

IV. Instrumente internationaler Sicherheit

3. Überblick/Diskussion

Thema
Vernetzte Sicherheitspolitik

Editorial

von Cornelia Frank

Brauchen neue Sicherheitsbedrohungen eine neue Sicherheitspolitik? Hat Europa eine tragfähige Antwort auf die neuen sicherheitspolitischen Herausforderungen gefunden und welche Ansatzpunkte liefert dafür die Europäische Sicherheits- und Verteidigungspolitik (ESVP)? Die außen, sicherheits- und verteidigungspolitische Dimension der Europäischen Union als gescheitertes Projekt der europäischen Integration darzustellen, ist in Politik, Publizistik und Wissenschaft seit jeher en vogue gewesen. Insbesondere im Zuge des Irak-Debakels ertönten allerlei Nachrufe auf die Gemeinsame Außen- und Sicherheitspolitik (GASP) der Europäischen Union. Mit dem Verweis auf die Uneinigkeit europäischer Regierungen erklärten Unkenrufe die GASP und damit auch die ESVP für tot. Indes ignorieren derlei Schwarzmalereien die schon längst erprobte Praxis und erreichte Qualität der EU als sicherheitspolitischer Akteur. Deutliche Fortschritte sind der EU beim institutionellen Ausbau von GASP und ESVP zu bescheinigen. Auf der politisch-strategischen Ebene sind dies das Politische und Sicherheitspolitische Komitee (PSK), der EU-Militärausschuss (EUMC), der Ausschuss für zivile Aspekte des Krisenmanagements (CIVCOM) sowie der EU-Militärstab (EUMS). Auf der militärisch-strategischen Ebene sind das Operations-Hauptquartier zu nennen, auf der operativen Ebene das Force Headquarters (FHQ) sowie auf der taktischen Ebene die Hauptquartiere der Teilstreitkräfte. Darüber hinaus hat die „Zivilmacht mit Zähnen“ ihr breites Handlungsspektrum in EU-geführten Missionen, wie etwa in Bosnien-Herzegowina, Mazedonien oder im Kongo, mehrfach unter Beweis gestellt. Ein beachtliches Entwick-

lungspotenzial birgt die ESVP nicht zuletzt aufgrund ihrer Mehrdimensionalität. Gemäß Titel V des EU-Vertrags ist die ESVP ein Rechtsinstitut. Zugleich ist sie eine Fähigkeitsinitiative des Europäischen Rats (European Headline Goal), im Sinne der Kommission eine Komponente der EU-Friedenspolitik sowie nach Artikel 17 des EU-Vertrags eine gemeinsame Verteidigungspolitik, die sich auf gemeinsame Organe und Kapazitäten stützt, wie etwa die zivil-militärische Kooperation (CIMIC). Darüber hinaus ermöglicht die ESVP gemäß der Evolutivklausel eine gemeinsame Verteidigung, als deren Kerne die Planungszelle, die Rüstungsagentur oder die battle groups betrachtet werden können. Weitere Dimensionen bilden das nationale und multinationale Handeln der Mitgliedstaaten als Akteure der zweiten Säule sowie die Europäische Sicherheitsstrategie (ESS). Mit der ESS eröffnet sich eine neue Entwicklungsperspektive für die ESVP, der fortan drei Funktionen zugeordnet sind: Neben dem Auf- und Ausbau adäquater sicherheitspolitischer Fähigkeiten, mit denen die neuen Sicherheitsbedrohungen bewältigt werden können, trägt die ESVP mit zivilen und militärischen Operationen zur Stabilisierung von Krisenregionen bei. Schließlich leitet sie die Transformation von einer segmentierten zur vernetzten Sicherheitspolitik ein. Was ist unter vernetzter Sicherheitspolitik zu verstehen? Hat Europa damit eine adäquate Antwort auf die neuen sicherheitspolitischen Herausforderungen gefunden? Inwiefern hält das Plädoyer für eine sicherheitspolitische Vernetzung dem Härtesten in der Praxis stand? Rede und Antwort steht Heiko Borchert.

Heiko Borchert

Vernetzte Sicherheitspolitik

Eine Antwort Europas auf die neuen sicherheitspolitischen Herausforderungen

Einführung

Die Bekämpfung sicherheitspolitischer Risiken wie der internationale Terrorismus, die Verbreitung von Massenvernichtungswaffen, die Organisierte Kriminalität, das Scheitern von Staaten, die Bewältigung regionaler Konflikte oder die Verwundbarkeit, die aus der wirtschaftlichen und technischen Verflechtung der Industriestaaten resultiert, bedarf der Kombination verschiedener wirtschaftlicher, politischer und militärischer Instrumente. Darauf weist die im Dezember 2003 verabschiedete Europäische Sicherheitsstrategie (ESS) zu Recht hin und leitet daraus die Forderung nach mehr Kohärenz durch Bündelung der vorhandenen Instrumente und Fähigkeiten ab.¹⁾ Implizit formuliert die ESS damit die Kerngedanken der sicherheitspolitischen Vernetzung, nämlich die adäquate institutionelle Abbildung eines umfassenden Sicherheitsbegriffs durch bessere Verzahnung der zivilen und militärischen Mittel sowie die Reform der bestehenden Sicherheitsorganisationen im Licht der neuen Sicherheitsherausforderung.

Der vorliegende Beitrag stellt zuerst die Gründe für den Wechsel zur sicherheitspolitischen Vernetzung und deren Kernprinzipien vor, illustriert diese anschließend anhand konkreter Beispiele aus der Praxis und zeigt zum Schluss auf, wo mit Blick auf die Realisierung der Vernetzung noch Handlungsbedarf besteht. Sicherheitspolitische Vernetzung stellt tatsächlich einen tragfähiger Ansatz zum Umgang mit den neuen Sicherheitsherausforderungen dar. Wie in anderen Bereichen ist der damit verbundene Wandel vom politischen Willen zur Veränderung abhängig, der damit maßgeblich über Erfolg oder Scheitern der sicherheitspolitischen Vernetzung als Leitidee für die Gestaltung der Sicherheitspolitik im 21. Jahrhundert entscheiden wird.

Kernprinzipien

Vernetzung erhöht die Kohärenz und steigert die Einsatzfähigkeit

Im Zentrum der Forderung nach sicherheitspolitischer Vernetzung stehen die Organisation und das Management des Sicherheitssektors. Dazu zählen militärische, polizeiliche und paramilitärische Streitkräfte, Grenzschutz, Nachrichtendienste, die entsprechenden Ministerien, die politischen Aufsichts- und Koordinierungsorgane sowie in zunehmendem Maße auch nichtstaatliche Akteure wie beispielweise die Industrie oder Nichtregierungsorganisationen. Sicherheitspolitische Vernetzung beschäftigt sich mit der Frage, wie ein umfassender Sicherheitsbegriff, der aufgrund seines Querschnittscharakters in die Zuständigkeit verschiedener staatlicher und nichtstaatlicher Akteure fällt, im Alltag umgesetzt werden kann. Dabei ist zwischen einer inhaltlichen und einer organisatorischen Komponente zu unterscheiden. Inhaltlich geht es mit der bereits zitierten Feststellung der ESS um die ausgewogene Balance zwischen den unterschiedlichen staatlichen und nichtstaatlichen Machtmitteln im Einklang mit den definierten politischen Ambitionen eines Landes. Organisatorisch richtet sich der Blick auf die bestehenden Strukturen, Prozesse und Instrumente zur Definition, Umsetzung und Weiterentwicklung der Sicherheitspolitik, die vor dem Hintergrund grundsätzlich veränderter Sicherheitsrisiken zu überprüfen und anzupassen sind. Die Kombination beider Aspekte trägt dazu bei, Ziele, Mittel und Verfahren der Sicherheitspolitik miteinander in Einklang zu bringen und bildet damit die Voraussetzung für risikoadäquate Sicherheitsstrategien.

Querschnittscharakter

Die Notwendigkeit der stärkeren Vernetzung ist auf eine Reihe unterschiedlicher Entwicklungen zurückzuführen:²⁾

- Erstens sprengen die im 21. Jahrhundert zu bewältigenden Herausforderungen die Problemlösungskapazitäten des Nationalstaates. Schon

Foto: picture alliance/dpa



PRT

Der in Afghanistan gewählte Ansatz der integrierten zivil-militärischen Wiederaufbauteams (Provincial Reconstruction Teams, PRT) soll die zivilen und militärischen Fähigkeiten im Bereich des Friedensaufbaus miteinander verzahnen. In Kundus und Feizabad betreibt die Bundeswehr solche PRTs, die mit dem hier im Sicherungseinsatz am Flugplatz abgebildeten Transportfahrzeug Dingo ausgerüstet ist.

seit einiger Zeit wird daher über Alternativen zu hoheitlichen Regelungs- und Steuerungsmechanismen nachgedacht. Hoch im Kurs stehen dabei partnerschaftlich ausgehandelte Lösungen, die auch nichtstaatliche Akteure einbeziehen und damit auf dieser Ebene zu einer Vernetzung der Akteure beitragen. Diese Diskussion wird,

- zweitens, begleitet durch die Bemühungen zur Modernisierung des Verwaltungshandelns, die sich unter anderem aus den Leistungsdefiziten der klassischen Bürokratie sowie der desolaten Haushaltslage der meisten Industrieländer erklären. Im Anschluss an die Übertragung von Managementgrundsätzen und -verfahren aus der Privatwirtschaft auf die öffentliche Verwaltung findet in zunehmendem Maße auch eine Verlagerung öffentlicher Aufgaben an private Leistungsträger statt. Daraus entsteht eine neue „vernetzte Verwaltung“, die sich dadurch auszeichnet, dass die Wirtschaft immer stärker in die öffentlichen Leistungserstellungsprozesse eingebunden wird.³⁾
- Drittens lösen die neuen sicherheitspolitischen Risiken bestehende Grundhypothesen der Sicherheitspolitik wie die Unterscheidung zwischen innerer und äußerer Sicherheit oder die

klare Abgrenzung zwischen militärischen und nicht-militärischen Aktionen zusehends auf. Damit wird aber nicht nur die auf diesen Annahmen basierende Kompetenzverteilung zwischen verschiedenen Ressorts und Sicherheitskräften infrage gestellt. Die neuen Aufgaben, die aus der Bewältigung dieser Risiken resultieren, sind in den bestehenden Strukturen nicht oder nur unzureichend abgebildet, was die Erarbeitung und Umsetzung koordinierter Strategien erschwert. Fördern diese drei Trends die Notwendigkeit der Vernetzung, so gibt es,

Grundhypothesen

- viertens, mit dem Fortschritt im Bereich der Informations- und Kommunikationstechnologie (IKT)

- 1) Ein sicheres Europa für eine bessere Welt. Europäische Sicherheitsstrategie, Brüssel, 12. Dezember 2003, S. 7, 13.
- 2) Heiko Borchert, „Vernetzte Sicherheitspolitik und die Transformation des Sicherheitssektors: Weshalb neue Sicherheitsrisiken ein verändertes Sicherheitsmanagement erfordern“, in ders. (Hrsg.), Vernetzte Sicherheit: Leitidee der Sicherheitspolitik im 21. Jahrhundert, Hamburg 2004, S. 53-79; Ashton B. Carter, „The Architecture of Government in the Face of Terrorism“, International Security 3/2001/02, S. 5-23.
- 3) Stephen Goldsmith and William D. Eggers, Governing by Network. The New Shape of the Public Sector, Washington, DC 2004.

eine Entwicklung, die konkrete Lösungsansätze zur physischen Vernetzung der sicherheitsrelevanten Akteure ermöglicht. Konsequent genutzt und unter Berücksichtigung wichtiger Faktoren wie der Befähigung der Mitarbeitenden zum Umgang mit der IKT und der Entwicklung der Organisationskultur können dadurch Arbeitsabläufe drastisch beschleunigt sowie physische und zeitliche Grenzen leichter überbrückt werden.

Eine wesentliche Erkenntnis aus der Auseinandersetzung mit den neuen Sicherheitsrisiken besteht darin, dass adäquate Sicherheitsstrukturen künftig deutlich flexibler sein müssen, um auf Veränderungen im

Transformation

relevanten Risikoumfeld reagieren zu können. Aus diesem Grund wird die sicherheitspolitische

Vernetzung über einen ergebnisoffenen Transformationsprozess realisiert. Dieser kann als „gesamtstrategisch und ressortübergreifend angelegter, multinational ausgerichteter, fortlaufender und vorausschauender Weiterentwicklungsprozess der außen- und sicherheitspolitischen Instrumente und der Entscheidungsfindung eines Staates an die sich verändernden Umfeldbedingungen“ verstanden werden.⁴⁾ Zwei Zielsetzungen stehen im Zentrum:

Es geht darum, die Kohärenz des politischen Handelns zu verbessern. Hierzu ist es erforderlich, dass die sicherheitsrelevanten Akteure ihre Ziele, Prozesse und Strukturen sowie ihre Fähigkeiten und Mittel systematisch aufeinander abstimmen. Vernetzung bezieht sich dabei auf die Berücksichtigung der relevanten Ebenen, auf denen Entscheidungen beschlossen und umgesetzt werden (beispielsweise supranational, national und sub-national), die einzubeziehenden staatlichen und nichtstaatlichen Akteure, die systematische Abstimmung der zu erbringenden Aufgaben auf ein sicherheitspolitisches Leistungskontinuum bestehend aus Krisenprävention, -management und -nachsorge sowie auf die zur Auswahl stehenden Instrumente (zum Beispiel diplomatische, wirtschaftliche, militärische, polizeiliche und zivilgesellschaftliche Mittel).

Mit Blick auf die zu lösenden Aufgaben soll die Einsatzfähigkeit der zur Verfügung stehenden Mittel signifikant gesteigert werden. Hierzu dient ein umfassender Informations- und Kommunikationsverbund für Aufklärung, Führung und Wirkung. Die konsequente Vernetzung von Akteuren, Sensoren und Effektoren ermöglicht beschleunigte Entscheidungs- und Handlungsabläufe und erlaubt es, die definierten Aufträge effizienter und effektiver zu erfüllen.⁵⁾

Die Verbesserung der Kohärenz und die Steigerung der Einsatzfähigkeit setzen die konsequente Wirk-

Fähigkeits- und Wirkungsorientierung

und Fähigkeitensorientierung der beteiligten Akteure voraus, damit deren Mittel in

der Vorbereitung oder im Einsatz jederzeit an die

aktuelle Lage angepasst und mit Blick auf die erzielten Ergebnisse verglichen und weiterentwickelt werden können. Die gemeinsame Führung bedingt ein gemeinsames Lagebewusstsein, das über ein Lagebild hergestellt wird. Das Lagebild ist als Informationsraum zu verstehen, der Ebenen übergreifend angelegt ist und mit Blick auf die zu erfüllenden Aufgaben relevante Informationen aus einer Fülle unterschiedlicher Quellen zur Verfügung stellt. Das gemeinsame Lagebild berücksichtigt neben den verschiedenen Akteuren und ihren Fähigkeiten oder Kapazitäten auch die unterschiedlichen Entscheidungs- und Handlungsebenen. Neben der operationsbezogenen Führung der Kräfte stärkt das Lagebild die Beurteilungsfähigkeit der Akteure und legt dadurch die Basis für die geforderten Effizienz- und Effektivitätsgewinne.⁶⁾

Vernetzung in der Praxis

Die Umsetzung der geforderten sicherheitspolitischen Vernetzung ist sehr anspruchsvoll. Die technischen Fragen zur Realisierung der Vernetzung sind dabei – bei aller Komplexität – in der Regel noch das geringste Problem. Noch herausfordernder ist die Restrukturierung der bestehenden Abläufe und Strukturen des

Sicherheitssektors, denn sicherheitspolitische Vernetzung stellt bestehende Gewohnheiten und Machtpositionen einzelner Akteure infrage. Es kann daher nicht deutlich genug betont werden, dass der Übergang von der ressortspezifischen zur vernetzten Organisation des Sicherheitssektors einen Willensakt darstellt, der ohne die Bereitschaft zur Veränderung nicht zu schaffen ist.

Willensakt

Diese Feststellung wird besonders deutlich, wenn man auf die unterschiedlichen Dimensionen blickt: Vernetzung auf der strategischen Ebene bezweckt vor allem die Verbesserung der ressortübergreifenden Zusammenarbeit zur Stärkung der Politikvorbereitung. Auf der operativen Ebene dient die Vernetzung der besseren Verzahnung ziviler und militärischer Mittel und fördert damit die Effektivität bei der Erreichung komplexer Ziele wie beispielsweise dem Friedensaufbau. Auf beiden Ebenen ist Vernetzung wesentlich davon abhängig, dass wichtige Funktionsbereiche wie Personal, Finanzen und Wissen sowie Aufbau- und Ablaufstrukturen, die die formalen Elemente beschreiben und die in jeder Institution zur Zielerreichung definiert werden müssen, stärker ins Blickfeld der Betrachtung rücken.

Der Africa Pool und der Global Conflict Prevention Pool der britischen Entwicklungshilfe-, Außen- und Verteidigungsministerien sind Beispiele, die verschiedene Aspekte der Vernetzung in einem Ansatz kombinieren. Das Ziel besteht in der integrierten Entwicklung politischer Strategien zum Umgang mit Konflikten. Die Vernetzung zwischen den drei Ressorts erfolgt in diesem Fall über gemeinsam

definierte Zielsetzungen, die darauf abgestimmte Formulierung der Strategien, die Bündelung (Pooling) finanzieller Ressourcen aus den Ministerien in einem gemeinsamen Topf sowie die gemeinsame Projektumsetzung inklusive Leistungsmessung und -beurteilung. Arbeitsausschüsse mit Vertretern aus allen Ressorts erlauben die integrale Betrachtung militärischer, entwicklungspolitischer, außenpolitischer, ökonomischer und polizeilicher Perspektiven.⁷⁾ Dieser Ansatz stand auch Pate beim Aktionsplan „Zivile Krisenprävention, Konfliktlösung und Friedenskonsolidierung“ des Auswärtigen Amtes, der Krisenprävention als Querschnittsaufgabe betrachtet und neue Ansätze zur ressortübergreifenden Koordinierung einführt.⁸⁾

Das Ziel, die zivilen und militärischen Fähigkeiten im Bereich des Friedensaufbaus besser miteinander zu verzahnen, verfolgt auch der in Afghanistan gewählte Ansatz der integrierten zivil-militärischen Wiederaufbauteams (Provincial Reconstruction Teams, PRT). Die Einordnung und der Stellenwert der zivilen Komponente variieren jedoch: Während diese im US-amerikanischen Fall dem militärischen Oberbefehlshaber untergeordnet ist, sind

Pooling

bei den deutschen PRTs beide Elemente gleichberechtigt. Die zivile Komponente ist als Teil der Außenstelle in Kabul organisiert, der militärische Teil ist in die NATO-Befehlsherkette integriert.⁹⁾ Für die Weiterentwicklung dieses Ansatzes wird es entscheidend sein, wie die Rückkoppelung zwischen der Vernetzung im Einsatz und der Führung auf der Stufe der Ministerien organisiert wird – ein Aspekt, der in Deutschland bislang erst ansatzweise geregelt ist.

Auch auf der europäischen Ebene sind erste Anzeichen der sicherheitspolitischen Vernetzung zu erkennen. Neben den bereits erwähnten strategischen Vorgaben aus der ESS ist insbesondere auf die Einrichtung der zivil-militärischen Planungszelle im Europäischen Militärstab hinzuweisen. Sie soll die Kapazitäten der EU zur Führung autonomer Einsätze verstärken und dabei insbesondere zur verbesserten Kohärenz zwischen den zivilen und militärischen Strukturen unter der Führung von Javier Solana beitragen.¹⁰⁾ Dieser Ansatz ist wegweisend, doch offene Fragen könnten dessen Effektivität behindern. Insbesondere erweist es sich im Brüsseler Alltag als Problem, dass diese Zelle im Militärstab und nicht auf einer übergeordneten Ebene angesiedelt ist. Zudem fehlen auf der nationalen Ebene bislang adäquate „Spiegelreferate“, die die Verzahnung ziviler und militärischer Einheiten in der nationalen Vorbereitung verbessern könnten.

Einen vergleichbaren Beitrag zur Zusammenführung militärischer und ziviler Belange leistet auch das neue EU-Sicherheitsforschungsprogramm mit seinen Vorbereitungsmaßnahmen. Um die Bereitstellung der benötigten sicherheitsrelevanten Fähigkeiten voranzubringen, will die EU die

Sicherheitsforschung fördern. Im Vordergrund stehen dabei Dual Use-Technologien, die gleichzeitig militärische und sicherheitsrelevante Anwendungen unterstützen.¹¹⁾ Die Innovationskraft dieser Maßnahmen ist seitens der EU davon abhängig, dass die Arbeiten der Europäischen Kommission und der Europäischen Verteidigungsagentur (EVA) ebenso optimal aufeinander abgestimmt werden wie die sicherheitsrelevanten Tätigkeiten der verschiedenen Generaldirektorien der Kommission.¹²⁾ Auf der nationalen Ebene müssen darüber hinaus die entsprechenden Vorbereitungen für die Sicherheitsforschung koordiniert werden, das heißt hierfür relevante Wissenschafts- und Technologiebereiche müssen identifiziert, gewichtet und im Rahmen einer mit Industrie und Wissenschaft erarbeiteten Strategie weiterentwickelt werden.

Als drittes europäisches Vernetzungsbeispiel kann schließlich die im EU-Verfassungsvertrag vorgesehene Solidaritätsklausel genannt werden. Diese sieht die gegenseitige Unterstützung der EU-Mitglieder im Falle einer natur- oder zivilisationsbedingten Katastrophe sowie eines terroristischen Anschlags auf dem EU-Territorium vor. Hierzu sollen alle der EU zur Verfügung stehenden zivilen und militärischen Mittel eingesetzt werden. Damit schlägt die Solidaritätsklausel die Brücke von der bislang auf den Außenbereich konzentrierten Europäischen Sicherheits- und Verteidigungspolitik zur „Innensicherheit“ der Unionsmitglieder. In der Praxis wird dieser konzeptionelle Brückenschlag neben den Problemen mit der Ratifizierung des EU-Verfassungsentwurfs durch den Umstand erschwert, dass das Haager Programm zur Stärkung

Solidaritätsklausel

- 4) Ralph Thiele, „Intervention und die Sicherheit zu Hause in Deutschland: Transformation der Sicherheitspolitik unter neuen Vorzeichen“, in Heiko Borchert (Hrsg.), Weniger Souveränität - Mehr Sicherheit. Schutz der Heimat im Informationszeitalter und die Rolle der Streitkräfte, Hamburg 2004, S. 97.
- 5) Konzeption der Bundeswehr, Berlin 2004, S. 11.
- 6) Ralph Thiele, „Transformation, vernetzte Operationsführung und die Rolle des Weltraums“, in Heiko Borchert (Hrsg.), Europas Zukunft zwischen Himmel und Erde. Weltraumpolitik für Sicherheit, Stabilität und Prosperität, Baden-Baden 2005, S. 83-98.
- 7) The Global Conflict Prevention Pool. A joint UK Government approach to reducing conflict, London 2003.
- 8) Norbert Eitelhuber, „Aktionsplan „Zivile Krisenprävention“, Europäische Sicherheit 6/2005, S. 61-63.
- 9) Michael Schmunk, „Neu im Werkzeugkasten der Nation-Builders: Berlins zivil-militärische Wiederaufbauteams am Hindukusch. Entstehung, Konzept und Erfolgchancen deutscher Provincial Reconstruction Teams“, in Claudia Gomm und Annett Günther (Hrsg.), Unterwegs in die Zukunft. Afghanistan - drei Jahre nach dem Aufbruch vom Petersberg, Berlin 2005, S. 329-361.
- 10) European Defence NATO/EU Consultation, Planning and Operations, 13990/04 EXT 1, Brussels, 28 January 2005.
- 11) Research for a Secure Europe. Report of the Group of Personalities in the field of security research. Luxembourg 2004.
- 12) Insbesondere Unternehmen und Industrie, Verkehr und Energie, Justiz, Freiheit und Sicherheit, Informationsgesellschaft und Medien sowie Außenbeziehungen.

von Freiheit, Sicherheit und Gerechtigkeit in der EU keine Bezüge zur zweiten Säule aufweist – damit ist der Anspruch der ESS, einen alle Säulen der EU umfassenden Sicherheitsansatz zu konzipieren, bislang nicht erfüllt.¹³⁾

Künftiger Handlungsbedarf

Sicherheitspolitische Vernetzung ist der richtige Ansatz, um die Forderung nach einem umfassenden

Sicherheitsbegriff institutionell abzubilden. Aus methodischer Sicht weisen die in zahlreichen Streitkräften des euro-atlantischen Raums eingeleiteten Transformationsprozesse, die im Kern alle auf der Befähigung zur vernetzten Operationsführung sowie den Prinzipien der Wirkungs- und Fähigkeitsorientierung basieren, hierfür den Weg. Künftig geht es darum, die dabei gesammelten Erfahrungen konsequent auf alle Akteure des Sicherheitssektors zu übertragen. Dabei sind zahlreiche Herausforderungen zu bewältigen, die im Sinne einer Auswahl abschließend skizziert werden sollen.¹⁴⁾

Vernetzung zwischen den Streitkräften

Die Grundsätze der vernetzten Operationsführung sind definiert, werden in Demonstratorenprogrammen erprobt und im Einsatz angewendet. Für die Zukunft liegt eine erste militärische Herausforderung in der konsequenten Berücksichtigung der Anforderung der vernetzten Operationsführung in allen Bereichen der Doktrin, Struktur, Ausbildung, Ausrüstung, Führung, Personal und Infrastruktur. Die durchgängige Abstimmung dieser Bereiche auf die Prinzipien der Vernetzung und der Transformation stellt neue Anforderungen an die Kohärenz bei Planung und Umsetzung und erhöht die Bedeutung der „weichen Faktoren“ in den Bereichen Doktrin, Ausbildung, Führung und Personal um Vernetzung im Alltag und in der Organisationskultur zu verankern. Eng damit verbunden ist, zweitens, die Gewährleistung der Interoperabilität zwischen den eigenen

Teilstreitkräften und den Streitkräften befreundeter Nationen. Obwohl es inzwischen insbesondere seitens der Industrie große Anstrengungen zur Definition offener und einheitlicher Standards für die vernetzte Operationsführung gibt, bleiben wichtige Fragen noch offen. Dazu zählt zum Beispiel auf der Hardwareseite die Sicherstellung der reibungslosen Integration alter Systeme in neue, konsequent auf die Anforderungen der vernetzten Operationsführung ausgerichtete Systemarchitekturen. Diese schon im nationalen Umfeld herausfordernde Aufgabe, wird durch die Erfordernisse der multinationalen und ressortübergreifenden Zusammenarbeit zusätzlich erschwert. Daneben ist zu

berücksichtigen, dass insbesondere die bestehenden US-Exportbestimmungen (International Trade in Arms Regulation) den Austausch des technologischen Know-Hows erschweren, wodurch multinationale Unternehmen teilweise daran gehindert werden, konzernintern vorhandene technologische Synergien zu Gunsten ihrer Kunden optimal zu nutzen. Vor diesem Hintergrund erweisen sich beispielsweise auch Fortschritte im Bereich der sicheren Datenübertragung (Kryptologie) als potenziell zweischneidiges Schwert, weil die Nichtweitergabe der entsprechenden Sicherheitsbestimmungen den positiven Effekt der Datensicherheit konterkarieren und dadurch die Zusammenarbeit erschweren kann.¹⁵⁾ Und schließlich ist zu beachten, dass der Trend zum Einsatz von Rüstungsmaterial ab Stange (Commercial of the Shelf, COTS) noch ungeklärte Konsequenzen für die Interoperabilität mit sich bringt, die unter anderem aus den schnelllebigem, zivilen Innovationszyklen oder der teilweise eingeschränkten Rückwärtskompatibilität zu alten Systemen resultieren.

Vernetzung zwischen Streitkräften und zivilen Sicherheitskräften

Angesichts der neuen Aufgaben im In- und Ausland kommt der reibungslosen Zusammenarbeit zwischen diesen beiden Akteursgruppen eine Schlüsselrolle zu. Um diese zu gewährleisten, ist es unerlässlich, eine gemeinsame Fähigkeitsanalyse und -planung vorzunehmen. Nur auf der Grundlage eines umfassenden Bilds der vorhandenen Stärken und Schwächen lassen sich Prioritäten für die künftige Fähigkeitsentwicklung sowie für den Einsatz der vorhandenen Fähigkeiten der Streitkräfte zu Gunsten der Sicherheitskräfte und umgekehrt vornehmen. Wichtig ist dabei insbesondere, dass diese Schritte in einem gemeinsamen Simulationsumfeld durchgeführt werden, damit Fähigkeiten in Abstimmung auf unterschiedliche Aufgaben und die daraus resultierenden Anforderungen identifiziert und entwickelt werden können.

Es müssen die Grundlagen dafür geschaffen werden, Streitkräfte und zivile Sicherheitskräfte im Einsatz gemeinsam führen zu können. Damit ist neben interoperablen Informations- und Kommunikationsstrukturen auch die Einbindung in ein gemeinsames Lagebild angesprochen. Hierzu müssen technische Schnittstellen bereinigt und verfahrensbezogene Unterschiede in den Einsatzgrundsätzen der Streit- und Sicherheitskräfte durch konzeptionelle Anpassung harmonisiert sowie durch gemeinsame Übungen im Vorfeld der Einsätze trainiert werden. Daher sind die Bemühungen der USA, bis 2009 ein Simulationsumfeld für das Training gemeinsamer, multinationaler, ressortübergreifender Operationen (Joint National Training Capability) zu schaffen, für die europäischen Partner von größtem Interesse.¹⁶⁾

Interoperabilität

Simulationsumfeld

Schließlich müssen methodische Ansätze entwickelt werden, um den Transformationsfortschritt innerhalb des gesamten Sicherheitssektors beurteilen zu können. Nur so ist es möglich, Stärken und Schwächen des bereits Geleisteten zu identifizieren und Schwerpunkte für die Zukunft zu setzen. Die EU und die NATO, in Teilbereichen auch die OSZE und der Europarat, könnten hierbei wesentliche Impulse für die Definition eines einheitlichen und gemeinsamen Beurteilungsrahmens schaffen.

Letztlich sind in einigen Staaten auch noch offene Rechtsfragen beispielsweise beim Einsatz der Streitkräfte im Innern zum Zweck der nationalen Sicherheitsvorsorge (Homeland Security in den USA) oder bei Auslandeinsätzen im Rahmen der EU-Solidaritätsklausel zu klären.

Vernetzung mit der Industrie

Die Vernetzung mit der Industrie ist entscheidend, um Technologiefortschritte der Industrie möglichst schnell in operationsbezogene Effizienzgewinne der Streit- und Sicherheitskräfte umzuwandeln. Das bedingt eine Anpassung der staatlichen Beschaffungsvorschriften und -verfahren. Die konsequent fähigkeitsorientierte Akquisition anstelle der bisherigen Ausrichtung an Plattformen stellt konzeptionell die größte Herausforderung dar. Zudem müssen bestehende Vorschriften und transformationsrelevante Neuerungen wie zum Beispiel die Betonung der Konzeptentwicklung und Erprobung (CDE) besser aufeinander abgestimmt werden, so dass der Industrie aus der frühen Beteiligung in der CDE-Phase keine Nachteile in der späteren Beschaffung erwachsen. Gleichzeitig sollten tragfähige finanzielle Lösungen gefunden werden, um die Entwicklungsrisiken der Industrie ausgewogener als bislang zu finanzieren.

Einher damit geht auch die Schaffung von Voraussetzungen, damit innovative Finanzierungsansätze,

Industriepolitische Konsequenzen

die es der öffentlichen Hand erlauben, sicherheitsrelevante Leistungen über Betreibermodelle einzukaufen, ohne dafür selbst die teuren Systeme und Geräte beschaffen und unterhalten zu müssen, nicht durch bestehende haushaltrechtliche Schranken behindert werden. In diesen Fragen könnte die EVA zusammen mit der Europäischen Kommission eine Schlüsselrolle bei der Harmonisierung vorhandener Bestimmungen spielen.

Die industriepolitischen Konsequenzen aus dem Übergang zum Modell des Systemintegrators sind vor allem mit Blick auf den Mittelstand zu untersuchen. Systemintegratoren definieren im Auftrag des Bedarfsträgers ein zu beschaffendes Gesamtsystem und leiten daraus die Spezifikationen der einzelnen Komponenten ab. Indem sie auch über Unterauftragnehmer entscheiden, üben die Systemintegratoren eine industriepolitische Funktion aus, die tendenziell eher die finanzstarken Unternehmen in dieser Rolle bevorzugt.¹⁷⁾

Diese und weitere Fragen sollten in Form eines strategischen Wissenschafts- und Technologiedialogs mit Wirtschaft und Wissenschaft behandelt werden. Ein solcher Dialog würde es ermöglichen, systematisch jene industriellen und wissenschaftlichen Schlüsselkompetenzen zu identifizieren, die besonders gefördert sowie von der Industrie über eigene Partner- und Allianznetze in internationale Kooperationsbeziehungen eingebracht werden sollen.

Vernetzung zwischen verschiedenen Ressorts

Im Bereich der ressortübergreifenden Zusammenarbeit liegt der größte Nutzen der sicherheitspolitischen Vernetzung, gleichzeitig sind auf dieser Ebene auch die größten Herausforderungen zu bewältigen. Diese ergeben sich aus dem Umstand, dass die Ansätze der Fähigkeits- und Wirkungsorientierung bislang weitgehend auf den Bereich der Streitkräfte beschränkt sind. Die Übertragung auf die zivilen Ressorts ist jedoch unbedingt erforderlich, um den von der ESS angesprochenen Policy Mix zwischen zivilen und militärischen Fähigkeiten herstellen zu können und die Grundlagen für den Vergleich der mit dem Einsatz dieser Fähigkeiten erzielbaren Wirkungen zu schaffen.

Aus dem Einsatz eines gemeinsamen, rollenbasierten und Ebenen übergreifenden Lagebilds als gesamtstaatliches Führungsinstrument ergeben sich neue Fragen, die konzeptionell noch weitgehend unbeantwortet sind: Bei welcher Institution soll ein solches Lagebild eingerichtet werden? Welche Informationen werden darin abgebildet? Wie werden die einzelnen Ressorts in das Lagebild eingebunden und welche Informationen müssen dazu in welcher Form bereitgestellt werden? Wie werden nichtstaatliche Akteure, die Zivilgesellschaft und die Industrie in das Lagebild eingebunden?

Eng mit dem Lagebild verknüpft, ist die Notwendigkeit einer Überprüfung der nachrichtendienstli-

Policy Mix

13) Siehe vor allem den fehlenden Bezug zu militärischen Fähigkeiten beim grenzüberschreitenden Krisenmanagement: The Hague Programme: strengthening freedom, security and justice in the European Union, 16054/04, Brussels, 13 December 2004, Kp. 2.4.

14) Ich danke Michael Krüger für wertvolle Hinweise zu den folgenden Ausführungen.

15) Stuart H. Starr, „The Challenges Associated with Achieving Interoperability in Support of Net-Centric Operations“, paper presented at the 10th ICCRTS Meeting, Washington, DC, June 2005, S. 9, 16.

16) Stuart (zit. in Fn 15), S. 14.

17) Burkhard Theile und Norbert Härle, „Streitkräftetransformation aus der Sicht der Rüstungsindustrie“, in Heiko Borchert (Hrsg.), Potentiale statt Arsenale. Sicherheitspolitische Vernetzung und die Rolle von Wirtschaft, Wissenschaft und Technologie, Hamburg 2004, S. 55-73.

chen Architektur. Hierbei geht es zum einen um die Verlagerung der Schwergewichte von der Sammlung zur Analyse der Informationen, wobei die besondere Herausforderung in der ressortübergreifenden Auswertung als Basis für die ressortgemeinsame Strategiedefinition liegt. Zum anderen wird es langfristig unerlässlich sein, vor dem Hintergrund der gesamtstaatlichen Bedürfnisse eine Strategie zur Auswertung offener Quellen (Open Source Intelligence) zu definieren, die Ziele, Mittel und Verfahren bestimmt und damit die effiziente Nutzung dieser Quellen auf der ressortübergreifenden und der ressortspezifischen Ebene ermöglicht.

Literatur

David S. Alberts, John J. Garstka, Frederick P. Stein, Network Centric Warfare. Developing and Leveraging Information Superiority, Washington, DC 1999.

Stephan Klingebiel und Katja Roehder, Entwicklungspolitisch-militärische Schnittstellen. Neue Herausforderungen in Krisen und Post-Konflikt-Situationen, Bonn 2004.

Reinhardt Rummel, Konfliktprävention: Etikett oder Markenzeichen europäischer Interventionspolitik?, Berlin 2003.

Edward A. Smith, Effects-Based Operations. Applying Network Centric Warfare in Peace, Crisis, and War, Washington, DC 2002

Zusammenfassung

Ein wesentliches Ziel vernetzter Sicherheitspolitik ist die integrierte Entwicklung politischer Strategien zum Umgang mit Konflikten. In der praktischen Sicherheitspolitik ist man hiervon noch ein Stück entfernt. Erste viel versprechende Beispiele sind dafür der Africa Pool und der Global Conflict Prevention Pool der britischen Regierung. Dieser Ansatz stand Pate beim Aktionsplan „Zivile Krisenprävention, Konfliktlösung und Friedenskonsolidierung“ des Auswärtigen Amtes. Militärische und zivile Fähigkeiten beim Aufbau in Afghanistan miteinander zu verbinden, ist mit der Aufstellung der Provinzial Reconstruction Teams (PRT) in der Provinz Kundus unter deutscher Führung gelungen. Sicherheitspolitische Vernetzung ist der richtige Ansatz, um die Forderung nach einem umfassenden Sicherheitsbegriff institutionell abzubilden.

moe

Zum Beitrag

Autor

Dr. Heiko Borchert, Jahrgang 1970, leitet ein Unternehmens- und Politikberatungsbüro in der Schweiz, ist Mitherausgeber der Schriftenreihe Vernetzte Sicherheit und Direktor für Sicherheit und Verteidigung am Düsseldorfer Institut für Aussen- und Sicherheitspolitik (DIAS) e.V.

Hinweise

www.vernetzte-sicherheit.net
Informationen und Zusatzmaterialien zur gleichnamigen Schriftenreihe

www.act.nato.int
NATO Allied Command Transformation

europa.eu.int/comm/environment/civil/index.htm
Europäische Kommission, Bereich Zivilschutz

europa.eu.int/comm/external_relations/cpcm/cp.htm
Europäische Kommission, Bereich Konfliktprävention

Impressum

Herausgeber
Streitkräfteamt, Informations- und Medienzentrale der Bundeswehr

Redaktion
Chefredakteur: Dieter Buchholtz (bu)
Verantwortlich: Rüdiger Michael M. A. (mi)
Dr. Michael Moerchel (moe)
E-Mail: mmoerchel@t-online.de
Telefon 02 28-2 42 21 00

Redaktionsbüro: Zentralredaktion SKA Abt. I / Medienzentrale
Pascalstraße, 10s, 53125 Bonn
Telefon 02 28-12 27 32; Bw-Kennziffer 3400
Telefax 02 28-12 27 49

E-Mail: info@reader-sipo.de
Internet: www.reader-sipo.de

Wissenschaftliche Beratung
Cornelia Frank, M.A. (cfr)
Institut für Politikwissenschaft
Universität Regensburg
E-Mail: cornelia.frank@politik.uni-regensburg.de

Druck
Druckerei Gerhards GmbH, Bonn
Gedruckt auf 100% Altpapier (chlorfrei gebleicht)

Hinweis
Namentlich gekennzeichnete Beiträge geben nicht unbedingt die Meinung des Herausgebers wieder. Für unverlangt eingesandte Manuskripte wird keine Gewähr übernommen. Texte und Illustrationen sind urheberrechtlich geschützt. Nachdrucke sind nur nach vorheriger schriftlicher Zustimmung durch die Redaktion und mit Quellenangabe erlaubt.

Redaktionsschluss: 25. September 2005.