 20. Januar 2004).

die erste Stufe (Abbildung 19), während Standards und – noch wichtiger – Konzepte zur Zusammenarbeit für die zweite und dritte Stufe weitgehend fehlen oder nur sehr punktuell realisiert worden sind. Beide Aspekte werfen eine Reihe von Grundsatzfragen auf, die im Hinblick auf die reibungslose Zusammenarbeit im vernetzten Sicherheitssektor beantwortet werden müssen.

Erstens braucht es konzeptionelle Grundlagen zur Gewährleistung der Kooperation im vernetzten Sicherheitssektor. Bisherige Bemühungen zur konsequenten Jointness zwischen allen Sicherheitskräften müssen deutlich verstärkt werden. Besondere Aufmerksamkeit ist daneben der Kooperation mit der Industrie – von der gemeinsamen Risikoanalyse, zur Konzepterarbeitung bis hin zu gemeinsamen Übungen – zu widmen. Dabei geht es um die Klärung individueller bzw. gemeinsamer Verantwortlichkeiten im Hinblick auf die Bewältigung neuer Sicherheitsrisiken.[61] Zudem müssen Konzepte für die Weiterführung der unternehmerischen Tätigkeit im sicherheitspolitischen Krisenfall (Business Continuity) entwickelt werden.[62] Diese sind auch um Aspekte des Schutzes der Unternehmen für ihre Mitarbeitenden vor spezifischen Risiken zu erweitern.[63] Ferner ist zu untersuchen, inwieweit vorhandene Spezialfähigkeiten der Unternehmen – man denke beispielsweise an Berufsfeuerwehren der chemischen Industrie oder das Fach-Know-how von IT-Experten – in Ressourcenpools mit den staatlichen Sicherheitskräften zusammengeführt werden könnten. Daneben muss die konsequente Berücksichtigung politischer Aspekte im Rahmen der unternehmerischen Chancen- und Risikoanalyse ausgebaut werden.[64] Und schließlich muss angesichts des grenzüberschreitenden Charakters heutiger Wirtschaftstätigkeit danach gefragt werden, welche dieser Maßnahmen sinnvollerweise auf europäischem Niveau koordiniert werden und welche Rolle dabei die Europäische Kommission sowie andere internationale Behörden spielen sollen.

Zweitens erhöht die sicherheitspolitische Vernetzung die Komplexität der Suche nach strategischen Partnern. Im engeren Sinn, d.h. vor allem mit Bezug auf Technologieaspekte, ist die Partnerwahl automatisch auch eine Vorentscheidung im Hinblick auf die Kooperationsfähigkeit in einem gemeinsamen (NCW-)Verbund. Entscheidend ist dabei die Frage, wie offen oder abschottend die technologischen Standards definiert werden. Neben der Option „politisches Kerneuropa" gibt es damit auch jene des „technologischen Kerneuropa", das angesichts bestehender Fähigkeitsprofile nicht notwendigerweise deckungsgleich sein muss. Wie das Beispiel unterschiedlicher Industriestandards zeigt, ist Marktabschottung durch divergierende Standards relativ leicht möglich – politisch wären die Folgen einer solchen Entwicklung jedoch fatal. Im weiteren Sinn, d.h. mit Blick auf die wachsende Zahl von Anspruchsgruppen, mit denen der Sicherheitssektor zusammenarbeiten muss, können strategische Partnerschaften

---

61 Gary Ahlquist and Heather Burns, „Bioterrorism: Improving Preparedness and Response", in Randall Rothenberg (ed.), *Enterprise Resilience: Risk and Security in the Networked World* (McLean: Booz Allen & Hamilton, 2003), S. 135-142; Stephen J. Lukasik, Seymour E. Goodman, and David W. Longhurst, *Protecting Critical Infrastructures Against Cyber-Attack,* Adelphi Paper 359 (Oxford: Oxford University Press, 2003).

62 Randy Starr, Jim Newfrock and Michael Delurey, „Enterprise Resilience: Managing Risk in the Networked Economy", in Rothenberg, *Enterprise Resilience*, S. 56-69.

63 Juliette N. Kayyem and Patricia E. Chang, „Beyond Business Continuity: The Role of the Private Sector in Preparedness Planning", in Juliette N. Kayyem and Robyn L. Pangi (eds.), *First to Arrive. State and Local Responses to Terrorism* (Cambridge, London: MIT Press, 2003), S. 95-120.

64 Sven Behrendt, and Parag Khanna, „Geopolitics and the Global Corporation", *strategy + business* 32 (Fall 2003), S. 69-75.

beispielsweise auch mit nichtstaatlichen Akteuren eingegangen werden. Denken wir an die sicherheitspolitische Rolle der biotechnologischen Industrie, so ist die enge Zusammenarbeit mit diesem Industriezweig langfristig erfolgsentscheidend. Ebenso erforderlich ist aber auch der aktive Dialog mit kritischen NGOs wie z.B. dem Sunshine-Project,[65] die in der Lage sind, die internationale Öffentlichkeit zu mobilisieren und durch ihren Widerstand gegen neue Technologien sicherheitspolitisch relevante Langzeitfolgen verursachen können.

Die Frage der Standards rückt, drittens, die Beziehung zwischen NATO und EU ins Zentrum der Betrachtung. Innerhalb der NATO spielt die vernetzte Operationsführung bereits eine wichtige Rolle bei der Streitkräftetransformation. Verschiedene Aspekte werden im Rahmen des Multinational Interoperability Council sowie des Joint Transformation/Multinational Joint Concept Development & Experimentation-Prozesses berücksichtigt. Die EU hat dagegen noch keine eigene Position zu diesem Thema.[66] Daraus wird vor allem dann ein Problem, wenn die jeweiligen Streitkräfteentwicklungsprozesse nicht aufeinander abgestimmt werden. Insofern ist, um ein Wortspiel zu bemühen, der „gap in minds", der hinter unterschiedlichen Streitkräftetransformationsprogrammen steht,[67] für die Koalitionsfähigkeit ausschlaggebender als die im Hinblick auf die technologiebedingte Entwicklung ausgesprochene Warnung „mind the gap".[68] Deshalb ist es höchste Zeit, dass sich die Mitglieder dieser Organisationen auf ein gemeinsames Verständnis oder Leitbild einigen, um auf dieser Basis gemeinsame Standards und Vorgehensweisen zu definieren.

Diese militärischen Transformationsüberlegungen sind, viertens, sinngemäß auf die in Abbildung 19 dargestellte zweite und dritte Stufe des vernetzten Sicherheitssektors anzuwenden. Zu diesem Zweck ist es erforderlich, zusammen mit anderen internationalen Organisationen wie z.B. der OSZE, die im Bereich der Polizeikräfte tätig ist, ein „ziviles" Pendant zur militärischen Transformation zu entwickeln. Dieses sollte ebenfalls transatlantisch angelegt sein und müsste das US-amerikanische Department of Homeland Security (DHS) sowie entsprechende europäische Partnerorganisationen berücksichtigen. Die Einbindung der Industrie ist dabei durch die Entsendung eigener Vertreter sowie die Teilnahme von Verbandsmitgliedern, die Koordinationsfunktionen übernehmen können, sicherzustellen.

Management des vernetzten Sicherheitssektors

Die Diskussion von Managementaspekten im Zusammenhang mit der Erörterung politisch-strategischer Implikationen der sicherheitspolitischen Vernetzung mag auf den ersten Blick überraschen. Bei genauerem Hinsehen wird jedoch schnell dreierlei deutlich: Erstens sind die

[65] Das Sunshine-Project liefert nach eigenen Angaben Forschung und Fakten über biologische Waffen. Die Initianten wollen die weltweite Ächtung biologischer Waffen stärken und den militärischen Missbrauch von Bio- und Gentechnologie aufdecken <http://www.sunshine-project.de> (Zugriff: 20. Januar 2004). Siehe hierzu auch: Hans Schuh, "Grippen, Gräber und Gelehrte", *Die Zeit* 16. Oktober 2003, S. 33-34.

[66] Mey/Krüger, *Vernetzt zum Erfolg?,* S. 43-45; Ralph Thiele, „Transformation – zur (R)evolution unserer Sicherheit", *Europäische Sicherheit* 52:1 (Januar 2003), S. 7-10, hier S. 9-10.

[67] So auch: John P. White and John Deutch, *Security Transformation. Report of the Belfer Center Conference on Military Transformation* (Carlisle: Strategic Studies Institute, U.S. Army War College, 2003), S. 4. <http://www.carlisle.army.mil/ssi/pubs/2003/sectrans/sectrans.pdf> (Zugriff: 20. Januar 2004). White und Deutch argumentieren, dass die Konsequenzen der US-Streitkräftetransformation für die Alliierten genauer untersucht werden müssen.

[68] Gompert/Kugler/Libicki, *Mind the Gap.*

bisherigen Bemühungen zur Reform des öffentlichen Sektors (New Public Management) noch von einer starken Binnensicht geprägt und vernachlässigen den Gedanken der systematischen Vernetzung der Verwaltung mit anderen Akteuren. Zweitens zieht die erfolgreiche Bewältigung der neuen technologischen Herausforderungen eine weitgehende Überprüfung und Angleichung der Beschaffungsverfahren und -grundsätze nach sich, wobei immer öfter Ansätze angewendet werden, die sich in der Privatwirtschaft bewährt haben.[69] Drittens erfordern die neuen sicherheitspolitischen Herausforderungen die grundlegende Reorganisation der bestehenden Sicherheitsinstitutionen. Dabei gilt für die den öffentlichen Sektor genauso wie für die moderne Betriebswirtschaftslehre:

> Konsequente Prozessorientierung führt zur Virtualisierung und Vernetzung von Unternehmen, denn Prozesse sind nicht an Unternehmensgrenzen gebunden, sie liegen vielmehr quer zur klassischen Taylor'schen Arbeitsteilung.[70]

Die Managementreform des vernetzten Sicherheitssektors ist demzufolge die entscheidende Voraussetzung dafür, dass die politischen Entscheidungsträger ihre Führungsfunktionen überhaupt wahrnehmen können. Einige der damit verbundenen Herausforderungen sollen in der Folge diskutiert werden. Zu diesem Zweck wird das in Abbildung 20 dargestellte Führungsmodell[71] als Orientierungshilfe eingesetzt. Dieses basiert auf der Logik der Prozessorientierung und unterscheidet zwischen vier zentralen Führungsaufgaben (in der Abbildung durch vier Fragen gekennzeichnet), die vor dem Hintergrund der definierten Vorgaben bzw. der gelebten Wirklichkeit interpretiert werden müssen, um die mit der Leistungserstellung erzielte Wirkung beurteilen zu können.

Managementsystem

Ein Managementsystem beschreibt die Gesamtheit der aufeinander abgestimmten Prozesse, Strukturen und Instrumente eines Unternehmens.[72] Im Zuge der wirkungsorientierten Verwaltungsführung gehen auch öffentliche Betriebe und Ministerien in zunehmendem Maß dazu über, solche Managementsysteme aufzubauen. Im Zeitalter der sicherheitspolitischen Vernetzung besteht in diesem Bereich eine doppelte Herausforderung: Einerseits müssen die Managementsysteme der Organisationen des Sicherheitssektors systematisch aufeinander abgestimmt werden. Richtig verstanden müssen für den gesamten Sicherheitssektor übergreifende Prozesse definiert werden, die in einem entsprechenden Prozessmodell zusammengefasst werden. Eine solche Aufgabe muss logischerweise auch ressortübergreifend koordiniert werden. In vielen Fällen werden diese Prozessmodell zudem in den Wirtschaftssektor hineingreifen (z.B. im Zusammenhang mit der Krisenvorsorge oder dem Schutz kritischer Infra-

---

[69] Michael J. Lippitz, Sean O'Keefe, and John P. White, „Advancing the Revolution in Business Affairs", in Ashton B. Carter and John P. White (eds.), *Keeping the Edge. Managing Defense for the Future* (Cambridge, London: MIT Press, 2001), S. 165-202.

[70] Fleisch, *Das Netzwerkunternehmen,* S. 11.

[71] Das Führungsmodell wurde vom Inspektorat (Interne Revision) des Eidg. Departements für Verteidigung, Bevölkerungsschutz und Sport (VBS) unter Mitwirkung des Autors entwickelt und wird dort als Standardinstrument eingesetzt.

[72] Knut Bleicher, *Das Konzept Integriertes Management* (Frankfurt a.M.: Campus, 1995), S. 248-271; Markus Schwaninger, *Managementsysteme* (Frankfurt a.M.: Campus, 1994).

struktur) bzw. unternehmerische Leistungen müssen in die Prozessmodelle des Sicherheitssektors integriert werden (z.B. im Hinblick auf die immer enger werdende Kooperation mit der Rüstungsindustrie). Deshalb sollte entweder ein managementorientiertes Vernetzungsgremium für den Sicherheitssektor geschaffen werden, oder die Kompetenzen bereits bestehender, ressortübergreifender Einrichtungen sollten durch diesen Aspekt ergänzt werden (Abbildung 21). Denkbar ist daneben auch, wie das Beispiel des US-amerikanischen Ministerium für Heimatschutz zeigt, die Ernennung von Managementverantwortlichen zur Bündelung einzelner Funktionen.[73]

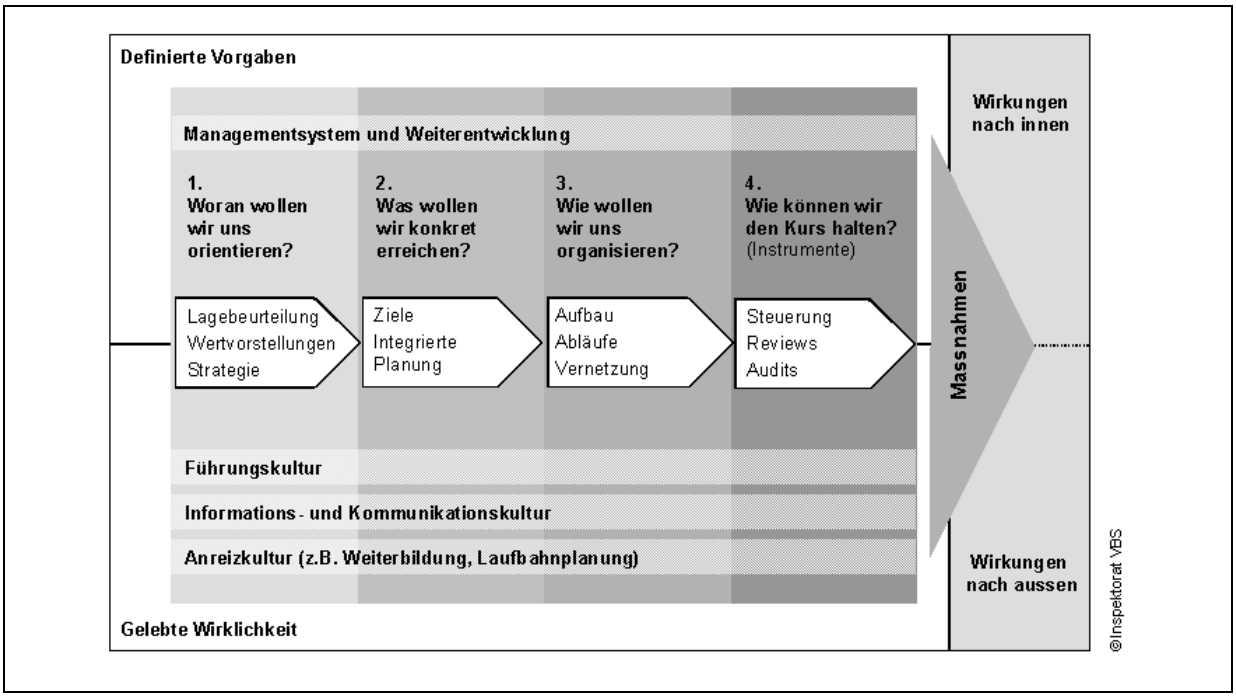

Abbildung 20: Allgemeines Führungsmodell

Andererseits muss die Kohärenz der einzelnen Managementsysteme auch innerhalb der Ministerien gewährleistet werden. Dabei offenbart sich die traditionelle Schwäche der zentralen Organisationseinheiten im Verhältnis zu den einzelnen „Geschäftseinheiten" der Ministerien. Gerade weil der technologische Fortschritt die Vernetzung der Organisationseinheiten erleichtert bzw. erfordert, ist es wichtig, dass die Managementkompetenz der zentralen Organisationseinheiten ausgebaut wird. Ansonsten besteht die Gefahr des „vernetzten Wildwuchses", bei dem jede Organisationseinheit eine eigene Richtung einschlägt. Dieses Risiko ist im Hinblick auf die militärischen Streitkräfte von besonderer Bedeutung, weil diese an „vorderster Front" der Technologieentwicklung stehen und innerhalb der Verteidigungsministerien traditionell eine Vorreiterrolle bei der technologiegetriebenen Organisationsentwicklung einnehmen.

[73] <http://www.dhs.gov/dhspublic/display?theme=54> (Zugriff: 20. Januar 2004).

Orientierung/Positionierung

Die Fähigkeit zur integrierten Strategiedefinition ist für den vernetzten Sicherheitssektor von zentraler Bedeutung. Die ressortspezifische Lagebeurteilung muss durch die gemeinsame ersetzt werden, und die politikbereichsspezifischen Strategien sind auf die sicherheitspolitische Gesamtstrategie abzustimmen. Wesentlich ist dabei die konsequente Orientierung an einem ressortübergreifenden Managementsystem. Diese muss durch zusätzliche Managementinstrumente ergänzt werden, die es erlauben, Chancen und Risiken systematisch zu erkennen, zu bewerten und zu verfolgen. Das gilt nicht nur für den politischen Bereich, in dem die Nachrichtendienste traditionell mit dieser Aufgabe betraut sind. Auf der Managementseite ist die Führung z.B. der komplexen technischen Projekte ohne entsprechende Managementinstrumente überhaupt nicht möglich. Sind diese nicht vorhanden, gehen die politischen Entscheidungsträger ein hohes Risiko ein – nicht nur hinsichtlich der Wirksamkeit der investierten Milliardenbeträge, sondern auch bezüglich der Einsatzfähigkeit der Sicherheitskräfte und der damit verbundenen politischen Glaubwürdigkeit.

Ferner ist zu berücksichtigen, dass der Trend zur Vernetzung die Zahl der für den Sicherheitssektor relevanten Anspruchsgruppen erhöhen wird. Reformkommissionen müssen beispielsweise gesellschaftlich breit abgestützt werden, und beim Einsatz in internationalen Missionen spielen die zivil-militärischen Beziehungen eine immer wichtigere Rolle. Es empfiehlt sich daher, auch im den Sicherheitssektor den Übergang zum systematischen Management der Beziehungen zu Anspruchsgruppen (Stakeholder Management) einzuleiten. Im Vordergrund stehen dabei die Identifizierung der wichtigsten Anspruchsgruppen, ihrer Absichten und Motive, die Auseinandersetzung mit ihrem Kooperationsverhalten, die Festlegung anspruchsgruppenspezifischer Zielsetzungen und die Definition von Mitteln und Verfahren, um die Zusammenarbeit mit den Anspruchsgruppen erfolgreich zu gestalten.[74]

Planung

Der Planungsbereich steht im Zeitalter der Vernetzung vor der großen Herausforderung, dass die ressortspezifischen Rivalitäten zwingend abgebaut werden müssen, soll die integrierte Planung Realität werden. Damit sind zwei zentrale Aspekte angesprochen: Zuerst muss das Verhältnis zwischen ressortübergreifenden Gremien und den ressorteigenen Planungsstäben geklärt werden. Die vollständige Zentralisierung der Planungsaktivitäten auf der obersten Stufe ist ebenso wenig sinnvoll wie die vollständige Delegation an die operativ tätigen Einheiten. Hier muss ein neues Gleichgewicht gefunden werden. Als Leitidee ist dabei anzuregen, dass die langfristigen und prospektiven Planungsaufgaben am ehesten gemeinsam und ressortübergreifend organisiert werden sollten, während die umsetzungsorientierten Planungsaufgaben[75] eher bei den Fachressorts liegen sollten. Eine vergleichbare Logik wird sich auch im Verhältnis zwischen nationaler und internationaler Planung aufdrängen. Da die Vernetzung nicht nur ressort-, sondern auch ebenenübergreifend sicherzustellen ist (Abbildung 19), müssen die na-

[74] Ronald K. Mitchell, Bradley R. Agle and Donna J. Wood, „Toward a Theory of Stakeholder Identification and Salience: Defining the Principle of Who and What Really Counts", *Academy of Management Review* 22:4 (1997), S. 853-886; James E. Post, Lee E. Preston and Sybille Sachs, „Managing the Extended Enterprise: The New Stakeholder View", *California Management Review* 45:1 (Fall 2002), S. 1-23.

[75] Planung bzw. Führung im Krisen- oder Anlassfall sind davon ausgenommen.

tionalen Planungsprozesse systematisch auf ihre Kompatibilität mit internationalen Planungsabläufen überprüft werden.[76] Dabei geht es neben der zeitlichen Synchronisation vermehrt auch um die inhaltliche Harmonisierung. International dürfte dies u.a. bedeuten, dass Überlegungen zu Fähigkeitszielen und Konvergenzkriterien noch wichtiger werden, weil sie das Bindeglied zwischen internationaler und nationaler Transformation darstellen. Demzufolge sind die entsprechenden Bemühungen nicht nur mit Nachdruck voranzutreiben, sondern auch inhaltlich vom Verteidigungsbereich auf alle Belange des vernetzten Sicherheitssektors zu erweitern.

Deutschland: Bundessicherheitsrat (BSR)

Unter dem Vorsitz des Bundeskanzlers bilden der Chef des Kanzleramts sowie die Minister des Äußeren, der Verteidigung, der Finanzen, des Inneren, der Justiz, der Wirtschaft sowie der wirtschaftlichen Zusammenarbeit und Entwicklung den BSR. Als Ausschuss des Bundeskabinetts berät der BSR über alle Fragen der Sicherheitspolitik, insbesondere in den Themenbereichen Verteidigung, Abrüstung und Rüstungskontrolle. Der BSR kann Entscheidungen vorbereiten bzw. selbst entscheiden sowie interministerielle Ausschüsse bilden. Die Ministerien sollen den BSR über Maßnahmen von sicherheitspolitischer Bedeutung informieren.
Quelle: Cord Meier-Klodt, Einsatzbereit in der Krise? Entscheidungsstrukturen der deutschen Sicherheitspolitik auf dem Prüfstand (Berlin: SWP, 2002).

Österreich: Nationaler Sicherheitsrat (NSR)

Die österreichische Bundesregierung zeichnet für die Sicherheitspolitik verantwortlich und wird dabei vom NSR beraten. Dem NSR gehören siebzehn stimmberechtigte und neun beratende Mitglieder an. Zur ersten Gruppe zählen neben dem vorsitzenden Bundeskanzler auch der Vizekanzler, die Minister für auswärtige Angelegenheiten, Verteidigung, Justiz und Inneres sowie Vertreter der politischen Parteien (alle stimmberechtigt). Die zweite Gruppe umfasst einen Beamten der Präsidentschaftskanzlei, einen Vertreter der Landeshauptleutekonferenz, den Generalsekretär für auswärtige Angelegenheiten, den Generaltruppeninspekteur, den Generaldirektor für öffentliche Sicherheit sowie je einen Vertreter des Bundeskanzlers, des Vizekanzlers sowie des Aussen- und Verteidigungsministeriums. Der NSR, der mindestes zweimal jährlich tagt, berät die Bundesregierung und die einzelnen Bundesminister in allen Fragen der Außen-, Sicherheits- und Verteidigungspolitik. Er ist u.a. bei der Teilnahme an Petersbergaufgaben und Maßnahmen gemäss Kapitel VII der UNO-Charta anzuhören. Daneben wurde im Bundeskanzleramt ein Ratssekretariat eingerichtet, das die Sitzungen vorbereitet. Es setzt sich aus den neun beratenden Mitgliedern des NSR zusammen. Zudem werden Koordinationsfunktionen zwischen den Ressorts stellt von der Abteilung „Sicherheitspolitische Angelegenheiten“ in der Sektion „Koordination“ im Bundeskanzleramt sichergestellt.
Quelle: Bundesgesetz zur Einrichtung eines Nationalen Sicherheitsrats vom 16. November 2001.

Schweiz: Sicherheitsausschuss (SiA) und Lenkungsgruppe Sicherheit (LGSi)

Der SiA soll die sicherheitspolitische Führungsfähigkeit des Bundesrats stärken. Er setzt sich aus den Ministern für Verteidigung, auswärtige Angelegenheiten sowie Polizei und Justiz zusammen und bereitet die Beratungen und Entscheidungen des Bundesrats in sicherheitspolitischen Fragen vor. Die LGSi unterstützt den SiA, indem sie u.a. die aktuelle Lage verfolgt und analysiert, für die Früherkennung sorgt sowie Szenarien und Strategien zuhanden des SiA erarbeitet. Der LGSi gehören die Spitzenbeamten der drei erwähnten Ministerien sowie weitere Verwaltungsvertreter (z.B. Generalstabschef, Chef des Strategischen Nachrichtendiensts, Staatssekretär für Wirtschaftsfragen) an. Daneben sorgt die nachrichtendienstliche Koordinationsstelle des Bundes, die aus dem Nachrichtenkoordinator, dem Lage- und Früherkennungsbüro und einem Sekretariat besteht, für die Zusammenarbeit zwischen den Nachrichtendiensten des Bundes.
Quelle: Weisungen über die Organisation der sicherheitspolitischen Führung des Bundesrats vom 3. November 1999.

Abbildung 21: Sicherheitspolitische Vernetzungsorgane in Deutschland, Österreich und der Schweiz

[76] Heiko Borchert und René Eggenberger, „Selbstblockade oder Aufbruch? Die Gemeinsame Sicherheits- und Verteidigungspolitik der EU als Herausforderung für die Schweizer Armee“, *Österreichische Militärische Zeitschrift* 40:1 (Januar/Februar 2002), S. 27-36, hier S. 34-35.

Organisation

Die größte organisatorische Herausforderung besteht in der ressortübergreifenden Prozessorientierung bzw. Vernetzung. Aus organisationstheoretischer Perspektive geht es darum, die Dominanz der Linienorganisation und der damit verbundenen Hierarchien, die auf das klassischen Bürokratiemodell von Max Weber zurückzuführen sind,[77] zugunsten der Vernetzungsorganisation abzubauen und die Prozesse entsprechend neu zu gestalten. Bleibt es dabei, dass insbesondere die Zuteilung der Finanz- und der Personalmittel entlang der bisherigen Linienorganisation – und damit eben auch der klassischen Ressortzuteilung – gesteuert wird, ist die Reorganisation nicht zu schaffen. Die Neuausrichtung muss daher auch in diesen Bereichen bewusst über sicherheitspolitische Vernetzungsgremien erfolgen.

Diese Veränderungen auf der Seite der Verwaltung werden auch das Parlament nicht unberührt lassen.[78] Wenn die sicherheitsrelevanten Ministerien über die Vernetzung näher zusammenrücken und daraus möglicherweise sogar der Aufbau integrierter Sicherheitskräfte resultiert, dann müssen auch die parlamentarischen Überwachungsorgane neu strukturiert werden.[79] Die bisherige Ressortaufteilung dürfte auch in diesem Bereich zugunsten eines umfassenden „Außen- und Sicherheitspolitischen Ausschusses des Parlaments" – dessen Zuständigkeit von der Außen-, über die Sicherheits- und die Verteidigungspolitik reicht und auch die Schnittstelle zu den Nachrichtendiensten, zur inneren Sicherheit sowie Wissenschaft und Forschung berücksichtigt – aufgegeben werden. Gleichzeitig muss die managementorientierte Beurteilungsfähigkeit solcher Ausschüsse nachhaltig gestärkt werden.

Kurs halten

Die Steuerung und die Weiterentwicklung des vernetzten Sicherheitssektors ist für die Bewältigung der komplexen neuen Sicherheitsherausforderung unerlässlich. David S. Alberts ist zuzustimmen, wenn er als Grundsatz festhält, dass „the entire notion of doctrine needs to be changed from one of publishing ‚the way' it should be done to a dynamic process of learning and sharing best practice."[80] Der Wandel von der Anordnungs- zur Lernkultur stellt jedoch nicht nur für die militärischen Streitkräfte, sondern auch für die Ministerien einen fundamentalen Kulturwandel dar. Die Fähigkeit des Lernens setzt neben dem Vorhandensein des Willens auch voraus, dass Informationen und Systeme zur Verfügung gestellt werden, die das Lernen ermöglichen.

Damit ist zum einen der Ausbau des strategischen Controlling (und Reporting) angesprochen. Dieses muss von den zentralen Organisationseinheiten der Ministerien aufgebaut und von den nachfolgenden Organisationsebenen entsprechend umgesetzt werden. Besonders

---

77 Max Weber, *Wirtschaft und Gesellschaft. Grundriss der verstehenden Soziologie* (Tübingen: J.C.B. Mohr, 1980), S. 125-128.

78 Siehe zu den damit verbundenen Folgen aus der Sicht der demokratischen Kontrolle der Streitkräfte: Marina Caparini, „Lessons Learned and Upcoming Research Issues in Democratic Control of Armed Forces and Security Sector Reform", in Hans Born, Marina Caparina, Philipp Fluri (eds.), *Security Sector Reform and Democracy in Transitional Societies* (Baden-Baden: Nomos, 2002), S. 207-216, hier S. 211-214.

79 So wurde in den USA ein neues Select Committee for Homeland Security geschaffen, um den Aufbau und die Arbeit des entsprechenden Ministeriums zu begleiten. Siehe: <http://hcw.house.gov> (Zugriff: 20. Januar 2004).

80 David S. Alberts, *Information Age Transformation*, S. 121.

wichtig ist in diesem Zusammenhang erneut der ressortübergreifende Blick, der durch einige zentrale und aggregierte Führungskenngrößen sichergestellt werden muss. Zu diesem Zweck sind neue Kenngrößen erforderlich, weil die neuen Anforderungen über die alten Indikatoren meist unzureichend erfasst werden.

Zum anderen stellt die Forderung nach Vernetzung neue Anforderungen an die für die Mittelzuteilung erforderlichen Instrumente. Das verhältnismäßig spröde Instrument der Kosten- und Leistungsrechnung spielt in diesem Zusammenhang eine besondere Rolle. Nur wenn es gelingt, die Kostenerfassung innerhalb des Sicherheitssektors zu vereinheitlichen und Transparenz über die Kosten der erbrachten Leistungen herzustellen, sind der Leistungsaustausch (z.B. der Einsatz militärischer Streitkräfte zugunsten des Innenministeriums) sowie das Zusammenlegen von Leistungen und Fähigkeiten in Ressourcenpools (z.B. der Aufbau eines Polizeipools bestehend aus Bundes- und Länderkräften) zu realisieren. Ohne diese Transparenz besteht die Gefahr, dass sich die einzelnen Ministerien bzw. Sicherheitskräfte aus Angst vor der möglichen Benachteiligung bei der Mittelvergabe der Zusammenarbeit verweigern oder diese nicht mit dem geforderten Nachdruck vorantreiben. Ebenso sind politische Grundlagenentscheidungen z.B. zur Frage der Ressortneuzuteilung im Zuge der Reorganisation ohne die geforderte Transparenz nicht möglich.[81]

Die Forderung nach neuen Kenngrößen führt uns zum zweiten wichtigen Bereich, nämlich der Fähigkeit zur Weiterentwicklung, die systematisch in die Managementsysteme des vernetzten Sicherheitssektors eingebaut werden muss. Holger Mey und Michael Krüger haben völlig recht, wenn sie im Hinblick auf die Streitkräfteentwicklung den Aufbau eines Transformationsaudits zur Identifizierung der Stärken und Schwächen vorschlagen, das in enger Zusammenarbeit zwischen Industrie und Amtsseite entwickelt werden soll.[82] Logischerweise muss diese Idee zur Forderung nach einem Bewertungsansatz für die Weiterentwicklung des gesamten Sicherheitssektors (Security Sector Assessment) erweitert werden. Ein solches Assessment sollte – in Analogie zum Planning and Review Process (PARP) der NATO sowie anderer international verfügbarer Instrumente – aus einem klar definierten Assessmentprozess bestehen und einen Fragekatalog zur Selbst- und Fremdbewertung beinhalten. Kernbereiche der Untersuchung, durch die auch die Forderung nach neuen Kenngrößen befriedigt werden kann, sollten sein:[83]

- Vernetztes Management der Sicherheitspolitik und des Sicherheitssektors
- Individuelle und gemeinsame Fähigkeitsorientierung
- Zusammenarbeitsfähigkeit im und über den Sicherheitssektor hinaus

---

[81] Das zeigte sich in der Schweiz z.B. bei der Zuweisung von Sicherheitsaufgaben an das Eidg. Departement für Verteidigung, Bevölkerungsschutz und Sport bzw. das Eidg. Justiz- und Polizeidepartement sowie bei der Kompetenzausscheidung zwischen Bund und Kantonen. Siehe: USIS, *Detailbericht III* (Bern, 24. September 2002), S. 48-56, <http://www.usis.ch/deutsch/berichte/pdf_usis_3/USIS_III_Text.pdf> (Zugriff: 20. Januar 2004).

[82] Mey/Krüger, *Vernetzt zum Erfolg?,* S. 12.

[83] Heiko Borchert, „Security Sector Reform Initiative (SSRI). How to advance security sector reforms with the help of a new assessment and development framework", Paper prepared for the Annual Conference of the Working Group Security Sector Reform of the Partnership for Peace Consortium of Defence Academies and Security Studies Institutes, Berlin, 15-17 June 2003, S. 10-19. Für weitergehende Vorschläge im Bereich der Streitkräfteentwicklung siehe: Alberts, *Information Age Transformation,* S. 79-110.

Die besondere Betonung der Vernetzung bringt es mit sich, dass das geforderte Assessment ein besonderes Augenmerk auf die Weiterentwicklung von Netzwerken richten muss. Damit sind sehr spezifische Fragestellungen angesprochen wie beispielsweise

- technische Aspekte der Simulation bzw. des Tests von IT-Netzwerken im Vorfeld ihres Einsatzes,[84]
- arbeitspsychologische Aspekte wie die Frage nach den Zusammenhängen zwischen der Arbeit in Netzwerken und den Rückwirkungen auf die Psyche, die Motivation und das Verhalten der Mitarbeitenden,[85]
- organisationstheoretische Fragen nach der optimalen „Konstruktion" von Netzwerken sowie
- soziologische Aspekte wie die Frage, aus welchen Gründen sich Menschen überhaupt in Netzwerken zusammenschließen und welche „Haltbarkeit" diese aufweisen (Social Network Analysis/Engineering).[86]

Kulturdimension

Die Transformation von Organisationen hängt bekanntermaßen erst in zweiter Linie von der Einführung neuer Technologie oder der Neugestaltung von Prozessen und Strukturen ab. Maßgeblich ist in erster Linie der Veränderungswille der Menschen.[87] Für die erfolgreiche Umsetzung der vernetzten Operationsführung oder der vernetzten Sicherheitspolitik ist dieser Veränderungswille eine zentrale Voraussetzung.[88] Schwierig gestaltet sich dieser kulturelle Wandel vor allem deshalb, weil die meisten Entscheidungsträger durch Linienorganisationen sozialisiert worden sind:

> It is difficult to create a culture of innovation when a procurement system can take 20 years to field a product. It is difficult to create a culture of innovation when communications are hampered by incompatible, slow, unsecured information and computer systems. It is difficult to create a culture of innovation under arcane rules, regulations, and personnel systems.[89]

---

[84] Damilan Kemp, „Key role is to understand networks as they evolve", *Jane's Defence Weekly* 8 October 2003, S. 30; Alberts, *Information Age Transformation,* S. 66-68; Alberts/Hayes, *Power to the Edge,* S. 235-236; Peter J. Dombrowski, Eugene Gholz and Andrew L. Ross, *Military Transformation and the Defense Industry after Next. The Defense Industrial Implications of Network-Centric Warfare,* Newport Papers 18 (Rhode Island: Naval War College, 2003), S. 83.

[85] Alberts, *Information Age Transformation,* S. 131-143.

[86] Art Kleiner, „Karen Stephenson's Quantum Theory of Trust", in Rothenberg, *Enterprise Resilience,* S. 38-53.

[87] Don M. Sinder, „Jointness, Defense Transformation, and the Need for a New Joint Warfare Profession," *Parameters* 33:3 (Autumn 2003), S. 17-30, hier S. 19.

[88] Hierzu weiterführend die aufschlussreichen Untersuchungsergebnisse von: Thomas G. Mahnken and James R. FritzSimonds, „Revolutionary Ambivalence: Understanding Officer Attitudes toward Transformation", *International Security* 28:2 (Fall 2003), S. 112-148.

[89] Mac Thornberry, „Fostering a culture of innovation", *Proceedings* 129:4 (April 2003), S. 44-50, hier S. 2 (zit. gem. Internetversion).

Die Vernetzung bedingt im Unterschied zum Bestehenden eine neue Kultur, die auf Vertrauen, Delegation, Eigeninitiative, Selbständigkeit und Eigenverantwortung basiert.[90] Wichtig wird es daher in einem ersten Schritt sein, dass vor allem die Führungskräfte und die Entscheidungsträger ihre Bereitschaft zur vernetzten Sicherheitspolitik mit Taten unterstreichen. Dazu zählen beispielsweise die Übernahme der Projektaufsicht in maßgeblichen Reformprojekten, die den Wandel zur Vernetzung fördern, die gemeinsame Strategieschöpfung in ressortübergreifenden Vernetzungsgremien sowie die Teilnahme an Aus- und Weiterbildungsveranstaltungen (z.B. der bewusst ressortübergreifend angelegte strategische Führungslehrgang an der Österreichischen Landesverteidigungsakademie),[91] Übungen und Simulationen, die die Sensibilität für die Notwendigkeit ressortübergreifender Zusammenarbeit erhöhen. Besonders wichtig ist in diesem Zusammenhang der Umgang mit der bereits erwähnten Schnittstelle zwischen politischer und militärischer Führung, um asymmetrische Entscheidungsprozesse zu verhindern.

Der zweite Schritt beinhaltet den Wandel im Informations- und Kommunikationsverhalten. Befürworter der vernetzten Operationsführung weisen korrekterweise darauf hin, dass die angebotsorientierte Informationsversorgung (Information Push) in einem komplexen Netzwerk leicht zur Informationsüberlastung seiner Mitglieder führen kann. Deshalb favorisieren sie die nachfrageorientierte Informationsbeschaffung (Information Pull), bei der sich jeder aufgrund seiner Bedürfnisse aus dem Netzwerk „bedient".[92] Das setzt jedoch voraus, dass die benötigten Informationen unaufgefordert zur Verfügung gestellt werden. In einem Zeitalter, in dem viele Wissen noch immer mit Macht verbinden (Herrschaftswissen) stößt diese Forderung allerdings an eine natürlich Barriere. Damit kämpfen vernetzte Operationsführung und vernetzte Sicherheitspolitik mit einem Problem, dass allen Verantwortlichen des Wissensmanagements wohl vertraut ist: aktives Informations- und Kommunikationsverhalten lässt sich nicht verordnen, sondern muss sich im Zeitablauf entwickeln.

Dazu können, und das ist das dritte Element, Anreize und Maßnahmen zur Befähigung der Mitarbeitenden unterstützend eingesetzt werden. So muss beispielsweise die Aus- und Weiterbildung der Mitarbeitenden der Sicherheitssektoren konsequent neu auf die Anforderungen der Vernetzung ausgerichtet werden. Gemeinsame Führungslehrgänge sollten ebenso selbstverständlich werden wie die Personalrotation zwischen den Ministerien und den Sicherheitskräften. Im Hinblick auf die Laufbahnplanung sollten bewusst ressortübergreifende Karrierewege geplant und angeboten werden. Ebenso sollte das Engagement in anderen Sicherheitsressorts genauso als Qualifizierungsmerkmal für die berufliche Beförderung eingeführt werden wie beispielsweise die Teilnahme an Auslandeinsätzen.[93]

---

[90] Ähnlich auch: Alberts/Hayes, *Power to the Edge,* S. 180-181. Hierzu weiterführend die aufschlussreichen Überlegungen von: Katharina Jörges und Stefan Süss, „Scheitert die Realisierung virtueller Unternehmen am realen Menschen?", *IO-Management* 69:7/8 (August 2000), S. 78-84.

[91] Siehe: <http://www.stratfuelg.gv.at/seite1.htm> (Zugriff: 20. Januar 2004).

[92] Das ist eine der Kernforderungen von: Alberts/Hayes, *Power to the Edge.*

[93] Hierzu weiterführend: Alberts/Gartska/Stein, *Network Centric Warfare,* S. 229 f.; Alberts, *Information Age Transformation,* S. 123-124; Alberts/Hayes, *Power to the Edge,* S. 223-232.

Vernetzte Fähigkeiten

Durch die eingangs festgestellten Veränderungen im relevanten Risiko- und Konfliktbild sowie die daraus resultierenden Konsequenzen für das Operationsbild rücken die Aufgabenprofile der Sicherheitskräfte näher zusammen. Damit gewinnen jene Fähigkeiten an Bedeutung, die dazu beitragen, die Vernetzung der Sicherheitskräfte sicherzustellen bzw. zu vereinfachen und von allen Sicherheitskräften nutzenbringend eingesetzt werden können. Solche Fähigkeiten können als „vernetzte Fähigkeiten" bezeichnet werden.

Die Aufarbeitung der Ereignisse des 11. September 2001 hat in den USA aber auch in Europa zu teilweise ernüchternden Einsichten über den Ausrüstungszustand und die Fähigkeitsprofile gewisser Sicherheitskräfte geführt. Über 100 Feuerwehrleute sollen beim Brand des World Trade Center allein deshalb gestorben sein, weil die Kommunikations- und Informationssysteme der Einsatz- und Rettungskräfte unzureichend aufeinander abgestimmt waren.[94] Darüber hinaus, so stellte eine Task Force des US Council on Foreign Relations fest, verfügen beispielsweise die US-amerikanischen Polizeikräfte nicht über das erforderliche Gerät, um einen mit Massenvernichtungswaffen angegriffenen Ort abzusichern. Den meisten Städten fehlen die Geräte, um herauszufinden, ob und in welchem Ausmaß die Einsatz- und Rettungskräfte an einem Schadensort gefährlichen Stoffen ausgesetzt sind.[95] In Europa präsentiert sich das Bild nicht besser. Im Anschluss an die Flutwasserkatastrophe in Deutschland im Jahr 2002 stellte der Kirchbach-Report gravierende Schwächen bei den Kommunikationssystemen der Behörden und Organisationen mit Rettungs- und Sicherheitsaufgaben fest und wies gleichzeitig auf konzeptionelle Schwächen in deren Zusammenarbeit hin.[96] Und im Zuge der Überprüfung des Systems der inneren Sicherheit in der Schweiz (USIS) wurden Defizite bei der unterschiedlich intensiven und sehr heterogen ausgeprägten Zusammenarbeit zwischen den Polizeikonkordaten sowie der mangelnden Interoperabilität der von den kantonalen Polizeikorps verwendeten Kommunikationssystemen festgestellt.[97]

Erste Anzeichen der Verbesserung sind in Sicht. So wird z.B. in Frankreich das Kommunikationssystem der Polizei auf die Feuerwehr und andere Akteure ausgedehnt, und es werden einheitliche Lagebilder unter Einschluss der Marine und der Küstenwache erstellt.[98] Ähnliche Bestrebungen gibt es auch in der Schweiz mit dem Aufbau des einheitlichen Kommunikationsnetzes POLYCOM.[99] Aus diesen Beispielen und den genannten Defizitbereichen lässt sich eine Liste jener vernetzten Fähigkeiten ableiten, die künftig besonderer Beachtung bedürfen. Dazu zählen u.a.:

---

94 Thomas Enders, „Herausforderung ‚Homeland Security' für die Industrie", *Europäische Sicherheit* 52:10 (Oktober 2003), S. 8-11, hier S. 8.

95 *Emergency Responders: Drastically Underfunded, Dangerously Unprepared* (New York: Council on Foreign Relations, 2003), S. 5.

96 *Flutkatastrophe 2002. Bericht der Unabhängigen Kommission der Sächsischen Staatsregierung,* S. 183-184, 241 ff.

97 USIS, *Analyse des Ist-Zustandes mit Stärken-/Schwächenprofil* (Bern: USIS, 2001), S. 15, 17 <http://www.usis.ch/deutsch/berichte/pdf_usis1/Medienrohstoff_d.pdf> (Zugriff: 20. Januar 2004).

98 Enders, „Herausforderung ‚Homeland Security' für die Industrie", S. 9.

99 USIS, *Teil II. Grobe Soll-Varianten, Sofortmassnahmen* (Bern: USIS, 2001). S. 20 <http://www.usis.ch/deutsch/berichte/pdf_usis2_voll/deutsch.pdf> (Zugriff: 20. Januar 2004).

- Führung (Command, Control, Communications, Computer, C4) als Kernvoraussetzung erfolgreicher Operationen
- Nachrichtengewinnung, Überwachung und Aufklärung (Intelligence, Surveillance, Reconnaissance, ISR), um ein gemeinsames Lagebild herzustellen
- Luft-, land- und seegestützte Verlegefähigkeit zur Verbesserung der Mobilität der Sicherheitskräfte
- Überlebensfähigkeit und Schutz der Sicherheitskräfte z.B. durch ABC-Abwehr, Suche und Rettung (Search and Rescue, SAR) oder den Einsatz non-letaler Wirkmittel
- Schutz der informationskritischen Infrastruktur zur Gewährleistung der Führung im militärischen, im zivil-militärischen und im zivilen Umfeld (inkl. Fähigkeiten zur elektronischen Kriegführung und für Informationsoperationen)

Im Hinblick auf die Definition der vernetzten Fähigkeiten, die als Ergänzung der jeweils spezifischen Fähigkeiten einzelner Sicherheitskräfte zu interpretieren sind, ist festzulegen, wer diese identifiziert und durch wen bzw. in welcher Form diese bereitgestellt weiterentwickelt werden. Aufgrund der bisherigen Ausführungen erscheint es sinnvoll, die Identifizierung und die Weiterentwicklung über die im vorangehenden Abschnitt angeregten Managementsysteme bzw. das umfassende Assessment des gesamten Sicherheitssektors abzuwickeln. Sicherheitspolitische Vernetzungsorgane sollten für die Festlegung der Schwerpunkte und die strategische Steuerung zuständig sein, während die jeweiligen Sicherheitskräfte für die Bewirtschaftung und das operative Management der Fähigkeiten verantwortlich zeichnen.

Angesichts knapper öffentlicher Budgets kann es nicht darum gehen, die Fähigkeitsdefizite der jeweiligen Sicherheitskräfte individuell zu beheben. Vielmehr müssen in diesem Zusammenhang Ideen wie die Rollenspezialisierung oder die Zusammenlegung von Ressourcen auf alle Sicherheitskräfte angewendet werden.[100] Das hätte beispielsweise zur Folge, dass ein ABC-Kompetenzpool mit Hilfe entsprechender militärischer ABC-Schutz- und Abwehrfähigkeiten, der Fachexpertise der chemischen und Biotech-Industrie, privaten und wissenschaftlichen Instituten der öffentlichen Hand sowie den Krankenhäusern eingerichtet werden könnte.[101] Dieser umfassende Ansatz des Public-Private Partnership (PPP) gelingt allerdings nur dann, wenn die Managementkompetenzen der Sicherheitskräfte gefördert und die Sensibilität für den erforderlichen Kulturwandel erhöht werden.

Rolle der Rüstungsindustrie

Der Trend zur technologischen und konzeptionellen Vernetzung der Akteure des Sicherheitssektors wird sich auch auf die Produkte, die Dienstleistungen und die Organisation der Rüstungsunternehmen sowie andere, sicherheitsrelevante Unternehmen auswirken. Die damit verbundene Herausforderung bringen Doug Harned und Jerry Lundquist auf den Punkt:

[100] Heiko Borchert und René Eggenberger, „Rollenspezialisierung und Ressourcenzusammenlegung. Wie Europas sicherheitspolitische Fähigkeiten gestärkt werden können“, in Hans-Georg Ehrhart und Burkard Schmitt (Hrsg.), *EU-Sicherheitspolitik im 21. Jahrhundert: Konzeptionen, Aktivitäten, Fähigkeiten, Herausforderungen* (Baden-Baden: Nomos, 2004, i.V.).

[101] So ähnlich auch Mey/Krüger, *Vernetzt zum Erfolg?,* S. 60.

> Since it is ultimately the contractors that will provide the technological insights to make defense transformation a reality, these challenges have the potential to slow the rate of change. And since technology development and acquisition cycles are lengthy, we may be a long way from achieving the transformational vision.[102]

Neben der Transformation der militärischen Streitkräfte und der umfassenden Reform des Sicherheitssektors steht also auch noch die Reorganisation der Rüstungsindustrie bevor. Diese Einsicht ist nicht neu, wirft jedoch insbesondere in Europa grundsätzliche Fragen zum Verhältnis zwischen öffentlichem Sicherheitssektor und wehrtechnischer Industrie auf.

Kundenanforderungen

Der Übergang zur Fähigkeits- und Wirkungsorientierung sowie die verstärkte Betonung der Netzwerkfähigkeit werden auf der Industrieseite zu einer Verlagerung von der Produkt- oder Plattformorientierung hin zur Systemorientierung führen.[103] Der Grundsatz der Jointness muss von der Industrie genauso berücksichtigt werden wie von den Sicherheitskräften, weshalb beide der Fähigkeit zur Systemintegration – bezogen auf die Management- und die IT-Systeme – mehr Beachtung schenken müssen. Die Industrie wird dadurch dreierlei analysieren müssen. Erstens muss sie ihr Leistungsportfolio im Bereich der vernetzten Fähigkeiten überprüfen bzw. verstärkt darauf ausrichten, weil dort der größte Mehrwert für den Kunden geschaffen werden kann. Zweitens wird sie bestehende Partnerschafts- und Allianznetze auf den Prüfstand stellen. Genügte bislang die Kooperation mit industriespezifischen Partnern, so wird künftig die Integration industriefremder Partner aus den Bereichen der Bio-, Gen- und Nanotechnologie, den Lebenswissenschaften (Life Sciences), der Medizin, der Informations- und Kommunikationstechnologie sowie aus Multimedia und Bildung an Bedeutung gewinnen. Drittens muss sich die Industrie auf einen breiteren Abnehmerkreis einstellen, der sich aus der Vernetzung des Sicherheitssektors ergibt. Das stellt auf der einen Seite eine Chance dar, weil sich die Absatzmöglichkeiten verbessern. Auf der anderen Seite ist jedoch zu erwarten, dass der Sicherheitssektor seine Einkaufsmacht künftig verstärkt durch ein konzertiertes Vorgehen stärken wird. Und so lange die europäische Integration in diesem spezifischen Industriebereich noch auf sich warten lässt, bedeutet dies eine Erhöhung der Komplexität bei der länder- und sektorspezifischen Marktbearbeitung. Zu guter Letzt ist auf den unternehmensspezifischen Reorganisationsbedarf hinzuweisen, der sich aus den genannten Entwicklungen ergibt.[104] Je besser und schneller es den Unternehmen gelingt, ihre eigenen Kompetenzen und Fähigkeiten im Sinne der geforderten Systemintegration zu bündeln, desto eher wächst auf der Kundenseite das Vertrauen in die unternehmerische Problemlösungskompetenz.

[102] Dougles S. Harned and Jerrold T. Lundquist, „What transformation means for the defense industry“, *The McKinsey Quarterly* 3 (2003), S. 50-63, hier S. 61.
[103] Mey/Krüger, *Vernetzt zum Erfolg?,* S. 57-65 und der Beitrag von Burkhard Theile in diesem Band.
[104] Harned/Lundquist, „What transformation means for the defense industry“, S. 60.

Zusammenarbeit

Es liegt auf der Hand, dass sich der bereits aus anderen Gründen enger werdende Schulterschluss zwischen Sicherheitssektor und wehrtechnischer Industrie im Zeitalter der Vernetzung noch verstärken wird. Die Industrie als Trägerin der wissenschaftlich-technische Kompetenz ist besonders in zwei Bereichen gefordert. Einerseits geht es um die systematische Unterstützung des Sicherheitssektors in bezug auf das wissenschaftlich-technische Trendmonitoring. Dies ist eine Dienstleistung, die für die Fähigkeitsplanung des Sicherheitssektors immer wichtiger wird und sinnvollerweise von diesem am Markt eingekauft werden sollte.[105] Eng damit verknüpft ist andererseits die Unterstützung des Sicherheitssektors beim Management unterschiedlicher Lebenszyklen der eingesetzten Technologien bzw. der daraus resultierenden Produkte. Diese Aufgabe resultiert aus dem verstärkten Einsatz ziviler Technologie (COTS) in sicherheitsrelevanten Anwendungen. Zivile Technologien weisen aufgrund anderer Marktbedürfnisse meist kürzere Lebenszyklen auf.[106] Das wirkt sich vor allem im militärischen Bereich auf die Unterhalts- und Kampfwertsteigerungsprogramme aus, deren Konzeption und Bewirtschaftung dadurch komplexer werden.

Der Sicherheitssektor muss seinerseits die adäquate Beurteilungskompetenz sicherstellen, um die Industrievorschläge prüfen zu können. Gleichzeitig trägt er die wesentliche Verantwortung dafür, dass PPP nicht nur auf dem technischen, sondern vor allem auf dem strategischen Niveau eingerichtet werden. Dabei gewinnt die umfassende Betrachtung von Krisenvorsorge, Krisenmanagement und Krisennachsorge gerade auch im Hinblick auf den Heimatschutz wesentlich an Bedeutung. Darüber hinaus muss der Sicherheitssektor gewisse Bedenken der Industrie sehr ernst nehmen. Das gilt beispielsweise für die Feststellung, dass Produktentwicklungen im Bereich der vernetzten Operationsführung zeit- und kostenintensiv sind. Gleichzeitig besteht ein hohes Risiko hinsichtlich der Fortführung von Projekten aus dem Entwicklungs- ins Produktionsstadium.[107] In Großbritannien, das in Europa eine führende Rolle bei verteidigungsorientierten PPPs einnimmt, werden die langen und teuren Bewerbungsprozesse im Verteidigungssektor von der Industrie zunehmend kritisch kommentiert.[108] In beiden Fällen fehlen bislang adäquate Modelle zur Kompensation der damit verbundenen Risiken. Da es sich hierbei um ein Problem handelt, mit dem zunehmend auch die übrigen Sicherheitskräfte sowie die anderen europäischen Länder konfrontiert werden, drängt sich ein europäischer Lösungsansatz beispielsweise unter Einbezug des neu zu schaffenden Europäischen Amts für Rüstung, Forschung und militärische Fähigkeiten auf.

Erweiterte Industriebasis

Unter den Vorzeichen der sicherheitspolitischen Vernetzung erweitert sich die sicherheitsrelevante Industriebasis in Richtung der bereits angedeuteten stärkeren Integration bislang als

[105] Dombrowski/Gholz/Ross, *Military Transformation and the Defense Industry after Next,* S. 27.
[106] Mey/Krüger, *Vernetzt zum Erfolg?,* S. 57 f.; Jochen Dietrich, „Führungsfähigkeit", in Karl von Wogau (Hrsg.), *Auf dem Weg zur Europäischen Verteidigung. Gemeinsam sind wir sicher* (Freiburg: Herder, 2003), S. 336-347, hier S. 341-343.
[107] Harned/Lundquist, „What transformation means for the defense industry", S. 59.
[108] David Mulholland, „Concerns rise over the value of private finance", *Jane's Defence Weekly* 23 October 2002, S. 16.

rein „zivil" charakterisierter Industriezweige. Der Sicherheitssektor und die Wirtschaft müssen erkennen, dass sich dadurch die Definition der als „strategisch bedeutend" eingestuften Industrien und Produkte grundlegend verändert. Die staatliche Förderung neuer Bereiche wie beispielsweise Bio- und Gentechnologie, Nanotechnologie oder Lebenswissenschaften ist vor diesem Hintergrund nicht nur als Beitrag zur Stärkung der nationalen Standortattraktivität, sondern auch als Unterstützung der sicherheitspolitischen Fähigkeitsprofile zu interpretieren. Daraus leitet sich die Forderung ab, dass die bislang künstliche Trennung zwischen militärischer und ziviler Forschung durch integrierte nationale und internationale Konzepte konsequent überwunden werden muss.[109] Gleichzeitig ist in den erwähnten Industrien die Sensibilisierung für die sicherheitspolitische Rolle und Verantwortung zu stärken (z.B. durch gemeinsame Übungen und Lehrgänge).

Europäisches Amt für Rüstung, Forschung und militärische Fähigkeiten

Im Hinblick auf die Steuerung der Beschaffungsaktivitäten des vernetzten Sicherheitssektors nimmt das im Aufbau befindliche europäische Amt für Rüstung, Forschung und militärische Fähgkeiten eine Schlüsselstellung ein.[110] Auch in diesem Bereich zwingt das Gesagte zu einigen Grundsatzüberlegungen. Erstens sollte das Amt mit Blick auf die Umsetzung des Konzepts der vernetzten Operationsführung die zentrale Integrationsfunktion übernehmen. Gegenwärtig verfolgen Großbritannien, Frankreich, Deutschland, die Niederlande, Spanien und Schweden eigene Modernisierungsprojekte im Bereich „Soldat der Zukunft".[111] Wenn die Befürworter der vernetzten Operationsführung mit ihren Thesen von der Kompetenzdelegation und der Selbstsynchronisation recht haben, dann erscheint es mehr als sinnvoll, dass diese Programme auf der „untersten Vernetzungsstufe" durch Harmonisierung bzw. Integration auf optimale Zusammenarbeitsfähigkeit ausgerichtet werden. Zweitens sollte überlegt werden, ob und in welcher Form das Mandat des Amts auf den gesamten Sicherheitssektor ausgedehnt werden kann, um knappe Mittel effizienter einzusetzen und technische Inkompatibilitäten durch gemeinsame Beschaffungsvorhaben zu verhindern. Drittens sollten die Einflussmöglichkeiten der Rüstungsagentur – in Zusammenarbeit mit anderen Organen wie z.B. dem EU-Militärstab – im Hinblick auf die Modernisierung und die Transformation des Sicherheitssektors ausgebaut werden. Es ist ein zentrales Problem, wenn nationale Verteidigungsbudgets noch keine oder keine adäquaten Mittel für Transformations- und Modernisierungsaufgaben vorsehen.[112] Deshalb ist es sinnvoll, auf der europäischen Ebene Kompetenzen zu schaffen

---

[109] *Towards an EU Defence Equipment Policy,* COM(2003) 113 final, Brüssel, 11. März 2003, S. 12, 17-18, <http://europa.eu.int/eur-lex/en/com/cnc/2003/com2003_0113en01.pdf>; *Life sciences and biotechnology. A strategy for Europe,* COM(2002) 27, Brüssel, <http://europa.eu.int/comm/biotechnology/pdf/com2002-27_en.pdf; *Life sciences and biotechnology – a strategy for Europe. Progress report and future orientations,* COM(2003) 96 final, Brüssel, 5. März 2003, <http://europa.eu.int/comm/biotechnology/pdf/com2003-96_en.pdf> (Zugriff: 20. Januar 2004).

[110] 2541. Tagung des Rates für allgemeine Angelegenheiten und Außenbeziehungen, 14500/03 (Presse 321) Brüssel, 17. November 2003, S. 11-17 <http://ue.eu.int/pressData/en/gena/77930.pdf> (Zugriff: 20. Januar 2004); Burkard Schmitt, *The European Union and armaments. Getting a bigger bang for the Euro,* Chaillot Papers No 63 (Paris: Institute for Security Studies, 2003).

[111] Ulf Hassgard, *The lowest echelon in Network Centric Warfare – possibilities and limitations in the soldier level command, control and communication system* (Stockholm: Swedish National Defence College, 2002).

[112] Dombrowski/Gholz/Ross, *Military Transformation and the Defense Industry after Next,* S. 83; Thornberry, „Fostering a culture of innovation", S. 5 (zit. gem. Internetversion).

und Mittel bereitzustellen, damit solche Aktivitäten künftig auf der Basis gemeinsamer Konzepte systematisch lanciert werden können. Damit ist schließlich, viertens, die Erweiterung des von der Rüstungsagentur zu berücksichtigenden Akteurskreises angesprochen. Die Agentur muss neben der Rüstungsindustrie auch mit anderen sicherheitsrelevanten Wirtschaftszweigen sprechen, um Projekte zu initiieren und abzustimmen. Dieser Aspekt muss aber auch bei der personellen Vertretung in der Agentur berücksichtigt werden. Es wird angesichts der vom Verteidigungs- auf den Sicherheitssektor erweiterten Perspektive nicht ausreichen, lediglich Vertreter des Verteidigungsministeriums in die Agentur zu entsenden. Andere Akteure aus dem Sicherheitssektor sowie aus anderen Ministerien – zu denken ist aufgrund der unterschiedlichen Ressortzuständigkeiten z.B. an die Bildungs- und Wissenschaftsministerien für die Forschung in sicherheitspolitisch relevanten zivilen Bereichen – sind dabei ebenso zu berücksichtigen.

Schlussfolgerungen

Die Ausführungen unterstreichen, dass die autonome nationale Entscheidungs- und Steuerungsfähigkeit im Zeitalter der sicherheitspolitischen Vernetzung endgültig ihre Grenzen erreichen wird. Ebenso verdeutlicht die Analyse der Konsequenzen, die aus vernetzter Operationsführung und vernetzter Sicherheitspolitik resultieren, die neo-funktionalistische These des Spill Over-Effekts, demzufolge (technischer) Fortschritt in einem Sektor zu weitreichendem (politischem) Handlungs- und Anpassungsbedarf in anderen Bereichen führt.

Die zentrale Schwäche des Neofunktionalismus, nämlich die Vernachlässigung der Politik, darf jedoch nicht zur Annahme verführen, dass der beschriebene Anpassungsbedarf geradezu automatisch erkannt und umgesetzt wird. Vielmehr geht es darum, dass die politischen Entscheidungsträger die beschriebenen Herausforderungen aktiv angehen. Dabei ist zweierlei hervorzuheben. Auf der nationalen Ebene rücken sicherheitspolitische Vernetzungsorgane und Koordinationsstellen in jeder Hinsicht ins Zentrum der Aufmerksamkeit. Diese sind künftig nicht nur für die sicherheitspolitische Lageanalyse, die Strategieschöpfung und die Führung in der normalen sowie in der außerordentlichen Lage zuständig. Sie werden auch die entscheidende Rolle bei der Koordination der Akteure und der Maßnahmen im Rahmen der vernetzten Operationsführung spielen. Zudem tragen sie in managementorientierter Hinsicht die Hauptverantwortung für die Sicherstellung der konzeptionellen Kohärenz (sicherheitspolitisches Managementsystem) und die ressortübergreifende Steuerung der Sicherheitsakteure sowie ihrer Mittel. Es versteht sich von selbst, dass ein derart anspruchsvolles Aufgabenspektrum kaum mit der bestehenden Ressourcenausstattung und den vorhandenen Fähigkeitsprofilen erbracht werden kann. Investitionen zur Stärkung sicherheitspolitischer Vernetzungsprozesse und -strukturen sollten daher besondere Priorität eingeräumt werden.

Ebenso müssen die Kompetenzen der internationalen Ebene gestärkt werden. Innerhalb des bestehenden intergouvernementalen Rahmens der Europäischen Sicherheits- und Verteidigungspolitik (ESVP) müssen die konzeptionelle Koordination und die Abstimmung wesentlich gestärkt werden. Das gilt für die vernetzte Operationsführung ebenso sehr wie für die vernetzte Sicherheitspolitik. Im ersten Fall müssen sich die EU-Mitglieder auf ein gemeinsames Konzept einigen und die dazu erforderlichen Umsetzungsprojekte über gemeinsame

Strukturen koordinieren. Im zweiten Fall muss Europa mehr dafür tun, dass sich die Logik der vernetzten Sicherheitspolitik und die damit einhergehende Reform der Sicherheitssektoren in den eigenen Ansätzen zur Konfliktvor- und -nachsorge spiegeln. Die Europäische Sicherheitsstrategie muss diesen Aspekt bewusst aufnehmen und im Rahmen spezifischer Programme vorantreiben. Zu diesem Zweck ist insbesondere ein Instrumentarium zur Bewertung der sicherheitspolitischen Vernetzungsfähigkeit der bestehenden und der neuen EU-Mitglieder sowie zur Transformation ihrer Sicherheitssektoren zu entwickeln, das sich an den oben diskutierten Grundsätzen orientiert. Daneben muss die Zusammenarbeit zwischen den Generaldirektorien der Europäischen Kommission sowie zwischen diesen und den neuen ESVP-Gremien ebenfalls im Sinne der angesprochenen Vernetzung überprüft und ausgebaut werden.

Abbildungsverzeichnis

Abkürzungsverzeichnis

ABC	Atomar-Biologisch-Chemisch
ACO	Allied Command Operations
ACT	Allied Command Transformation
BOA	Boule Opérationelle Aéroterrestre
BSR	Bundessicherheitsrat
C2	Command and Control
C4	Command, Control, Communications, Computers
CD&E	Concept Development and Experimentation
CIE	Collaborative Information Environment
COTS	Commercial off the Shelf
CPM	Costumer, Product, Management
CROP	Common Relevant Operational Picture
DARPA	Defense Advanced Research Projects Agency
DGA	Délégation Générale pour l'Armement
EBO	Effects Based Operations
EBP	Effects Based Planning
ESVP	Europäische Sicherheits- und Verteidigungspolitik
FachInfoSys	Fachinformationssystem
FCS	Future Combat System
FRES	Future Rapid Effect System
FSD	Full Spectrum Dominance
FüInfoSys	Führungsinformationssystem
FüSys	Führungssystem
IRF	Industrial Research Fellow
ISR	Intelligence, Surveillance, and Reconnaissance
IT	Informationstechnologie
JIP	Joint Interactive Planning
JWID	Joint Warrior Interoperability Demonstrations
LGSi	Lenkungsgruppe Sicherheit
MC02	Millennium Challenge 2002
MOTS	Military off the Shelf
NATO	North Atlantic Treaty Organization
NBD	Network Based Defense
NCC	Network Centric Capability
NCO	Network Centric Operations
NCW	Network Centric Warfare
NEC	Network Enabled/Enhanced Capabilities
NECS	Network Enabled Collective Security
NetOpFü	Vernetzte Operationsführung
NRF	NATO Response Force
NSR	Nationaler Sicherheitsrat
ONA	Operational Net Assessment
PARP	Planning and Review Process
PPP	Public-Private Partnership
RDO	Rapid Decisive Operations
RMA	Revolution in Military Affairs
SACEUR	Supreme Allied Commander Europe

SAC-T	Supreme Allied Commander Transformation
SAR	Search and Rescue
SCALANT	Supreme Allied Commander Atlantic
SiA	Sicherheitsausschuss
SJFHQ	Standing Joint Farces Headquarters
TDL	Technische Datenlinks
UNO	United Nations Organization
USIS	Überprüfung des Systems der inneren Sicherheit in der Schweiz
USJFCOM	United States Joint Forces Command
VPR	Verteidigungspolitische Richtlinien
ZASBw	Zentrum für Analysen und Studien der Bundeswehr

Die Autoren

Dirk Böcker, Generalleutnant, ist seit Oktober 2002 Stellvertreter des Generalinspekteurs der Bundeswehr. Im Rahmen seiner mehr als 30jährigen Karriere bei der Luftwaffe war er unter anderem Abteilungsleiter beim Luftwaffenkommando in Köln-Wahn, Referats- und Stabsabteilungsleiter im Führungsstab der Luftwaffe, Stellvertreter des Kommandierenden Generals Luftwaffenkommando Nord sowie Kommandierender General Luftwaffenkommando Süd und Commander Combined Air Operations Centre 4 sowie Befehlshaber des Luftwaffenführungskommandos.

Heiko Borchert (hb@borchert.ch) leitet ein Unternehmens- und Politikberatungsbüro und ist Direktor für Sicherheit und Verteidigung am Düsseldorfer Institut für Außen- und Sicherheitspolitik (DIAS). Er hat Internationale Beziehungen an der Universität St. Gallen (HSG) studiert und dort mit einer Arbeit über Europas Sicherheitsarchitektur promoviert sowie am Zentrum für Vergleichende und Internationale Studien (ETH/Universität Zürich) gearbeitet. Er doziert regelmäßig an Universitäten und Hochschulen und hat zahlreiche Publikationen zum Themenschwerpunkt Sicherheit und Verteidigung veröffentlicht.

Hubert Feigl (hubert.feigl@t-online.de) war leitender Mitarbeiter der Stiftung Wissenschaft und Politik (SWP) und ist heute als selbständiger Berater tätig. Er studierte Physik (Chemie) an der TU München (Abschluss als Diplomphysiker, Promotion zum Dr. rer. nat.). Nach längerer universitärer Forschungstätigkeit als Projektleiter am Institut für Physikalische Chemie und Elektrochemie wechselte er zur SWP, der offiziellen deutschen Einrichtung für wissenschaftliche Politikberatung. Er beschäftigte sich dort als Leiter einer Arbeitsgruppe schwerpunktmäßig mit den konzeptionell-strukturierenden Auswirkungen neuer rüstungstechnischer Entwicklungen und wurde auf diesem Gebiet in vielfältiger Form für offizielle Bedarfsträger beratend tätig.

Martin Neujahr (martinneujahr@bundeswehr.org), Major i.G., ist Konzeptentwickler am Zentrum für Analysen und Studien der Bundeswehr in Waldbröl. Nach dem Studium der Betriebswirtschaftslehre mit dem Schwerpunkt Wirtschaftsinformatik an der Universität der Bundeswehr in München schlossen sich mehrere Verwendungen im Bereich Command and Control von Luftstreitkräften an, bevor er an der Führungsakademie der Bundeswehr die Generalstabsausbildung absolvierte. Seitdem arbeitet er im Management des deutschen Anteils am internationalen Concept Development & Experimentation-Programm.

Burkhard Theile (burkhard.theile@rheinmetall-detec.com) leitet die Hauptabteilung Strategische Unternehmensentwicklung und Technologie der Rheinmetall DeTec AG in Ratingen. Er hat in Braunschweig Maschinenbau und Physik studiert und das Studium als Diplomphysiker abgeschlossen. Er wurde von der naturwissenschaftlichen Fakultät der TU Braunschweig mit einer raumfahrtwissenschaftlichen Arbeit zum Dr. rer. nat. promoviert. Sein Berufsleben schließt Tätigkeiten als Hochschullehrer und leitende Funktionen in der Industrie auf den Ge-

bieten Raumfahrt und Wehrtechnik ein. Fünf Jahre lang leitete er die Firmenvertretung eines deutschen Unternehmens in Washington/USA.