Institut für Strategie- Politik- Sicherheits- und Wirtschaftsberatung, Berlin

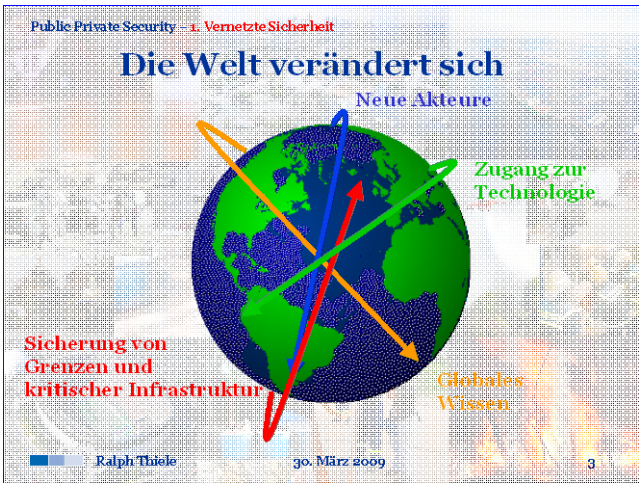
Public Private Security -

Möglichkeiten und Grenzen integrierter Konzepte und Projekte

von Ralph Thiele

Im Frühjahr 2009 hat der National Intelligence Council aus den U.S.A. in Berlin seine Studie Global Trends 2025 vorgestellt. Die Kernbotschaft lautet: Die Grundlagen unserer Sicherheit verändern sich. Schon in 15 Jahren werden wir die Welt kaum noch wiedererkennen: Neue Akteure – Neue Regeln – Neue Weltordnung.

Im 21. Jahrhundert bestimmen Vernetzte Systeme, Wissen und Hochtechnologie die Zukunft öffentlicher und privater Sicherheit wie auch unternehmerischer Wertschöpfung. Sicherheitsvorsorge wird zunehmend zur Gemeinschaftsaufgabe von staatlichen Behörden, NGOs, Wirtschaft, Forschung und Wissenschaft. Es bieten sich viele neue Chancen. Es gibt auch neue Risiken. Für viele Unternehmen gilt: Chancen nutzen, Netzwerke bilden oder andernfalls Übernahmekandidat werden. Das ist für andere Stakeholder nicht grundsätzlich anders.



Prophylaxe wird immer wichtiger für die „Äußere“ wie auch für die „Innere“ Sicherheit. Das Beispiel Afghanistan zeigt: Ereignisse und Entwicklungen, die weit außerhalb Europas stattfinden, haben Einfluss auf Deutschland. Sie können die Streitkräfte zum Handeln fordern. Dabei reicht die Spannbreite von Konflikten, die oft ganze Regionen destabilisieren, über die Bedrohung durch den internationalen Terrorismus, bis hin zu Folgen globaler Umweltprobleme, eine sichere Energieversorgung oder der Zugang zu begrenzten Ressourcen.

Vernetzte Sicherheit

Die Sicherheit von Staaten und ihren Gesellschaften hat inhaltlich bedeutende Erweiterungen erfahren. So wird Sicherheit nicht nur von außen und mit Gewalt gefährdet, sondern insbesondere auch, wenn das staatliche System von der Gesellschaft nicht mehr akzeptiert, wenn der gesellschaftliche Konsens gestört oder gar zerstört wird oder wenn die Gesellschaft Prozessen ausgesetzt wird, die sie aus eigener Kraft nicht mehr zu steuern vermag. Dies betrifft ebenfalls Vorgänge, die ihren Ursprung nicht in dem betreffenden Staat, sondern in seiner internationalen Umwelt haben. Genau dies verleiht den modernen, asymmetrischen Sicherheitsrisiken deren besondere Durchschlagskraft, denn deren Akteure zielen mit Bedacht auf gesellschaftliche Prozesse und den gesellschaftlichen Konsens.

Die Gefahr der asymmetrischen Bedrohung korrespondiert mit der Komplexität moderner Gesellschaften, in denen heterogene politische, wirtschaftliche, gesellschaftliche, technologische, ökologische, geographische und kulturelle Faktoren eng miteinander verwoben sind. Die aus dem hohen Grad der Vernetzung resultierenden Abhängigkeiten laden förmlich zum Missbrauch ein. So etabliert sich beispielsweise Organisierte Kriminalität im Umfeld von Freiheitskämpfern und Terroristen zur Durchsetzung wirtschaftlicher Interessen. Drogengeschäfte, illegale Migration, Menschen- und Waffenhandel haben nicht nur destabilisierende Folgen für die globalisierte Weltwirtschaft, sondern auch für die gesellschaftlichen Prozesse einschließlich der inneren Sicherheit der betroffenen Gesellschaften.

Die Aufgaben für zivile und militärische Sicherheitskräfte ändern sich mit den veränderten Aufgabenstellungen. Stabilisierungseinsätze im Ausland in nur partiell militärisch befriedetem Gebiet werden zu einer wahrscheinlichen Einsatzoption. Internationalen Friedenskontingenten stehen verdeckt kämpfende nationale Widerstandsgruppen und internationale Terrorgruppen gegenüber, die u.U. von an Destabilisierung interessierten Nationalstaaten unterstützt werden. Die Fähigkeiten polizeilicher Stabilisierungskräfte sind eng mit militärischen Fähigkeiten zu orchestrieren, damit es keine offenen Nahtstellen zwischen den Aufgabenbereichen gibt. Abstimmung und Synergie ist auch erforderlich im Zusammenhang mit dem Aufbau von Sicherheitsbehörden, Justiz, Entwicklungshilfe, Wirtschaftsförderung, Korruptionsbekämpfung u.a.m.

Die Wechselwirkungen der angeführten Faktoren kann kein einzelner Akteur – sei es ein Staat, ein Ministerium oder eine Sicherheitsbehörde – übersehen oder gar steuern. Jeder Akteur für sich wäre mit der Bewältigung dieser Risiken, ihrer Ursachen und ihrer Folgen überfordert. Dadurch verschiebt sich die gesamte Betrachtungsweise von den einzelnen Ressorts zu einem zwingend erforderlichen ganzheitlichen Ansatz.

Diese Überlegungen lassen sich auf den internationalen Kontext übertragen. Längst sind die Staaten nicht mehr die alleinigen und ausschlaggebenden Akteure im internationalen System. Sie sind nicht mehr in der Lage, ihre Politik alleine um- und durchzusetzen. Sie sind voneinander sowohl räumlich, institutionell als auch funktional abhängig – Regierungen, Wirtschaften und Gesellschaften gleichermaßen. Deren Interesse an Sicherheit und Prosperität kann nur noch in der Zusammenarbeit gewährleistet werden.

Der ressortübergreifende Ansatz *Vernetzter Sicherheit* geht von einem gesamtstaatlichen Verständnis der Sicherheitspolitik aus, in dem die sicherheitsrelevanten staatlichen und nichtstaatlichen Akteure gleichermaßen beteiligt sind. *Vernetzte Sicherheit* will das Entstehen von Risiken und Bedrohungen durch präventive Maßnahmen verhindern. In einem ganzheitlichen Ansatz sollen zahlreiche interdependente bzw. zu vernetzende Kooperations- und Gestaltungsinstrumente zur Anwendung kommen: Politische, militärische, polizeiliche,

nachrichtendienstliche, wirtschaftliche, soziale, bildungspolitische, kulturelle, informations- und kommunikationstechnische, ökologische sowie jene aus dem breiten Wirkbereich der inneren Sicherheit. Hierzu muss die Konzeptidee der *Vernetzten Sicherheit* Zug um Zug zu einem tragfähigen sicherheitspolitischen Konzept sowie zu einem überzeugenden Leistungsmerkmal von deutschen Sicherheitskräften und -akteuren entwickelt werden.

In der NATO ist das übergreifende Konzept der Vernetzten Sicherheit als „Comprehensive Approach" mittlerweile Grundlage für die Einsätze in Afghanistan und auf dem Balkan. Es sieht danach aus, dass "Vernetzte Sicherheit" zum Kern einer weiterentwickelten NATO-Strategie werden könnte BK Merkel unterstrich in Ihrer Regierungserklärung vom 26.03.09 zum NATO-Gipfel in Kehl: *„Die Nato ist Teil einer vernetzten Sicherheit. Dieser von Deutschland seit Jahren verfolgte Ansatz hat sich bewährt. "* Implizit wird auf diesem Weg das Gewicht Europas in der transatlantischen Allianz verstärkt, denn es werden vermehrt zivile Beiträge gebraucht, die nur die Europäische Union beisteuern kann Ein Zusammenrücken von NATO und EU wird absehbar. Beide Organisationen werden auf die Stakeholder der Public Private Security zurückgreifen.

Im Verbund erfolgreich

Die meisten Akteure haben in den vergangenen beiden Jahrzehnten erfahren – und erkennen inzwischen auch an –, dass sie nur im Verbund ihre jeweiligen Zielsetzungen erreichen können. So ist eine wichtige Zielsetzung der *Vernetzten Sicherheit,* die Kohärenz des Denkens und Handelns im Politikfeld Sicherheit durch eine neue Form der Zusammenführung vorhandener Mittel und Fähigkeiten zu verbessern. Der Schlüssel zum Erfolg liegt im synergetischen Zusammenwirken der relevaten Akteure und Instrumente. Dabei ist das Militärische nur ein Mittel im Verbund. Die gestiegene Komplexität zwingt zu einer neuen, ganzheitlichen sicherheitsbezogenen Problemwahrnehmung – Sicherheitspolitik als lernendes System.

Der Prozess der sicherheitspolitischen Transformation muss permanent Antworten auf die sich verändernden Herausforderungen suchen, die der globale gesellschafts- und sicherheitspolitische Wandel mit sich bringt. Die Transformation des Sicherheitssektors betrifft v.a. die zivilen Sicherheitsinstitutionen. Ohne deren Leistungsfähigkeit geht es nicht. Deshalb müssen deren Einsatzdoktrinen, Prozessen, Strukturen, Fähigkeiten sowie Ausrüstung für die neuen, veränderten Aufgabenstellungen fit gemacht werden. Gerade zivile und krisenpräventive Instrumente wie auch Maßnahmen der Friedensstützung und des post-Konfliktaufbaus gewinnen an sicherheitspolitischen Stellenwert.

Darüber hinaus müssen sich auch Industrie und Wirtschaft auf erhebliche Veränderungen einstellen:

- Die konvergierenden Aufgaben der inneren wie äußeren Sicherheit erfordern eine neuartige Sicherheitsarchitektur, gekennzeichnet durch konsequent ressortübergreif-

ende Vernetzung aller staatlichen und nichtstaatlichen Akteure. Das Zusammenwirken der Schlüsselakteure aus allen Bereichen der Gesellschaft wird unabdingbar.

- Moderne (vernetzte) Operationsführung erfolgt in allen Sicherheits- und Geschäftsfeldern um ein Vielfaches vernetzter.
- Die Befähigung zur Selbstsynchronisierung weitgehend autonom handelnder Elemente (*"Power to the Edge")* [1] gewinnt an Bedeutung – ganz im Sinne der deutschen Auftragstaktik. Dies gilt nicht nur für das militärische, sondern auch für das zivile und das industrielle Umfeld.
- Das Spektrum, die Leistung und die Art einzusetzender intelligenter Sensoren und Wirkmittel/Instrumente erweitern sich rapide. Entscheidend ist die angestrebte Wirkung. Von dieser aus wird zurückgerechnet: Was muss ich tun, damit ich die beabsichtigte Wirkung erziele?
- Die Anforderungen an Informationsbedarf, -management und -sicherheit steigen drastisch.
- Innovation und Tempo sind die Schlüssel für moderne Sicherheitskonzepte und zugleich die Antwort auf zunehmend asymmetrische Bedrohungslagen. Innovation und Tempo werden damit auch zur notwendigen Voraussetzung für Prosperität und Überleben von Gesellschaft, Unternehmen und nicht zuletzt Streitkräften.
- Existierende Budgetzwänge zwingen zu einer Balance von sinnvollem Einsatz leistungsfähiger *„Legacy-Systems“* einerseits und neuartiger *„Disruptive Technologies“* andererseits.
- Die Komplexität moderner "*System of System*"-Lösungen lässt sich nur im Zusammenwirken von Bedarfsträgern und Bedarfsdeckern, Industrie und Forschung (aller Stakeholder) bewältigen. Hierzu sind neue Wege zu gehen. Diese stehen zu dem in Streitkräften, Sicherheitskräften und Industrie gewohnten Denken sowie zu den bekannten, klassischen Lösungen oft in direktem Widerspruch.

Die Vielzahl der Akteure, das Ressortprinzip und nicht zuletzt das Föderalismusprinzip erschweren den sicherheitsrelevanten politischen Akteuren die Koordination und Kooperation. Inhaltlich führen unterschiedliche konzeptionelle Ansätze und Vorgehensweisen verschiedener Ressorts bereits auf nationaler Ebene zu voneinander abweichenden Handlungsansätzen. Sie setzen sich bei der Lagebeurteilung und den einzusetzenden Kräften vor Ort bzw. auch in internationalen Gremien fort. Hinzu kommt ein den eigenen Ressortkontext bevorzugender Fokus, der die vor dem eigenen Erfahrungshintergrund wahrgenommenen Notwendigkeiten priorisiert und demgegenüber Erfahrungen und Notwendigkeiten anderer Ressorts weniger berücksichtigt. Gefahrenlagen werden unterschiedlich interpretiert. Dies resultiert in konträren Problemlösungs- und Handlungsstrategien.

Demgegenüber bieten die wachsenden, intensiven, gemeinsamen Einsatzerfahrungen – die zwangsläufig gemeinsame Anwesenheit im Krisengebiet – bei nationalen und internationalen Einsätzen sowie eine wachsende Kultur kooperativer Entscheidungsfindung einen wichtigen Anknüpfungspunkt für einen gemeinsamen Implementierungsansatz.

[1] Alberts, David. S. ; Hayes, Richard E.: Power to the Edge, Command … Control … in the Information Age, Washington 2003

Militärische Aspekte

Die Integration technischer und wissenschaftlicher Innovation in die Streitkräfte ist für zeitgemäße Streitkräfteplanung unausweichlich. Die vorhandenen Konzepte, Strukturen, Prozesse und Instrumente müssen dem jeweiligen Stand von Wissenschaft und Technik entsprechen, um jene Fähigkeiten zu generieren, die Streitkräfte zur effektiven und zugleich auch effizienten – in Zeiten knapper Kassen ist dieser Punkt nicht unwesentlich – Auftragserfüllung brauchen.

Für eine erfolgreiche Transformation sind Wirtschaft, Wissenschaft und Technologie entscheidende Treiber der Streitkräfteentwicklung, denn sie befördern diese mit ihrem innovativen Potenzial. Der verstärkte Rückgriff auf zivile und kommerziell verfügbare Technologien fördert darüber hinaus insbesondere jene Anwendungen und Lösungen, die zur Überwindung der Grenzen zwischen innerer und äußerer Sicherheit beitragen und dadurch die Herausbildung einer vernetzten, ressortübergreifenden Sicherheitspolitik unterstützen.

Die Rahmenbedingungen sind herausfordernd, denn die Bundeswehr:

- hat keine zusätzlichen Budgetmittel zur Finanzierung der Transformation und kann nur durch Einsparungen an anderer Stelle die erforderliche Finanzierung der Transformation sicherstellen,
- wählt seit Einführung eines neuen Verfahrens zur Planung und Beschaffung neuer Ausrüstung (CPM) ihre Lieferanten auf Systemebene aus. Komponentenhersteller müssen neue Wege finden, um ihre Produkte an die Bundeswehr zu verkaufen.
- ist Verpflichtungen zur Bereitstellung von Streitkräftekontingenten für den Einsatz in multinationalen Einsätzen eingegangen,
- hat die Verpflichtung, die Planung an die finanziellen Gegebenheiten anzupassen,
- hat durch Mittelbindung für Großvorhaben über die nächsten Jahre praktisch keine finanziellen Freiräume für neue Investitionen,
- muss schwer planbaren Mittelbedarf für Auslandseinsätze und den materiellen Sofortbedarf für solche Einsätze bereitstellen können.

Da die staatlichen Sicherheitsinstitutionen oftmals allein nicht die Problemursachen und mögliche Lösungen im Voraus erkennen und benennen können, erfordert Transformation eine neue Kooperationskultur mit Industrie, Wirtschaft und Wissenschaft. Militärische Planer und Ingenieure der unterschiedlichsten Fachrichtungen, Techniker, Systemanalytiker und Operations-Research Fachleute, Haushälter, Informationsverarbeitungspersonal aus Ministerien, Wirtschaft, Forschung und Dienstleistungsbereichen, Truppe und Ämter Streitkräfte und kommerzielle Anbieter, Rüstungsindustrie, Wissenschaft und Forschung müssen hierzu in leistungsfähige, auftragsgerechte Netzwerke integriert werden, die so ausgelegt sind, dass sie im Gegensatz zu den vorhandenen Systemen fortlaufend weiterentwickelt werden können.

Verschwimmende Grenzen

Die innere Sicherheit zu gewährleisten, ist eine Kernaufgabe des demokratischen Rechtsstaates. Hierauf gründet ein wesentlicher Teil seiner Legitimation. Spätestens seit den Terroranschlägen vom 11. September 2001 verschwimmen die Grenzen zwischen innerer und äußerer Sicherheit und damit zwischen Innen- und Außenpolitik zunehmend. Im Äußeren sind polizeiliche Stabilisierungskräfte mit militärischen Fähigkeiten bei internationalen Interventionen in instabilen Weltregionen und „failing states“ auf eine neue Art zu verzahnen.

Im Inneren erfordern neue Bedrohungsformen Fähigkeiten zu deren Abwehr, die eine intensivere Zusammenarbeit als bisher im Rahmen der Amtshilfe (Art. 35 GG) erfordern.

Im Rahmen des Aufbaus rechtsstaatlicher Sicherheitsstrukturen in Krisenregionen, steht das Innenministerium als Teil einer vernetzten, ressortübergreifenden Außen- und Sicherheitspolitik vor wachsenden Anforderungen. Engagement ist für die Nachhaltigkeit erfolgreicher Stabilisierungspolitik entscheidend. Die modernen Bedrohungen erfordern heute polizeiliches Handeln auch außerhalb der deutschen Grenzen. Im Rahmen des sogenannten „Capacity Building", also dem Aufbau rechtsstaatlicher Sicherheitsstrukturen in Krisenregionen, steht das Bundesministerium des Innern als Teil einer ressortübergreifenden deutschen Außen- und Sicherheitspolitik vor wachsenden Anforderungen.

Asymmetrische Konflikte und neue Kriege zeichnen sich durch lang anhaltende Destabilisierungen ganzer Großregionen aus. Hinzu kommen neue symmetrische Herausforderungen, beispielsweise technologische Aufrüstung besonders im IKT-Bereich z.B. „Cyber war". Die Privatisierung des Krieges löst die Unterscheidung von innerer und äußerer Sicherheit sowie von Krieg und Frieden zunehmend auf. Organisierte Kriminalität etabliert sich zwischen Revolutionären und Freiheitskämpfern, zwischen dem Guerillakrieg gegen militärische Strukturen und dem Terrorismus gegen zivile Strukturen, zur Durchsetzung wirtschaftlicher Interessen – mit destabilisierenden Folgen für die globalisierte Weltwirtschaft (Drogen, illegale Migration). Nichtstaatliche Akteure wie Terroristen, Banden, Warlords und Kriegsunternehmer dominieren das moderne Gefechtsfeld. Deren vielschichtige und komplizierte wechselseitige Abhängigkeiten und Beziehungen zur Bevölkerung prägen die Einsatzrahmenbedingungen.

Gleichzeitig muss sich gerade das Innenministerium in besonderem Maße auf die transnationalen Bedrohungen wie Terrorismus, Proliferation und organisierte Kriminalität einstellen, die immer häufiger Folge zerfallener staatlicher Ordnungen sind. Hinzu kommt die zunehmende Bevölkerungskonzentration in den heimischen Städten, die – aus Sicht der Täter – als attraktives Bedrohungsziel besonderen Risiken ausgesetzt ist.

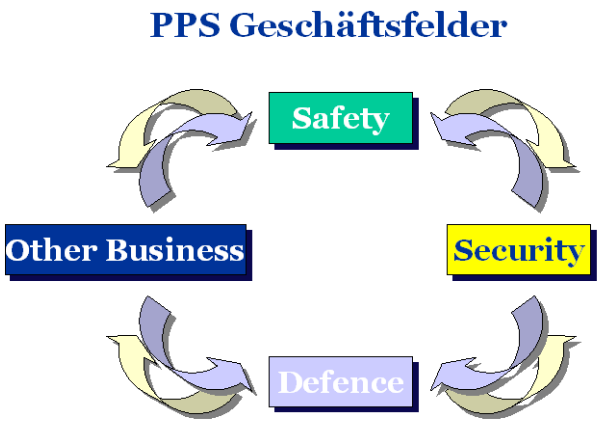
Kritische Infrastruktur

Die nationale Sicherheitsvorsorge hängt von funktionsfähigen Infrastrukturen wie Energie-, Wasser- und Informationsversorgung, Verkehrsnetzen, Lebensmittel- und Gesundheitsversorgung ab, um nur einige Beispiele zu nennen, ebenso wie vom reibungslosen Austausch wirtschaftlicher Prozesse. Unsere Gesellschaft ist darauf angewiesen, dass die gewohnte Versorgung zuverlässig funktioniert und dass die Mobilität des Einzelnen jederzeit gewährleistet ist. Doch Warenströme und Logistikketten, Versorgungsinfrastrukturen und Verkehrsleitsysteme sind verwundbar gegen Ausfälle. Diese Verwundbarkeiten machen Versorgungsinfrastrukturen zu Angriffszielen sowohl für terroristische Aktivitäten, als auch für Täter mit kriminellem Hintergrund. Sicherheitsvorsorge muss aber auch die Folgen von Naturkatastrophen oder Unfällen besonderen Ausmaßes und die Begrenzung der Schäden einschließen.

Die Informationsrevolution hat unternehmerische Abläufe drastisch beschleunigt und Produktions- bzw. Leistungserstellungsprozesse grundlegend verändert. In vielgliedrigen unternehmerischen Wertschöpfungsprozessen werden zahlreiche Akteure laufend koordiniert und aufeinander abgestimmt. Dieser ausgeprägt arbeitsteilige Prozess ist extrem störanfällig – sei es z.B. für technische Verzögerungen aufgrund des Ausfalls kritischer Infrastrukturkomponenten, durch Anschläge an wichtigen Standorten oder durch die

Unterbrechung strategisch wichtiger Versorgungswege und sei es nur durch Piraterie. Auch für die Wirtschaft wird die Sicherheitsvorsorge immer mehr zu einer Gemeinschaftsaufgabe**.** Der Schlüssel zur Bewältigung der aktuellen und künftigen Sicherheitsherausforderungen liegt dabei in der engen öffentlich-privaten Sicherheitszusammenarbeit, denn: Ohne das Know-how und die systemische Mitwirkung von Wissenschaft, Forschung und Industrie können staatliche Sicherheitskräfte ihren Auftrag nicht erfüllen; ohne das einsatzbezogene Wissen der Sicherheitskräfte bleiben wissenschaftliche und technologische Innovation ohne Wirkung.

Vernetzte Sicherheit als gesamtstaatlicher und ressortübergreifender Ansatz, der auf einem umfassenden Sicherheitsverständnis basiert, muss die verfügbaren staatlichen und privaten Mittel und Fähigkeiten derart einsetzen, dass symmetrische und asymmetrische Risiken möglichst erst gar nicht auftreten bzw. weitgehend unterbunden werden, um die Bevölkerung, die demokratischen Institutionen, die kritische Infrastruktur sowie die damit verbundenen Funktionen vor dem Eintritt der Risiken und ihren Konsequenzen zu schützen und um die Folgen eines Krisenereignisses zu lindern sowie die Rückkehr zum Ausgangszustand zu ermöglichen. Generell sollten deshalb bei Sicherheitstechnologien und -systemen die relevanten Akteure (z.B. Ministerien, Technologieentwickler, Bedarfsträger, Versicherungen, Ämter) an einem Strang ziehen. Forschung und Entwicklung, Förderung und Beschaffung müssen als untrennbar Verbund für Prosperität und Sicherheit gesehen werden. Forschung, Entwicklung und Förderung ohne Beschaffung machen keinen Sinn. Der Marktvorteil ist durch den Vorzeigeeffekt gegeben und erlaubt zugleich den heimischen Bedarfsträgern auf den neuesten Stand der Technik zurückzugreifen.



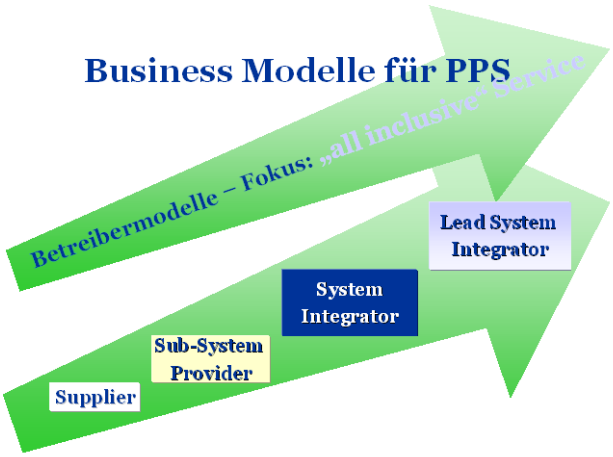
Public Private Security

Vor diesem Hintergrund entsteht der Markt für Public Private Security – ein riesiger Wachstumsmarkt. Nach Erhebungen von Roland-Berger wird der Markt für Global Security bis 2015 überdurchschnittlich wachsen. Produkte und Anbieterstrukturen entwickeln sich derzeit mit hoher Dynamik. Das Zeitfenster zur freien Gestaltung von Prozessen und Architekturen, Konzepten, Produkten und Dienstleistungen schließt sich allerdings in absehbarer Zeit. Wer sich jetzt einbringt, hat allerdings gute Chancen, Größennachteile zu kompensieren

Der Wirtschaftsfaktor Sicherheitsindustrie war schon immer ein wichtiger Baustein für die Sicherheit und Prosperität von Nationen. Neu ist im Geschäftsfeld der Public Private Security (PPS): Safety, Security und Defence lassen sich nicht länger getrennt voneinander behandeln. Die Technologien und Anwendungsoptionen gestatten mehr und mehr multifunktional ineinandergreifende Systemlösungen. Diese erfordern technologie- und ordnungspolitisch integrale Kompetenz und bedingen die ganzheitliche Förderung von Sicherheitslösungen.

Am Markt dominierten über Jahrzehnte hinweg die Anbieter proprietärer Teilsysteme. Diese Modelle laufen zusehends aus. Mit der Konvergenz der Märkte für Safety-, Security- und Defence-Produkte ergeben sich enorme Entwicklungsperspektiven und Synergieeffekte. Das gilt auch für Synergien über die Anwendung Sicherheit hinaus – Potenzial bieten hier beispielsweise Qualitätssicherung, Zuverlässigkeit und Energieeffizienz. Die Kunden wollen im Bereich Sicherheit vermehrt Systemlösungen, die verschiedene Aspekte integriert berücksichtigen. Für Unternehmen wird deren Performance im und mit Systemen zunehmend der Kern ihrer Wertschöpfung, die sich in der Begrifflichkeit des „Lead System Integrator“ trifft. Dies hat auch für die Urteilsfähigkeit des Staates und seiner Einrichtungen Bedeutung.

- Die Lead-System-Integratoren adressieren aufgrund ihrer Erfahrungen v. a. systemische Lösungsangebote zur Vermeidung von besonders kritischen Großschadensfällen. Sie übernehmen „Lead-Aufgaben“ für Regierungen, beispielsweise im Change Management für IT- und C4ISR Architekturen, für die Integration „disparater" Programme“, für „Capability-Based“ und Multi-Programm-Ansätze. Sie beraten Regierungen hinsichtlich Strategie und Risikomanagement.



- Die Systemintegratoren beschäftigen sich v. a. mit den „täglich nötigen Schutzmaßnahmen“. Sie übernehmen Program-Management-Aufgaben, die Systemintegration von Produkten, Plattformen und/oder Funktionen unter „Government Lead“, aber durchaus mit Blick auf globale Märkte. Sie adressieren komplexe Systemlösungen und sind große technologieorientierte Unternehmen der Sicherheitswirtschaft. Die meisten dieser Unternehmen agieren international und bestehen schon seit längerer Zeit am zivilen Markt. Sie kooperieren im Komponentenbereich meist eng mit dem technologieorientierten Mittelstand.

- Der technologieorientierte Mittelstand bildet die Gruppen der Subsystemlieferanten und Komponentenhersteller. In ihr sind sowohl junge wie auch etablierte Unternehmen (überwiegend kleine und mittelständische Unternehmen (KMU)) mit unterschiedlicher Affinität zu Hightech-Lösungen zu finden. Diese Gruppe greift neue Technologien auf, entwickelt innovative Lösungen und führt sie bei ausreichenden Ressourcen zu Produkten. In einigen Bereichen fehlen ihnen jedoch direkte Kundenkontakte. Hier sind sie auf die Systemintegratoren bzw. die Lead-System-Integratoren angewiesen. Ihre Produkte eignen sich für Dual-Use und globale Märkte. Sie produzieren meist für sehr verschiedene Auftraggeber.

- Die Gruppe der Dienstleister wird vor allem durch KMU und Kleinstunternehmen (ein bis zwei Personen) geprägt. Im Markt sind aber durchaus auch größere mittelständische Unternehmen und neuerdings auch multinationale Großunternehmen vertreten. Vor allem die Sicherheitsdienstleister profitieren vom Trend der Industrie und der

öffentlichen Hand, sich auf die Kernkompetenzen zu konzentrieren und Sicherheitsdienstleistungen auszulagern.

Jüngste Entwicklungen – beispielsweise in Großbritannien – belegen, dass der Staat über das Outsourcen von Systemkompetenzen seine Urteilsfähigkeit im Feld der Systemintegration riskieren kann. Paul Cornish und Andrew Dorman urteilen in den International Affair vom März 2009 vernichtend*: „Wir kommen daher zu dem Schluss, dass die Verteidigungskonzepte, Planung und Analyse im Vereinigten Königreich den Status des organisatorischen, bürokratischen und intellektuellen Verfalls (decay) erreicht haben"*. Nach ihrem Urteil ist Großbritannien im Outsourcen und in der Abstützung auf industrielle Expertise zu weit gegangen. Dies erweise sich nun als problematisch, da Lücken in der Urteilsfähigkeit die Diskrepanz zwischen Regierungsvorgaben, Einsatz bezogenen Konzepten und verfügbaren Haushaltsmitteln nicht länger zu übersehen sind.

Selbstverständlich darf sich der Staat weder in der Beschaffung noch in der Systemkompetenz von Beratungsunternehmen abhängig machen. Der Staat kann seiner Verantwortung für das Gesamtsystem einschließlich der Sicherheit seiner Bürgerinnen und Bürger nur gerecht werden, wenn er das nationale Sicherheitssystem als Ganzes länger eigenständig urteilsfähig überblickt. Systemfähig und urteilsfähig – das ist die Herausforderung für alle Akteure der *Vernetzen Sicherheit*.

Wo bleibt der Netzwerkdirigent?

Terroristische Bedrohungen und Piraterie, Wirtschaftsspionage und zerfallende Staaten u.a.m. führen weltweit zu wachsender Nachfrage nach Sicherheitslösungen. Die Konvergenz der Märkte für Safety-, Security- und Defence-Produkte eröffnet zusätzliche Entwicklungsperspektiven. Produkte, Anbieter- und Nachfragestrukturen entwickeln sich mit großer Dynamik. Kunden wollen ganzheitliche und flexible Systemlösungen, die unterschiedliche Sicherheitsaspekte, Produkte und Dienstleistungen integriert berücksichtigen. Der Sicherheitsmarkt befindet sich im Umbruch.

Die Stakeholder sollen in und für Deutschland Chancen nutzen, Risiken begrenzen und Netzwerke bilden. Doch: Wo bleibt der Netzwerkdirigent?

Längst sind deutsche kritische Infrastrukturen (KI) sowie deren Schutz zu 80 % in unternehmerischen Händen. Der Handlungsbedarf ist groß:

- Ein gemeinsames Öffentlich-Privates Lagebild zum Schutz von KI gibt es nicht.
- Öffentliche Auftraggeber achten weniger auf Innovation und Qualität, sondern primär auf Kosten. In der Sicherheitsforschung sind sie als Bedarfsträger unterrepräsentiert.
- Nationale Leuchtturmprojekte gibt es nicht.
- Die Beteiligung an europäischer Sicherheitsforschung erfolgt unter Standard.
- Die Exportförderung hat „Sicherheit" (noch) nicht als Wachstumsmarkt entdeckt.
- Die Großindustrie ist im globalen zivilen Sicherheitsmarkt (noch) wenig schlagkräftig.
- Der Mittelstand hinkt – bei beachtlicher Innovation und Kompetenz – seinen internationalen Wettbewerbern hinterher.
- Wissenschaft & Forschung tun sich schwer, Technologie von angewandter Forschung in den Markt zu transferieren.

Die veränderten Sicherheitsherausforderungen verlangen nach Lösungen jenseits der klassischen Trennung von innen und außen, von staatlicher und privater Zuständigkeit sowie der von den jeweiligen Akteuren eingesetzten Mittel und Fähigkeiten. Sie verlangen die Vernetzung der Akteure, darüber hinaus aber auch einen Netzwerkdirigenten, der mit Blick auf deutsche Sicherheit und Prosperität alle Stakeholder an einem Strang ziehen lässt.

Sein Aufgabenportfolio ist enorm, denn hierzu ist

- die Sicherheitswirtschaft als eine wettbewerbsfähige Branche in den Bereichen Safety, Security und Defence zu etablieren bzw. weiter zu entwickeln,
- Wachstums- und Beschäftigungspotenzial konsequent zu nutzen,
- die dazu erforderliche institutionelle Entwicklungsinfrastruktur zu gestalten,
- die bisherige Vernetzung der Beteiligten zu vertiefen,
- die vorhandene Forschungskompetenz sowie das industrielle Umfeld bestmöglich einzubinden.

Die industriellen und staatlichen Verantwortungsträger sind in die Pflicht zu nehmen, nicht nur die Forschung von sicherheitsbezogenen Fähigkeiten voranzutreiben, sondern diese auch tatsächlich zu beschaffen und zu nutzen. Dabei hat jeder Akteur die auf seine Rolle bezogenen Aufgaben zu erfüllen:

- Regierung und Behörden als Regelsetzer, Dirigent, Bedarfsträger, Förderer und Beschaffer;
- Industrie und Wirtschaft als Anbieter, Finanzier und Nachfrager von Sicherheitslösungen sowie als Betreiber sicherheitsrelevanter Dienstleistungen und Infrastrukturen;
- Forschung und Wissenschaft als Motor innovativer Lösungen von morgen und Ausbilder qualifizierten, wissenschaftlich gebildeten Fachpersonals

Die anhaltende Weltfinanz- und Weltwirtschaftskrise wird die Umsetzungsproblematik verschärfen. Zu erwarten sind Streichungen in den Haushalten aller Ministerien. Auch PPP Projekte kommen unter Druck, da es unter den aktuellen Umständen außerordentlich schwierig ist, Geldgeber zu finden. In Einzelfällen wird dies dann der Regierungshaushalt übernehmen müssen, was den klammen Haushalt zusätzlich belastet. Auch die bereits eingegangenen PPP Projekte könnten sich als eine erhebliche Belastung für zukünftige Haushalte darstellen.

Die vertraute Trennschärfe von technischer Sicherheit, innerer Sicherheit und Verteidigung gibt es nicht mehr. Stakeholder vernetzen sich – Staat, NGOs, Wirtschaft, Industrie, Wissenschaft und Gesellschaft. Sicherheitskräfte und „First Responder“ brauchen das Know-how von Wissenschaft, Forschung und Industrie für ihre anspruchsvollen Aufgaben. Einsatzerprobt lassen sich deren Systeme wiederum weltweit besser vermarkten. Die synergetische Vernetzung von Wissen und Hochtechnologie bestimmt zunehmend die Zukunft von Sicherheit und Prosperität. Es ist viel zu tun. Aber es lohnt sich.

****

Anmerkung: Der Beitrag gibt die persönliche Meinung des Autors wieder.

Ralph Thiele

Oberst i.G. Ralph Thiele ist Vorstand der Politisch-Militärischen Gesellschaft (PMG) Berlin.