Vernetzte Sicherheit 7

Heiko Borchert (Hrsg.)

Wettbewerbsfaktor Sicherheit

Staat und Wirtschaft im Grand Pas de Deux für Sicherheit und Prosperität

Nomos

Die Reihe „Vernetzte Sicherheit“
wird herausgegeben von

Ralph Thiele und Heiko Borchert

Band 7

Vernetzte Sicherheit 7

Heiko Borchert (Hrsg.)

Wettbewerbsfaktor Sicherheit

Staat und Wirtschaft im Grand Pas de Deux für Sicherheit und Prosperität

Nomos

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://www.d-nb.de abrufbar.

ISBN 978-3-8329-3778-2

Die Bände 1 - 3 der Schriftenreihe sind erschienen bei
Verlag E. S. Mittler & Sohn, Hamburg

1. Auflage 2008

Inhalt

Abbildungs- und Tabellenverzeichnis 7

Abkürzungsverzeichnis 8

Grand Pas de Deux für Sicherheit und Prosperität: Einführung 11
Heiko Borchert

Sicherheitspartnerschaft zwischen Staat und Wirtschaft: Anforderungen an die Sicherheitszusammenarbeit mit der Wirtschaft 27
Uwe Christian Fischer

Sicherheit als strategischer Erfolgsfaktor im globalen Wettbewerb 47
Thomas Menk

Wenn die Lichter ausgehen: Der Schutz kritischer Energieinfrastrukturen zwischen Monopol und Wettbewerb 59
Heiko Borchert und Karina Forster

Kein Anschluss unter dieser Nummer: Der Schutz kritischer Informations- und Kommunikationstechnologie 79
Stefan Brem und Ruedi Rytz

Außer Betrieb: Sicherheit der kritischen Transportinfrastruktur an den Beispielen Hafen und Flughafen 97
Johannes Prinz

Öffentlich-private Zusammenarbeit im österreichischen Sicherheitskonzept für die EURO 08 112
Günther Marek und Maximilian Prinz

Alles Gute kommt von oben: Die Förderung luftgestützter Innovation in einem Intellectual Property Cluster 124
Ralph Thiele

Prosperität finanziert Sicherheit: Der Einsatz analytischer Intelligenz im staatlichen Erkenntnisprozess 142
Jan-Erik Schmidt

Was wäre wenn? Der Beitrag der Modellbildung und Simulation zum Umgang mit modernen Sicherheitsherausforderungen 161
Andreas Lang und Olav Hansen

Die Autoren 176

Grand Pas de Deux für Sicherheit und Prosperität: Einführung

Heiko Borchert

In an interdependent world, the risks faced by any individual, firm, region or country depend not only on its own choices but also on those of others.[1]

For chief executives (...) it is time to invest more time and resources in furthering the public-private partnership. Helping legislators craft appropriate security standards will indeed be an integral part of your business strategy.[2]

Sicherheit und Prosperität sind traditionell zwei Seiten der gleichen Medaille. Beobachter weltgeschichtlicher Zusammenhänge wie Paul Kennedy leiten daher die sicherheitspolitische Entwicklung weitgehend aus den weltwirtschaftlichen Verhältnissen ab.[3] Im gegenwärtigen Sicherheitsumfeld ist diese Betrachtung nach wie vor gültig. Allerdings ist der einfache Analogieschluss, dass durch eine vorherrschende wirtschaftliche Stellung automatisch auch die Sicherheit einer Nation gewährleistet ist, heute aus einer Reihe von Gründen weniger denn je zulässig. Vielmehr sind es die Offenheit moderner Gesellschaften und ihrer Volkswirtschaften sowie die daraus resultierenden Abhängigkeiten und Wechselwirkungen zwischen unterschiedlichen politischen und wirtschaftlichen Handlungsfeldern, die genau analysiert werden müssen und eine bessere Abstimmung zwischen den Akteuren der öffentlichen Hand und des Privatsektors erfordern.

Die zielgerichtete Zusammenarbeit zwischen Staat und Wirtschaft ist ein zentraler Erfolgsfaktor, um mit der Dynamik und der Komplexität einer globalisierten Welt Schritt halten und um die Sicherheitsherausforderungen des 21. Jahrhunderts erfolgreich meistern zu können. Der Grand Pas de Deux, der dem vorliegenden Sammelband seinen sinnbildlichen Untertitel gibt, beschreibt die Notwendigkeit der engen Abstimmung von Sicherheits- und Wirtschaftspolitik und einer neuen Qualität der Zusammenarbeit zwischen Staat und Wirtschaft. In dem Maß, wie durch die Sicherheitspolitik Rahmenbedingungen für innovative unternehmerische Leistungen defi-

1 Geoffrey Heal at. al., „Interdependent Security in Interconnected Networks", in Philip E. Auerswald et. al. (eds.) *Seeds of Disaster, Roots of Response. How Private Action Can Reduce Public Vulnerability* (Cambridge: Cambridge University Press, 2006), S. 258-275, hier S. 258.

2 Ralph W. Shrader and Mike McConnell, „Security and Strategy in the Age of Discontinuity: A Management Framework for the Post-9/11 World", in Randall Rothenberg (ed.), *Enterprise Resilience: Risk and Security in a Networked World* (McLean: Booz Allen Hamilton, 2003), S. 12-28, hier S. 25.

3 Paul Kennedy, *The Rise and Fall of the Great Powers. Economic Change and Military Conflict from 1500 to 2000* (New York: Vintage Books, 1989).

niert werden, schafft der Staat nicht nur Anreize zur Verbesserung der unternehmerischen Sicherheitsvorsorge. Das Innovationspotenzial der Wirtschaft und der Wissenschaft kann darüber hinaus freigesetzt werden, um Konzepte, Produkte und Systemlösungen zu entwickeln und anzubieten, die gleichzeitig Sicherheit und Prosperität fördern. Das gilt in ganz besonderem Maß für so wichtige Bereiche wie die Systemintegration, die Modellbildung und Simulation, die Datensicherheit, die mobile und sichere Kommunikation und Datenübertragung, neue Werkstoffe, die Bio-, Gen- und Nanotechnologie, unbemannte Plattformen oder integrierte Schutzlösungen für das zivile und das militärische Umfeld. Die Leistungen von Wirtschaft und Wissenschaft in diesen Bereichen ist in hohem Maß wissensintensiv und damit relevant für die Wertschöpfung einer Volkswirtschaft. Zudem trägt die Expertise in diesen Feldern auch direkt zur Bereitstellung adäquater sicherheitspolitischer Fähigkeiten bei und ist damit unerlässlicher Bestandteil der nationalen Sicherheitsvorsorge.

Die Erfahrungen im Zuge der Transformation der Streitkräfte lehren allerdings, dass die Industrie alleine kaum in der Lage ist, die notwendigen Reformen einzuleiten, die erforderlich sind, um die von den staatlichen Behörden geforderten Sicherheitssysteme, -produkte, -dienstleistungen und -technologien bereitzustellen. Für die nationale Sicherheitsvorsorge sollte daraus die Lehre gezogen werden, dass die staatlichen Stellen ihre Partner in Wirtschaft und Wissenschaft aktiv begleiten sollten, um deren Geschäftsmodelle auf die neuen Sicherheitsherausforderungen anzupassen. Neben seiner Funktion als Kunde schlüpft der Staat dadurch auch in die Rolle des Coachs seiner nicht-staatlichen Partner. Durch neue Ansätze der Zusammenarbeit auf allen Stufen des Lebenszyklus' eines Systems (d.h. von der Risiko- und Bedarfsanalyse über Produktentwicklung, Indienststellung sowie Wartung und Unterhalt) können Staat und Wirtschaft bzw. Wissenschaft einander gegenseitig dazu befähigen ihre jeweiligen Rollen und Beiträge im Umgang mit den zu lösenden Sicherheitsherausforderungen neu zu definieren. Das gilt insbesondere für die zunehmend wichtiger werdende Systemfähigkeit. Diese integriert die bestehenden Produkt-, Dienstleistungs- und Technologiekompetenzen zu umfassenden Lösungsansätzen für die staatlichen Auftraggeber und definiert damit ein eigenständiges Marktsegment. Erfolg in diesem Marktsegment ist abhängig von entsprechenden Kompetenzen, die sich in der Praxis bewähren müssen. Durch die Beauftragung mit der Durchführung konkreter Projekte und die Förderung der Forschung kann der Staat dazu beitragen, dass seine Partner in Wirtschaft und Wissenschaft solche Systemfähigkeiten aufbauen, erhalten und stärken.

Die Notwendigkeit des Grand Pas de deux leitet sich aus fünf Überlegungen ab:

- Erstens sind die auf Vernetzung und Optimierung der Abläufe ausgelegten *globalen Wirtschaftsprozesse* anfällig für Verzögerungen des Leistungserstel-

lungsprozesses,[4] die z.B. aus technischem Versagen, gezielten – mitunter terroristischen – Angriffen oder aus der Verschärfung von Sicherheitsbestimmungen resultieren können. Nach den Anschlägen im September 2001 in den USA war die Sperrung des Luftraums über den Vereinigten Staaten eine der ersten Sicherheitsmaßnahmen. Mit dem Ergebnis, dass die privaten Logistikunternehmen ihre Fracht nicht mehr per Lufttransport versenden konnten und dadurch signifikante Verzögerungen in der Zustellung und in den davon abhängigen Wirtschaftsprozessen entstanden. Dieses Beispiel verdeutlicht, dass Sicherheitsbestimmungen als Folge eines neuen Risikobildes zu relevanten wirtschaftlichen Zusatzbelastungen führen können, beispielsweise durch höhere Versicherungsprämien, die Umgestaltung von Geschäftsprozessen, die Einführung neuer Technologien, den erhöhten Personalbedarf oder den Bau neuer Infrastruktur.[5] Daher ist die enge Abstimmung zwischen Staat und Wirtschaft bei der Definition von Sicherheitsmaßnahmen dringend geboten.

- Zweitens ist die *Sicherheit von Unternehmen* in unterschiedlicher Weise gefährdet. Abgesehen von den Risiken, die mit der eigentlichen Erstellung der jeweiligen Produkte und Dienstleistungen verbunden sind, reicht das Spektrum vom Produktboykott, der Produktpiraterie und der Wirtschaftsspionage über Angriffe gegen die Mitarbeitenden und die Infrastruktur von Unternehmen bis hin zum Ausfall der Mitarbeitenden und dem Rückgang des Konsums bei Pandemien. Die damit verbundenen Kosten sind signifikant. Nach Schätzungen beliefen sich 2003 die weltweiten Kosten von Unternehmen durch Cyber-Attacken auf 12,5 Milliarden $.[6] Die Kosten für die Wirtschaftsspionage werden in Deutschland auf knapp 20 Milliarden € geschätzt, und die Schäden der Wirtschaftskriminalität werden auf bis zu 43 Milliarden € beziffert.[7] Im Fall der Terroranschläge auf New York und Washington D.C. im Jahr 2001 beliefen sich die geschätzten finanziellen Einbußen der Tourismusindustrie auf 16 Milliarden $, der Flugverkehrslinien auf 15 Milliarden $ und der Finanzdienstleister auf 77 Milliarden $.[8] Schließlich liegt der geschätzte Schaden, der aus Produktfälschungen resultiert, je nach Betrachtungsweise

4 Nach einer Studie des Bundesverbands Materialwirtschaft, Einkauf und Logistik (BME) vom September 2007 verfügte knapp die Hälfte der vom Verband in Deutschland befragten Unternehmen, die über die Bahn versorgt werden, über keinen oder nur einen Tag Sicherheitsreserve in der Belieferung mit Gütern. Siehe: Holger Hildebrandt, „Trends in der Logistik“, *Griephan Global Security,* 1/2008, S. 15- 18, hier S. 15.

5 *Erfolg in der Secure Economy. Wachstum und Wohlstand in einer sicheren Wirtschaft* (o.O.: Deloitte, 2004), S. 3-4.

6 *Erfolg in der Secure Economy,* S. 1.

7 „Gefahr aus dem Ausland“, Der Tagesspiegel, 23. Oktober 2007, <http://www.tagesspiegel.de/wirtschaft/Spionage;art271,2404817> (Zugriff: 28. Februar 2008).

8 Erik Belfrage, „Public-private sector cooperation“, in Alyson J. K. Bailes and Isabel Frommelt (eds), *Business and Security. Public-Private Sector Relationships in a New Security Environment* (Oxford: Oxford University Press, 2004), S. 33-36, hier S. 34.

zwischen 200 bis 1.000 Milliarden $.[9] Schutz-, Abwehr- und Gegenmaßnahmen gegen die unterschiedlichen Risiken können nicht von einzelnen Unternehmen oder Sicherheitsbehörden ergriffen werden, sondern bedürfen der branchenübergreifenden Abstimmung und der engen Zusammenarbeit zwischen öffentlichen und privaten Akteuren.

- Drittens sind in den meisten Industrienationen private Unternehmen die Eigentümer und Betreiber der kritischen Infrastrukturen (KRITIS), z.B. in den Bereichen Energie, Transport, Kommunikation. In Deutschland befinden sich gut 85 % dieser kritischen Infrastrukturen in privatem Besitz.[10] Die Verschiebung der Besitzverhältnisse in diesem Bereich ist unmittelbar relevant für die staatliche Sicherheitsvorsorge. Bis in die jüngste Zeit war nämlich die *Sicherstellung der Gemeinwohlorientierung,* die mit den Leistungen verbunden sind, die auf Basis der kritischen Infrastruktur angeboten werden, eine der ureigensten Aufgaben des Staates. Aufgrund der festgestellten Verlagerung der Besitzverhältnisse ist diese Funktion des Staates unmittelbar abhängig von der Leistungsfähigkeit und von der Sicherheitsvorsorge der privaten KRITIS-Eigentümer und -Betreiber. Daraus ergibt sich die Notwendigkeit der engen Einbindung privater KRITIS-Akteure in staatliche Schutzmaßnahmen, Übungen und sowie in die Fähigkeitsanalyse und -planung.
- Eng mit dem dritten Punkt verbunden ist, viertens, die Tatsache, dass wesentliche Komponenten der eigentlichen *staatlichen Leistung* inzwischen ebenfalls *von Unternehmen erbracht* werden. Der „vernetzte Staat" teilt mit seinen Partnern die Verantwortung für die Leistungserbringung, muss gleichzeitig aber auch neue Aufgaben übernehmen sowie neue Kompetenzen entwickeln, um die Netzwerkbeziehungen aufzubauen, zu pflegen und weiterzuentwickeln. Das Ausmaß privater Leistungserbringung für den Staat reicht dabei im Sicherheitsbereich von der Unterstützung z.B. bei der Informations- und Datenverwaltung, dem Betrieb von Kommunikationslösungen über die Ausrüstung von Streitkräften und zivilen Einsatzkräften bis hin zur Bereitstellung von Impfstoffen. Ob und in welchem Umfang der „vernetzte Staat" seine eigentlichen Aufgaben erfüllen kann, wird daher ebenfalls maßgeblich von der Sicherheitsvorsorge und der Leistungsfähigkeit seiner privatwirtschaftlichen Partner bestimmt.
- Schließlich stellen wir fest, dass die *privatwirtschaftlichen Partner selbst immer stärker voneinander abhängen.* Diese Entwicklung ist ein direktes Ergebnis der Auslagerung verschiedener Unternehmensfunktionen, die primär aus kostengetriebenen Optimierungsüberlegungen resultiert. Natürlich ist betriebswirtschaftliche Effizienz wichtig, doch wie ist diese zu beurteilen, wenn sie – wie z.B. in der Logistik oder beim Management der Infrastruktur der modernen Datenverwaltung – zu kritischen Abhängigkeiten führt?

9 „Produktfälschung als globales Problem. Die OECD bezeichnet Asien als wichtigsten Produktionsort", *Neue Zürcher Zeitung,* 30. Oktober 2007, S. 21.

10 <http://www.bsi.de/literat/faltbl/F17KritischeInfrastruktur.htm> (Zugriff: 28. Februar 2008.)

> If FedEx runs supply-chain operations for 50 firms, multiple operating systems are replaced by a single one. The one may be more effective, and even inherently more secure, than most of the 50 were, but hackers now can concentrate their attacks on one target.[11]

Angesichts dieser Überlegungen ist die Öffentlich-Private Sicherheitspartnerschaft das Gebot der Stunde. Sie ist sicherheits- wie wettbewerbspolitisch gleichermaßen von Bedeutung. Sicherheitspolitisch ermöglicht erst die enge Abstimmung zwischen Staat und Wirtschaft/Wissenschaft die Entwicklung von Sicherheitskonzepten und die Bereitstellung sicherheitsrelevanter Fähigkeiten, die den modernen Sicherheitsherausforderungen gerecht werden. Wettbewerbspolitisch ist die enge Verzahnung von politischen und wirtschaftlichen Interessen notwendig, um die Wettbewerbsposition der eigenen Industrie im globalen Wettbewerb z.B. durch Informationsaustausch, den Einsatz für die Harmonisierung sicherheitsrelevanter Bestimmungen oder das Erschließen neuer Märkte zu stärken.[12]

Diese Sicherheitspartnerschaft erfordert allerdings von allen beteiligten Akteuren die Übernahme neuer Aufgaben und Verantwortlichkeiten sowie in gewissen Bereichen auch Verhaltensänderungen. Wie Abbildung 1 verdeutlicht, darf diese Sicherheitspartnerschaft auch nicht nur auf die Beziehung zwischen Staat und Wirtschaft im Sinne der klassischen Öffentlich-Privaten Partnerschaft (ÖPP) reduziert werden. Vielmehr sollte sie um die Notwendigkeit der verstärkten Kooperation und Koordination zwischen staatlichen Akteuren (Öffentlich-Öffentliche Partnerschaft) und zwischen Unternehmen (Privat-Private Partnerschaft) ergänzt werden.[13] Diese beiden Zusatzdimensionen bilden gewissermaßen die Klammer, innerhalb derer sich die Öffentlich-Private Sicherheitspartnerschaft entwickeln kann.

Die Öffentlich-Öffentliche Partnerschaft ist die zentrale Voraussetzung für eine neue Qualität der Sicherheitszusammenarbeit, denn ohne eine bessere Vernetzung zwischen den Ressorts im Hinblick auf Lageanalyse, Führung, Planung, Einsatzdurchführung und -auswertung sowie Ausbildung und Beschaffung fehlen wichtige Rahmenbedingungen für die Kooperation mit nicht-staatlichen Akteuren. Die Privat-Private Partnerschaft bildet hierzu das Pendant auf der wirtschaftlichen Seite und trägt dem Umstand Rechnung, dass die vielgliedrigen Wertschöpfungsketten der heutigen Wirtschaftsprozesse eine Reihe von Akteuren umfassen, die im Sinne eines Total Security Management[14] ganzheitlich betrachtet werden müssen. Untersuchun-

11 Robert A. Miller and Irving Lachow, *Strategic Fragility: Infrastructure Protection and National Security in the Information Age,* Defense Horizons 59 (Washington, D.C.: Center for Technology and National Security Policy, 2008), S. 3.

12 Hierzu auch: Positionspapier zur Bedeutung der Sicherheit in der Industrie für Deutschland (Berlin: BDI, 2006), S. 10-11.

13 Amit Kumar, „Developing Homeland Security Partnerships: A Comparative Analysis From the Area of Financial Security“, *HSI Journal of Homeland Security,* 24 August 2007, <http://www.homelandsecurity.org/newjournal/Articles/displayArticle2.asp?article=163> (Zugriff: 29. Februar 2008).

14 Luke Ritter, J. Michael Barrett, Rosalyn Wilson, *Securing Global Transportation Networks. A Total Security Management Approach* (New York: McGraw Hill, 2007).

gen zeigen denn auch, dass die Bereitschaft von Unternehmen, in die Verbesserung ihrer Sicherheit zu investieren, wesentlich davon abhängt, wie viele Unternehmen ebenfalls von den gleichen Sicherheitsherausforderungen betroffen sind und in welchem Umfang diese in ihre Sicherheit investieren.[15]

Dimensionen	Herausforderungen	Schlüsselaufgaben
Öffentlich ⇕ Öffentlich	▪ Diffuse Risiken mit unterschiedlichen Ursachen vs. bestehende Ressortzuständigkeiten ▪ Steigerung der organisatorischen Flexibilität und der institutionellen Lernfähigkeit ▪ Verbesserung der Kohärenz politischer Maßnahmen	▪ Förderung gesamtstaatlicher Ansätze für Lageanalyse, Führung, Planung, Einsätze, Ausbildung und Beschaffung ▪ Wechselwirkungen zwischen sub-nationaler, nationaler und internationaler Ebene beachten
Öffentlich ⇕ Privat	▪ Vernetzter Staat ist abhängig von unternehmerischer Leistungsfähigkeit ▪ Unternehmerische Sicherheitsvorsorge beeinflusst staatliche Sicherheitsvorsorge ▪ Unternehmen als Ziele sicherheitsgefährdender Aktionen ▪ Aufwirkungen von Sicherheitsmaßnahmen auf die Wirtschaft ▪ Sicherheit vs. Liberalisierung ▪ Selbststeuerung des Marktes vs. Regulierung	▪ Sicherheitspartnerschaften auf strategischer und projektspezifischer Ebene (Prozesse, Strukturen, Instrumente, Fähigkeiten) ▪ Finanzierung der Sicherheitsaufgaben sicherstellen ▪ Regulatives Umfeld weiterentwickeln (Anreizmechanismen)
Privat ⇕ Privat	▪ Wertschöpfungsketten der globalen Wirtschaft erhöhen inter- und intra-unternehmerische Abhängigkeiten ▪ Sicherheit als Investition in die Zukunfts-robustheit des eigenen Geschäftsmodells vs. Sicherheit als Kostenfaktor	▪ Unternehmenssicherheitsvorsorge als integraler Bestandteil betrieblicher Wertschöpfungsketten ▪ Sektorspezifische und sektorüber-greifende Betrachtung der Abhän-gigkeiten

Abbildung 1: Drei Dimensionen der Sicherheitspartnerschaft

Im Hinblick auf die stärkere gemeinsame Betrachtung staatlicher und wirtschaftlicher (Sicherheits-)Interessen spielt der Mittelstand eine besondere Rolle. Dienstleistungs- und Wissensgesellschaften schöpfen ihre Kraft aus der Leistungsfähigkeit des Mittelstandes. Durch zwei große Entwicklungslinien gerät dieser jedoch immer mehr unter Druck. Zum einen erhöhen sich die Forderungen an den Mittelstand in den unterschiedlichsten Politikfeldern – von der Sozial-, über die Umwelt- und Energie- bis hin zur Finanzpolitik. Der finanzielle Spielraum, aus dem z.B. Investitionen in die Sicherheit der Geschäftsprozesse finanziert werden, schrumpft dadurch. Zum anderen lagern multinationale Konzerne einen immer größeren Teil ihrer Entwicklungs- und Herstellungsrisiken an die Zulieferer aus. Gleichzeitig spielen diese eine immer wichtigere Rolle, wenn es darum geht, selbst Systemfähigkeiten zu entwickeln bzw. die Systemfähigkeiten der Konzerne durch Expertise in Schlüsselbereichen zu unterstützen. Klein- und mittelgroße Unternehmen tragen dadurch eine immer größere Verantwortung für ihren eigenen Erfolg und

15 Heal, „Interdependent Security in Interconnected Networks“, S. 260.

auch für den Erfolg der multinationalen Konzerne. Diesen Erfolg können sie jedoch langfristig nur gewährleisten, wenn sie über eine ausreichende Finanzkraft verfügen.

Begleitet wird dieser Prozess beispielsweise in Deutschland durch eine zunehmende Polarisierung der Einkommensverteilung. Während die einkommensstarken und die einkommensschwachen Bevölkerungsteile zunehmen, schrumpft die gesellschaftliche Mittelschicht. Das legt die Schlussfolgerung nahe, dass bei der Diskussion über die möglichen Folgekosten von Sicherheitsmaßnahmen nicht nur die Belastungsfähigkeit der Unternehmen, sondern auch diejenige der Bürgerinnen und Bürger verstärkt beachtet werden sollte.[16]

Wie die einzelnen Beiträge des vorliegenden Sammelbands verdeutlichen, gibt es für die konkrete Ausgestaltung der Öffentlich-Privaten Sicherheitspartnerschaft zahlreiche Ideen und konkrete Empfehlungen. Zusammenfassend können an dieser Stelle vier Punkte besonders hervorgehoben werden:

- *Regulative Rahmenbedingungen*
  Grundvoraussetzung der Öffentlich-Privaten Sicherheitspartnerschaft sind die rechtlichen Rahmenbedingungen, die eine Zusammenarbeit zwischen der Wirtschaft und den staatlichen Sicherheitsbehörden überhaupt erst ermöglichen. Hierfür besteht in Deutschland Handlungsbedarf, denn im Unterschied zu anderen Ländern sind die Grundlagen hierfür noch nicht ausreichend geschaffen.[17] Darüber hinaus sollte den Wechselwirkungen zwischen Sicherheit und Wettbewerb mehr Beachtung geschenkt werden. Dabei spielen vier Aspekte eine wichtige Rolle.
  Erstens wird die Diskussion über Regulierung zu oft einseitig als Eingriff in die Wettbewerbskräfte dargestellt. Sie sollte viel stärker unter dem Gesichtspunkt der Anreizregulierung geführt werden. Dabei geht es darum, durch marktkonforme Anreize wie z.B. Steuererleichterungen oder die Änderung der Abschreibungsmodalitäten die Bereitschaft von Unternehmen zu Sicherheitsinvestitionen zu fördern.[18] Eine wichtige Rolle spielen in diesem Zusammenhang auch Finanzanalysten, Rating-Agenturen und Versicherungen. Mit ihrer Bewertung von Sicherheitsinvestitionen und von Unternehmen, die in ihre Sicherheit investieren, können sie wichtige Impulse dafür setzen, Sicherheit als Beitrag zur Steigerung des Unternehmenswertes und nicht nur als Kostenfaktor zu interpretieren.
  Zweitens ist ein enger Dialog zwischen Staat und Wirtschaft nötig, um die möglichen Konsequenzen veränderter Sicherheitsbestimmungen im nationalen und im internationalen Kontext zu erörtern. Im Vordergrund steht die Bemü-

16 Markus M. Grabka und Joachim R. Frick, „Schrumpfende Mittelschicht – Anzeichen einer dauerhaften Polarisierung der verfügbaren Einkommen?“, *Wochenbericht des DIW Berlin,* 75:10 (7. März 2008), S. 101-108.

17 Positionspapier zur Bedeutung der Sicherheit in der Industrie für Deutschland, S. 11.

18 Heiko Borchert, „Engaging the Science and Technology Community in the Fight against Terrorism“, in Andrew James (ed.), *Science and Technology for the Anti-Terrorism Era* (Amsterdam: IOS Press, 2006), S. 111-124.

hung, Wettbewerbsnachteile infolge von Sicherheitsbestimmungen zu vermeiden. So belaufen sich z.B. die Flugsicherheitsgebühren in Dubai auf 0,31 € pro Passagier, während in Frankfurt 2,84 € pro Passagier anfallen.[19] Die Öffentlich-Private Sicherheitspartnerschaft soll durch den intensiven Informationsaustausch und die Positionsabstimmung zwischen Staat und Wirtschaft dazu beitragen, dass Handelsströme über Sicherheitsbestimmungen nicht zum Wettbewerbsnachteil der eigenen Wirtschaft in andere Länder umgeleitet werden.[20]

Drittens sollte auch verstärkt analysiert werden, wie Sicherheitsvorschriften in die globalisierten wirtschaftlichen Wertschöpfungsprozesse eingreifen und wie sie sich beispielsweise auf die Zusammenarbeit zwischen Unternehmen auswirken. Es kann nämlich sein, dass nationale Sicherheitsbestimmungen z.B. zum Schutz sensitiven Materials und Know-hows die unternehmerischen Anreize zur internationalen Zusammenarbeit reduzieren. Das kann sich möglicherweise nicht nur negativ auf die Innovationsfähigkeit der entsprechenden Unternehmen auswirken, sondern kann auch deren Fähigkeit beeinträchtigen, sicherheitsrelevante Produkte und Lösungen anzubieten.[21]

Schließlich ist auch zu beachten, dass Sicherheitsbestimmungen nicht nur auf die Wettbewerbskräfte einwirken. Umgekehrt können auch Deregulierung und Marktkonsolidierung sicherheitsrelevante Auswirkungen nach sich ziehen, mit unter sogar die Sicherheit gefährden. Dieses Risiko besteht z.B. im Energiebereich vor allem dann, wenn unter Wettbewerbsdruck z.B. Reservekapazitäten abgebaut werden, die Personaldecke ausgedünnt oder gar Investitionen zugunsten sicherheitsrelevanter Vorkehrungen ausbleiben.[22] Im Softwarebereich stellt sich angesichts des verstärkten Rückgriffs auf Standardsoftware anstelle spezifischer Entwicklungen die Frage nach der Zuverlässigkeit der jeweiligen Anbieter und möglicher Sicherheitsrisiken in ihren Anwendungen, die auch die Geschäftsprozesse der Nutzer beeinflussen können.[23] Und schließlich sind

19 *Booming Middle East carriers – The largest threat beside LCC* (München: Arthur D. Little GmbH, 2008), S. 5.

20 Genau darum bemüht sich die deutsche Bundesregierung nach eigenen Angaben gegenwärtig im Hinblick auf die Umsetzung des US-Safe-Port-Act aus dem Jahr 2006, der eine 100prozentige Durchleuchtung aller Seecontainer mit dem Transportziel USA vorsieht. Siehe: Folgen des US-Safe-Port-Act und der US-House Resolution No. 1 für die Bundesrepublik Deutschland vom 5. Februar 2008, BT-Drs. 16/7971.

21 Eine solche Gefahr sieht Stephen Brooks z.B. in den US-Bestimmungen, die für die biotechnologische und chemische Industrie im Umgang mit der Entwicklung von Mitteln zur Abwehr und Bekämpfung von BC-Kampfstoffen erlassen wurden. Siehe: Stephen Brooks, *Producing Security. Multinational Corporations, Globalization, and the Changing Calculus of Conflict* (Princeton/Oxford: Princeton University Press, 2005), S. 245.

22 David Buchan, „The Threat Within: Deregulation and Energy Security", *Survival,* 44:3 (Autumn 2002), S. 105-116; Stephen Thomas and David Hall, *Restructuring and outsourcing of electricity distribution in the EU* (London: Public Services International Research Unit, 2003).

23 In den USA wurde daher kürzlich in einer Studie gefordert, dass Software und Anbieter von Commercial off the shelf-Lösungen verstärkt auf ihre möglichen Sicherheitsimplikationen un-

in jüngster Zeit die Aspekte der Kontrolle von und des Eigentums an Unternehmen aus sicherheitsrelevanten Branchen durch die Konsolidierung innerhalb bestimmter Marktsegmente und den Vermögenszuwachs von Investoren aus Schwellenländern (Stichwort: Staatsfonds) in den Mittelpunkt der öffentlichen Diskussion gerückt. Bestehende Regelungen zum Schutz wissenschaftlich-industrieller Schlüsselunternehmen und ihres Know-hows müssen im Lichte neuer sicherheitspolitischer Herausforderungen, machtpolitischer Verschiebungen in den internationalen Beziehungen und dem Interesse an einem freien Kapitalverkehr neu ausbalanciert werden.

- *Plattformen und Prozesse*
  Die Öffentlich-Private Sicherheitspartnerschaft bedarf eines adäquaten institutionellen Rahmens für den Informationsaustausch und für die Zusammenarbeit. Ansätze dazu sind in Deutschland über die Arbeitsgemeinschaft für Sicherheit der Wirtschaft e.V. als zentrale Koordinierungsstelle zur Weitergabe von Sicherheitsinformationen zwischen Staat und Wirtschaft vorhanden.[24] Darauf lässt sich aufbauen, wobei zwei Stoßrichtungen unterschieden werden können.
  Im Hinblick auf den Umgang mit konkreten Gefahren kann ein Beispiel aus Großbritannien als Anregung dienen. Zur Bekämpfung ausländischer Hackerangriffe hat der britische Inlandsgeheimdienst MI5 das private Beratungsunternehmen KPMG mit dem Aufbau eines Monitoringsystems betraut. Dieses soll es ermöglichen, dass die Führungskräfte britischer Unternehmen in einem gesicherten Informationsraum Daten und Erfahrungen zum Umgang mit Cyberattacken und möglichen Abwehr- und Gegenmaßnahmen austauschen können.[25]
  Darüber hinaus sollte auf der strategischen Ebene die Systematisierung des Informationsaustauschs zwischen Staat und Wirtschaft im Hinblick auf die Erstellung eines gemeinsamen, rollenorientierten öffentlich-privaten Lagebildes in Angriff genommen werden. Dadurch könnte ein Führungsinstrument geschaffen werden, das gleichzeitig strategische Entscheidungsprozesse unterstützt und für das Krisenmanagement die Zusammenführung von Informationen aus Lagebildern staatlicher und privater Leitstellen befördern kann.

- *Risiko- und Chancendialog*
  Eng mit dem zweiten Punkt verbunden ist die Idee des öffentlich-privaten Risiko- und Chancendialogs. Dabei geht es zum einen natürlich um den Austausch von Informationen mit Blick auf mögliche Risiken und Gefährdungsla-

tersucht werden. Siehe: Defense Science Board, *Mission Impact of Foreign Influence on DoD Software* (Washington, D.C.: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, 2007).

24 <http://www.asw-online.de> (Zugriff: 28. Februar 2008).

25 *Intelligence Online,* 13. Dezember 2007, S. 5

gen, der durch den Vorschlag eines gemeinsamen, rollenorientierten öffentlich-privaten Lagebildes unterstützt wird. Darüber hinaus könnten im Rahmen eines solchen Dialogs sicherheitsrelevante Entwicklungen im In- und Ausland auch viel stärker für die Abstimmung politischer und unternehmerischer Strategien genutzt werden. Zu denken ist beispielsweise an das Sicherheitsengagement im Ausland. Dieses leistet nicht nur einen Beitrag zur Stabilität am jeweiligen Einsatzort, sondern böte auch die Möglichkeit, Marktpotenziale für Sicherheitslösungen nationaler Anbieter zu erschließen. Eine ähnliche Überlegung gilt auch für die Abstimmung der politischen und der unternehmerischen Positionen im Hinblick auf die Bewältigung von Sicherheitsaufgaben im Rahmen internationaler Organisationen und die diesbezügliche politische Flankierung der Industrieinteressen[26] oder für die Nutzung internationaler Förderprogramme im Sicherheitsbereich zur Unterstützung der eigenen Industrie- und Wissenschaftskompetenzen.[27]

- *Sicherheitsstandards*
  Wer Standards setzt, definiert Märkte. Dies bedeutet, dass Sicherheitsmärkte oftmals nur durch Standards oder andere regulative Rahmenbedingungen entstehen. Der Gesetzgeber wird somit durch seine Tätigkeit in diesem Bereich entweder zum „Geburtshelfer" für bestimmte Industriezweige oder er verschafft der eigenen Industrie möglicherweise durch unterlassenes oder zu spätes Handeln einen Wettbewerbsnachteil, weil andere die Standards bereits definiert haben.
  Standards können aber auch von der Wirtschaft selbst entwickelt werden, z.B. durch das „Lernen vom Besten" (Best Practice). In diesem Sinne sind die in verschiedenen Ländern und auch auf der europäischen Ebene laufenden Bemühungen zur Definition von Standards für sicherheitsrelevante Geschäftsprozesse zu interpretieren.[28] Diese können einen Beitrag zur Verbesserung der unternehmerischen Sicherheitsvorsorge leisten, vorausgesetzt, dass die jeweiligen Standards entsprechend der Risiko- und Gefährdungslage weiterentwickelt und die Einhaltung der Standards überprüft werden.

Vor diesem Hintergrund decken die einzelnen Beiträge des vorliegenden Sammelbandes ein breites Themenspektrum ab. Den Auftakt bilden die beiden Beiträge von Uwe Christian Fischer und Thomas Menk zur Sicherheitspartnerschaft aus staatlicher bzw. unternehmerischer Perspektive.

26 Als ein Beispiel kann die Einführung von Systemen zur Personenkontrolle auf Basis biometrischer Anwendungen genannt werden.

27 So schaffte es z.B. Frankreich, aus dem 2007 mit gut 150 Millionen € dotierten EU-Sicherheitsforschungsprogramm mit 13 % einen höheren Projektanteil zu akquirieren als Großbritannien oder Deutschland. Siehe: *Intelligence Online,* 14. Februar 2008, S. 8.

28 „Societal Security: Guideline for incident preparedness and operational continuity management" (ISO/PAS 22399:2007), <http://www.iso.org/iso/catalogue_detail?csnumber=50295> (Zugriff: 8. April 2008).

Uwe Christian Fischer sieht in der Wirtschaftsspionage, dem illegalen Wissenstransfer, der Organisierten Wirtschaftskriminalität sowie im Terrorismus ein Risikopotenzial, das die technologischen Kernkompetenzen des Wirtschaftsstandorts Deutschlands und sein Auslandsengagement gefährden können. Angesichts eines wachsenden Sicherheitsbedürfnisses der Unternehmen und knapper werdenden Ressourcen des Staates betrachtet er die Öffentlich-Private Sicherheitspartnerschaft als einen möglichen Pfeiler zur Umsetzung des Konzepts der Vernetzten Sicherheit. Fischer stellt in seiner umfassenden Betrachtung allerdings fest, dass die Entwicklung zugunsten einer solchen Sicherheitspartnerschaft in Deutschland, verglichen mit den anglo-amerikanischen Ländern, eher schleppend verläuft. Bislang fehlt es, nach seiner Beurteilung, an einer ordentlichen Institutionalisierung einer solchen Partnerschaft, an personeller Vernetzung und insbesondere an den erforderlichen Sicherheitsregeln. Um diese Defizite zu beheben, schlägt Fischer verschiedene Ansatzpunkte vor: Er rät zu einem verbesserten Informationsaustausch vor allem bezüglich konkreter Risikobewertungen, zu einer stärkeren Einbeziehung der Wirtschaft in die nationalen Sicherheitsstrategien sowie zur Einsetzung einer ressortübergreifend besetzen Lenkungsgruppe mit Wirtschaftsvertretern. Ein neuer Ressortkreis „Sicherheit der Wirtschaft“ und ein gemeinsam besetztes Gemeinschaftsbüro einer Koordinierungsstelle der Bundesregierung könnten Beratung und Hilfestellung bei besonderen Sicherheitsvorkommnissen leisten. Im Hinblick auf die einleitend angesprochenen regulativen Rahmenvorgaben sieht Fischer im Vorgehen für ein nationales Kryptokonzept einen Ansatz, der auch auf andere sicherheitsrelevante Felder übertragen werden könnte. Dabei spielt die Sicherheitsforschung eine wichtige Rolle.

Thomas Menk stellt aus der Sicht eines global tätigen Unternehmens dar, dass neben den wirtschaftsexternen Faktoren wie z.B. internationalen Konflikten, informationellen Angriffen auf das Unternehmenswissen sowie kriminellen Handlungen gegen Unternehmen vor allem die wirtschaftsinternen Risiken, die aus der globalen Vernetzung der Wirtschaftsprozesse resultieren, immer mehr an Bedeutung gewinnen. Das traditionelle unternehmerische Sicherheitsmanagement, das sich auf Wach- und Schutzfunktionen konzentriert, kann diesen Herausforderungen nicht gerecht werden. Es berücksichtigt weder die Risikofelder, die von strategischer Bedeutung sind, noch ist es systematisch mit den unternehmerischen Wertschöpfungsprozessen verknüpft. Menk plädiert daher für den Aufbau eines integrierten Risiko- und Sicherheitsmanagements. Dieses basiert auf der ganzheitlichen Betrachtung unternehmensrelevanter Sicherheitsrisiken und legt den Fokus auf deren umfassende und frühe Aufklärung bzw. Identifizierung. Zu seiner Umsetzung bedarf das integrierte Risiko- und Sicherheitsmanagement einer unternehmensweit zuständigen Sicherheitsorganisation, die alle Sicherheitsprozesse im Unternehmen definiert und steuert. Sicherheit wird dabei als integraler Bestandteil der normalen Geschäftsprozesse verstanden. Dieses umfassende Risiko- und Sicherheitsmanagement leistet damit einen aktiven Beitrag zur betrieblichen Wertschöpfung. Darüber hinaus sind sichere und erfolgreiche Unternehmen wichtig für die staatliche Sicherheitsvorsorge. In der Art und Weise, wie Staat und Wirtschaft zusammenarbeiten, um das Gemeinwohlziel Sicherheit zu gewährleisten, sieht Menk noch Verbesserungspotenzial. Geht es um die Beurteilung der nationalen und der internationalen Sicherheitslage, könnte der

Informationsaustausch noch intensiver sein. Aus seiner Sicht wäre die Errichtung integrierter, öffentlich-privater Frühwarnstrukturen ein Ansatz, um dieses Ziel zu erreichen. Ebenso sollte die Wirtschaft aus seiner Sicht in einen möglichen nationalen Sicherheitsrat einbezogen werden.

Nach diesen strategischen Grundsatzüberlegungen richten Heiko Borchert und Karina Forster, Johannes Prinz sowie von Stefan Brem und Ruedi Rytz den Blick auf die Bemühungen zur Gewährleistung der Sicherheitsvorsorge in drei wichtigen Bereichen der kritischen Infrastruktur. Energie, Transport und Kommunikation können gewissermaßen als „Kern" der kritischen Infrastrukturen interpretiert werden, von denen alle anderen Sektoren der kritischen Infrastruktur weitgehend abhängen. Günther Marek und Maximilian Prinz verdeutlichen zudem die Herausforderungen zum Schutz von Großveranstaltungen am Beispiel der Fußball-Europameisterschaft 2008.

Der Beitrag von Heiko Borchert und Karina Forster basiert auf der Prämisse, dass die Sicherheit der Energieversorgung ohne die Sicherheit der Energieinfrastrukturen nicht gewährleistet werden kann. Die steigende Energienachfrage, die Forderung nach Diversifizierung mit Blick auf die Energielieferländer und die Versorgungswege, die Verknüpfung der europäischen Energieinfrastrukturen mit anderen Regionen sowie die Einspeisung erneuerbarer Energieträger werden die Abhängigkeit von funktionierenden Energieinfrastrukturen weltweit erhöhen. Angesichts der Einsicht in die Verwundbarkeit der Energieinfrastrukturen, die aus der Vernetzung der Infrastrukturkomponenten, aus spezifischen Gefährdungen, aber teilweise auch aus der erheblichen Unterfinanzierung resultieren, werden auf nationaler, europäischer und globaler Ebene unterschiedliche Ansätze zur Verbesserung ihres Schutzes ergriffen. Vor diesem Hintergrund stellen die Autoren in einem Modell die wesentlichen analytischen Dimensionen der Energieinfrastruktursicherheit dar, skizzieren die Schwerpunkte des Europäischen Programms zum Schutz kritischer Infrastrukturen und gehen auf den künftigen Handlungsbedarf ein. Dabei machen sie sich u.a. stark für adäquate institutionelle Rahmenbedingungen auf internationaler und europäischer Ebene, um die verschiedenen Politikfelder sowie die staatlichen und privatwirtschaftlichen Maßnahmen besser aufeinander abstimmen zu können. Wie andere Autoren des vorliegenden Sammelbandes sehen auch Borchert und Forster in der Erarbeitung von Sicherheitsstandards eine wichtige Aufgabe, um Anreize für Investitionen zu schaffen. Zudem plädieren sie dafür, die möglichen Beiträge der Streitkräfte zum Schutz der kritischen Energieinfrastrukturen systematisch zu analysieren, lokale Gemeinschaften in Energierohstoffförder- und -transitländer stärker in Sicherheitsüberlegungen einzubeziehen und das grenzüberschreitende Krisenmanagement für den Fall infrastrukturbedingter Zwischenfälle in Europa auszubauen.

Johannes Prinz geht auf die Herausforderungen im Bereich Transportverkehr an den Beispielen Flug- und Seehäfen ein. Die besondere Sicherheitsrelevanz dieser Einrichtungen erklärt sich aus der hohen Akkumulation von Personen und Gütern an wenigen Knotenpunkten, die in globale Verkehrsströme eingebunden sind. Dieses zentrale Wesensmerkmal der kritischen Transportinfrastruktur bringt es denn auch mit sich, dass auf der internationalen und auf der nationalen Ebene unzählige Akteure unterschiedlichster Herkunft koordiniert werden müssen. Das geht kaum ohne ein

gemeinsames Lagebild. Wie Prinz darstellt, liegt die zentrale Herausforderung der gemeinsamen Lagebilderstellung weniger im technischen Bereich, sondern vielmehr in der Art und Weise, wie Personen aus unterschiedlichen Organisationen mit Informationen umgehen und wie sie diese interpretieren. Damit spricht er die wichtige Schnittstellenproblematik an, die immer entsteht, wenn Prozesse organisationsübergreifend aufeinander abgestimmt werden sollen. Standardisierung ist dabei für Prinz das Schlüsselinstrument, um von organisationsspezifischen, meist proprietären Lösungen zu organisationsgemeinsamen und offenen Ansätzen zu kommen. Gleichzeitig betont er auch den marktbildenden Charakter von Standards, die gerade für Klein- und Mittelunternehmen von herausragender Bedeutung sind. Prinz spricht darüber hinaus zwei wichtige Aspekte an, die bei der Förderung sicherheitstechnischer Anwendungen nicht vernachlässigt werden dürfen. Zum einen bedeutet der Ersatz menschlicher Arbeitskraft durch technische Anwendungen auch die Verlagerung von Verantwortung. Nicht in jedem Bereich der sicherheitsrelevanten Aufgaben ist dies jedoch möglich bzw. wünschenswert. Zum anderen sind technische Lösungen nicht frei von Zielkonflikten, die sich beispielsweise aus Ansätzen zur Förderung von Safety (Umgang mit endogenen Risiken) und Security (Umgang mit exogenen Risiken) ergeben können.

Stefan Brem und Ruedi Rytz beschäftigen sich mit der Sicherheit der kritischen Informations- und Kommunikationsinfrastruktur. Ausgehend von einer Betrachtung des relevanten Risikospektrums entwickeln die Autoren theoretische Überlegungen zur Rolle des Staates als Sicherheitsproduzent im Bereich kritischer Infrastrukturen und illustrieren diese anhand konkreter Lösungsansätze, die in der Schweiz zum Schutz der kritischen Informations- und Kommunikationsinfrastruktur ergriffen wurden. Brem und Rytz führen aus, dass mit Ausnahme des Cyberterrorismus bislang alle anderen Hauptbedrohungskategorien (Naturgefahren, menschliches und technisches Versagen) zu teilweise erheblichen Beeinträchtigungen der Leistungsfähigkeit der Informationsinfrastruktur geführt haben. Die Gefährdung der kritischen Informationsinfrastruktur ist daher reell und erfordert entsprechende Abwehr- und Sicherungsmaßnahmen. Nach Ansicht der Autoren tragen jedoch der Zeitgeist des schlanken Staates und die dynamischen Markt- und Technologieentwicklung dazu bei, dass Regierungen nicht länger als Eigentümer oder Betreiber kritischer Informations- und Kommunikationsinfrastrukturen auftreten. Marktversagen, unvollständige Information und Moral Hazard sind aus Sicht der Autoren allerdings die wichtigsten Gründe, weshalb sich die Regierungen in diesem Bereich nicht bloß auf eine reine Laissez-faire-Politik zurückziehen können. Gefragt ist daher ein Mittelweg, der Elemente der öffentlich-privaten Zusammenarbeit mit Anreizmechanismen und gegebenenfalls gesetzlichen Maßnahmen kombiniert. Vor allem der partnerschaftliche Ansatz hat sich dabei in der Schweiz als Grundansatz zur Erarbeitung eines umfassenden Krisenmanagement- und Schutzsystems für die kritische Informations- und Kommunikationsinfrastruktur bewährt. So führten beispielsweise die von staatlichen Behörden und der Wirtschaft gemeinsam durchgeführten Risikoanalysen zu freiwilligen Maßnahmen zwischen den kritischen Infrastruktursektoren Telekommunikation und Energie, ohne dass der Staat gesetzgeberisch eingreifen musste. Ebenso gelang es, durch die enge öffentlich-private Abstimmung verschiedene Versuche der

Wirtschaftsspionage rechtzeitig zu erkennen und geeignete Gegenmaßnahmen zu treffen.

Günther Marek und Maximilian Prinz vermitteln aus österreichischer Sicht einen Blick in die Vorbereitung der Sicherheitsmaßnahmen für die gemeinsam mit der Schweiz ausgetragene Fußballeuropameisterschaft 2008. Die große mediale, sportliche und wirtschaftliche Bedeutung dieses Turniers erklärt den hohen Stellenwert der Sicherheitsfragen. Um den störungsfreien Verlauf dieses Ereignisses und die Sicherheit aller daran beteiligten Personen zu gewährleisten, setzen die Verantwortlichen auf die 3D-Einsatzphilosophie (Dialog, Deeskalation und Durchsetzung) sowie auf die enge Zusammenarbeit mit einer Vielzahl nationaler und internationaler, staatlicher und nicht-staatlicher Akteure. Die enge Kooperation dient der Prävention und dem Krisenmanagement. Bei der Prävention geht es u.a. um die Unterstützung privater Organisationen im Hinblick auf die zu bewältigenden Sicherheitsherausforderungen (z.B. Bereitstellen relevanter Informationen). Bei dem besonders wichtigen Aspekt der Stadionsicherheit war das Innenministerium bereits in die Planung neuer Stadien eingebunden und konnte Sicherheitsüberlegungen in einer frühen Phase einbringen. Im Rahmen des Krisenmanagements schenkten die Verantwortlichen gemeinsamen Planspielen mit allen sicherheitsrelevanten Akteuren große Beachtung. Diese wurden an den verschiedenen Austragungsorten durchgeführt und trugen dazu bei, die Zusammenarbeit zu verbessern sowie Führungs- und Einsatzverfahren aufeinander abzustimmen. Die Ausführungen der Autoren unterstreichen, dass ein Großereignis wie die EURO 08 für die Konzeption der nationalen Sicherheitsvorsorge aus mehreren Gründen relevant ist. Zum einen verdeutlicht ein solcher Anlass Entwicklungen, die auch sonst stattfinden, aber weniger auffallen. Das gilt vor allem für die Übernahme staatlicher Sicherheitsleistungen durch private Akteure. Zum anderen können aus den Ansätzen des Krisenmanagements für Großveranstaltungen und aus Erkenntnissen über das Verhalten großer Menschenmengen Lehren für den Schutz der Öffentlichkeit in offenen Räumen abgeleitet werden.[29] Darüber hinaus könnten solche Veranstaltungen auch genutzt werden, um sicherheitsrelevante Technologien im Einsatz zu testen. Das stärkt die Fähigkeiten der Sicherheitskräfte und dient der Herausbildung von Märkten für zivile Sicherheitsanwendungen.

Die drei abschließenden Beiträge illustrieren den Zusammenhang zwischen Sicherheitsförderung und Prosperitätsentwicklung anhand luftgestützter Fähigkeiten, der Zusammenführung komplexer Daten- und Informationsbestände in Lagebildern sowie der Modellbildung und der Simulation.

Im Mittelpunkt des Beitrags von Ralph Thiele steht der Aufbau sicherheits-, industrie- und wissenschaftspolitisch relevanter Cluster am Beispiel von zwei Projekten aus dem Österreichischen Sicherheitsforschungsprogramm KIRAS. Ausgehend vom Konzept der Vernetzten Sicherheit erläutert er die grundsätzliche Bedeutung luftgestützter Beiträge für die Bewältigung von Sicherheitsaufgaben sowie für die wirkungsvolle Unterstützung des Entscheidungszyklus‘ von der strategischen bis auf

29 So auch: *Forschung für die zivile Sicherheit. Programm der Bundesregierung* (Berlin: Bundesministerium für Bildung und Forschung, 2007), S. 22.

die operative Ebene. Dabei konzentriert er seine Ausführungen auf die Rolle unbemannter fliegender Plattformen. Er unterstreicht die Rolle mittelständischer Unternehmen, die – teilweise im Unterschied von den Angeboten führender multinationaler Konzerne – Produkte mit sehr breitem Aufgabenspektrum sowie sinkenden Investitions- und Betriebskosten anbieten. Damit solche Produkte entwickelt und hergestellt werden können, bedürfen gerade mittelständische Unternehmen eines entsprechenden innovativen Milieus, in dem sie von den Beziehungen zu anderen Unternehmen und Wissenschaftseinrichtungen profitieren. Der hierfür erforderliche Wissens- und Technologietransfer, die Förderung der Mitarbeiterkompetenzen durch Aus- und Weiterbildung sowie die Organisation des Austauschs von Daten, Informationen und Wissen kann durch die Clusterpolitik unterstützt werden. Besonders wichtig ist aus Thieles Sicht dabei die Fähigkeit, das Bewusstsein und das Verständnis aller Clusterpartner für die aktuelle Sicherheits- und Marktlage sowie deren künftige Entwicklung im Rahmen eines gemeinsamen Lagebildes zu fördern und zu verstärken. Die beiden KIRAS-Projekte „Sicherheit aus der Luft“ und „Periodische Überwachung kritischer Infrastrukturen“ dienen diesen Zielsetzungen und können als prototypische Beispiele des im vorliegenden Sammelband postulierten Zusammenhangs zwischen Sicherheits- und Prosperitätsförderung durch enge öffentlich-private Zusammenarbeit interpretiert werden.

Jan-Erik Schmidt legt in seinem Beitrag dar, welche informationstechnischen Schritte ein Gemeinwesen unternehmen kann, um seine Führungskräfte zu befähigen, eine komplexe Umwelt zu verstehen und darin erfolgreich zu agieren. Dabei stellt er einen direkten Zusammenhang her zwischen der sicherheitspolitischen Vernetzung, der damit verbundenen Forderung nach Wirkungsorientierung, den hierfür benötigten (finanztechnischen) Grundsätzen und Steuerungsinstrumenten sowie dem Beitrag von Business Intelligence. Information alleine verschafft noch keine Vorteile im Umgang mit komplexen Situationen. Vielmehr kommt es auf die Art und Weise an, wie Daten und Informationen verfügbar gemacht, welche Zusammenhänge durch Kombinationen von Informationsbausteinen dargestellt und welche Entscheidungen auf Basis der daraus gewonnenen Erkenntnissen schließlich getroffen werden. Business Intelligence kann dabei als Ansatz „höherer Intelligenz“ im Umgang und in der Auswertung mit Daten und Informationen verstanden werden. Schmidt verdeutlicht den aktuellen Sachstand mit einem Blick für die Schwächen der Verwaltungssteuerung im Übergang von der Input- zur Outputsteuerung (Wirkungsorientierung). Er diskutiert eingehend die technischen Herausforderungen, die zu bewältigen sind und stellt die Fähigkeit zur Integration verschiedener Komponenten moderner informationstechnischer Systeme als wesentliche Erfolgsvoraussetzung dar. Anhand konkreter Beispiele verdeutlicht er den Mehrwert von Business Intelligence-Lösungen und erläutert den Stellenwert von Lagebildern für die Führung im militärischen Umfeld bzw. im Kontext der nationalen Sicherheitsvorsorge. In dem Maß, wie Business Intelligence-Anwendungen zu neuen Erkenntnissen beitragen, so Schmidts Fazit, leisten sie einen wichtigen Beitrag zur Förderung von Sicherheit und Prosperität.

Andreas Lang und Olav Hansen argumentieren, dass die Komplexität moderner Sicherheitsherausforderungen simplifizierende Lösungsansätze verbieten. Vielmehr

sind Methoden und Verfahren erforderlich, um die Ursachen und Wirkungen von Sicherheitsherausforderungen, ihren Konsequenzen und möglichen Abwehr- und Gegenmaßnahmen zu verstehen. Die Modellbildung und die Simulation unterstützen Planer, Entscheider und Operateure bei dieser anspruchsvollen Aufgabe. Modellbildung und Simulation ermöglichen es u.a., die Wirkung von Maßnahmen zu testen, bevor diese ergriffen werden, wodurch Risiken minimiert und der Einsatz knapper Ressourcen optimiert werden können. Das ist von entscheidender Bedeutung, um beispielsweise Aussagen über die Wirkungsweise und die Folgen bzw. die Kosten von Sicherheitsmaßnahmen machen zu können. Gemäß der Darstellung der Autoren tragen unterschiedliche technologische Trends dazu bei, dass der Einsatz von Rechnersystemen zur Modellbildung und Simulation zunehmend einfacher und flexibler wird und die Leistungsfähigkeit der Systeme erhöhen. Daher dürften Modellbildung und Simulation künftig auch verstärkt im Rahmen der nationalen Sicherheitsvorsorge eingesetzt werden. Im Hinblick auf die spezifischen Rahmenbedingungen der nationalen Sicherheitsvorsorge und des Schutzes kritischer Infrastrukturen müssen jedoch neue methodische Ansätze entwickelt werden. Nur dann ist es möglich, kritische Infrastrukturen mit ihren Eigenschaften, in ihrem Verhalten und in ihrer gegenseitigen Abhängigkeit richtig darstellen zu können. Anhand eines Szenariobeispiels (Anschlag mit einer schmutzigen Bombe auf einen US-Hafen) illustrieren Lang und Hansen den Erklärungsgehalt und die Wirkungsweise der Modellbildung und Simulation. Gerade weil im Rahmen der nationalen Sicherheitsvorsorge unterschiedliche staatliche und nicht-staatliche Akteure zusammenarbeiten müssen, wäre es sinnvoll, diese in kollaborative Anwendungen der Modellbildung und Simulation einzubinden. Die Autoren machen allerdings klar, dass hierzu noch verschiedene methodische und technische Hürden zu nehmen sind.

Einige der in diesem Sammelband veröffentlichten Beiträge wurden im Rahmen eines Autorenworkshop am 19. September 2007 auf Einladung des Herausgebers in der Landesvertretung Baden-Württembergs in Berlin diskutiert. Andere Beiträge wurden spezifisch für diesen Sammelband verfasst. Der Herausgeber dankt den Autoren für die gute Zusammenarbeit. Die Durchführung des Workshops und die Drucklegung wurden von den Unternehmen Thales und Frequentis finanziell unterstützt. Weiterführende Materialien zu diesem Sammelband stehen über www.vernetzte-sicherheit.net zum Download zur Verfügung.