**Heiko Borchert**

Strategische Analysen

# Vernetzte Sicherheitspolitik

## Politisch-strategische Implikationen eines neuen Leitbildes

---

Wien, im
Februar 2004

Büro für
Sicherheitspolitik

*Der Autor:*

***Heiko Borchert leitet ein Unternehmens- und Politikberatungsbüro und ist Direktor für Sicherheit und Verteidigung am Düsseldorfer Institut für Außen- und Sicherheitspolitik (DIAS).***

***Eine leicht überarbeitete Fassung dieses Beitrags erscheint demnächst in: Heiko Borchert (Hrsg.), Vernetzte Sicherheit. Leitidee der Sicherheitspolitik im 21. Jahrhundert (Hamburg: Verlag E.S. Mittler & Sohn, 2004).***

## Impressum

Herausgeber und für den Inhalt verantwortlich:
Sektionschef Hon.Prof. DDr. Erich Reiter
Redaktion: Mag. Walter Matyas, Doris Washiedl
Korrektorat: Doris Washiedl, Melitta Strouhal
Eigentümer, Verleger und Hersteller:
Büro für Sicherheitspolitik des
Bundesministeriums für Landesverteidigung

Amtsgebäude Stiftgasse 2a, 1070 Wien
Tel. (+43-1) 5200/27000, Fax (+43-1) 5200/17068
Gestaltung: Doris Washiedl
Vervielfältigung: Vzlt Johann Jakob
Druck- und Reprostelle der Landesverteidigungsakademie Wien

Aktuelle Informationen zu Publikationen des Büros für Sicherheitspolitik und der Landesverteidigungsakademie finden Sie im Internet:

**<http://www.bundesheer.at/wissen-forschung/bsp/publikat.shtml>**

# Inhaltsverzeichnis

„Too many of the new [security] missions are institutionally 'homeless': nowhere are clear authority, adequate resources, and appropriate accountability brought together in a clear managerial focus."

Ashton B. Carter[1]

„Each nation must review national legal or political restrictions or caveats which reduce the usability of deployed forces."

George Robertson[2]

## Zusammenfassung

„Die netzwerkzentrierte Kriegführung (Network Centric Warfare – NCW) oder, breiter gefasst, die vernetzte Operationsführung stellt im Kern die richtige Antwort auf die neuen sicherheitspolitischen Herausforderungen dar. Diese können nur dann effektiv gelöst werden, wenn es gelingt, die Ziele, die Prozesse und die Strukturen sowie die Fähigkeiten und die Mittel der relevanten Akteure systematisch miteinander zu vernetzten. Diese Einsicht darf jedoch nicht bloß auf den Verteidigungsbereich beschränkt bleiben, sondern muss konsequent auf alle Akteure des Sicherheitssektors – das heißt militärische, polizeiliche, paramilitärische Streitkräfte, Grenzschutz, Nachrichtendienste, die entsprechenden Ministerien sowie die politischen Aufsichts- und Koordinationsorgane – ausgeweitet werden."

Das daraus resultierende Leitbild der vernetzten Sicherheitspolitik ist mit weitreichenden Konsequenzen verbunden. Die Forderung nach sicherheitspolitischer Vernetzungsfähigkeit verstärkt den Druck zur kompatiblen Ausgestaltung der politischen Systeme, führt zu einer neuen und erweiterten Betrachtungsweise der Koalitions- und Zusammenarbeitsfähigkeit, die alle Akteure des Sicherheitssektors und die Industrie umfassen muss, erhöht die Komplexität des Managements des vernetzten Sicherheitssektors, lenkt den Blick auf vernetzte Fähigkeiten, die von allen Sicherheitsakteuren gemeinsam genutzt werden, und bedingt neue Formen der Zusammenarbeit zwischen dem Sicherheitssektor und der Rüstungsindustrie sowie anderen sicherheitspolitisch relevanten Industriezweigen.

Die beiden Eingangszitate beschreiben das Spannungsfeld, in dem sich moderne Sicherheitspolitik bewegt: Einerseits ist der Sicherheitssektor nur schlecht auf die neuen Sicherheitsrisiken vorbereitet, andererseits liegt es gerade in der Natur dieser Risiken, dass sie oftmals ein schnelles und abgestimmtes Vorgehen erfordern, um die vorhandenen Mittel erfolgreich zu deren Bekämpfung einsetzen zu können.

Diese Einsicht ist nicht wirklich neu. Die Ereignisse der jüngsten Vergangenheit wie die unzureichende Zusammenarbeit der US-Nachrichtendienste im Vorfeld der Anschläge vom 11. September 2001 oder die Schwierigkeiten der Abstimmung verschiedener Sicherheitskräfte im Inland beziehungsweise im Rahmen von internationalen Operationen haben die damit verbundenen Probleme lediglich sehr plastisch vor Augen geführt. Gleichwohl wurde bislang mit zu wenig Nachdruck an der Umsetzung der aus dieser Einsicht resultierenden Konsequenzen gearbeitet.

Sicherheitspolitik kann heute weder ausschließlich national noch ressortspezifisch betrieben werden, sondern erfordert internationale und ressortübergreifende Konzeption und Koordination. In einem umfassenden Verständnis von Sicherheit ist die Verteidigung einer von mehreren Politikbereichen und das Militär eines von mehreren Instrumenten. Militärisch relevante Konzepte und Entwicklungen müssen daher vor diesem umfassenden Hintergrund interpretiert werden. Das gilt insbesondere für die Vision der vernetzten Operationsführung, die im Kern die richtige Antwort auf die neue Herausforderung gibt – nämlich die Vernetzung der relevanten Akteure, ihrer Mittel und ihrer Organisationen.[3]

Im vorliegenden Aufsatz geht es darum, die gedankliche Brücke von der vernetzten Operationsführung als spezifische Anwendung zur vernetzten Sicherheitspolitik als neue Leitidee zu schlagen. Zu diesem Zweck begründet das erste Kapitel zunächst die Notwendigkeit des Übergangs zur vernetzten Sicherheitspolitik. Daran anschließend werden die Herausforderungen und die Konsequenzen der vernetzten Sicherheitspolitik mit Blick auf fünf Kernbereiche analysiert. Dem folgen einige Überlegungen zur

---

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

2 George Robertson, „Securing the Peace: The NATO Vision", Secretary General's Speech at the NATO Public Diplomacy Conference, Brussels, 16 October 2003 <http://www.nato.int/docu/speech/2003/s031016c.htm> (Zugriff: 20.1.2004).

3 So auch: Holger H. Mey und Michael K.-D. Krüger, *Vernetzt zum Erfolg? „Network-Centric Warfare" – zur Bedeutung für die Bundeswehr*, ISA-Studie Nr. 9 (Frankfurt: Report Verlag, 2003), S. 16.

künftigen Rolle sicherheitspolitischer Vernetzungsorgane und zum europäischen Handlungsbedarf.

## 1. Vernetzte Sicherheitspolitik

Im Wesentlichen bedingen drei Entwicklungen den Übergang von der ressortgesteuerten zur vernetzten Sicherheitspolitik (Abbildung 1):[4]

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

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

*EU-Entwicklung:* In Europa erhöht die Vertiefung und die Erweiterung der EU den Druck zur kohärenten Politikvorbereitung und -umsetzung. Inhaltlich müssen die vielfältigen und teilweise neuen Instrumente der Außen-, Sicherheits- und Verteidigungspolitik der EU besser mit den vorhandenen Instrumenten der Außenwirtschafts-, Entwicklungs-, Justiz- und Innenpolitik abgestimmt werden.

„In contrast to the massive visible threat in the Cold War, none of the new threats is purely military; nor can any be tackled by purely military means. Each requires a mixture of instruments. Proliferation may be contained through export controls and attacked through political, economic, and other pressures while the underlying political causes are also tackled. Dealing with terrorism may require a mixture of intelligence, police, judicial, military and other means. In failed states, military instruments may be needed to restore order, humanitarian means to tackle the immediate crisis. Regional conflicts need political solutions but military assets and effective policing may be needed in the post conflict phase. Economic instruments serve reconstruction, and civilian crisis management helps restore civil government. The European union is particularly well equipped to respond to such multi-faceted situations".[5]

Das bleibt nicht ohne Rückwirkung auf die nationalen Planungen und Konzepte in diesen Politikbereichen sowie deren Abstimmung mit internationalen Beschlüssen.

Diese drei politischen Treiber erklären, weshalb die sicherheitspolitische Vernetzung immer wichtiger wird. Daneben gilt es aufgrund des *technologischen Fortschritts* einen vierten Aspekt zu berücksichtigen, der diese Vernetzung im Sinne der technischen Verknüpfung der Sicherheitsministerien und -akteure auch tatsächlich möglich macht. Die daraus resultierenden Optionen wurden in den neunziger Jahren vor allem von den US-amerikanischen Streitkräften erkannt und unter dem Hinweis auf eine sich abzeichnende „Revolution in Military Affairs" (RMA) in neuen Konzepten umgesetzt.[6] Die Idee der vernetzten

---

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

[5] European Security Strategy, 18595/03, Brüssel, 8. Dezember 2003, S. 9 <http://register.consilium.eu.int/pdf/en/03/st15/st15895.en03.pdf> (Zugriff: 30. Dezember 2003).

[6] Hierzu grundlegend: *Joint Vision 2010* (Washington, D.C.: US Joint Chiefs of Staff, 1996), <http://www.dtic.mil/jv2010/jv2010.pdf> (Zugriff: 20.1.2004); *Joint Vision 2020* (Washington, D.C.: US Joint Chiefs of Staff, 2000), <http://www.dtic.mil/jointvision/jvpub2.htm> (Zugriff: 20.1.2004); Bill Owens with Ed Offley, *Lifting the Fog of War* (Baltimore, London: The Johns Hopkins University Press,

Operationsführung stellt die logische Fortsetzung der vor allem auf das Ziel der Informationsüberlegenheit ausgerichteten Bemühungen dar. Ziel ist es „[to network] sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization".[7] Die wesentlichen Vorteile liegen in der erhöhten Transparenz hinsichtlich des Lagebildes (Battlespace Awareness), der Verkürzung der Entscheidungsprozesse, der Erhöhung des Operationstempos und der verbesserten Wirkung im Einsatz. Wie in der Folge dargestellt wird, lassen sich diese Überlegungen sinngemäß auf die Reorganisation des gesamten Sicherheitssektors übertragen.

Die aus den angesprochenen Entwicklungen abgeleitete Forderung nach einer sicherheitspolitischen Vernetzung basiert auf der Einsicht, dass sicherheitsrelevante Akteure die aktuellen und künftigen Herausforderungen nur dann meistern können, wenn sie ihre Ziele, ihre Prozesse und Strukturen sowie ihre Fähigkeiten und Mittel bewusst miteinander vernetzen.[8] Neu an diesem Verständnis sind die Erweiterung des Kreises der relevanten Akteure sowie die bewusste Durchbrechung bestehender Organisationsgrenzen. Sicherheitspolitische Vernetzungsfähigkeit bezieht sich demzufolge auf

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

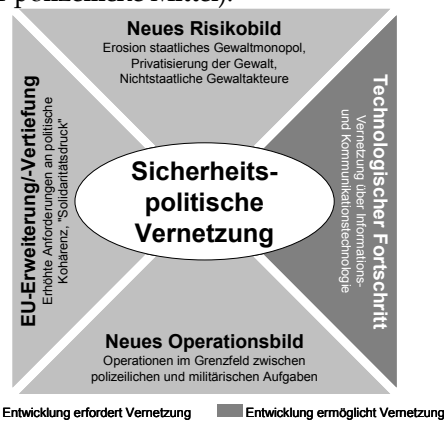


Abbildung 1: Treiber der sicherheitspolitischen Vernetzung

Dieses vernetzte Verständnis von Sicherheit liegt auch implizit dem neuen Sicherheitskonzept Österreichs zugrunde. Dieses folgt der Leitidee der umfassenden Sicherheitsvorsorge und basiert auf drei Prinzipien:

- Die *umfassende Sicherheit* betont den Querschnittscharakter der Sicherheitspolitik und legt die enge Verzahnung der unterschiedlichen Politikbereiche nahe.
- Die *präventive Sicherheit* stellt auf die Konfliktvermeidung durch die vorteilhafte Gestaltung des sicherheitspolitisch relevanten Umfelds ab und unterstreicht vor allem die Notwendigkeit der engen Abstimmung zwischen den involvierten Akteuren und dem Einsatz der unterschiedlichen sicherheitspolitisch relevanten Instrumente.
- Schließlich betont das Prinzip der *europäischen Solidarität* die Unteilbarkeit von Sicherheit und legt die enge Koordination zwischen der internationalen und der nationalen Ebene nahe.[9]

Die Forderung nach konsequenter sicherheitspolitischer Vernetzung hält Herausforderungen von neuer Komplexität bereit. Das gilt für die Reform der militärischen Streitkräfte genauso wie für die Neugestaltung der nationalen sowie der internationalen Sicherheitssektoren. In vielerlei Hinsicht ist die Reform der Sicherheitssektoren

2001); Eliot A. Cohen, „A Revolution in Warfare", *Foreign Affairs* 75:2 (March/April 1996), S. 37–54; Michael O'Hanlon, *Technological Change and the Future of Warfare* (Washington, D.C.: Brookings, 2000).

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

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

9 *Umfassende Sicherheitsvorsorge. Das sicherheitspolitische Konzept Österreichs* (Wien: Dezember 2002), S. 5–6. Mit Blick auf die daraus resultierenden Konsequenzen hat Bundespräsident Klestil kürzlich zum Überdenken der Neutralität aufgerufen. Siehe: Thomas Klestil, „TV-Ansprache des Bundespräsidenten vom 1.1.2004" <http://www.hofburg.at/de/praesidenten/klestil/reden2004/inla/Neujahr.pdf> (Zugriff: 20.1.2004).

sogar die Voraussetzung, damit die militärischen Streitkräfte reibungslos mit den anderen Sicherheitskräften kooperieren können und dadurch maximale Synergiegewinne realisiert werden. „If adapting to wartime conditions is desperately difficult", so führen MacGregor Knox und William Murray in ihrer Untersuchung über historische und künftige militärische Revolutionen aus, „those involved in peacetime innovation confront almost insoluble problems: it is here that the leaders of military institutions earn their pay".[10] Diese Schlussfolgerung kann nahtlos auf die Erwartungen an die politischen Entscheidungsträger übertragen werden, denn es sind in erster Linie diese, die die Grundlagen für die sicherheitspolitische Vernetzung schaffen müssen.

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

## 2. Kompatibilität der politischen Systeme

Die Befürworter der vernetzten Operationsführung argumentieren, dass der erhöhte Informationsaustausch die Qualität der Information steigert, die Aussicht auf ein gemeinsames Lagebild verbessert und damit die enge Zusammenarbeit und die teilautonome Führung (Self-Synchronization) der an einer Operation Beteiligten ermöglicht.[11] Die Realisierung dieser Vorteile steht jedoch unter einem Vorbehalt:

The „operations an RMA [Revolution in Military Affairs] will make possible and necessary will not achieve their most potent form unless the interagency process can meet the demands of revolutionized military forces. (…) If operations are too fast for coordination with policymakers, then they will be ineffective, no matter how successful militarily, because they will unfold before policy can properly shape them. Worse, operations may present policymakers with faits accomplis and thus determine policy".[12]

Diese Feststellung lenkt die Aufmerksamkeit auf einen bislang eher vernachlässigten Punkt: die Kompatibilität der politischen Systeme der an multinationalen Operationen beteiligten Staaten. Marc Houben und Dirk Peters haben kürzlich darauf hingewiesen, dass die erfolgreiche Entsendung multinationaler Einheiten ohne Synchronisation der Entscheidungsprozesse der daran beteiligten Staaten kaum möglich ist.[13] Die Bedeutung dieses Aspekts ergibt sich im Wesentlichen aus drei Punkten: Erstens werden multinationale Operationen mit Beteiligung militärischer und anderer Sicherheitskräfte künftig den Standardrahmen internationaler Einsätze bilden. Zweitens sieht der Entwurf des EU-Verfassungsvertrags die Einführung der Prinzipien der strukturierten Zusammenarbeit im

---

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

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

12 David Tucker, „The RMA and the Interagency: Knowledge and Speed vs. Ignorance and Sloth", *Parameters* 30:3 (Autumn 2000), S. 66–76 <http://www.carlisle.army.mil/usawc/Parameters/00autumn/tucker.htm> (Zugriff: 20.1. 2004), S. 2, 5 (Internetversion).

13 Marc Houben and Dirk Peters, *The Deployment of Multinational Military Formations: Taking Political Institutions into Account,* CEPS Policy Brief No 36 (Brussels: Centre for European Policy Studies, 2003), S. 1 <http://shop.ceps.be/downfree.php?item_id=1038?> (Zugriff: 20.1.2004).

militärischen Bereich vor und erhöht damit die Komplexität der intergouvernementalen Entscheidungsfindung.[14] Drittens steht vernetzte Operationsführung in unmittelbarem Zusammenhang mit der Idee wirkungsorientierter Operationen (Effects Based Operations), wobei deren Möglichkeiten und Grenzen vor allem in internationalen Koalitionen wesentlich durch die Kohärenz der daran teilnehmenden Partner und deren Verhalten bestimmt werden.[15]

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

### 2.1. Inhaltliche Kompatibilität

In diesem Bereich sind zuerst die bekannten Unterschiede zwischen den nationalen Sicherheitskulturen anzusprechen, die sich auf die grundsätzliche Bereitschaft zum Einsatz militärischer Streitkräfte sowie die damit verbundenen Vorgaben auswirken.[16] Wenn die Annahme zutrifft, dass es über die vernetzte Operationsführung zu einer Angleichung der militärischen Doktrin auf dem Weg der Technologieintegration kommt, dann ist es entscheidend, welcher Staat beziehungsweise welche Staatengruppe federführend ist – zumindest so lange, wie nationale Unterschiede in der Einschätzung sicherheitspolitisch relevanter Risiken bestehen. Javier Solanas Entwurf einer EU-Sicherheitsstrategie kann in diesem Zusammenhang als wichtiger Baustein zur Angleichung der Perzeptionen interpretiert werden, indem er die wichtigsten sicherheitspolitischen Bedrohungen (Terrorismus, Proliferation von Massenvernichtungswaffen, regionale Konflikte, gescheiterte Staaten und Organisierte Kriminalität) analysiert und Europas strategische Ziele (Stabilität und gute Regierungsführung, funktionsfähige multilaterale Ordnung, Umgang mit alten und neuen Risiken) definiert.[17]

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

„Die amerikanische RMA wird von europäischen und asiatischen Verbündeten nicht kopiert werden (können); vielmehr gilt es, die amerikanischen Aktivitäten gerade bezüglich NCW als Maßstab zu akzeptieren, jedoch *eigene* Antworten und Herausforderungen in gesellschaftlicher, wirtschaftlicher und militärischer Hinsicht zu finden und eigene Fähigkeiten in den Prozess einzubringen, damit regionalen Erfordernissen Rechnung getragen und die Vernetzung mit den USA im *eigenen* Sinne mitgestaltet wird."[18]

Wie diese europäischen Antworten allerdings aussehen könnten, ist bislang unklar. Die weltweite Ausrichtung und die damit verbundene Forderung nach globaler Machtprojektion, die das US-Streben nach Informationsüberlegenheit und damit auch die konsequente Ausnutzung technologischer Fortschritte im militärischen Bereich erklären, finden in Europa keine entsprechende Antwort. Richtigerweise wird daher die Diskussion über ein europäisches Leitbild der vernetzten Operationsführung dazu führen müssen, dass die während langer Zeit beiseite geschobene Frage nach der Rolle und dem Stellenwert militärischer Mittel als einem Instrument der Konfliktlösung und der Stabilisierung endlich beantwortet wird. Das ist die wesentliche Voraussetzung, um die im folgenden Abschnitt diskutierte Koalitions- und Zusammenarbeitsfähigkeit gewährleisten zu können.

Kleinstaaten, die der Erörterung außen- und sicherheitspolitischer Ambitionen traditionell skeptisch gegenüberstehen, dürfen sich dieser Diskussion nicht entziehen. Wenn im Zeitalter neuer Sicherheitsrisiken die Grenzen zwischen

---

14 Udo Diedrichs and Mathias Jopp, „Flexible Modes of Governance: Making CFSP and ESDP Work", *The International Spectator* 38:3 (July 2003), S. 15–30, hier S. 29. Siehe zur strukturierten Zusammenarbeit im Verteidigungsbereich Art. I-40.6 und Art. III-213 des Entwurfs zum EU-Verfassungsvertrag. Zit. gemäß: Entwurf eines Vertrags über eine Verfassung für Europa, CONV 850/03, Brüssel, 18.7.2003 <http://european-convention.eu.int/docs/Treaty /cv00850.de03.pdf> (Zugriff: 20.1.2004).

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

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

17 *A Secure Europe in a Better World,* 15895/03, Brüssel, 8.12.2003, S. 5–12 <http://register.consilium.eu.int/pdf/en/03/st15/ st15895.en03.pdf> (Zugriff: 20.1.2004).

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

innerer und äußerer Sicherheit verwischen, die informationstechnologischen Veränderungen die Schutzwirkung des Raums aufheben[19] oder zumindest wesentlich einschränken und das Prinzip der Vernetzung den Wert der Unabhängigkeit in Frage stellt, dann entsteht ein zunehmender Druck zur Solidarität mit den Verbündeten. Im Austausch für Sicherheit in der Gemeinschaft müssen konkrete Gegenleistungen erbracht werden, die im besten Fall die vorhandenen sicherheitspolitischen Fähigkeiten Europas ergänzen, nicht duplizieren. Der „Mut zur Lücke" – im übertragenen Wortsinn – fällt Kleinstaaten oft leichter als anderen Ländern; daher sollten sie diese Option nutzen.

## 2.2. Strukturelle Kompatibilität

Die Aspekte der inhaltlichen Kompatibilität kommen auch in den strukturellen Elementen des politischen Systems zum Ausdruck. Dabei sind insbesondere die Wechselwirkungen zwischen der Rolle und den Kompetenzen der politischen Behörden, der Entscheidungsfindung und den rechtlichen Rahmenbedingungen zu berücksichtigen. Alexander Siedschlag hat in einer vergleichenden Länderstudie gezeigt, dass die Regierungen Deutschlands, Frankreichs, Großbritanniens, Italiens und Schwedens bei der Entscheidung über Auslandseinsätze eine deutliche Vorrangstellung einnehmen, wobei in Deutschland und Schweden Parlamentsvorbehalte bestehen. Umfangreiche innenpolitische Abstimmungsbedürfnisse sind vor allem dann erforderlich, wenn es um größere, langfristige militärische Operationen geht und ein internationales Mandat nicht vorliegt.[20] Allerdings hat sich gerade der deutsche Verteidigungsminister Peter Struck anlässlich des fiktiven Einsatzszenarios zur Entsendung der NATO Response Force, das beim informellen Ministertreffen in Colorado Springs (Herbst 2003) durchgeführt wurde, über die Langsamkeit deutscher Entscheidungsprozesse beklagt und Reformen angemahnt.[21]

Der Zusammenhang zwischen den Kompetenzen von Exekutive und Legislative sowie dem Tempo der Entscheidungsfindung ist vor dem Hintergrund des Kernnutzens der Beschleunigung von entscheidender Bedeutung. Auch wenn es richtig ist, dass der Informationsbedarf und der Handlungsbedarf auf der politischen und der militärischen Führungsebene unterschiedlich ausgeprägt sind und die vernetzte Operationsführung damit auf diesen Ebenen unterschiedlich beurteilt werden muss,[22] so besteht doch die Gefahr asymmetrischer Entscheidungsprozesse. Dass diese die Effektivität der militärischen Operationsführung und damit auch die Kohärenz einer internationalen Koalition wesentlich beeinträchtigen können, hat das Beispiel des Kosovo-Krieges eindrücklich vor Augen geführt.[23] Ebenso zeigen Einsatzauswertungen aus der US-Intervention in Afghanistan, dass innerhalb eines 20-minütigen „Sensor to Shooter"-Zyklus gut 18 Minuten für den Führungs- und Entscheidungsprozess benötigt wurden.[24]

Wenn es so ist, dass das durch die vernetzte Operationsführung erhöhte Maß an Flexibilität – das unter anderem aus der Beschleunigung der militärischen Entscheidungen und der Operationsführung resultiert – zusätzliche Optionen eröffnet,[25] dann ist vor dem Hintergrund der jüngsten multinationalen Erfahrungen zu erwarten, dass die politischen Entscheidungsträger unter einem erhöhten Druck stehen, die politischen Ziele des Militäreinsatzes klar zu

---

19 Hierzu weiterführend: James N. Rosenau, *Distant Proximities: Dynamics Beyond Globalization* (Princeton: Princeton University Press, 2003).

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

21 „Struck will Einsätze schneller billigen können", *Süddeutsche Zeitung* 10.10.2003 <http://www.sueddeutsche.de/deutschland/artikel/336/19317/print.html> (Zugriff: 20.1.2004). Die SPD-Fraktion hat am 20.10.2003 einen ersten Entwurf des neuen Parlamentsbeteiligungsgesetzes vorgelegt.

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

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

24 Ralph Thiele, „Network Centric Warfare: Relevanz für deutsche Streitkräfte?", Präsentation für das DGAP-Expertengespräch vom 31. Januar 2003, Folie 17 <http://www.dgap.org/bfz/veranstaltung/Praes_Thiele_030131.ppt> (Zugriff: 20.1.2004).

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

definieren.[26] Dabei ist davon auszugehen, dass die Wahrscheinlichkeit des politischen „Durchgriffs" auf die verschiedenen militärischen Führungsebenen, die gemäß Skeptikern zu übermäßiger Zentralisierung und Kompetenzstreitigkeiten in der Befehlsgebung führen kann,[27] vor allem dann am größten ist, wenn der Einsatz militärischer Mittel innenpolitisch umstritten ist. Sind die politischen Zielsetzungen der militärischen Intervention nicht klar definiert, wird die Politik – nicht zuletzt unter dem Druck der öffentlichen Meinung beziehungsweise mit Blick auf die Wählerunterstützung – laufend nachsteuern. Dabei muss unter anderem auch der Eindruck vermittelt werden, dass die politischen Entscheidungsträger das Zepter in der Hand halten, und dies können sie durch „Mikromanagement" nachhaltig unterstreichen.

Diese Hypothese lässt sich aus Martha Finnemores Untersuchung ableiten, die aufzeigt, dass sich die Gründe zur Rechtfertigung militärischer Intervention in jüngster Zeit wesentlich verändert haben. Ausschlaggebend dafür waren unter anderem der abnehmende normative Wert militärischer Gewalt in der internationalen Politik und die zunehmende Verrechtlichung derselben.[28] Gerade rechtliche Aspekte spielen unter den Gesichtspunkten der vernetzten Operationsführung eine wesentliche Rolle, denn sie können – zum Beispiel über die Ausgestaltung der Rules of Engagement – die Bewegungsfreiheit (Agilität) der militärischen Truppen einschränken oder die Entscheidungsprozesse zur Freigabe von Zielen verlangsamen. Es ist deshalb davon auszugehen, dass die Auseinandersetzung über das künftige Leitbild der Kriegführung – vernetzte Operationsführung ja oder nein und wenn ja nach US-amerikanischem oder europäischem Muster (so es letzteres denn gibt) – wesentlichen Einfluss auf die Debatte über das Gewaltverbot und die Präemption im Rahmen der Weiterentwicklung der UN-Charta ausüben wird.[29]

## 3. Koalitions- und Zusammenarbeitsfähigkeit

Die Fähigkeit zur Zusammenarbeit genießt im militärischen Bereich traditionell eine hohe Beachtung, weil sie eine wesentliche Voraussetzung der Glaubwürdigkeit internationaler Koalitionen darstellt.[30] Im Zeitalter der sicherheitspolitischen Vernetzung müssen diese Fähigkeiten vor dem Hintergrund zweier neuer Herausforderungen, nämlich der Auswirkungen des technologischen Fortschritts und der Erweiterung des relevanten Akteurskreises, analysiert werden.

### 3.1. Technologie

Über die Frage, ob die Integration neuer Technologien in die militärischen Streitkräfte die multinationale Zusammenarbeit erleichtert oder erschwert, herrscht Uneinigkeit. Auf der einen Seite wird argumentiert, dass die vernetzte Operationsführung bestehende Interoperabilitätsprobleme insbesondere zwischen den transatlantischen Partnern noch vergrößern wird, weil die USA konsequent auf dieses neue Leitbild setzen, während sich die Europäer auf kein gemeinsames Konzept einigen können.[31] Aus einer kritischen, eher dem neo-realistischen Weltbild verpflichteten Analyse der internationalen Beziehungen wird darüber hinaus auf die Unverlässlichkeit zwischenstaatlicher Beziehungen verwiesen. Der heutige Freund kann der morgige Feind sein. Informationsaustausch werde daher nur sehr punktuell erfolgen, und insbesondere die USA dürften kaum bereit sein, ihren Verbündeten den vollständigen Zugang zu ihren Netzen zu gewährleisten.[32]

Auf der anderen Seite sehen Befürworter insbesondere in den neuen technologischen Möglichkeiten ein Instrument, um die Kohäsion internationaler Allianzen zu stärken. Erst das gemeinsam erarbeitete Lagebild schafft die Grundlage für gemeinsame Situationsanalysen und hilft, Misstrauen und Unsicherheit bezüglich

---

26 So ähnlich auch: Wesley K. Clark, „Iraq: What Went Wrong", *The New York Review of Books* 50:16 (23.10.2003), S. 52–54, v.a. S. 54.

27 Vego, „Network-Centric Warfare", S. 25; Pierre Forgues, *Command in a Network-Centric War* (Toronto: Canadian Forces College, 2000) <http://198.231.69.12/papers/amsc3/forgues2.doc> (Zugriff: 20.1.2004).

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

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

30 Diese Feststellung gilt in besonderem Maß für die wirkungsorientierte Operationsführung. Siehe: Smith, *Effects Based Operations*, S. 336–346.

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

32 Vego, „Network-Centric Warfare", S. 26; Robert Chekan, *The Future of Warfare: Clueless Coalitions?* (Toronto: Canadian Forces College, 2001) <http://198.231.69.12/papers/amsc4/chekan.doc> (Zugriff: 20.1.2004).

der Informationsweitergabe zwischen den Alliierten abzubauen. Zudem profitieren Koalitionskräfte von der Einbindung in das gemeinsame Netzwerk, weil ihr Optionenspektrum durch gemeinsame Aktionen im Verbund erweitert wird. Und weil ein beachtlicher Anteil der erforderlichen Technologie nicht proprietär, sondern am Markt erhältlich ist (Commercial off the shelf – COTS), werden der Technologietransfer und die Streitkräftetransformation vereinfacht.[33]

Eine Zwischenposition nehmen schließlich die technologiekritischen Experten ein. Aus ihrer Sicht sind die von den RMA-/NCW-Befürwortern vertretenen Positionen kaum haltbar. Daher ist es eher unwahrscheinlich, dass technologische Entwicklungen die internationale Zusammenarbeit behindern oder es den USA sogar erlauben, sich aus ihren Überseestützpunkten zurückzuziehen und sich auf die „Kriegführung auf Distanz" zu verlegen.[34]

### 3.2. Erweiterter Akteurskreis

Neben diesen technologischen Aspekten ist zu beachten, dass die Zahl der relevanten Akteure im Zeitalter der sicherheitspolitischen Vernetzung sprunghaft ansteigt. Die bisherigen Überlegungen zur Zusammenarbeit zwischen Teilstreitkräften (Jointness) beziehungsweise zur internationalen Kooperation in gemeinsamen Verbänden (Combinedness) müssen, wie Abbildung 2 verdeutlicht, ergänzt werden. Zuerst ist der Blick von der militärischen Kooperation auf die Zusammenarbeit aller Sicherheitskräfte zu richten. Dazu zählen neben der Polizei sowie paramilitärischen Einheiten auch die Kräfte des Grenzschutzes sowie die Nachrichtendienste. Im Hinblick auf die Herausforderungen des Heimat- und Bevölkerungsschutzes sind zusätzlich unter anderem die Feuerwehr und die Sanität zu berücksichtigen. Darüber hinaus muss künftig zwingend auch die Schnittstelle zwischen dem öffentlichen Sektor und der Industrie berücksichtigt werden, denn diese spielt bei der Krisenvorsorge und der Krisenbewältigung eine zunehmend wichtige Rolle.[35] Gewisse Sicherheitsthemen wie beispielsweise der Schutz der kritischen Infrastruktur oder die Vorsorge gegenüber bioterroristischen Risiken sind ohne die Mitarbeit der Industrie überhaupt nicht zu bewältigen.

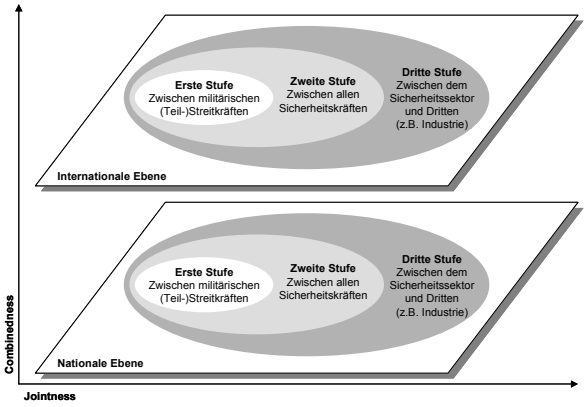


Abbildung 2: Jointness, Combinedness und sicherheitspolitische Vernetzung

Mit dieser erweiterten Betrachtung von Jointness und Combinedness steht der Sicherheitssektor jedoch vor einer „herkulischen Herausforderung". Die bisherigen Bemühungen zur Sicherstellung der Zusammenarbeitsfähigkeit beschränken sich beinahe vollständig auf die erste Stufe (gemäß Abbildung 2), während Standards und – noch wichtiger – Konzepte zur Zusammenarbeit für die zweite und dritte Stufe weitgehend fehlen oder nur sehr punktuell realisiert worden sind. Beide Aspekte werfen eine Reihe von Grundsatzfragen auf, die im Hinblick auf die reibungslose Zusammenarbeit im vernetzten Sicherheitssektor beantwortet werden müssen:

Erstens braucht es konzeptionelle Grundlagen zur Gewährleistung der Kooperation im vernetzten Sicherheitssektor. Bisherige Bemühungen zur konsequenten Jointness zwischen allen Sicherheitskräften müssen deutlich verstärkt werden. Besondere Aufmerksamkeit ist daneben der Kooperation mit der Industrie – von der gemeinsamen Risikoanalyse über die Konzepterarbeitung bis hin zu gemeinsamen Übungen – zu widmen. Dabei geht es um die Klärung individueller beziehungsweise gemeinsamer Verantwortlichkeiten im Hinblick auf die Bewältigung neuer Sicherheitsrisiken.[36] Zudem müssen

---

33 William A. Owens, „The Once and Future Revolution in Military Affairs", *Joint Forces Quarterly* 31 (Summer 2002), S. 55–61, hier S. 60 <http://www.dtic.mil/doctrine/jel/jfq_pubs/1131.pdf> (Zugriff: 20.1.2004); Alberts/Garstka/Stein, *Network Centric Warfare,* S. 226.

34 O'Hanlon, *Technological Change and the Future of Warfare,* S. 44–160.

35 So auch: Manuel W. Wik, *Network-Based Defence for Sweden – Latest Fashion or a Strategic Step Into the Future?* (Stockholm: Defence Materiel Administration, 2002), S. 25 <http://www.kkrva.se/kkrvaht_4_2002_04.pdf> (Zugriff: 20.1.2004).

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

Konzepte für die Weiterführung der unternehmerischen Tätigkeit im sicherheitspolitischen Krisenfall (Business Continuity) entwickelt werden.[37] Diese sind auch um Aspekte des Schutzes der Unternehmen für ihre Mitarbeiter vor spezifischen Risiken zu erweitern.[38] Ferner ist zu untersuchen, inwieweit vorhandene Spezialfähigkeiten der Unternehmen – man denke beispielsweise an Berufsfeuerwehren der chemischen Industrie oder das Fach-Know-how von IT-Experten – in Ressourcenpools mit den staatlichen Sicherheitskräften zusammengeführt werden könnten. Daneben muss die konsequente Berücksichtigung politischer Aspekte im Rahmen der unternehmerischen Chancen- und Risikoanalyse ausgebaut werden.[39] Schließlich muss angesichts des grenzüberschreitenden Charakters heutiger Wirtschaftstätigkeit auch danach gefragt werden, welche dieser Maßnahmen sinnvollerweise auf europäischem Niveau koordiniert werden und welche Rolle dabei die Europäische Kommission sowie andere internationale Behörden spielen sollen.

Zweitens gestaltet sich die Suche nach strategischen Partnern durch die sicherheitspolitische Vernetzung noch komplexer. Im engeren Sinn, das heißt vor allem mit Bezug auf Technologieaspekte, ist die Partnerwahl automatisch auch eine Vorentscheidung im Hinblick auf die Kooperationsfähigkeit in einem gemeinsamen (NCW-)Verbund. Entscheidend ist dabei die Frage, wie offen oder abschottend die technologischen Standards definiert werden. Neben der Option „politisches Kerneuropa" gibt es damit auch jene des „technologischen Kerneuropa", das angesichts bestehender Fähigkeitsprofile nicht notwendigerweise deckungsgleich sein muss. Wie das Beispiel unterschiedlicher Industriestandards zeigt, ist Marktabschottung durch divergierende Standards relativ leicht möglich – politisch wären die Folgen einer solchen Entwicklung jedoch fatal. Im weiteren Sinn, das heißt mit Blick auf die wachsende Zahl von Anspruchsgruppen, mit denen der Sicherheitssektor zusammenarbeiten muss, können strategische Partnerschaften beispielsweise auch mit nichtstaatlichen Akteuren eingegangen werden. Denken wir an die sicherheitspolitische Rolle der biotechnologischen Industrie, so ist die enge Zusammenarbeit mit diesem Industriezweig langfristig erfolgsentscheidend. Ebenso erforderlich ist aber auch der aktive Dialog mit kritischen NGOs wie zum Beispiel dem Sunshine-Project,[40] die in der Lage sind, die internationale Öffentlichkeit zu mobilisieren und durch ihren Widerstand gegen neue Technologien sicherheitspolitisch relevante Langzeitfolgen zu verursachen.

Die Frage der Standards rückt drittens die Beziehung zwischen NATO und EU ins Zentrum der Betrachtung. Innerhalb der NATO spielt die vernetzte Operationsführung bereits eine wichtige Rolle bei der Streitkräftetransformation. Verschiedene Aspekte werden im Rahmen des Multinational Interoperability Council sowie des Joint Transformation/Multinational Joint Concept Development & Experimentation-Prozesses berücksichtigt. Die EU hat dagegen noch keine eigene Position zu diesem Thema.[41] Daraus wird vor allem dann ein Problem, wenn die jeweiligen Prozesse zur Streitkräfteentwicklung nicht aufeinander abgestimmt werden. Insofern ist, um ein Wortspiel zu bemühen, der „gap in minds", der hinter unterschiedlichen Streitkräftetransformationsprogrammen steht,[42] für die Koalitionsfähigkeit ausschlaggebender als die im Hinblick auf die technologiebedingte Entwicklung ausgesprochene Warnung „mind the gap".[43] Deshalb ist es höchste Zeit, dass sich die Mitglieder dieser Organisationen auf ein gemeinsames Verständnis oder Leitbild einigen, um auf dieser Basis gemeinsame Standards und Vorgehensweisen zu definieren.

---

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

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

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

40 Das Sunshine-Project liefert nach eigenen Angaben Forschung und Fakten über biologische Waffen. Die Initianten wollen die weltweite Ächtung biologischer Waffen stärken und den militärischen Missbrauch von Bio- und Gentechnologie aufdecken <www.sunshine-project.de> (Zugriff: 20.1.2004). Siehe hierzu auch: Hans Schuh, „Grippen, Gräber und Gelehrte", *Die Zeit* 16.10.2003, S. 33–34.

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

42 So auch: John P. White and John Deutch, *Security Transformation. Report of the Belfer Center Conference on Military Transformation* (Carlisle: Strategic Studies Institute, U.S. Army War College, 2003), S. 4 <http://www.carlisle.army.mil/ ssi/pubs/2003/sectrans/sectrans.pdf> (Zugriff: 20.1.2004). White und Deutch argumentieren, dass die Konsequenzen der US-Streitkräftetransformation für die Alliierten genauer untersucht werden müssen.

43 Gompert/Kugler/Libicki, *Mind the Gap*.

Diese militärischen Transformationsüberlegungen sind viertens sinngemäß auf die in Abbildung 2 dargestellte zweite und dritte Stufe des vernetzten Sicherheitssektors anzuwenden. Zu diesem Zweck ist es erforderlich, zusammen mit anderen internationalen Organisationen wie zum Beispiel der OSZE, die im Bereich der Polizeikräfte tätig ist, ein „ziviles" Pendant zur militärischen Transformation zu entwickeln. Dieses sollte ebenfalls transatlantisch angelegt sein und müsste das US-amerikanische Department of Homeland Security (DHS) sowie entsprechende europäische Partnerorganisationen berücksichtigen. Die Einbindung der Industrie ist dabei durch die Entsendung eigener Vertreter sowie die Teilnahme von Verbandsmitgliedern, die Koordinationsfunktionen übernehmen können, sicherzustellen.

## 4. Management des vernetzten Sicherheitssektors

Die Diskussion von Managementaspekten im Zusammenhang mit der Erörterung politisch-strategischer Implikationen der sicherheitspolitischen Vernetzung mag auf den ersten Blick überraschen. Bei genauerem Hinsehen wird jedoch schnell dreierlei deutlich: Erstens sind die bisherigen Bemühungen zur Reform des öffentlichen Sektors (New Public Management) noch von einer starken Binnensicht geprägt und vernachlässigen den Gedanken der systematischen Vernetzung der Verwaltung mit anderen Akteuren. Zweitens zieht die erfolgreiche Bewältigung der neuen technologischen Herausforderungen eine weitgehende Überprüfung und Angleichung der Beschaffungsverfahren und -grundsätze nach sich, wobei immer öfter Ansätze angewendet werden, die sich in der Privatwirtschaft bewährt haben.[44] Drittens erfordern die neuen sicherheitspolitischen Herausforderungen, darauf hat das Eingangszitat von Ashton B. Carter hingewiesen, die grundlegende Reorganisation der bestehenden Sicherheitsinstitutionen. Dabei gilt für den öffentlichen Sektor genauso wie für die moderne Betriebswirtschaftslehre:

„Konsequente Prozessorientierung führt zur Virtualisierung und Vernetzung von Unternehmen, denn Prozesse sind nicht an Unternehmensgrenzen gebunden, sie liegen vielmehr quer zur klassischen Taylor'schen Arbeitsteilung."[45]

Die Managementreform des vernetzten Sicherheitssektors ist demzufolge die entscheidende Voraussetzung dafür, dass die politischen Entscheidungsträger ihre Führungsfunktionen überhaupt wahrnehmen können. Einige der damit verbundenen Herausforderungen sollen in der Folge diskutiert werden. Zu diesem Zweck wird das in Abbildung 3 dargestellte Führungsmodell[46] als Orientierungshilfe eingesetzt. Dieses basiert auf der Logik der Prozessorientierung und unterscheidet zwischen vier zentralen Führungsaufgaben (in der Abbildung durch vier Fragen gekennzeichnet), die vor dem Hintergrund der definierten Vorgaben beziehungsweise der gelebten Wirklichkeit interpretiert werden müssen, um die mit der Leistungserstellung erzielte Wirkung beurteilen zu können.

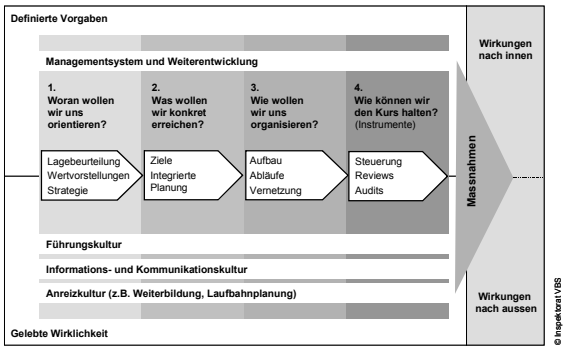


Abbildung 3: Allgemeines Führungsmodell

### 4.1. Managementsystem

Ein Managementsystem beschreibt die Gesamtheit der aufeinander abgestimmten Prozesse, Strukturen und Instrumente eines Unternehmens.[47] Im Zuge der wirkungsorientierten Verwaltungsführung sind auch öffentliche Betriebe und Ministerien dazu übergegangen, solche Managementsysteme aufzubauen. Im Zeitalter der sicherheitspolitischen Vernetzung besteht in diesem Bereich eine doppelte Herausforderung: Einerseits müssen die Managementsysteme der Organisationen des Sicherheits-

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

45 Fleisch, *Das Netzwerkunternehmen*, S. 11.

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

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

sektors systematisch aufeinander abgestimmt werden. Richtig verstanden müssen für den gesamten Sicherheitssektor übergreifende Prozesse definiert werden, die in einem entsprechenden Prozessmodell zusammengefasst werden. Eine solche Aufgabe muss logischerweise auch ressortübergreifend koordiniert werden. In vielen Fällen werden diese Prozessmodelle zudem in den Wirtschaftssektor hineingreifen (z.B. im Zusammenhang mit der Krisenvorsorge oder dem Schutz kritischer Infrastruktur), umgekehrt müssen unternehmerische Leistungen in die Prozessmodelle des Sicherheitssektors integriert werden (z.B. im Hinblick auf die immer enger werdende Kooperation mit der Rüstungsindustrie). Deshalb sollte entweder ein managementorientiertes Vernetzungsgremium für den Sicherheitssektor geschaffen werden, oder die Kompetenzen bereits bestehender ressortübergreifender Einrichtungen sollten durch diesen Aspekt ergänzt werden. Denkbar ist daneben auch, wie das Beispiel des US-amerikanischen Ministeriums für Heimatschutz zeigt, die Ernennung von Managementverantwortlichen zur Bündelung einzelner Funktionen.[48]

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

## 4.2. Orientierung/Positionierung

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

Ferner ist zu berücksichtigen, dass der Trend zur Vernetzung die Zahl der für den Sicherheitssektor relevanten Anspruchsgruppen erhöhen wird. Reformkommissionen müssen beispielsweise gesellschaftlich breit abgestützt werden, und beim Einsatz in internationalen Missionen spielen die zivil-militärischen Beziehungen eine immer wichtigere Rolle. Es empfiehlt sich daher, auch im Sicherheitssektor den Übergang zum systematischen Management der Beziehungen zu Anspruchsgruppen (Stakeholder Management) einzuleiten. Im Vordergrund stehen dabei die Identifizierung der wichtigsten Anspruchsgruppen, ihrer Absichten und Motive, die Auseinandersetzung mit ihrem Kooperationsverhalten, die Festlegung anspruchsgruppenspezifischer Zielsetzungen und die Definition von Mitteln und Verfahren, um die Zusammenarbeit mit den Anspruchsgruppen erfolgreich zu gestalten.[49]

## 4.3. Planung

Der Planungsbereich steht im Zeitalter der Vernetzung vor der großen Herausforderung, dass die ressortspezifischen Rivalitäten zwingend abgebaut werden müssen, soll die integrierte Planung Realität werden. Damit sind zwei

[48] <http://www.dhs.gov/dhspublic/display?theme=54> (Zugriff: 20.1.2004).

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

zentrale Aspekte angesprochen: Zuerst muss das Verhältnis zwischen ressortübergreifenden Gremien und den ressorteigenen Planungsstäben geklärt werden. Die vollständige Zentralisierung der Planungsaktivitäten auf der obersten Stufe ist ebenso wenig sinnvoll wie die vollständige Delegation an die operativ tätigen Einheiten. Hier muss ein neues Gleichgewicht gefunden werden. Als Leitidee ist dabei anzuregen, dass die langfristigen und prospektiven Planungsaufgaben am ehesten auf der ressortübergreifenden Koordinationsstufe organisiert werden sollten, während die umsetzungsorientierten Planungsaufgaben[50] bei den Fachressorts besser angesiedelt wären. Eine vergleichbare Logik wird sich auch im Verhältnis zwischen nationaler und internationaler Planung aufdrängen. Da die Vernetzung nicht nur ressort-, sondern auch ebenenübergreifend sicherzustellen ist (siehe Abbildung 2), müssen die nationalen Planungsprozesse systematisch auf ihre Kompatibilität mit internationalen Planungsabläufen überprüft werden.[51] Dabei geht es neben der zeitlichen Synchronisation vermehrt auch um die inhaltliche Harmonisierung. International dürfte dies unter anderem bedeuten, dass Überlegungen zu Fähigkeitszielen und Konvergenzkriterien noch wichtiger werden, weil sie das Bindeglied zwischen internationaler und nationaler Transformation darstellen. Demzufolge sind die entsprechenden Bemühungen nicht nur mit Nachdruck voranzutreiben, sondern auch inhaltlich vom Verteidigungsbereich auf alle Belange des vernetzten Sicherheitssektors zu erweitern.

### 4.4. Organisation

Die größte organisatorische Herausforderung besteht in der ressortübergreifenden Prozessorientierung beziehungsweise Vernetzung. Dabei geht es darum, die Dominanz der Linienorganisation und der damit verbundenen Hierarchien zugunsten der Vernetzungsorganisation abzubauen und die Prozesse entsprechend neu zu gestalten. Bleibt es dabei, dass insbesondere die Zuteilung der Finanz- und Personalmittel entlang der bisherigen Linienorganisation – und damit eben auch der klassischen Ressortzuteilung – gesteuert wird, ist eine solche Reorganisation nicht zu schaffen. Die Neuausrichtung muss daher auch in diesen Bereichen bewusst über sicherheitspolitische Vernetzungsgremien erfolgen, am besten über eine sicherheitspolitische Koordinationsstelle im Bundeskanzleramt.

Diese Veränderungen auf der Seite der Verwaltung werden auch das Parlament nicht unberührt lassen.[52] Wenn die sicherheitsrelevanten Ministerien über die Vernetzung näher zusammenrücken und daraus möglicherweise sogar der Aufbau integrierter Sicherheitskräfte resultiert, dann müssen auch die parlamentarischen Überwachungsorgane neu strukturiert werden.[53] Die bisherige Ressortaufteilung dürfte auch in diesem Bereich zugunsten eines umfassenden „Außen- und Sicherheitspolitischen Ausschusses des Parlaments“ aufgegeben werden, dessen Zuständigkeit von der Außen- über die Sicherheits- bis zur Verteidigungspolitik reicht und auch die Schnittstelle zu den Nachrichtendiensten, zur inneren Sicherheit sowie Wissenschaft und Forschung berücksichtigt. Gleichzeitig muss die managementorientierte Beurteilungsfähigkeit solcher Ausschüsse nachhaltig gestärkt werden.

### 4.5. Kurs halten

Die Steuerung und die Weiterentwicklung des vernetzten Sicherheitssektors sind für die Bewältigung der komplexen neuen Sicherheitsherausforderung unerlässlich. David S. Alberts ist zuzustimmen, wenn er als Grundsatz festhält, dass „the entire notion of doctrine needs to be changed from one of publishing ‘the way’ it should be done to a dynamic process of learning and sharing best practice“.[54] Der Wandel von der Anordnungs- zur Lernkultur stellt jedoch nicht nur für die militärischen Streitkräfte, sondern auch für die Ministerien einen fundamentalen

---

50 Planung und Führung im Krisenfall sind davon ausgenommen.

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

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

53 So wurde in den USA ein neues Select Committee for Homeland Security geschaffen, um den Aufbau und die Arbeit des entsprechenden Ministeriums zu begleiten. Siehe: <http://hcw.house.gov> (Zugriff: 20.1.2004).

54 David S. Alberts, *Information Age Transformation. Getting to a 21st Century Military* (Washington, D.C.: CCRP, 2002), S. 121.

Kulturwandel dar. Die Fähigkeit des Lernens setzt neben dem Vorhandensein des Willens auch voraus, dass Informationen und Systeme zur Verfügung gestellt werden, die das Lernen ermöglichen.

Damit ist zum einen der Ausbau des strategischen Controlling (und Reporting) angesprochen. Dieses muss von den zentralen Organisationseinheiten der Ministerien aufgebaut und von den nachfolgenden Organisationsebenen entsprechend umgesetzt werden. Besonders wichtig ist in diesem Zusammenhang erneut der ressortübergreifende Blick, der durch einige zentrale und aggregierte Führungskenngrößen sichergestellt werden muss. Zu diesem Zweck sind neue Kenngrößen erforderlich, weil die neuen Anforderungen über die alten Indikatoren meist unzureichend erfasst werden.

Zum anderen stellt die Forderung nach Vernetzung neue Anforderungen an jene Instrumente, die eingesetzt werden, um die Mittelzuteilung vorzunehmen. Das verhältnismäßig spröde Instrument der Kosten- und Leistungsrechnung spielt in diesem Zusammenhang eine besondere Rolle. Nur wenn es gelingt, die Kostenerfassung innerhalb des Sicherheitssektors zu vereinheitlichen und Transparenz über die Kosten der erbrachten Leistungen herzustellen, sind der Leistungsaustausch (z.B. der Einsatz militärischer Streitkräfte zugunsten des Innenministeriums) sowie das Zusammenlegen von Leistungen und Fähigkeiten in Ressourcenpools (z.B. der Aufbau eines Polizeipools bestehend aus Bundes- und Länderkräften) zu realisieren. Ohne diese Transparenz besteht die Gefahr, dass sich die einzelnen Ministerien beziehungsweise Sicherheitskräfte aus Angst vor einer möglichen Benachteiligung bei der Mittelvergabe der Zusammenarbeit verweigern oder diese nicht mit dem geforderten Nachdruck vorantreiben. Ebenso sind politische Grundlagenentscheidungen – etwa zur Frage der Ressortneuzuteilung im Zuge der Reorganisation – ohne die geforderte Transparenz nicht möglich.[55]

Die Forderung nach neuen Kenngrößen führt uns zum zweiten wichtigen Bereich, nämlich der Fähigkeit zur Weiterentwicklung, die systematisch in die Managementsysteme des vernetzten Sicherheitssektors eingebaut werden muss. Holger Mey und Michael Krüger haben völlig Recht, wenn sie im Hinblick auf die Streitkräfteentwicklung den Aufbau eines Transformationsaudits zur Identifizierung der Stärken und Schwächen vorschlagen, das in enger Zusammenarbeit zwischen Industrie und Amtsseite entwickelt werden soll.[56] Logischerweise muss diese Idee zur Forderung nach einem Bewertungsansatz für die Weiterentwicklung des gesamten Sicherheitssektors (Security Sector Assessment) erweitert werden. Ein solches Assessment sollte – in Analogie zum Planning and Review Process (PARP) der NATO sowie anderer international verfügbarer Instrumente – aus einem klar definierten Assessmentprozess bestehen und einen Fragekatalog zur Selbst- und Fremdbewertung beinhalten. Kernbereiche der Untersuchung, durch die auch die Forderung nach neuen Kenngrößen befriedigt werden kann, sollten sein:[57]

- vernetztes Management der Sicherheitspolitik und des Sicherheitssektors,
- individuelle und gemeinsame Fähigkeitsorientierung sowie
- Zusammenarbeitsfähigkeit im und über den Sicherheitssektor hinaus.

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

- technische Aspekte der Simulation beziehungsweise des Tests von IT-Netzwerken im Vorfeld ihres Einsatzes,[58]

---

55 Die damit verbundenen Probleme zeigten sich z.B. in der Schweiz bei der Zuweisung von Sicherheitsaufgaben an das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport bzw. das Eidgenössische Justiz- und Polizeidepartement sowie bei der Kompetenzausscheidung zwischen Bund und Kantonen. Siehe: USIS, *Detailbericht III* (Bern, 24. September 2002), S. 48–56 <http://www.usis.ch/deutsch/berichte/pdf_usis_3/USIS_III_Text.pdf> (Zugriff: 20.1.2004).

56 Mey/Krüger, *Vernetzt zum Erfolg?*, S. 12.

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

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

- arbeitspsychologische Aspekte wie die Frage nach den Zusammenhängen zwischen der Arbeit in Netzwerken und den Rückwirkungen auf die Psyche, die Motivation und das Verhalten der Mitarbeiter,[59]
- organisationstheoretische Fragen nach der optimalen „Konstruktion" von Netzwerken sowie
- soziologische Aspekte wie die Frage, aus welchen Gründen sich Menschen überhaupt in Netzwerken zusammenschließen und welche „Haltbarkeit" diese aufweisen (Social Network Analysis/Engineering).[60]

### 4.6. Kulturelle Dimension

Die Transformation von Organisationen hängt bekanntermaßen erst in zweiter Linie von der Einführung neuer Technologie oder der Neugestaltung von Prozessen und Strukturen ab. Maßgeblich ist in erster Linie der Veränderungswille der Menschen.[61] Für die erfolgreiche Umsetzung der vernetzten Operationsführung oder der vernetzten Sicherheitspolitik ist dieser Veränderungswille eine zentrale Voraussetzung.[62] Schwierig gestaltet sich dieser kulturelle Wandel vor allem deshalb, weil die meisten Entscheidungsträger in Linienorganisationen sozialisiert worden sind.

„It is difficult to create a culture of innovation when a procurement system can take 20 years to field a product. It is difficult to create a culture of innovation when communications are hampered by incompatible, slow, unsecured information and computer systems. It is difficult to create a culture of innovation under arcane rules, regulations, and personnel systems."[63]

Die Vernetzung bedingt im Unterschied zum Bestehenden eine neue Kultur, die auf Vertrauen, Delegation, Eigeninitiative, Selbstständigkeit und Eigenverantwortung basiert.[64] Wichtig wird es daher in einem ersten Schritt sein, dass vor allem die Führungskräfte und die Entscheidungsträger ihre Bereitschaft zur vernetzten Sicherheitspolitik mit Taten unterstreichen. Dazu zählen beispielsweise die Übernahme der Aufsicht in maßgeblichen Reformprojekten, die den Wandel zur Vernetzung fördern, die gemeinsame Strategiedefinition sowie die Teilnahme an Aus- und Weiterbildungsveranstaltungen,[65] Übungen und Simulationen, die die Sensibilität für die Notwendigkeit ressortübergreifender Zusammenarbeit erhöhen. Besonders wichtig ist in diesem Zusammenhang der Umgang mit der bereits erwähnten Schnittstelle zwischen politischer und militärischer Führung, um asymmetrische Entscheidungsprozesse zu verhindern.

Der zweite Schritt beinhaltet den Wandel im Informations- und Kommunikationsverhalten. Befürworter der vernetzten Operationsführung weisen korrekterweise darauf hin, dass die angebotsorientierte Informationsversorgung (Information Push) in einem komplexen Netzwerk leicht zur Informationsüberlastung seiner Mitglieder führen kann. Deshalb favorisieren sie die nachfrageorientierte Informationsbeschaffung (Information Pull), bei der sich jeder entsprechend seinen Bedürfnissen aus dem Netzwerk „bedient".[66] Das setzt jedoch voraus, dass die benötigten Informationen unaufgefordert zur Verfügung gestellt werden. In einem Zeitalter, in dem viele Wissen noch immer mit Macht verbinden (Herrschaftswissen), stößt diese Forderung allerdings an eine natürliche Barriere. So kämpfen vernetzte Operationsführung und vernetzte Sicherheitspolitik mit einem Problem, das allen Verantwortlichen des Wissensmanagements wohl vertraut ist: Aktives Informations- und Kommunikationsverhalten lässt sich nicht verordnen, sondern muss sich mit der Zeit entwickeln.

Dazu können, und das ist das dritte Element, Anreize und Maßnahmen zur Befähigung der Mitarbeiter unterstützend eingesetzt werden. So muss beispielsweise die Aus- und Weiterbildung der Mitarbeiter der Sicherheitssektoren konsequent neu auf die Anforderungen der Vernetzung ausgerichtet werden. Gemeinsame Führungslehr-

---

59 Alberts, *Information Age Transformation,* S. 131–143.

60 Art Kleiner, „Karen Stephenson's Quantum Theory of Trust", in Rothenberg, *Enterprise Resilience,* S. 38–53.

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

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

63 Mac Thornberry, „Fostering a culture of innovation", *Proceedings* 129:4 (April 2003), S. 44–50, hier S. 2 (zitiert nach Internetversion).

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

65 <http://www.stratfuelg.gv.at/seite1.htm> (Zugriff: 20.1.2004).

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

gänge sollten ebenso selbstverständlich werden wie die Personalrotation zwischen den Ministerien beziehungsweise den Sicherheitskräften. Im Hinblick auf die Laufbahnplanung sollten bewusst ressortübergreifende Karrierewege geplant und angeboten werden. Ebenso sollte das Engagement in anderen Sicherheitsressorts genauso als Qualifikation für die berufliche Beförderung gelten wie beispielsweise die Teilnahme an Auslandseinsätzen.[67]

## 5. Vernetzte Fähigkeiten

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

Die Aufarbeitung der Ereignisse des 11. September 2001 hat in den USA zu teilweise ernüchternden Einsichten über den Ausrüstungszustand und die Fähigkeitsprofile gewisser Sicherheitskräfte geführt. Über 100 Feuerwehrleute sollen beim Brand des World Trade Center allein deshalb gestorben sein, weil die Kommunikations- und Informationssysteme der Einsatz- und Rettungskräfte unzureichend aufeinander abgestimmt waren.[68] Auch stellte eine Task Force des US Council on Foreign Relations fest, dass die US-amerikanischen Polizeikräfte nicht über das erforderliche Gerät verfügen, um einen mit Massenvernichtungswaffen angegriffenen Ort abzusichern. Den meisten Städten fehlen die Geräte um herauszufinden, ob und in welchem Ausmaß die Einsatz- und Rettungskräfte an einem Schadensort gefährlichen Stoffen ausgesetzt sind.[69]

In Europa präsentiert sich das Bild nicht besser. Im Anschluss an die Flutwasserkatastrophe in Deutschland im Jahr 2002 stellte der Kirchbach-Report gravierende Mängel bei den Kommunikationssystemen der Behörden und Organisationen mit Rettungs- und Sicherheitsaufgaben fest und wies gleichzeitig auf konzeptionelle Schwächen in deren Zusammenarbeit hin.[70] Im Zuge der Überprüfung des Systems der inneren Sicherheit in der Schweiz (USIS) wurden Defizite bei der unterschiedlich intensiven und sehr heterogen ausgeprägten Zusammenarbeit zwischen den Polizeikonkordaten und bei der Interoperabilität der von den kantonalen Polizeikorps verwendeten Kommunikationssysteme festgestellt.[71]

Erste Anzeichen der Verbesserung sind in Sicht. So wird zum Beispiel in Frankreich das Kommunikationssystem der Polizei auf die Feuerwehr und andere Akteure ausgedehnt, und es werden unter Einschluss der Marine und der Küstenwache einheitliche Lagebilder erstellt.[72] Ähnliche Bestrebungen gibt es auch in der Schweiz mit dem Aufbau des einheitlichen Kommunikationsnetzes POLYCOM.[73] Aus diesen Beispielen und den genannten Defizitbereichen lässt sich eine Liste jener vernetzten Fähigkeiten ableiten, die künftig besonderer Beachtung bedürfen. Dazu zählen unter anderem

- Führung (Command, Control, Communication, Computers – C4) als Kernvoraussetzung erfolgreicher Operationen,
- Nachrichtengewinnung, Überwachung und Aufklärung (Intelligence, Surveillance, Reconnaissance – ISR), um ein gemeinsames Lagebild herzustellen,
- luft-, land- und seegestützte Verlegefähigkeit zur Verbesserung der Mobilität der Sicherheitskräfte,
- Überlebensfähigkeit und Schutz der Sicherheitskräfte zum Beispiel durch ABC-Abwehr, Suche und Rettung (Search and Rescue – SAR) oder den Einsatz non-letaler Wirkmittel sowie

---

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

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

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

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

71 USIS, *Analyse des Ist-Zustandes mit Stärken-/Schwächenprofil* (Bern: USIS, 2001), S. 15, 17 <http://www.usis.ch/deutsch/berichte/pdf_usis1/Medienrohstoff_d.pdf> (Zugriff: 20.1. 2004).

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

73 USIS, *Teil II. Grobe Soll-Varianten, Sofortmassnahmen* (Bern: USIS, 2001). S. 20 <http://www.usis.ch/deutsch/berichte/pdf_usis2_voll/deutsch.pdf> (Zugriff: 20.1.2004).

- Schutz der informationskritischen Infrastruktur zur Gewährleistung der Führung im militärischen, im zivil-militärischen und im zivilen Umfeld (inkl. Fähigkeiten zur elektronischen Kriegführung und zu Informationsoperationen).

Im Hinblick auf die Definition der vernetzten Fähigkeiten, die als Ergänzung der jeweils spezifischen Fähigkeiten einzelner Sicherheitskräfte zu interpretieren sind, ist festzulegen, wer diese identifiziert und durch wen beziehungsweise in welcher Form diese bereitgestellt und weiterentwickelt werden. Den bisherigen Überlegungen folgend erscheint es sinnvoll, die Identifizierung und die Weiterentwicklung über die im vorangehenden Kapitel angeregten Managementsysteme beziehungsweise das umfassende Assessment des gesamten Sicherheitssektors abzuwickeln. Dabei sollte die Bundesregierung die Schwerpunkte festlegen, und ein sicherheitspolitisches Koordinationsgremium im Bundeskanzleramt sollte die strategische Steuerung übernehmen. Die jeweiligen Sicherheitskräfte zeichnen für die Bewirtschaftung und das operative Management der Fähigkeiten verantwortlich.

Angesichts knapper öffentlicher Budgets kann es nicht darum gehen, die Fähigkeitsdefizite der jeweiligen Sicherheitskräfte individuell zu beheben. Vielmehr müssen Ansätze wie die Rollenspezialisierung oder die Zusammenlegung von Ressourcen auf alle Sicherheitskräfte angewendet werden.[74] Das hätte beispielsweise zur Folge, dass ein ABC-Kompetenzpool mit Hilfe entsprechender militärischer ABC-Schutz- und Abwehrfähigkeiten sowie der Fachexpertise der chemischen und Biotech-Industrie, von privaten und öffentlichen wissenschaftlichen Instituten sowie Krankenhäusern eingerichtet werden könnte.[75] Dieser umfassende Ansatz der Public Private Partnership (PPP) gelingt allerdings nur dann, wenn man die Managementkompetenzen der Sicherheitskräfte fördert und die Sensibilität für den erforderlichen Kulturwandel erhöht.

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

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

## 6. Rolle der Rüstungsindustrie

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

„Since it is ultimately the contractors that will provide the technological insights to make defense transformation a reality, these challenges have the potential to slow the rate of change. And since technology development and acquisition cycles are lengthy, we may be a long way from achieving the transformational vision."[76]

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

### 6.1. Kundenanforderungen

Der Übergang zur Fähigkeits- und Wirkungsorientierung und die verstärkte Betonung der Netzwerkfähigkeit werden auf der Industrieseite zu einer Verlagerung von der Produkt- oder Plattformorientierung hin zur Systemorientierung führen.[77] Der Grundsatz der Jointness muss von der Industrie genauso berücksichtigt werden wie von den Sicherheitskräften, weshalb beide der Fähigkeit zur Systemintegration – bezogen auf die Management- und die IT-Systeme – mehr Beachtung schenken müssen. Die Industrie wird dadurch dreierlei analysieren müssen: Erstens muss sie ihr Leistungsportfolio im Bereich der vernetzten Fähigkeiten prüfen beziehungsweise verstärkt darauf ausrichten, weil dort der größte Mehrwert für den Kunden geschaffen werden kann. Zweitens wird sie bestehende Partnerschafts- und Allianznetze auf den Prüfstand stellen. Genügte bislang die Kooperation mit industriespezifischen Partnern, so wird künftig die Integration industriefremder Partner aus den Bereichen Bio-, Gen- und Nanotechnologie,

[76] Dougles S. Harned and Jerrold T. Lundquist, „What transformation means for the defense industry", *The McKinsey Quarterly* 3 (2003), S. 50–63, hier S. 61.

[77] Mey/Krüger, *Vernetzt zum Erfolg?*, S. 57–65.

Lebenswissenschaften (Life Sciences), Medizin, Informations- und Kommunikationstechnologie, Multimedia und Bildung an Bedeutung gewinnen. Drittens muss sich die Industrie auf einen breiteren Abnehmerkreis einstellen, der sich aus der Vernetzung des Sicherheitssektors ergibt. Das stellt auf der einen Seite eine Chance dar, weil sich die Absatzmöglichkeiten verbessern. Auf der anderen Seite ist jedoch zu erwarten, dass der Sicherheitssektor seine Einkaufsmacht künftig vermehrt durch ein konzertiertes Vorgehen stärken wird. Und solange die europäische Integration in diesem spezifischen Industriebereich noch auf sich warten lässt, bedeutet dies eine Erhöhung der Komplexität bei der länder- und sektorspezifischen Marktbearbeitung. Zu guter Letzt ist auf den unternehmensspezifischen Reorganisationsbedarf hinzuweisen, der sich aus den genannten Entwicklungen ergibt.[78] Je besser und schneller es den Unternehmen gelingt, ihre eigenen Kompetenzen und Fähigkeiten im Sinne der geforderten Systemintegration zu bündeln, desto eher wächst auf der Kundenseite das Vertrauen in die unternehmerische Problemlösungskompetenz.

## 6.2. Zusammenarbeit

Es liegt auf der Hand, dass sich der bereits aus anderen Gründen enger werdende Schulterschluss zwischen Sicherheitssektor und wehrtechnischer Industrie im Zeitalter der Vernetzung noch verstärken wird. Die Industrie als Trägerin der wissenschaftlich-technischen Kompetenz ist besonders in zwei Bereichen gefordert: Einerseits geht es um die systematische Unterstützung des Sicherheitssektors in Bezug auf das wissenschaftlich-technische Trendmonitoring. Dies ist eine Dienstleistung, die für die Fähigkeitsplanung des Sicherheitssektors immer wichtiger wird und sinnvollerweise von diesem am Markt eingekauft werden sollte.[79] Eng damit verknüpft ist andererseits die Unterstützung des Sicherheitssektors beim Management unterschiedlicher Lebenszyklen der eingesetzten Technologien beziehungsweise der daraus resultierenden Produkte. Diese Aufgabe resultiert aus dem verstärkten Einsatz ziviler Technologie (COTS) in sicherheitsrelevanten Anwendungen. Zivile Technologien weisen aufgrund anderer Marktbedürfnisse meist kürzere Lebenszyklen auf.[80] Das wirkt sich vor allem im militärischen Bereich auf die Unterhalts- und Kampfwertsteigerungsprogramme aus, deren Konzeption und Bewirtschaftung dadurch komplexer werden.

Der Sicherheitssektor muss seinerseits die adäquate Beurteilungskompetenz sicherstellen, um die Industrievorschläge prüfen zu können. Gleichzeitig trägt er die wesentliche Verantwortung dafür, dass PPPs nicht nur auf dem technischen, sondern vor allem auf dem strategischen Niveau eingerichtet werden. Dabei gewinnt die umfassende Betrachtung von Krisenvorsorge, Krisenmanagement und Krisennachsorge gerade auch im Hinblick auf den Heimatschutz wesentlich an Bedeutung. Darüber hinaus muss der Sicherheitssektor gewisse Bedenken der Industrie sehr ernst nehmen. Das gilt beispielsweise für die Feststellung, dass Produktentwicklungen im NCW-Bereich zeit- und kostenintensiv sind. Gleichzeitig besteht ein hohes Risiko hinsichtlich der Fortführung von Projekten aus dem Entwicklungs- ins Produktionsstadium.[81] In Großbritannien, das in Europa eine führende Rolle bei verteidigungsorientierten PPPs einnimmt, werden die langen und teuren Bewerbungsprozesse im Verteidigungssektor von der Industrie zunehmend kritisch kommentiert.[82] In beiden Fällen fehlen bislang adäquate Modelle zur Kompensation der damit verbundenen Risiken. Da es sich hierbei um ein Problem handelt, mit dem zunehmend auch die übrigen Sicherheitskräfte sowie die anderen europäischen Länder konfrontiert werden, drängt sich ein europäischer Lösungsansatz beispielsweise unter Einbezug des neu zu schaffenden Europäischen Amts für Rüstung, Forschung und militärische Fähigkeiten auf.

## 6.3. Erweiterte Industriebasis

Unter den Vorzeichen der sicherheitspolitischen Vernetzung erweitert sich die sicherheitsrelevante Industriebasis in Richtung der bereits angedeuteten stärkeren Integration bislang als rein „zivil" charakterisierter Industriezweige. Der Sicherheitssektor und die Wirtschaft müssen erkennen, dass sich dadurch die Definition der als

78 Harned/Lundquist, „What transformation means for the defense industry", S. 60.

79 Dombrowski/Gholz/Ross, *Military Transformation and the Defense Industry after Next*, S. 27.

80 Mey/Krüger, *Vernetzt zum Erfolg?*, S. 57f.; Jochen Dietrich, „Führungsfähigkeit", in Karl von Wogau (Hrsg.), *Auf dem Weg zur Europäischen Verteidigung. Gemeinsam sind wir sicher* (Freiburg: Herder, 2003), S. 336–347, hier S. 341–343.

81 Harned/Lundquist, „What transformation means for the defense industry", S. 59.

82 David Mulholland, „Concerns rise over the value of private finance", *Jane's Defence Weekly* 23 October 2002, S. 16.

„strategisch bedeutend" eingestuften Industrien und Produkte grundlegend verändert. Die staatliche Förderung neuer Bereiche wie Bio- und Gentechnologie, Nanotechnologie oder Lebenswissenschaften ist vor diesem Hintergrund nicht nur als Beitrag zur Stärkung der nationalen Standortattraktivität, sondern auch als Unterstützung der sicherheitspolitischen Fähigkeitsprofile zu interpretieren. Daraus leitet sich die Forderung ab, dass die bislang künstliche Trennung zwischen militärischer und ziviler Forschung durch integrierte nationale und internationale Konzepte konsequent überwunden werden muss.[83] Gleichzeitig ist in den erwähnten Industrien die Sensibilisierung für ihre jeweilige sicherheitspolitische Rolle und Verantwortung zu stärken (z.B. durch gemeinsame Übungen und Lehrgänge).

### 6.4. Europäisches Amt für Rüstung, Forschung und militärische Fähigkeiten

Im Hinblick auf die Steuerung der Beschaffungsaktivitäten des vernetzten Sicherheitssektors nimmt das im Aufbau befindliche europäische Amt für Rüstung, Forschung und militärische Fähigkeiten eine Schlüsselstellung ein.[84] Auch in diesem Bereich zwingt das Gesagte zu einigen Grundsatzüberlegungen:

Erstens sollte das Amt mit Blick auf die Umsetzung des Leitbilds der vernetzten Operationsführung die zentrale Integrationsfunktion übernehmen. Gegenwärtig verfolgen Großbritannien, Frankreich, Deutschland, die Niederlande, Spanien und Schweden eigene Modernisierungsprojekte im Bereich „Soldat der Zukunft".[85] Wenn die Vernetzungsbefürworter mit ihren Thesen von der Kompetenzdelegation und der Selbstsynchronisation Recht haben, dann erscheint es mehr als sinnvoll, dass diese Programme auf der „untersten Vernetzungsstufe" durch Harmonisierung beziehungsweise Integration auf optimale Zusammenarbeitsfähigkeit ausgerichtet werden.

Zweitens sollte überlegt werden, ob und in welcher Form das Mandat des Amtes auf den gesamten Sicherheitssektor ausgedehnt werden kann, um knappe Mittel effizienter einzusetzen und technische Inkompatibilitäten durch gemeinsame Beschaffungsvorhaben zu verhindern.

Drittens sollten die Einflussmöglichkeiten der Rüstungsagentur – in Zusammenarbeit mit anderen Organen wie zum Beispiel dem EU-Militärstab – im Hinblick auf die Modernisierung und die Transformation des Sicherheitssektors ausgebaut werden. Es ist ein zentrales Problem, wenn nationale Verteidigungsbudgets noch keine oder keine adäquaten Mittel für Transformations- und Modernisierungsaufgaben vorsehen.[86] Deshalb ist es sinnvoll, auf der europäischen Ebene Kompetenzen zu schaffen und Mittel bereitzustellen, damit solche Aktivitäten künftig auf der Basis gemeinsamer Konzepte systematisch lanciert werden können.

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

---

83 *Towards an EU Defence Equipment Policy,* COM(2003) 113 final, Brüssel, 11. März 2003, S. 12, 17–18 <http://europa.eu.int/eur-lex/en/com/cnc/2003/com2003_0113en01.pdf>; *Life sciences and biotechnology. A strategy for Europe,* COM(2002) 27, Brüssel <http://europa.eu.int/comm/biotechnology/pdf/com2002-27_en.pdf>; *Life sciences and biotechnology – a strategy for Europe. Progress report and future orientations,* COM(2003) 96 final, Brüssel, 5. März 2003 <http://europa.eu.int/comm/biotechnology/pdf/com2003-96_en.pdf> (Zugriff: 20.1.2004).

84 2541. Tagung des Rates für allgemeine Angelegenheiten und Außenbeziehungen, 14500/03 (Presse 321) Brüssel, 17. November 2003, S. 11–17 <http://ue.eu.int/pressData/en/gena/77930.pdf> (Zugriff: 20.1.2004); Burkard Schmitt, *The European Union and armaments. Getting a bigger bang for the Euro,* Chaillot Papers No 63 (Paris: Institute for Security Studies, 2003).

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

86 Dombrowski/Gholz/Ross, *Military Transformation and the Defense Industry after Next,* S. 83; Thornberry, „Fostering a culture of innovation", S. 5 (zitiert nach Internetversion).

## 7. Schlussfolgerungen

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

Die zentrale Schwäche des Neofunktionalismus, nämlich die Vernachlässigung der Politik, darf jedoch nicht zur Annahme verführen, dass der beschriebene Anpassungsbedarf geradezu automatisch erkannt und umgesetzt wird. Vielmehr geht es darum, dass die politischen Entscheidungsträger die beschriebenen Herausforderungen aktiv angehen. Dabei ist zweierlei hervorzuheben:

Auf der nationalen Ebene rücken sicherheitspolitische Vernetzungs- und Koordinationsorgane und die Kontaktstellen in den jeweiligen Ministerien ins Zentrum der Aufmerksamkeit. Diese Organe sind künftig nicht nur für die sicherheitspolitische Lageanalyse, die Strategieschöpfung und die Führung in der normalen sowie in der außerordentlichen Lage zuständig. Sie werden auch die entscheidende Rolle bei der Koordination der Akteure und der Maßnahmen im Rahmen vernetzter Operationen spielen. Zudem tragen sie in managementorientierter Hinsicht die Hauptverantwortung für die Sicherstellung der konzeptionellen Kohärenz (sicherheitspolitisches Managementsystem) und die ressortübergreifende Steuerung der Sicherheitsakteure sowie ihrer Mittel. Es versteht sich von selbst, dass ein derart anspruchsvolles Aufgabenspektrum kaum mit der bestehenden Ressourcenausstattung und den vorhandenen Fähigkeitsprofilen erbracht werden kann. Investitionen zur Stärkung sicherheitspolitischer Vernetzungsprozesse und -strukturen sollte daher besondere Priorität eingeräumt werden.

Ebenso müssen die Kompetenzen der internationalen Ebene gestärkt werden. Innerhalb des bestehenden intergouvernementalen Rahmens der Europäischen Sicherheits- und Verteidigungspolitik (ESVP) müssen die konzeptionelle Koordination und die Abstimmung wesentlich gestärkt werden. Das gilt für die vernetzte Operationsführung ebenso sehr wie für die vernetzte Sicherheitspolitik. Im ersten Fall müssen sich die EU-Mitglieder auf ein gemeinsames Konzept einigen und die dazu erforderlichen Umsetzungsprojekte über gemeinsame Strukturen koordinieren. Im zweiten Fall muss Europa mehr dafür tun, dass sich die Logik der vernetzten Sicherheitspolitik und die damit einhergehende Reform der Sicherheitssektoren in den eigenen Ansätzen zur Konfliktvor- und -nachsorge spiegeln. Die Europäische Sicherheitsstrategie muss diesen Aspekt bewusst aufnehmen und im Rahmen spezifischer Programme vorantreiben. Zu diesem Zweck ist insbesondere ein Instrumentarium zur Bewertung der sicherheitspolitischen Vernetzungsfähigkeit der bestehenden und der neuen EU-Mitglieder sowie zur Transformation ihrer Sicherheitssektoren zu entwickeln, das sich an den oben diskutierten Grundsätzen orientiert. Daneben muss die Zusammenarbeit zwischen den Generaldirektorien der Europäischen Kommission sowie zwischen diesen und den neuen ESVP-Gremien ebenfalls im Sinne der angesprochenen Vernetzung überprüft und ausgebaut werden.