

Veröffentlicht in: Europäische Sicherheit, 53:6 (Juni 2004), S. 33-38.

Heiko Borchert

Vernetzte Sicherheitspolitik und die Transformation des Sicherheitssektors

Die aktuellen Diskussionen um die Neuverteilung der Aufgaben zwischen den verschiedenen Sicherheitskräften im Rahmen der internationalen Stabilisierungsbemühungen, der Heimatsicherheit (Homeland Security) oder des Kampfs gegen den internationalen Terrorismus sind nur drei Beispiele, die eines verdeutlichen: unsere Sicherheitsinstitutionen sind schlecht auf die neuen sicherheitspolitischen Herausforderungen vorbereitet. Während die neuen Sicherheitsrisiken transnational, teilweise asymmetrisch und vernetzt sind, basieren die Sicherheitsinstitutionen nach wie vor auf ressortspezifischen Überlegungen. Weil die sicherheitspolitischen Aufgaben neu zugeordnet werden müssen, drängt sich die Transformation des Sicherheitssektors auf, der die militärischen, polizeilichen und paramilitärischen Streitkräfte, die übrigen Sicherheits- und Rettungskräfte, den Grenzschutz und die Nachrichtendienste sowie die politischen Aufsichtsorgane umfasst. Von grundlegender Bedeutung ist dabei die Idee der sicherheitspolitischen Vernetzung, die im vorliegenden Aufsatz mit Blick auf die Zusammenarbeitsfähigkeit, das Management des Sicherheitssektors sowie den Aufbau vernetzter Fähigkeiten diskutiert wird.

Vernetzte Sicherheitspolitik

Vernetzte Sicherheitspolitik geht 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. Um dieses umfassende Sicherheitsverständnis in die Praxis umzusetzen, müssen der Kreis der relevanten Akteure erweitert sowie das Management des Sicherheitssektors verstärkt beachtet werden. Sicherheitspolitische Vernetzungsfähigkeit erfordert einen integrierten Ansatz, der die verschiedenen Ebenen der Beschlussfassung und der Umsetzung, die relevanten Akteure, die zu erfüllenden Aufgaben sowie die vorhandenen Instrumente miteinander kombiniert.

Die Gründe für die Forderung nach konsequenter Vernetzung sind vielfältig: Transnationale Sicherheitsrisiken und der Bedeutungsgewinn nicht-staatlicher Gewaltakteure, die sich zur Finanzierung ihrer Vorhaben u.a. der weltwirtschaftlichen Globalisierung bedienen, tragen dazu bei, dass kaum noch trennscharf zwischen innerer und äusserer Sicherheit unterschieden werden kann. Daraus folgt, dass neue Kombinationen von Sicherheitsinstrumenten und Operationsformen erforderlich sind, um diese Risiken und ihre Ursachen in den verschiedenen Phasen der Konfliktverhütung und -bewältigung erfolgreich zu bekämpfen. Parallel dazu erhöhen die Vertiefung und die Erweiterung der Europäischen Union (EU) die Anforderungen an die kohärente Politikvorbereitung und -umsetzung, denn die bessere Abstimmung zwischen der Aussen-, Sicherheits-, Verteidigungs-, Aussenwirtschafts-, Entwicklungs-, Justiz- und Innenpolitik auf der europäischen Ebene beeinflusst die nationale Planung in diesen Bereichen. Und schliesslich ermöglicht der technologische Fortschritt die physische Vernet-

zung der Sicherheitskräfte. Der unter dem Stichwort der vernetzten Operationsführung (Network Centric oder Network Enabled Warfare) lancierte militärischen Transformationsprozess will durch die systematische Verknüpfung aller entscheidungs- und operationsrelevanten Elemente dazu beitragen, die Transparenz bei der Entscheidungsfindung zu verbessern, die Entscheidungsprozesse zu verkürzen, das Operationstempo zu erhöhen und die Wirkung im Einsatz zu steigern. Diese Ziele beziehen sich auf allgemeine organisationstheoretische Überlegungen und können daher sinngemäss auf die Transformation des gesamten Sicherheitssektors übertragen werden.

Zusammenarbeitsfähigkeit

Glaubwürdiges internationales Handeln setzt die Fähigkeit zur Kooperation voraus. Sicherheitspolitische Vernetzungsfähigkeit macht es erforderlich, die Kooperationsfähigkeit in zweifacher Hinsicht zu erweitern: Zuerst müssen die bisherigen Überlegungen zur Zusammenarbeitsfähigkeit zwischen den militärischen Streitkräften auf alle Sicherheitskräfte übertragen werden. Dieser Schritt ist unerlässlich, um die reibungslose Kooperation innerhalb des Sicherheitssektors zu gewährleisten. Zusätzlich 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 bedingt neue Konzepte 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 durch sicherheitspolitische Überlegungen ergänzen und die vorhandenen Konzepte zur Weiterführung der unternehmerischen Tätigkeit im Krisenfall überprüfen. 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. Ferner ist darüber nachzudenken, wie die Zusammenarbeit durch gemeinsame Standards (z.B. Doktrin, Planung, Beschaffung, Einsatz und Ausbildung) erleichtert und gefördert werden kann. Angesichts des Risikos, dass divergierende nationale Lösungsansätze zu unterschiedlichen Standards führen können, die ihrerseits die internationale Kooperation behindern und eventuell auch wirtschaftliche Wettbewerbsnachteile mit sich bringen, sollte die EU hier eine Koordinationsfunktion übernehmen. Und schliesslich braucht es national wie international neue Instrumente, um die Einhaltung der Standards im vernetzten Sicherheitssektor zu überprüfen bzw. in gemeinsamen Ausbildungs- und Trainingsprogrammen einzuüben.

Management des vernetzten Sicherheitssektors

Diese Bestandsaufnahme macht deutlich, dass die Zuordnung von Verantwortung, Kompetenzen und Mitteln im Umgang mit den Sicherheitsrisiken gegenwärtig noch nicht den neuen

Herausforderungen entspricht. Die Transformation des Sicherheitssektors, die auf der Logik der vernetzten Sicherheitspolitik basiert, sollte daher an den folgenden fünf Punkten ansetzen.

Konzeptioneller Dreh- und Angelpunkt moderner Organisationen sind sogenannte *Managementsysteme*, d.h. die Gesamtheit der aufeinander abgestimmten Prozesse, Strukturen und Instrumente einer Organisation. Die neuen Sicherheitsrisiken machen es einerseits erforderlich, Prozesse zu definieren, die ressortübergreifend den gesamten Sicherheitssektor und die Industrie umfassen sowie in einem übergreifenden Managementsystem zusammengefasst werden. Andererseits müssen die ressortspezifischen Managementsysteme angepasst werden, um der Zusammenarbeit in einem erweiterten Akteurskreis Rechnung zu tragen. Beide Aspekte müssen eng aufeinander abgestimmt werden, was beispielsweise durch die Ernennung von Managementverantwortlichen, den Aufbau managementorientierter Vernetzungsgremien oder den verstärkten Einbezug bestehender, ressortübergreifender Institutionen (z.B. Bundessicherheitsrat, BSR bzw. dessen Ausschüsse) gewährleistet werden kann.

Ebenso bedeutend ist die Fähigkeit zur *integrierten Strategiedefinition*. Politikbereichsspezifische Strategien müssen aus einer sicherheitspolitischen Gesamtstrategie abgeleitet werden, die ihrerseits das Ergebnis einer gemeinsamen Lagebeurteilung ist. Dieser Ansatz erfordert es, Kompetenzen und Verantwortungen abgestimmt auf die definierten Ziele prozessorientiert zuzuweisen. Das britische Beispiel des Global Conflict Prevention Pool, an dem sich das Aussen-, Verteidigungs- und Entwicklungshilfeministerium beteiligen, verdeutlicht, dass dieses Vorhaben durch die enge, ressortübergreifende Vernetzung auf allen Arbeitsstufen wesentlich erleichtert wird. 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 anspruchsvolle organisatorische Reformprojekte sowie für den Umgang mit moderner Technologie. Weil schliesslich auch die Zahl der relevanten Anspruchsgruppen durch die Vernetzung zunimmt, drängt sich der Übergang zum systematischen Management der Beziehungen zu Anspruchsgruppen (Stakeholder Management) auf, indem die Motive und das Kooperationsverhalten von Anspruchsgruppen untersucht sowie die eigenen Ziele, Mittel und Verfahren zur erfolgreichen Zusammenarbeit mit diesen definiert werden.

In der Folge muss auch die *Planung* im vernetzten Sicherheitssektor verstärkt integriert werden. Im Verhältnis zwischen ressortübergreifender und ressorteigener Planung erscheint es sinnvoll, die langfristigen Planungsaufgaben, die zur Harmonisierung der Perzeptionen und der Interessen der daran beteiligten Ressorts beitragen können, ressortübergreifend zu koordinieren (z.B. auf Stufe BSR). Die Koordination und die Integration auf dieser Stufe erlauben es den nachgeordneten Bereichsebenen, intelligenter zu planen, knappe Mittel effektiver und effizienter einzusetzen sowie die ressortspezifische Planung stärker als bislang auf gemeinsame Vorgaben auszurichten. Dieser Ansatz sollte auch im Verhältnis zwischen nationaler und internationaler Planung verfolgt werden. Hierbei geht es neben der zeitlichen Abstimmung der Planungsrhythmen immer mehr auch um die inhaltliche Harmonisierung. Als Bindeglied zwischen der nationalen und der internationalen Ebene spielen z.B. gemeinsame Fähigkeitsziele oder Konvergenzkriterien eine zunehmend wichtige Rolle. Sie sollten daher ebenfalls auf alle Belange des vernetzten Sicherheitssektors ausgerichtet und konsequent in die Planung integriert werden.

Bei der Reform der *Organisationsstrukturen* geht es vor allem darum, die traditionelle Dominanz der ressortspezifischen Linienorganisation durch die ressortübergreifende Prozessorientierung zu ergänzen bzw. in einigen Bereichen auch zu ersetzen. Neu geschaffene Vernetzungsgremien können in der Praxis nur dann Wirkung erzielen, wenn die Prozesse zur Zieldefinition sowie zur Zuteilung von Finanz- und Personalmitteln konsequent ressortübergreifend gesteuert werden. Denkbar ist, dass die diesbezügliche Abstimmung über den BSR bzw. die entsprechenden Koordinationsfunktionen des Bundeskanzleramts sichergestellt wird. Die vernetzungsorientierte Neugestaltung der Verwaltungsstrukturen dürfte daneben auch zu einer Neuordnung der Zuständigkeiten der parlamentarischen Aufsichtsorgane führen. Ziel sollte es sein, die Aussen-, Sicherheits- und Verteidigungspolitik, die Arbeit der Nachrichtendienste sowie die Schnittstellen zu anderen Politikbereichen wie der Aussenwirtschafts-, Entwicklungs-, Wissenschafts- und Industriepolitik in umfassender Weise zu betrachten.

Um den vernetzten Sicherheitssektor auf Kurs zu halten, müssen die *Steuerungsinstrumente* angepasst werden. Neben dem Gesagten gewinnt dabei vor allem das strategische Controlling und Reporting an Bedeutung. Dieses kann jedoch nur dann greifen, wenn auch steuerungsrelevante Führungsinformationen (z.B. Kosten der Leistungserbringung) für den vernetzten Sicherheitssektor generiert werden können. Zudem muss die konsequente Weiterentwicklung des Sicherheitssektors gerade in Zeiten diffuser Sicherheitsrisiken gewährleistet werden. Das könnte beispielsweise mit einem Bewertungsansatz für den Sicherheitssektor (Security Sector Assessment) erreicht werden. Dieser sollte neben der Eigenbeurteilung auch die Fremdbewertung durch Dritte (wie z.B. beim NATO-Planning and Review Process) vorsehen und ein besonderes Augenmerk auf Schlüsselaspekte wie das vernetzte Management, die ressortspezifische und ressortgemeinsame Fähigkeitsorientierung sowie die Zusammenarbeitsfähigkeit legen.

Die skizzierten Veränderungen sind allerdings ohne Wandel der *Organisationskultur* nicht zu schaffen. Die Organisationskultur des vernetzten Sicherheitssektors basiert auf Vertrauen, Delegation, Eigeninitiative, Selbständigkeit und Eigenverantwortung. Um diese Ziele zu erreichen, sind Führungskräfte und Mitarbeitende gleichermaßen gefordert: Führungskräfte können ihren Veränderungswillen z.B. durch die Übernahme der Projektaufsicht in Reformvorhaben zur Stärkung der sicherheitspolitischen Vernetzung oder durch die Teilnahme an entsprechenden Aus- und Weiterbildungsveranstaltungen unter Beweis stellen. Das Engagement der Mitarbeitenden kann u.a. durch gemeinsame Führungslehrgänge oder durch die Personalrotation zwischen den Ministerien und den Sicherheitskräften sowie zwischen dem öffentlichen und dem privatwirtschaftlichen Sektor gefördert werden. Ebenso sollte die Laufbahnplanung gezielt ressortübergreifende Karrierewege anbieten, und im Hinblick auf die berufliche Beförderung sollten Einsätze in anderen Sicherheitsressorts als Qualifizierungskriterien eingesetzt werden.

Vernetzte Fähigkeiten

Die neuen Sicherheitsrisiken bewirken, dass die Aufgabenprofile der Sicherheitskräfte zusehends überlappen bzw. zusammenrücken. Das lenkt die Aufmerksamkeit auf sogenannte "vernetzte Fähigkeiten", die von allen Sicherheitskräften eingesetzt werden können und dadurch die Vernetzung zwischen diesen vereinfachen bzw. ermöglichen. Angesichts der gegenwärtigen

gen Interoperabilitätsprobleme zwischen den verschiedenen Kommunikations- und Führungssystemen der einzelnen Sicherheitskräfte ist der gesamte Führungsbereich (C4) erfolgskritisch für die Durchführung gemeinsamer Operationen. Ebenso wichtig sind die Nachrichtengewinnung, Überwachung und Aufklärung zur Erstellung eines gemeinsamen Lagebildes, die Verlegfähigkeit 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).

Die notwendigen konzeptionellen Schritte zur Definition und zur Bereitstellung der vernetzten Fähigkeiten können im Rahmen des angeregten Security Sector Assessment, durch Konzeptentwicklung sowie durch experimentelle Überprüfung eingeleitet werden. Wichtig ist dabei insbesondere, dass ein Vernetzungsorgan (z.B. BSR) die Schwerpunkte festlegt und die strategische Steuerung koordiniert, während die jeweiligen Sicherheitskräfte für die Bewirtschaftung und das operative Management der Fähigkeiten verantwortlich zeichnen. Die angespannte Haushaltslage macht es zudem erforderlich, dass Ansätze wie die Rollenspezialisierung oder die Zusammenlegung von Ressourcen in diesem Zusammenhang konsequent angewendet werden. So könnte beispielsweise 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.

Schlussfolgerungen

Das Leitbild der vernetzten Sicherheitspolitik basiert auf der Einsicht, dass Sicherheitspolitik heute weder ausschliesslich national noch bloss ressortspezifisch betrieben werden kann. Weil internationale und ressortübergreifende Konzeption und Kooperation erforderlich sind, müssen 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 verbunden werden. Diese Transformation muss national und international aktiv gestaltet werden.

Auf der nationalen Ebene geht es vor allem um die Stärkung der sicherheitspolitischen Vernetzungsorgane sowie der ressortübergreifenden Koordinationsprozesse. Sicherheitspolitische Basisaufgaben wie Lageanalyse, Strategiebestimmung und Fähigkeitsdefinition müssen unter Einbezug aller Akteure des Sicherheitssektors integriert erfolgen. Ressortspezifische Zielsetzungen und Programme sind konsequent aus dieser übergeordneten Sichtweise abzuleiten. Die inhaltliche Harmonisierung gelingt nur, wenn das Management des vernetzten Sicherheitssektors gestärkt wird. Hier geht es darum, die 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 Reformbemühungen müssen auf der internationalen Ebene konsequent fortgesetzt werden. Dabei wird die EU eine Schlüsselrolle spielen, weil sie verschiedene Politikfelder miteinander kombinieren kann. Erste Anzeichen wie die integrale Behandlung der zivilen und der militärischen Komponenten der EU-Sicherheitspolitik im Aussenministerrat oder die ge-

meinsame Planung und Führung ziviler und militärischer Einsätze durch die neue operative EU-Planungszelle sind ermutigend, reichen aber noch nicht aus. Die Europäische Sicherheitsstrategie muss die Logik der vernetzten Sicherheitspolitik übernehmen 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. Die EU sollte daher die Idee des Security Sector Assessment zur Beurteilung der sicherheitspolitischen Vernetzungsfähigkeit der alten und neuen Mitglieder anwenden. Kooperiert sie in dieser Frage eng mit anderen Organisationen wie NATO, OSZE und Europarat, dann besteht die Möglichkeit, dass die internationalen Programme zum Wiederaufbau, zur Reform und zur Weiterentwicklung der Sicherheitssektoren besser aufeinander abgestimmt und damit die strukturelle Konfliktprävention wesentlich gestärkt werden können.

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).