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

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

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.

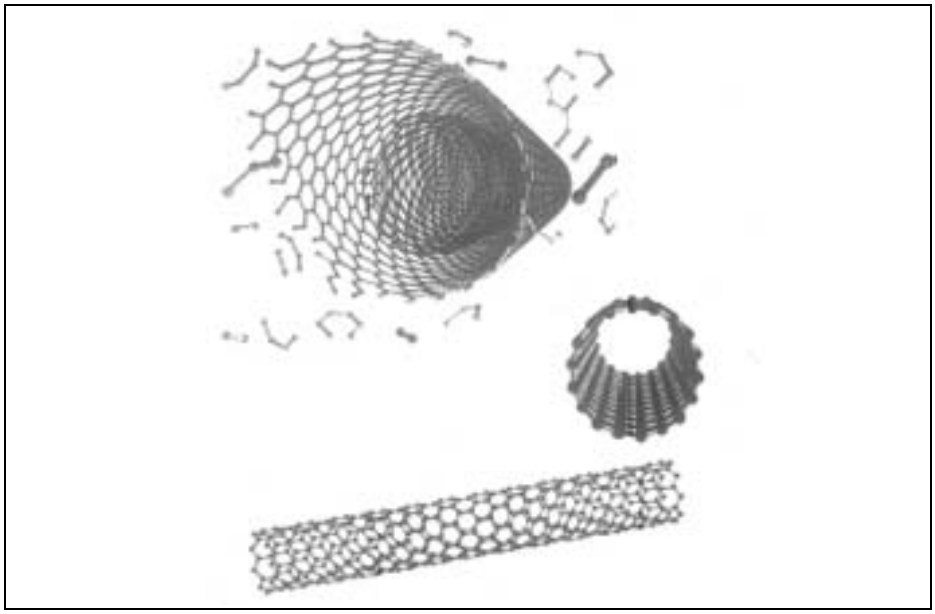

Abbildung 1: Nanotechnische Kristallgitter. Das Beispiel der „Nanoröhre“

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.