SWP-Studie
Stiftung Wissenschaft und Politik
Deutsches Institut für Internationale
Politik und Sicherheit

Gebhard Geiger

Rüstungspotentiale neuer Mikrotechnologien

Konsequenzen für internationale Sicherheit und Rüstungskontrolle

S 24
Juni 2003
Berlin

SWP
Stiftung Wissenschaft und Politik
Deutsches Institut für Internationale Politik und Sicherheit

Ludwigkirchplatz 3–4
10719 Berlin
Telefon +49 30 880 07-0
Fax +49 30 880 07-100
www.swp-berlin.org
swp@swp-berlin.org

ISSN 1611-6372

Inhalt

Rüstungspotentiale neuer Mikrotechnologien
Konsequenzen für internationale Sicherheit und Rüstungskontrolle

Die rüstungstechnische Entwicklung wird zunehmend von neuen Mikrotechnologien beherrscht, die sich gleichermaßen für militärische wie kommerzielle Verwendung eignen. Es handelt sich in erster Linie um die sogenannte Nanotechnologie, um nanotechnische Anwendungen in der Informationselektronik sowie um die Biotechnologie, letztere hauptsächlich auf gentechnischer Basis. Unter Nanotechnologie (von griechisch nano = Zwerg) versteht man Entwurf, Bau und Anwendung besonders kleiner Mikrosysteme mit Abmessungen von der Größenordnung eines Nanometers, das ist der millionste Teil eines Millimeters. Physikalisch gesehen befaßt sich die Nanotechnologie mit dem technischen Eingriff in die Wechselwirkung zwischen einzelnen Atomen und Molekülen.

Die fortschreitende Miniaturisierung technischer Systeme und ihrer Bauteile hat für die militärische Waffen- und Gerätetechnik ebenso wie für Rüstungskontrolle und die Verifikation von Rüstungskontrollverträgen weitreichende Folgen. Mikrotechnologien, allen voran die digitale Informationstechnik, haben bereits in den beiden vergangenen Jahrzehnten eine Revolution des Militärwesens (Revolution in Military Affairs) bewirkt. Die Umwälzungen erstrecken sich auf alle Ebenen der Rüstung, Organisation und Streitkräfteplanung, Strategie, Taktik und militärischen Operation bis hin zur internationalen Sicherheit.

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, tiefgreifende 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.

Aufgrund ihrer Leistungsmerkmale können die neuen Mikrotechnologien neuartige, erhebliche Gefährdungen der internationalen Sicherheit hervorrufen. Durch eine extrem gesteigerte Wirksamkeit bei gleichzeitiger ziviler, kommerzieller Verbreitung

erschließen moderne Technologien auch nichtstaatlichen internationalen Organisationen ein beträchtliches Gewaltpotential. Rüstungskontrollpolitisch ist das Potential kaum mehr sinnvoll zu erfassen, offensive und defensive Rüstungsziele sind praktisch nicht mehr voneinander zu unterscheiden.

In dieser Lage kommt Deutschland und seinen EU-Partnern heute eine leistungsfähige Forschung und Entwicklung auf den Innovationsgebieten der Nano-, Informations- und Biotechnologie zugute. Herkömmliche wissenschaftlich-technische Bereiche wie Luft- und Raumfahrt, Sensorik, Material- und Fertigungstechnik können von der innovativen Grundlagenforschung ebenfalls profitieren.

Was angesichts der sicherheitspolitischen Herausforderungen moderner Mikrotechnologien in den deutschen und europäischen Forschungs- und Technologieprogrammen allerdings fehlt, ist die Sicherheits- und sicherheitspolitische Komponente. Wie ein Vergleich mit der militärischen Beteiligung an der amerikanischen »National Nanotechnology Initiative« zeigt, werden die Auswirkungen der Nanotechnologie auf die militärische Sensorik, Logistik, Automatisierung, künstliche Intelligenz und zahlreiche weitere Rüstungsgebiete in Europa nicht ausreichend berücksichtigt. Zum anderen fehlt der Bundesrepublik seit vielen Jahren eine angemessene sicherheits- und technologiepolitische Antwort auf die Gefährdungen ihrer informationsabhängigen kritischen Infrastrukturen durch Computerspionage, -sabotage und Internetmißbrauch. Es ist damit zu rechnen, daß mit der weiter fortschreitenden Miniaturisierung von Informationssystemen auf nanotechnischer Grundlage auch die sicherheitspolitische Kontrolle dieser Systeme schwächer wird, während das politische und kriminelle Mißbrauchspotential wächst.

Frühwarnung, Abschreckung und Vergeltung von Bedrohungen beziehungsweise Verletzungen der internationalen Sicherheit werden durch moderne Waffensysteme auf mikrotechnologischer Basis, aber auch aufgrund der Verwundbarkeit mikrotechnologisch fundierter und gesteuerter Systeme erschwert. Um so notwendiger sind defensive Strategien und Maßnahmen zum Schutz, zur Abwehr und zur Schadensminimierung im Verteidigungsfall. Konkret heißt dies, daß bestehende gesetzliche Regelungen des deutschen Zivil- und Katastrophenschutzes erweitert und wechselseitig stärker aufeinander bezogen werden müssen, um den neuartigen technologischen Herausforderungen der Sicherheit (Schutz ziviler informationsabhängiger Infrastrukturen im Konfliktfall, Schutz der Zivilbevölkerung gegen gentechnisch produzierte Massenvernichtungswaffen) gerecht zu werden.

In der internationalen Rüstungskontrollpolitik wird die kooperative Vertragsverifikation zunehmend einseitigen, nichtkooperativen Überprüfungsmethoden (Aufklärung, Spionage) weichen. Eine Sicherheitspolitik mit neuen Dimensionen ist daher erforderlich, bei der sich geheimdienstliche, militärische und polizeiliche Aufklärung an den spezifischen Gefährdungspotentialen moderner mikrotechnologischer Waffensysteme orientieren.

Neue Dimensionen der Mikrotechnologie

Informationselektronik und Biotechnologie werden heute oft als die Schrittmacher der technischen Innovation schlechthin angesehen. So gilt etwa die Computertechnik – zu Recht – als die gemeinsame Grundlage für zahlreiche weitere wissenschaftlich-technische und wirtschaftlich-soziale 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 sogenannten Nanotechnologie zu. Ihre sicherheits- und rüstungspolitischen Konsequenzen sollen hier in der Wechselbeziehung mit anderen Technologien, aber auch mit politisch-gesellschaftlichen Veränderungen von der Art der Globalisierung (weltweite Vernetzung) der Märkte oder der Kommunikationsmedien untersucht werden. Im Vordergrund stehen die sicherheitspolitischen Probleme der Nanotechnologie als einer ausgeprägten »dual-use«-Technologie.

Nanotechnologie

Unter Nanotechnologie versteht man das Forschungs- und Entwicklungsgebiet, das sich mit dem technischen Eingriff in die Wechselwirkung zwischen einzelnen Atomen und Molekülen befaßt. Der Ausdruck »nano« (griechisch Zwerg) wird zur Bezeichnung sehr kleiner physikalischer Längeneinheiten benutzt. Ein Nanometer entspricht dem millionsten Teil eines Millimeters. Atomdurchmesser liegen größenordnungsmäßig im Bereich von einem Zehntelnanometer. 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 Design und Katalyse neuer Kunststoffe (Keramik, Polymere usw.) in der Chemie.[1] Medizinische und pharmazeutische Nanotechnologie zielen indessen auf die Herstellung von Nanoteilchen – und deren präzise gesteuerten 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).

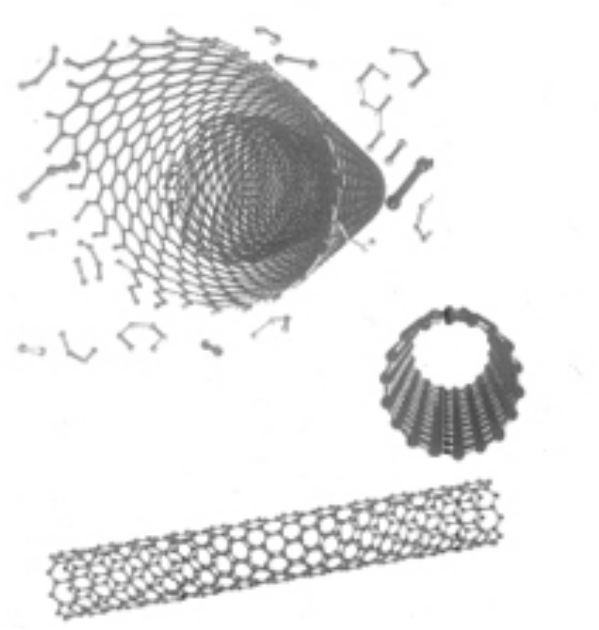
Erforschung und gezielte technische Manipulation einzelner atomarer und molekularer Systeme nutzen quantenphysikalische Ströme und Kräfte, insbesondere den sogenannten quantenmechanischen Tunneleffekt, um einzelne Atome und Moleküle und damit die Struktur der Materie sichtbar zu machen.[2] Dieser revolutionären 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. Angestrebt wird die massenhafte, kommerzielle Herstellung möglichst einfacher atomarer und molekularer Bauteile, die zu Kunststoffen mit neuartigen Eigenschaften führen.

1 Philip S. *Antón*/Richard *Silberglitt*/James *Schneider*, The Global Technology Revolution, Santa Monica, CA 2001; Nanotechnologie, Spektrum der Wissenschaft – Spezial, (2001) 2; Michael *Köhler*, Nanotechnologie, Weinheim 2001; Horst-Günter *Rubahn*, Nanophysik und Nonotechnologie, Stuttgart 2002.

2 Heinrich *Hörber*/Thomas *Früh*, Die Sanfte Sonde, in: Spektrum der Wissenschaft – Spezial, (2001) 2, S. 24–29.

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.[3]

Abbildung 1
Nanotechnische Kristallgitter.
Das Beispiel der »Nanoröhre«



Quelle: Spektrum der Wissenschaft – spezial, Nanotechnologie (2002) 2.

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 hochtechnisierten 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. Jedenfalls muß sich die sicherheitspolitisch orientierte Technikfolgenforschung rechtzeitig den sehr realen Herausforderungen dieser immer noch jungen Disziplin stellen. 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] Die folgenden Rahmendaten und Zahlen machen die forschungs- und technologiepolitische Dynamik der Entwicklung deutlich.

In Deutschland unterstützen Bund, Länder und Privatwirtschaft die nanotechnische Forschung und Entwicklung auf vielfältige Weise im Hochschulbereich, in zahlreichen Forschungszentren und in der Industrie.[5] Die Hochschulen haben neue Lehrangebote beziehungsweise ganze nanowissenschaftliche Ausbildungsgänge neu geschaffen.[6] Das Bundesministerium für Bildung und Forschung (BMBF) schätzt die Aufwendungen der öffentlichen Hand und der Industrie zur Förderung nanowissenschaftlicher und -technischer Vorhaben im Jahre 2001 auf insgesamt 217 Millionen Euro. Der Beitrag für grundfinanzierte Hochschul

3 Philip G. *Collins*/Phaedon *Avouris*, Elektronik, atomar neu gestrickt, in: Spektrum der Wissenschaft – Spezial, (2001) 2, S. 48–55.

4 *Antón*/*Silberglitt*/*Schneider*, Global Technology Revolution [wie Fn. 1], S. 25–26.

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

6 Markus *Breidenich*, Perspektiven gibt es in der Nanowelt in Hülle und Fülle, in: Frankfurter Allgemeine Zeitung, 7.12.2002, S. 55.

forschung ist bei dieser Summe nicht einmal mitberücksichtigt (Tabelle 1).[7] Die EU fördert die Nanowissenschaft und -technik als eigenes Schwerpunktgebiet innerhalb des 6. Rahmenprogramms, das Forschungsvorhaben auf europäischer Ebene in den Jahren zwischen 2002 und 2006 umfaßt. Bei einem Gesamtvolumen von 17,5 Milliarden Euro entfallen auf diesen Zeitraum 1,3 Milliarden Euro auf die Grundlagenforschung und industrielle Umsetzung der Nanotechnologie.[8] Unter den außereuropäischen Ländern dominieren die USA und Japan mit ehrgeizigen Förderprogrammen (Tabelle 2).[9]

Tabelle 1
Aufwendungen der öffentlichen Hand und der Wirtschaft für Nanotechnologie in Deutschland, Stand 2001 (Mio. Euro)

	Gesamtsumme	*Öffentliche Mittel*	*Industrieanteil*
BMBF-Projektförderung	96,6	54,1	42,5
BMWi-Projektförderung	8,0	6,0	2,0
Institutionelle Förderung	112,7	93,0	19,7
Summe (Mio. Euro)	217,3	153,1	64,2

Quelle: BMBF.

Tabelle 2
Nanotechnologie-Förderung im internationalen Vergleich (Mio. Euro)

	2001	*2002*
Deutschland	153	198
Europa (inkl. D)	298	439
USA	467	643
Japan	500	1100

Quelle: BMBF.

So etwa verdoppeln die USA derzeit ihre Ausgaben nahezu jährlich auf einem bereits hohen Ausgangsniveau. An der amerikanischen »National Nanotechnology Initiative« sind nahezu alle großen Forschungsorganisationen des Landes und viele Bundesministerien in Washington beteiligt, darunter das Verteidigungsministerium mit dem zweitgrößten Betrag – dem größten nach dem Beitrag der National Science Foundation zugunsten der Grundlagenforschung. Einen Überblick gibt Tabelle 3.

Tabelle 3
Nanotechnologie-Initiative in den USA, Forschungsförderung von 2000 bis 2002 (Mio. Dollar)

Department (Dpt.) / Agency	*FY 2000 NNI Budget*	*FY 2001 Enacted*	*FY 2002 Request/Enacted*
Dpt. of Defense	70	110	133 /180.0
Dpt. of Energy	58	93	97 /91.1
Dpt. of Justice	–	–	1.4 /1.4
Dpt. of Transportation (FAA)	–	–	– /2
Environmental Protection Agency	–	–	5 /5
National Aeronautics and Space Administration	5	20	46 /46
National Institutes of Health	32	39	45 /40.8
National Institute of Standards and Technology	8	10	17.5 /37.6
National Science Foundation	97	150	174 /199.0
Dpt. of Agriculture	–	–	– /1.5
Total	270	422	518.9 /604.4 (+43%)

Quelle: M. C. *Roco*, National Nanotechnology Investment (NNI) in the FY 2002. Budget Request by the President, Washington, DC. 2002.

»Elektronik vom Allerkleinsten«

In den neueren amerikanischen Militärdoktrinen[10] 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.[11] Angesichts

7 *BMBF*, Nanotechnologie in Deutschland – Standortbestimmung [wie Fn. 5], S. 18.
8 Ebd., S. 19.
9 Ebd., S. 20–21.

10 John M. *Shalikashvili* (Hg.), Joint Vision 2010, Washington, DC 1996; Henry H. *Shelton* (Hg.), Joint Vision 2020, Washington, DC 2000.
11 John *Arquilla*/David F. *Ronfeldt* (Hg.), In Athena's Camp. Preparing for Conflict in the Information Age, Santa Monica,

der sich abzeichnenden nanotechnischen Hardware-Entwicklungen vermittelt die RMA bisher allerdings kaum mehr als einen ersten Vorgeschmack auf kommende informationstechnische Umwälzungen. Sie lassen sich in ihren Grundzügen wie folgt umreißen.

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.[12] Bei nanotechnisch gefertigten Speicherchips erwartet man Kapazitäten bis zu 64 Gigabytes.[13] Weitere beträchtliche Steigerungen des Datenspeichervolumens und der Datenübertragungsgeschwindigkeit lassen sich erzielen, sofern es in Zukunft gelingt, die quantenmechanischen Zustände einzelner Elektronen (die sogenannte 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 voraussichtlich 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.[14]

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.[15]

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 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 sogenannten »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 hochentwickelte C^4ISR-Technologien (command, control, communications, computing, intelligence, surveillance, reconnaissance) wird es einer High-tech-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.[16]

CA 1997; Zalmay M. *Khalilzad*/John P. *White* (Hg.), The Changing Role of Information in Warfare, Santa Monica, CA 1999.

12 »Elektronik vom Allerkleinsten« titelte hierzu die Zeitschrift Spektrum der Wissenschaft – Spezial (2001) 2; *Antón/Silberglitt/Schneider*, Global Technology Revolution [wie Fn. 1], S. 25–26.

13 1 Gigabyte = 10^9 Bytes.

14 *Antón/Silberglitt/Schneider*, Global Technology Revolution [wie Fn. 1], S. 25–26.

15 *National Research Council USA, Board on Physics and Astronomy*, Physics in an New Era, Washington, DC 2001, S. 35.

16 *Shalikashvili*, Joint Vision 2010 [wie Fn. 10]; *Shelton*, Joint Vision 2020 [wie Fn. 10]; *Computer Science and Telecommunications Board, National Research Council USA*, Realizing the Potentials of C^4I: Fundamental Challenges, Washington, DC 1999.

Biotechnologie

Die Bandbreite der modernen biotechnischen Forschung und Entwicklung ist selbst bei einer sehr kursorischen Betrachtung nahezu unüberschaubar. Im folgenden werden nur solche Gebiete berücksichtigt, die – neben zivilen, kommerziellen Anwendungen der Gentechnik – entweder zur waffentechnischen Entwicklung oder zur Biowaffenkontrolle und zum Schutz von Truppen und Zivilbevölkerung einen unmittelbaren Bezug aufweisen.[17]

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 industrielle Fortpflanzung genetisch modifizierter, identischer Organismen (Klonen).[18] 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.[19]

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).[20]

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.[21] 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 extrem 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, 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.[22]

17 Es wird damit keineswegs unterstellt, daß dieser militärische und sicherheitspolitische Bezug notwendig oder in irgendeinem Sinne typisch für biotechnische Verfahren, Erkenntnisse oder Produkte ist.

18 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.

19 *Committee on Opportunities in Biotechnology for Future Army Applications, National Research Council USA*, Opportunities in Biotechnology for Future Army Applications, Washington, DC 2001.

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

21 *Antón*/*Silberglitt*/*Schneider*, Global Technology Revolution [wie Fn. 1], S. 7.

22 Frederick B. *Rudolph*/Larry V. *McIntire* (Hg.), Biotechnology: Science, Engineering, and Ethical Challenges for the 21st Century, Washington, DC 1996; *Grace*, Botechnology [wie Fn. 20].

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.[23] 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 weitreichenden zivilen und militärischen Anwendungen entstanden.[24] Als Beispiel sei hier lediglich auf den Einfluß der Neurophysiologie und Künstlichen Intelligenz auf Sensorik, Datenverarbeitung, Test und Simulation von Wechselwirkungen Mensch–Maschine hingewiesen.[25] Wechselwirkungseffekte zwischen unterschiedlichen technischen Trends können sich sicherheitspolitisch als ebenso folgenreich erweisen wie die hier untersuchten Technologien selbst.

23 *Antón/Silberglitt/Schneider*, Global Technology Revolution [wie Fn. 1], S. 6.
24 Scott P. *Layne*/Tony J. *Beugelsdijk*/C. Kumar N. *Patel* (Hg.), Firepower in the Lab: Automation in the Fight against Infectious Diseases and Bioterrorism, Washington, DC 2001.
25 Christa *Maar*/Ernst *Pöppel*/Thomas *Christaller* (Hg.), Die Technik auf dem Weg zur Seele – Forschungen an der Schnittstelle Gehirn/Computer, Reinbek 1996; Rodney *Brooks*, Menschmaschinen – Wie uns die Zukunftstechnologien neu erschaffen, Frankfurt a.M. 2002; Claudia *Borchard-Tuch*/Michael *Groß*, Was Biotronik alles kann, Weinheim 2002.

Trends und Verwendungsmerkmale der neuen Technologien

»Dual use«

Bei den hier untersuchten Technologien ist eine eindeutige Zuordnung zur ausschließlich militärischen oder zivilen Anwendung über weite Strecken nicht erkennbar.[26] 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 sehr genau, wenn sie den informationsgesteuerten Verbund von Teilstreitkräften als ein »System von Systemen« bezeichnet.[27]

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.[28]

In Aufzählungen herkömmlicher biologischer Kampfstoffe und Waffen nehmen die einschlägigen Biotoxine, Seuchen- und Krankheitserreger oft viele Druckseiten ein.[29] 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 Know-how weltweit stark gestiegen.

26 »Dual-use«-Technologien sind als solche in der Technikgeschichte nicht neu. Doch daß handelsübliche Produkte sich in der über den Ladentisch verkauften Form auch als Rüstungsgüter optimal eignen, wie das bei informationstechnischer Hard- und Software oft der Fall ist, versteht sich keineswegs von selbst.

27 *Shalikashvili*, Joint Vision 2010 [wie Fn. 10].

28 *Interagency Working Group on Nanoscience, Engineering and Technology, National Science and Technology Council,* National Nanotechnology Initiative: Leading to the Next Industrial Revolution, Washington, DC 2000, Kap. 4; *Board on Physics and Astronomy*, *National Research Council USA,* Physics in an New Era, Kap. 8; John L. *Peterson*/Dennis M. *Egan*, Small Security: Nanotechnology and Future Defense, Washington, DC: Center for Technology and National Security Policy, National Defense University, März 2002 (Defense Horizons, No. 8).

29 Joseph *Cirincione*/Jon B. *Wolfsthal*/Miriam *Rajkumar*, Deadly Arsenals: Tracking Weapons of Mass Destruction, Washington, DC 2002, S. 57–61.

Zur Erläuterung einige Beispiele. Botulin ist eine für den Menschen hochgiftige 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).[30] 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 pharmakologische Laborexperimente mit botulinerzeugenden Bakterien und bakteriellen Viren zur Gewinnung geeigneter Impfstoffe, Antikörper und Immunglobuline.[31] 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.[32]

Ein anderes Beispiel für den ausgeprägten »dual-use«-Charakter biotechnischer Produkte und Methoden bietet die Übertragung pathogener oder tödlicher Erreger beziehungsweise Wirkstoffe durch gentechnisch modifizierte Nahrungsmittel und Mikroorganismen als Ausbreitungsmedien (Vektoren). Das Beispiel erläutert den Fall experimenteller »dual-use«-Techniken. Realisiert wurde die Möglichkeit der Übertragung von Krankheitserregern durch gentechnisch modifizierte Vektoren im Tierversuch mit dem Ziel der verstärkten Produktion des Eiweißstoffes Interleukin-4 nach Infektion von Labormäusen mit einem gentechnisch modifizierten Mäusepockenvirus als Vektor, der das Interleukin-4-Gen überträgt. Mit den Experimenten war zunächst beabsichtigt, durch eine verstärkte Interleukin-4-Produktion die Fruchtbarkeit von Mäusen zu hemmen, um auf diesem Wege Mäuseplagen zu bekämpfen. Die Experimente zeigten jedoch, daß die Übertragung des Interleukin-4-Gens eine tödliche Blockade der körpereigenen Immunreaktion gegen das Mäusepocken-Virus bewirkt. Die Versuchstiere starben selbst dann, wenn sie zuvor gegen Mäusepocken geimpft worden waren.[33] Ohne eine solche gentechnische Veränderung ist das fragliche Virus für Mäuse kaum schädlich, als Vektor für das Interleukin-4-Gen wird es zum tödlichen Seuchenerreger.

Im Gegensatz zu den »echten« Pocken (Variola vera) ist das Mäusepocken-Virus für den Menschen ungefährlich. Doch zeigt das Beispiel, daß und wie im Prinzip Immunreaktionen gegen Pockenerreger gentechnisch unterdrückt werden können.

In verschiedenen westlichen Ländern, darunter auch in Deutschland, erwägt man, 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 hochansteckende, 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.[34]

30 Judith *Miller*/Stephen *Engelberg*/William *Broad*, Germs: Biological Weapons and America's Secret War, New York 2001; Jonathan B. *Tucker*/Raymond A. *Zilinskas* (Hg.), The 1971 Smallpox Epidemic in Aralsk, Kazakhstan, and the Soviet Biological Warfare Program, Monterey, CA 2002: Center for Nonproliferation Studies, Monterey Institute of International Studies (Occasional Papers, No. 9), S. 9–11.

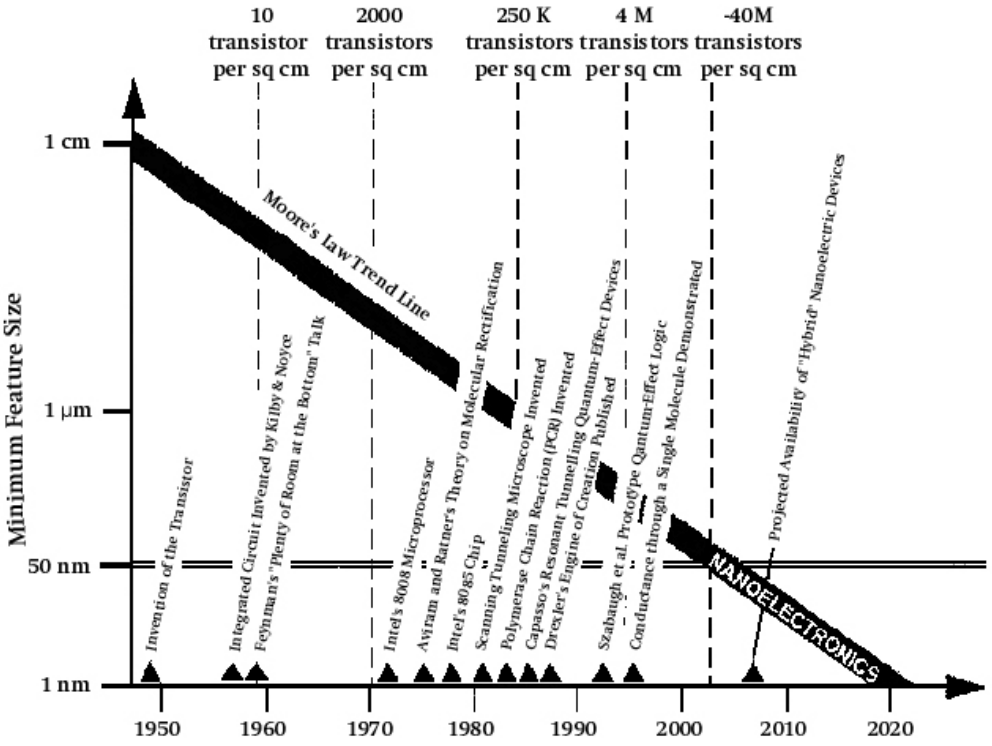
31 Stephen S. *Arnon,* Botulinum Toxin As a Bioweapon, in: *Knobler/Mahmoud/Pray*, Biological Threats [wie Fn. 20], S. 62.

32 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* (Hg.), Biological Warfare and Disarmament: New Problems/New Perspectives, Lanham, MD 2002, S. 81.

33 Ronald. J. *Jackson*/Alistair J. *Ramsay*/Carina D. *Christensen*/Sandra *Beaton*/Diana F. *Hall*/Ian A. *Ramshaw*, Expression of Mouse Interleukin-4 by a Recombinant Ectromelia Virus Suppresses Cytolytic Lymphocyte Responses and Overcomes Genetic Resistance to Mousepox, in: Journal of Virology, 75 (2001) 3, S. 1205–1210.

34 *Tucker/Zilinskas*, 1971 Smallpox Epidemic [wie Fn. 30]; Silvia P. *Westphal*, How to Make a Killer Virus, in: New Scientist, 175 (2002) 2352, S. 6–7.

Abbildung 2
Miniaturisierung in der Chiptechnik*



* Die Flächendichte der Transistoren bei handelsüblichen integrierten Halbleiterelementen (Chips) verdoppelt sich alle ein bis zwei Jahre (Gordon Moore, Intel-Mitbegründer, 1965). Der schräge schwarze Balken im Diagramm gibt die tatsächliche historische Entwicklung wieder. Sie folgt im großen und ganzen dem »Mooreschen Gesetz«.

Quelle: M. M. *Montemerlo*/J. C. *Love*/G. J. *Opiteck*/D. *Goldhaber-Gordon*/J. C. *Ellenbogen*, Technologies and Designs for Electronic Nanocomputers, Mt. Lean, VA 1996, S. 2.

Miniaturisierung

Unter Miniaturisierung versteht man die Entwicklung immer kleinerer Bauteile und Geräte bei gleichbleibender oder sogar steigender technischer Leistung. 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 (Abbildung 2). 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.[35] Für den Biowaffengebrauch sind insbesondere folgende mikrobiologischen Produkte, Eigenschaften und Verfahren wesentlich:

- Massenproduktion von gentechnisch veränderten, schädlichen Mikroorganismen;
- gentechnische Produkte, die biochemische (toxische, letale, nichtletale 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).

Hochtechnologie als handelsübliche Massenware

Viele heute bereits verfügbare »dual-use«-Produkte setzen anspruchsvolles technisches Know-how 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 entwikkeln 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,[36] 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 extreme Anforderungen an die Verarbeitung großer Datenmengen und an die automatisierte Labortechnik.[37] 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 Know-how und unverfänglicher »dual-use«-Ausrüstung. Die tatsächliche Waffenproduktion kann dann kurzfristig und nach Bedarf erfolgen.

35 A. Paul *Alivisatos*, Nanopartikel im Kampf gegen Krankheiten, in: Spektrum der Wissenschaft – Spezial (2001) 2, S. 56–63; Madeline *Drexler*, Secret Agents: The Menace of Emerging Infections, Washington, DC 2002.

36 J. Craig *Venter*, High-Throughput Sequencing, Information Generation and the Future of Biology, in: *Layne/Beugelsdijk/Patel*, Firepower [wie Fn. 24], S. 261–266.

37 *Layne/Beugelsdijk/Patel*, Firepower [wie Fn. 24].

Mikrotechnologische Herausforderungen der internationalen Sicherheit

Militärische Rüstung und Kriegführung

In sicherheitspolitischen Analysen der RMA gelten »dual-use«-Technologien als zweischneidig. Einerseits sind sie im Vergleich zu herkömmlichen, reinen Militärtechnologien preisgünstig und leistungsfähig. In der Tat haben handelsübliche Computer, Software und vorwiegend kommerziell genutzte Informationsnetze wie das Internet Entscheidendes zur RMA beigetragen.[38] Andererseits gelten moderne informationsgestützte Systeme gerade wegen ihrer weltweiten Vernetzung und öffentlichen Zugänglichkeit als verwundbar gegenüber Angriffen vom Typ des Informationskriegs (information warfare).[39] Denn elektronische Rechner, Datenspeicher, Netze und Software bieten vielfältige Schwachstellen und Angriffspunkte für die Computerspionage und die absichtliche, verdeckte Veränderung, Fälschung, Unterbrechung und Vernichtung elektronisch verbreiteter, gespeicherter und verarbeiteter Information. Militärische wie zivile Infrastrukturen (Streitkräfte, staatliche Verwaltung, Industrie, Wirtschaft, Verkehr usw.) sind daher in dem Maße in ihrer Funktionsfähigkeit gefährdet, in dem sie sich auf öffentliche, weltweit vernetzte Informations- und Kommunikationssysteme stützen.[40]

Ein Großteil der sicherheitspolitischen Problematik moderner Technologien liegt nun 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 zwiespältige Situation auf die Dauer eher verschärfen denn beseitigen. »Dual-use«-Eigenschaften, Massenproduktion und globale Verbreitung geben potentiellen Akteuren – ob Staaten, Armeen, nichtstaatlichen internationalen Organisationen oder 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[41] 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.

38 *Khalilzad/White*, Changing Role [wie Fn. 11]; *Computer Science and Telecommunications Board, National Research Council USA*, Realizing the Potentials [wie Fn. 16].

39 *Computer Science and Telecommunications Board, National Research Council USA*, Realizing the Potentials [wie Fn. 16], Kap. 3.

40 Alexander *Roßnagel*/Peter *Wedde*/Volker *Hammer*/Ulrich *Pordesch*, Verletzlichkeit der ›Informationsgesellschaft‹, Opladen 1989; Gebhard *Geiger* (Hg.), Sicherheit der Informationsgesellschaft, Baden-Baden 2000; Gebhard *Geiger*, »Information Warfare« – Bedrohung und Schutz IT-abhängiger gesellschaftlicher Infrastrukturen, in: Datenschutz und Datensicherheit, 24 (2000) 3, S. 129–136.

41 *Geiger*, Sicherheit [wie Fn. 40].

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 Wirkung 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.[42]

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 »dual-use«-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.[43] 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.[44]

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,[45] desgleichen der Einsatz bestimmter Biowaffen. Tabelle 4 (S. 18) erläutert das Verhältnis von Aufwand (Herstellungskosten) und Wirksamkeit von waffentauglichem Anthrax (Milzbranderregern) im Vergleich zu verschiedenen nichtbiologischen Waffentypen.[46] Der in der Tabelle wiedergegebene Kostenwirksamkeitsfaktor gilt als ein Indikator für die Verwendbarkeit dieses Kampfstoffs zur asymmetrischen Kriegführung. Jedenfalls war die Herstellung von Milzbranderregern und ihres hochgiftigen Wirkstoffs bereits verschiedentlich Gegenstand der gentechnischen B-Waffenforschung. Beispiele wie die des Informationskriegs und der biotechnisch erzeugten Massenvernichtungswaffen stützen die Vermutung, daß in künftigen internationalen Konflikten die Erfolgschancen asymmetrischer Strategien durch die hier untersuchten technologischen Trends begünstigt werden.

Tabelle 4
»Kostenwirksamkeit« von Massenvernichtungswaffen

Waffentyp	*Materialkosten pro qkm Wirkungsfläche (US-Dollar)*	*Waffenmaterial, das nötig ist, um 50% der Bevölkerung in einem Gebiet von 120 qkm zu töten*
konventionell	2,000	1 Megatonne
nuklear	800	50 kg
chemisch (Sarin)	600	158 t
biologisch (Anthrax)	1	6,5 kg

Quelle: *National Defense University*, Industrial Studies 200, Bio Technology, Washington, DC 2000.

42 Ken *Alibek*, Biological Weapons: Past, Present, and Future, in: *Layne/Beugelsdijk/Patel*, Firepower [wie Fn. 24], S. 177.
43 *Committee on Research and Development Needs for Improving Civilian Medical Response to Chemical and Biological Terrorism Incidents, National Research Council USA*, Chemical and Biological Terrorism: Research and Development to Improve Civilian Response, Washington, DC 1999.
44 Brian *Nichiporuk*, U.S. Military Opportunities: Information Warfare Concepts of Operation, in: *Khalilzad/White*, Changing Role [wie Fn. 11], S. 183–191; *Shelton*, Joint Vision 2020 [wie Fn. 10].
45 Gebhard *Geiger*, Offensive Informationskriegführung – Die »Joint Doctrine for Information Operations« der US-Streitkräfte: sicherheitspolitische Perspektiven, Berlin: Stiftung Wissenschaft und Politik, Februar 2002 (S 2/02), S. 12–13.
46 *National Defense University*, Industrial Studies 2000, Bio Technology, Washington, DC 2000.

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 hochansteckenden Erregern infiziert – eine Seuche auszulösen versuchen. Mit Angriffen vom Typ des Informationskriegs lassen sich im Erfolgsfall elektronisch vernetzte Bereiche des öffentlichen Lebens lähmen (cyber terrorism). 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.[47] 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.

Nichtletale 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.[48] Materialien mit neuen Eigenschaften auf nanotechnologischer Basis sowie chemische Kampfstoffe, die im Bedarfsfall betäubend wirken, sonst aber bei 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 nichtletaler 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,[49] 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 »dual-use«-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

47 *Peterson/Egan,* Small Security [wie Fn. 28].

48 E. R. *Bedard*, Nonlethal Capabilities: Realizing the Opportunities, Washington, DC: Center for Technology and National Security Policy, National Defense University, März 2002 (Defense Horizons, No. 9).

49 Alan P. *Zelikoff*, An Impractical Protocol, in: Arms Control Today, 31 (2001) 4, S. 27–31. Siehe zum Beispiel auch die Konzeptionen einer »Rüstungskontrolle im Cyberspace«, denen es an allen vernünftigen, realistischen und praktikablen Voraussetzungen mangelt; hierzu *Geiger*, Offensive Informationskriegführung [wie Fn. 45].

sich beim Versuch einer »Rüstungskontrolle im Cyberspace« in bezug auf ein geeignetes Verifikationsregime noch erheblich verschärfen.[50] 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 »dual-use«-Charakter sind es vor allem die oben dargestellten Trends und Technikfolgen, die es kaum mehr gestatten, mögliche Waffenverwendungen moderner Mikro- und Nanotechnologien selbst bei internationalen Kontrollen vom Typ der Vor-Ort-Inspektionen ausreichend zu überprüfen:

- Die extreme Miniaturisierung ihrer Bauteile macht Waffen sowie sonstige Rüstungsgüter (technische Kampfkraftverstärker, Sensoren, Navigationsgeräte für Lenkwaffen, Kampfstoffe usw.) vergleichsweise leicht handhabbar, leicht zu tarnen und zu verstekken. Größere Rüstungsproduktionsanlagen entfallen oder können leicht und ohne wesentliche Leistungseinbußen auf getrennte Standorte verteilt werden. Als Rüstungsproduktionsanlagen sind sie dann praktisch nicht mehr erkennbar.
- Hochtechnologie als global verfügbare Massenware erschließt nichtstaatlichen internationalen Organisationen (etwa Terrorgruppen) ein (Zer-)Störungspotential, das in seiner Wirksamkeit militärischen Mitteln nahekommt. Eine technisch geschickte Kopplung bestehender Trends kann Produktionskapazitäten und Produktionsgeschwindigkeit von Waffen und Kampfstoffen um Größenordnungen steigern. Dies gilt insbesondere für den computergestützten gentechnischen Entwurf, Test und Herstellung von biologischen Massenvernichtungswaffen, erst recht von solchen mit neuen, unbekannten Eigenschaften, für die keine (Immun-) Abwehr existiert.
- Produktionspotentiale wie Know-how und unverfängliche »dual-use«-Laborgeräte, mit denen aber im Bedarfsfall die Massenproduktion hochwirksamer Rüstungsgüter kurzfristig aktiviert werden kann, sind prinzipiell durch Rüstungskontrollvorschriften schwer zu erfassen, die Einhaltung solcher Vorschriften in der Praxis ebenso schwer zu verifizieren. Selbst wenn man, wie bei der Chemiewaffenkontrolle,[51] bei Verdachtsinspektionen die Beweislast für Vertragstreue im Zweifelsfall der inspizierten Partei aufbürdet, besagt der Nachweis der Vertragstreue wenig: Daß ein bestehendes »dual-use«-Potential erwiesenermaßen bisher nicht zu verbotenen Rüstungszwecken genutzt wurde, schließt nicht aus, daß dies demnächst massiv der Fall sein wird. Unter diesen Voraussetzungen kann die Vertragsverifikation kein auf die Wahrnehmung von Sachverhalten gestütztes (d.h. rationales) Vertrauen begründen.
- Um die weltweit rasch wachsende Zahl an einschlägigen biotechnischen Laboratorien, Produktionsstätten, Vertriebseinrichtungen und industriellen Anwendungen einem Verifikationsregime zu unterwerfen, müßten alle diese Einrichtungen bei einer internationalen Verifikationsbehörde deklariert werden und von dieser gegebenenfalls auch inspiziert werden können. Ähnlich absurd stellt sich die Situation in bezug auf die Offensivpotentiale des Informationskriegs dar. Hier kann im Prinzip jeder PC, der an das Internet angeschlossen ist, und jedes internetfähige Mobiltelephon die Funktion einer Offensivwaffe übernehmen – ganz zu schweigen von den zahllosen Softwareprogrammen (Viren, »hacker tools«, kryptographische Codes) mit potentiell globaler Schadenswirkung, die im Internet offen angeboten werden und die sich jedermann nach Belieben herunterladen kann.[52] In Fällen dieser Art unterscheidet sich die Verifikationsproblematik deutlich von der Situation in der herkömmlichen Nuklear- und Chemiewaffenkontrolle. Die beiden Kontrollregime erstrecken sich unter anderem auf eine eng begrenzte Anzahl deklarierter »dual-use«-Einrichtungen und -Materialien mit auffälligen, relativ leicht kontrollierbaren Betriebs- und Gebrauchsmerkmalen.
- Mit dem Verschwinden großer Rüstungsproduktionsanlagen und Waffenarsenale zugunsten mikrotechnischer Rüstungspotentiale wird die Logik der Rüstungskontrolle grundsätzlich in Frage gestellt. Produktionsanlagen und Rüstungsgüter auf »dual-use«-Basis müssen im Rahmen von Vor-Ort-Inspektionen nicht nur auf aktuelle, sondern immer auch auf potentielle Vertragsverletzungen hin überprüft werden. Zudem müssen solche potentiellen Verstöße von »falschem Alarm« unterscheidbar sein. Das Problem besteht darin, daß potentielle Sachverhalte grundsätzlich hypothetisch sind, also keine Beobachtungstatsachen. Mit anderen Worten,

50 *Geiger*, Offensive Informationskriegführung [wie Fn. 45].
51 Übereinkommen über das Verbot der Entwicklung, Herstellung, Lagerung und des Einsatzes chemischer Waffen und über die Vernichtung solcher Waffen, Anhang 2: Anhang über die Durchführung und Verifikation, Teil II, Absatz 51.

52 *Geiger*, Offensive Informationskriegführung [wie Fn. 45].

Verifikationsaufgaben in diesem Bereich können prinzipiell nicht durch reine Beobachtung (Augenschein, Messungen, Zählungen, chemische Analysen usw.) im Rahmen von Vor-Ort-Inspektionen gelöst werden. Das Vorhandensein von »dual-use«-Einrichtungen und -Materialien kann nicht einmal als Indiz für ein Vergehen gewertet werden, sofern nicht zusätzliche Verdachtsmomente für einen akuten oder unmittelbar bevorstehenden (also gerade keinen potentiellen!) Vertragsverstoß sprechen.

Rüstungskontrollverträge wie das internationale Chemiewaffenabkommen von 1993 sehen meist aufwendige Klärungsverfahren vor, um diese Probleme wenn schon nicht zu vermeiden, so doch wenigstens handhabbar zu machen. In der Verifikationspraxis ist immer mit Klärungsbedarf dieser Art zu rechnen, weil jeder legale, zivile oder defensive Gebrauch der fraglichen Technologien als ein potentieller Vertragsverstoß mißverstanden werden kann. Aber nicht nur die der Kontrolle unterliegenden Technologien, sondern das Verifikationsregime als solches kann immer auch zu politischen Zwecken mißbraucht werden. So kann etwa eine Vertragspartei die zivile (defensive) Nutzung einer Technologie durch eine andere Partei vorsätzlich falsch interpretieren und ihr in agitatorischer Absicht einen Verstoß unterstellen. Sie kann dies tun, um die andere Partei politisch zu diskreditieren, sie außenpolitisch unter Druck zu setzen, sie zu bedrohen oder gar mit einem wohlfeilen Vorwand einen geplanten militärischen Angriff gegen sie als Präventivschlag zu tarnen. Bei herkömmlichen Verifikationsregimen wie beispielsweise dem des Chemiewaffen-Abkommens sind diese Möglichkeiten des Mißbrauchs gering, da Untersuchungen von, und das Urteil über Vertragsverstöße dem Exekutivrat und Technischen Sekretariat der Vertragsorganisation obliegen und nicht den einzelnen Vertragsstaaten. Bei der Kontrolle der hier vorgestellten neuen Mikrotechnologien sind aber die Überprüfungsmethoden und das Urteilsvermögen internationaler Behörden naturgemäß stark eingeschränkt, was umgekehrt willkürlichen Interpretationen und Maßnahmen einzelner Staaten mehr Spielraum läßt. Offenbar ist genau dies die Auffassung der amerikanischen Regierungsbehörden in bezug auf die Verfikationsmöglichkeiten der Biowaffenkontrolle[53] und die Kontrollierbarkeit von Offensivwaffen des Informationskriegs.[54]

Die mikrotechnologische Herausforderung der Exportkontrolle

Auf die gleichen prinzipiellen Schwierigkeiten trifft die Exportkontrolle im Falle moderner Mikrotechnologien. Vorliegende Spezialuntersuchungen zur Exportkontrolle bei elektronischen Bauteilen für Hochleistungsrechner, optoelektronischen Geräten sowie rüstungstauglichen Kunststoffen und Materialien bestätigen dies in allen Einzelheiten.[55] Bei allen diesen potentiellen Rüstungsgütern handelt es sich um Produkttypen, die in naher Zukunft sowohl in ihrer technischen Leistung wie in ihrer »dual-use«-Fähigkeit durch nanotechnische Entwicklungen noch erheblich gesteigert werden. Ihre »dual-use«-Eignung, aber auch praktische Probleme bei der Kontrolle von Miniaturgeräten und -bauteilen (Entdecken, Identifizieren, Statistik, Dunkelziffern usw.), stellen die Exportkontrolle von Rüstungsgütern vor kaum mehr lösbare Aufgaben. »Kontrollierbarkeit hängt ... nicht nur von den speziellen Eigenschaften einer Technologie ab, sondern von ihrer Verfügbarkeit auf den globalen Märkten und von den organisatorischen und betrieblichen Rahmenbedingungen ihrer Verbreitung und Nutzung. Besonders problematisch ist die Kontrolle hochleistungsfähiger Informationstechnologie und ihrer Komponenten (Software, Mikroprozessoren, Betriebssysteme). Die für eine Kontrolle relevanten Eigenschaften variieren stark, und aufgrund hoher technologischer Entwicklungsraten und weltweiter Verbreitung ist innovative Spitzentechnologie dem Standard meist nur um wenige Jahre voraus.«[56]

Angesichts der neuen Herausforderungen für die Exportkontrolle gelten wirtschaftliche Anreize zur Kooperation zwischen Exportländern und Empfängern als geeignet, die Verbreitung rüstungstauglicher

53 Michael *Moodie*, Building on Faulty Assumptions, in: Arms Control Today, 34 (2001) 4, S. 20–22.

54 *Geiger,* Offensive Informationskriegführung [wie Fn. 45].
55 *Office of International Affairs, National Research Council USA* (Hg.), Dual-Use Technologies and Export Control in the Post-Cold War Era, Washington, DC 1994; Lynn E. *Davis*, Arms Control, Export Regimes, and Multilateral Cooperation, in: *Khalilzad/White*, Changing Role [wie Fn. 11], S. 361–377.
56 Seymour *Goodman*/Vladimir *Levin*/Ivan *Safranov*/Peter *Wolcott*/Aleksey *Zabrodin*, High-Performance Computing: Controllability and Cooperation, in: *Office of International Affairs, National Research Council USA*, Dual-Use Technologies [wie Fn. 55], S. 35.

Mikrotechnologien einzudämmen. In begrenztem Umfang liegen hierzu positive Erfahrungen über den Export von westlichen »dual-use«-Technologien in die ehemaligen Ostblockstaaten und in Drittweltländer vor.[57]

Daß für eine Kooperation bei der Proliferationskontrolle immer der notwendige wirtschaftliche Anreiz besteht, muß jedoch bezweifelt werden. In Zukunft wird möglicherweise das Gegenteil zur Regel werden. Der wirtschaftliche Anreiz zur Verbreitung technischer Innovationen kann für viele Exportländer überwiegen, selbst wenn sie befürchten müssen, daß die Exportgüter zu Rüstungszwecken verwendet werden. Vergleichsfälle dieser Art sind aus der Exportkontrolle nuklearer Reaktortechnologien bekannt.[58] Jedenfalls ist damit zu rechnen, daß sich die Interessenlage vieler Handelspartner beim Export von nichtnuklearen »dual-use«-Technologien in Zukunft ähnlich darstellt.

Negative Ergebnisse dieser Art sind erst recht zu erwarten, wenn terroristische Motive beim Verkauf oder Erwerb von Hochtechnologie- und Massenvernichtungswaffen im Spiel sind. Dann muß der ökonomische Anreiz zur Kooperation bei der Nichtverbreitung als Instrument der Exportkontrolle von vornherein versagen.

57 *Office of International Affairs, National Research Council USA* (Hg.), Dual-Use Technologies [wie Fn. 55].

58 Zum Beispiel der russische nukleare Technologietransfer nach Iran; vgl. hierzu Andrew *Koch*/Jeanette *Wolf*, Iran's Nuclear Facilities: a Profile, Monterey, CA: Center for Non-Proliferation Studies, 1998.

Sicherheitspolitische Aufgaben und Lösungsansätze

Die skizzierten technologischen Trends stellen jetzt und in Zukunft eine Reihe von sicherheitspolitischen Aufgaben, die sich aus deutscher Sicht wie folgt umreißen lassen.

Für moderne Streitkräfte wird die RMA kein zeitlich begrenzter Umwälzungsprozeß bleiben, der früher oder später wieder längere rüstungstechnische Innovationszyklen beschert und längerfristige Beschaffungsprogramme zuläßt. Die hier untersuchten Trendmerkmale moderner Mikrotechnologien deuten vielmehr darauf hin, daß der rasche, tiefgreifende technische Wandel für die Streitkräfte ein Dauerzustand bleiben wird. Seine Auswirkungen erstrecken sich gleichermaßen auf Bewaffnung, Führungs-, Nachrichten-, Aufklärungs- und Transportsysteme sowie natürlich auch auf die zivilen, technisch-wirtschaftlichen Rahmenbedingungen der Rüstungsplanung beziehungsweise des Streitkräfteeinsatzes.

Die dargestellten technologischen Trends können neuartige, erhebliche Gefährdungen der internationalen Sicherheit hervorrufen. Durch eine extrem gesteigerte Wirksamkeit bei gleichzeitiger ziviler, kommerzieller Verbreitung erschließen moderne Technologien auch nichtstaatlichen internationalen Organisationen 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. Ob und inwieweit einzelne Staaten oder auch Terrorgruppen bereits heute oder in absehbarer Zukunft dieses technologische Potential zu nutzen in der Lage sind, ist für ein grundlegendes sicherheitspolitisches Verständnis der neuen Herausforderungen unerheblich.

In dieser Lage benötigen Deutschland und seine EU-Partner auch weiterhin 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 innovativen Grundlagenforschung ebenfalls profitieren. So gesehen, ist beispielsweise die intensive Förderung der Nanotechnik durch Staat und Industrie in Deutschland[59] sowie durch das 6. EU-Rahmenprogramm[60] angemessen. Denn nur wenn die europäischen Länder die neuen Technologien selbst mitentwickeln und beherrschen lernen, können sie auch deren sicherheitspolitischen Herausforderungen erfolgreich begegnen.

Was hingegen gerade angesichts dieser Herausforderungen in den deutschen und europäischen Förderprogrammen über weite Strecken fehlt, ist die Sicherheits- und sicherheitspolitische Komponente. Art und Ausmaß der Lücken sollen hier anhand zweier Vergleiche kurz erläutert werden.

Zum einen ist der Blick auf den Anteil des amerikanischen Verteidigungsministeriums am Forschungsetat der »National Nanotechnology Initiative« der USA aufschlußreich (Tabelle 3, S. 9). Er zeigt, daß in vergleichbaren deutschen und europäischen Forschungsprojekten die Auswirkungen der Nanotechnologie auf die militärische Sensorik, Logistik, Automatisierung, künstliche Intelligenz und zahlreiche weitere Rüstungsgebiete (Tabellen 5 und 6, S. 24f) nicht angemessen berücksichtigt werden.[61] Sofern die wehrtechnische Entwicklung in Europa von einer direkten Beteiligung an diesen Programmen ausgeschlossen bleibt und insbesondere die Bundeswehr darauf verzichten muß, die technische Innovation sozusagen aus erster Hand zu nutzen, kann von der überfälligen Modernisierung der deutschen Streitkräfte nicht nur keine Rede sein – die Bundesrepublik setzt auch ihre Bündnisfähigkeit im Kreise der High-Tech-Armeen in der NATO aufs Spiel. Die militärischen Vorteile, die Spitzentechnologie bietet, werden verschenkt. Das Pentagon hat in den zurückliegenden Jahren eine ganze Generation neuer Technologien entwickelt. Viele dieser Entwicklungen

59 *BMBF*, Nanotechnologie in Deutschland – Standortbestimmung [wie Fn. 5].

60 *European Commission*, The Sixth Framework Programme in Brief, Brüssel 2002.

61 In den einschlägigen Programmen fehlt jeglicher Hinweis auf Nanotechnologie im Kontext von Verteidigung und Sicherheitspolitik. Vgl. etwa *BMBF*, Nanotechnologie in Deutschland – Standortbestimmung [wie Fn. 5]; *BMBF*, Nanotechnologie in Deutschland – Strategische Neuausrichtung, Bonn 2002; *European Commission*, Sixth Framework [wie Fn. 60].

Tabelle 5
Militärische Nutzungsmöglichkeiten der Nanotechnologie*

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, hochmobile funkgestützte Systeme zur abstandsfähigen Gefechtsfeldüberwachung.
3. Erhöhte menschliche Leistungsfähigkeit durch verbesserte Überwachungssysteme einschließlich der Messung physiologischer Zustände der Soldaten.
4. Informationsdominanz durch leistungsfähigere IT. 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.

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

Tabelle 6
Mittelfristig verfügbare militärische Nutzungsmöglichkeiten für intelligente Hochtechnologien aus Sicht des Pentagon*

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 hochentwickelte 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.

Quelle: Hans *Binnendijk*/Richard L. *Kugler*, Managing Change: Capability, Adaptability, and Transformation, Washington, DC: Center for Technology and National Security Polics, National Defense University, Juni 2001 (Defense Horizons, No. 1), S. 5.

werden mittelfristig einsatzbereit sein und die US-Streitkräfte erheblich stärken.

Zum anderen fehlt der Bundesrepublik seit vielen Jahren eine angemessene sicherheits- und technologiepolitische Antwort auf die Gefährdungen ihrer mikroelektronisch vernetzten Systeme und Infrastruktur.[62] Es ist damit zu rechnen, daß mit der weiter fortschreitewnden Miniaturisierung von Informationssystemen auf nanotechnischer Grundlage auch die sicherheitspolitische Kontrolle dieser Systeme schwächer wird, während das Potential für politischen und kriminellen Mißbrauch wächst.

Frühwarnung, Abschreckung und Vergeltung von Bedrohungen beziehungsweise Verletzungen der internationalen Sicherheit werden durch die Miniaturisierung moderner Waffensysteme erschwert. Um so notwendiger sind defensive Strategien und Maßnahmen zum Schutz, zur Abwehr und zur Schadensprävention im Verteidigungsfall. Die Bundesrepublik und ihre Verbündeten können sich verstärkt mit Maßnahmen auf folgenden Gebieten schützen:

- Passive Sicherheit von Personen (Truppen, Zivilbevölkerung) und Infrastruktureinrichtungen durch geeignete technische, medizinische, gesetzliche, organisatorische Vorkehrungen gegen den Mißbrauch moderner Technologien, die sich aufgrund ihrer Tendenz zur Miniaturisierung bei uneingeschränkter öffentlicher Verfügbarkeit, ihrer Leistungsmerkmale und ihrer spezifischen Anwendungsbedingungen einer wirksamen sicherheitspolitischen Kontrolle entziehen.
- Verstärkte sicherheitspolitische Ausrichtung des Gesundheitswesens und des Katastrophenschutzes angesichts der modernen mikrobiologischen Herausforderungen der inneren und äußeren Sicherheit.
- Angemessene Ausweitung des Zivilschutzes über seine bisherigen, auf den rein militärischen Verteidigungsfall bezogenen Aufgaben hinaus.

Die beiden letztgenannten Punkte betreffen insbesondere Vorbereitungen für einen ausreichenden Impfschutz und breitangelegte Therapiemaßnahmen im Fall eines Angriffs mit mikrobiologischen Waffen. Hinzu kommt die Bereitstellung einer leistungsfähigen Labortechnik und Datenverarbeitung zur schnellen Identifikation und Analyse neuartiger gentechnisch produzierter Kampfstoffe im Angriffsfall sowie eine leistungsfähige sicherheitspolitisch orientierte Technikfolgenforschung auf dem Gebiet mikrophysikalischer und -biologischer Technologien.

Eine neue Sicherheitspolitik ist auch angesichts des dargestellten, technologisch bedingten Verifikationsdilemmas in der internationalen Rüstungskontrolle erforderlich. Offenbar sind die USA zunehmend geneigt, sich in Fragen der Vertragstreue von Rüstungskontrollpartnern auf ihre eigene zivile und militärische geheim- und nachrichtendienstliche Aufklärung statt auf die Vertragsverifikation zu verlassen.[63] Dies wird an ihren Vorbereitungen zum offensiven Informationskrieg ebenso deutlich wie an ihrer ablehnenden Haltung gegenüber einem vertraglichen Verifikationsregime in der Biowaffenkontrolle.[64] Unabhängig davon, ob andere Länder eine Rüstungskontrolle im »cyber space« und ein Biowaffen-Verifikationsregime bevorzugen: Es wird ihnen mangels Alternativen nichts anderes übrigbleiben, als entweder ebenfalls zu einseitigen, nichtkooperativen Überwachungsmethoden zu greifen oder eben auf beide, Aufklärung und Verifikation, zu verzichten. Mit anderen Worten, sie werden entweder dem amerikanischen Beispiel mehr oder weniger folgen oder vor den sicherheitspolitischen Herausforderungen neuer mikrotechnologischer Trends überhaupt die Augen verschließen müssen. Jedenfalls ist davon auszugehen, daß künftige Rüstungstechnologien auf »dual-use«-Basis die Möglichkeiten der Vertragsverifikation in der internationalen Rüstungskontrolle immer weiter einschränken werden.

62 *Geiger*, Sicherheit[wie Fn. 40]; *ders.*, »Information Warfare« [wie Fn. 40]; Gebhard *Geiger*, Information und Infrastruktursicherheit – Grundzüge eines sicherheits- und technologiepolitischen Forschungs- und Entwicklungsprogramms, unveröffentlichtes Arbeitspapier, Ebenhausen: Stiftung Wissenschaft und Politik, 2000.

63 Kurz bevor die USA die Genfer Verhandlungen zum Biowaffen-Verifikationsregime scheitern ließen, wurde im März 2001 eine neue CIA-Behörde, Weapons Intelligence, Nonproliferation and Arms Control Center, mit nicht weniger als 500 (!) Mitarbeitern gegründet. Ihre Aufgabe ist es, »den [...] Präsidenten und Kongreß über globale Fragen der Nichtverbreitung und Rüstungskontrolle besser zu informieren«; Bericht von V. *Loeb*, CIA Is Stepping Up Attempts to Monitor Spread of Weapons, in: Washington Post, 12.3.2001, S. A15.

64 Information Warfare Doctrine; *Geiger*, Offensive Informationskriegführung; O. *Meier*, Neither Trust nor Verify, Says US, in: The Bulletin of the Atomic Scientists, 57 (2001) 6, S. 19–21.

Abkürzungen

BMBF	Bundesministerium für Bildung und Forschung
BMWi	Bundesministerium für Wirtschaft und Technologie
C^4ISR	Command, Control, Communications, Computing, Intelligence, Surveillance, Reconnaissance
CIA	Central Intelligence Agency
FAA	Federal Aviation Agency
FY	Fiscal Year
NNI	National Nanotechnology Investment
RMA	Revolution in Military Affairs