

Heiko Borchert

Vernetzte Sicherheitspolitik: Bausteine eines neuen Leitbildes

Abstract: The new security risks are network centric, transnational and asymmetric. They originate from problems within rather than between states and involve non-state actors ready to use force to accomplish their mission. Today's security institutions are not ready to meet this challenge. A fundamental reform is necessary in order to establish cross-organizational processes and structures, improve the cooperability among various security sector actors and strengthen joint capabilities needed to tackle the new security risks.

Key words: Security sector transformation, interagency coordination, cooperability, capability orientation

Im Gegensatz zu der massiv erkennbaren Bedrohung zur Zeit des Kalten Krieges ist keine der neuen Bedrohungen rein militärischer Natur und kann auch nicht mit rein militärischen Mitteln bewältigt werden. Jede dieser Bedrohungen erfordert eine Kombination von Instrumenten. *Europäische Sicherheitsstrategie vom 8. Dezember 2003¹*

Die neuen sicherheitspolitischen Herausforderungen machen es erforderlich, dass die Ziele, die Prozesse und die Strukturen sowie die Mittel und die Fähigkeiten der relevanten Akteure des Sicherheitssektors – d.h. die militärischen, polizeilichen und paramilitärischen Streitkräfte, die übrigen Sicherheitskräfte, der Grenzschutz und die Nachrichtendienste sowie die politischen Aufsichtsorgane – besser und systematischer aufeinander abgestimmt werden. Das daraus resultierende Leitbild der vernetzten Sicherheitspolitik ist mit weitreichenden Konsequenzen verbunden. Die Diskussion im Rahmen des vorliegenden Aufsatzes legt zuerst dar, welche Entwicklungen den Übergang zur vernetzten Sicherheitspolitik erforderlich machen und geht danach auf drei miteinander verknüpfte Aspekte ein: die umfassende Betrachtung der Zusammenarbeitsfähigkeit in einem deutlich erweiterten Akteurskreis, das Management des vernetzten Sicherheitssektors sowie der Aufbau vernetzter Fähigkeiten, die von allen Akteuren des Sicherheitssektors genutzt werden können.

Vernetzte Sicherheitspolitik

Die Forderung nach einer verbesserten Abstimmung zwischen der Sicherheitspolitik und anderen Politikbereichen im Allgemeinen sowie zwischen den zur Verfügung stehenden Instrumenten im Besonderen ist auf verschiedene Entwicklungen zurückzuführen.² Erstens hat die Erosion des staatlichen Gewaltmonopols bei gleichzeitiger Privatisierung der Gewalt und dem Aufstreben nicht-staatlicher Gewaltakteure in zahlreichen Regionen der Welt ein neues Kon-

Eine ausführlichere Fassung dieses Beitrags erscheint demnächst in: Heiko Borchert (Hrsg.), *Vernetzte Sicherheit. Leitidee der Sicherheitspolitik im 21. Jahrhundert*, Hamburg/Berlin/Bonn 2004.

1 Ein sicheres Europa in einer besseren Welt. Europäische Sicherheitsstrategie, Brüssel, 12. Dezember 2003 <<http://ue.eu.int/solana/docs/031208ESSIIDE.pdf>> (Zugriff: 7. Januar 2004), S. 7.

2 Heiko Borchert und Reinhardt Rummel, Von segmentierter zu vernetzter Sicherheitspolitik in der EU-25. In: *Österreichische Militärische Zeitschrift* 3/2004 (i.V.).

flikt- und Risikobild geschaffen. Daraus resultieren neue Gefahren für die internationale Stabilität und Sicherheit wie beispielsweise die Proliferation von Massenvernichtungswaffen oder ethnisch motivierte Kriege, die zu Massenvertreibungen führen können. Weil die Anwendung von Gewalt in diesen Regionen wirtschaftlich vorteilhaft ist, entstehen sogenannte Bürgerkriegsökonomien, die über die weltwirtschaftliche Verflechtung direkt mit den Industrieländern verknüpft sind. Das neue Risikobild schlägt somit direkt und indirekt auf die stabilen Regionen der Welt zurück und erschwert dadurch die Unterscheidung zwischen innerer und äusserer Sicherheit sowie den Einsatz der dafür bislang vorgesehenen Mittel.³

Geht es, zweitens, um die Bekämpfung dieser neuen Risiken sowie ihrer Ursachen, so wird schnell klar, dass dafür neue Operationsformen gefordert sind. Die jüngste Entwicklung internationaler Stabilisierungsoperationen zeigt, dass die dazu eingesetzten Kräfte neben den klassischen Kampfaufgaben vermehrt Schutzaufgaben übernehmen. Dadurch kommt es zu einer Vermischung von militärischen mit polizeilichen Aufgaben in einem bislang konzeptionell kaum durchdrungenen Graubereich. Dabei 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. Parallel dazu erhöht, drittens, die Vertiefung und die Erweiterung der Europäischen Union (EU) die Anforderungen an die kohärente Politikvorbereitung und -umsetzung. Die Notwendigkeit, die vielfältigen und teilweise neuen Instrumente der EU-Aussen-, Sicherheits- und Verteidigungspolitik besser mit den vorhandenen Elementen aus den Bereichen der Aussenwirtschafts-, der Entwicklungs-, der Justiz- und der Innenpolitik abzustimmen bleibt nicht ohne Folgen für die nationale Planung in diesen Bereichen sowie die Koordination mit internationalen Initiativen und Beschlüssen.

Neben diesen politischen Entwicklungen ist zu berücksichtigen, dass der technologische Fortschritt die physische Vernetzung der Sicherheitsorgane und -kräfte tatsächlich ermöglicht bzw. vereinfacht. Vor diesem Hintergrund ist vor allem in den USA in den 90er Jahren ein umfassender militärischer Transformationsprozess lanciert worden, der durch die systematische Verknüpfung aller entscheidungs- und operationsrelevanten Elemente dazu beitragen soll, die Transparenz bei der Entscheidungsfindung zu verbessern, die Entscheidungsprozesse zu verkürzen, das Operationstempo zu erhöhen und die Wirkung im Einsatz zu steigern.⁴ Diese Überlegungen zur Anpassung von Verfahren und Strukturen im Informationszeitalter, die bislang vor allem im militärischen Bereich konkretisiert worden sind, können wegen ihres grundlegenden Charakters sinngemäss auf den gesamten Sicherheitssektor übertragen werden.

Vernetzte Sicherheitspolitik geht wie andere Ansätze davon aus, dass politisch-gesellschaftliche, wirtschaftliche, militärische, wissenschaftlich-technologische und ökologische Aspekte berücksichtigt werden müssen, um Krisen zu verhindern, deren Eskalation einzudämmen bzw. erforderlichenfalls zu bekämpfen sowie zur Stabilisierung im Nachgang eines Konflikts beizutragen. Es ist gerade dieses umfassende Verständnis von Sicherheit, das im

3 Hans-Georg Ehrhart, Die Europäische Union, die ESVP und das neue Sicherheitsdilemma. In: WeltTrends 38/2003, S. 135-144.

4 Hierzu grundlegend: David S. Alberts, John J. Garstka and Frederick P. Stein, Network Centric Warfare. Developing and Leveraging Information Superiority, 2nd ed., Washington, D.C. 2000.

Hinblick auf die Umsetzung die Erweiterung des relevanten Akteurskreises sowie die verstärkte Berücksichtigung organisatorischer und prozeduraler Aspekte erfordert. Sicherheitspolitische Vernetzungsfähigkeit bezieht sich demzufolge auf die

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

Zusammenarbeitsfähigkeit

Als Voraussetzung glaubwürdigen internationalen Handels ist die Fähigkeit zur Zusammenarbeit unerlässlich. Im Zeitalter der sicherheitspolitischen Vernetzung muss der Begriff jedoch in zweifacher Hinsicht erweitert werden.⁵ Zuerst müssen die bisherigen Überlegungen zur Zusammenarbeit zwischen den militärischen Streitkräften durch den Einbezug aller Sicherheitskräfte erweitert werden. Dieser Schritt ist unerlässlich, um die reibungslose Kooperation innerhalb des Sicherheitssektors zu gewährleisten. Zweitens ist die Privatwirtschaft konsequent in alle Überlegungen zur Sicherstellung der Zusammenarbeit einzubeziehen, denn in wichtigen Fragen wie beispielsweise dem Schutz der kritischen (Informations-)Infrastruktur oder der Vorsorge vor bioterroristischen Risiken kann Sicherheit nicht mehr ohne die Mitarbeit der Industrie bewältigt werden. Gleichzeitig ist zu beachten, dass diese doppelte Erweiterung nicht nur auf der nationalen, sondern auch auf der internationalen Ebene vollzogen werden muss, um dem transnationalen Charakter der neuen Sicherheitsrisiken Rechnung zu tragen.

Diese erweiterte Betrachtung der Zusammenarbeitsfähigkeit erfordert in einem ersten Schritt neue konzeptionelle Grundlagen zur Klärung der individuellen und der gemeinsamen Verantwortlichkeiten im Umgang mit den Sicherheitsrisiken. Die Privatwirtschaft ist dabei besonders gefordert, denn sie muss ihr eigenes Chancen- und Risikomanagement stärker durch sicherheitspolitische Überlegungen erweitern und gleichzeitig die vorhandenen Konzepte zur Weiterführung der unternehmerischen Tätigkeit im Krisenfall (Business Continuity) überprüfen bzw. auf- und ausbauen.⁶ Gleichzeitig muss untersucht werden, ob und wie spezifische Fähigkeiten der Privatwirtschaft (z.B. Expertise zum Schutz der Informationstechnologie) mit denjenigen der staatlichen Sicherheitskräfte kombiniert werden können. In einem

5 Der Zusammenhang zwischen technologischem Fortschritt und der Zusammenarbeitsfähigkeit wird an dieser Stelle nicht diskutiert. Siehe hierzu: David C. Gompert, Richard L. Kugler und Martin C. Libicki, *Mind the Gap. Promoting a Transatlantic Revolution in Military Affairs*, Washington, D.C. 1999; Alberts/Garstka/Stein, *Network Centric Warfare*; Michael O'Hanlon, *Technological Change and the Future of Warfare*, Washington, D.C. 2000.

6 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 2003, S. 95-120.

zweiten Schritt ist darüber nachzudenken, wie die Zusammenarbeit durch gemeinsame Standards (z.B. Doktrin, Planung, Beschaffung, Einsatz und Ausbildung) erleichtert und gefördert werden kann. Militärische Erfahrungen können hierzu sinngemäss übertragen werden, um beispielsweise auch im Bereich der zivilen Sicherheit Transformationsprozesse zu initiieren, die die systematische Weiterentwicklung der Fähigkeiten unter Einbezug der Industrie ermöglichen. Angesichts des Risikos, dass divergierende nationale Ansätze in diesem Bereich möglicherweise zu unterschiedlichen Standards führen, die ihrerseits die internationale Kooperation behindern und eventuell auch wirtschaftliche Wettbewerbsnachteile mit sich bringen, sollte die EU aufgrund ihres multidisziplinären Ansatzes die wichtige Koordinationsrolle übernehmen. Schliesslich ist auch daran zu denken, dass es national wie international neue Instrumente braucht, um die Einhaltung der Standards im vernetzten Sicherheitssektor zu überprüfen. Zudem sollte deren Anwendung durch gemeinsame Ausbildungs- und Trainingsansätze eingeübt werden, wodurch das Verständnis für das Denken und das Handeln der involvierten Partner erhöht und Vertrauen aufgebaut werden können.

Management des vernetzten Sicherheitssektors

Die neuen sicherheitspolitischen Herausforderungen machen nicht vor den traditionellen Organisationsgrenzen halt. Gleichwohl werden Managementaspekte im Zusammenhang mit sicherheitspolitischen Fragestellungen generell zu selten thematisiert. Völlig zu recht weist Ashton B. Carter darauf hin, dass viele der neuen sicherheitspolitischen Aufgaben "institutionell heimatlos" sind, das heisst es fehlt die klare Zuordnung von Verantwortung, Kompetenzen und Mitteln zu deren Bewältigung.⁷ Jede Reform, die diesen Missstand beheben und dazu beitragen soll, die Fähigkeit der Sicherheitskräfte und der Ministerien im Umgang mit diesen Herausforderungen zu verbessern, muss daher prozessorientiert und ressortübergreifend angelegt sein. Das bedingt eine Reihe grundlegender Veränderungen in der Organisation und im Management des Sicherheitssektors.

Konzeptioneller Dreh- und Angelpunkt moderner Organisationen sind sogenannte *Managementsysteme*, d.h. die Gesamtheit der aufeinander abgestimmten Prozesse, Strukturen und Instrumente einer Organisation.⁸ Die zunehmende Bedeutung von Managementsystemen im öffentlichen Sektor ist vor allem auf neue Ansätze der wirkungsorientierten Verwaltungsführung zurückzuführen. Im Umgang mit den neuen sicherheitspolitischen Herausforderungen sind zwei Dimensionen der Weiterentwicklung auszumachen. Einerseits sind die Managementsysteme der Ministerien und der Sicherheitskräfte, die gemeinsam den Sicherheitssektor definieren, besser aufeinander abzustimmen. Konkret geht es darum, für den gesamten Sicherheitssektor übergreifende Prozesse zu definieren, die in einem Prozessmodell zusammengefasst werden und dabei insbesondere auch die Schnittstelle zur Privatindustrie (z.B. zum Einbezug der Wirtschaft in die Krisenvorsorge bzw. das Krisenmanagement) systematisch berücksichtigen. Andererseits muss die Kohärenz der organisations- und ressortspezifischen

7 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 2001, S. 1-26, hier S. 2.

8 Markus Schwaninger, Managementsysteme, Frankfurt 1994.

Managementsysteme vor dem Hintergrund der intensiveren Zusammenarbeit gewährleistet werden. Hier sind vor allem die zentralen Leitungsbereiche der Ministerien gefordert, um die entsprechenden Vorgaben zu entwickeln und deren Einhaltung bzw. Weiterentwicklung sicherzustellen. Da beide Aspekte nahtlos aufeinander abgestimmt werden müssen, drängen sich die Ernennung von Managementverantwortlichen⁹ sowie der Aufbau eines managementorientierten Vernetzungsgremiums für den Sicherheitssektor auf, um diese Arbeiten zu koordinieren. Eventuell besteht auch die Möglichkeit, bestehende ressortübergreifende Einrichtungen (z.B. Bundessicherheitsrat bzw. dessen Ausschüsse) mit dieser Aufgabe zu betrauen.

Ebenso bedeutend ist die Fähigkeit des vernetzten Sicherheitssektors zur *integrierten Strategiedefinition*. Politikbereichsspezifische Strategien müssen aus einer sicherheitspolitischen Gesamtstrategie abgeleitet werden, die ihrerseits das Ergebnis einer gemeinsamen Lagebeurteilung ist. Dieser Ansatz bedingt ein funktionierendes Managementsystem, das es erlaubt, Kompetenzen und Verantwortungen abgestimmt auf die definierten Ziele prozessorientiert zuzuweisen. Zudem sind Führungsinstrumente erforderlich, die es ermöglichen, Chancen und Risiken systematisch zu erkennen, zu bewerten und zu verfolgen. Dies gilt vor allem mit Blick auf die anspruchsvollen organisatorischen Reformprojekte sowie für den Umgang mit moderner Technologie (z.B. IT-Projekte). Zusätzlich ist zu berücksichtigen, dass sich die Zahl der relevanten Anspruchsgruppen durch den Trend zur Vernetzung erhöht, beispielsweise bei der Berufung von Reformkommissionen oder bei der Zusammenarbeit mit nicht-staatlichen Akteuren im Einsatzgebiet. Es empfiehlt sich daher, auch im Sicherheitssektor den Übergang zum systematischen Management der Beziehungen zu Anspruchsgruppen (Stakeholder Management) einzuleiten, indem die Motive und das Kooperationsverhalten von Anspruchsgruppen untersucht sowie die eigenen Ziele, Mittel und Verfahren zur erfolgreichen Zusammenarbeit mit diesen definiert werden.

Die Forderung nach konsequenter Prozessorientierung und der Übergang zur integrierten Strategiedefinition haben zur Folge, dass auch die *Planung* im vernetzten Sicherheitssektor verstärkt integriert werden muss. Zuerst geht es darum, das Verhältnis zwischen ressortübergreifender und ressorteigener Planung zu klären, wobei weder die vollständige Zentralisierung noch die komplette Dezentralisierung als sinnvolle Lösungen in Frage kommen. Ein neues Gleichgewicht könnte beispielsweise gefunden werden, indem die langfristigen Planungsaufgaben, die zur Harmonisierung der Perzeptionen und der Interessen der daran beteiligten Ressorts beitragen können, ressortübergreifend koordiniert werden, z.B. auf der Stufe des Bundessicherheitsrats. Die Koordination und die Integration auf dieser Stufe erlauben es den nachgeordneten Bereichsebenen, intelligenter zu planen und dadurch knappe Mittel effektiver und effizienter einzusetzen. Die daraus abgeleiteten ressortspezifischen Planungsaufgaben würden wie bisher von den Fachressorts verantwortet, wären jedoch stärker als bislang an gemeinsamen Planungsvorgaben ausgerichtet. Dieser Ansatz sollte auch mit Blick auf das Verhältnis zwischen internationalen und nationalen Planungsaufgaben verfolgt werden. Hierbei geht es neben der zeitlichen Abstimmung der Planungsrhythmen immer mehr auch um die inhaltliche Harmonisierung, die beispielsweise über gemeinsame Fähigkeitsziele oder Kon-

9 Beim Aufbau des US-amerikanischen Department for Homeland Security wurde die Position des Under Secretary for Management geschaffen, um die managementspezifischen Aufgaben in einer Funktion zu bündeln. Siehe hierzu: <<http://www.dhs.gov/dhspublic/display?theme=54>> (Zugriff: 7. Januar 2004).

vergenzkriterien sichergestellt werden kann. Als Bindeglied zwischen der nationalen und der internationalen Ebene spielen diese eine zunehmend wichtige Rolle und sollten daher ebenfalls auf alle Belange des vernetzten Sicherheitssektors ausgerichtet werden.

Die bisherigen Überlegungen müssen in adäquate *Organisationsstrukturen* überführt werden. Dabei geht die wesentliche Herausforderung von der Notwendigkeit aus, die traditionelle Dominanz der ressortspezifischen Linienorganisation durch die ressortübergreifende Prozessorientierung zu ergänzen bzw. in einigen Bereichen auch zu ersetzen. Entscheidend ist, dass neu geschaffene Vernetzungsgremien in der Praxis tatsächlich Wirkung erzielen und nicht über die Linie unterlaufen werden. Zu diesem Zweck ist es erforderlich, die Prozesse zur Zieldefinition sowie zur Zuteilung von Finanz- und Personalmitteln konsequent ressortübergreifend zu steuern. Denkbar ist, dass die diesbezügliche Abstimmung über den Bundessicherheitsrat bzw. die entsprechenden Koordinationsfunktionen des Bundeskanzleramts sichergestellt wird. Bewegt sich die Verwaltung stärker in Richtung Vernetzungsorganisation, hat dies natürlich auch Auswirkungen auf die entsprechenden parlamentarischen Aufsichtsorgane. So hat beispielsweise das US-Repräsentantenhaus ein neues Select Committee for Homeland Security geschaffen, um den Aufbau und die Arbeit des entsprechenden Ministeriums zu begleiten.¹⁰ In vergleichbarer Weise dürfte die Forderung nach sicherheitspolitischer Vernetzung zu einer Neuordnung der Zuständigkeiten der parlamentarischen Ausschüsse führen. Ziel muss es sein, die Aussen-, Sicherheits- und Verteidigungspolitik, die Arbeit der Nachrichtendienste sowie die Schnittstellen zu anderen Politikbereichen wie der Aussenwirtschafts-, Entwicklungs- und Forschungspolitik in umfassender Weise zu betrachten.¹¹

Soll der vernetzte Sicherheitssektor auf Kurs gehalten werden, ist gleichzeitig über neue *Steuerungsinstrumente* nachzudenken. Hierzu leistet die ressortübergreifende Prozessorientierung bereits einen wesentlichen Beitrag. Daneben gewinnt das strategische Controlling und Reporting an Bedeutung. Dieses kann jedoch nur dann greifen, wenn auch steuerungsrelevante Führungsinformationen für den vernetzten Sicherheitssektor generiert werden können. Ein "trockenes" Instrument wie die Kosten- und Leistungsrechnung spielt mit Blick auf die vernetzte Sicherheitspolitik eine wichtige Rolle. Nur wenn es innerhalb des Sicherheitssektors gelingt, die Kostenerfassung zu vereinheitlichen und Transparenz über die Kosten der erbrachten Leistungen herzustellen, sind der Leistungsaustausch (z.B. in Form eines Einsatzes des Militärs zugunsten des Innenministeriums) sowie das Zusammenlegen von Ressourcen und Fähigkeiten (z.B. für die Nachrichtengewinnung, Aufklärung und Überwachung) überhaupt zu realisieren. Daneben ist zu beachten, dass die konsequente Weiterentwicklung des Sicherheitssektors gerade in Zeiten teilweise diffuser Sicherheitsrisiken besonders wichtig ist. Im Zusammenhang mit der Streitkräfteentwicklung ist daher zu recht der Aufbau eines Transformationsaudits vorgeschlagen worden, mit dessen Hilfe Stärken und Schwächen systematisch identifiziert werden können.¹² Diese Idee muss um die Forderung nach einem Bewertungsansatz für die Weiterentwicklung des gesamten Sicherheitssektors (Security Sector Ass-

10 <<http://hsc.house.gov>> (Zugriff: 7. Januar 2004).

11 Dies betrifft im Deutschen Bundestag z.B. die Zusammenarbeit zwischen den Ausschüssen für auswärtige Angelegenheiten, Verteidigung, Umwelt, Naturschutz und Reaktorsicherheit, Bildung, Forschung und Technikfolgenabschätzung sowie für wirtschaftliche Zusammenarbeit und Entwicklung.

12 Holger H. Mey und Michael K.-D. Krüger, Vernetzt zum Erfolg? "Network-Centric Warfare" – zur Bedeutung für die Bundeswehr, Frankfurt 2003, S. 12.

essment) ergänzt werden. Dieser sollte neben der Eigenbeurteilung auch die Fremdbewertung durch Dritte, analog beispielsweise zum Planning and Review Process (PARP) der NATO, vorsehen und ein besonderes Augenmerk auf Schlüsselaspekte wie das vernetzte Management, die ressortspezifische und ressortgemeinsame Fähigkeitsorientierung sowie die Zusammenarbeitsfähigkeit legen.

Die erfolgreiche Gestaltung der skizzierten Veränderungen erfordert den grundsätzlichen Wandel der vorherrschenden *Organisationskultur*. Im Unterschied zum Bestehenden bedingt die sicherheitspolitische Vernetzung eine neue Kultur, die auf Vertrauen, Delegation, Eigeninitiative, Selbständigkeit und Eigenverantwortung basiert. Die Herstellung des Kulturwandels ist eine entscheidende Führungsaufgabe, die nur gelingen kann, wenn die Mitarbeitenden aktiv in diesen Prozess einbezogen werden. Der erste Punkt verlangt, dass die Führungskräfte ihren Veränderungswillen durch konkrete Taten unter Beweis stellen. Beispielsweise durch die Übernahme der Projektauficht in Reformprojekten, die die sicherheitspolitische Vernetzung stärken, oder durch die Teilnahme an Aus- und Weiterbildungsveranstaltungen, die die Sensibilität für die ressortübergreifende Zusammenarbeit fördern. Um das Engagement der Mitarbeitenden zu erhöhen, muss z.B. die Aus- und Weiterbildung konsequent auf die neuen Anforderungen der Vernetzung ausgerichtet werden. Gemeinsame Führungslehrgänge¹³ sollten ebenso selbstverständlich werden wie die Personalrotation zwischen den Ministerien und den Sicherheitskräften sowie zwischen dem öffentlichen und dem privatwirtschaftlichen Sektor. Die Laufbahnplanung sollte gezielt ressortübergreifende Karrierewege anbieten, und im Hinblick auf die berufliche Beförderung sollten Einsätze in anderen Sicherheitsressorts als Qualifizierungskriterien eingesetzt werden.¹⁴

Vernetzte Fähigkeiten

Durch die eingangs beschriebenen Veränderungen im sicherheitspolitischen Umfeld rücken die Aufgabenprofile der Sicherheitskräfte näher zusammen. Damit gewinnen jene Fähigkeiten an Bedeutung, die dazu beitragen, die Vernetzung der Sicherheitskräfte sicherzustellen bzw. zu vereinfachen und von allen Sicherheitskräften nutzenbringend eingesetzt werden können. Solche Fähigkeiten können als "vernetzte Fähigkeiten" bezeichnet werden.

Die Aufarbeitung der Ereignisse des 11. September 2001 hat in den USA aber auch in Europa zu teilweise ernüchternden Einsichten über den Ausrüstungszustand und die Fähigkeitsprofile gewisser Sicherheitskräfte geführt. Über 100 Feuerwehrleute sollen beim Brand des World Trade Center allein deshalb gestorben sein, weil die Kommunikations- und Informationssysteme der Einsatz- und Rettungskräfte unzureichend aufeinander abgestimmt waren.¹⁵ Darüber hinaus verfügen beispielsweise die US-amerikanischen Polizeikräfte nicht über

13 Ein gutes, bewusst ressortübergreifend angelegtes Beispiel ist der strategische Führungslehrgang an der österreichischen Landesverteidigungsakademie. Siehe: <<http://www.stratfuehg.gv.at/seite1.htm>> (Zugriff. 7. Januar 2004).

14 David S. Alberts, *Information Age Transformation. Getting to a 21st Century Military*, Washington, D.C. 2002, S. 123-124; David S. Alberts and Richard Hayes, *Power to the Edge. Command and Control in the Information Age*, Washington, D.C. 2003, S. 223-232.

15 Thomas Enders, Herausforderung "Homeland Security" für die Industrie. In: *Europäische Sicherheit*, 10/2003, S. 8-11, hier S. 8.

das erforderliche Gerät, um einen mit Massenvernichtungswaffen angegriffenen Ort abzuschern. Den meisten Städten fehlen die Geräte, um herauszufinden, ob und in welchem Ausmaß die Einsatz- und Rettungskräfte an einem Schadensort gefährlichen Stoffen ausgesetzt sind.¹⁶ Auch in Europa gibt es ähnliche Schwächen beispielsweise im Bereiche der konzeptionellen Grundlagen der Zusammenarbeit zwischen den Behörden und Organisationen mit Rettungs- und Sicherheitsaufgaben oder der Interoperabilität der von diesen eingesetzten Kommunikationssystemen.¹⁷ Allerdings gibt es erste Anzeichen der Verbesserung im Sinne der angeregten Vernetzung, indem beispielsweise Kommunikationssysteme auf alle Sicherheitskräfte ausgedehnt werden (Frankreich, Schweiz) oder gemeinsame Lagebilder unter Einschluss militärischer und ziviler Sicherheitskräfte erarbeitet werden (Frankreich).¹⁸ Aus diesen Beispielen und den genannten Defizitbereichen lässt sich eine Liste jener vernetzten Fähigkeiten ableiten, die künftig besonderer Beachtung bedürfen. Dazu zählen u.a. die Führung als Kernvoraussetzung erfolgreicher Operationen, die Nachrichtengewinnung, Überwachung und Aufklärung für ein gemeinsames Lagebild, die Verlegungsfähigkeit zur verbesserten Mobilität der Sicherheitskräfte sowie die Überlebensfähigkeit und der Schutz zur Sicherheit der eingesetzten Kräfte bzw. ihres Materials (z.B. durch ABC-Schutz und -Abwehr oder elektronischen Schutz).

Im Hinblick auf die Definition der vernetzten Fähigkeiten ist festzulegen, wer diese identifiziert und durch wen bzw. in welcher Form diese weiterentwickelt werden. Aufgrund der bisherigen Ausführungen erscheint es sinnvoll, die Identifizierung und die Weiterentwicklung über das angeregte Managementsysteme bzw. das umfassende Assessment des gesamten Sicherheitssektors abzuwickeln. Ein Vernetzungsorgan wie der Bundessicherheitsrat sollte für die Festlegung der Schwerpunkte zuständig sein und die strategische Steuerung mit Hilfe der koordinierenden Rolle des Bundeskanzleramts wahrnehmen, während die jeweiligen Sicherheitskräfte für die Bewirtschaftung und das operative Management der Fähigkeiten verantwortlich zeichnen. Angesichts knapper öffentlicher Budgets kann es allerdings nicht darum gehen, die Fähigkeitsdefizite der jeweiligen Sicherheitskräfte individuell zu beheben. Vielmehr müssen Ideen wie die Rollenspezialisierung oder die Zusammenlegung von Ressourcen und Fähigkeiten unter Einbezug aller Akteure des Sicherheitssektors konsequent angewendet werden.¹⁹ Das hätte beispielsweise zur Folge, dass ein ABC-Kompetenzpool mit Hilfe entsprechender militärischer ABC-Schutz- und Abwehrfähigkeiten, der Fachexpertise der chemischen und Biotech-Industrie, privaten und wissenschaftlichen Instituten der öffentlichen Hand sowie den Krankenhäusern eingerichtet werden könnte.²⁰

16 Emergency Responders: Drastically Underfunded, Dangerously Unprepared, New York 2003, S. 5.

17 Flutkatastrophe 2002. Bericht der Unabhängigen Kommission der Sächsischen Staatsregierung, S. 183-184, 241 ff.; USIS, Analyse des Ist-Zustandes mit Stärken-/Schwächenprofil, Bern 2001, S. 15, 17 <http://www.usis.ch/deutsch/berichte/pdf_usis1/Medienrohstoff_d.pdf> (Zugriff: 7. Januar 2004).

18 Enders, Herausforderung 'Homeland Security' für die Industrie, S. 9; USIS, Teil II. Grobe Soll-Varianten, Sofortmassnahmen, Bern 2001, S. 20 <http://www.usis.ch/deutsch/berichte/pdf_usis2_voll/deutsch.pdf> (Zugriff: 7. Januar 2004).

19 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 2004 (i.V.).

20 So ähnlich auch: Mey/Krüger, Vernetzt zum Erfolg?, S. 60.

Schlussfolgerungen

Sicherheitspolitik kann heute weder ausschliesslich national noch ressortspezifisch betrieben werden, sondern erfordert internationale und ressortübergreifende Konzeption und Koordination. Das Leitbild der vernetzten Sicherheitspolitik trägt dieser Einsicht Rechnung, indem es die Ziele und die Strategien, die Prozesse und die Strukturen sowie die Fähigkeiten und die Mittel der Akteure des Sicherheitssektors – unter Einschluss der Industrie – systematisch aufeinander abstimmt und miteinander verbindet. Der Übergang vom traditionellen zum vernetzten Ansatz erfolgt jedoch nicht automatisch, sondern muss national wie international aktiv gestaltet werden.

Auf der nationalen Ebene besteht die zentrale Herausforderung in der Stärkung der sicherheitspolitischen Vernetzungsorgane sowie der ressortübergreifender Koordinationsprozesse. Sicherheitspolitische Basisaufgaben wie Lageanalyse, Strategiebestimmung und Fähigkeitsdefinition müssen integriert, d.h. unter Einbezug aller Akteure des Sicherheitssektors, erfolgen. Ressortspezifische Zielsetzungen und Programme sind konsequent aus dieser übergeordneten Sichtweise abzuleiten. Daneben ist, als Voraussetzung für das Erreichen der geforderten inhaltlichen Harmonisierung, dem Management des vernetzten Sicherheitssektors stärkere Beachtung zu schenken. Hier geht es darum, wesentliche Prozesse zur Lageanalyse, zur Strategiebestimmung sowie zur Steuerung und zur Weiterentwicklung des Sicherheitssektors konsequent ressortübergreifend zu gestalten. Gleichzeitig sollten Investitionen in gemeinsame Fähigkeiten sowie zum Ausbau sicherheitspolitischer Vernetzungsorgane und ressortübergreifender Koordinationsprozesse vorrangig behandelt werden.

Diese nationalen Reformbemühungen müssen auf der internationalen Ebene konsequent fortgesetzt werden. Die Forderung nach sicherheitspolitischer Vernetzung betrifft sowohl die Gestaltung der Abläufe und der Strukturen in den wichtigsten internationalen Organisationen als auch deren Zusammenarbeit. In Europa dürfte dabei die EU eine Schlüsselrolle spielen, weil sie wie kaum eine zweite Organisation in der Lage ist, verschiedene Politikfelder miteinander zu kombinieren. Erste Anzeichen wie die integrale Behandlung der zivilen und der militärischen Komponenten der EU-Sicherheitspolitik im Aussenministerrat oder die gemeinsame Planung ziviler und militärischer Einsätze über die neue operative EU-Planungszelle sind ermutigende Zeichen, reichen aber noch nicht aus.²¹ Die Europäische Sicherheitsstrategie muss sich die Logik der vernetzten Sicherheitspolitik zu eigen machen und die damit verbundene Transformation des Sicherheitssektors konsequent vorantreiben. Die daraus resultierende Harmonisierung und Synchronisierung der nationalen Prozesse und Strukturen erleichtert künftig den Einsatz der zur Verfügung stehenden Sicherheitskräfte. Gleichzeitig wirken die Stärkung der staatlichen Institutionen sowie die verbesserte Zusammenarbeit zwischen diesen der ungewollten Privatisierung des staatlichen Gewaltmonopols entgegen und verbessern die Gefahren- bzw. die Bedrohungsabwehr. Deshalb sollte die EU spezifische Instrumente zur Bewertung der sicherheitspolitischen Vernetzungsfähigkeit der bisherigen und der neuen Mitglieder entwickeln. Es empfiehlt sich, diese Aufgabe eng mit anderen Organisationen wie der NATO, der OSZE und dem Europarat abzustimmen, da diese in einzelnen Bereichen über

21 EU operational planning. The politics of defence. In: IISS Strategic Comments 10/2003.

spezifische Expertise verfügen, die sinnvollerweise berücksichtigt wird. Diese enge Zusammenarbeit wird es insbesondere im Hinblick auf die Stabilisierung von Krisenregionen ermöglichen, die internationalen Programme zum Wiederaufbau bzw. zur Reform und zur Weiterentwicklung der Sicherheitssektoren besser aufeinander abzustimmen.

Autorenangabe

Dr. Heiko Borchert führt ein Unternehmens- und Politikberatungsbüro und ist Direktor für Sicherheit und Verteidigung am Düsseldorfer Institut für Aussen- und Sicherheitspolitik (DI-AS).