Heiko Borchert (Hrsg.)

# Potentiale statt Arsenale

## Sicherheitspolitische Vernetzung und die Rolle von Wirtschaft, Wissenschaft und Technologie

Vernetzte Sicherheit

Herausgegeben von Ralph Thiele und Heiko Borchert

Band 2

Heiko Borchert (Hrsg.)

# Potentiale statt Arsenale

## Sicherheitspolitische Vernetzung und die Rolle von Wirtschaft, Wissenschaft und Technologie

Seit 1789

Verlag E.S. Mittler & Sohn GmbH
Hamburg · Berlin · Bonn

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: 3-8132-8036-2
© 2004 by Verlag E.S. Mittler & Sohn, Hamburg; Berlin; Bonn
Alle Rechte vorbehalten
Produktion: Hans-Peter Herfs-George
Druck und Bindung: Storck Verlag, Hamburg
Printed in Germany

Das Erscheinen dieses Bandes wurde von der Rheinmetall DeTecAG gefördert.

Inhalt

**Heiko Borchert** ..... **7**
Potentiale statt Arsenale: Einleitung

**Gebhard Geiger** ..... **11**
Die sicherheitspolitische Bedeutung der Mikrowissenschaften und der Mikrotechnik

**Ralph Thiele** ..... **34**
Transformation und die Notwendigkeit der systemischen Gesamtbetrachtung

**Burkhard Theile und Norbert Härle** ..... **55**
Streitkräftetransformation aus der Sicht der Rüstungsindustrie

**René Eggenberger und Heiko Borchert** ..... **74**
Wissenschaft und Technologie in der Schweizer Armee

**Thomas Pankratz und Alfred Vogel** ..... **95**
Der Aufbau sicherheitspolitischer Fähigkeiten und der Beitrag von Wirtschaft und Wissenschaft: Status quo der Sicherheitsforschung in Österreich

**Abbildungs- und Tabellenverzeichnis** ..... **112**

**Abkürzungsverzeichnis** ..... **113**

**Die Autoren** ..... **115**

Heiko Borchert

## Potentiale statt Arsenale: Einleitung

Die Transformation der Streitkräfte ist darauf ausgerichtet, deren strukturelle Flexibilität und Lernfähigkeit zu verbessern, um dadurch Entscheidungsüberlegenheit herzustellen, kohärente Wirkungen zu erzeugen sowie streitkräftegemeinsame Einsätze und Unterstützung zu erbringen. Die Ausrichtung auf diese Eigenschaften ergibt sich aus den Anforderungen des sicherheitspolitischen Umfeldes, das sich durch Unübersichtlichkeit der Konfliktursachen, ihrer Entwicklung und der damit verbundenen Konsequenzen auszeichnet. Das verlangt von den staatlichen Machtinstrumenten im Allgemeinen und von den Streitkräften im Speziellen eine hohe Anpassungsfähigkeit, um schnell und effektiv auf unvorhergesehene Entwicklungen und Ereignisse reagieren zu können.

Bei der Gewährleistung dieser Anpassungsfähigkeit spielen Wirtschaft, Wissenschaft und Technologie eine Schlüsselrolle. Sie sind zum einen Treiber der Streitkräfteentwicklung, indem sie diese mit innovativen Fähigkeiten unterstützten. Zum anderen fördert der verstärkte Rückgriff auf zivile Technologie wegen der Möglichkeit der Mehrfachnutzung insbesondere jene Anwendungen und Lösungen, die zur Überwindung der Grenzen zwischen innerer und äußerer Sicherheit beitragen und dadurch die Herausbildung einer vernetzten Sicherheitspolitik unterstützen. „Potentiale statt Arsenale“ beschreibt daher den programmatischen Kern der Transformation: An die Stelle vorgefertigter Produkte und Dienstleistungen tritt die Fähigkeit, situationsabhängig jene Lösungen herbeizuführen, die es den staatlichen Sicherheitsinstitutionen im Verbund mit ihren Partnern erlauben, den im In- und im Ausland auftretenden sicherheitspolitischen Herausforderungen wirkungsvoll zu begegnen. Da die staatlichen Sicherheitsinstitutionen oftmals selbst nicht in der Lage sein werden, die Problemursachen und mögliche Lösungen im Voraus zu erkennen und zu benennen, bedingt Transformation eine neue Kooperationskultur mit der Wirtschaft und der Wissenschaft. Die damit verbundenen Chancen und Risiken beschreiben die fünf Beiträge des vorliegenden Sammelbandes.

Gebhard Geiger analysiert mit den technologischen Langfristentwicklungen einen wesentlichen Aspekt des neuen sicherheitspolitischen Umfelds. Seine Ausführungen zur Mikrowissenschaft und zur Mikrotechnik verdeutlichen, dass veränderte Werkstoffe und neue Produkteigenschaften sicherheitspoltische

Chancen eröffnen, beispielsweise in Bereichen wie der Aufklärung, der Datensicherheit, der Identifizierung biologischer Kampfstoffe oder der Verbesserung des individuellen Schutzes. Da es sich hierbei allerdings um Mehrzwecktechnologien handelt, die sowohl defensiv als auch offensiv genutzt werden können, erhöht sich auch das Risikopotential durch Missbrauch oder durch die Einschränkung der Wirksamkeit sicherheitspolitischer Instrumente (z.B. Rüstungskontrolle). Im Interesse der kontinuierlichen Auseinandersetzung mit den Folgen technologischer Trends ist es daher geboten, wissenschaftliche Basistechnologien (z.B. Mikrosysteme, Biotechnik) stärker mit sicherheitspolitischen Anwendungen zu verknüpfen und gleichzeitig die enge Vernetzung mit wissenschaftlichen und außerwissenschaftlichen Einrichtungen sicherzustellen.

An der Einsicht von Gebhard Geiger, dass der tief greifende technische Wandel für die Streitkräfte ein Dauerzustand bleiben wird, setzt der Beitrag von Ralph Thiele zur Streitkräftetransformation in der Bundesrepublik Deutschland an. Um in einem erweiterten Aufgabenspektrum schnelle, flexible und präzise Einsätze unter Anwendung möglichst geringer eigener Kräfte realisieren zu können, sind neue Konzepte und Verfahren erforderlich. Die vernetzte Operationsführung, die im Kern den konzertierten Einsatz aller staatlichen Machtinstrumente zum Gegenstand hat, basiert entscheidend auf der wirkungsorientierten Planung. Diese fasst viele bislang unabhängig voneinander erbrachte Planungsarbeiten in einem kohärenten, simulationsgestützten Ganzen zusammen. Dabei kommt der Konzeptentwicklung und Erprobung (Concept Development and Experimentation, CD&E) eine Schlüsselfunktion zu. Ziel ist es, über alle Planungsebenen hinweg einen aus verschiedenen Schritten bestehenden Prozess zu institutionalisieren, der die Entwicklung von Konzepten, ihre Bewertung sowie ihre Weiterentwicklung und Verfeinerung ermöglicht. Gerade weil es angesichts der erforderlichen Betrachtung aller relevanten Wechselwirkungen so gut wie unmöglich ist, im Voraus zu wissen, welcher Ansatz sich in der Praxis bewähren wird, gewinnen Modellbildung und Simulation an Bedeutung. Damit lassen sich konzeptionelle Überlegungen, organisatorische Vorstellungen sowie Innovationen im technologischen Bereich kritisch auf ihre Praktikabilität, ihre Zuverlässigkeit und ihre Kostenfolgen überprüfen.

Hierzu wie auch zur Bereitstellung der von der Bundeswehr benötigten Fähigkeiten ist der enge Schulterschluss mit der Industrie angezeigt. Darauf weist neben Ralph Thiele auch der Beitrag von Burkhard Theile und Norbert Härle hin. Sie argumentieren, dass die Transformation der Streitkräfte wesentlich von der erfolgreichen Einbindung und von der Transformation der Rüstungsindustrie

abhängen wird. Wenn sich der Kunde vernetzt, dann ist auch die Industrie zu bereichsübergeifendem Denken und Handeln aufgefordert. Transformation bedeutet dabei für die Industrie u.a. die verstärkte Ausrichtung auf Innovation und Weiterentwicklung in enger Abstimmung mit dem Kunden, z.B. durch integrierte Kunden-Lieferanten-Teams (Integrated Project Teams, IPT) und gemeinsame Konzeptentwicklung. Gerade weil die Konzeptentwicklung im internationalen Rahmen die künftigen Fähigkeitsanforderungen an die Streitkräfte bestimmt, ergeben sich daraus indirekte Abhängigkeiten der nationalen Industrie. Diese sucht daher nach neuen Wegen, um sich z.B. auch am NATO CD&E-Prozess beteiligen zu können. Daneben erfordern die neuen Kundenbedürfnisse und die Komplexität technischer Lösungen und Risiken neue Leistungen bei der Systemintegration. Der Systemintegrator definiert das Gesamtsystem, leitet daraus Spezifikationen für die Systemkomponenten ab und nimmt Managementfunktionen für den Kunden war. Weil er über die Auswahl von Lösungswegen und damit auch von Unterauftragnehmern entscheidet, haben seine Entscheidungen auch industriepolitische Auswirkungen. Diese Entwicklung dürfte tendenziell eher die finanzstarken Unternehmen in der Rolle des Systemintegrators bevorzugen, während sich für Mittelständler vor allem dann Chancen eröffnen, wenn sie bahnbrechende Technologien vom Markt schnell in die Streitkräfte integrieren können.

Die Integration technischer und wissenschaftlicher Innovation in die Streitkräfte ist auch für die Streitkräfteplanung eine große Herausforderung, wie die beiden Fallbeispiele aus der Schweiz und aus Österreich illustrieren. In beiden Fällen geht es um die Frage, wie die vorhandenen Konzepte, Strukturen, Prozesse und Instrumente angepasst werden müssen, um jene Fähigkeiten zu generieren, die für die Streitkräfte von heute und morgen relevant sind.

René Eggenberger und Heiko Borchert legen dar, wie diese Zielsetzung durch die Integration der Arbeiten im Bereich Wissenschaft und Technologie (W+T) in die langfristig angelegten Prozesse der Streitkräfte- und der Unternehmensentwicklung im Verwaltungsbereich Verteidigung des Eidgenössischen Departements für Verteidigung, Bevölkerungsschutz und Sport erreicht werden soll. Zu diesem Zweck wurde ein eigener W+T-Prozess definiert, der von der Abteilung Prospektivplanung konsequent fähigkeitsorientiert geführt und in IPT zwischen Bedarfsträgern und Bedarfsdeckern umgesetzt wird. Inhaltlich stehen dabei vor allem die für die vernetzte Operationsführung zentralen Fähigkeitsbereiche der Führung, Informationsgewinnung, Aufklärung und Überwachung (C4ISR) im Mittelpunkt. Die Neuausrichtung der Streitkräfteentwicklung auf

diesen Schwerpunkt verlangt den Umbau eines nach klassischen Geschichtspunkten entwickelten „W+T-Erbes“ in Richtung Sensortechnologie, Informations- und Kommunikationstechnologie sowie Systemanalyse. Daneben gewinnen „menschbezogene“ Disziplinen aus den Sozial- und Geisteswissenschaften an Bedeutung, u.a. um die vielfältigen Wechselbeziehungen an der Schnittstelle zwischen Mensch und Maschine beurteilen, in der Aus- und Weiterbildung neue Schwerpunkte setzen sowie um objektiv nachvollziehbare und begründbare Entscheidungsgrundlagen für die militärische und politische Führung bereitstellen zu können.

Thomas Pankratz und Alfred Vogel führen aus, dass die Bemühungen zum systematischen Aufbau der sicherheits- und verteidigungspolitischen Forschung in Österreich noch am Anfang stehen. Mit ihrer Feststellung, dass wissenschaftliche und technologische Expertise die Attraktivität als internationaler Kooperationspartner steigern kann und damit auch den selbst definierten Anspruch Österreichs als „aktiver Akteur“ in der europäischen Integrationspolitik unterstützt, geben die Autoren die Zielrichtung der künftigen Bemühungen vor. Die konzeptionellen Grundlagen für dieses neue Politikfeld werden gegenwärtig unter Leitung der Österreichischen Akademie der Wissenschaft erarbeitet. Als besonderes vielversprechend erweist sich dabei gerade unter transformationsrelevanten Gesichtspunkten die Bereitschaft der Universitäten und anderer Forschungseinrichtungen zur engen Zusammenarbeit mit dem Bundesministerium für Landesverteidigung (BMLV). Dieses dürfte aufgrund seiner Expertise sowie besonderer Strukturen, z.B. verfügt nur das BMLV über eine eigene Wissenschaftskommission, eine zentrale Rolle in diesem neuen Themenfeld spielen, muss dazu aber die konzeptionellen Defizite in diesem Bereich abbauen.

Die Beiträge dieses Sammelbandes wurden für einen im Mai 2004 durchgeführten und vom Düsseldorfer Institut für Außen- und Sicherheitspolitik initiierten TRIAS-Expertenworkshop erarbeitet. TRIAS schließt in einer Arbeitsplattform das Zentrum für Transformation der Bundeswehr (Waldbröl), die Abteilung Prospektivplanung im Planungsstab der Schweizer Armee (Bern) und das Büro für Sicherheitspolitik im Bundesministerium für Landesverteidigung (Wien) zusammen und fördert den systematischen Dialog und Erfahrungsaustausch in Bezug auf sicherheitspolitische und streitkräfterelevante Langfristentwicklungen. Der Herausgeber dankt allen Beteiligten herzlich für die engagierte Mitarbeit sowie die Unterstützung der TRIAS-Initiative. Besonderer Dank gilt der Rheinmetall DeTec AG, die den Expertenworkshop und die Drucklegung des Sammelbandes finanziell unterstützt hat.

Gebhard Geiger

# Die sicherheitspolitische Bedeutung der Mikrowissenschaften und der Mikrotechnik*

Informationselektronik und Biotechnologie werden heute oft als die Schrittmacher der technischen Innovation schlechthin angesehen. Insbesondere die Computertechnik bildet die gemeinsame Grundlage für eine kaum mehr überschaubare Anzahl aktueller wissenschaftlich-technischer und wirtschaftlich-sozialer Veränderungen. Sie reichen von der rechnergestützten Sequenzierung des Genoms über die Globalisierung der Wirtschaft bis hin zum Betrieb von Satellitensystemen und bemannten Weltraumstationen. Allerdings stützen sich Informations- und Biotechnologie ihrerseits auf immer neue Ergebnisse der mikrophysikalischen Forschung, die zur Entwicklung von Mikroprozessoren (Chips), der Lasertechnik und zu zahlreichen neuartigen Materialien und Materialeigenschaften mit nahezu unerschöpflichen Nutzungspotentialen geführt haben.

Eine zentrale Rolle kommt zunehmend der so genannten Nanotechnologie zu.[1] Physikalisch gesehen befasst sich die Nanotechnologie mit dem Entwurf, dem Bau und der Anwendung besonders kleiner Mikrosysteme von der Größenordnung einzelner Atome und Moleküle. Ihre sicherheits- und rüstungspolitischen Konsequenzen sollen hier in der Wechselbeziehung mit anderen Technologien – insbesondere solchen auf biowissenschaftlicher Grundlage – aber auch mit politisch-gesellschaftlichen Veränderungen von der Art der Globalisierung (weltweite Vernetzung) der Märkte oder der Kommunikationsmedien skizziert werden. Im Vordergrund stehen die sicherheitspolitischen Probleme der so genannten Dual Use-Technologien, die sich gleichermaßen für militärische wie kommerzielle Verwendungen eignen.

---

* Der vorliegende Beitrag ist eine überarbeitete, aktualisierte Fassung meiner unveröffentlichten Studie *Rüstungspotentiale neuer Mikrotechnologien* (Berlin: Stiftung Wissenschaft und Politik, 2003).

1 Von griech nano = Zwerg; 1 Nanometer = der millionste Teil eines Millimeters.

**Nanotechnologie**

Unter Nanotechnologie versteht man das Forschungs- und Entwicklungsgebiet, das sich mit dem technischen Eingriff in die Wechselwirkung zwischen einzelnen Atomen und Molekülen befasst. Atomdurchmesser liegen größenordnungsmäßig im Bereich von einem Zehntel Nanometer. Dementsprechend versteht man unter physikalisch-chemischen Nanostrukturen besonders kleine Mikrosysteme mit Abmessungen von bis zu etwa 100 Nanometern.

Schwerpunktgebiete der nanotechnischen Forschung und Entwicklung sind heute unter anderem Elektronik, Optik und Energietechnik in der Physik sowie Entwurf und Katalyse neuer Kunststoffe (Keramik, Polymere u. a.) in der Chemie.[2] Medizinische und pharmazeutische Nanotechnologie zielen indessen auf die Herstellung von Nanoteilchen – und deren präzise gesteuertem Transport im Organismus – zu diagnostischen und therapeutischen Zwecken, weiterhin auf die Behandlung einzelner Tumorzellen bei gleichzeitiger Schonung des gesunden Gewebes sowie auf die Verträglichkeit von Medikamenten und Werkstoffen (Pharmakologie).

Erforschung und gezielte technische Manipulation einzelner atomarer und molekularer Systeme nutzen quantenphysikalische Ströme und Kräfte, insbesondere den so genannten quantenmechanischen Tunneleffekt, um einzelne Atome und Moleküle und damit die Struktur der Materie sichtbar zu machen.[3] Dieser revolutionären experimentellen Technik entsprechen neuartige Fertigungstechniken, mit der sich physikalisch-chemische Nanostrukturen gewissermaßen Stück für Stück aus atomaren Bauteilen zusammensetzen lassen. Herkömmliche Fabrikationsverfahren beruhen darauf, physikalische Prozesse und chemische Reaktionen über die Regelung makroskopischer Fertigungs- und Reaktionsbedingungen wie Druck, Temperatur und Rohstoffzufuhr zu steuern (Top Down-Verfahren). Demgegenüber verfolgt die Nanotechnik eine Art Bottom Up-Methode bei der Montage von Molekülen, Kristallen und Werkstoffen aus einzelnen atomaren Bauteilen. Verfahren dieser Art benutzt man beispielsweise zur extrem dünnen Beschichtung von Oberflächen, zur Feinsteuerung des Kristallwachstums oder zur Katalyse (Prozessführung) nanochemischer Reaktionen.

---

2 „Nanotechnologie", *Spektrum der Wissenschaft–Spezial*, 2 (2001); Michael Köhler, *Nanotechnologie* (Weinheim: Wiley-VCH, 2001). Horst-Günter Rubahn, *Nanophysik und Nanotechnologie* (Stuttgart: Teubner, 2002); Bharat Bhushan (ed.), *Springer-Handbook of Nanotechnology* (Berlin: Springer, 2004).

3 Heinrich Hörber und Thomas Früh, „Die sanfte Sonde", *Spektrum der Wissenschaft–Spezial*, 2 (2001), S. 24-29.

Angestrebt wird die massenhafte, kommerzielle Herstellung möglichst einfacher atomarer und molekularer Bauteile, die zu Kunststoffen mit neuartigen Eigenschaften führen. Abbildung 1 zeigt die Anordnung von sechseckigen Kohlenstoffringen zu einem zylinderförmigen Gitter (Nanoröhre) von 1,2 Nanometern Durchmesser als Beispiel. Nanoröhren sind fester als Stahl und dabei doch elastisch, zugfest, thermisch äußerst stabil und zeichnen sich durch besondere elektronische Leitfähigkeitsmerkmale aus.

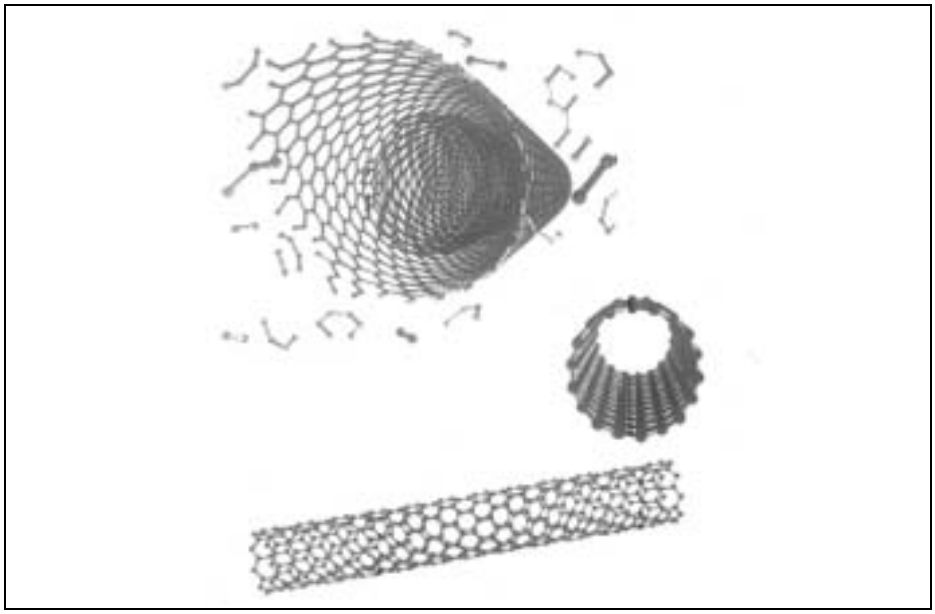


Abbildung 1: Nanotechnische Kristallgitter. Das Beispiel der „Nanoröhre"

Quelle: „Nanotechnologie", *Spektrum der Wissenschaft-Spezial,* 2 (2001), S. 49-50.

Künftige Verwendungsmöglichkeiten für die Bottom Up-Verfahren der Kunststoffherstellung rücken die Nanotechnologie heute bereits ins Zentrum des sicherheitspolitischen Forschungsinteresses. Mit ihrer Hilfe können in Zukunft auch neuartige chemische (toxische, nichtletale usw.) Kampfstoffe in beliebigen Mengen erzeugt werden. Sie bedürfen weder großer, weithin sichtbarer Fabrikationsanlagen noch langfristiger Produktionszyklen oder einer breiten Rohstoffbasis. Ähnliches gilt für die rasche, massenhafte nanotechnische Fertigung waffenfähiger Materialien und Rüstungsgüter.

Die enormen Nutzungspotentiale physikalischer, chemischer und biologischer Anwendungen der Nanotechnologie liegen auf der Hand. Sie ermöglicht die Synthese völlig neuartiger Stoffe und Materialien, die in der Natur nicht vorkommen und für den jeweiligen Anwendungszweck „maßgeschneiderte" Eigenschaften besitzen. Hierzu zählen unter anderem der (widerstands- und verlustfreie) Ladungs- und Energietransport, die Energie- und Datenspeicherung sowie eine nahezu unüberschaubare Anzahl mechanischer, elektromagnetischer, optischer, thermischer und chemischer Merkmale bis hin zu solchen des biologischen Stoffwechsels. Tatsächlich ist es beim heutigen Stand der Entwicklung weniger eine Frage der physikalischen Möglichkeiten denn der Zeit, daß mit fortschreitender Nanotechnik eine völlig neuartige „zweite Natur" entsteht, die sich selbst von der bereits hoch technisierten heutigen Welt in wesentlichen Elementen unterscheidet.

Die Zukunftsperspektiven der Nanotechnologie scheinen oft in Nachbarschaft zur Science-Fiction zu liegen, sind aber alles andere als utopisch. Nanotechnische Forschung wird weltweit mit erheblichem finanziellem Aufwand betrieben, während weitreichende wissenschaftlich-technische Neuerungen auf allen oben erwähnten Gebieten heute bereits an der Tagesordnung sind.[4]

**„Elektronik vom Allerkleinsten"**

In den neueren amerikanischen Militärdoktrinen[5] gilt die moderne Informations- und Kommunikationstechnik als Auslöser einer Revolution in Military Affairs (RMA). Die Umwälzungen wurden hauptsächlich durch die umfassende elektronische Vernetzung des militärischen Führungs- und Nachrichtenwesens bewirkt. Sie erstrecken sich auf alle Ebenen der Rüstung, Organisation und Streitkräfteplanung, Strategie, Taktik und militärischen Operation.[6] Angesichts der sich abzeichnenden nanotechnischen Hardware-Entwicklungen vermittelt die RMA bisher allerdings kaum mehr als einen ersten Vorgeschmack auf kommende informationstechnische Umwälzungen.

---

4 Bundesministerium für Bildung und Forschung (BMBF), *Nanotechnologie in Deutschland – Standortbestimmung* (Bonn: BMBF, 2002).

5 John M. Shalikashvili (ed.), *Joint Vision 2010* (Washington, DC: Joint Chiefs of Staff, 1996). Henry H. Shelton (ed.), *Joint Vision 2020* (Washington, DC: Joint Chiefs of Staff, 2000).

6 John Arquilla and David F. Ronfeldt (eds.), *In Athena's Camp. Preparing for Conflict in the Information Age* (Santa Monica, CA: Rand, 1997); Zalmay M. Khalilzad and John P. White (eds.), *The Changing Role of Information in Warfare* (Santa Monica, CA: Rand, 1999).

Schätzungen gehen davon aus, daß es bis zur Mitte des nächsten Jahrzehnts gelingen wird, integrierte elektronische Schaltelemente (Mikroprozessoren) mit Längenabmessungen im Nanometerbereich zu bauen, die in der Lage sind, Milliarden Operationen gleichzeitig („parallel") auszuführen.[7] Bei nanotechnisch gefertigten Speicherchips erwartet man Kapazitäten bis zu 64 Gigabytes.[8] Weitere beträchtliche Steigerungen des Datenspeichervolumens und der Datenübertragungsgeschwindigkeit lassen sich erzielen, sofern es in Zukunft gelingt, die quantenmechanischen Zustände einzelner Elektronen (die so genannte Spinpolarisation) gezielt zu verändern. Die Anzahl der Operationen, die ein „Quantencomputer" auf dieser Basis parallel auszuführen in der Lage ist, kann gegenüber nanotechnisch gefertigten Mikroprozessoren nochmals nahezu beliebig gesteigert werden. Die Technik des Quantencomputers befindet sich allerdings erst in den Anfängen. Bei all ihren immensen Leistungspotentialen hat sie mit erheblichen Fertigungs- und Betriebsproblemen zu kämpfen (Instabilität der elektronischen Quantenzustände und der in ihnen gespeicherten Information). Ob diese Probleme jemals technisch überwunden werden können und ob dies unter wirtschaftlichen Bedingungen möglich sein wird, kann im Augenblick kein Fachmann sagen.

Wie immer die Lösung aussehen wird – jedenfalls ist die Informationselektronik bereits dabei, aus dieser Not eine Tugend zu machen und die Störanfälligkeit der Quanteninformation zur Lösung drängender technischer Probleme zu nutzen. Verschlüsselte Nachrichten, die als Quanteninformation gespeichert oder übertragen werden, sind weitgehend spionagesicher: Jeder unberechtigte Versuch, einen fremden Code zu „knacken", muss ihn zerstören. Die „Quantenkryptographie" mit zahlreichen künftigen zivilen und militärischen Anwendungen macht sich diesen Zusammenhang zunutze.[9]

In Verbindung mit der Nanoelektronik tragen noch weitere Hardware-Entwicklungen in Physik, Chemie und nicht zuletzt in den Biowissenschaften zur künftigen Informationstechnik bei. Zu nennen sind hier in erster Linie die Optoelektronik, Laser- und Glasfasertechnik sowie intelligente Materialien (Smart Materials), die auf Licht-, Druck-, Temperaturschwankungen, Chemikalien, elektrische und magnetische Signale usw. auf technisch exakt vorprogrammierte Weise reagieren. Eine der wesentlichen Folgen wird eine erhebliche

---

[7] „Elektronik vom Allerkleinsten" titelte hierzu die Zeitschrift *Spektrum der Wissenschaft – Spezial*, 2 (2001).

[8] 1 Gigabyte = $10^9$ Bytes.

[9] Ulf von Rauchhaupt, „Mit verschränktem Licht sicher verschlüsselt", *Frankfurter Allgemeine Sonntagszeitung* 11. Juli 2004, S. 53.

Steigerung der Datenübertragungskapazität und -geschwindigkeit der Informationsnetze sein, die die skizzierten neuen Chip- und Computerleistungen auf der Netzwerkebene unterstützen und ergänzen. Dies gilt insbesondere für die Datenübertragung mittels Laserimpulsen durch billige und leistungsfähige Glasfaserkabel sowie die Nutzung schneller optischer Schaltelemente, die so genannten Optical Switches, beim Befördern (Routing) von Lasersignalen durch Datennetze.

Vom Standpunkt ihrer militärischen Anwendungsmöglichkeiten aus gesehen, werden alle diese technischen Neuerungen in ihrer Gesamtheit zu einem einzigen Ergebnis führen: Sie werden die RMA auf absehbare Zeit weiter vorantreiben, das heißt beschleunigen und, gemessen an ihren bisherigen Auswirkungen, noch einmal erheblich steigern. Gestützt auf hoch entwickelte C4ISR-Technologien[10] wird es einer hoch technisierten Armee in Zukunft mehr denn je möglich sein,

- sich dem Gegner auf allen Gebieten der militärischen Information und Kommunikation überlegen zu erweisen (Information Dominance);
- unterschiedliche militärische Fähigkeiten zu einem „System der Systeme" zusammenzuführen;
- ein in Echtzeit koordiniertes Gefecht aller Teilstreitkräfte und Waffensysteme zu führen; und dabei
- intelligente, unbemannte, distanzfähige und nahezu perfekt getarnte Präzisionswaffen einzusetzen.[11]

**Biotechnologie**

Wegen ihrer revolutionären Folgen steht die Gentechnik heute und wahrscheinlich auch in absehbarer Zukunft im Mittelpunkt sowohl des wissenschaftlichen Forschungsinteresses als auch der öffentlichen Debatte um Nutzen und Risiken moderner Biowissenschaften. Grundlegende gentechnische Forschungsfelder sind die Analyse und die gezielte Veränderung des Erbguts von Pflanzen, Tieren und Menschen sowie die künstliche, experimentelle und inzwischen längst auch

[10] Command, Control, Computers, Communications, Intelligence, Surveillance, Reconnaissance.

[11] Shalikashvili, *Joint Vision 2010;* Shelton, *Joint Vision 2020;* Computer Science and Telecommunications Board, National Research Council USA, *Realizing the Potentials of C4I: Fundamental Challenges* (Washington, DC: National Academy Press, 1999).

industrielle Fortpflanzung genetisch modifizierter, identischer Organismen (Klonen).[12] Ihre möglichen Dual Use-Verwendungen sind breit gestreut:

- Experimentelle Grundlagenforschung und angewandte (z.B. pharmakologische, ökologische) Forschung
- Medizinische Diagnose, Therapie und Bekämpfung von Krankheitserregern und Epidemien
- Biokatalysatoren für die chemische Verfahrenstechnik
- Offensive, letale und nichtletale Kampfstoffe, aber auch medizinische Abwehr von und Impfschutz gegen solche Kampfstoffe
- Technischer Biowaffenschutz und Detektoren für biologische Kampfstoffe[13]

Hinzu kommt der mögliche Gebrauch von solchen gentechnischen Produkten, die sich wegen ihrer toxischen Wirkung und raschen, unbemerkten Ausbreitung in der Umwelt und in menschlichen Populationen zu terroristischen Angriffen auf die Zivilbevölkerung eignen („Bioterrorismus").[14]

Manipulationen des Erbguts von Lebewesen gehören zu den herkömmlichen Biotechnologien, so etwa bei der Züchtung geeigneter pflanzlicher und tierischer Eigenschaften oder auch bei der Bestrahlung von Samen zu experimentellen Zwecken. Bei herkömmlichen Verfahren der Tier- und Pflanzenzucht treten jedoch genetische Innovationen ausschließlich nach dem Zufallsprinzip (Mutation) auf. Ob dabei neue, technisch erwünschte Erbeigenschaften entstehen, bleibt meist seltenen Zufallsereignissen überlassen. Hingegen kann durch Gentransfer neues genetisches Material „maßgeschneidert" werden. Der gezielte gentechnische Eingriff übertrifft daher herkömmliche Biotechnologien bei weitem an Möglichkeiten zur Feinsteuerung der angestrebten Effekte und an „Treffsicherheit". Durch Gentransfer lassen sich insbesondere Mikroorganismen (Pilze, Viren, Bakterien u.a.) in ihren physiologischen Reaktionen derart modifizieren,

---

12 Das „Klonen", das heißt die Vervielfältigung genetisch identischer Organismen, gilt nicht als Gentechnik im engeren Sinne, kann aber mit gentechnischen Experimenten, Methoden usw. verknüpft werden.

13 Committee on Opportunities in Biotechnology for Future Army Applications, National Research Council USA, *Opportunities in Biotechnology for Future Army Applications* (Washington, DC: National Academies Press, 2001).

14 Eric S. Grace, *Biotechnology Unzipped: Promises and Realities* (Washington, DC: National Academies Press, 1997); Stacey L. Knobler, Adel A. F. Mahmoud and Leslie A. Pray (ed.), *Biological Threats and Terrorism: Assessing the Science and Response Capabilities* (Washington, DC: National Academies Press, 2002).

daß sie Giftstoffe oder Hormone wie etwa das Humaninsulin produzieren, gegen Antibiotika resistent oder anfällig werden oder – bei Übertragung auf andere Organismen – deren Immunreaktionen verstärken oder hemmen. Für die medizinische Diagnose und Therapie, Immunologie und Epidemiologie bietet die Gentechnik daher neue, bisher ungeahnte Möglichkeiten. Unter sicherheitspolitischen Gesichtspunkten stehen diesen Nutzungspotentialen enorme Möglichkeiten des Missbrauchs durch biologische Kriegführung und Bioterrorismus gegenüber. Viele dieser Möglichkeiten sind erst in Einzelfällen nachgewiesen, oder die Produkte gentechnischer Manipulationen erweisen sich als instabil und nicht überlebensfähig, so dass die Erfolgschancen der Gentechnik in vielen Anwendungsfällen durchaus kritisch gesehen werden müssen. Doch sind die Grenzen der gentechnischen Manipulierbarkeit des Lebens anscheinend noch längst nicht absehbar, geschweige denn erreicht. Ähnliche Feststellungen gelten für das Klonen von Organismen. Klonen wird sich voraussichtlich als *der* „Mechanismus" durchsetzen, mit dem sich gentechnisch erzeugte Eigenschaften auf die schnellstmögliche Art und Weise „an den Markt" bringen lassen, „auf Lager" gehalten werden können und mit dem die (Massen-)Produktion identischer Organismen zu Forschungs- und kommerziellen Zwecken langfristig aufrechterhalten werden kann. Die gleichen Möglichkeiten bietet das Klonen genetisch modifizierter Organismen für deren Gebrauch als Biowaffen beziehungsweise für die Produktion von Biotoxinen auf gentechnischer Basis.

Mit den experimentellen Techniken und Anwendungen des Gentransfers sind die aktuellen Möglichkeiten der Biotechnologie noch längst nicht erschöpft. Insbesondere im Zusammenwirken zwischen biomedizinischen, physikalisch-chemischen und informationstechnischen Innovationen sind in jüngster Zeit technologische Forschungs- und Entwicklungsgebiete mit weit reichenden zivilen und militärischen Anwendungen entstanden.[15] Als Beispiel sei hier lediglich auf den Einfluss der Neurophysiologie und Künstlichen Intelligenz auf Sensorik, Datenverarbeitung, Test und Simulation von Wechselwirkungen des Mensch-Maschine-Verhältnisses hingewiesen.[16] Wechselwirkungseffekte zwischen un-

[15] Scott P. Layne, Tony J. Beugelsdijk and C. Kumar N. Patel (ed.), *Firepower in the Lab: Automation in the Fight against Infectious Diseases and Bioterrorism* (Washington, DC: National Academies Press, 2001).

[16] Christa Maar, Ernst Pöppel und Thomas Christaller (Hrsg.), *Die Technik auf dem Weg zur Seele – Forschungen an der Schnittstelle Gehirn/Computer (*Reinbek: Rowohlt, 1996); Rodney Brooks, *Menschmaschinen – Wie uns die Zukunftstechnologien neu erschaffen* (Frankfurt a. M.: Fischer, 2002); Claudia Borchard-Tuch und Michael Groß, *Was Biotronik alles kann* (Weinheim: Wiley–VCH, 2002).

terschiedlichen technischen Trends können sich sicherheitspolitisch als ebenso folgenreich erweisen wie die hier untersuchten Technologien selbst.

**Trends und Verwendungsmerkmale der neuen Technologien**

*Dual Use*

Bei den hier skizzierten Technologien ist eine eindeutige Zuordnung zur ausschließlich militärischen oder zivilen Anwendung über weite Strecken nicht erkennbar. Hinzu kommt, daß sich moderne Mikrotechnologien meist auch für andere sicherheitspolitisch bedeutsame Zwecke eignen – etwa für solche des Terrorismus, der organisierten Kriminalität und natürlich auch zu deren Bekämpfung. Was diese Technologien für terroristische und kriminelle Zwecke nützlich macht, sind in aller Regel genau ihre Dual Use-Eigenschaften. Dual Use-Eigenschaften bieten daher auch im Hinblick auf die erweiterte Bedrohung durch Terrorismus oder internationale Kriminalität wesentliche Ansatzpunkte für die sicherheitspolitische Analyse.

Ganz allgemein lässt sich feststellen, daß eine Technologie in dem Maße mehrzweckfähig ist, in dem sie nicht nur wirtschaftlichen, wissenschaftlichen und anderen politisch-gesellschaftlichen Zielen gleichzeitig dient, sondern auch notwendige Voraussetzung für die Entwicklung und den Betrieb anderer Technologien und technischer Systeme schafft. Diese Stützungsfunktion ist für die moderne Informationstechnologie offenkundig. Sie beruht allerdings weniger darauf, daß (die Verfügbarkeit von) Information eine Ressource ist, auf die jeder jederzeit angewiesen ist, sondern daß Information heute in allen Lebensbereichen zur (programmierten, automatisierten, intelligenten) Systemsteuerung eingesetzt wird. In dem Maße, in dem es militärische und zivile Aufklärungs-, Telekommunikations-, Satelliten- und Transportsysteme gibt, ist die digitale Kommunikation immer auch eine Mehrzwecktechnologie. Diesen Aspekt trifft die bereits zitierte amerikanische Streitkräftedoktrin Joint Vision 2010 sehr genau, wenn sie den informationsgesteuerten Verbund von Teilstreitkräften als ein System von Systemen bezeichnet.

Ähnlich offenkundig ist die Dual Use-Verwendbarkeit nanotechnischer Erkenntnisse, Verfahren und Produkte. Sie erstreckt sich auf alle oben skizzierten Gebiete der Information und Kommunikation, Material- und Werkstoffherstellung (einschließlich Kampfstoffen beziehungsweise nano- und gentechnisch

hergestellter Impfstoffe zu deren Abwehr), Sensorik und Lasertechnik sowie Transport und Verkehr, Energie- und Antriebstechnik.[17]

In Aufzählungen herkömmlicher biologischer Kampfstoffe und Waffen nehmen die einschlägigen Biotoxine, Seuchen- und Krankheitserreger oft viele Druckseiten ein.[18] Inzwischen hat die moderne Biotechnologie das Spektrum von Prozessen, Reaktionen und gentechnischen Produkten mit pathogenen beziehungsweise toxischen Wirkungen auf Mensch und Umwelt noch einmal stark erweitert. Ein zusätzliches, wesentliches Problem liegt in der ausgeprägten Mehrzweck-Eignung vieler ihrer Verfahren und Produkte: Ein und dieselbe Technik kann der biologischen Kriegführung ebenso dienen wie terroristischen, wissenschaftlichen, medizinisch-therapeutischen und kommerziellen Zwecken. Selbst unter rein militärischen Gesichtspunkten kann sie sowohl mit berechtigter defensiver als auch mit verbotener offensiver Absicht eingesetzt werden. Schließlich sind im Zuge der biotechnischen Revolution die Verfügbarkeit und die Verbreitung von Dual Use-Laborgeräten samt dazugehörendem gentechnischem Wissen weltweit stark gestiegen.

Zur Erläuterung einige Beispiele. Botulin ist eine für den Menschen hoch giftige Substanz, die, von Bakterien erzeugt, verschiedentlich als Kampfstoff hergestellt und gelagert wurde, darunter von den USA (bis 1969) und der Sowjetunion, von dieser auch noch lange nach dem internationalen Verbot biologischer Waffen (1972).[19] Botulin kann heute von unterschiedlichen Arten gentechnisch manipulierter Bakterien produziert werden. Auf zivile Anwendungen des Botulin trifft man bei der medizinischen Behandlung schwerer Lähmungserscheinungen und in der kosmetischen Industrie. Der Schutz von Truppen und Zivilbevölkerung gegen bioterroristische Angriffe erfordert gentechnische und

---

[17] Interagency Working Group on Nanoscience, Engineering and Technology, National Science and Technology Council, *National Nanotechnology Initiative: Leading to the Next Industrial Revolution* (Washington, DC: Office of Science and Technology Policy, The White House, 2000), Kap. 4; Board on Physics and Astronomy, National Research Council USA, *Physics in an New Era* (Washington, DC: National Academies Press, 2001), Kap. 8; John L. Peterson and Dennis M. Egan, *Small Security: Nanotechnology and Future Defense* (Washington, DC: Center for Technology and National Security Policy, National Defense University, 2002).

[18] Joseph Cirincione, Jon B. Wolfsthal and Miriam Rajkumar, *Deadly Arsenals: Tracking Weapons of Mass Destruction* (Washington, DC: Carnegie Endowment for International Peace, 2002), S. 57-61.

[19] Judith Miller, Stephen Engelberg and William Broad, *Germs: Biological Weapons and America's Secret War* (New York: Simon and Schuster, 2001); Jonathan B. Tucker and Raymond A. Zilinskas (eds.), *The 1971 Smallpox Epidemic in Aralsk, Kazakhstan, and the Soviet Biological Warfare Program* (Monterey, CA: Center for Nonproliferation Studies, Monterey Institute of International Studies, 2002), S. 9-11.

pharmakologische Laborexperimente mit botulinerzeugenden Bakterien und bakteriellen Viren zur Gewinnung geeigneter Impfstoffe, Antikörper und Immunglobuline. Die dabei verwendeten Methoden und Techniken, die Erkenntnisse und die gezüchteten Viren- und Bakterienstämme sind im Prinzip auch offensiv nutzbar. Zum Beispiel ist es aufschlussreich beziehungsweise notwendig, um wirksame Impfstoffe gegen Botulin zu gewinnen, mit Organismen zu experimentieren, die einen bereits bestehenden Impfschutz überwinden können oder die resistent gegen Antibiotika sind. Erkenntnisse hierüber und die Verfügung über solche Organismen stellen einerseits ein erhebliches sicherheitspolitisches Bedrohungspotential dar, andererseits fallen sie als zivile beziehungsweise defensive Forschungsergebnisse nicht unter das Entwicklungsverbot für Biowaffen.[20]

Ein anderes Beispiel für den ausgeprägten Mehrzweck-Charakter biotechnischer Produkte und Methoden bietet die Übertragung pathogener oder tödlicher Erreger beziehungsweise Wirkstoffe durch gentechnisch modifizierte Nahrungsmittel und Mikroorganismen als Ausbreitungsmedien (Vektoren). Weiterhin gibt es experimentelle Hinweise darauf, daß Immunreaktionen gegen Krankheitserreger – möglicherweise auch gegen das für den Menschen tödliche Pockenvirus *Variola vera* – gentechnisch unterdrückt werden können. So erwägt man etwa in verschiedenen westlichen Ländern, darunter auch in Deutschland, nach langen Jahren der Unterbrechung im Bedarfsfall in mehr oder weniger begrenztem Umfang wieder zur Pockenschutzimpfung zurückzukehren. Die Maßnahmen sind zum Schutz vor einem terroristischen Angriff gedacht, bei dem das hoch ansteckende, oft tödlich wirkende Variola-Virus freigesetzt wird. Es sind jedoch auch Angriffe mit genetisch veränderten Pockenviren denkbar, die möglicherweise den Impfschutz durchbrechen. Über Experimente mit geeigneten Virusarten oder gar über die gezielte Virus-Herstellung gibt es nur Vermutungen, doch gelten die hierzu notwendigen experimentellen Verfahren heute als Standardtechnologie.

*Miniaturisierung*

Unter Miniaturisierung versteht man die Entwicklung immer kleinerer Bauteile und Geräte bei gleich bleibender oder sogar steigender technischer Leistung.

[20] Zur Diskussion um gleichermaßen offensiv wie defensiv nutzbare gentechnische Produkte siehe Victor W. Sidel, *Defense against Biological Weapons: Can Immunization and Secondary Prevention Succeed?*, in Susan Wright (ed.), *Biological Warfare and Disarmament: New Problems/New Perspectives* (Lanham, MD: Rowan and Littlefield, 2002), S. 81.

Kleine, leistungsfähige Geräte sind meist leichter und oft auch leichter handhabbar, energiesparend und billiger – wenn nicht in der Anschaffung, so doch im Betrieb. Für die militärische Waffen- und Gerätetechnik bedeutet Miniaturisierung daher meist eine beträchtliche Verbesserung unter den Gesichtspunkten der Waffen- wie auch der Kostenwirksamkeit.

Als Beispiel sei an die jahrzehntelange, fortschreitende Miniaturisierung elektronischer Bauteile in der Informationstechnik erinnert. Sie hat nicht nur ungeahnte Speicherkapazitäten und Rechnerleistungen bei Computerchips und PCs im Vergleich zu den herkömmlichen Großrechnern bewirkt, sondern die gesamte zivile wie militärische Kommunikation, Datenverarbeitung, Sensorik und Aufklärung, Satellitennavigation und Systemsteuerung revolutioniert. Im Zusammenwirken mit der Nanotechnologie werden diese Trends auf absehbare Zeit verlängert und intensiviert.

Auch die (sicherheits-)politischen und sozialen Folgen der Biotechnologie sind unter dem Gesichtspunkt der fortschreitenden Miniaturisierung biotechnischer Verfahren und Produkte zu beurteilen. Dies gilt im gleichen Maße für gentechnische Produkte wie für ihre industrielle Herstellung, ihre Ausbreitung, einschließlich Transport und Vermarktung und ihre (militärische, zivile, kommerzielle, terroristische usw.) Verwendung.[21] Für den Biowaffengebrauch sind insbesondere folgende mikrobiologischen Produkte, Eigenschaften und Verfahren wesentlich:

- Massenproduktion von gentechnisch veränderten, schädlichen Mikroorganismen
- Gentechnische Produkte, die biochemische (toxische, letale, nicht-letale usw.) Wirkungen erzeugen, verstärken oder blockieren
- Verseuchung von Umwelt und Nahrungsketten mit Pathogenen und Schadstoffen, die wegen ihrer mikroskopischen Eigenschaften nur schwer zu entdecken und zu identifizieren sind
- Verbreitung schädlicher Mikroorganismen durch Aerosole und durch Ansteckung mit Seuchen (Truppen, Zivilbevölkerung)

[21] A. Paul Alivisatos, „Nanopartikel im Kampf gegen Krankheiten“, *Spektrum der Wissenschaft–Spezial*, 2 (2001), S. 56-63; Madeline *Drexler, Secret Agents: The Menace of Emerging Infections* (Washington, DC: Joseph Henry Press, 2002).

*Hochtechnologie als handelsübliche Massenware*

Viele heute bereits verfügbare Dual Use-Produkte setzen anspruchsvolles technisches Wissen voraus und erfordern, wie beispielsweise Computerchips, komplizierte Herstellungsverfahren. Dennoch gelten sie als handelsübliche Massenware, die auf den Märkten öffentlich und frei erworben und von jedem, auch Nichtexperten, zu beliebigen Zwecken genutzt werden kann. Selbst wenn Produkte dieser Art nur in Hochtechnologieländern hergestellt werden (können), sind sie doch in aller Regel weltweit verbreitet und werden ebenso global genutzt. Alles deutet darauf hin, daß sich nicht nur die Informations-, sondern auch Nano- und Biotechnologie nur in dem Maße entwickeln werden, in dem sie mittelbar oder unmittelbar zur Produktion von Massengütern führen.

*Gekoppelte Trends*

Technologische Trends weisen heute in aller Regel enge ursächliche Wechselbeziehungen auf. Computer und Datenverarbeitung haben die Nanotechnologie überhaupt erst möglich gemacht, die ihrerseits der Informationselektronik neue, enorme Entwicklungsspielräume eröffnet. Entsprechendes gilt für die zahlreichen, oben skizzierten zivilen und militärischen Folgen und Anwendungen der Nano- und Informationstechnologie.

Auch die moderne Biotechnologie ist in vielerlei Beziehungen das Produkt einer sehr leistungsfähigen Informationsverarbeitung, insbesondere die Bioinformatik, die computergestützte experimentelle und industrielle Prozesssteuerung, die softwaregestützte biochemische Stoffanalyse und die automatisierte Sequenzierung des Genoms,[22] besonders spektakulär die des Humangenoms durch Craig Venter in den Jahren 2000/01.

Die Wechselbeziehungen zwischen informations- und biotechnologischen Entwicklungen sind von besonderem sicherheitspolitischem Interesse. Denn auch bei ihnen zeigen sich die defensive und offensive Nutzung technologischer Trends als Kehrseiten ein und derselben Medaille. Der Schutz vor biologischen Massenvernichtungswaffen verlangt eine leistungsfähige Bioinformatik von der gleichen Art, wie sie heute das exakte Verständnis von Infektionskrankheiten (Art, Erreger, Ausbreitungsmechanismen usw.) erfordert. Die Aufgabe, schädliche Erreger und Wirkstoffe möglichst früh zu erkennen und zu analysieren, stellt

[22] J. Craig Venter, „High-Throughput Sequencing, Information Generation and the Future of Biology“, in Scott P. Layne, Tony J. Beugelsdijk and C. Kumar N. Patel (eds.), *Firepower in the Lab: Automation in the Fight against Infectious Diseases and Bioterrorism* (Washington, DC: National Academies Press, 2001), S. 261-266.

extreme Anforderungen an die Verarbeitung großer Datenmengen und an die automatisierte Labortechnik. Umgekehrt kann die gleiche Computer- und Labortechnik zur massenhaften Vermehrung pathogener Mikroorganismen und Toxine eingesetzt werden, zur Computersimulation ihrer Ausbreitungswege oder auch zur Abschätzung der Folgen eines geplanten Biowaffenangriffs.

*Potentiale statt Arsenale*

Die Möglichkeit einer Massenproduktion von Biowaffen mittels einer leistungsfähigen, digitalisierten Labortechnik macht herkömmliche große und auffällige Fabrikationsanlagen in Zukunft überflüssig. Ebenso erübrigt sich die massenhafte Lagerung biologischer Kampfstoffe. Zur offensiven Nutzung der Biotechnologie genügt zunehmend das Bereithalten von Produktionspotentialen – von technischem Wissen und unverfänglicher Dual Use-Ausrüstung. Die tatsächliche Waffenproduktion kann dann kurzfristig und nach Bedarf erfolgen.

## Internationale Sicherheit

*Militärische Rüstung und Kriegführung*

Die fortschreitende Miniaturisierung technischer Systeme und ihrer Bauteile hat für die militärische Waffen- und Gerätetechnik ebenso wie für Rüstungskontrolle weitreichende Folgen (Tabelle 1). Mikrotechnologien – allen voran die digitale Informationstechnik – haben bereits in den beiden vergangenen Jahrzehnten eine Revolution des Militärwesens bewirkt. Für moderne Streitkräfte wird diese Revolution kein zeitlich begrenzter Umwälzungsprozess bleiben. Die hier untersuchten Trendmerkmale moderner Nano- und Biotechnologien deuten vielmehr darauf hin, daß der rasche, tief greifende technische Wandel für die Streitkräfte ein Dauerzustand bleiben wird. Seine Auswirkungen erstrecken sich gleichermaßen auf Bewaffnung, Führungs-, Nachrichten-, Aufklärungs- und Transportsysteme und natürlich auch auf die zivilen, technisch-wirtschaftlichen Rahmenbedingungen der Rüstungsplanung beziehungsweise des Streitkräfteeinsatzes (Tabelle 2).

1. *Technologien des Informationskriegs:* Computer, Datenverarbeitung und elektronische Netze, die teilstreitkräfteübergreifende Operationen schneller und wirksamer machen.
2. *Raketenabwehr:* Während früher feindliche Raketen nur mit nuklearen Sprengköpfen zerstört werden konnten, gestatten neue Technologien das Abfangen von Geschossen mit rein kinetischem Energieaufwand.
3. *Robotik:* Heute nutzen die US-Streitkräfte unbemannte Flugkörper (Drohnen) zur luftgestützten Aufklärung. In Zukunft werden Luftwaffeneinsätze, langfristig auch der Waffeneinsatz am Boden und zur See mit ferngesteuerten Robotern möglich sein.
4. *Tarnkappen-Technologie:* Bereits heute besitzen Mehrzweck-Kampfflugzeuge und Jagdflugzeuge wie F-22 und F/A-18E/F neben einer niedrigen Radarsignatur hoch entwickelte Flugeigenschaften und Nutzlastkapazitäten.
5. *Technologien der Landkriegführung:* Die Digitalisierung begünstigt leichtere, schnellere, wendigere Panzer und Fahrzeuge mit höherer taktischer Mobilität und Feuerkraft.
6. *Neue Schiffstypen der Kriegsmarine:* Neue Antriebstechnik, Bewaffnung und elektronische Systeme.
7. *Hochintelligente Waffen:* Gestützt auf Trägheitsnavigationssysteme, Satellitendaten und Zielsuchsysteme, wird die nächste Generation intelligenter Geschosse und Bomben größere Treffsicherheit und Waffenwirksamkeit besitzen.
8. *Abstandsfähigkeit und Präzisionswaffen für die Abstandsverteidigung*.

Die Basistechnologien Information und Kommunikation, Materialien, Optoelektronik und Energieversorgung werden zunehmend auf Nanobasis zur Verfügung gestellt. Aus Kostengründen dürften nicht alle der aufgelisteten Verwendungen für europäische Streitkräfte in Frage kommen.

Tabelle 1: Mittelfristig verfügbare militärische Nutzungsmöglichkeiten für intelligente Hochtechnologie aus Sicht des US-Verteidigungsministeriums

Quelle: Hans Binnendijk and Richard L. Kugler, *Managing Change: Capability, Adaptability, and Transformation* (Washington, DC: Center for Technology and National Security Polics, National Defense University, 2001), S. 5.

1. *Hochleistungs-Trägersysteme* (Flugzeuge, Schiffe, U-Boote und Satelliten) aufgrund stärkerer, leichterer, wartungsarmer und „intelligenter" Materialien mit niedriger Radarsignatur.
2. *Verbesserte Sensorik* aufgrund empfindlicherer und trennscharfer Sensoren für elektromagnetische und nukleare Strahlung sowie chemisch-biologische Wirkstoffe. Miniaturisierte, hoch mobile funkgestützte Systeme zur abstandsfähigen Gefechtsfeldüberwachung.
3. *Erhöhte menschliche Leistungsfähigkeit* durch verbesserte Überwachungssysteme einschließlich der Messung physiologischer Zustände der Soldaten.
4. *Informationsdominanz* durch leistungsfähigere Informationstechnologie. Kleinere elektronische Speicher mit niedriger Betriebsspannung, kleinere und schnellere Schaltelemente durch bessere Prozessoren, sichere Kommunikationssysteme mit größerer Bandbreite.
5. *Ferngesteuerte Roboter* zur Lösung gefährlicher Aufgaben.
6. *Fortschreitende Automatisierung* bei Instandhaltung, Steuerung und Management von Waffen- und Trägersystemen.
7. *Verbesserte Sanitätsversorgung* auf dem Gefechtsfeld durch Verwendung biokompatibler Materialien und nanotechnischer Verfahren.
8. *Sanierung* chemisch oder biologisch verseuchter Gefechtsfelder durch nanochemische Reinigungsmittel und Verfahren.
9. *Niedrigere Kosten* pro Produkt-Lebenszyklus durch nanotechnische und nanobeschichtete Materialien und zustandsabhängige Wartung.

Viele dieser militärischen Verwendungen liegen im Rahmen herkömmlicher europäischer Rüstungsprogramme.

Tabelle 2: Militärische Nutzungsmöglichkeiten der Nanotechnologie

Quelle: W. M. Tolles, „National Security Aspects of Nanotechnology", in National Science Foundation (ed.), *Societal Implications of Nanoscience and Nanotechnology* (Washington, DC: National Science Foundation, 2001), S. 173-187.

Ein Großteil der sicherheitspolitischen Problematik moderner Technologien liegt weiterhin darin, daß sie – ähnlich der digitalen Vernetzung – gleichermaßen zur militärischen Stärke wie zur Verwundbarkeit eines Landes beitragen können. Sieht man von sehr speziellen sicherheitstechnischen Entwicklungen wie der Quantenkryptographie ab, wird die Nanotechnologie diese zwie-

spältige Situation auf die Dauer eher verschärfen denn beseitigen. Dual Use-Eigenschaften, Massenproduktion und globale Verbreitung geben potentiellen Akteuren – ob Staaten, Armeen, nicht-staatliche Akteure (inkl. Terrorgruppen) – zu jedem beliebigen offensiven oder defensiven Zweck die neueste und wirksamste Hochtechnologie an die Hand. Die fortschreitende Miniaturisierung der Gerätetechnik erlaubt immer kleinere, leichtere, einfach zu handhabende und leicht zu tarnende Wirkmittel, Trägersysteme und Sensoren (z.B. Satelliten, Aufklärungsdrohnen) mit automatisierter Fernsteuerung (z.B. kleine, leichte, aber hochwirksame, präzisionsgesteuerte Lenkwaffen). Technologien mit diesen Eigenschaften ermöglichen Angriffsszenarien, für die es keine Frühwarnung gibt und bei denen jeder Versuch der Abschreckung versagen muss, weil der Täter weiß, daß er mit an Sicherheit grenzender Wahrscheinlichkeit unerkannt bleibt. Militärische oder auch terroristische Angriffe werden damit in bisher unbekanntem Maße distanz- und eindringfähig gegenüber Territorien und politisch-gesellschaftlichen Infrastrukturen.

Diese Schlussfolgerungen treffen in vielerlei Hinsicht bereits auf den offensiven Informationskrieg zu und gewinnen mit fortschreitender Nanotechnologie weiter an sicherheitspolitischer Bedeutung. Auch auf die Waffenwirksamkeit moderner Biotechnologien lassen sie sich direkt übertragen. Die Analogien beruhen auf den Dual Use-Eigenschaften, den Trends zur Miniaturisierung und zu verdeckten, aber jederzeit und kurzfristig zu aktivierenden biotechnischen Rüstungspotentialen.

Verglichen mit nuklearen und chemischen Massenvernichtungswaffen sind biologische Waffen in ihrer Vielfalt und damit in der Vielfalt ihrer Wirkungsweisen einzigartig. Durch gentechnische Veränderungen kann diese Vielfalt noch weiter gesteigert werden. Bereits viele der herkömmlichen Biowaffen sind im Vergleich zu Nuklear- und Chemiewaffen leichter herzustellen und anzuwenden, während die hierzu notwendigen modernen gentechnischen Dual Use-Verfahren, Laborgeräte und Produkte inzwischen als Standardtechnologien gelten.

Die Unterschiede zwischen den zahlreiche Pathogenen und Biotoxinen, die sich zum Waffeneinsatz eignen, werden von den Eigenschaften jedes einzelnen Erregers und Schadstoffproduzenten bestimmt, seiner Virulenz, Lebensdauer nach der Freisetzung und natürlich auch von der Art der Krankheit, die er verursacht. Erreger können heimlich hergestellt und ausgebracht werden, sowohl über das Vergiften von Nahrungsketten als auch von Boden, Luft und Gewässern – ohne Vorwarnung und wirksame Abschreckung. Um ihre volle schädliche Wir-

kung zu entfalten, sind nicht viele akute Opfer erforderlich, etwa durch Einatmen von Aerosol. Zum Entfachen einer Seuche genügen wenige primäre Infektionen, sofern der Erreger nur hinreichend leicht übertragbar ist.[23]

*Asymmetrische Strategien*

In internationalen sicherheitspolitischen Konflikten sind auch wirtschaftlich-technisch-militärische Großmächte heute in dem Maße gefährdet, in dem ihre Zivilbevölkerung und Infrastrukturen mit Mitteln angegriffen werden können, die sich auf hochwirksame, aber allgemein verfügbare Mehrzweck-Technologien stützen. Gerade die am weitesten fortgeschrittenen Hochtechnologieländer sind mit einer völlig neuartigen, diffusen Sicherheitsproblematik konfrontiert, die selbst für eine Großmacht wie die USA mit militärischen Mitteln allein nicht zu lösen ist. Man spricht von „asymmetrischer" Kriegführung in Bezug auf den Versuch, einem militärisch überlegenen Konfliktgegner durch einen Angriff auf die Zivilbevölkerung oder auf seine technisch-wirtschaftliche Infrastruktur die militärische oder politische Handlungsfähigkeit zu rauben.

Asymmetrische Strategien zielen somit auf die Verwundbarkeit der Hochtechnologie-Gesellschaft. Die Asymmetrie beruht auf einer ungleichen Gewichtsverteilung zwischen Angriffs- und Verteidigungsaufwand sowie zwischen Aufwand und Ertrag für den Angreifer. Asymmetrische Angriffe (Ort, Zeitpunkt, Mittel) sind ganz in das Ermessen des Angreifers gestellt, während der Verteidiger seine gesamte Infrastruktur unablässig schützen muss. Sie sind in dem Sinne „preisgünstiger" und selbst für einen unterlegenen Konfliktgegner „erschwinglich", als sie deutlich weniger Aufwand erfordern als ihre Prävention und Abwehr. Angriffe vom Typ des Informationskriegs sind in diesem Sinne asymmetrisch,[24] desgleichen der Einsatz bestimmter Biowaffen. So war etwa die Herstellung von Milzbranderregern und ihres hochgiftigen Wirkstoffs (Anthrax) bereits verschiedentlich Gegenstand der gentechnischen B-Waffenforschung. Beispiele wie die des Informationskriegs und der biotechnisch erzeugten Massenvernichtungswaffen stützen die Vermutung, daß in künftigen internationalen

[23] Ken Alibek, „Biological Weapons: Past, Present, and Future", in Scott P. Layne, Tony J. Beugelsdijk and C. Kumar N. Patel (eds.), *Firepower in the Lab: Automation in the Fight against Infectious Diseases and Bioterrorism* (Washington, DC: National Academies Press, 2001), S. 177.

[24] Gebhard Geiger, *Offensive Informationskriegführung – Die „Joint Doctrine for Information Operations" der US-Streitkräfte: sicherheitspolitische Perspektiven* (Berlin: Stiftung Wissenschaft und Politik, 2002), S. 12-13.

Konflikten die Erfolgschancen asymmetrischer Strategien durch die hier untersuchten technologischen Trends begünstigt werden.

*Terrorismus*

Aufgrund ihrer enormen Leistungspotentiale bei gleichzeitig leichter Handhabbarkeit und unauffälligem, perfekt zu tarnendem Einsatz eignen sich die hier untersuchten neuen Mikrotechnologien besonders für terroristische Angriffe. Erschwerend kommt hinzu, daß bei Angriffen mit nanotechnischer Waffenwirkung eine Frühwarnung beziehungsweise Abschreckung zunehmend unmöglich wird. Selbstmordattentäter abzuschrecken ist ohnehin praktisch unmöglich, sofern sie etwa – mit hoch ansteckenden Erregern infiziert – eine Seuche auszulösen versuchen. Mit Angriffen vom Typ des Informationskriegs lassen sich im Erfolgsfall elektronisch vernetzte Bereiche des öffentlichen Lebens lähmen. Zur Störung des öffentlichen Lebens treten beim terroristischen Einsatz chemischer und biologischer Waffen der Schrecken der Zivilbevölkerung sowie die Öffentlichkeitswirkung der Medienberichte hinzu, die in ihren sicherheitspolitischen Auswirkungen kaum mehr sinnvoll abzuschätzen sind.

Andererseits können moderne nano- und biotechnische Verfahren und Produkte vieles zur Entdeckung und Abwehr akuter terroristischer Bedrohungen leisten. Zahlreiche Anwendungen bieten sich an, von Technologien zur kriminalistischen Täteridentifikation und -verfolgung, Satellitensensorik und -überwachung bis hin zur elektronischen Datenerfassung und -analyse. Die Aufgaben der inneren und der äußeren Sicherheit eines Staates überlagern sich hier in dem Maße, in dem zu ihrer Lösung von modernen Mehrzweck-Technologien Gebrauch gemacht wird.

*Nicht-letale Waffen*

Im modernen Streitkräfteeinsatz tritt der klassische Kriegsfall zunehmend hinter Aufgaben der Konfliktverhütung, Krisenprävention und der möglichst gewaltfreien Beendigung von Bürgerkriegen zurück. Zur Lösung dieser Aufgaben wird zunehmend der Einsatz von Waffen erwogen, die zwar abschreckend, im Allgemeinen jedoch nicht tödlich wirken. Das prekäre Gleichgewicht zwischen Waffenwirksamkeit und deren Begrenzung ist nicht zuletzt eine technische Aufgabe.[25] Materialien mit neuen Eigenschaften auf nanotechnologischer Basis sowie chemische Kampfstoffe, die im Bedarfsfall betäubend wirken, sonst aber bei

[25] E. R. Bedard, *Nonlethal Capabilities: Realizing the Opportunities* (Washington, DC: Center for Technology and National Security Policy, National Defense University, 2002).

Mensch und Umwelt keine dauerhaften Schäden verursachen, kommen hierfür als Lösung in Frage, sofern sie nicht unter das Chemiewaffenverbot fallen. Die Befreiung der Moskauer Geiseln aus der Hand tschetschenischer Rebellen, bei der im Oktober 2002 die falsche Dosierung eines Betäubungsgases über 100 Todesopfer gefordert hat, unterstreicht die Dringlichkeit des Bedarfs. Allerdings sind geeignete Dual Use-Lösungen für diese Art nicht-letaler Wirkstoffe anscheinend noch nicht für alle zukünftigen realistischen Einsatzszenarien verfügbar.

*Rüstungskontrolle und Vertragsverifikation*

Moderne Technologien auf mikrophysikalischen und gentechnischen Grundlagen erschweren die verifikationsgestützte Rüstungskontrolle in ihren wesentlichen Elementen. Mit dieser These verbindet sich der Anspruch, daß Vertragsverifikation wesentlich mehr sein muss als nur gut gemeint,[26] und mehr leisten muss als Datenaustausch und Vertrauensbildung. Sie muss diese Leistungen auch möglichst unzweideutig und fälschungssicher erbringen können, und zwar durch Überprüfung technischer und anderer sicherheitspolitisch relevanter Sachverhalte. Wo dies nach Lage der Dinge nicht möglich ist, stößt jeder noch so sinnvolle Rüstungskontrollansatz an prinzipielle Grenzen.

Bei Rüstungsgütern mit ausgeprägten Mehrzweck-Eigenschaften ist diese Grenze schnell erreicht. Ob beispielsweise eine auf dem Markt frei verfügbare kryptographische Software eine Offensivwaffe im Informationskrieg ist oder ein legitimes, legales und überdies absolut notwendiges (!) Mittel des Datenschutzes, hängt einzig und allein von der Gebrauchsabsicht des Nutzers ab. Internationale kriegsrechtliche Vorschriften lassen sich daher extrem schwer auf den offensiven Informationskrieg anwenden, von einer Verifikation von Sachverhalten des Computermißbrauchs ganz zu schweigen. Diese Situation würde sich beim Versuch einer „Rüstungskontrolle im Cyberspace“ in bezug auf ein geeignetes Verifikationsregime noch erheblich verschärfen. Entsprechendes gilt für das längst angebahnte Zusammenwachsen von Informations- und Nanotechnologie, aber auch für militärische Verwendungen nanotechnischer Werkstoffe, optoelektronischer Geräte und ihrer Herstellungsverfahren. Neben ihrem Mehrzweck-Charakter sind es vor allem die oben dargestellten Trends und Technik-

[26] Alan P. Zelikoff, „An Impractical Protocol”, *Arms Control Today* 31:4 (May 2001), S. 27-31. Siehe z.B. auch die Konzeptionen einer „Rüstungskontrolle im Cyberspace“, denen es an allen vernünftigen, realistischen und praktikablen Voraussetzungen mangelt. Hierzu weiterführend: Geiger, *Offensive Informationskriegführung*.

folgen, die es kaum mehr gestatten, mögliche Waffenverwendungen moderner Mikro- und Nanotechnologien selbst bei internationalen Kontrollen vom Typ der Vor-Ort-Inspektionen ausreichend zu überprüfen.

**Verhältnis von innerer zu äußerer Sicherheit eines Staates**

Es stellt sich die Frage, wie ein Staat die Missbrauchsabsichten eines Angreifers feststellen und gegebenenfalls verhindern kann, der sich auf massenwirksame Dual Use-Hochtechnologie stützt, beispielsweise zu erpresserischen (terroristischen) Zwecken genetisch veränderte pathogene Organismen freisetzt. Die Frage berührt das sicherheitspolitisch zentrale Problem, politisch motivierte von kriminellen Handlungen, organisierte Handlungsweisen von Aktionen einzelner Täter unterscheiden zu können, um angemessen, das heißt, entweder mit den Mitteln der Landesverteidigung oder der Strafverfolgung zu reagieren. Da die Unterscheidung in der Praxis grundsätzlich schwierig, wenn nicht gar unmöglich ist, werden in der Fachwelt zunehmend umfangreiche Kooperationsprogramme zwischen Justiz, Verteidigung, Nachrichtendiensten und Zivilschutz zur Bekämpfung von Angriffen – welcher Organisationsstufe und Absicht auch immer – gefordert. Die großen Schadenspotentiale moderner Hochtechnologiewaffen, die zu ihrem Einsatz gegebenenfalls keiner militärischen Organisation mehr bedürfen, machen darüber hinaus eine wirksame Koordinierung von Zivil- und Katastrophenschutz notwendig. Besondere technische Aufgabengebiete sind im Bereich der verschränkten inneren und äußeren Sicherheit von Staaten und Bündnissen:

- Zivile und militärische Überwachung und Aufklärung (Sensorik, elektronische Datenauswertung, Alarmsysteme, Notfallkommunikation)
- Zivile und militärische Aufgaben der Grenzsicherung und Grenzkontrollen (elektronische Sensorik, satellitengestützte Systeme u.a.)
- Zivile und militärische Aufgaben der Materialkontrolle (z. B. nukleare und radiologische Materialien) und Exportkontrolle

**Sicherheitspolitisches und sicherheitstechnisches Forschungsprogramm der EU**

Zusätzlich zum laufenden 6. Rahmenprogramm der EU-Forschungsförderung finanziert die Europäische Kommission seit 2004 ein eigenes sicherheitspolitisches Programm, in dem die angewandte (d.h. industrielle) technologische Si-

cherheitsforschung eine zentrale Rolle spielt.[27] Darüber hinaus soll die Sicherheitsforschung im künftigen 7. Rahmenprogramm ein Schwerpunktgebiet bilden. Bei ihren Beschlüssen geht die EU-Kommission davon aus, daß Sicherheitsforschung in der europäischen Forschungsförderung bisher zu wenig berücksichtigt wurde, in Zukunft aber nicht länger vernachlässigt werden darf. Darüber hinaus soll die künftige EU-Forschungsförderung die „künstliche Unterscheidung" von ziviler und militärischer Nutzung aufgeben, die den Dual Use-Charakter moderner Technologien ignoriert und daher deren Entwicklung hemmt – zu Lasten der europäischen Sicherheit und zum Schaden der europäischen Industrie und Wirtschaft.

Mit dieser Kehrtwende bei der seit Jahrzehnten praktizierten Forschungspolitik beginnt die EU-Kommission, den hier skizzierten wissenschaftlich-technischen Langfristentwicklungen und ihrer sicherheitspolitischen Bedeutung Rechnung zu tragen. Soweit die neuen Programmschwerpunkte bereits erkennbar sind, zielt die künftige EU-Forschungsförderung allerdings zunächst auf industrielle Entwicklungen wie weltraumgestützte Navigations-, Kommunikations- und Überwachungssysteme sowie informationstechnisch vernetzte Systeme der Sicherheitspolitik. Im Interesse langfristiger, tragfähiger Entwicklungen muss das 7. Rahmenprogramm daher die systematische Verknüpfung von wissenschaftlichen Basistechnologien (Mikrosysteme, Biotechnik u. a.) mit den sicherheitspolitischen Anwendungen verstärkt fördern und herbeiführen. Hierzu kann nicht zuletzt die Hochschulforschung wesentlich beitragen, die im neuen Sicherheitsforschungsprogramm der EU neben der industriellen Forschung und Entwicklung anscheinend noch nicht angemessen berücksichtigt wird. So sieht etwa die EU-Projektförderung im Rahmen der Preparatory Action 2004-2006 überhaupt keinen Beitrag der Hochschulforschung vor – im Gegensatz zu den ehrgeizigen und wissenschaftlich anspruchsvollen Programmen in den USA (beispielsweise der National Nanotechnology Initiative[28]). Sicherheit als vernetztes Aufgabengebiet erfordert auch die Vernetzung der zuständigen – wissenschaftlichen wie außerwissenschaftlichen – Einrichtungen und erst recht der damit verbundenen Forschungs- und Entwicklungsbereiche.

[27] Siehe hierzu auch den Beitrag von Thomas Pankratz und Alfred Vogel in diesem Band.
[28] <http://www.nano.gov/> (Zugriff: 20. Juli 2004).

**Schluss**

Die dargestellten technologischen Trends tragen zu neuartigen, erheblichen Gefährdungen der internationalen Sicherheit bei. Durch eine extrem gesteigerte Wirksamkeit bei gleichzeitiger ziviler, kommerzieller Verbreitung erschließen sie auch nicht-staatliche Akteure ein beträchtliches Gewaltpotential. Rüstungskontrollpolitisch ist dieses Potential kaum mehr sinnvoll zu erfassen. Offensive und defensive Rüstungsziele sind praktisch nicht mehr voneinander zu unterscheiden. Selbst Massenvernichtungswaffen können auf Dual Use-Basis unter weitgehender Geheimhaltung entwickelt, getestet und schließlich auch angewandt werden.

In dieser Lage benötigen Hochtechnologieländer eine leistungsfähige Forschung und Entwicklung auf den Innovationsgebieten der Nano-, Informations- und Biotechnologie. Herkömmliche wissenschaftlich-technische Bereiche wie Luft- und Raumfahrt, Sensorik, Material- und Fertigungstechnik werden von der Grundlagenforschung ebenfalls profitieren. Nur wenn die europäischen Länder die neuen Technologien selbst mitentwickeln und beherrschen lernen, können sie auch deren sicherheitspolitischen Herausforderungen erfolgreich begegnen.

Ralph Thiele

# Transformation und die Notwendigkeit der systemischen Gesamtbetrachtung

## Komplexität und Transformation

Sollte man in ein Wort fassen, was die sicherheitspolitische Lage heute von der Zeit des Kalten Krieges fundamental unterscheidet, so ist es Komplexität. Mit dem Wandel vom Industrie- zum Informationszeitalter finden sich Deutschland, Europa und die Mehrzahl unserer Partner in der Welt eingebunden in ein globales Netzwerk von Herausforderungen für unsere Sicherheit. Terrorismus und Proliferation von Massenvernichtungswaffen, scheiternde Staatsautorität und die sukzessive globale Vernetzung unserer Sicherheit, eine unübersichtliche Qualität und Quantität von Akteuren und Risiken – die Liste ist lang. Nano- und Biotechnologien, die absehbaren Fortschritte in Miniaturisierung, Robotik und Sensorik verleihen den bereits erkennbaren Risiken zusätzliche Brisanz und öffnen die Tür für ganz neue Risikokategorien.[29] Die Felder der inneren und äußeren Sicherheit, der Wirtschaft und der sozialen Weiterentwicklung verbinden sich zunehmend. Dabei entstehen zwangsläufig wachsende Überlappungsflächen, die von staatlicher und suprastaatlicher Autorität nicht hinreichend abgedeckt werden und in denen Terrorismus und grenzüberschreitende organisierte Kriminalität Fuß fassen. Das Ausmaß an Gefährdung der Funktionsfähigkeit unserer Gesellschaften, deren Prosperität und sogar Existenz ist ohne geschichtliches Vorbild.

Mit den sicherheitspolitischen Anforderungen und den Möglichkeiten moderner Informations- und Kommunikationstechnologien können und müssen sich die sicherheitspolitischen und damit auch die militärischen Konzepte wandeln. Die in Deutschland eingeleitete Transformation will überzeugende Antworten auf die Herausforderungen von heute und morgen entwickeln. Multinationale Sicherheitsvorsorge ist ein grundlegendes Prinzip deutscher Sicherheits- und Verteidigungspolitik. Der Schutz Deutschlands und seiner Bürgerinnen und Bürger lässt sich nur in engem Zusammenwirken mit der Gemeinschaft unserer internationalen Freunde, Partner und Verbündeten sicherstellen, im Rahmen der Sicherheitsarchitektur aus Vereinten Nationen, NATO, Europäischer Union und

[29] Siehe hierzu den Beitrag von Gebhard Geiger in diesem Band.

der Organisation für Sicherheit und Zusammenarbeit in Europa. Damit liegt es im Interesse Deutschlands, sowohl den Transformationsprozess der NATO als auch entsprechende Entwicklungen der Europäischen Union mitzugestalten.

Bei der Transformation der Bundeswehr geht es in den Worten des Generalinspekteurs der Bundeswehr, General Wolfgang Schneiderhan, um die „Umwandlung von etwas Bestehendem in etwas Neues". Die Bundeswehr ist in allen Planungskategorien an ein neues, erweitertes Aufgabenspektrum anzupassen, begleitet von einem signifikanten Sprung in ihrer Wirksamkeit. Der Transformationskurs ist konsequent auf eine verbesserte Einsatzfähigkeit der Bundeswehr in den wahrscheinlichen Einsätzen ausgerichtet: Konfliktverhütung und Krisenbewältigung, einschließlich des Kampfes gegen den internationalen Terrorismus. Dies dient zugleich dem Schutz Deutschlands und seiner Bürgerinnen und Bürger. Hierzu sind Aufgaben, Fähigkeiten und die Ausrüstung mit den verfügbaren Finanzmitteln in eine Balance zu bringen.

Die Transformation der Bundeswehr ist als ein fortlaufender, vorausschauender Weiterentwicklungsprozess konzipiert. Mit hoher Dynamik soll die Bundeswehr auf die anspruchsvollen Einsatzerfordernisse in Doktrin und Struktur, Ausbildung und Ausrüstung, Führung, Personal und Infrastruktur an sich ändernde Rahmenbedingungen angepasst werden. Zugleich soll sie konzeptionell auf die hieraus resultierenden Herausforderungen vorbereitet und durch eine wirksame, leistungsfähige aufbau- und ablauforganisatorische Struktur getragen werden. Die Fähigkeiten der Bundeswehr als Ganzes ergeben sich künftig nicht mehr schlicht als Summe der Fähigkeiten einzelner Teilstreitkräfte oder Organisationsbereiche, sondern vielmehr als Ergebnis vernetzter Fähigkeiten und Synergien – auch im multinationalen Kontext.

Methodisch umgesetzt wird dieser Prozess durch Konzeptentwicklung und Experimentierung (Concept Development and Experimentation, CD&E). Die Transformationsprozesse der Bundeswehr sind dabei nachhaltig und hinsichtlich der Zielerreichung jederzeit transparent und bewertbar auszugestalten. Mit Blick auf Organisation und Ausrüstung, Ausbildung und Einsatz kommen sowohl der Fähigkeit zur schnellen Entwicklung relevanter Konzepte als auch den unterstützenden Simulationssystemen besondere Bedeutung zu. Sie gestatten eine zweckmäßige Komplexitätsreduktion mit dem Ergebnis überlegener Entscheidungs- und Führungsprozesse und nicht zuletzt ebenfalls überlegener Wirkung im Einsatz.

**Vernetzte, wirkungsorientierte Operationsführung**

In militärischen Auseinandersetzungen gewinnt diejenige Streitkraft, die unter komplexen Rahmenbedingungen ihre Machtmittel am wirkungsvollsten zum Einsatz bringen kann. Die hergebrachte Fokussierung auf Massierung und Feuerkraft ist kein zukunftsweisendes Rezept gegen die veränderten Risiken, insbesondere nicht gegen Akteure, die mit ihrem Streben nach Großschadensereignissen unsere Sicherheit bedrohen. Taktgeber für einen militärischen Erfolg sind künftig eher Faktoren wie Information und Wissen, Flexibilität und Mobilität, Integration und Vernetzung. Die Fähigkeit zur vernetzten Operationsführung (NetOpFü) ist damit ein Kernelement der Transformation.

Vernetzte Operationsführung zielt auf die Fähigkeit zu schnellen, flexiblen und präzisen Einsätzen unter Anwendung möglichst geringer eigener Kräfte – auf dem Gefechtsfeld oder auch im Informationsraum. Verbesserte Führungsfähigkeit hat dabei eine zentrale Bedeutung. Führung ordnet und lenkt den Einsatz der eigenen Kräfte und Mittel hinsichtlich der politisch geforderten Wirkung. Deutlich beschleunigte Führungsprozesse gründen auf einem streitkräftegemeinsamen, ebenengerechten und aktuell aufbereiteten Lagebild (Common Relevant Operational Picture, CROP) sowie einer schnellen Entwicklung und Abstimmung der eigenen Handlungsoptionen. Netzwerkgestützt können Informationen in stetig steigender Qualität, Quantität und Aktualität gewonnen und sinnvoll genutzt werden. Die verzugsarme, unterbrechungsfreie und umfassende Informationsversorgung aller Beteiligten ist die Grundlage für vernetztes Planen und Handeln. Daraus resultiert Führungsüberlegenheit, die wiederum echtzeitnah, effizient und effektiv in auftragsgerechte Wirkungsüberlegenheit umgesetzt werden kann.

Bei der vernetzten Operationsführung werden Sensoren, Effektoren sowie Führungs- und Unterstützungselemente aller Ebenen über eine zweckmäßige Architektur systematisch in einem Netzwerk verbunden. Modularisierung, Standardisierung und leistungsfähige Informations- und Kommunikationstechnologien sind dabei von herausragender Bedeutung. Auf dieser Grundlage werden neue Informationsdienste, -strukturen und Organisationsformen denkbar, ebenso neue Einsatzdoktrinen und Ausbildungskonzepte. Verbände können kleiner, schneller, wendiger, modular und multifunktional sein. Sie können verteilt operieren und brauchen nicht mehr physisch, sondern nur noch in ihrer Wirkung massiert zu werden. Insbesondere ermöglicht die Vernetzung eine deutliche Reduzierung des Zeitbedarfs zwischen Zielerfassung, Identifizierung, Auswahl des

am besten geeigneten Wirkmittels, der Zielbekämpfung und der Ermittlung der Wirkung im Ziel.

Netzwerkgestützte Konzepte gibt es in Theorie und Praxis bereits schon weit über ein Jahrzehnt, in Streitkräften seit über sechs Jahren. Sie wurden von Militärs in der ganzen Welt einer kritischen Überprüfung unterzogen. Amerikanische und britische Streitkräfte konnten die Überlegenheit vernetzter Operationsführung im Kampfeinsatz unter Beweis stellen. Sie bewährte sich dort durchweg – bei allem Bedarf an Weiterentwicklung. Im Bereich von Stabilitätsoperationen wurden hingegen die deutlich erweiterten Möglichkeiten vernetzter Fähigkeiten bisher noch nicht erkennbar genutzt. Hier wird in den USA zurzeit eine Fülle neuer konzeptioneller Überlegungen auf den Weg gebracht.[30]

Mit vernetzter Operationsführung hängt wirkungsorientierte Operationsführung, die so genannten Effects Based Operations (EBO), eng zusammen. Neue Operationsformen erfordern neue Führungsprozesse. Simulationssysteme reduzieren die Planungskomplexität und unterstützen die Entscheidungsfindung. Sie machen die Planung transparent und unterstützen die Ausbildung der militärischen Führung. Die Geschwindigkeit der Führungsprozesse und die sofortige Verfügbarkeit aller relevanten Daten auf allen Führungsebenen und in den Waffensystemen verschaffen den operierenden Kräften einen erheblichen Zeitvorteil und den entscheidenden Informationsvorsprung. Hierdurch werden die Wirkung sowie die Überlebens-, Durchsetzungs- und Reaktionsfähigkeit erhöht. Die Nutzung des Raums im Sinne freier Operationen wird erleichtert, da verfügbare Informationen über Nachbarn und Feind stets „präsent" sind. Ein streitkräftegemeinsames, ebenengerechtes und aktuell aufbereitetes Lagebild, schnell aufwachsend und sofort „sichtbar", ermöglicht eine parallele, dynamisierte Planung und Kontrolle. Es bietet den Verbänden die Chance, den Gegner dort zu schlagen, wo ihn die „Sensoren" gerade entdecken.

Dies fordert und fördert die Bereitschaft, nach Auftrag zu handeln, erkannte Gelegenheiten zu nutzen und nicht erst auf das Ergebnis einer langen Befehlskette zu warten. Die gelegentlich von Kritikern beschworene Gefahr einer Automatisierung der Entscheidungsfindung oder des ständigen befehlstaktischen Durchgriffs von ganz oben nach ganz unten ist weder real noch plausibel. Vernetzte, wirkungsorientierte Operationsführung gewinnt über Dezentralisation und Auftragstaktik deutlich an Qualität, insbesondere hinsichtlich hoher Trans-

[30] Stabilitätsoperationen sind derzeit einer der Hauptuntersuchungsgegenstände in den Washingtoner Think Tanks.

aktionsraten und Operationsgeschwindigkeiten. Auf dieser Grundlage lässt sich Komplexität auf jeder Führungsebene beherrschen.

Unter EBO sind eine Reihe von militärischen und ressortübergreifenden Aktionen zu verstehen. Sie werden einheitlich geplant und durchgeführt und berücksichtigen alle physischen und verhaltensrelevanten Faktoren, die für die Erreichung von politischen wie auch militärischen strategischen und operativen Zielen erforderlich sind. Als ein neues Konzept der Kriegführung beschreiben EBO, wie militärische Fähigkeiten im integrierten Zusammenspiel mit den anderen Machtinstrumenten von Staaten und Bündnissen zur Anwendung gebracht werden sollen. Militärische Maßnahmen zielen dabei auf Wirkungen, die dazu beitragen, den politischen und militärischen Zusammenhalt des Gegners zu schwächen, seinen Kampfwillen zu brechen und seine Machtinstrumente zu neutralisieren.

Der Gegner wird aus einer Systemperspektive analysiert, bei der Schlüsselverbindungen und neuralgische Punkte identifiziert werden. Diese sollen dann mit den am besten geeigneten Mitteln beeinflusst werden. Operational Net Assessment (ONA) nutzt als Wissens-Synthesewerkzeug geheimdienstliche und militärische Nachrichtengewinnung, aber auch akademische und allgemein zugängliche Wissensquellen. Es sorgt für einen kontinuierlichen Wissensstrom und unterstützt die Entscheidungen des operativen militärischen Führers mit Blick auf die angestrebten Wirkungen im gegnerischen System. Es identifiziert Verbindungslinien und neuralgische Punkte, Aufgaben und Maßnahmen, die für die Erreichung dieser Wirkungen wichtig sind. Im multinationalen Verbund erleichtert ONA die Informationsteilhabe der Partner durch ein integriertes, abgesichertes Lagebild.

Auf dieser Informationsgrundlage erfolgt wirkungsorientierte Planung (Effects Based Planning). Sie organisiert Operationen im vernetzten Informationsumfeld. Als Wirkungen sind dabei jene Ergebnisse zu verstehen, die ein Staat oder ein Bündnis durch den Einsatz seiner Machtinstrumente – auch nichtstaatlicher Organisationen mit sicherheitspolitischer Relevanz – erzielen will. Diese Ergebnisse werden durch die Beeinflussung von neuralgischen Punkten mittels Aktionen im diplomatischen, informativen, militärischen und wirtschaftlichen Kontext erzielt. Den Aktionen werden Ressourcen zugeordnet, die in den Operationen die angestrebten Wirkungen erzielen sollen. Der militärische Führer auf operativer Ebene plant und führt die wirkungsorientierten Operationen aus einem Ständigen Gemeinsamen Führungsstab (Standing Joint Forces Headquarters, SJFHQ). Dieser Führungsstab plant Operationen, auch im virtuellen

Raum, zusammen mit externen Partnern, von denen sich manche in anderen Regionen oder Kontinenten befinden und auch von dort aus operieren. Zusammen bilden sie ein eingespieltes Team und setzen gemeinsame Planungen in wirkungsorientierte Operationen um.

Wirkungsorientierte Planung ist eine komplexe Herausforderung. Sie bedeutet die Integration vieler bislang unabhängiger Planungsarbeiten in ein koordiniertes, kohärentes, simulationsgestütztes Ganzes. Sie erweitert die Palette der rein militärischen Optionen, die einem Führer auf operativer Ebene zur Auswahl stehen, um die volle Bandbreite nationaler, internationaler und interinstitutioneller Fähigkeiten und gestattet ihm, schnell und wirkungsvoll zu reagieren, selbst wenn sich die Bedingungen außerordentlich rasch ändern. Die militärischen Maßnahmen können auf diese Weise streitkräftegemeinsam, ressortübergreifend, multinational und auch mit den nicht-militärischen Beteiligten weitaus besser abgestimmt werden als je zuvor.

Wirkungsorientierte Streitkräfte erzielen drei Schlüsselleistungen: Entscheidungsüberlegenheit, kohärente Wirkungen sowie streitkräftegemeinsame Einsätze und Unterstützung.

- *Entscheidungsüberlegenheit* kennzeichnet die Fähigkeit, aufgrund eines besseren Informationsstandes Entscheidungen schneller treffen und umsetzen zu können, als der Gegner reagieren kann. Der gesicherte Zugang zu Informationen ist von entscheidender Bedeutung. Auf der Grundlage von Informationsüberlegenheit und eines streitkräftegemeinsamen, auf den jeweiligen Entscheidungsbedarf zugeschnittenen Lagebildes können Operationsgeschwindigkeit und Effektivität drastisch verbessert werden. Die Entscheidungsdurchläufe werden auf Stunden und gelegentlich sogar auf Minuten verkürzt.
- *Kohärente Wirkungen* werden erzielt, wenn die Machtinstrumente von Staaten und Bündnissen konzertiert eingesetzt werden, also integriert in einen kohärenten Gesamtrahmen möglicher Aktionen. Eine verbesserte Abstimmung mit internationalen, nationalen und nicht-staatlichen Stellen sowie ein ganzheitlicher Planungsansatz fördern die Chancen für die Wiederherstellung von Stabilität und Frieden. Ein kontinuierlicher Informations- und Wissensabgleich mit Partnern in möglichen Konfliktgebieten verbessert das Verständnis des gegnerischen Systems, seiner Verbindungen und neuralgischen Punkte und ermöglicht so ein frühzeitiges Eingreifen gleich zu Beginn einer Krise.

- *Streitkräftegemeinsamer Einsatz und effektive Unterstützung* dieser Kräfte bedingt die Fähigkeit, Lagevorteile durch zügiges eigenes Handeln zu erreichen und verteilte Operationen über die gesamte Tiefe und Breite des Einsatzraumes durchzuführen. Die Einsatzkräfte sind zuverlässig und nachhaltig logistisch zu unterstützen. Entwicklungs- und Erprobungsprogramme treiben die Verbesserung zukünftiger Fähigkeiten voran. Dem entspricht der fähigkeitsorientierte Ansatz der Bundeswehrplanung. Eine streitkräftegemeinsame herausfordernde, einsatznahe, multinationale Ausbildung muss die neuen Einsatzkonzepte unterlegen. Streitkräftegemeinsames Denken, Führen, Handeln und Wirken im Einsatz gelingt deutlich wirkungsvoller, wenn die Einsatzkräfte in einer auf streitkräftegemeinsame Lösungsmechanismen optimierten Ausbildungseinrichtung ausgebildet, trainiert und überprüft werden können. Transformation erfordert als wesentliche Dimension eine Veränderung des Denkens. Streitkräftegemeinsame Ausbildung und Training sind Schlüsselelemente zur Verankerung veränderter Einstellungen und Denkmuster.

**Zentrum für die Transformation der Bundeswehr**

Die Transformation der Bundeswehr mit Blick auf die wahrscheinlichen Einsätze erfordert Fähigkeiten, mit denen sie in künftigen Krisen und Konflikten als leistungsstarker, koalitionsfähiger Partner bestehen kann. Im Einsatz für Stabilität in Krisenregionen muss die Truppe durch Struktur und Auftrag, Ausbildung und mentale Vorbereitung auf den Einsatz in die Lage versetzt werden, das gesamte Aufgabenspektrum von Kampfhandlungen bis zu parallelen oder nachfolgenden friedensstabilisierenden Maßnahmen wahrzunehmen. Dies schließt natürlich nicht aus, dass sich die Ausbildungs- und Ausrüstungsschwerpunkte der mit unterschiedlichen Aufgaben befassten Truppenteile deutlich unterscheiden. Der Aufbau der Versorgung und erster Grundstrukturen staatlicher Organisation im Krisengebiet erfordert zudem das enge Zusammenwirken mit zivilen Aufbauhelfern.

Mit Blick auf die vielschichtigen Anforderungen ist ein adäquater Streitkräftemix (Forces Mix) der eingesetzten Kräfte unentbehrlich. Die Entscheidung der politischen und militärischen Führung, in der Bundeswehr Eingreif-, Stabilisierungs- und Unterstützungskräfte aufzustellen und dabei der Fähigkeit zur vernetzten Operationsführung insbesondere bei den Eingreifkräften eine Schlüsselrolle einzuräumen, setzt die bisher gewonnenen Erkenntnisse und

Erfahrungen um. Die Bundeswehr schlägt mit dem Prozess der Transformation einen Weg kontinuierlicher Erneuerung und Veränderungen ein – einen Weg zu struktureller Flexibilität und Lernfähigkeit.

Transformation muss organisiert werden. Sie erfordert eine inhaltliche und planerische Neuausrichtung der Bundeswehr. Diese muss als kontinuierlicher, vorausschauender Anpassungsprozess sicherstellen, dass die Bundeswehr mit den in ihrem Umfeld immer schneller ablaufenden politischen, gesellschaftlichen, wirtschaftlichen und technologischen Umwälzungen Schritt hält. Der Generalinspekteur der Bundeswehr ist als Gesamtverantwortlicher für die Bundeswehrplanung zugleich der Gesamtverantwortliche für die Transformation der Bundeswehr. Sein Stellvertreter vertritt die deutschen Interessen in Bezug auf Transformation auf Abteilungsleiter-Ebene im nationalen und multinationalen Bereich. Zur Koordinierung wurde im Verteidigungsministerium auf der Ebene der Stabsabteilungsleiter mit der Koordinierungsgruppe Transformation ein organisationsübergreifendes Gremium eingerichtet. Hier werden konkrete Transformationsprojekte identifiziert und mit Ressourcen hinterlegt. Diese Gruppe wird auf Referatsebene von einer Arbeitsgruppe Transformation unterstützt. Ein Sekretariat bereitet die Sitzungen der Koordinierungsgruppe vor und nach. Innerhalb der Arbeitsgruppe können zur Behandlung von Einzelfragen Unterarbeitsgruppen gebildet werden. Alle Bereiche des Verteidigungsministeriums sind beteiligt. Zusätzliche Expertise kann jederzeit hinzugezogen werden.[31]

Das neue Zentrum für Transformation der Bundeswehr unterstützt seit dem 29. Juni 2004 das Ministerium bei der Bewältigung dieser Aufgaben. Die ministeriellen Entwicklungs-, Planungs- und Entscheidungsprozesse erfordern leistungsfähige Strukturen an zentraler Stelle im nachgeordneten Bereich. Das neue Zentrum baut auf der bereits vorhandenen Expertise und den Ressourcen des Zentrums für Analysen und Studien der Bundeswehr (ZASBw) auf und entwickelt diese weiter. Das Zentrum arbeitet im nachgeordneten Bereich des Verteidigungsministeriums auf der Grundlage von Weisungen und Vorgaben zu. Seine Aufgaben umfassen insbesondere

- die strategische Zukunftsanalyse,
- die Unterstützung des Ministeriums durch Expertise für Sicherheitspolitik und Militärstrategie,

[31] Hierzu weiterführend: Gerhard Schulz und Hans Reimer, „Transformation der Bundeswehr – der Weg in die Zukunft“, *Europäische Sicherheit* 53:5 (Mai 2004), S. 31-37.

- die Erarbeitung konzeptioneller Vorgaben für die Transformation der Streitkräfte,
- die Durchführung und Auswertung der experimentellen Überprüfung von Konzepten und Prototypen – national wie auch in internationaler Kooperation – mit Blick auf die Weiterentwicklung der Fähigkeiten der Schwerpunkte „Streitkräftegemeinsamkeit", „Interoperabilität" und „Multinationalität",
- das Einsteuern der Ergebnisse in die Bundeswehrplanung, insbesondere über die Fähigkeitsanalyse,
- die Unterstützung der multinationalen Streitkräfteplanung,
- die Erarbeitung und Pflege des Analyse- und Modellinstrumentariums der Bundeswehr im Bereich Operations Research/Modellbildung und Simulation.

Hierzu koordiniert es organisationsbereichsübergreifend die Aktivitäten der mit Fragen der Weiterentwicklung beauftragten Dienststellen. Alle relevanten Akteure unterhalb der ministeriellen Ebene werden in die Aktivitäten des Zentrums für Transformation der Bundeswehr eingebunden, denn bei der Transformation geht es um Integration und Synergie. So werden die verschiedenen Handlungsfelder wirkungsvoll in ihrer Komplexität zusammengeführt und frühzeitig koordiniert sowie die beteiligten Dienststellen zweckmäßig für die Transformation der Bundeswehr genutzt.

Das Zentrum für Transformation der Bundeswehr verfügt über drei Säulen:

- In der *Abteilung Weiterentwicklung der Bundeswehr* wird analysiert, wie sich die Bundeswehr an veränderte Herausforderungen anpassen muss. Daraus resultieren Anstöße für die Konzeptentwicklung, die Streitkräfteplanung und die materielle Ausrüstungsplanung der Streitkräfte. Grundlagen dafür sind Ergebnisse der Zukunftsanalyse, der Fähigkeitsanalyse, der einsatzbegleitenden Auswertung, wissenschaftliche Erkenntnisse und Ergebnisse aus der Forschungs- und Studienarbeit sowie der technologischen Entwicklungen und der nationalen wie multinationalen Prozesse im Bereich CD&E. Für zielgerichtete Transformation werden Doktrinen und Führungsvorschriften im Einklang mit den neuen Aufgaben entwickelt bzw. weiterentwickelt.
- Die *Abteilung Concept Development & Experimentation* unterstützt das Ministerium bei der Verbesserung der Einsatzfähigkeit der Bundeswehr

durch die aktive Ausgestaltung nationaler und multinationaler CD&E-Prozesse. Sie leistet mit dem SJFQH-Anteil und der Wissensüberlegenheitszelle unentbehrliche Beiträge in der Anfangsphase realer Operationen und unterstützt den Planungsprozess auf operativer militärstrategischer Ebene. Einsatzbegleitende Auswertung vermittelt wichtige Erkenntnisse und Rückkopplungen für die Konzeptentwicklung. Damit leistet die Abteilung einen entscheidenden Beitrag zur Weiterentwicklung von streitkräftegemeinsamen Fähigkeiten im multinationalen Kontext.

- Die *Abteilung Operations Research, Entwicklung und Einsatz von Modellen und Simulation* erarbeitet die konzeptionellen Grundlagen im Bereich Operations Research. Sie koordiniert die bi- und multinationale Zusammenarbeit mit transnationalen und NATO-Gremien, dem Allied Command Transformation (ACT), der NATO C3 Agency (NC3A) sowie Instituten befreundeter Nationen. Darüber hinaus wird dieser Abteilung mit dem Integrierten Testbed eine Plattform für das Zusammenwirken von Bedarfsträger, Bedarfsdecker, Forschung und Industrie zugeordnet. Durch Realisierung einer vernetzten Infrastruktur für Modellbildung und Simulation (M&S), die Dual-Use und damit Nutzung durch Dritte nicht nur zulässt, sondern mit Blick auf die vollständige Ausschöpfung des Innovationspotentials ausdrücklich fördert, werden Doktrinen, Konzepte, Strukturen sowie Software- und Hardware-Komponenten für die NetOpFü-Befähigung der Bundeswehr prototypisch entwickelt und im Systemzusammenhang auf ihre Tauglichkeit geprüft.

Das *Integrierte Testbed* verbindet die Innovationszyklen von Industrie und Wirtschaft mit der Transformation der Bundeswehr wie ein Getriebe. Es dient der Unterstützung von Analyse, Bedarfsermittlung und Bedarfsdeckung, einschließlich der Erprobung und prototypischen Entwicklung. Das Testbed ist modular so aufgebaut, dass es für unterschiedliche Transformationszwecke flexibel und wirtschaftlich genutzt werden kann. Es besteht aus Modellen und Simulationssystemen für alle Führungs- und technischen Ebenen, dient aber ebenfalls den Analyse-, Experimental-, Test-, Übungs- und Ausbildungszentren der Bundeswehr. Hier können Optionen für Einsatz- und Operationsplanung sowie für die Unterstützung von Ausbildung und Übungen analysiert werden. Darauf aufbauend lassen sich entsprechende einsatzfähige Systeme entwickeln.

Das neue Zentrum für Transformation fängt als Motor der Transformation der Bundeswehr nicht bei Null an. Es kann sich auf Initiativen, Ergebnisse und Expertise abstützen, die das ZASBw bereits seit fast zwei Jahren entwickelt hat. Seit Anfang 2003 nimmt dieses bereits eine Schlüsselfunktion in der transformatorischen Ausgestaltung der Bundeswehr ein – durchaus auch hinsichtlich multinationaler Transformationsprozesse. Es beteiligt sich – in enger Abstimmung mit dem Verteidigungsministerium – aktiv an der Transformation der US-Streitkräfte und nutzt hieraus gewonnene Erkenntnisse für die Weiterentwicklung der Bundeswehr. Außerdem wurde im Oktober 2003 im ZASBw der Aufbau des Bereiches CD&E-Management begonnen, der „Konzeptentwicklung und Experimentierung" als Methode der Transformation nutzt, um insbesondere bundeswehrgemeinsame und multinationale Projekte voranzutreiben.

Das Zentrum für Transformation wird diesen Kurs konsequent weitergehen müssen. Dies gilt insbesondere mit Blick auf die Zusammenarbeit mit den Organisationsbereichen und den multinationalen Partnern. Für das Zentrum selbst wird es darauf ankommen, sich bereichsübergreifend auf die gemeinsame Zielsetzung auszurichten und neue Verfahren der internen und externen Kooperation zu entwickeln.

Eine Reihe zum Teil bereits initiierter und für die Transformation der Streitkräfte bedeutender Projekte werden die Arbeit des Zentrums für Transformation wesentlich prägen:

- *Multinationale Experimente* im Rahmen der NATO sowie auf bi- und multilateraler Basis sind ein unverzichtbarer Baustein für die Entwicklung neuer Konzepte, die alle Bereiche militärischen Denkens und Handelns nach vorne bringen. Sie schaffen eine wesentliche Grundlage für die Interoperabilität der Bundeswehr im Kontext multinationaler Einsätze, insbesondere auch im Rahmen der NATO Response Force (NRF). Mit dem Aufbau von Battlelabs in Potsdam und in Ottobrunn ist bereits der Nukleus einer leistungsfähigen deutschen Experimentalumgebung geschaffen worden.
- Die *Fähigkeit zur vernetzten Operationsführung* ist eine Grundvoraussetzung für einen bedeutsamen Beitrag der Bundeswehr zur multinationalen Krisenprävention und -reaktion. Die konzeptionelle Grundlagenarbeit hierzu einschließlich der Koordinierung und Implementierung geeigneter Projekte wird sich in der Arbeit des Zentrums für Transformation spiegeln. Beispiele hierfür sind die Konzeptarbeiten für die ver-

netzte Operationsführung oder das streitkräftegemeinsame, ebenengerechte und aktuell aufbereitete Lagebild.

- Technologie ist nur ein Aspekt vernetzter Operationsführung. Insbesondere kommt es darauf an, streitkräftegemeinsames Denken und Handeln in der Bundeswehr durchgängig zu verankern. *Streitkräftegemeinsame Ausbildung und Erziehung* sind hierfür entscheidend. Die Weiterentwicklung des Gefechtssimulationszentrums (GSZ) in Wildflecken zu einem streitkräftegemeinsamen Trainingszentrum ist ein großer Schritt in diese Richtung, den das Zentrum für Transformation der Bundeswehr in Konzeption und Realisierung mitgestalten wird.
- Studien liefern wichtige Grundlagenarbeit für die Implementierung von Transformationszielen. Mit einer *Studieninitiative* des neuen Zentrums für Transformation werden transformationsrelevante Fragestellungen gesichtet, aufeinander abgestimmt und in ein konkretes Arbeitsprogramm umgesetzt. Somit weist die Studienarbeit den Weg für die gezielte Förderung wichtiger Projekte sowie die Entwicklung innovativer Ansätze. Alle Organisationsbereiche der Bundeswehr sind daran beteiligt. Die Themenfelder umfassen sämtliche transformationsrelevanten Bereiche, darunter: Zusammenwirken der Teilstreitkräfte bei NetOpFü-Operationen unterschiedlichster Art; Steigerung der Führungsfähigkeit vernetzter Streitkräfte in allen Belangen; Entwicklung und Nutzung neuer Technologien und Einsatzgrundsätze für zukünftige Einsätze; Konzipierung einer streitkräftegemeinsamen Ausbildung zu Inhalten der NetOpFü; Ausbau der Fähigkeiten zu Modellbildung und Simulation etc. Hier wird die gedankliche Basis für die künftige Einsatzfähigkeit der Streitkräfte geschaffen.
- Der Transformationsfokus der Bundeswehr liegt im kommenden Jahrzehnt absehbar im Bereich von Führung und Einsatzplanung. Darauf ist die Transformation konsequent auszurichten. Dabei geht es nicht nur um Grundlagenarbeit. Erkenntnisse werden umgehend umgesetzt. Ein Beispiel hierfür ist das *SJFHQ*. Dieses Führungselement neuen Zuschnitts verbindet modernste Technologie zur Führungsunterstützung mit dem neuartigen Konzept zur vernetzten Operationsführung auf Grundlage eines wirkungsorientierten Ansatzes. Dieser erfordert ein ganzheitliches Lagebild, welches weit über rein militärische Aspekte hinausgeht. ONA leistet hierzu den entscheidenden Beitrag. Die hohe Bedeutung der Zusammenarbeit der Bundeswehr mit anderen staatli-

chen und nicht-staatlichen Organisationen findet ihre Berücksichtigung. Die Ausgestaltung eines SJFHQ mit den genannten Fähigkeiten wird wesentlich durch das Zentrum für Transformation vorangetrieben.

In der Ausgestaltung der Transformation ist die Industrie für die Bundeswehr ein unverzichtbarer Partner. Rasche Innovation ohne engen Schulterschluss mit der Industrie ist eine Illusion. Aufgabe des Zentrums für Transformation wird es sein, den Dialog und die *Kooperation mit der Industrie* zu intensivieren und leistungsfähige Mechanismen der konkreten Zusammenarbeit zu entwickeln. Ziel ist die Koppelung von technologischer Innovation mit konzeptionellen Überlegungen zur Transformation der Streitkräfte. Erste Schritte zu einer stärkeren Integration der deutschen bzw. europäischen Industrie in multinationale Transformationsprozesse wurden bereits eingeleitet.

**Der CD&E-Prozess und die Bedeutung von Modellbildung und Simulation**

CD&E ist das Werkzeug der Transformation. Damit hat es auch im Zentrum für Transformation eine besondere Rolle. CD&E soll Transformation im Sinne eines System of Systems-Ansatzes vorantreiben. Es dient als ein ineinander greifender iterativer Zyklus der Entwicklung von Konzepten, ihrer Bewertung und sukzessiven experimentellen Weiterentwicklung und Verfeinerung. CD&E ist streitkräftegemeinsam – in vielen Bereichen sogar bundeswehrgemeinsam – angelegt. Es überspannt alle Planungsebenen in optimierenden Rückkopplungsschleifen. Dabei wird analysiert, inwieweit technische Möglichkeiten und Grenzen den Einsatz von Streitkräften und anderen Machtinstrumenten von der taktischen bis hin zur sicherheitspolitischen Ebene beeinflussen. Modelle und Simulation unterstützen diesen Prozess.

Frühzeitiges Erkennen und Nutzen von Innovationspotential sind von entscheidender Bedeutung für zukunftsfähige Streitkräfte. Deshalb engagiert sich Deutschland im CD&E-Prozess mit einem anspruchsvollen Ansatz. Mit Blick auf die vielfältigen Aktivitäten in der Experimentierung neuer operativer Konzepte konzentriert sich die Bundeswehr auf

- die Abbildung neuer Ziele und Wirkungen,
- die Weiterentwicklung der Abbildung menschlichen Verhaltens, besonders von Entscheidungsverhalten,

- Informationsoperationen und die Weiterentwicklung des Simulationssystems auf Kriegs- und Krisenschauplatzebene,
- das Simulationsverbundsystem auf Kriegs- bzw. Krisenschauplatzebene Joint Operations Army-Navy-Air Force (JOANA), das in die multinationale Föderation von Simulationssystemen eingebracht wurde.

Wegen des multinationalen Charakters der Experimente werden auch auf multinationaler Ebene einheitliche Standards gebraucht. Nicht zuletzt mit Blick auf die knappen personellen und finanziellen Ressourcen ist ein koordiniertes Vorgehen zweckmäßig. Schließlich geht es beim multinationalen Ansatz um die Interoperabilität der beteiligten Partner. Auf Initiative der USA wurde mit Kanada, Australien, England, Frankreich und Deutschland der Multinational Interoperability Council (MIC) als Steuerkopf einer umfassenden und hoch qualifizierten CD&E-Gemeinschaft gebildet. Dieser treibt unter US-Federführung die Transformation der Streitkräfte der Teilnehmernationen voran. Die hier entwickelten neuen Standards und Einsatzkonzepte werden absehbar die Ausrichtung von NATO und Europäischer Union nachhaltig beeinflussen. Bereits im März 2003 beschloss der Militärische Führungsrat die Forcierung der Bundeswehrbeteiligung an der multinationalen CD&E-Gemeinschaft und die Aufwertung vom Beobachter- zum Partnerstatus. Mittels der erwähnten CD&E-Abteilung im Zentrum für Transformation der Bundeswehr wurde die Voraussetzung zu einer qualifizierten Beteiligung geschaffen. Damit sichert sich Deutschland Stimme, Kenntnis und Beitragsfähigkeit in einer transformationsgerichteten multinationalen Konzeptentwicklung und Experimentierung.

International ist die Nutzung von CD&E für die Streitkräftetransformation in den USA bisher besonders ausgeprägt und am weitesten fortgeschritten. Aber auch beispielsweise Großbritannien, Schweden und jüngst auch Frankreich gehen diesen Weg konsequent.[32] In der vom U.S. Joint Forces Command in Norfolk geführten streitkräftegemeinsamen Konzeptentwicklung der US-Streitkräfte zeichnen sich derzeit eine Reihe von Schwerpunkten ab, die sich auch in der Konzeptentwicklung der Streitkräfte anderer Nationen niederschlagen werden, natürlich auch bei der Bundeswehr. Ein Joint Operations Concept dient in den USA als streitkräftegemeinsames operatives und strukturbestimmendes Dachkonzept. Vier Joint Operating Concepts sollen bestimmte Einsatzformen ausgestalten. Die Themenstellungen sind Major Combat Operations, Stability Opera-

[32] Die umfassende Ausrichtung der Bundeswehr an einem leistungsfähigen CD&E wurde bereits im vorangehenden Abschnitt ausgeführt.

tions, Strategic Deterrence und Homeland Security. Darüber hinaus sichert eine Vielzahl von Prototypenentwicklungen die Umsetzung des SJFHQ-Konzepts. Deren Tragfähigkeit und Eignung wird derzeit durch Experimentierung belegt.

Die meisten multinationalen Experimente werden verteilt durchgeführt. Die Partner kooperieren über Kontinente hinweg im engen virtuellen Schulterschluss. Deshalb werden auf dem multinationalen Labor-Netzwerk so genannte Collaborative Tool Suites eingesetzt. Diese integrieren Web-basierte Kommunikationsmöglichkeiten, darunter Sprache, E-Mail, Datenaustausch, Chat, Videokonferenz etc. In Deutschland wurden bereits Ottobrunn und Potsdam als die Standorte von Experimententwicklung und -durchführung sowie Gelsdorf als Standort des Zentrums für Nachrichtenwesen der Bundeswehr für System of Systems-Analysen und ONA angeschlossen. Für die Zukunft bietet sich an, weitere Zentren anzuschließen, zum Beispiel die Führungsakademie in Hamburg und das Simulationszentrum in Wildflecken, Einrichtungen des Bundesamtes für Wehrtechnik und Beschaffung und des IT-Amtes sowie bestimmte Ausbildungs- und Weiterentwicklungsdienststellen der Bundeswehr. Das alles kann nur mit einem langfristigen Engagement gelingen.

Konzeptentwicklung und deren experimentelle Überprüfung unterstützt die Transformation unter Nutzung von Modellbildung und Simulation. Komplexe Systemzusammenhänge und militärische Fähigkeiten, einschließlich ihrer technologischen Dimension, lassen sich mit Hilfe wirklichkeitsnaher Simulation aus ganzheitlicher Perspektive analysieren. Durch Simulation lassen sich neue konzeptionelle Überlegungen und organisatorische Vorstellungen, neue Managementverfahren und Innovation im technologischen Bereich ganz praktisch, zuverlässig und kostengünstig prüfen. Darüber hinaus trägt eine leistungsfähige Simulations- und Testumgebung dazu bei, in Führung, Einsatz und Ausbildung quantitative oder qualitative Komplexität zu reduzieren. Insbesondere unterstützt sie die Entscheidungsfindung bei hohem operativem Tempo und unter der Belastung durch eine vorbildlose Informationsflut.

Multinationales CD&E muss entsprechend durch ein ebenfalls multinational verwendbares M&S-Instrumentarium unterlegt werden. Die Bundeswehr will sich mit ihren M&S-Möglichkeiten frühzeitig in die aufwachsenden NATO-CD&E-Prozesse einbringen. Dabei sollen frühere Investitionen in das bereits vorhandene deutsche Instrumentarium sinnvoll genutzt werden. Deutsche Modelle und Simulationssysteme sollen also aktiv – gelegentlich durchaus auch unentgeltlich – in das multinationale und NATO-CD&E-Umfeld eingebracht wer-

den. Insbesondere das Allied Command Transformation mit seinem Joint Warfare Center in Stavanger ist ein idealer Partner.

Neue Konzepte und Doktrinen, neue Systemen und Verbundlösungen stellen natürlich auch immer höhere Anforderungen an Modelle und Simulationssysteme. Gerade bei der Umsetzung der vernetzten Operationsführung wird deutlich, dass für die Bundeswehr eine leistungsfähige Simulations- und Testumgebung erst noch zu schaffen ist. Es kommt darauf an, auch unter Zeitdruck die Eignung von nicht-technischen und technischen Lösungskonzepten beurteilen und realisieren zu können. Dafür ist ein realitätsnahes Systemumfeld bereitzustellen. Neue Konzepte und Komponenten sind in einem Gesamtverbund zu integrieren.

Vorhandene und auch neu zu entwickelnden Modelle und Simulatoren werden Zug um Zug vernetzt werden müssen – national, aber auch multinational. Manche sind in einer übergreifend gestalteten Architektur miteinander zu verbinden. Andere sind für die fallweise experimentelle Vernetzung vorzubereiten – z.B. mit Führungs- und Informationssystemen oder auch technischen Simulatoren. Die amtlichen, industriellen und akademischen Battlelabs und Testbeds, Forschungs- und Ausbildungseinrichtungen müssen hierzu weiterentwickelt werden, damit sie bei Bedarf „angebunden" werden können. Dies erfordert eine kohärente Netzarchitektur, nicht ein völlig neues Netz. Letztlich kommt es weniger darauf an, alle realen Systeme mit allen simulierten Systemen kontinuierlich zu vernetzen. Es geht vielmehr darum, die Vernetzbarkeit dieser Ressourcen an sich zu ermöglichen und – wenn erforderlich – sehr schnell eine auftragsbezogene und zeitlich begrenzte Vernetzung durchführen zu können.

Auch der Forderungskatalog hinsichtlich inhaltlicher Ergänzungen ist umfangreich. So sind derzeit die Einsatzbedingungen in den asymmetrischen Szenarien der „Neuen Kriege" in den vorhandenen Modellen noch nicht angemessen abgebildet. Die militärisch relevanten Wirkungen nicht-militärischer Akteure sind sichtbar und analysierbar, mess- und bewertbar abzubilden. Die Modellierung menschlichen Verhaltens ist zu erforschen und in die Systeme einzubringen. Neue Modellierungstechniken, wie z.B. das Agent Based Modelling,[33] verdienen eine eingehende Befassung. Die Eignung dieser Simulationssysteme für die Unterstützung von militärischer und politischer Entscheidungsfindung ist

[33] Agent Based Modelling simuliert modellhaft das Verhalten von Akteuren (z.B. als Einzelperson, Volksgruppe, Glaubensgemeinschaft. Diese bilden die „Agents".), um daraus Rückschlüsse über die Grundlagen, die Regeln und die Wechselwirkungen sozialen Verhaltens bzw. sozialer Beziehungen ableiten zu können.

zu prüfen und zu verbessern. Neue Informations- und Datenquellen z.B. aus der Nachrichtengewinnung und Aufklärung sind zu erschließen und zweckmäßig aufzubereiten. Die für militärische Konzepte und Planungen relevanten, bewerteten Daten müssen automatisiert in die Simulation eingehen und verwertbar in militärische Entscheidungsfindung und operative Anwendungen einfließen können. Nicht zuletzt mit Blick auf wirkungsorientierte Operationsführung ist auch die Abbildung neuer Kategorien von Zielen und Wirkungen in den Modellen erforderlich. Mit Blick auf Stabilitätsaufgaben werden auf der gesamtstrategischen Ebene Modelle gebraucht, mit denen man einen sicherheitspolitischen Wirkungsverbund aller Machtinstrumente unter Einschluss militärischer Maßnahmen planen, bewerten und optimieren, multinational abstimmen und kommunizieren kann.

Für das Operations Research und M&S der Bundeswehr ergeben sich insgesamt vor allem drei Schwerpunkte:

- Operations Research und M&S werden künftig als analytische Unterstützung bei CD&E eine wichtige Rolle spielen. Im Bereich der Konzeptentwicklung dient M&S dabei absehbar vor allem der nicht-technischen Analyse. Bei der Validierung von Prototypen werden technische und nicht-technische Anwendungen von M&S zu integrieren sein, damit die Wirksamkeit der Lösungen im operativen Umfeld aus einer systemischen Gesamtsicht bewertet und verglichen werden kann.
- Operations Research und M&S müssen einen integrierten, leistungsfähigen Verbund von Hilfsmitteln und Werkzeugen für die Analyse operativer Aufgabenstellungen und konkreter Lösungsansätze zur Verfügung stellen. Dieser Verbund unterstützt die am multinationalen CD&E-Prozess beteiligten Stellen auf Grundlage validierter und abgestimmter Analysemechanismen und Bewertungskriterien.
- Operations Research und M&S behalten insbesondere im Rahmen der Fähigkeitsanalyse ihre grundsätzliche Funktion und Bedeutung für die Bundeswehrplanung. Für die Unterstützung der nationalen und multinationalen CD&E-Prozesse sind damit zusätzliche Ressourcen einzusetzen.

**Die Rolle der Industrie**

Der Erfolg der Transformation der deutschen Streitkräfte ist entscheidend von der gelungenen Einbindung der Industrie und deren raschen Innovationszyklen abhängig.[34] Kooperationsfähigkeit und Interoperabilität mit unseren multinationalen Verbündeten und Partnern, insbesondere aber auch die Fähigkeit zur vernetzten Operationsführung der Bundeswehr können nur im engen Schulterschluss mit der Industrie gelingen. Jeder muss seine spezifischen Fähigkeiten einbringen – militärische Planer und Ingenieure der unterschiedlichsten Fachrichtungen, Systemanalytiker und Operations Research-Fachleute, Haushälter und Datenverarbeitungspersonal. Die rasche Implementierung von Ergebnissen erfordert seitens der Bundeswehr die Bereitschaft, auch Lösungen, die z.B. nur 80 % der gewünschten Gesamtfunktionalität zur Verfügung stellen, in den Einsatz zu bringen und darüber hinaus auch die Überprüfung der Verfahren der materiellen Bedarfsdeckung mit Blick auf ihre Beschleunigung. Auf industrieller Seite ist der Ausbau der Simulations- und Demonstrationsfähigkeit für neue konzeptionelle Ansätze und technologische Lösungen ein wichtiger Faktor in der zügigen Realisierung neuer Fähigkeiten.

Die Rolle der wehrtechnischen Industrie – insbesondere die Rolle der Großunternehmen – wandelt sich. Zwar gibt es zum Beispiel in Modellbildung und Simulation oder auch Kryptotechnologie noch eine Zukunft für nationale Kompetenz und nationale Fähigkeiten. Dennoch gilt grundsätzlich: Der vormals nationale Sicherheitspartner wird zu einem europäischen Sicherheitspartner. Der militärische Technologieanbieter wird zu einem Integrator und Nutzer ziviler Technologien. Der klassische Produktentwickler wird zu einem innovativen Hersteller von Demonstratoren. Industrielle Kooperation auch unter Konkurrenten – insbesondere hinsichtlich der Bildung einheitlicher, aber offener Standards – wird maßgeblich zum Erfolg von vernetzter Operationsführung beitragen. Bedarfsträger und Bedarfsdecker, Industrie und Forschung können nur in partnerschaftlicher Zusammenarbeit Deutschland und Europa zu leistungsstarken transatlantischen Bündnispartnern machen. Dabei geht es nicht um das Duplizieren des amerikanischen Ansatzes. Ziel ist eine deutsche Befähigung im europäischen Verbund mit transatlantischer Ausrichtung. Dazu sind nationale und europäische Transformationsprojekte von Bedeutung. Diese gilt es zu entwickeln.

Bei der Transformation der Bundeswehr steht Qualität vor Quantität, Potential vor Arsenal. Dies gilt letztlich auch für die in Deutschland ansässige In-

[34] Siehe hierzu auch den Beitrag von Burkhard Theile und Norbert Härle in diesem Band.

dustrie – und hier nicht nur die Rüstungsindustrie. Sie muss den Anschluss an die rasanten Entwicklungen in den USA, Schweden und Großbritannien finden. Wenn Streitkräfte sich signifikant ändern, hat dies auch Auswirkungen auf die Industrie. Die militärische Transformation zieht eine industrielle Transformation nach sich. Ohnehin gelten auch für die Wirtschaft die Grundsätze der vernetzten Operationsführung. Dort wurden sie schließlich von Admiral a.D. Cebrowski für die Streitkräfte entdeckt. Es liegt damit im Interesse der Industrie, die militärische Transformation zu unterstützen und zugleich die eigene industrielle Transformation voranzutreiben. Nur wenn die Industrie eigene „network enabled capabilities" aufweist, kann sie ihre Kunden bei deren Umsetzung kompetent unterstützen.

Die Industrie spielt eine Schlüsselrolle für die Versorgung der Bundeswehr mit Material und Ausrüstung, das die angestrebten neuen Fähigkeiten angemessen technologisch reflektiert. Die Bundeswehr erwartet von der engen Kooperation mit der Industrie rasche und konkrete Ergebnisse bei der Umsetzung der vernetzten Operationsführung. Dabei gewinnen gegenüber den „traditionellen Verteidigungsfirmen" leistungsstarke kommerzielle Zulieferer mit bahnbrechenden Technologien an Bedeutung. Zivile „Entrepreneur"-Firmen wie auch Informations- und Kommunikationsfirmen sind über die Integration von Commercial off the Shelf-Technologien (COTS) wichtige Katalysatoren für eine dynamische Streitkräftetransformation. Die Informationstechnologie hat hier eine besondere Bedeutung u.a. im Kontext der Informations- und Entscheidungsüberlegenheit, bei der Implementierung von neuen Prozessen und Verfahren zur wirkungsorientierten Operationsführung, zur Vermeidung von Informationsüberlastung, aber auch bei der Verdichtung von Information zu Wissen durch Verfahren des Wissensmanagements und der „künstlichen Intelligenz".

Die „traditionellen" Verteidigungsfirmen bleiben jedoch aufgrund ihrer langjährigen Erfahrung mit den komplexen Integrationsaufgaben im Verteidigungsbereich unentbehrlich. Die Fähigkeit, COTS-Produkte an militärische Anforderungen anzupassen sowie deren Integration zu militärischen Systemen wird zur wesentlichen rüstungswirtschaftlichen Kernfähigkeit. Dies unterstreichen Entwicklungen in den USA und Australien, in Großbritannien und Schweden. Hinsichtlich zukünftiger System of Systems-Architekturen und der Demonstration von neuen Fähigkeiten und Lösungen werden sie aufgrund ihres umfassenden Verständnisses von militärischen Abläufen wie auch Kunden- und Beschaffungsstrukturen innovative Lösungen kompetent anbieten können. Während die Bedeutung der Plattformen und der großen Stückzahlen sinkt, lautet die neue

Herausforderung: die Entwicklung und das Management von System of Systems-Konzepten und die schnelle Demonstration von leistungsfähigen Lösungen durch Simulation.

Eine wichtige Rolle für zukunftsorientierte technologische Transformation spielen darüber hinaus die mittelständische Industrie und hier insbesondere die „kleineren" Unternehmen. Für die mittelständige Industrie wird es darauf ankommen, ihre Leistungsfähigkeit und ihr Innovationspotential gegenüber der Bundeswehr transparent zu machen und sich in den Transformationsprozess aktiv einzubringen. Gerade wegen ihrer oft unkonventionellen Lösungsideen sind sie für eine wichtige Rolle im CD&E-Prozess prädestiniert.

**Ausblick**

Die Transformation der Bundeswehr hat ein klares Unternehmensziel: Verbesserte Einsatzfähigkeit für die neuen Aufgaben – im multinationalen Kontext und mit einer belastbaren Durchhaltefähigkeit. Im Vordergrund stehen dabei einerseits eine deutlich stärker ausgeprägte Fähigkeit zum streitkräftegemeinsamen Einsatz im multinationalen Rahmen, andererseits der Erwerb einer Erstbefähigung zu vernetzter Operationsführung bis zum Jahr 2006 insbesondere mit Blick auf den deutschen Beitrag zur NRF.

Drei neue Taktgeber werden den Transformationsfortschritt der Bundeswehr bestimmen, die Fähigkeit,

- hohe Transaktionsraten und Operationsgeschwindigkeiten zu entwickeln,
- strukturelle Lernfähigkeit und Flexibilität zu etablieren und
- Komplexität auf jeder Ebene zu beherrschen.

Dem entspricht der absehbare Transformationsfokus der Bundeswehr im kommenden Jahrzehnt: Führung und Einsatzplanung. Es geht darum, zügig sichtbaren Nutzen für die Einsatzkräfte der Bundeswehr zu generieren. Ein erfolgreicher, dynamischer Beginn erfordert:

- Forcieren der *Vernetzung* als Voraussetzung für eine vernetzte Operationsführung. Dabei liegt der Fokus auf den deutschen Beiträgen zur NRF. Schließlich ist die NRF das Testbed zur NetOpFü-Befähigung der NATO-Streitkräfte.

- Zügige Einrichtung eines *SJFHQ*. Mit der Weisung für die Weiterentwicklung der Streitkräfte ist die Einrichtung eines Kommandos Operative Führung der Eingreifkräfte (KdoOpFüEingrKr) vorgesehen. Der Aufstellung kommt im Hinblick auf die Führung des deutschen Anteils zur NRF hohe Bedeutung zu, denn die Bundeswehr muss zu wirkungsorientierter Operationsplanung in einem von Jointness und Combinedness geprägten Umfeld befähigt werden.
- Ausbau der *ONA-Fähigkeit*. Als eine Voraussetzung für die zu errichtenden Datenbanken über potentielle Einsatzgebiete ist die Erfassung der einschlägigen Expertise sicherzustellen.
- Ausbau des *Gefechtssimulationszentrums* in Wildflecken zu einem *streitkräftegemeinsamen Trainingszentrum*. Insbesondere die Ausbildung in der Bundeswehr muss den zukünftigen Bedingungen – Joint und Combined – Rechnung tragen. Die Ausbildungsorganisation und Übungen müssen eine stärker ausgeprägte streitkräftegemeinsame Kultur reflektieren.
- Bereitstellung eines *streitkräftegemeinsamen, ebenengerechten und aktuell aufbereiteten Lagebildes* als wesentliche Voraussetzung für effektbasierte Operationsplanung und Einsätze.
- Fähigkeit zur *Zusammenarbeit mit nationalen und internationalen staatlichen und nicht-staatlichen Organisationen*.

Der rasche Aufbau und die Herstellung der Arbeitsfähigkeit des Zentrums für Transformation sind wichtige Voraussetzungen für nachhaltigen Erfolg bei der Transformation der Bundeswehr. Die Methoden zur Umsetzung der Transformationsziele liegen auf der Hand: verfügbare Kräfte bündeln, Schwerpunkte bilden, Risiken in Kauf nehmen. Eine Transformation dieses Zuschnitts dient dem Schutz Deutschlands und seiner Bürger, einer größeren Handlungsfähigkeit in der deutschen Außen- und Sicherheitspolitik, und sie gibt nicht zuletzt auch den Soldaten und zivilen Mitarbeitern der Bundeswehr die erforderliche Orientierung und Leistungsfähigkeit.

Burkhard Theile und Norbert Härle

# Streitkräftetransformation aus der Sicht der Rüstungsindustrie

Der Grundstein für die Transformation der europäischen NATO-Streitkräfte wurde anlässlich des Prager NATO-Gipfels im November 2002 gelegt. Die Streitkräftetransformation ist allerdings nicht auf die NATO beschränkt, auch europäische Nationen außerhalb des NATO-Bündnisses transformieren ihre Streitkräfte. Die Geschwindigkeiten und die Ressourcen der Streitkräfteneugestaltung variieren von Nation zu Nation. In Deutschland können die Verteidigungspolitischen Richtlinien (VPR) vom Mai 2003, die ministerielle Weisung für die Weiterentwicklung der Bundeswehr vom 1. Oktober 2003, die im Dezember 2003 veröffentlichten Konzept- und Strukturvorstellungen und die Weisung des Generalinspekteurs vom 1. März 2004 als Grundlagenpapiere für die Umgestaltung der Bundeswehr gesehen werden.

Transformation hat viele Facetten und Komponenten. Zentral für die Transformation stehen neue Konzepte und neue Szenarien. Zur optimalen Unterstützung ist eine informationstechnische Vernetzung notwendig, die dadurch zu einem wichtigen Teilaspekt der Transformation wird. Transformierte Streitkräfte sollen effektiv und effizient auf die derzeitig wahrscheinlichsten militärischen Herausforderungen reagieren können. Durch ständig arbeitende Einsatzführungskommandos werden kritische Regionen kontinuierlich aufgeklärt, überwacht, und es werden wahrscheinliche Szenarien simuliert. Streitkräfte müssen dann in der Lage sein, schnell auf unkonventionelle militärische Probleme reagieren zu können. Der militärische Erfolg ist die Leitlinie des Handelns, militärische Operationen werden wirkungsorientiert angelegt und durchgeführt. In der Vergangenheit wurden militärische Operationen über hierarchische Strukturen geführt. Die heute zur Verfügung stehenden Technologien und weltumspannende Infrastrukturen wie Satellitenkommunikation ermöglichen die vernetzte Operationsführung. Das hat weitreichende Auswirkungen auf die Doktrin, die Ausrüstung, die Führung, die Ausbildung und das Personal sowie auf die Industrie.

Transformierte Streitkräfte setzen streitkräftegemeinsam fähigkeitsorientierte Systeme ein; die Plattformorientierung der Teilstreitkräfte wird abgelöst. Fähigkeitsorientierte Systeme haben im Allgemeinen eine höhere Komplexität als eine Plattform. Sie werden deshalb mit Hilfe eines neuen Verfahrens, der Konzeptentwicklung und Erprobung (Concept Development and Experimentati-

on, CD&E)[35] entwickelt. Die Transformation hat rüstungstechnische und rüstungswirtschaftliche Folgen. Den daraus resultierenden Herausforderungen muss sich die Industrie stellen.

Im militärischen und rüstungstechnischen Kontext ist der Begriff Transformation nicht scharf definiert, er soll deshalb durch sechs industrierelevante Kernaussagen charakterisiert werden:

- Die Transformation der Streitkräfte ist ein unumkehrbarer Prozess: Er bleibt nicht auf die Streitkräfte begrenzt, auch die Industrie muss transformieren.
- Die Transformation ist nicht Revolution, sondern Evolution: Sie ist ein kontinuierlich fortschreitender Prozess unter ständiger Einbeziehung neuer Verfahren, Technologien und Geräte.
- Die Fähigkeitsorientierung ist der primäre Treiber der Transformation. Vernetzung, Plattformen und Informationssysteme sind die wesentlichen Säulen.
- Die Transformation der Streitkräfte zielt auf Steigerung der Einsatzeffizienz: Sie ist kein Mittel, um Geld zu sparen, sondern um vorhandene Budgetmittel effektiver einzusetzen.
- Die Industrie muss synchron mit den Streitkräften transformieren, um die notwendigen Leistungen und Produkte liefern zu können. Die Transformation der Streitkräfte wird mittel- bis langfristig zu Veränderungen in der rüstungsindustriellen Basis führen: Die Chancen sind dabei größer als die Risiken.
- Die Transformation ist ein komplexer Prozess und verlangt neuartige Ansätze. Sie kann nur im Dialog aller Beteiligten effizient durchgeführt werden.

In den folgenden Abschnitten sollen die durch die Transformation bedingten Anforderungen an die Industrie, rüstungswirtschaftliche Fragestellungen und der industrielle Transformationsprozess behandelt werden.

[35] Siehe zu den diesbezüglichen Bemühungen der Bundeswehr den Beitrag von Ralph Thiele in diesem Band.

**Technologieansatz: Vernetzung**

Der wichtigste und zentralste Ansatz ist die Vernetzung der verschiedensten Systeme. Dieser Ansatz ist die Basis für Network Centric Warfare (NCW) oder Network Enabled Capabilities (NEC). Grundidee ist, dass fortgeschrittene Informationstechnologie und die Kommunikationstechnik durch eine universelle und offene Architektur mit Standardschnittstellen die Vernetzung von Aufklärung, Führung und Effektoren ermöglichen und damit zur erheblichen Reduktion der Zeit zwischen der Beobachtung einer Gefahr und der Aktion dagegen führt. Gleichzeitig wird eine erheblich bessere Qualität in der Wahl und der Durchführung der Aktionen erreicht. Die Vernetzung schließt die Logistik selbstverständlich mit ein, die dadurch effektiver und koordinierter wird und Personen, Ausrüstung und Ersatzteile zum richtigen Zeitpunkt an den richtigen Ort bringen kann. Anstatt durch Verbesserung der Plattformen wird durch die Vernetzung mit erheblich weniger Mitteln eine effektivere und auch effizientere Truppe erreicht.

Die Problematik bei der Vernetzung ist die Definition einer übergreifenden Architektur und der notwendigen Standards, insbesondere, da sich das Netzwerk aus sehr heterogenen, militärischen Systemen zusammensetzt (z.B. Fahrzeuge bis Einzeltruppen, Flugzeuge, Schiffe, Aufklärungssysteme und Satelliten). Durch die Vernetzung wird Intelligenz (Software und Kommunikation) die Masse ersetzen, weniger Personal und weniger Ausrüstung benötigt werden und die Einsätze präziser und effizienter werden, wobei die Plattformen leichter und mobiler sein können. Dadurch soll schließlich eine schnellere Dominanz im Gefechtsfeld erreicht werden.

**Anforderungen an die Industrie**

Genau wie die Streitkräfte muss auch die Industrie in einen Lernprozess eintreten und ihre Produkte und Leistungen an die militärischen Forderungen anpassen. Beispielsweise erfordert der Ansatz, militärische Einsätze teilstreitkräfteübergreifend (Joint) und in Koalition durchzuführen (Combined), auch ein übergreifendes Denken in der Industrie. Bisher getrennt operierende Geschäftsbereiche müssen enger zusammenarbeiten. Kooperationen zwischen Firmen gegebenenfalls auch im internationalen Umfeld mit unterschiedlichen Produkten und Erfahrungen werden immer mehr eine Rolle spielen. Der erweiterte Sicherheitsbegriff, der nicht mehr ausschließlich das Militär berücksichtigt und auch das militärische Einsatzspektrum stark in den Bereich von polizeilichen Aufgaben

erweitert, erfordert eine neue Sicht der Industrie, die sich dadurch einem Kunden mit veränderten Bedürfnissen und Anforderungen gegenüber sieht.

Die kontinuierliche und schnelle Innovation erfordert schnelles Entwickeln von neuen Konzepten und Technologien in der Industrie. Industrielle Forschung spielt daher immer mehr eine wichtige Rolle zu Lasten der Stückzahlen von Plattformen. Neue Projekte werden wahrscheinlich immer kleiner werden und stark vom Fortschritt in der kommerziellen Welt abhängen, wodurch auch die Bedeutung der zivilen Industrie als Taktgeberin sicherheitspolitischer und militärischer Innovation zunimmt.

Die Industrie muss sich schwerpunktmäßig mit acht Themenkomplexen befassen:

- Wahrung der Kontinuität des operativen Geschäftes, gekennzeichnet durch Auftragseingang, Umsatz und Ergebnis. Das ist zum Erhalt der rüstungstechnischen Kompetenz notwendig. Hier ist die Industrie ganz wesentlich von der Auftragsvergabe des Bundesverteidigungsministeriums und von der Exportgenehmigungspraxis abhängig.
- Bereitstellen von transformationsgerechten Produkten und Dienstleistungen in einem Umfeld, in dem der Auftraggeber gleichzeitig die neuen Konzepte erarbeitet und verändert.
- Ausbau transformationsspezifischer rüstungstechnischer Fähigkeiten auf den Gebieten Systemtechnik, Software-Entwicklung, Kommunikationstechnik, Modellierung und Nachweiserbringung.
- Verstärkter Fokus auf Innovation und Weiterentwicklung eng abgestimmt mit den Kunden. Forschung ist heute fundamental wichtig, da Innovation ein treibender Faktor für die militärische Überlegenheit ist.
- Neugestaltung der Zusammenarbeit mit dem militärischen Nutzer mit dem Ziel, technologische Anstöße zu geben und Herstellerwissen und Nutzeranforderungen parallel in die Entwicklungen einfließen zu lassen. Damit kann die Industrie Entwicklungen für potentielle, neue Produkte definieren und starten, um schnelle Lösungen zu bieten.
- Die Industrie muss schnell reagieren und sich auf neuartige Anforderungen, unvorhergesehene Problemstellungen bei den Streitkräften, neue Szenarien und neue Wettbewerbserfordernisse einstellen.
- Interindustrielle und internationale Kooperation zur Lösung komplexer systemtechnischer Aufgaben und zur Erlangung von Interoperabilität im

internationalen Umfeld für den Streitkräfteeinsatz in Koalition mit anderen Nationen.
- Der zu erwartende Minderbedarf von Plattformen muss durch andere Leistungen und Produkte ausgeglichen werden. Software, Forschung und innovative Entwicklungen rücken in den Vordergrund.

Das Umfeld ist durch rüstungsindustrielle Konsolidierung und hohen Wettbewerbsdruck gekennzeichnet. Unter dem Gesichtspunkt der Transformation werden nachfolgend Produkte und Dienstleistungen, rüstungstechnische Fähigkeiten und Zusammenarbeitsfragen mit den Streitkräften und anderen Unternehmen behandelt.

*Produkte und Dienstleistungen*

Die Industrie hat in der Vergangenheit militärische Produkte durch ständige Weiterentwicklung leistungsgesteigert. Daraus resultierte ein als Nachfolgedenken bezeichneter Weg des technischen Fortschritts. Immer bessere Sensoren, Waffen, Panzer, Flugzeuge oder Schiffe wurden entwickelt. Konsequenterweise verfügten einige Unternehmen über Spitzentechnologien im Rüstungsbereich. Kanonen, Munition und Systeme wie der Kampfpanzer Leopard, die Panzerhaubitze 2000 oder Unterseeboote sind Beispiele für internationale Technologieführerschaft.

Die Transformation verdrängt das einzelne Waffensystem wie das Flugzeug oder den Panzer von einem exponierten Platz bei einer Teilstreitkraft in die Position eines Netzwerkknotens. Transformierte Streitkräfte erzielen ihre Wirkung durch den koordinierten Einsatz von Plattformen, Sensoren, Effektoren und Entscheidern. Die optimalen Systemverbunde oder Netzwerke müssen fallweise erzeugt werden. Nach wie vor sind die Leistungsfähigkeit der Plattformen und der Waffen von entscheidender Bedeutung für den Schutz der Soldaten und die Wirkung im Einsatz. Die vernetzte Operationsführung ermöglicht jedoch einen effektiveren Einsatz militärischen Gerätes.

Der zukünftige Rüstungsbedarf der Bundeswehr wird aus dem Fähigkeitsprofil der Streitkräfte abgeleitet. Dieses Fähigkeitsprofil wird durch sechs ineinander greifende Fähigkeitskategorien gebildet:

- Führungsfähigkeit
- Nachrichtengewinnung und Aufklärung
- Mobilität

- Wirksamkeit im Einsatz
- Unterstützung und Durchhaltefähigkeit
- Überlebensfähigkeit und Schutz

Plattformen wie der Schützenpanzer Puma oder der Kampfhubschrauber gehören in die Fähigkeitskategorie „Wirksamkeit im Einsatz", der Wiesel in die Fähigkeitskategorie „Unterstützung und Durchhaltefähigkeit". Die Plattformen sind eine notwendige, aber keine hinreichende Voraussetzung für transformierte Streitkräfte. Aus der Fähigkeitsorientierung folgen neue, in der Tabelle 3 zusammengefasste Aufgabenstellungen für die Industrie.

Das *System of Systems* oder der Systemverbund ist das vernetzte System militärischer Ausrüstung und Infrastrukturen. Ganz unterschiedliche Systeme wie Satellitennavigation, Kommunikation, Fahrzeuge, Flugzeuge, einzelne Sensoren und der Soldat können vernetzt operieren. Der Systemintegrator hat vielfältige systemanalytische Fragestellungen und Schnittstellenprobleme zu lösen und die Funktion des gesamten Systems zu gewährleisten. In der Vergangenheit wurde die Systemintegration industriell nur bis zur Plattformebene wahrgenommen. Voraussetzung für einen qualitativ hochwertigen und umfassenden System of Systems-Ansatz ist die Nutzung der Kernkompetenzen unterschiedlicher Hersteller. Grundvoraussetzung dafür ist die Vereinbarung einer offenen Architektur mit definierten Standard-Schnittstellen, so dass jede Firma ihre Komponenten in das Gesamtsystem einbringen kann.

Die *Konzeptentwicklung und Erprobung* (CD&E) ist ein neuartiger Risiko mindernder Weg zur Lösung komplexer rüstungstechnischer und operativer Fragestellungen. Bekanntlich gibt es für eine Problemstellung oft mitunter völlig verschiedenartige Lösungen. Braucht man beispielsweise ein Produkt bestimmter Eigenschaften an einem vorgegebenen Ort, so kann man es über unterschiedliche Transportwege mit unterschiedlichen Mitteln, wie Bahn, Auto, Flugzeug transportieren oder alternativ an dem Ort des Bedarfes eine Produktionsstätte einrichten. Randbedingungen wie zeitliche Verfügbarkeit, Kosten, Gefährlichkeit, politische Akzeptanz (vgl. Atommülltransporte), Herstellungsmittel, Rohstoffe, Werkzeuge müssen in Systemmodellen miteinander verknüpft werden, um die beste Lösung zu finden. CD&E ist eine neue Lösungsmethodik unter Einbeziehung von Studien und numerischen Modellen bzw. Simulationen.

| **Rüstungstechnischer Bedarf**[36] | **Industrieller Beitrag** |
|---|---|
| System of Systems | • Offene Systemarchitekturen mit Standard-Schnittstellen<br>• Systemintegrator |
| Vernetzung | • Schnittstellen, Netzwerktechnologien, Kommunikations-management, Kommunikationskanäle |
| Konzeptentwicklung (CD&E) | • Technologische Anstöße zur Konzeptentwicklung<br>• Innovative Technologien<br>• Entwurf und Durchführung von Experimenten<br>• Experimentanalyse<br>• Modellierung, Simulation (Simulationswerkbank)<br>• Prototypentwicklung |
| Neue Führungs-systemgeneration | • Übergreifende Führungssysteme auf allen Ebenen<br>• Unterstützung der übergreifenden, militärischen Prozesse (basierend auf den neuartigen Konzepten)<br>• Informationsfilter und Wissensmanagement<br>• Prozessunterstützung zur Durchführung von effektbasier-ten Operationen (Operational Net Assessment, ONA)<br>• Infrastruktur zur Informationsverteilung und verteilten Zusammenarbeit (Common Information Environment, CIE)<br>• Gemeinsames Lagebild (Common Relevant Operational Picture, CROP)<br>• Schnelle Entscheidungen (Datenfusion, Entscheidungshil-fen, Simulation) |
| Nachrichtengewinnung, Aufklärung und Überwachung (ISR) | • Intelligente und neuartige Sensoren<br>• Datenfusion<br>• Auswerteverfahren<br>• Informationsverteilung |
| Präzisionswaffensysteme | • Loiterfähigkeit<br>• Komponente im System of Systems<br>• Zielerfassung und Zielführung |
| Informationsoperationen | • Verfahren und Technik |
| Stabilitätsoperationen | • Angepasste Ausrüstung |
| Kampf gegen Terrorismus | • Systeme zum Schutz und Sicherung von Personen und Einrichtungen |

Tabelle 3: Transformationsrelevante rüstungstechnische Fähigkeiten

[36] Einige in der Tabelle benutzte Begriffe werden weiter unten erläutert.

Das *Operational Net Assessment* (ONA) ist ein wesentliches Kernstück der vernetzten Operationsführung. Voraussetzung für ONA ist eine möglichst umfangreiche Kenntnis über die militärischen, zivilen, sozialen und sonstigen Strukturen eines Gegners. Diese Kenntnisse werden genutzt, um durch wirkungsorientierte Operationen (EBO) mit möglichst geringem Aufwand das militärisch notwendige Ziel zu erreichen. Der Einsatz der Medien gehört mit in diesen Bereich.

*Schnelle Entscheidungen* und schnelles Handeln sind weitere Kernelemente transformierter Streitkräfte. In der Operation selbst müssen die eigenen Handlungszyklen schneller sein als die des Gegners. Aus einer Vielzahl von Daten werden Informationen und Wissen erzeugt. Hierzu sind neuartige Verfahren zur Interoperabilität, Datenfusion und Entscheidungsvorbereitung zu entwickeln.

*Neue Konzepte* sind eine technologische Herausforderung an die Industrie. Sie nutzen in der Regel innovative Technologien. Unbemannte Fluggeräte kleiner Dimensionen (Minidrohnen), der Einsatz von Webcams zur Aufklärung oder unbemannte Fahrzeuge sind hier als Beispiele zu nennen.

*Parallelentwicklungen* entspringen transformationsspezifischen Denkmodellen. Unter Parallelentwicklung wird der militärische Einsatz eines Teilsystems bei weiterlaufender Entwicklung des Gesamtsystems verstanden.

*Nachrichtengewinnung und Aufklärung* sind Schlüsselfähigkeiten transformierter Streitkräfte. Das Konzept der transformierten Streitkräfte beruht auf wirkungsorientierten Operationen mit dem Ziel, die Mittel des Gegners nicht oder nicht hinreichend zur Wirkung kommen zu lassen. Dazu ist eine vollständige und aktuelle Lagekenntnis mit allen relevanten Informationen, nichtmilitärischen eingeschlossen, eine unabdingbare Voraussetzung.

Die Rüstungsindustrie muss demzufolge vorhandene Fähigkeiten durch neue „transformationsgerechte“ Leistungen ergänzen. Mittel- bis langfristig wird das industrielle Leistungsspektrum signifikante Änderungen erfahren. Wie aus Tabelle 3 hervorgeht, werden die Anforderungen auf dem Softwaresektor steigen. Software und Hardware sind jedoch eng miteinander verknüpft. So werden die durch Software unterstützten Systemlösungen wiederum Anregungen zu neuen Hardwarekomponenten liefern. Beispielsweise können militärische Schutzkonzepte alternativ oder in Kombination durch Schnelligkeit, kleinere Signaturen, Täuschen und aktivem Selbstschutz bestehen. Autonome oder halb autonome Systeme zu Lande, zu Wasser und in der Luft werden weitere Innovationsfelder sein.

Die industrielle Basis für transformierte Streitkräfte schließt den Systemintegrator, den Plattformspezialisten, den technologischen Innovator, den Informationsmanager, den Sensorspezialisten und Informationsmanipulator ein. Die veränderten Anforderungen an die Industrie werfen auch industriepolitische Fragestellungen auf, die im Abschnitt „Transformation der Industrie" angesprochen werden.

*Rüstungstechnische Fähigkeiten*

Die Produkte, Dienstleistungen und rüstungstechnischen Fähigkeiten der Industrie müssen an die Anforderungen transformierter Streitkräfte angepasst werden.

Ein Systemverbund von Plattformen, Sensoren und Effektoren hat eine sehr große Zahl von Kombinations- und Wirkungsmöglichkeiten. Der Systemarchitekt oder Systemintegrator (engl., Lead System Integrator, LSI) hat die Aufgabe, eine bestmögliche Lösung für die Herstellung einer militärischen Fähigkeit zu definieren. Seine Rolle, die es bislang in der Wehrtechnik nicht gab, ist in Abbildung 2 veranschaulicht. Oberhalb der Plattformebene (Schiffe, Flugzeuge, Panzer) wurden die Systeme vom Nutzer zusammengeführt. Der Systemintegrator definiert das Gesamtsystem und leitet daraus die Spezifikationen für die Systemkomponenten ab. Er beherrscht komplexe Systemarchitekturen und nimmt Managementfunktionen für den Auftraggeber war. Dazu verfügt der Systemintegrator über ein numerisches Modell des Gesamtsystems und kann die Systemeigenschaften analytisch oder durch Simulation ermitteln. Er kann verbindliche Aussagen über das Verhalten des Gesamtsystems machen. Seine Fähigkeit besteht darin, sehr komplexe und umfangreiche Datenbasen und Modellrechnungen zu beherrschen und daraus die Aufgaben für die Untersystemhersteller zu definieren.

Die Rolle des LSI ist im Rahmen der Entwicklung des Future Combat System (FCS) des amerikanischen Heeres entstanden. Ziel dieses ehrgeizigen und durchaus auch umstrittenen Programms ist es, die Rolle militärischen Großgerätes wie Kampfpanzer durch ein vernetztes System von Land- und Luftfahrzeugen unter Einbeziehung globaler amerikanischer Aufklärungsnetze, Kommunikationsnetze und Terrainmodelle zu ersetzen. Die zum System gehörenden Fluggeräte sind, wie ein großer Teil der Landfahrzeuge, unbemannt. Die Waffenwirkung und den Schutz eines Kampfpanzers durch Kombination kleinerer Systeme zu erzeugen, ist eine große technologische und operative Herausforderung. Die Vernetzung ist das Rückgrat des FCS. Davon ausgehend werden die Eigenschaften der Knoten (Fahr-, Flugzeuge, Sensoren, Waffen etc.) festgelegt.

Daher spricht man in den Vereinigten Staaten auch von Network Centric Warfare, der netzwerkzentrierten Kriegsführung.

Als LSI für das FCS wurde ein Team aus Boeing und SAIC ausgewählt. Boeing konnte die großen Erfahrungen und eine Managementsoftware aus der Entwicklung der B777 als Vorteil gegenüber Mitbewerbern einbringen. Die Lösung des komplexen Systems Verkehrsflugzeug qualifiziert durchaus zur Lösung anderer hochkomplexer Systemaufgaben, denn die Systemabhängigkeiten sind bei einem Flugzeug besonders ausgeprägt. Hierzu ein sehr einfaches Beispiel: Der Energieverbrauch im Heck des Flugzeuges bestimmt den Leitungsquerschnitt, der wiederum die Gesamtmasse mit Folgen für den Schwerpunkt. Der Leitungsquerschnitt darf nicht unnötig überdimensioniert sein, da jedes unnötige Gramm Masse zu Lasten zahlender Nutzlast geht. Ein zu kleiner Querschnitt ist ein Sicherheitsrisiko. Veränderungen im Laufe der Entwicklung haben weitreichende Konsequenzen, nicht nur für den Integrator, sondern auch für verschiedene Unterauftragnehmer. In jeden Entwicklungsschritt sind alle Betroffenen unmittelbar einzubeziehen. Das konnte und kann Boeing bei der Flugzeugentwicklung, und das traut das Pentagon der Firma auch bei der Entwicklung des FCS zu.

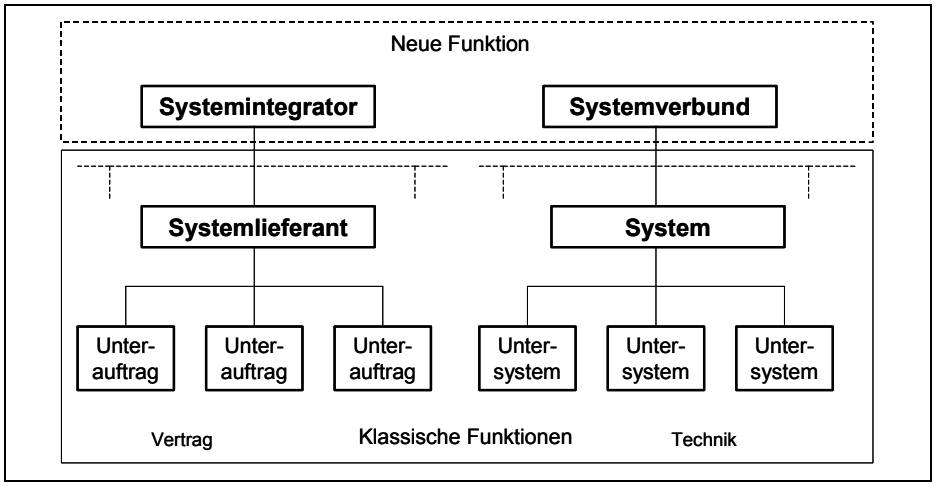



Abbildung 2: Der Systemintegrator ist für die Integration des Systemverbundes verantwortlich

In Europa geht man schon aus Kostengründen weniger radikal vor. Zunächst sollen vorhandene Systeme vernetzungsfähig gemacht und die erforderlichen Kommunikationsmittel beschafft werden. Im Vereinigten Königreich benutzt man daher den Begriff netzwerkgenerierte Fähigkeiten (Network Enabled Capabilities, NEC) und in Deutschland bekanntermaßen vernetzte Operationsführung (NetOpFü). Damit wird auch in Europa eine industrielle Tätigkeit oberhalb der Plattformebene stattfinden. Diese bisher vom militärischen Kunden nicht in Anspruch genommene Fähigkeit hat die Industrie.

Die Rolle der Industrie als Systemintegrator verändert auch die Regeln in der Zusammenarbeit mit anderen Unternehmen und dem Auftraggeber, denn er hat auch Risiken zu übernehmen, die der Plattformhersteller nicht kennt. Die Leistungen einer Plattform können in überschaubarer Weise festgelegt und überprüft werden. Die Fähigkeiten eines Systemverbundes sind dagegen so komplex, dass sie nur durch Versuche und Simulationen in allen Facetten überprüft werden können. Dabei haben die verwendeten Modelle und Simulationen einen Einfluss auf die Bewertung. Die Beseitigung von Leistungsdefiziten in einem komplexen System kann nur durch enge Kooperation der Beteiligten geschehen.

Hier sind fallweise neue Zusammenarbeitsmodelle zu entwickeln. Im zivilen Flugzeugbau gibt es Entwicklungsvorhaben mit Unterauftragnehmern, die das Risiko mittragen. Bei Defiziten haben dann Problemlösungen den Vorrang vor Schuldzuweisungen. Im Sinne der Risikovermeidung wird der Systemintegrator vorzugsweise auf bewährte Unterlieferanten oder eigene Produkte zurückgreifen. Das hat auch rüstungswirtschaftliche Auswirkungen, die unten detaillierter erörtert werden.

Ein weiteres neues und interessantes Tätigkeitsgebiet ist CD&E. Erkannte militärische Fähigkeitslücken können auf unterschiedlichste Weise geschlossen werden. Eine der Möglichkeiten, und darauf wird auch in der neuesten Ausgabe des CPM (Mai 2004) hingewiesen, ist die Nutzung von Ergebnissen aus CD&E. Im CD&E-Prozess werden Konzepte entwickelt und überprüft. Als Mittel werden Seminare, Studien, numerische Modelle, Einzelsimulationen und Simulationen im Verbund mit anderen Simulationen und Hardware eingesetzt. Die Wehrtechnik kennt Entwicklungssimulatoren z.B. für Fahr- und Flugzeuge, und in der zivilen Industrie werden Modellierungs- und Simulationswerkzeuge schon seit geraumer Zeit beispielsweise zur Auslegung komplexer Fertigungseinrichtungen eingesetzt. Auf diese Weise kann vor Beginn von Baumaßnahmen festgestellt werden, ob jedes Teil zur richtigen Zeit am richtigen Ort ist.

Im CD&E-Prozess können die Machbarkeit eines Systems, die Risiken der Herstellung und die Systemwirkung untersucht werden. Die Streitkräfte der USA und der NATO haben das CD&E-Verfahren als neue Vorgehensweise für die Beschaffung von Ausrüstung für die Streitkräfte eingeführt. Das Allied Command Transformation (ACT) führt den NATO CD&E- Prozess. Das Vorgehen durch Konzeptentwicklung und Erprobung liefert über die reine Problemlösung hinaus wichtige Aussagen für die Doktrin, die Führung, die Logistik und andere militärische Sparten.

Die Vorgehensweise über CD&E verlangt rüstungstechnische Fähigkeiten der Industrie auf den Gebieten „Innovative technische Lösungen, Modellierung und Simulation". Die Gebiete Modellierung und Simulation werden von der Industrie schon in weiten Bereichen beherrscht. Das Zuschneiden dieser Fähigkeiten auf die jeweilige Fragestellung und die iterative Konzeptentwicklung in Zusammenarbeit mit dem Kunden sind neuartige Aufgaben für die Industrie.

Simulationen für die vernetzte Operationsführung sind bereits in Funktion gezeigt worden. Die Systemübersicht des Demonstrators der Firma RDE illustriert Abbildung 3. Der Demonstrator ist ein erster Prototyp für ein CD&E-Testbed, bei dem ein Modell zur Simulation von Streitkräften im Sinne von Computer Generated Forces (TacSi®) genutzt und mit mehreren realen Führungssystemen sowie einer Steuereinheit des Luftabwehrsystems ASRAD zusammengeschaltet wurde. Die Teilsysteme agierten dann in einem gemeinsamen, simulierten Szenario.

Der Demonstrator bedient sich einer als „Neue Generation Simulatorkern" (NGS) bezeichneten Infrastruktur. NGS stellt alle grundlegenden Funktionalitäten für ein CD&E-Testbed oder für ein Distributed Continuous Experimentation Environment (DCEE) zur Verfügung. Mit NGS kann aus einer Bibliothek unterschiedlicher Simulationsmodelle die Simulation eines Systemverbundes zusammengeschaltet werden. Die Simulationsmodelle können der vorhandenen Hardware zugeordnet und als ein Gesamtsystem gesteuert werden. Abhängig vom Zweck der Gesamtsimulation können entsprechende Module – z. B. für die Aufzeichnung und Auswertung – eingebunden werden. NGS kann gleichzeitig über HLA, DIS und Corba kommunizieren und besitzt damit Schnittstellen für alle wichtigen Standards zur Interoperabilität mit anderen Simulationssystemen.[37] Über den NATO-Kommunikationsstandard DEM (C2IEDM als Datenmodell), der auch im NGS realisiert ist, können auch reale Führungssysteme direkt an die

[37] HLA: High Level Architecture; DIS: Distributed Integrated Simulation, Corba: Common Object Request Broker Architecture.

Simulation angeschlossen werden.[38] Originalgeräte, insbesondere die „Link-16-Hardware“, lassen sich in die NGS-Simulation einbinden. Der bei der Eurosatory 2004 gezeigte Demonstrator operierte bereits mit einem Hardware-Sensor und -Effektor.

Eine weitere Komponente des Demonstrators ist TacSi®. TacSi® simuliert Streitkräfte selbstständig oder interaktiv (Computer Generated Forces, CGF). Bei der Konfiguration lassen sich Streitkraftstrukturen aufbauen und die zugehörigen Einheiten zusammenstellen. TacSi® simuliert jeden einzelnen Simulationsteilnehmer in Echtzeit inklusive der inneren Zustände. Durch hohe Parametrisierbarkeit der Module ist es möglich, eine große Bandbreite von verschiedenartigsten Szenarien zu simulieren.

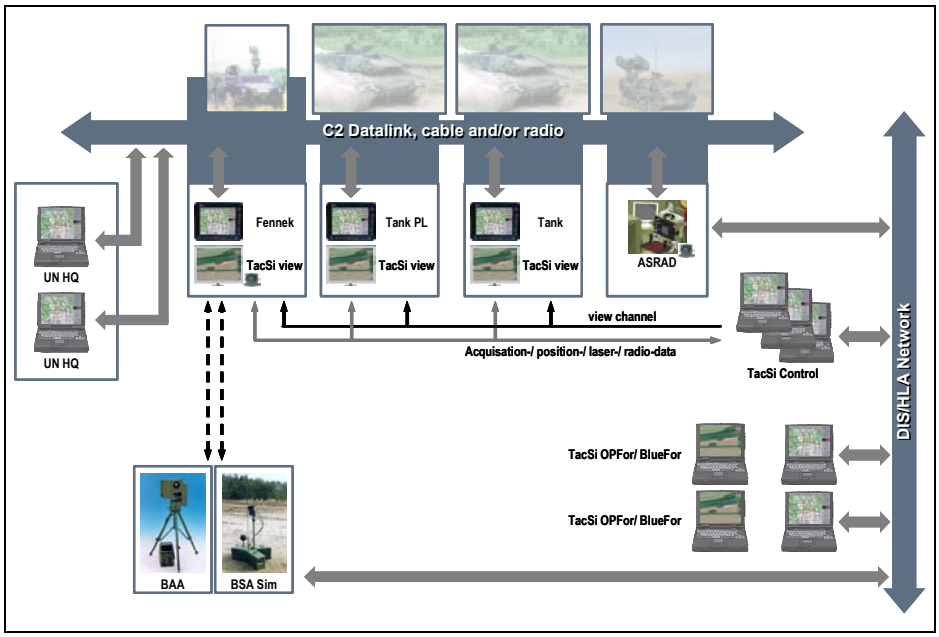



Abbildung 3: Systemübersicht für die Demonstration eines vernetzten Gefechts- und Simulationssystems gezeigt von der Firma RDE auf der Eurosatory 2004

[38] DEM: Data Exchange Mechanism, C2IEDM: Command & Control Information Exchange Data Model

*Zusammenarbeit mit dem militärischen Kunden*

Industrielle Leistungen für transformierte Streitkräfte können nach den bisher praktizierten Zusammenarbeitsregeln bei der Herstellung von Untersystemen und Plattformen nicht erbracht werden. Die Herstellung militärischer Fähigkeiten durch vernetzte Systeme ist nur durch eine vernetzte Hersteller-Kundenbeziehung möglich. Diese Veränderung betrifft einmal die industrielle Auftragnehmer-Unterauftragnehmer-Beziehung und zum zweiten die Zusammenarbeit der Streitkräfte mit der Industrie. Integrierte Kunden-Lieferanten-Teams sind in der Privatwirtschaft nichts Neues und werden in anderen Ländern wie in den USA auch im militärischen Bereich praktiziert.

Transformierte Streitkräfte müssen in der Lage sein, sowohl konzeptionell als auch materiell ohne Verzug auf unerwartete Herausforderungen zu reagieren. Es ist nicht möglich, das Material für alle denkbaren Varianten moderner kriegerischer Auseinandersetzungen bereitzuhalten. Das US-amerikanische Office of Force Transformation fordert die Fähigkeit der Parallelentwicklung von Methoden, Prozessen, Organisationen und Technologien. Was damit gemeint ist, wurde 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. Solche aus einer unmittelbaren militärischen Forderung entstehenden Aufgabenlösungen sind ein Element der Transformation und können nur durch eine „transformierte" Industriebasis erfüllt sowie in enger Zusammenarbeit mit dem Kunden abgewickelt werden.

Die nun notwendige Neugestaltung der industriell-militärischen Zusammenarbeit führt insbesondere in Deutschland zu einer Vielfalt von rechtlichen Problemen mit haushalts-, vergabe-, wettbewerbs-, vertrags- und personalrechtlichen Facetten. Der Schutz geistigen Eigentums ist ein vorherrschendes Problem der Industrie.

## Rüstungswirtschaftliche Fragestellungen

Transformation wird bei der NATO als kontinuierlicher Prozess verstanden und das ist sie auch. Die sicherheitspolitischen und militärischen Herausforderungen durch asymmetrische Gegner werden sich ständig ändern. Entsprechend müssen die militärischen Fähigkeiten unter Berücksichtigung technischer und technologischer Fortschritte weiterentwickelt werden. Analysen und die Weiterentwicklung des Systems Streitkräfte sind die Antwort auf die dynamische Bedrohung

der westlichen Industrienationen. Fähigkeitsanpassungen werden überwiegend durch neue Architekturen, veränderte Komponenten, Software und neue Einsatzkonzepte erzielt. Daraus resultiert eine neue Geschäftsgrundlage für die Industrie: 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 aufrechterhalten oder zu entwickeln sind.

Die VPR weisen auf die Notwendigkeit des Erhalts technologischer Kernfähigkeiten als Voraussetzung für die internationale Kooperationsfähigkeit hin. Die Industrie wird sich unter Berücksichtigung nationaler Prioritäten und der Einflüsse seitens NATO und EU mit der Frage befassen, welche Technologien und Fähigkeiten unter Beachtung betriebswirtschaftlicher Kriterien erhalten werden können. Transformationsfähige Technologien liegen nicht in der Schublade. In den USA werden in das Thema Transformation derzeit hohe dreistellige Millionenbeträge investiert, die im Fiskaljahr 2005 auf über eine Milliarde steigen werden. Schweden entwickelt in einem vor drei Jahren begonnenen und auf zehn Jahre angelegten Programm Technologien für netzwerkgestützte Operationen und damit für transformierte Streitkräfte. Die derzeitige nationale Budgetlage ermöglicht die Streitkräftetransformation nur in Teilbereichen. Die Industrie wird das Vorgehen des Bundesverteidigungsministeriums einerseits und das der NATO/EU andererseits als Wegweiser für rüstungswirtschaftliche Weichenstellungen nutzen.

*Rüstungswirtschaftliche Relevanz des CD&E-Prozesses*

Die Bundesrepublik hat sich zu einer Beteiligung an der NATO Response Force (NRF) verpflichtet. Die NRF ist eine transformierte Streitkraft. Die VPR legen fest, dass Einsätze der Bundeswehr, von Evakuierungsmaßnahmen abgesehen, nur gemeinsam mit Verbündeten durchgeführt werden und dass Rüstungskooperation im transatlantischen und europäischen Rahmen den Vorrang hat. Zudem sollen deutsche Streitkräfte auch im Rahmen von EU-Missionen eingesetzt werden. Die EU hat dazu das Konzept der Battle Groups entworfen. Die rüstungstechnischen und Ausrüstungsprobleme sollen im Rahmen des European Headline Goal (EHG) gelöst werden.

Diese politischen Vorgaben und die Streitkräftetransformation haben industriepolitische Konsequenzen. Der Bündniseinfluss engt die nationalen rüs-

tungstechnischen und -politischen Gestaltungsmöglichkeiten ein. Das wird die Festlegung des Rüstungsbedarfs stark beeinflussen. Zukünftige Streitkräftefähigkeiten, die im Rahmen von CD&E entwickelt werden, werden durch NATO-Gremien gebilligt. Damit entsteht eine indirekte Abhängigkeit der deutschen Rüstungsindustrie von Entscheidungen der NATO.

Im Mai 2004 ist eine neue Ausgabe der Verfahrensbestimmungen für die Bedarfsermittlung und Bedarfsdeckung in der Bundeswehr erschienen. Darin wird ausdrücklich auf die Berücksichtigung von Ergebnissen aus dem CD&E-Prozess hingewiesen. Die Industrie muss sich daher in diesen Prozess einbringen. Hier sind von Seiten der Amtsseite noch wichtige Fragen zu klären. Der CD&E-Prozess ist kein Beschaffungsprozess nach dem mittlerweile obsoleten Wehrmaterialentstehungsgang sondern ein iterativ gestalteter Entwicklungsprozess, der durchaus als lernendes System verstanden werden kann. Firmen, die am CD&E-Prozess mitgewirkt haben, dürfen keinen Restriktionen bei einer Beschaffung unterliegen, weil man auf wertvolle Systemkenntnisse verzichten würde und ein wesentlicher Aspekt des CD&E damit konterkariert würde.

Die europäischen Nationen, die Mitglieder in der NATO und der EU sind, werden dem Prinzip des Single Set of Forces folgend die gleichen Streitkräftekontingente je nach Bedarfslage der NATO oder der EU zur Verfügung stellen. Das Tempo, das die NATO beim Aufbau und der Zertifizierung der NRF vorlegt, kann die EU nicht mithalten. Rüstungswirtschaftliche Einflüsse durch die EU sind im Zusammenhang mit der Transformation bereits durch Betrachtung der NATO-Einflüsse abgedeckt. Daran wird auch die Einrichtung der europäischen Rüstungsagentur, die gemäss aktueller Planung nur über geringe Budgetmittel verfügen soll, auf mittlere Sicht nichts ändern.

Aus Industriesicht ist daher die Verbindung zum ACT unverzichtbar, um die rüstungswirtschaftlichen Auswirkungen des CD&E-Prozesses beurteilen zu können. Da der NATO CD&E-Prozess noch neu ist, muss die Industrie derzeit Wege finden, wie sie sich effektiv in diesen Prozess einbringen kann und damit an der Weiterentwicklung der im Bündnis operierenden Streitkräfte beteiligt bleibt.

*Auswirkungen des CPM (Customer, Product, Management)*

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 Fähigkeitsorientierung führt zu einem von oben nach unten gerichteten Ablauf, wie er durch den CPM festgelegt wird. Der Generalinspekteur ist im Rahmen seiner Gesamtverantwortung für die bundeswehrübergreifende Fähigkeitsanalyse, für die Schwerpunktsetzung, die Weiterentwicklung der Bundeswehr, die zentrale Bedarfsermittlung und für die Einsatzfähigkeit der Streitkräfte verantwortlich. Aus einer festgestellten Fähigkeitslücke werden Systemfähigkeitsforderungen und daraus schließlich funktionale Forderungen hergeleitet. Diese werden durch einen Hauptauftragnehmer in Wehrmaterial umgesetzt. Hierzu hat nach der neuesten Ausgabe des CPM die Industrie u.a. den Nachweis der Herstellbarkeit eines die funktionalen Forderungen unter realen Bedingungen erfüllenden, künftigen Produktes zu erbringen. Der Hauptauftragnehmer hat damit die Systemverantwortung und trägt das Risiko für die Erfüllung der Leistungen. Seine übergeordnete Verantwortung für die Herstellung der mit dem Auftraggeber vereinbarten Leistungen und Fähigkeiten gibt ihm notwendigerweise die Freiheit zur Auswahl von Lösungswegen und damit auch von Unterauftragnehmern.

Damit kann der militärische Kunde nur noch in Ausnahmefällen auf die Auswahl von Unterauftragnehmern Einfluss nehmen. Der Hauptauftragnehmer muss zur Minderung seines Risikos freie Hand bei der Auswahl der Unterauftragnehmer haben, denn der Kunde wird schwer beurteilen können, welche Auswirkungen die Eigenschaften eines von ihm gewollten Untersystems auf die Funktionalität des Gesamtsystems haben. Durch diesen Freiraum ist es dem Hauptauftragnehmer möglich, in Grenzen Industriepolitik zu gestalten. Mittelbis langfristig kann dies eine vertikale industrielle Integration zu Folge haben.

Generell verlagert der CPM Risiken vom Auftraggeber zum Auftragnehmer. Eine Plattform oder ein System sind technisch spezifizierbar. Eine Systemleistung ist wesentlich schwieriger eindeutig festlegbar. Große Firmen werden hier einfacher mit den Risiken umgehen können.

**Transformation der Industrie**

Wie dargestellt, muss die Rüstungsbasis für transformierte Streitkräfte ein breites Spektrum von Fähigkeiten und Leistungen zur Verfügung stellen. Nur große Unternehmen können die Ressourcen für eine Abdeckung des gesamten Spektrums aufbringen. Kleinere Unternehmen werden ihre strategischen Positionen

neu überdenken müssen, da das Geschäftsmodell „Entwicklung-Serie“ nicht mehr die Regel, sondern vielfach die Ausnahme sein wird.

Die klassische Rüstungsplanung ist bekanntermaßen durch lange Entwicklungszeiten gekennzeichnet. Die Streitkräftetransformation ist eine Auswirkung der Revolution in militärischen Angelegenheiten (RMA). Transformierte Streitkräfte erwarten und benötigen schnelle Ergebnisse von der Industrie. Die Industrie muss hier Strukturen schaffen, die schnelle Reaktionen erlauben.

Der Übergang zu transformierten Streitkräften hat, wie oben dargestellt, einen veränderten Ausrüstungsbedarf, andere Programmstrukturen und andere Laufzeiten zur Folge. Die Industrie kann der Notwendigkeit zur Erwirtschaftung von Gewinnen nur nachkommen, wenn sie den erforderlichen Strukturwandel und die verlangten Fähigkeitsänderungen aufgrund rechtzeitig bekannter Planungen einleiten kann.

Die Überführung der primär plattform- und komponentenorientierten Technologiebasis in eine transformationsorientierte ist kein Selbstläufer und muss in einer zwischen Auftraggeber und Auftragnehmer koordinierten Weise geschehen. Die aus der Vergangenheit stammenden, derzeit laufenden oder anlaufenden Vorhaben sind die, wenn auch schwache, Lebensader der Rüstungsindustrie, die es zu erhalten gilt, bis transformationsspezifische Aufgaben hinreichend sichere Planungsdaten für die Industrie liefern.

Der Transformationsprozess ist durch hohe Dynamik gekennzeichnet. Eine durch stabile Strukturen und festgelegte Regelwerke definierte Auftraggeber-Auftragnehmer-Beziehung wird sich nicht so bald einstellen. Eine wesentliche Eigenschaft der Transformation ist gerade die ständige Veränderung. Das Militär und die Industrie sind gehalten, neue Formen des Informationsaustausches und der Zusammenarbeit zu etablieren.

Transformation ist nicht allumfassend. Über viele Jahre wird auch das klassische Rüstungsmaterial 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.

## Zusammenfassung

Transformierte Streitkräfte stellen militärische Überlegenheit durch Vernetzen von Informationen, Wissen und militärischer Ausrüstung her. Dies hat Auswirkungen u.a. auf die Ausrüstung der Streitkräfte und die von der Industrie zu

erbringenden Leistungen. Die Transformation ist ein andauernder Prozess und kann nur in enger Kooperation von Auftraggeber und Auftragnehmer vollzogen werden. Anstelle von physikalischen Plattformspezifikationen werden Auftragnehmerleistungen vielfach durch Fähigkeitskriterien festgelegt. Der Systemintegrator ist eine neue Rolle für die Industrie. Die industrielle Aufgabe als Lieferant und Dienstleister transformierter Streitkräfte ist einerseits mit wirtschaftlichen Risiken verbunden, birgt aber andererseits auch sehr große Chancen für neue Arten der industriellen Wertschöpfung. Die große Aufmerksamkeit, die die Transformation derzeit erfährt, darf nicht darüber hinwegtäuschen, dass klassisches Rüstungsmaterial, wenn auch in verringerten Stückzahlen, zum Bedarf des Militärs gehört und die Industrie auch hier weiterhin eine Aufgabe hat.

René Eggenberger und Heiko Borchert*

# Wissenschaft und Technologie in der Schweizer Armee

Wissenschaftlich-technischer und militärischer Fortschritt sind traditionell aufs Engste miteinander verknüpft. Die rüstungstechnologischen Kompetenzen spielen eine entscheidende Rolle, um die militärische Ausrüstung entwickeln, produzieren, unterhalten und an veränderte Gegebenheiten anpassen zu können. Daneben gewinnt das wissenschaftliche Know-how immer mehr an Bedeutung. Da Streitkräfte heute immer stärker im internationalen Umfeld zur Krisenprävention und zum Krisenmanagement eingesetzt werden, sind verstärkte und thematisch weiter gefasste Analyse- und Planungskapazitäten gefragt. Ebenso stehen Streitkräfte unter einem erheblichen Spardruck, was die Nachfrage nach ökonomischen Ansätzen im Umgang mit knappen Mitteln erhöht.

Die wissenschaftlich-technischen Kompetenzen der Schweizer Streitkräfte konzentrierten sich bislang vor allem auf die technischen Felder. Geisteswissenschaftliche Kompetenzen hatte man sich zwar auch angeeignet. Allerdings beschränkte sich der Erwerb auf punktuelle Bereiche wie beispielsweise militärsoziologische, pädagogische, militärhistorische, militärrechtliche oder militär- bzw. fliegerärztliche Untersuchungen. Im Gesamtkontext aller militärischen Anstrengungen konzentrierten sich die Bemühungen – bei geringer themenübergreifender Koordinierung oder Synergienutzung – bislang auf den eigenen Verantwortungsbereich der Beteiligten. Wissenschaft und Technologie (W+T) wurde deshalb eher unsystematisch und vor allem Bottom Up betrieben, was Duplizierungen und fallweise Mehrfachfinanzierungen zur Folge hatte. Zudem erschwerten das Fehlen eines gemeinsamen W+T-Verständnisses sowie der Mangel an einheitlichen Prozessen und Instrumenten die systematische Erhebung des W+T-Bedarfs der Streitkräfte und die zuverlässige Erfassung der dafür eingesetzten personellen und finanziellen Mittel.

Vor dem Hintergrund des Sicherheitspolitischen Berichts 2000 und des neuen Armeeleitbildes hat der Verwaltungsbereich Verteidigung im Eidgenössischen Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) den Ist-Zustand seiner W+T-Aktivitäten systematisch erhoben, ausgewertet und be-

* Die Autoren danken Rudolf Hüppi, Ivano Marques und Mauro Mantovani, die als Mitglieder der Kerngruppe wesentlich zur Erarbeitung der Konzeptionsstudie „Wissenschaft und Technologie des VBS für die Armee“ (Bern: Planungsstab der Armee, 2002) beigetragen haben.

urteilt. Die Konzeptionsstudie „Wissenschaft und Technologie des VBS für die Armee“ definiert die neuen inhaltlichen und strukturellen Grundlagen für die Umsetzung der W+T-Bemühungen. W+T wird dabei bewusst breit interpretiert,[39] um den neuen Erfordernissen gerecht zu werden und die Vielfalt der unterschiedlichen Tätigkeiten abzudecken. Drei Leitideen charakterisieren den neuen Ansatz:

- Der W+T-Bedarf der Streitkräfte wird konsequent aus den strategischen, prospektiven Vorgaben abgeleitet (Top Down-Philosophie).
- Zu diesem Zweck wird ein W+T-Prozess umgesetzt, der systematisch in den Hauptprozess der Streitkräfte- und Unternehmensentwicklung[40] eingebunden ist.
- Inhaltlich wird W+T konsequent fähigkeitsorientiert geplant und über integrierte Projektteams (IPT), die Bedarfsträger und Bedarfsdecker zusammenbringen, bedarfsorientiert geführt.

**Systematische Erhebung des W+T-Bedarfs:**
**Von der Sicherheitspolitik zu W+T Kompetenzen der Streitkräfte**

Um die von der Sicherheitspolitik geforderten Leistungen zu erbringen, benötigen die Schweizer Streitkräfte spezifische Fähigkeiten, die durch wissenschaftlich-technische Kompetenzen aufgebaut und sichergestellt werden müssen. Dabei wird generell zwischen zwei verschiedenen Formen von Kompetenzen unterschieden. Erstens werden Fachkompetenzen durch gezielte Investitionstätigkeiten des VBS langfristig sichergestellt. Zweitens wird die Kompetenz, Produkte und Dienstleistungen zu erbringen, in denjenigen Bereichen aufgebaut, denen eine strategische Bedeutung beigemessen wird. Diese basieren auf den erworbenen W+T-Kompetenzen. Folgendes Beispiel illustriert die unterschiedli-

[39] Die Weisung über den Ausschuss für Wissenschaft und Technologie im Eidgenössischen Departement für Verteidigung, Bevölkerungsschutz und Sport übernimmt diese Interpretation sinngemäß: „Wissenschaft und Technologie (W+T) im Sinne dieser Weisungen umfasst alle Tätigkeiten mit der Zielsetzung, mittels Forschung, Wissensmanagement und anderen wissenschaftlichen Mitteln und Methoden zu Erkenntnissen zu gelangen, die den Entscheidungsprozess und die Aufgabenerfüllung auf allen Stufen des Departementes erleichtern und verbessern.“

[40] Am Kopf dieses umfassenden Prozesses steht der Weißbuchprozess. Im Rahmen der Erarbeitung des Weißbuches der Streitkräfte im Sinne des Antrags des Chefs der Armee an den Departementschef VBS erfolgen sowohl die Analyse des für W+T maßgebenden Umfeldes als auch die Ausarbeitung der W+T-Strategie.

chen Komponenten des gewählten W+T-Verständnisses: Im Rahmen der politischen Vorgaben soll der Verwaltungsbereich Verteidigung in einem definierten Umfeld u.a. Beiträge zur internationalen Friedensunterstützung und Krisenbewältigung erbringen. Diese sind in Form von Aufträgen an die Streitkräfte, den daraus abgeleiteten Aufgaben sowie den erwarteten Leistungen definiert. Zu diesem Zweck müssen die Streitkräfte bestimmte Fähigkeiten wie u.a. Nachrichtengewinnung, Aufklärung und Überwachung, Mobilität, Logistik etc. besitzen, die es erlauben, einen solchen Auftrag vorzubereiten und umzusetzen. Um diese Fähigkeiten bereitzustellen, sind wissenschaftlich-technische Kompetenzen erforderlich. Im Falle der Nachrichtengewinnung, Aufklärung und Überwachung geht es beispielsweise um Aspekte der Informationstechnologie, der Sensorik, der Optronik und Informationsverarbeitung, der Telematik, der Navigation etc. Diese Kompetenzen werden als W+T-Felder bezeichnet. Sie werden abgestimmt auf die sicherheitspolitische Lage und die definierten Aufträge im Rahmen eines festgelegten W+T-Prozesses (Abbildung 5) systematisch identifiziert, definiert und bewirtschaftet.

Die W+T-Kompetenzen des Verwaltungsbereichs Verteidigung tragen dazu bei, die zur Auftragserfüllung erforderlichen Grundlagen systematisch zu erarbeiten und den wirkungsorientierten Einsatz der Mittel zu gewährleisten. Im streitkräfteplanerischen Sinne leisten die W+T-Kompetenzen einen Beitrag, um die Fähigkeit zur umfassenden Analyse der Entwicklungen im sicherheitspolitisch und technologisch relevanten Umfeld zu verbessern und die Fähigkeit zu pro-aktivem Handeln durch den Ausbau der Früherkennung und der Prospektive zu stärken. Dies wiederum ermöglicht es, auf wissenschaftlicher Grundlage die Maßnahmen zur Anpassung der Aufträge der Armee, ihrer Doktrin, ihrer Prozesse und ihrer Strukturen frühzeitig erkennen und vorschlagen zu können. Damit werden der Grundstein für die systematische und bedarfsorientierte Planung der Streitkräfte gelegt, die notwendigen Beiträge zur materiellen Sicherstellung gewährleistet sowie die Grundlagen und Inhalte für die zukunftsorientierte Aus- und Weiterbildung definiert und entwickelt. Mit Blick auf die Zukunft dürften die Streitkräfte auch befähigt werden, bestehende nationale und internationale Kooperationsmöglichkeiten besser wahrzunehmen bzw. neue Kooperationsmöglichkeiten systematisch aufzubauen.

**W+T-Prozess**

Die aktuelle Reform der Schweizer Streitkräfte folgt der Idee der Prozessorientierung als Schlüsselansatz zur Leistungsverbesserung von Organisationen. Die-

ses Vorgehen soll dazu beitragen, das Produkt „Sicherheit und Stabilität" konsequent auf den wirklichen Bedarf auszurichten, die wertschöpfenden Tätigkeiten systematisch aufeinander abzustimmen und dadurch die permanente Weiterentwicklung der Streitkräfte zu ermöglichen. Im Rahmen der Streitkräfteentwicklung (Abbildung 4) werden die Vorgaben in die Bereitschaftserstellung und in die „Produktion" der Einsätze bzw. der Leistungen umgesetzt. Wissenschaft und Technologie kommt in diesem Zusammenhang – analog der Rolle der Doktrin – die Funktion einer konzeptionellen Klammer und einer Teilstrategie zu, die auf der Basis der Streitkräftemodelle und der Joint Vision wesentliche Grundlagen für die übrigen Teilstrategien, die mittel- und langfristige Streitkräfte- und Unternehmensentwicklungsplanung sowie die nachfolgenden Planungsschritte definiert.

Wissenschaft und Technologie folgt der Top Down-Philosophie und wird künftig in einem vier Schritte umfassenden Prozess geplant, gesteuert und umgesetzt (Abbildung 5). Ausgangspunkt des W+T-Prozesses – und damit der erste Schritt – ist die eingehende Situationsanalyse, die gleichzeitig die Grundlage der Streitkräfte- und Unternehmensentwicklung darstellt. Auf der Basis der aus den Streitkräftemodellen abgeleiteten Joint Vision werden in einem zweiten Schritt die W+T-Vision sowie die W+T-Strategie definiert. Letztere identifiziert den W+T-Bedarf des Verwaltungsbereichs Verteidigung, benennt und priorisiert die W+T-Felder (Kompetenzen) und definiert im Rahmen des W+T-Plans, mit welchen Zielen die unterschiedlichen Fähigkeiten bearbeitet werden sollen. Im Zentrum des dritten Schritts steht die operative Umsetzung des W+T-Plans durch die Leistungserbringer, die sowohl inner- als auch außerhalb des VBS bzw. der Bundesverwaltung angesiedelt sein können. Die erzielten Ergebnisse werden im vierten Schritt konsequent auf ihre Wirkung überprüft. Die projektspezifische Evaluation wird auf der Stufe des Verwaltungsbereichs Verteidigung konsolidiert, um daraus Konsequenzen für die Modifizierung bzw. Beibehaltung des W+T-Bedarfs sowie des W+T-Plans abzuleiten.

Abbildung 4: Hauptprozess Streitkräfte- und Unternehmensentwicklung gemäß Prozessmodell Armee XXI

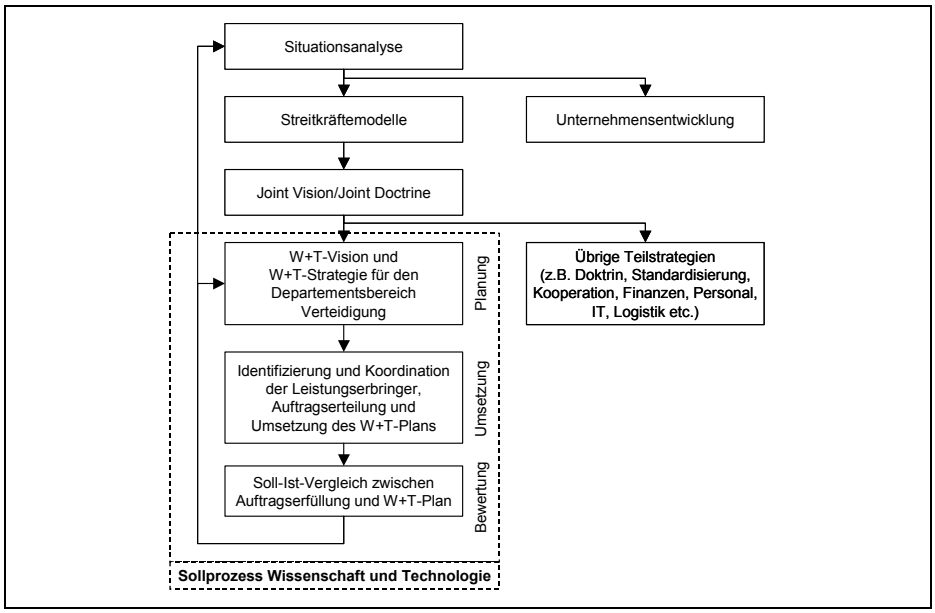



Abbildung 5: W+T-Sollprozess für den Verwaltungsbereich Verteidigung

*Analyse*

Die Situationsanalyse untersucht in enger Zusammenarbeit mit den relevanten Organisationen die politisch-militärischen Vorgaben, die Entwicklungen im maßgebenden Umfeld sowie eigene und fremde (Einsatz-)Erfahrungen (Lessons Learned). Daraus ergeben sich Schlussfolgerungen für die Bedeutung der erforderlichen Fähigkeiten des Verwaltungsbereichs Verteidigung sowie die notwendigen W+T-Felder (Kompetenzen). Da bislang eine systematische Definition der erforderlichen Fähigkeiten des Verwaltungsbereichs Verteidigung fehlte, wurde diese erstmals durch die erwähnte Konzeptionsstudie erarbeitet. Dieser bewusst gewählte, fähigkeitsorientierte Ansatz bietet den Vorteil, dass er sich unmittelbar am Leistungsprofil des Verwaltungsbereichs Verteidigung orientiert und gleichzeitig für alle Beteiligten eine „unité de doctrine" sicherstellt. Zudem ist er dynamisch und erlaubt die systematische Entwicklung der Streitkräfte, während der klassische, an einem konkreten Bedrohungsbild ausgerichtete Ansatz statisch ist und sich lediglich auf ein punktuelles, möglicherweise nie eintretendes Ereignis ausrichtet. Im Sinne einer Startkonfiguration wurden die in Abbildung 6 dargestellten elf Fähigkeitskategorien, die jeweils artverwandte Fähigkeiten zu einer Gruppe zusammenfassen, identifiziert: Von zentraler Bedeutung sind die

Fähigkeiten in den Bereichen der Führung (C4), Informationsgewinnung, Aufklärung und Überwachung (links oben), gefolgt von den Fähigkeiten, die der systematischen Weiterentwicklung des Verwaltungsbereichs Verteidigung dienen (links unten). Personalrekrutierung und Ausbildung spielen vor allem im Zusammenhang mit den zentralen Fähigkeiten (links oben) eine Rolle, während die übrigen Bereiche (rechts oben) eher von nachgeordneter Bedeutung sind.

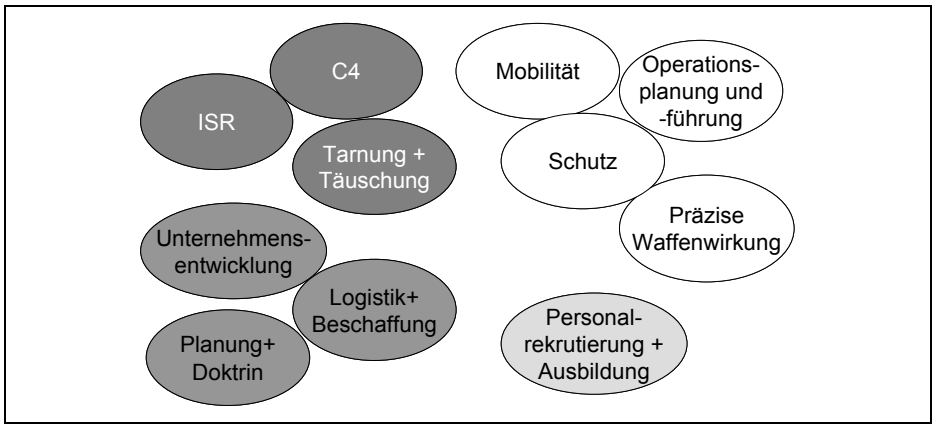



Abbildung 6: Fähigkeitskategorien der Schweizer Armee

*Vision*

Anhand der Situationsanalyse werden die W+T-Bemühungen in der W+T-Vision und der W+T-Strategie präzisiert. Der W+T-Vision kommt die Bedeutung einer Grundsatzerklärung zu, die abgestimmt auf die langfristigen Planungsrhythmen der Prospektive periodisch überarbeitet wird. Sie lautet:

> Die Streitkräfte der Zukunft müssen in der Lage sein, Veränderungen der Umfeldbedingungen abzuschätzen bzw. auf solche flexibel zu reagieren. Dies setzt die Fähigkeit voraus, doktrinale Vorgaben, die Aus- und Weiterbildung, die Rekrutierung sowie die Ausrüstung und Materialbeschaffung rasch anzupassen. Wissenschaft und Technologie tragen dazu bei, diese Veränderungen zu erfassen und zu beurteilen sowie die daraus resultierenden Maßnahmen ableiten und beschließen zu können. Wissenschaft und Technologie unterstützen den Verwaltungsbereich Verteidigung darin, seine Leistungen jederzeit auftrags- und lagekonform zu erbringen.

*Strategie*

Die W+T-Strategie stellt sicher, dass der Verwaltungsbereich Verteidigung die zur Auftragserfüllung erforderlichen wissenschaftlichen und technischen Kompetenzen erhält. Die Strategie wird in drei Schritten konkretisiert: Zuerst wird der W+T-Bedarf bestimmt. Dieser ergibt sich aus den Aufträgen, die der Verwaltungsbereich Verteidigung erfüllen muss, und wird über die in Abbildung 6 dargestellten Fähigkeitskategorien definiert. Auf dieser Grundlage können in einem zweiten Schritt die W+T-Felder identifiziert werden. Diese sind dynamisch definiert, d.h. neue Erkenntnise können zu Schwergewichtsverlagerungen führen. Im Sinne einer Ausgangslage wurden bislang 28 W+T-Felder ermittelt (Abbildung 7).

- ABC-Schutz
- Ausbildungstechnologie
- Autonome intelligente Systeme
- Ballistik
- Elektromagnetische Verträglichkeit, Elektromagnetischer Puls
- Elektronik
- Expolsivstoffe und Pyrotechnik
- Informationstechnologie und Computerwissenschaft
- Kommunikationstechnologie
- Luftfahrttechnik
- Medizin, Sport und Ernährung
- Mikrotechnik
- Munition
- Navigation
- Philosophie und Geschichte
- Politikwissenschaft
- Psychologie und Soziologie
- Raumfahrttechnik
- Schutzbautechnik
- Schutztechnik
- Sensortechnologie
- Signaturenmanagement
- Systemanalyse
- Terramechanik
- Umweltwissenschaft
- Waffentechnik
- Werkstofftechnik
- Wirtschafts- und Verwaltungswissenschaft

Abbildung 7: W+T-Felder der Schweizer Armee (alphabetische Reihenfolge)

Die W+T-Felder werden anschließend priorisiert. Maßgeblich dafür sind die Bedeutung eines W+T-Feldes für die Sicherstellung der Fähigkeiten und seine inhaltliche Verknüpfung mit anderen W+T-Feldern („Multiplikatoreffekt“). Als Beispiele für die Gewichtung nach Bedeutung sei hier auf die Sensorik- oder Kommunikationstechnologie hingewiesen, wenn man an Fähigkeiten im

C4ISTAR-Bereich[41] denkt. Als typische Multiplikatoren mögen die Elektronik, Informationstechnologie oder Werkstofftechnik stehen, da diese Kompetenzen in beinahe allen Bereichen zu effizienteren und leistungserhöhenden Lösungen für bestimmte Fähigkeiten beitragen. Die Resultate werden in fähigkeitsspezifischen „Radarbildern" dargestellt (Abbildung 8).

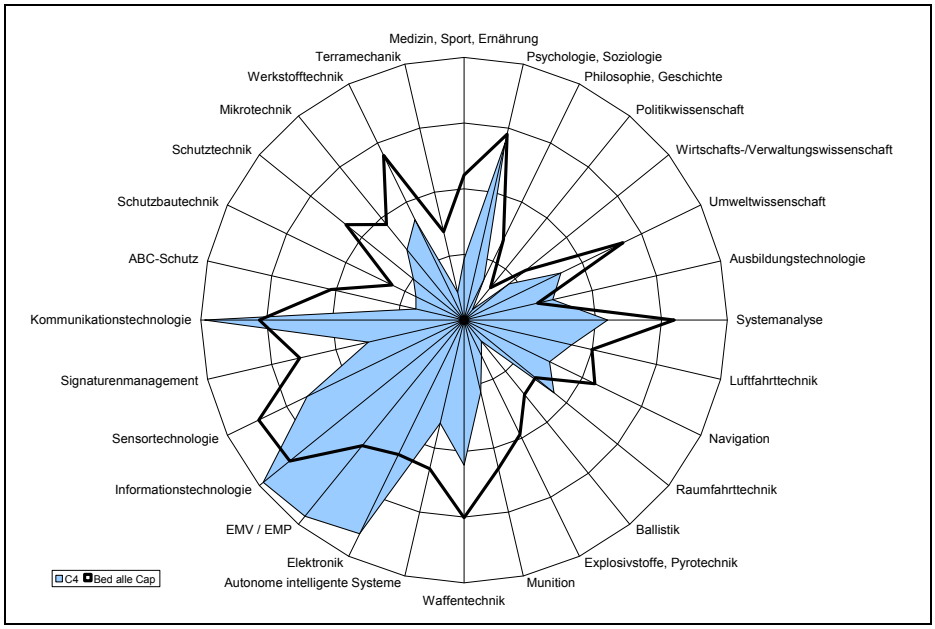



Abbildung 8: W+T-Felder für die Nachrichtengewinnung, Überwachung und Aufklärung

Interpretation: Die graue Fläche kennzeichnet die Bedeutung der W+T-Felder für die spezifische Fähigkeit; die schwarze Linie verdeutlicht die Bedeutung der W+T-Felder für alle Fähigkeiten. Die Differenz gibt an, ob ein W+T-Feld von einer Fähigkeit über- oder unterdurchschnittlich stark beansprucht wird. Die Nachrichtengewinnung ist u. a. überdurchschnittlich stark auf Informations- und Kommunikationstechnologie, jedoch in geringerem Ausmaß auf Waffentechnik oder Ballistik angewiesen.

Der dritte Schritt besteht schließlich darin, die bisherigen Aussagen im Rahmen des W+T-Plans zu konkretisieren. Dieser beschreibt umfassend, mit welchen Zielen die elf Fähigkeitskategorien (Abbildung 6) bearbeitet und wel-

[41] Command, Control, Communications, Computers, Intelligence, Surveillance, Target Acquisition, and Reconnaissance.

che W+T-Felder dazu in welcher Form benötigt werden. Daher bildet er als zentrales Arbeitsdokument auch die Grundlage für die Definition der Leistungsaufträge zwischen Bedarfsträger und Bedarfsdecker. In der Folge sollen die Aussagen des W+T-Plans anhand der für die vernetzte Operationsführung zentralen Fähigkeitskategorie Nachrichtengewinnung, Überwachung und Aufklärung kurz illustriert werden.

Inhaltlich geht es bei der Nachrichtengewinnung, Überwachung und Aufklärung um die Abstimmung aller dazugehörenden Aufgaben im Einsatzbereich der Streitkräfte über alle Führungsebenen hinweg. Die Kommandanten und Stabsoffiziere sollen zur richtigen Zeit, am richtigen Ort, in der erforderlichen Qualität über ein aktuelles, teilstreitkräfteübergreifendes Lagebild verfügen. Diese Fähigkeit setzt neben den Investitionen in die erforderlichen technischen Systeme auch voraus, dass diese von der Daten- und Informationssammlung, über die Auswertung, die Verteilung und die Verarbeitung bzw. Integration in die Entscheidungsabläufe reibungslos zusammenwirken können, um auf Umfeldveränderungen rasch reagieren zu können. Das Zusammenspiel von Nachrichtengewinnung, Überwachung und Aufklärung ist allerdings nicht nur eine Frage der Technologie. Gerade in multinationalen Einsätzen spielen darüber hinaus doktrinale, strukturelle und kulturelle Unterschiede in der Führung militärischer Verbände sowie spezifische Aspekte an der politisch-militärischen Nahtstelle (z.B. politischer „Durchgriff" auf die Nachrichtengewinnung, politische Entscheidungskompetenz im Rahmen der Zielidentifizierung) eine besondere Rolle. Auf der Ebene des einzelnen Kommandanten, Stabsoffiziers oder Stabsgehilfen sind die Form, in der Resultate präsentiert werden sollen, das Vertrauen in die zur Verfügung gestellte Technologie sowie die praktische Handhabung der Mittel von zentraler Bedeutung (Human Interface).

Was die Schwerpunkte betrifft, sollen in erster Linie vier Felder bearbeitet werden:

- Konzeptionelle Abklärungen sollen darlegen, wie die aktuellen Defizite auf der strategischen Stufe behoben werden können. Lösungsansätze zur verstärkten Integration oder zum Einsatz technischer Systeme sollen auf ihre Machbarkeit sowie ihre Chancen und Risiken untersucht werden.
- Auf der operativ-taktischen Stufe sind die Voraussetzungen für die technische und doktrinale Interoperabilität zu schaffen; dabei ist den Zusammenhängen zwischen Nachrichtengewinnung, Überwachung und

Aufklärung sowie Kommunikation und Mobilität besondere Bedeutung zu schenken. Soweit erforderlich sind Anpassungen im Bereich der Doktrin bzw. der Führungsstrukturen und -abläufe vorzunehmen.

- In den Bereichen Konzeption und Doktrin geht es darum, die internationale Entwicklung zu verfolgen (Monitoring) sowie die Konsequenzen und den Handlungsbedarf für die Schweizer Armee aufzuzeigen. Das besondere Interesse gilt dabei den Anforderungen, die aus unterschiedlichen doktrinalen Ansätzen wie der Information Dominance (z.B. USA) bzw. der Information Superiority (z.B. Großbritannien) resultieren.
- Abgestimmt auf die Frage, welcher Sensor zu welcher Zeit mit welchem Zweck zu wessen Gunsten welche Information liefert, geht es schließlich auf der technischen Ebene darum, das Sensornetzwerk in die vorhandene Führungs- und Kommunikationsinfrastruktur zu integrieren und das Sensormanagement (inklusive Sensorfusion) mit den Führungsprozessen und der Operationsgeschwindigkeit zu synchronisieren. Dabei sind die Rolle des Soldaten als Sensor und Zielbezeichner sowie der autonomen intelligenten Systeme speziell zu untersuchen.

Die Bedeutung der einzelnen W+T-Felder für die Fähigkeitskategorie Nachrichtengewinnung, Überwachung und Aufklärung werden mittels Radarbildern (Abbildung 8) dargestellt.

*Umsetzung, Bewertung und Steuerung*

Die operative Umsetzung des W+T-Plans erfolgt durch die Leistungserbringer und kann innerhalb des VBS (z.B. W+T-Kompetenzzentrum der armasuisse, Kommando Höhere Kaderausbildung, Militärakademie) und/oder durch externe Partner (z.B. Industrie, Hochschulen, Institute, Experten) sichergestellt werden. Wichtig ist, dass Synergien bei der Auswahl und bei der Koordinierung der Leistungserbringer in maximaler Weise genutzt werden. Vor allem die Bedarfsdecker müssen gewährleisten, dass die Kompetenzen in den von ihnen bearbeiteten W+T-Feldern sichergestellt werden. Dies erfordert entsprechende Reportingmaßnahmen seitens der Bedarfsdecker und den Aufbau adäquater Controllinginstrumente seitens der Bedarfsträger. Zudem müssen die Bedarfsdecker das Wissensmanagement und den Wissenszugang für den Bedarfsträger sicherstellen. Es ist vor allem die Aufgabe des neu geschaffenen W+T-Ausschusses des

VBS, diese Koordinierungsaufgabe zu übernehmen und die entsprechenden Steuerungsmaßnahmen zu veranlassen.

Die Ergebnisse des umgesetzten W+T-Plans werden schließlich im Rahmen des W+T-Prozesses auf ihre Wirkung untersucht. Zum einen prüft der Bedarfsträger, ob der Bedarfsdecker die Vorgaben erfüllt hat. Zum anderen werden diese projektspezifischen Betrachtungen für den Verwaltungsbereich Verteidigung zusammengefasst, um die Zielsetzungen des W+T-Plans mit den erarbeiteten Ergebnissen zu vergleichen. Die Resultate dieser Analyse können dazu führen, dass der W+T-Bedarf bzw. der W+T-Plan beibehalten oder modifiziert wird.

**W+T-Strukturen**

Die Neuausrichtung der W+T-Bemühungen hat zu strukturellen Veränderungen geführt. Mit Blick auf die durch die sicherheitspolitische Vernetzung erhöhten Anforderungen interessieren an dieser Stelle vor allem der neue W+T-Ausschuss des VBS sowie die Reorganisation innerhalb des Verwaltungsbereichs Verteidigung.

*W+T-Ausschuss des VBS*

Zur Sicherstellung des zweckmäßigen Einsatzes beschränkter Ressourcen im W+T-Bereich des VBS hat der Verteidigungsminister den W+T-Ausschuss eingesetzt, der strategische Koordinierungsfunktionen wahrnimmt[42] und sich aus Vertretern der Verwaltungsbereiche Verteidigung, Bevölkerungsschutz, Sport, armasuisse sowie der Direktion für Sicherheitspolitik zusammensetzt. Der Verteidigungsminister bezeichnet ein Mitglied der Departementsleitung – aktuell der Rüstungschef – als Vorsitzenden des W+T-Ausschusses.

Der W+T-Ausschuss ist verantwortlich dafür, dass die W+T-Bemühungen der genannten Verwaltungsbereiche ressortübergreifend auf eine gemeinsame Situations-, Risiko- und Trendanalyse abgestützt werden. Da die Analysen fachspezifisch autonom in den einzelnen Verwaltungseinheiten durchgeführt werden, kommt dem Gremium die Aufgabe zu, die gegenseitige Information sicherzustellen, Doppelspurigkeiten rechtzeitig zu erkennen bzw. zu verhindern und die Zielsetzungen sowie das Vorgehen zur Sicherstellung der entsprechenden

[42] Weisungen über den Ausschuss für Wissenschaft und Technologie (W+T-Ausschuss) im Eidgenössischen Departement für Verteidigung, Bevölkerungsschutz und Sport vom 4. November 2003.

Kompetenzen aufeinander abzustimmen. In den W+T-Bereichen erarbeitetes Wissen soll mittels Wissensmanagement allen Verwaltungsbereichen zur gemeinsamen Nutzung zugänglich gemacht werden. Erkannte Schwachstellen sollen identifiziert und analysiert sowie geeignete Maßnahmen zu deren Behebung auf Stufe VBS beantragt werden. W+T-Belange sollen künftig durch den W+T-Ausschuss mit den anderen Departementen koordiniert werden. Grundlage dazu bildet ein langfristiger, auf Stufe Departement abgestimmter Forschungs- und Entwicklungsplan des VBS, der sich zeitlich an der Legislaturplanung (Vierjahreszyklus) orientiert. Um Schwerpunkte zu setzen und steuernde Funktionen wahrzunehmen, verfügt der W+T-Ausschuss über entsprechende finanzielle Mittel. Mit einem jährlichen Bericht des W+T-Ausschusses zuhanden der Departementsleitung legt das Gremium Rechenschaft über die Zielerreichung ab und beantragt allfällig notwendig werdende Korrekturmaßnahmen.

*Integrierte Projektteams (IPT) und übergreifende Koordinierung*

Die W+T-spezifischen Tätigkeiten innerhalb des Verwaltungsbereichs Verteidigung werden soweit als möglich über bestehende Organisationseinheiten und Prozesse abgewickelt (Abbildung 9). Hauptverantwortlicher des neuen W+T-Prozesses ist der Chef der Prospektivplanung. Die Prospektivplanung befasst sich mit der längerfristigen Entwicklung der Schweizer Armee. Sie erarbeitet die Grundlagen für die „künftige“ Armee sowie den grundlegenden Änderungsbedarf der „aktuellen“ Armee. Die vorgenommene Zuweisung gewährleistet die nahtlose Abstimmung zwischen dem militärischen Gesamtplanungsprozess und dem spezifischen W+T-Prozess. Neben der Verantwortung für den W+T-Prozess leistet die Prospektivplanung konkrete Beiträge zur inhaltlichen Bestimmung des W+T-Bedarfs und koordiniert die Definition des W+T-Bedarfs seitens der Organisationseinheiten der Armeeführung (u.a. Planungsstab der Armee, Führungsstab der Armee).

Auf der Stufe der Teilstreitkräfte Heer und Luftwaffe sowie des Kommandos Höhere Kaderausbildung und der Logistikbasis der Armee werden die jeweiligen Doktrin- und Planungseinheiten mit den gleichen Aufgaben betraut. Sie koordinieren in Absprache mit den IPT und den W+T-Verantwortlichen der Prospektivplanung die Definition des W+T-Bedarfs und melden diesen der Prospektivplanung, die daraus den W+T-Plan der Streitkräfte erstellt. Diese enge Zusammenarbeit legt den Grundstein für die bessere Harmonisierung der Entwicklungen in den Bereichen Planung, Doktrin, Beschaffung, Rekrutierung und Ausbildung sowie bei den Prozessen und Strukturen. Zusätzlich werden die Di-

rektion für Sicherheitspolitik und die armasuisse einbezogen, um die Abstimmung mit den langfristigen politischen Vorgaben bzw. den vorhandenen W+T-Kompetenzen sicherzustellen.

Im Rahmen der neuen Zusammenarbeit spielen IPT eine Schlüsselrolle.[43] Für jede Fähigkeitskategorie wird ein IPT gebildet, das im Sinne der Jointness über alle relevanten Planungs- und Umsetzungsebenen hinweg die Vernetzung zwischen den zur Bearbeitung der entsprechenden Fähigkeit erforderlichen Bedarfsträgern und Bedarfsdeckern sicherstellt. Bei der Umsetzung werden zusätzlich die Teilstreitkräfte (inkl. Lehrverbände), das Kommando Höhere Kaderausbildung, die Logistikbasis der Armee, die armasuisse (inkl. W+T-Kompetenzzentrum), die Wissenschaft, die Industrie und relevante internationale Gremien berücksichtigt. Der Mehrwert dieses Ansatzes besteht darin, alle zur Bewirtschaftung einer Fähigkeit erforderlichen Kompetenzen und Blickwinkel in einer Expertengruppe zusammenzufassen. In dieser vernetzten Struktur übernehmen die Mitarbeiter der Prospektivplanung treuhänderisch die Funktion der Fähigkeitsverantwortlichen, u.a. indem sie die W+T-spezifischen Arbeiten ausführen und sich zu diesem Zweck eng mit den Linienverantwortlichen und den IPT abstimmen.

**Zusammenarbeit mit Dritten**

Der Nutzung von Synergien mit allen Partnern der bestehenden W+T-Netzwerke kommt im Zeichen der knappen Ressourcen und des steigenden W+T-Bedarfs immer größere Bedeutung zu. Die damit verbundenen Möglichkeiten sollen am Beispiel der Zusammenarbeit mit dem W+T-Kompetenzzentrum der armasuisse sowie der ressortübergreifenden Forschung im Bereich Sicherheits- und Friedenspolitik kurz erläutert werden.

[43] Dieser Ansatz orientiert sich an britischen und US-amerikanischen Erfahrungen. Dort werden integrierte Projektteams vor allem eingesetzt, um das einheitliche Management von Rüstungsprojekten über ihren gesamten Lebensweg zu ermöglichen.

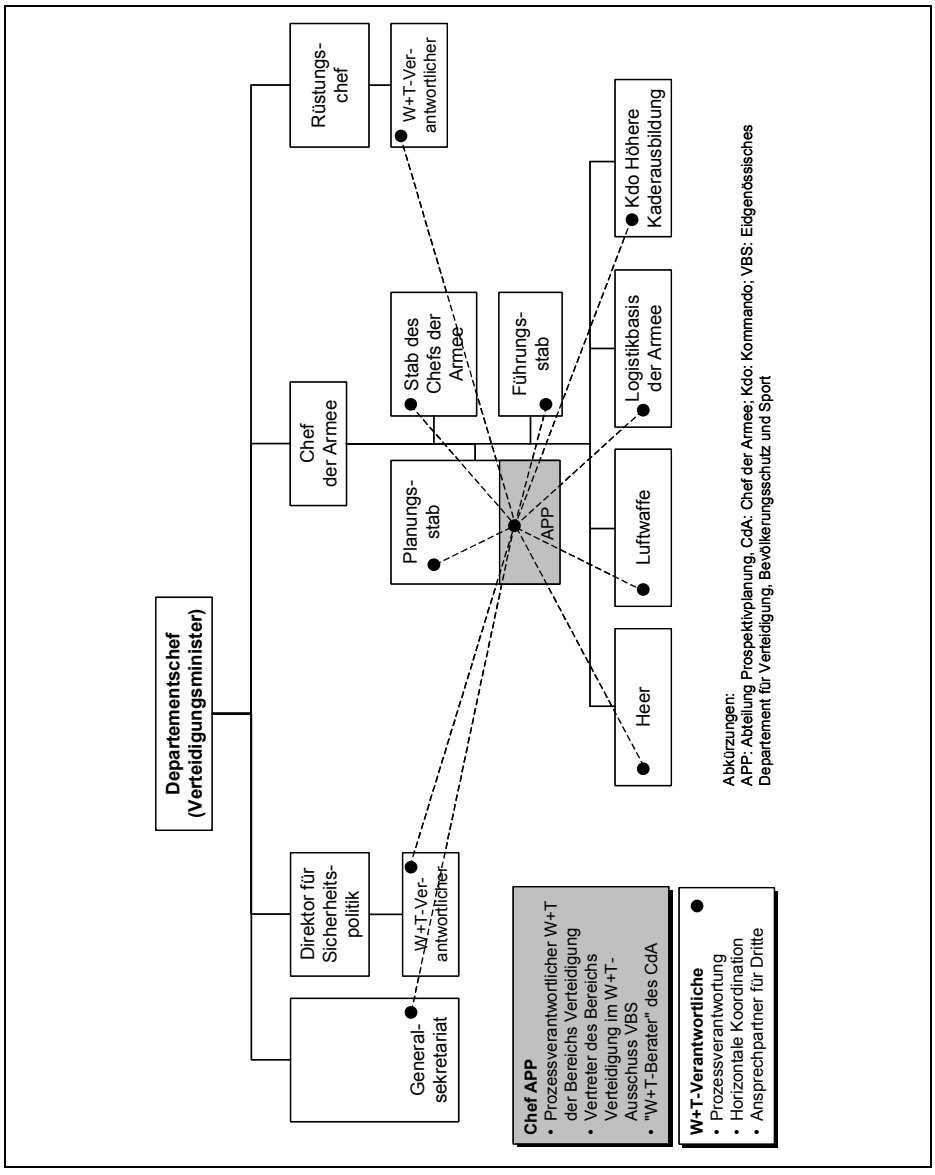



Abbildung 9: W+T-Struktur im Verwaltungsbereich Verteidigung

*W+T-Kompetenzzentrum der armasuisse*

Hauptansprechpartner des Verwaltungsbereichs Verteidigung bei technologischen Fragestellungen ist das W+T-Kompetenzzentrum der armasuisse. Mit gut 250 Mitarbeitenden setzt diese Verwaltungseinheit die Vorgaben des Planungsstabs in folgenden Schwerpunktbereichen um:

- Sensorik und Informationsverarbeitung
- Telematik und Elektronik
- Waffen, Munition und Schutz mit einem zusätzlichen Schwerpunkt Präzision
- Luftverteidigung
- Systemanalyse und technische Informatik zur effizienten und kostengünstigen Unterstützung von Evaluationen komplexer Systeme, der Einsatzoptimierung und der umweltschonenden Ausbildung
- ABC-Schutz mit Fokus Fachwissen zugunsten der sicherheitspolitischen Anstrengungen für Prävention und Verhinderung von Proliferation nuklearer, biologischer und chemischer Waffen
- Werkstofftechnik mit Forschungsschwerpunkt zur Erhöhung der Qualität und Leistung sowie Kostenoptimierung von Systemen
- Multidisziplinäre Probleme im Sinne fachübergreifender und systemorientierter Lösungen

Die Leistungsvereinbarung zwischen dem Planungsstab und der armasuisse definiert die Rahmenbedingungen der Arbeit des W+T-Kompetenzzentrums. Darin werden insbesondere die finanziellen und dadurch indirekt auch die personellen Ressourcen festgelegt. Die Finanzierung erfolgt durch den Planungsstab im Rahmen eines Globalbudgets mit einer Laufzeit von vier Jahren, das in jährlichen Tranchen zugewiesen wird. Die Vorgaben aus der Leistungsvereinbarung und der erwähnten Konzeptionsstudie werden durch das W+T-Kompetenzzentrum in den Langfristigen Forschungsplan überführt. Dieser umfasst die organisatorische sowie programmatische Umsetzung der Vorgaben und konkretisiert die vorgegebenen Schwerpunkte für vier Jahre. Diese Planung wird im Sinne der Identifizierung konkreter Forschungsprojekte noch einmal in jährlichen Forschungsprogrammen mit projektspezifischen Zielsetzungen präzisiert, die finanziellen und personellen Ressourcen zugewiesen, die mitarbeitenden internen Stellen sowie die externen Partner des Netzwerkes bestimmt und verpflichtet.

Auf dieser Grundlage werden die internen Controllingaufgaben des Chefs des W+T-Zentrum wahrgenommen. Sämtliche Projekte werden mit Hilfe des Wissensmanagements dokumentiert und je nach Klassifizierung selektiv zur Nutzung zur Verfügung gestellt. Ein jährlich erscheinendes Dokument „Forschungsberichteverzeichnis" der armasuisse gibt in kurzer Form Aufschluss über die inhaltlichen Forschungsresultate und deren Zugänglichkeit.

Darüber hinaus unterhält das W+T-Kompetenzzentrum ein weit ausgreifendes Partnernetzwerk mit Hochschulen, Instituten und vor allem auch der Industrie. Stellvertretend für die Aktivitäten soll hier auf die Zusammenarbeitsvereinbarung zwischen dem VBS und dem Rat der Eidgenössischen Technischen Hochschulen (ETH-Rat)[44] hingewiesen werden. In einer Absichtserklärung zur Forschungszusammenarbeit wird vereinbart, dass Synergien künftig stärker genutzt werden sollten, z.B. durch die gemeinsame Bearbeitung von Forschungsprojekten, den gegenseitigen Wissens- und Technologietransfer, die Entsendung von Doktoranden an die Institutionen des ETH-Bereiches, die Initiierung von Dissertationen, die Aus- und Weiterbildung von Mitarbeiterinnen und Mitarbeitern der Bundesämter sowie die Veröffentlichung gemeinsamer wissenschaftlicher Publikationen. Die konkrete Zusammenarbeit erfolgt jeweils auf der Grundlage projektspezifischer Verträge.

*Ressortforschung „Sicherheits- und Friedenspolitik"*

Die Ressortforschung „Sicherheits- und Friedenspolitik" leistet einen wichtigen Beitrag, indem sie das Verständnis für die Wirkungszusammenhänge zwischen verschiedenen sicherheitspolitischen Instrumenten fördert und wissenschaftliche Grundlagen für fundierte Entscheidungen der Politik zur Verfügung stellt. Die Schwerpunkte entsprechen den in den verschiedenen Berichten des Bundesrates als prioritär identifizierten sicherheits- und friedenspolitischen Herausforderungen und lassen sich in vier Bereiche gliedern: Außensicherheitspolitik, Friedenspolitik Schutz der Bevölkerung und technische Forschung.

Die außensicherheitspolitische Forschung wird vom Eidgenössischen Departement für auswärtige Angelegenheiten (EDA) und dem VBS mittels eines gemeinsam verwalteten Kredites betrieben. Forschungsfelder sind:

[44] Absichtserklärung betreffend Forschungszusammenarbeit zwischen dem Eidgenössischen Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) und dem Rat der Eidgenössischen Technischen Hochschulen (ETH-Rat) vom 18. Dezember 2003.

- Sicherheitspolitik der Schweiz in einem sich wandelnden strategischen Umfeld
- Nonproliferation, Rüstungskontrolle, Abrüstung und Verifikation
- Gute Dienste und internationale Aktionen zur Friedensunterstützung
- Katastrophenbewältigung

Die vom EDA koordinierte friedenspolitische Forschung trägt dazu bei, den Stellenwert der Friedenspolitik innerhalb der Schweizer Außenpolitik zu klären. Zu diesem Zweck werden Themen wie Konfliktursachen, Erscheinungsformen und Gesetzmäßigkeiten heutiger Gewaltkonflikte sowie angemessene friedenspolitische Interventionsmodelle und Konfliktlösungsstrategien untersucht.

Die unter der Federführung des VBS durchgeführte Forschung zum Schutz der Bevölkerung will den Schutz der Bevölkerung, ihrer Lebensgrundlagen und Kulturgüter gegenüber Katastrophen und Notlagen stetig verbessern. Konkret geht es um die periodische Überprüfung und Aktualisierung der Gefährdungsszenarien und Risikopotentiale, um die Erweiterung und Vertiefung von Erkenntnissen über das gesellschaftliche Verhalten gegenüber Katastrophen, um die Verbesserung der Methoden für die Maßnahmenplanung sowie um die Bereitstellung von Grundlagen zur Optimierung der Ereignisauswertung.

Die technische Forschung wird, wie bereits dargelegt, über das W+T-Kompetenzzentrum sichergestellt.

**W+T-Felderportfolio**

Zur Umsetzung des W+T-Prozesses wurde ein W+T-Felderportfolio erstellt. Dieses vergleicht die Bedeutung der identifizierten W+T-Felder mit dem aktuellen Aufwand (Personal, Finanzen), den der Verwaltungsbereich Verteidigung zur Sicherstellung der jeweiligen Kompetenz betreibt (Abbildung 10).[45] Dadurch können Investitionspotentiale bzw. Desinvestitions- oder Umlagerungsbereiche identifiziert werden: Bei den im Bereich der Diagonalen liegenden W+T-Feldern stimmt der aktuelle Aufwand in etwa mit der Bedeutung überein. In diesen Fällen besteht somit kein unmittelbarer Handlungsbedarf. Dieser besteht da-

[45] Weil die Bestandsaufnahme kein klares Bild über den Aufwand vermittelt, wurde dieser auf einer qualitativen Skala von 1 (sehr geringer Aufwand) bis 5 (sehr hoher Aufwand) geschätzt. Dazu wurde der für ein spezifisches W+T-Feld betriebene Aufwand mit dem gesamten W+T-Aufwand verglichen.

gegen in zwei anderen Bereichen: Links oben liegen die W+T-Felder mit Investitionspotential, die bei der künftigen Mittelzuteilung primär zu berücksichtigen sind, rechts unten diejenigen mit Abbaupotential (z.B. Schutzbautechnik) bzw. Verlagerungspotential (z.B. ABC: von Schutz zu Abwehr und von C zu AB). Insgesamt verdeutlicht Abbildung 10 eindrücklich das „W+T-Erbe" einer nach klassischen Überlegungen organisierten Armee.

**Ausblick**

Abbildung 10 zeigt gleichzeitig auch die Stoßrichtung des W+T-Bedarfs im Rahmen der künftigen Streitkräfteentwicklung auf, der stichwortartig wie folgt umschrieben werden kann:

Das *Prinzip der Vernetzung* spielt in allen für den Verwaltungsbereich Verteidigung relevanten Bereichen eine zunehmend wichtige Rolle. Damit ist beispielsweise die Zusammenarbeit mit anderen Ministerien, mit der Industrie, mit ausländischen zivilen und militärischen Partnern, mit internationalen Organisationen etc. angesprochen. Gerade im Hinblick auf die erfolgreiche Integration moderner Technologie in die Streitkräfte wird die gesamtheitliche Sicht zum Erfolgsfaktor. Schließlich gilt es, die komplexen Wechselwirkungen zwischen Mensch und Maschine auf allen Ebenen – von der Doktrin über die Materialauswahl, die Rekrutierung, die Ausbildung und die Kaderselektion bis hin zu den für die Wartung und den Unterhalt komplexer Systeme zuständigen Personen – konsequent zu berücksichtigen. „Menschbezogene" Disziplinen aus dem Bereich der Sozial- und Geisteswissenschaften gewinnen dadurch an Bedeutung.

Das breitere Einsatzspektrum der Streitkräfte und veränderte sicherheitspolitische Rahmenbedingungen erhöhen den Bedarf an *objektiv nachvollziehbaren und begründbaren Entscheidungsgrundlagen.* Um die strategische Flexibilität und die Anpassungsfähigkeit der Armee sicherzustellen, gewinnt das Denken in Alternativen (Szenarioplanung) an Bedeutung. Für die verschiedenen Einsatzoptionen sind alternative Streitkräftemodelle zu entwickeln (z.B. mit Unterstützung von Operations Research[46]), und bestehende doktrinale Lücken müssen geschlossen werden. Militärwissenschaftliche Grundlagenarbeiten werden für die Erläuterung und die Weiterentwicklung der Position des Verwaltungsbereichs Verteidigung immer wichtiger und verlangen nach entsprechenden wissenschaftlichen Kompetenzen.

[46] Siehe hierzu auch die Ausführungen von Ralph Thiele in diesem Band.

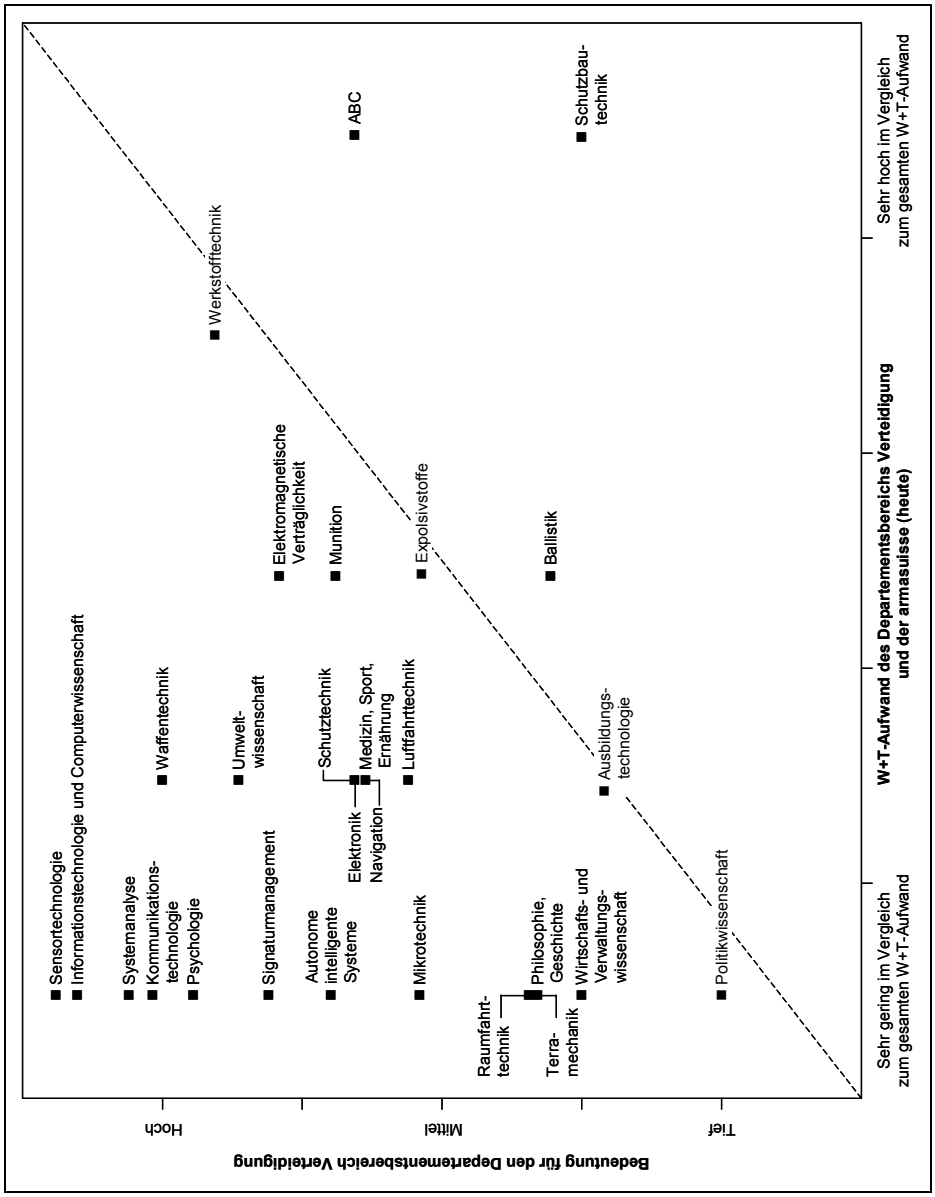



Abbildung 10: W+T-Felderportfolio des Verwaltungsbereichs Verteidigung

Der konzeptionelle Nachholbedarf wirkt sich entsprechend auf die *Aus- und Weiterbildung* aus. Die Sensibilisierung für die Strategieschöpfung und das Denken in strategischen Dimensionen bzw. Alternativen (anstelle des klassischen „Rezeptbuchansatzes") sind ebenso stärker zu betonen wie die Vorbereitung auf neue Einsatzherausforderungen (z. B. friedensunterstützende Operationen in unbekanntem Gelände oder Informationsoperationen). Moderne Simulations-, Informations- und Kommunikationsmittel können eingesetzt werden, um das Wissen der an verschiedenen Orten stationierten Angehörigen der Armee sowie des Zivilpersonals zu erhalten bzw. den neuen Erkenntnissen anzupassen.
Die stärkere Betonung *internationaler Einsätze* erhöht den Bedarf an mobilen, flexiblen, schnell und leicht verlegbaren Streitkräften, die überlebens- und durchhaltefähig sein müssen. Zudem haben *technische Innovationen* wie Abstandswaffen, unbemannte Flugkörper, Sensoren, leistungsfähige und mobile Datenkommunikation zu teilweise weitreichenden Veränderungen in der Art und Weise der Kriegführung beigetragen. Daraus ergeben sich entsprechende Konsequenzen für die technischen Kompetenzen**,** die gewährleistet werden müssen. Die Analyse und die Verfolgung dieser Entwicklung gewinnen dadurch ebenso an Bedeutung wie die Fähigkeit, daraus die relevanten Konsequenzen für die Schweizer Streitkräfte ableiten zu können (Beurteilungsfähigkeit). Der hohe Finanzbedarf, der in diesen Bereichen erforderlich ist, legt es zudem nahe, die Mitarbeit in internationalen Gremien sowie in internationalen Rüstungsprojekten zu intensivieren und gleichzeitig neue, zeitlich straffere und inhaltlich flexiblere Evaluations- bzw. Beschaffungsabläufe zu konzipieren.

Thomas Pankratz und Alfred Vogel

# Der Aufbau sicherheitspolitischer Fähigkeiten und der Beitrag von Wirtschaft und Wissenschaft: Status quo der Sicherheitsforschung in Österreich

## Einleitung

Wie und in welcher Weise sicherheitspolitische Fähigkeiten entwickelt werden, hängt grundsätzlich von der Definition von Sicherheit und in weiterer Folge davon ab, was unter Sicherheitspolitik verstanden wird. In diesem Kontext ist dann die Frage zu analysieren, welchen Beitrag Wissenschaft und Wirtschaft zum Ausbau dieser sicherheitspolitischen Fähigkeiten leisten können.

Diese Fragestellung wird im Folgenden primär unter dem Aspekt der Sicherheitsforschung behandelt. Grundvoraussetzung zur Entwicklung von Fähigkeiten im Allgemeinen sowie von sicherheitspolitischen Fähigkeiten im Speziellen ist die Fähigkeit, die richtigen Fragen stellen zu können sowie die richtigen bzw. geeigneten Antworten auf diese Fragen zu geben. Vor allem angesichts der Komplexität und Interdependenz der neuen Bedrohungen und der sich hieraus ergebenden Szenarien ist systemisches Wissen notwendiger als bisher. Durch Sicherheitsforschung sollen vorhandenes relevantes Wissen, sowohl innerhalb als auch außerhalb des Ressorts, gebündelt und die Entwicklung künftigen Wissens in Richtung der Gewährleistung von Sicherheit artikuliert werden. Der Aspekt der Sicherheitsforschung scheint besonders wegen zwei Punkten hervorhebenswert: Zum einen ist eine solche kohärent ausgerichtete Forschung in Österreich, wenn überhaupt, erst in Ansätzen und nur wage zu erkennen. Zum anderen herrscht aber nicht zuletzt wegen des European Security Research Programme (ESRP) der EU ein erheblicher Druck, sich mit dieser Thematik auseinander zu setzen. Dynamisiert wird diese Diskussion zudem durch den Umstand, dass das 7. EU-Forschungsrahmenprogramm, zu dem das ESRP als bedeutender Baustein zählen wird, im ersten Halbjahr 2006 während der österreichischen EU-Präsidentschaft beschlossen werden soll.

Da dieser Prozess in Österreich erst anläuft, ist dieser Beitrag als Momentaufnahme des Status quo zu verstehen, aus der sich aber bereits einige Konturen der Sicherheitsforschung in Österreich ableiten lassen. Von zentraler Bedeutung in der nunmehr einsetzenden Diskussion ist die Frage nach einer national abge-

stimmten Definition von Sicherheitsforschung sowie der Positionierung der relevanten Akteure in diesem Bereich.

## Zur Definition von Sicherheitspolitik, sicherheitspolitischen Fähigkeiten und Sicherheitsforschung

Ausgangspunkt für eine Annäherung an einen Definitionsansatz aus österreichischer Sicht ist die österreichische Sicherheits- und Verteidigungsdoktrin vom Dezember 2001, die die Leitlinie für die Sicherheitspolitik Österreichs darstellt. Gemäß der Doktrin ist Sicherheitspolitik umfassend zu konzipieren und zu verwirklichen sowie als vorrangige politische Aufgabe des Staates zu verstehen.

Als sicherheitspolitische Fähigkeiten sind demnach zunächst alle Fähigkeiten zu verstehen, die dieses Konzept der umfassenden Sicherheitspolitik fördern und unterstützen. Zudem zählen dazu auch alle Fähigkeiten, die dazu betragen, dass ein Staat die Rolle eines „aktiven Akteurs" wahrnehmen kann.

Der konzeptionelle Ansatz des *aktiven Akteurs* geht davon aus, dass die Position eines Staates im internationalen Geschehen einerseits durch objektive Faktoren (wie etwa Größe, Bevölkerung, Wirtschaftsleistung, Geographie, Rohstoffe, etc.) und andererseits durch strukturelle Faktoren (wie Einbindung in Internationale Organisationen oder Struktur des internationalen Systems) bestimmt ist. Diese Faktoren definieren den Handlungs- und Gestaltungsspielraum sowie das Handlungspotential eines Staates. Darüber hinaus ist die internationale Position durch den Willen des jeweiligen Staates bestimmt, eine aktive Akteursrolle einnehmen zu wollen (= politischer Ambitionslevel), das heißt sich im Bereich der High Politics zu engagieren. Der aktive Akteur setzt die objektiven und strukturellen Faktoren zur Durchsetzung eigener Interessens- und Ordnungsvorstellungen ein. Neben anderen Parametern, wie z.B. die militärischen Beiträge bei internationalen Operationen, zeichnet sich ein aktiver Akteur dadurch aus, dass ein hohes Maß an Partizipation in allen Bereichen der internationalen Politik und keine Fokussierung auf einen politischen Teilbereich bzw. eine geographische Region (aktiv in der Breite) gegeben ist. Dies schließt aber bestimmte Schwerpunktsetzungen bzw. die Konzentration auf einzelne Politikbereiche, Fähigkeiten oder Regionen nicht aus (aktiv in der Tiefe). In der Partizipationstiefe und -breite manifestiert sich somit das außen- und sicherheitspolitische Profil des Akteurs. Dies impliziert auch, dass das jeweilige außen- und sicherheitspoli-

tische Profil identifizierbar und sichtbar sein sollte.[47] Aufgabe der Sicherheitsforschung wäre es demnach, das Umfeld zu beobachten und zu analysieren, die eigenen Kapazitäten zu überprüfen und gegebenenfalls weiter zu entwickeln und somit eine Partizipation sicherzustellen.

Die Notwendigkeit einer Diskussion zum Thema Sicherheitsforschung ergibt sich ferner aus der generellen sicherheitspolitischen Entwicklung, die auf die immer schwieriger werdende Unterscheidung zwischen äußerer und innerer Sicherheit hinweist, wodurch Homeland Defence zu einem zentralen Thema der sicherheitspolitischen Debatte wird. Für Österreich ist zudem auch die aufbauend auf den Ergebnissen der Bundesheerreformkommission zu erwartende Um- und Restrukturierung des Bundesheeres zu nennen.

Als unmittelbarer Auslöser für die Debatte um Sicherheitsforschung kann das von der EU initiierte ESRP gesehen werden. Grundsätzlich gibt die EU keine exakte Definition, was unter Security Research zu verstehen ist. Dennoch ist aus verschiedenen Dokumenten ableitbar, welche Konzeption dieser Begriff umfasst. Auch wenn die EU vom Prinzip der umfassenden Sicherheit ausgeht, steht im Mittelpunkt der Forschungsaktivitäten die Überlegung, dass es vor allem technologischer und naturwissenschaftlicher Innovationen bedarf, um den neuen Bedrohungen begegnen zu können.[48] Zwar können Technologien per se keine Sicherheit gewähren, aber ohne die Unterstützung der Technologie ist Sicherheit undenkbar.

Hieraus ergibt sich in weiterer Folge, dass Security Research primär als naturwissenschaftlich-technischer Zugang verstanden wird, der anwendungsorientiert (mission-oriented) zu sein hat. Dies kann auch aus den Schwerpunktbereichen, wie sie von der EU hinsichtlich des Preparatory Action Plan dargestellt werden, abgeleitet werden. Zu diesen zählen:[49]

---

47 Hierzu weiterführend: Johann Frank und Thomas Pankratz, „Das Konzept des aktiven Akteurs als Beurteilungskriterium für den Nutzen internationaler Einsätze des Bundesheeres“ (Wien: Büro für Sicherheitspolitik, 2004, unveröffentlichtes Arbeitspapier).

48 „Europe must use its technological strengths to build the capability for deploying significant resources for peacekeeping, humanitarian aid and state-building activities (…).” Zit. gemäß: European Commission, *On the Implementation of the Preparatory Action on the enhancement of the European industrial potential in the field of Security Research. Towards a programme to advance European security through Research and Technology,* COM (2004) 72 final, Brüssel, 3. Februar 2004, S. 6 <http://europa.eu.int/eur-lex/en/com/cnc/2004/com2004_0072en01.pdf> (Zugriff: 16. Juli 2004).

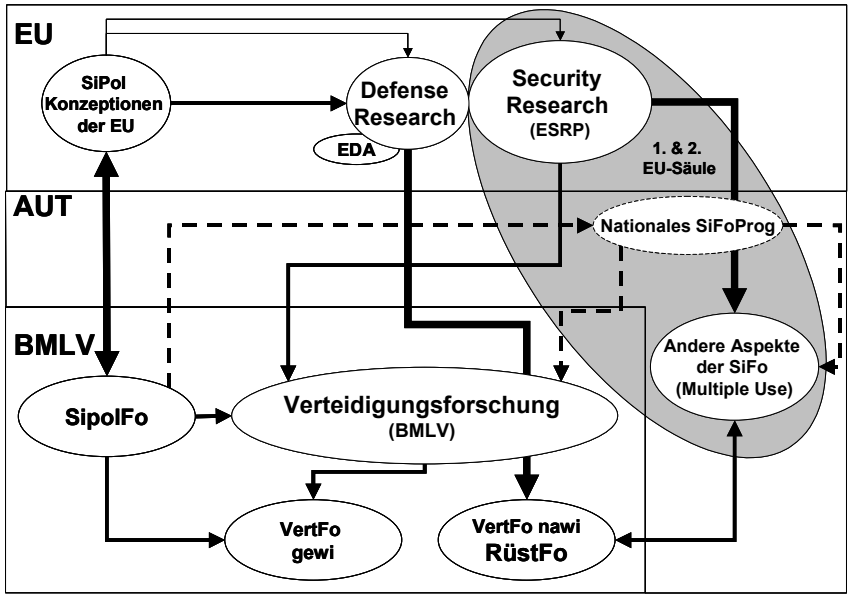
49 European Commission, *On the Implementation of the Preparatory Action on the enhancement of the European industrial potential in the field of Security Research,* S. 7.

- Improving situation awareness
- Optimising security protection and protection of networked systems
- Protection against terrorism (including bio-terrorism and incidents with biological, chemical and other substances)
- Enhancing crisis management (including evacuation, search and rescue operations, active agents control and remediation)
- Achieving interoperability and integrated systems for information and communication

Hinzuweisen ist in diesem Zusammenhang, dass sozial- und geisteswissenschaftliche Ansätze im Umgang mit den neuen Bedrohungen trotz des Hinweises auf den umfassenden Sicherheitsbegriff im dargestellten Ansatz der Europäischen Kommission von nachgeordneter Bedeutung sind. Ausgehend vom oben angeführten in Österreich geltenden Begriff von Sicherheitspolitik folgt, dass sich Sicherheitsforschung an diesem umfassenden Verständnis von Sicherheit zu orientieren hat und über die Begrifflichkeiten von Security bzw. Defence Research hinausgeht. Abbildung 11 verweist auf dieses umfassende Verständnis. Hieraus ergibt sich in umgekehrter Weise, dass erstens Security Research und Defence Research nur einen bestimmten Teilbereich von Sicherheitspolitik erfassen und zweitens nur ein Teil des Verteidigungsministeriums betroffen ist. Dies unter anderem auch deswegen, da Security Research im Verständnis der EU im Bereich der 1. und 2. Säule angesiedelt ist und somit das Ressort nur indirekt berührt bzw. da Defence Research sich im Grunde nur auf Rüstungsforschung im engeren Sinne bezieht. In diesem Zusammenhang wäre deshalb zu überlegen, inwieweit nicht der bisher gängige Begriff der sicherheitspolitischen Forschung weiter zu verwenden wäre. Dies auch unter dem Aspekt, dass die Sicherheits- und Verteidigungsdoktrin den Bereich der sicherheitspolitischen Forschung explizit erwähnt und auch fordert, diesen auszubauen, „um ein umfassendes Bild über sicherheits- und verteidigungspolitische Belange“ zu erhalten.[50]

Aus Abbildung 11 ergibt sich auch die essentielle Rolle der sicherheitspolitischen Forschung, da diese nicht nur die ressortinterne Forschung, sondern auch die Forschung in Österreich sowie diejenige der EU beeinflusst und nur diese eine Vernetzung zwischen allen Bereichen der Sicherheitsforschung herstellt.

[50] *Österreichische Sicherheits- und Verteidigungsdoktrin. Entschließung des Nationalrates* (Wien: Bundeskanzleramt, 2001), S. 11.




Abkürzungen
AUT Österreich, BMLV Bundesministerium für Landesverteidigung, EDA Europäische Verteidigungsagentur, Gewi Geisteswissenschaften, Nawi Naturwissenschaften, SiFo Sicherheitsforschung, SiFoProg Sicherheitsforschungsprogramm, SipolFo Sicherheitspolitische Forschung, RüstFo Rüstungsforschung, VertFo Verteidigungsforschung

Abbildung 11: Begriffssystem Sicherheitsforschung
Quelle: Direktion für Sicherheitspolitik

Wesentliches Ziel der Sicherheitsforschung ist die Analyse der Voraussetzungen, Kapazitäten und Fähigkeiten, Strukturen und Prozesse zur Gewährleistung von Sicherheit. Daher müsste Sicherheitsforschung die folgenden zentralen Forschungsfelder umfassen:

- Analyse der Ursachen und Konsequenzen von Bedrohungen für das staatlichen System als Ganzes sowie der Bürgerinnen und Bürger in den Dimensionen Bedrohungserkennung, Bedrohungsvermeidung und Folgen der Bedrohungen;
- Schutz- und Abwehrmaßnahmen vor Bedrohungen und effektives Krisenmanagement (zu diesem Punkt ist auch die Transformation der Streitkräfte zu zählen);

- Von zentraler Bedeutung für die Analyse sind folgende Bedrohungsszenarien: Technische und Naturkatastrophen, Bedrohungen durch Krankheiten, Bedrohungen, die sich aus dem zivilisatorischen Fortschritt ergeben sowie Bedrohungen aus der Gesellschaft, hier insbesondere Terrorismus, Organisierte Kriminalität und die Proliferation von Massenvernichtungswaffen.

Ausgehend sowohl von dem oben erwähnten umfassenden Sicherheitsverständnis als auch von der Komplexität und der Interdependenz der so genannten „neuen Bedrohungen" (neue Bedrohungen als nicht abgrenzbare Querschnittsmaterie), ist davon auszugehen, dass eine Analyse derselben nur erfolgen kann durch einen

- systematischen multi- bzw. interdisziplinären, nicht nur naturwissenschaftlich-technischen, sondern auch sozial- und geisteswissenschaftlichen Forschungsansatz und breiten Wissenszugang, der
- im Rahmen nationaler als auch internationaler Kooperationen,
- auf einer gesamthaften und gesamtstaatlichen Betrachtungsweise beruht.

Von besonderer Bedeutung ist, dass die Kooperation zwischen militärischen und zivilen Stellen, dem öffentlichen und privaten Sektor sowie der Wirtschaft verstärkt wird, um Synergieeffekte zu erzielen. Dies wird auch im Endbericht der Bundesheerreformkommission erkannt, indem die „weitere Verstärkung der systematischen Zusammenarbeit aller sicherheitsrelevanten staatlichen und gesellschaftlichen Institutionen unter Bereithaltung der für das jeweilige Aufgabenspektrum spezifischen Ressourcen in den einzelnen Ressorts" [51] bzw., an anderer Stelle, „die Kooperation zwischen Forschungseinrichtungen, der Wirtschaft und des Bundesheeres zu verstärken" empfohlen werden.[52] Ähnlich wird auch in der Sicherheits- und Verteidigungsdoktrin gefolgert, dass eine enge Kooperation und Vernetzung relevanter Organisationen und Institutionen im In- und Ausland anzustreben ist.[53] Gerade hinsichtlich internationaler Kooperationen ist es – insbesondere auch unter dem Aspekt des in der „Tiefe" agierenden

[51] *Bundesheer 2010. Bericht der Bundesheerreformkommission* (Wien: Bundesheerreformkommission, 2004), S. 52.
[52] *Bundesheer 2010,* S. 63.
[53] *Österreichische Sicherheits- und Verteidigungsdoktrin,* S. 11.

aktiven Akteurs – von essentieller Bedeutung, etwas Spezifisches, d. h. eine besondere wissenschaftliche bzw. technologische Expertise, als Gegenleistung für erhaltene Leistungen bzw. Wissen anbieten zu können. Gibt es nichts anzubieten, kann dies massive negative Effekte haben, indem sich beispielsweise die Attraktivität als Kooperationspartner in der Beurteilung Dritter reduziert bzw. die Grundlagen fehlen, um anspruchsvolle sicherheitspolitische Paradigmenwechsel und Transformationsprojekte (z.B. in Richtung vernetzter Operationsführung) in Angriff nehmen zu können. Dementsprechend wäre es gerade aus der Sicht eines Staates mit begrenzten Ressourcen anzudenken, dass sich dieser auf bestimmte Bereiche der Sicherheitsforschung konzentriert.

Darüber hinaus wird es entscheidend sein, die Forschung auch hinsichtlich eines längerfristigen Zeitrahmens (ca. 15-20 Jahre) zu konzipieren und dabei auf längerfristige Planungsüberlegungen abzustimmen.[54]

## Organisation der Sicherheitsforschung

Zurzeit sind alle relevanten Akteure in Österreich in einer Phase der Definition des jeweiligen Begriffsverständnisses von Sicherheitsforschung sowie ihrer eigenen Positionierung in diesem Politikfeld. Die Vertretung der Interessen Österreichs bei der EU wird durch das Bundesministerium für Bildung, Wissenschaft und Kultur (BMBWK) im Einvernehmen mit dem Bundesministerium für Innovation, Verkehr und Technologie (BMVIT) wahrgenommen. Die Koordinierung innerhalb Österreichs erfolgt derzeit ebenfalls in dieser Konstellation, wobei diese Kompetenzfrage noch nicht endgültig geklärt ist. Weiteres ist die Errichtung einer Plattform beim BMBWK unter Einbindung aller relevanten Akteure geplant.

Seitens BMVIT ist vorgesehen, ein nationales Sicherheitsforschungsprogramm zu entwickeln. Hierzu wurde ein Forschungsauftrag an die Österreichische Akademie der Wissenschaften (ÖAW) mit folgenden Zielen vergeben:

- Definition des Begriffes Sicherheitsforschung
- Erarbeitung von Grundlagen für ein nationales Sicherheitsforschungsprogramm
- Erarbeitung von Grundlagen für die Errichtung einer Forschungsstelle an der Österreichischen Akademie der Wissenschaften

[54] Siehe hierzu auch den Beitrag von René Eggenberger und Heiko Borchert in diesem Band.

Die ÖAW soll sich also gewissermaßen als Think Tank für den Bereich Sicherheitsforschung etablieren. Das Bundesministerium für Landesverteidigung ist in diesen laufenden Prozess durch eine Vertretung in der Plattform beim BMBWK, durch eine Vertretung bei Besprechungen im BMVIT und durch direkten Kontakt zur ÖAW eingebunden.

## Die Rolle des Bundesministeriums für Landesverteidigung in der Sicherheitsforschung

Bei der Sicherheitsforschung ist zwischen Forschung im Bundesministerium für Landesverteidigung (BMLV) sowie Forschung außerhalb des Ressorts zu unterscheiden: Von Bedeutung ist hier auch die Kooperation des Ressorts mit anderen Forschungseinrichtungen sowie der Industrie und Wirtschaft. Bei der Analyse des Inputs aus Wirtschaft und Wissenschaft ist grundsätzlich festzustellen, dass die Inputs von der Wirtschaft primär von außerhalb des Ressorts kommen, wohingegen wissenschaftliche Inputs sowohl von außerhalb als auch innerhalb kommen.

*Bundesministerium für Landesverteidigung*

Grundsätzlich ist davon auszugehen, dass die Entwicklung der Sicherheits- und der Verteidigungspolitik eines Staates sowie von Institutionen auf dem besten verfügbaren Wissen beruht. Dies trifft in der Folge somit auch auf die Entwicklung der Streitkräfte, deren Organisation, Ausrüstung sowie Ausbildung und Taktik zu. Die Bundesheerreformkommission empfiehlt daher im Endbericht, dass „durch Nutzung wissenschaftlicher Erkenntnisse und spezifischer Forschung des Bundesheeres Änderungen im Bedrohungsbild auf Grund der Erfahrungen im internationalen Krisenmanagement, der geostrategischen Entwicklung und der subjektiven Bedrohungswahrnehmung der Bevölkerung laufend zu beurteilen und die sich daraus ableitenden Erkenntnisse in die Entwicklung der Streitkräfte einzubringen“ sind.[55] Je besser die Mittel, die Fähigkeiten und die Strukturen der Streitkräfte auf die zu lösenden sicherheitspolitischen Anforderungen angepasst sind, um so eher werden diese auch entsprechend eingesetzt werden können.

Das BMLV hat jedoch schon immer über den „engen“ militärischen Bereich einen wesentlichen Anteil zur umfassenden Sicherheit in Österreich beige-

[55] *Bundesheer 2010,* S. 50.

tragen. So unter anderem dadurch, dass das BMLV laufend substantielle Inputs für die Erstellung der sicherheitspolitischen Bedrohungsanalyse liefert. Zudem verfügt das BMLV mit der Direktion für Sicherheitspolitik, der Landesverteidigungsakademie oder der Wissenschaftskommission über Strukturen, die andere Ministerien nicht haben. Insbesondere im Bereich der sicherheitspolitischen Forschung nimmt das BMLV eine führende Funktion ein. Dies vor allem wegen der eigenen Kompetenzen und Ressourcen, der finanziell unterstützten Stiftungsprofessur an der Universität Innsbruck, der Förderung verschiedener nationaler Institute (z. B. OIIP, ÖIES) und insbesondere durch die enge Kooperation mit ausländischen Forschungseinrichtungen. Die Positionierung des BMLV in anderen Bereichen wird sich erst mittelfristig ergeben. Zuerst sind massive Defizite im Forschungs- und Technologiebereich des BMLV durch die Definition einer kohärenten Forschungsstrategie und eines Forschungsprogramms sowie ein effizientes Forschungsmanagement zu beheben.[56]

Das in Österreich für militärische Forschung aufgebrachte Budget kann mit rund 10 Mio. Euro sowohl im nationalen als auch internationalen Vergleich als überaus gering betrachtet werden. Damit hat Forschung sicherlich nicht die Bedeutung, die sie im Vergleich mit Staaten ähnlicher wirtschaftlicher Größenordnung haben sollte.[57] Betrachtet man die Forschungsaktivitäten im BMLV, so ergibt sich folgende Gliederung:[58]

- Strategie- und politikwissenschaftliche Forschung
- Geistes- und sozialwissenschaftliche Forschung
- Wehrmedizinische Forschung
- Naturwissenschaftliche und wehrtechnische Forschung
- Militärhistorische Forschung
- Militärökonomische-wirtschaftswissenschaftliche Forschung
- Militärische Führungsforschung

---

[56] Bemerkung von Göran Roos (Co-Autor der Studie „Recommendations for an effective research and technology management system within the BMLV") im Rahmen der Veranstaltung „Wissenschaft, Forschung, Landesverteidigung" am 9. Juni 2004 in Wien.

[57] Aussage Bundesminister Platter im Rahmen der Veranstaltung „Wissenschaft, Forschung, Landesverteidigung" am 9. Juni 2004 in Wien.

[58] Herbert Strunz, „Forschungskonzept für den Fachhochschul-Studienlehrgang Militärische Führung" (Wien: Bundesministerium für Landesverteidigung, 1999, unveröffentlichtes Arbeitspapier); S. 8 f. Der Forschungsthemenkatalog des Forschungsbeirates beim BMLV ordnet dem sozial- und geisteswissenschaftlichen Bereich auch die strategie- und politikwissenschaftliche, die militärhistorische, die militärökonomische-wirtschaftswissenschaftliche sowie die militärische Führungsforschung zu.

Sicherheitsforschung im Ressort (Inhouse Reseach) findet vor allem an der Landesverteidigungsakademie sowie im Rüstungsstab und im Amt für Rüstung und Wehrtechnik statt.

Die Landesverteidigungsakademie (LVAk) ist die höchste militärische Bildungs- und Forschungseinrichtung des Österreichischen Bundesheeres. Sie untersteht der Dienst- und Fachaufsicht des Chefs des Generalstabes und kann als das Zentrum des BMLV für die meisten Bereiche der Sozial- und Geisteswissenschaften bezeichnet werden. Die in Forschung und Lehre abgedeckten Gebiete umfassen die Hauptdisziplinen der höheren militärischen Führung (Operation, Taktik, Logistik, Führungs- und Organisationslehre); Strategie und Sicherheitspolitik unter Einschluss von internationalem Recht, Rüstungskontrolle und Rüstungstechnik; Militärgeographie, Militärsoziologie, Militärethik, Militärpädagogik und militärische Zeitgeschichte; Friedenssicherung und Konfliktmanagement einschließlich Analyse der Entwicklung von Streitkräftestrukturen und Doktrinen. Angemerkt werden muss in diesem Zusammenhang, dass die Forschung an der LVAK zurzeit primär im Dienste der Ausbildung der höheren Offiziere zu sehen ist sowie dass die Forschungsergebnisse kaum anderen ressortinternen Stellen zugestellt werden.[59]

Das Amt für Rüstung und Wehrtechnik sowie der Rüstungsstab spielen eine wichtige Rolle für den Bereich der Sicherheitsforschung weil hier die Nachfrage nach neuem Wissen und auch die Expertise von neuem Wissen durch Studien, Tests und der gleichen vor allem im Bereich der Rüstungs- und IKT-Technik generiert werden. Allerdings ist der Informationsfluss zwischen diesen und den übrigen Bereichen des Ressorts aktuell noch als ungenügend zu bewerten.[60]

Besonders hervorzuheben sind ferner auch die Direktion für Sicherheitspolitik und die Wissenschaftskommission im BMLV. Die Direktion für Sicherheitspolitik spielt eine sehr wichtige Rolle, da sie neben der Beratung des Bundesministers sowie der Dienststellen des BMLV in allgemeinen und ressortspezifischen Angelegenheiten der Sicherheitspolitik auch die sicherheitspolitische Forschung zu ihren wesentlichen Aufgaben zählt.

---

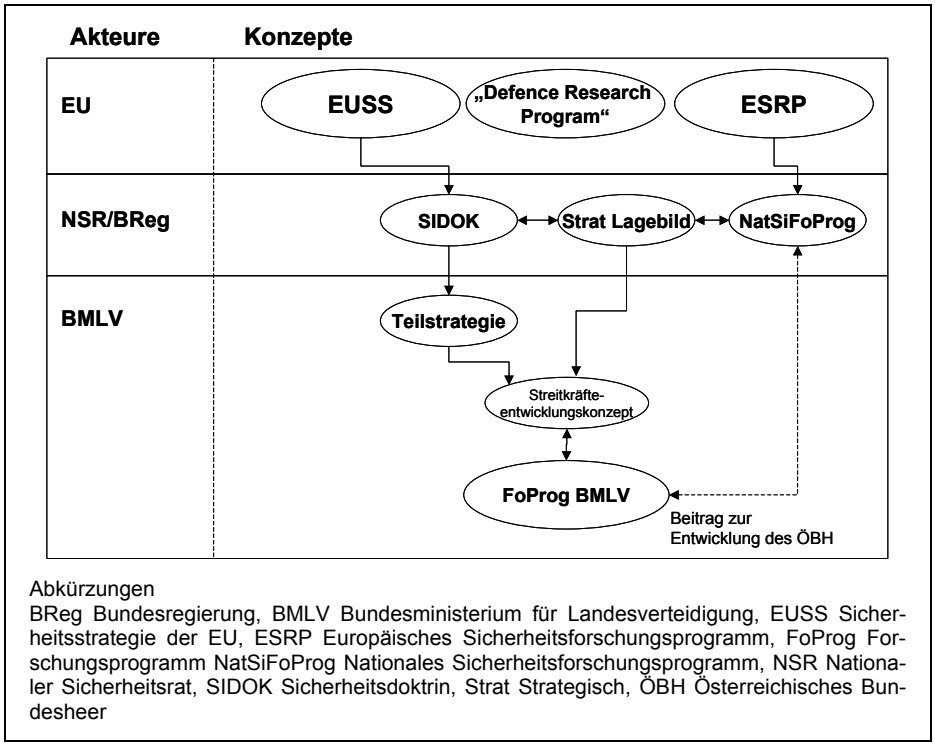
[59] Bemerkung von Göran Roos (Co-Autor der Studie „Recommendations for an effective research and technology management system within the BMLV") im Rahmen der Veranstaltung „Wissenschaft, Forschung, Landesverteidigung" am 9. Juni 2004 in Wien.

[60] Bemerkung von Göran Roos (Co-Autor der Studie „Recommendations for an effective research and technology management system within the BMLV") im Rahmen der Veranstaltung „Wissenschaft, Forschung, Landesverteidigung" am 9. Juni 2004 in Wien.

Die Wissenschaftskommission im BMLV wurde 1992 eingerichtet und fungiert als wissenschaftliches Beratungsgremium des Ressorts. Zahlreiche Entwicklungen im Bereich des Österreichischen Bundesheeres wurden durch diese Kommission beeinflusst[61], und es wurden im Rahmen dieser Kommission auch zahlreiche Forschungsprojekte abgewickelt.

*Mitwirkung des BMLV am ESRP*

Wie oben erwähnt, ist die Positionierung des BMLV hinsichtlich der Mitwirkung am ESRP noch unter Diskussion, so dass noch keine abschließende Beurteilung gegeben werden kann.




Abkürzungen
BReg Bundesregierung, BMLV Bundesministerium für Landesverteidigung, EUSS Sicherheitsstrategie der EU, ESRP Europäisches Sicherheitsforschungsprogramm, FoProg Forschungsprogramm NatSiFoProg Nationales Sicherheitsforschungsprogramm, NSR Nationaler Sicherheitsrat, SIDOK Sicherheitsdoktrin, Strat Strategisch, ÖBH Österreichisches Bundesheer

Abbildung 12: Zusammenwirken verschiedener nationaler Konzepte bei der Mitwirkung Österreichs im Rahmen des ESRP

Quelle: Direktion für Sicherheitspolitik

[61] So beispielsweise die Umwandlung der Militärakademie in den Fachhochschullehrgang Militärische Führung.

Wesentlich scheinen zwei Punkte: Erstens muss die Vernetzung der verschiedenen sicherheitspolitisch relevanten Konzepte hergestellt werden. Wie aus Abbildung 12 ersichtlich, kommt hierbei dem Lagebildprozess eine essentielle Rolle zu, da dieser in unmittelbarer Wechselwirkung sowohl mit der Sicherheits- und Verteidigungsdoktrin sowie dem zu entwickelnden Sicherheitsforschungsprogramm steht.[62]

Zweitens müssen die wesentlichen Interessen des BMLV im Rahmen der Mitwirkung am ESRP ausformuliert werden (Abbildung 13). Diese sind:

- Beeinflussung des Gesamtprozesses. Aus Abbildung 13 wird hier insbesondere die zentrale Rolle des BMLV über die Mitwirkung am Nationalen Sicherheitsrat[63] ersichtlich
- Einbringen der eigenen spezifischen Fähigkeiten
- Verbesserung der eigenen Fähigkeiten und Kapazitäten

Aus Abbildung 13 wird auch ersichtlich, dass neben dem ESRP auch nationale Projekte zu etablieren sein werden, da nur hierdurch die von der EU geforderte Mitfinanzierung erreicht werden kann.

*Außerhalb des Ressorts*

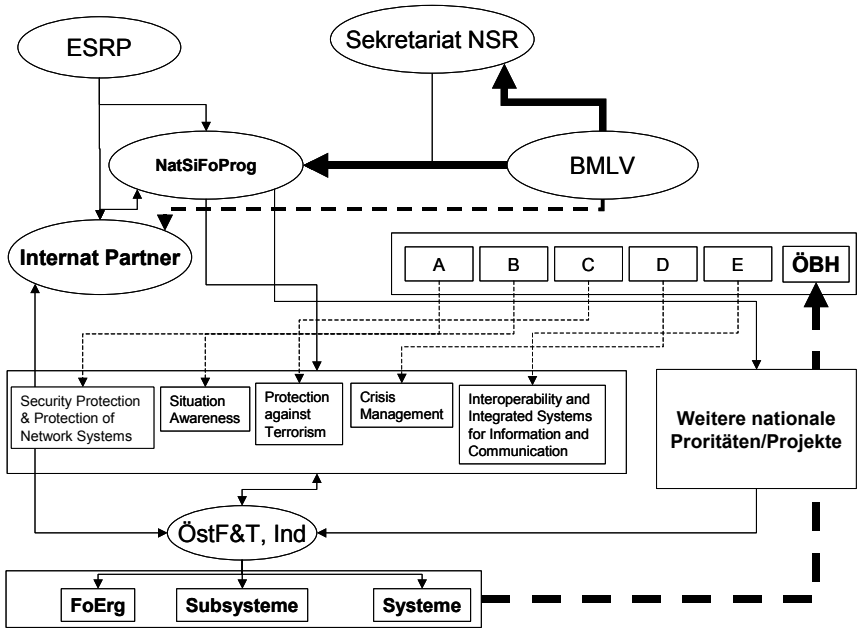
In Österreich sind die Ausgaben für Forschung und Entwicklung eher bescheiden und betrugen 2001 etwa 1,8 % des Bruttoinlandprodukts (BIP); damit liegt Österreich im EU-Vergleich an neunter Stelle von 15 Staaten. Geplant ist jedoch, die öffentlichen und privaten Ausgaben für Forschung gemessen am BIP (Forschungsquote) bis 2005 auf 2,5 % des BIP anzuheben. Zurzeit kommen rund 40 % der Forschungsgelder von der öffentlichen Hand, 60 % aus privaten Mitteln. Die Bundesregierung plant in diesem Zusammenhang auch, die Ansiedelung von internationalen Konzernen in Österreich weiter zu fördern, da von diesen auch größere Forschungsaktivitäten erwartet werden. Daneben strebt man an, mögliche industrielle Kooperationen, die sich aus Gegengeschäften im Rüstungsbereich ergeben, zu nutzen.[64]

---

62 Diese Abbildung stellt den vorläufigen, noch nicht abgeschlossenen Diskussionsstand dar; Änderungen sind noch möglich.

63 Der Nationale Sicherheitsrat (NSR) ist ein politisches Organ, in welchem Vertreter der Legislative und der höchsten Ebene der Exekutive die Regierung in Belangen der Außen-, Sicherheits- und Verteidigungspolitik beraten.

64 Herbert Strunz und Monique Dosch, „Sicherheitspolitik und Wirtschaft", *Österreichische Militärische Zeitschrift* 41:4 (Juli-August 2003), S. 429-442, hier S. 436.




Abkürzungen
A-E exemplarisch für verschiedene Dienststellen des BMLV, BMLV Bundesministerium für Landesverteidigung, ESRP Europäisches Sicherheitsforschungsprogramm, FoErg Forschungsergebnisse, Ind Industrie NatSiFoProg Nationales Sicherheitsforschungsprogramm, NSR Nationaler Sicherheitsrat, ÖstF&T Österreichische Forschung und Technologie, ÖBH Österreichisches Bundesheer

Abbildung 13: Mögliche Einbindung und Mitwirkung des Bundesministeriums für Landesverteidigung im Rahmen des Europäischen Sicherheitsforschungsprogramms
Quelle: Direktion für Sicherheitspolitik

**Kooperation mit anderen Forschungseinrichtungen**

Grundsätzlich kann eine große Bereitschaft beobachtet werden, dass Universitäten und andere Forschungseinrichtungen mit dem BMLV zusammenarbeiten (Abbildung 14). Dennoch muss festgestellt werden, dass das BMLV zurzeit nicht den richtigen Nutzen aus dieser Kooperationsbereitschaft ziehen kann.[65]

[65] Bemerkung von Göran Roos (Co-Autor der Studie „Recommendations for an effective research and technology management system within the BMLV") im Rahmen der Veranstaltung „Wissenschaft, Forschung, Landesverteidigung" am 9. Juni 2004 in Wien.

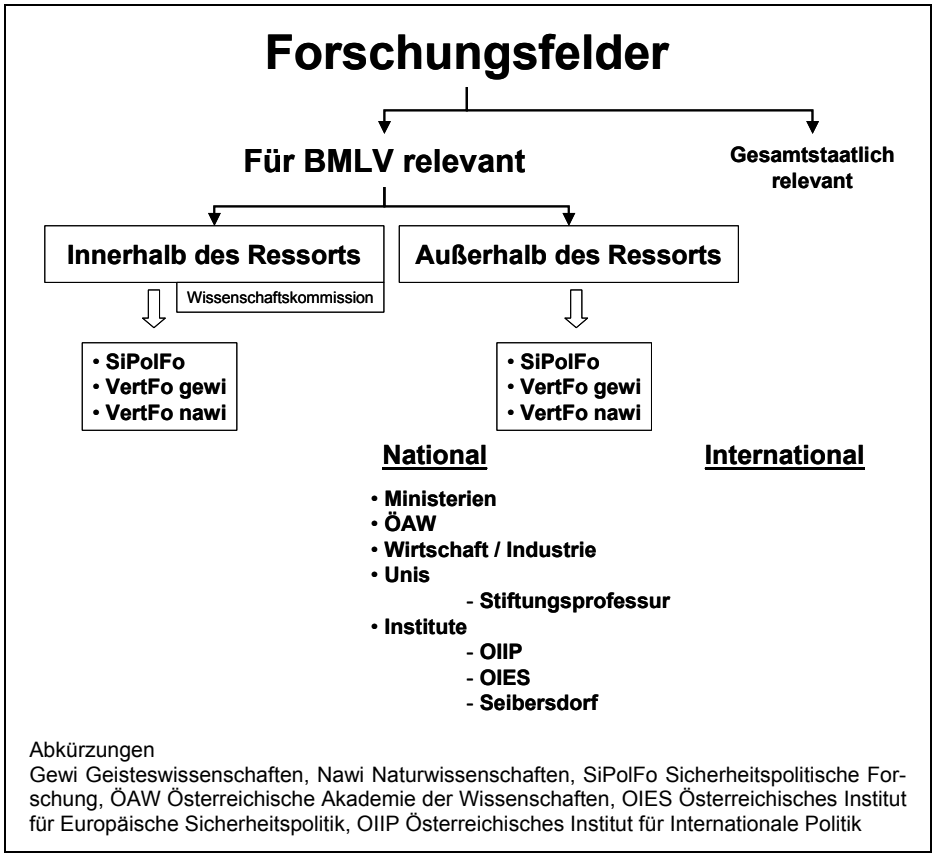



Abbildung 14: Übersicht der Forschungskooperationspartner
Quelle: Direktion für Sicherheitspolitik

*Internationale Kooperation*

Grundsätzlich beteiligt sich Österreich an allen relevanten Institutionen der Forschung im Bereich der Sicherheits- und Verteidigungspolitik, wie etwa Western European Armaments Group (WEAG) oder der nunmehr im Entstehen begriffenen Europäischen Verteidigungsagentur. In der Sicherheits- und Verteidigungsdoktrin wird als Rahmen der Forschungskooperation, insbesondere der sicherheitspolitischen Forschung, auf die Partnerschaft für den Frieden hingewiesen.[66] Wie oben erwähnt, kommt dem BMLV gerade im Bereich der sicherheitspoliti-

[66] *Österreichische Sicherheits- und Verteidigungsdoktrin,* S. 14.

schen Forschung durch die enge Kooperation mit internationalen Forschungseinrichtungen auch deswegen eine in Österreich herausragende Stellung zu.

*Kooperation mit der Wirtschaft und Industrie*

Im Endbericht der Bundesheerreformkommission wird zurecht darauf verwiesen, dass Militär und Wirtschaft in einem engen Zusammenhang stehen, da die relative Stellung eines Staates im internationalen Staatengefüge in einem erheblichen Ausmaß durch seine wirtschaftliche Kraft und militärische Stärke bestimmt wird. Bemerkenswerterweise werden jedoch im Bericht nur die möglichen Auswirkungen von sicherheitspolitischen Entscheidungen bzw. der Streitkräfteentwicklung auf die Wirtschaft analysiert, nicht jedoch die Rolle der Wirtschaft für die Sicherheitspolitik.

Grundsätzlich ist davon auszugehen, dass es verschiedene Ansätze für eine Kooperation zwischen Wirtschaft und Industrie auf der einen und dem BMLV auf der anderen Seite gibt (etwa in Form von Partnerschaften). Im Bereich der „klassischen" Rüstung ist der potentielle Nutzungsgrad zurzeit aber als gering zu bewerten. Dies vor allem deswegen, weil Österreich kaum über eine nennenswerte Rüstungsindustrie verfügt,[67] die daraus möglicherweise resultierenden Erfahrungen daher sehr gering sind und durch das Fehlen einer kohärenten Forschungsstrategie des BMLV auch nicht richtig genutzt werden können.

Es gibt zwar hoch qualitative Cluster (z.B. im Flugzeugbau), doch wie es scheint, fehlen dem BMLV entsprechende Strukturen, um mit diesen kommunizieren und kooperieren zu können. Zudem sollte dieses Potential nicht überbewertet werden. Eine Analyse des Spin Off-Potentials der zivilen Forschung und Entwicklung zeigt, dass etwa 12 % der Forschungsaktivitäten der österreichischen Wirtschaft ein hohes und etwa 32 % ein mittleres Potential für den militärischen Sektor besitzen. Besonders hohes Potential liegt in den Bereichen Metall und Maschinenbau sowie in der Nachrichtentechnik.[68]

## Schluss

Als sicherheitspolitische Fähigkeiten sind solche Fähigkeiten zu verstehen, die von einem umfassenden Begriff der Sicherheitspolitik ausgehend, alle Bemühungen eines Staates, seine Rolle als aktiver Akteur wahrzunehmen, unterstüt-

[67] Beschäftigte (2002, total): ca. 1'940, Umsatz (2002): ca. 187,2 Mio. Euro. Zit. gemäß: *Austrian Military Suppliers* (Wien: Wirtschaftskammer Österreich, 2002), S. IV.

[68] Strunz/Dosch, „Sicherheitspolitik und Wirtschaft", S. 437.

zen. Von essentieller Bedeutung hierfür sind die wissenschaftliche Analyse der Bedrohungen, verschiedener Bedrohungsszenarien, Schutz- und Abwehrmaßnahmen vor Bedrohungen sowie effektives Krisenmanagement.

Ohne wissenschaftliche und technologische Weiterentwicklung besteht für jedes Land die Gefahr, ins Abseits zu geraten und den wirtschaftlichen, wissenschaftlichen bzw. politischen Anschluss zu verlieren und dadurch die Rolle eines aktiven Akteurs einzubüßen. Zentrale Ansatzpunkte um einer solchen Entwicklung entgegenzuwirken sind die Schaffung entsprechender Rahmenbedingungen im Forschungs- und Entwicklungsbereich sowie die Zusammenarbeit der staatlichen und privaten Forschungsinstitutionen auf höchstem Niveau.

Einem Kleinstaat wie Österreich sind im Bereich der Forschung Grenzen gesetzt. Dies trifft sowohl für die Forschung im Allgemein sowie für den Bereich der Sicherheitsforschung im Speziellen zu. Die Tatsache, dass es für den Bereich der Sicherheitsforschung keine längerfristig angelegte Forschungsstrategie gibt und Forschung im BMLV zumeist von einem Bottom Up-Ansatz geleitet wird, verdeutlicht allerdings, dass diese Grenzen teilweise selbst verursacht sind. Deswegen kommt der stringenten, strategischen Neuausrichtung dieses Aufgabenbereichs sowie der verstärkten Zusammenarbeit zwischen den Ministerien, der Wissenschaft und der Wirtschaft eine zentrale Rolle zu, da die knappen Mittel durch hierbei erzielte Synergien effektiver genutzt werden können. Zur gleichen Zeit bildet eine solche Kooperation auf nationaler Ebene auch die Basis für eine zielführende und effektive Integration in die internationalen, vor allem europäischen Strukturen.

Österreich verfügt zweifelsohne über ein gewisses Potential im Bereich Sicherheitsforschung sowohl im staatlichen als auch nicht-staatlichen Rahmen. Ein wesentliches Problem ist aber, dass diese Kapazitäten bislang noch nicht in der Form zusammengeführt wurden, um hieraus den bestmöglichen Nutzen erzielen zu können. Wichtig scheint daher für die Zukunft, dass

- eine nationale kohärente Sicherheitsforschungsstrategie entwickelt wird, in welcher eine Abstimmung nicht nur zwischen den staatlichen Institutionen, sondern auch den nicht-staatlichen Institutionen und der Wirtschaft erfolgt;
- diese Strategie auf die sicherheitspolitischen Herausforderungen des 21. Jahrhunderts Bezug nimmt, längerfristig angedacht ist und auch auf längerfristige Planungsprozesse abgestimmt ist;

- hierbei sowohl ein Top Down- als auch Bottom Up-Ansatz verfolgt wird;
- ein entsprechendes Forschungsmanagement und Qualitätssicherung gegeben sind und
- die Kooperation der Ministerien untereinander sowie mit den Universitäten und anderen Forschungseinrichtungen und der Wirtschaft verbessert wird.

Dies alles ist erst in Ansätzen vorhanden. Auch wenn in Österreich im Vergleich zum von der EU verwendeten Begriff Security Research ein breiteres Verständnis von Sicherheitsforschung gegeben ist, so ist doch zu erwarten, dass das ESRP der EU einen wichtigen Impuls für den Auf- und Ausbau der sicherheitspolitischen Forschungsbemühungen in Österreich liefern wird.

## Abbildungs- und Tabellenverzeichnis


Abbildung 1: Nanotechnische Kristallgitter. Das Beispiel der „Nanoröhre“ ..... 13
Abbildung 2: Der Systemintegrator ist für die Integration des Systemverbundes verantwortlich ..... 64
Abbildung 3: Systemübersicht für die Demonstration eines vernetzten Gefechts- und Simulationssystems gezeigt von der Firma RDE auf der Eurosatory 2004 ..... 67
Abbildung 4: Hauptprozess Streitkräfte- und Unternehmens-entwicklung gemäß Prozessmodell Armee XXI ..... 78
Abbildung 5: W+T-Sollprozess für den Verwaltungsbereich Verteidigung ..... 79
Abbildung 6: Fähigkeitskategorien der Schweizer Armee ..... 80
Abbildung 7: W+T-Felder der Schweizer Armee ..... 81
Abbildung 8: W+T-Felder für die Nachrichtengewinnung, Überwachung und Aufklärung ..... 82
Abbildung 9: W+T-Struktur im Verwaltungsbereich Verteidigung ..... 88
Abbildung 10: W+T-Felderportfolio des Verwaltungsbereichs Verteidigung ..... 93
Abbildung 11: Begriffssystem Sicherheitsforschung ..... 99
Abbildung 12: Zusammenwirken verschiedener nationaler Konzepte bei der Mitwirkung Österreichs im Rahmen des ESRP ..... 105
Abbildung 13: Mögliche Einbindung und Mitwirkung des Bundesministeriums für Landesverteidigung im Rahmen des Europäischen Sicherheitsforschungsprogramms ..... 107
Abbildung 14: Übersicht der Forschungskooperationspartner ..... 108

Tabelle 1: Mittelfristig verfügbare militärische Nutzungsmöglich-keiten für intelligente Hochtechnologie aus Sicht des US-Verteidigungsministeriums ..... 25
Tabelle 2: Militärische Nutzungsmöglichkeiten der Nanotechnologie ..... 26
Tabelle 3: Transformationsrelevante rüstungstechnische Fähigkeiten ..... 61

# Abkürzungsverzeichnis

| | |
|---|---|
| ACT | Allied Command Transformation |
| APP | Abteilung Propsektivplanung |
| BIP | Bruttoinlandprodukt |
| BMBWK | Bundesministerium für Bildung, Wissenschaft und Kultur |
| BMLV | Bundesministerium für Landesverteidigung |
| BMVIT | Bundesministerium für Innovation, Verkehr und Technologie |
| C2IEDM | Command and Control Information Exchange Data Model |
| C4 | Command, Control, Communications, Computers |
| CD&E | Concept Development and Experimentation |
| CdA | Chef der Armee |
| CIE | Common Information Environment |
| Corba | Common Object Request Broker Architecture |
| COTS | Commercial off the Shelf |
| CPM | Customer, Product, Management |
| CROP | Common Relevant Operational Picture |
| DEM | Data Exchange Mechanism |
| DIS | Distributed Integrated Simulation |
| EBO | Effects Based Operations |
| EDA | European Defence Agency |
| EDA | Eidgenössisches Departement für auswärtige Angelegenheiten |
| ESRP | European Security Research Program |
| ETH | Eidgenössische Technische Hochschule |
| EU | Europäische Union |
| EUSS | European Union Security Strategy |
| F&T | Forschung und Technologie |
| FCS | Future Combat System |
| FoErg | Forschungsergebnisse |
| FoProg | Forschungsprogramm |
| FST A | Führungsstab der Armee |
| Gewi | Geisteswissenschaften |
| GSZ | Gefechtssimulationszentrum |
| HE | Heer |
| HLA | High Level Architecture |
| IKT | Informations- und Kommunikationstechnologie |
| IPT | Integriertes Projektteam |
| ISR | Intelligence, Surveillance, Reconnaissance |

| | |
|---|---|
| JOANA | Joint Operations Army-Navy-Air Force |
| KdoOpFüEingrKr | Kommando Operative Führung der Eingreifkräfte |
| LBA | Logistikbasis der Armee |
| LSI | Lead System Integrator |
| LVAk | Landesverteidigungsakademie |
| LW | Luftwaffe |
| M&S | Modellbildung und Simulation |
| MIC | Multinational Interoperability Council |
| NATO | North Atlantic Treaty Organization |
| NatSiFoProg | Nationales Sicherheitsforschungsprogramm |
| Nawi | Naturwissenschaften |
| NC3A | NATO C3 Agency |
| NCW | Network Centirc Warfare |
| NEC | Network Enabled Capabilities |
| NetOpFü | Vernetzte Operationsführung |
| NGS | Neue Generation Simulatorkern |
| NRF | NATO Response Force |
| NSR | Nationaler Sicherheitsrat |
| ÖAW | Österreichische Akademie der Wissenschaften |
| ÖBH | Österreichisches Bundesheer |
| ÖIES | Österreichisches Institut für Europäische Sicherheitspolitik |
| OIIP | Österreichisches Institut für Internationale Politik |
| ONA | Operational Net Assessment |
| RMA | Revolution in Military Affairs |
| SIDOK | Sicherheitsdoktrin |
| SiFoProg | Sicherheitsforschungsprogramm |
| SiPol | Sicherheitspolitik |
| SipolFo | Sicherheitspolitische Forschung |
| SJFHQ | Standing Joint Forces Headquarters |
| TA | Target Acquisition |
| VBS | Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport |
| VertFo | Verteidigungsforschung |
| VPR | Verteidigungspolitische Richtlinien |
| W+T | Wissenschaft und Technologie |
| WEAG | Western European Armaments Group |
| ZASBw | Zentrum für Analysen und Studien der Bundeswehr (seit Juli 2004: Zentrum für Transformation der Bundeswehr) |
| ZD | Zentrale Dienste |

# Die Autoren

**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.

**René Eggenberger** (rene.eggenberger@gst.admin.ch) ist seit 1996 als Prospektivplaner tätig und seit 2001 Chef der Abteilung Prospektivplanung im Planungsstab der Schweizer Armee. Zuvor war er in der Sektion Führung und Einsatz verantwortlich für die Operationsplanung und war als Instruktor der Infanterie in der Ausbildung tätig. Er hat an der Universität Basel in Analytischer Anorganischer Chemie promoviert und einen einjährigen Weiterbildungskurs am Royal College of Defence Studies, London, absolviert.

**Gebhard Geiger** (gebhard.geiger@swp-berlin.org) arbeitet als wissenschaftlicher Mitarbeiter in der Forschungsgruppe Sicherheitspolitik der Stiftung Wissenschaft und Politik, Berlin, und ist Privatdozent an der TU München. Seine aktuellen Arbeitsschwerpunkte umfassen technologische Trends und internationale Sicherheit. Er hat Politikwissenschaft an der University of California at Los Angeles studiert sowie in Physik und Wissenschaftsphilosophie an der Universität München bzw. an der Technischen Universität München promoviert.

**Norbert Härle** (harle.norbert@rheinmetall-de.com) leitet seit Januar 2004 die Produktstrategie in der Geschäftseinheit Flugsysteme bei Rheinmetall Defence Electronics GmbH, wo er zuvor in den Bereichen Simulation und Strategische Geschäftsentwicklung tätig war. Er hat an der Ruhr-Universität Bochum und an der Purdue University in Indiana, USA, Elektrotechnik studiert und promovierte 1988 in Bochum in der Signalverarbeitung. 1988 bis 1994 leitete er ein europäisches Projekt (ESPRIT) bei Krupp Atlas Elektronik GmbH in Bremen. Im Mai 1994 wurde er Professor (Lecturer) für Regelungstechnik an der Queensland University of Technology in Brisbane, Australien.

**Burkhard Theile** (burkhard.theile@rheinmetall-detec.com) leitet die Hauptabteilung Strategische Unternehmensentwicklung und Technologie der Rheinmetall DeTec AG. 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 Gebieten Raumfahrt und Wehrtechnik ein. Fünf Jahre lang leitete er die Firmenvertretung eines deutschen Unternehmens in Washington/USA.

**Ralph Thiele** (ralphthiele@bundeswehr.org) ist Kommandeur des Zentrums für Transformation der Bundeswehr in Waldbröl. Davor war er Chef de Cabinet und Chef des Stabes am NATO Defence College, Rom, Dozent für Militärstrategie an der Führungsakademie der Bundeswehr, Hamburg, sowie Referent im Planungsstab des Bundesministeriums für Verteidigung bzw. im Führungsstab der Luftwaffe. Er hat Wirtschafts- und Organisationswissenschaften an der Universität der Bundeswehr, München, sowie Politikwissenschaft an der Hochschule für Politik, München, studiert und die Generalstabsausbildung an der Führungsakademie der Bundeswehr, Hamburg, absolviert.

**Thomas Pankratz** (thomas.pankratz@bmlv.gv.at) arbeitet im Büro für Sicherheitspolitik des Bundesministeriums für Landesverteidigung, Wien. Zudem ist er Lektor am Institut für Politikwissenschaft der Universität Wien und arbeitet als systemischer Trainer. Er hat Politikwissenschaft, Geschichte und Philosophie an der Universität Wien studiert sowie verschiedene Studien zum Thema Sicherheitspolitik verfasst.

**Alfred Vogel** (alfred.vogel@oeaw.ac.at) ist Präsidialdirektor der Österreichischen Akademie der Wissenschaften in Wien. Physikstudium (Dipl.-Ing., Dr. techn., Technische Universität, Wien) und MBA-Studium (International Management Development Institute, Lausanne). Berufstätigkeiten als Hochschullehrer (TU-Wien, ETH-Lausanne) und für das Bundesministerium für Landesverteidigung. Danach Leitungsfunktionen in der wehrtechnischen Industrie und an der Österreichischen Akademie der Wissenschaften. Neben der Akademiefunktion Konsulent der Arbeitsgemeinschaft Sicherheit und Wirtschaft der Wirtschaftskammer Österreich.