BDI
Bundesverband der
Deutschen Industrie e.V.

Grundsatzpapier

Sicherheit für das Industrieland Deutschland

Vorwort

Sicherheit ist in jeder Gesellschaft für Wohlstand, politische und soziale Stabilität von grundlegender Bedeutung.

Globalisierung und technischer Fortschritt eröffnen dem Industrieland Deutschland hervorragende Chancen. Sie bergen aber auch neue, komplexe Sicherheitsherausforderungen. International vernetzte Wertschöpfungsketten und Infrastrukturen werden zunehmend verwundbar für Angriffe und Störungen Dritter.

Die Bewältigung aktueller und künftiger Sicherheitsherausforderungen bedarf deshalb eines gesamtgesellschaftlichen, alle relevanten Sicherheitsfacetten erfassenden Sicherheitsverständnisses. Gemeinsame Sicherheitsinteressen und die Mittel zu ihrer Verfolgung müssen durch Politik, Wirtschaft und Gesellschaft definiert und ausgestaltet werden. Dabei muss die sicherheitspolitische Rolle und der bedeutende Beitrag der deutschen Industrie zu unser aller Sicherheit stärker berücksichtigt werden.

Die deutsche Industrie übernimmt bereits heute im Bereich des Wirtschaftsschutzes, der Cybersicherheit und der Sicherheit in Handels- und Logistikketten die primäre Verantwortung für ihren Eigenschutz, den Schutz ihrer Mitarbeiter und für die Sicherheit der durch sie betriebenen 90 Prozent aller Infrastrukturen. Als Hersteller leistungsfähiger Sicherheitstechnologie ist sie zudem für die sicherheitspolitische Handlungsfähigkeit und Souveränität unseres Staates unerlässlich.

Der BDI legt mit diesem Grundsatzpapier »Sicherheit für das Industrieland Deutschland« erstmals einen Gesamtüberblick über die aus Sicht der deutschen Industrie wichtigsten Herausforderungen im Themenkomplex Sicherheit mit konkreten Handlungsempfehlungen vor.

- Wirtschaftsschutz in der deutschen Industrie stärken
- IT- und Cybersicherheit erhöhen
- Schutz internationaler Handel- und Logistikketten gewährleisten
- Rahmenbedingungen der Sicherheits- und Verteidigungsindustrie verbessern

Unser Ziel ist es, einen konstruktiven Beitrag für die erforderliche Entwicklung eines gemeinsamen Sicherheitsverständnisses von Staat, Wirtschaft und Gesellschaft zu leisten. Die Politik ist gefordert, gemeinsam mit der Industrie die dargelegten Vorschläge in einen ganzheitlichen Ansatz zur Stärkung der Sicherheit Deutschlands zu überführen und umzusetzen.

Claus Günther
CEO Diehl Defence Holding GmbH
Vorsitzender des
Ausschusses für Sicherheit
Bundesverband der Deutschen Industrie e.V.

Dr. Markus Kerber
Hauptgeschäftsführer und
Mitglied des Präsidiums
Bundesverband der Deutschen Industrie e.V.

Executive Summary

Vorwort ... 3

I. Wirtschaftsschutz in der deutschen Industrie stärken ... 6
1. Ausgangslage und Herausforderungen ... 6
1.1 Verständnis der deutschen Industrie von Wirtschaftsschutz ... 6
1.2 Steigende Sicherheitsrisiken ... 6
1.3 Wirtschaftsschutz ist primäre Verantwortung der Unternehmen ... 6
1.4 Fehlende Kohärenz bei staatlichen Unterstützungsmaßnahmen ... 7
2. Handlungsempfehlungen ... 8
2.1. Ausarbeitung eines »Nationalen Konzepts für Wirtschaftsschutz« ... 9
2.2 Gründung einer Dachinitiative »Allianz für Wirtschaftsschutz« ... 8
2.3 Benennung einer zentralen Ansprechstelle für Wirtschaftsschutzfragen ... 8

II. IT- und Cybersicherheit erhöhen ... 9
1. Ausgangslage und Herausforderungen ... 9
1.1 Digitale Vernetzung: Rückgrat der modernen Informationsgesellschaft ... 9
1.2 Umfassende Vernetzung birgt auch Risiken ... 9
1.3 Hohes Eigeninteresse der Unternehmen an sicheren IT-Systemen ... 10
2. Handlungsempfehlungen ... 11
2.1 Prävention durch Aufklärung ... 11
2.2 Enge Kooperation zwischen Staat, Industrie und Gesellschaft ... 11
2.3 Freiwilligkeit vor Meldepflicht ... 11
2.4 Internationale Zusammenarbeit ausbauen ... 12

III. Schutz internationaler Handels- und Logistikketten gewährleisten ... 13
1. Ausgangslage und Herausforderungen ... 13
1.1. Die Bedeutung sicherer Handels- und Logistikketten für die deutsche Industrie ... 13
1.2. Heterogene Sicherheitsanforderungen ... 13
1.3. Fehlende Kohärenz bei Sicherheitsregularien und -standards ... 14
1.4. Grenzüberschreitende Zusammenarbeit mit Strafverfolgungs-, Zoll- und Sicherheitsbehörden ... 14
2. Handlungsempfehlungen ... 14
2.1. Verbesserung der internationalen Sicherheitskooperationen ... 14
2.2 Weiterentwicklung internationaler Sicherheitsstandards ... 15

IV. Rahmenbedingungen der Sicherheits- und Verteidigungsindustrie (SVI) verbessern ... 16
1. Ausgangslage und Herausforderungen ... 16
1.1. Die Bedeutung der Sicherheits- und Verteidigungsindustrie (SVI) ... 16
1.2. Markt- und Industriestrukturen ... 16
1.3. Sinkende Beschaffungsbudgets in Deutschland und Europa ... 16
1.4. Beschaffung in Deutschland ... 16
1.5. Europäischer Beschaffungsmarkt ... 17
1.6. Globale Märkte/Exporte ... 17
1.7. Forschung und Technologie (F&T) ... 17
2. Handlungsempfehlungen ... 17
2.1. SVI ist strategischer Bestandteil der nationalen Sicherheitsvorsorge ... 17
2.2. Stärkung und Erhalt der Innovationskraft und des Know-hows ... 17
2.3. Förderung des Außenhandels ... 18
2.4. Beschaffung national und EU-weit ... 18

Impressum ... 19

I. Wirtschaftsschutz in der deutschen Industrie stärken

1. Ausgangslage und Herausforderungen

1.1 Verständnis der deutschen Industrie von Wirtschaftsschutz

Unternehmen können nur dort erfolgreich agieren, wo sie gegen äußere Beeinträchtigungen und Angriffe durch Dritte gesichert sind. Der Schutz zentraler Unternehmenswerte in Form von Mitarbeitern, Know-how, Vermögenswerten und Betriebsstätten im In- und Ausland ist daher unabdingbar. Dies ist die Aufgabe des Wirtschaftsschutzes.

Wirtschaftsschutz ist zu definieren als die Summe aller Maßnahmen von Politik, Behörden und Wirtschaft zur Minimierung von Sicherheitsrisiken für die Unternehmen.

1.2 Steigende Sicherheitsrisiken

Die Sicherheitsrisiken für die deutsche Industrie im Bereich des Wirtschaftsschutzes sind vielfältig: Wirtschafts- und Industriespionage, organisierte Kriminalität, Terrorismus oder auch die Auswirkungen von Katastrophen. Diese nehmen im Zuge der Globalisierung und des technischen Fortschritts an Komplexität zu.[1] Selbst räumlich weit entfernte Ereignisse können sich angesichts international verflochtener Wirtschaftsprozesse binnen kürzester Zeit unmittelbar auf deutsche Unternehmen nachteilig auswirken.

Der allein durch illegale Wissensabschöpfung jährlich entstehende volkswirtschaftliche Schaden wird von Sicherheitsexperten im zweistelligen Milliardenbereich veranschlagt, wobei das genaue Ausmaß aufgrund der hohen Dunkelziffer an Vorkommnissen nicht ermittelbar ist. Laut jüngsten Studien sind in den vergangenen fünf Jahren rund ein Drittel der deutschen Industrieunternehmen Opfer von Industriespionage geworden. Klein- und mittelständische Unternehmen (KMU) waren dabei besonders häufig betroffen. Die Angriffe auf das Unternehmens-Know-how erfolgen vorwiegend über eigene Mitarbeiter, ausländische Geschäftspartner und in einem stark zunehmenden Maße über das Internet/IT-Netzwerke.

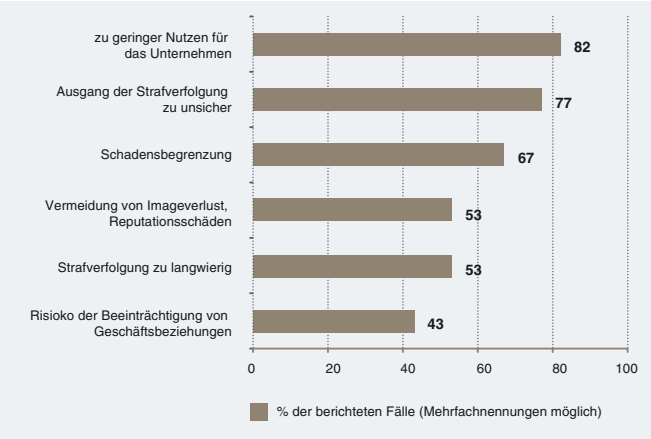
1.3 Wirtschaftsschutz ist primäre Verantwortung der Unternehmen

Ihre Unternehmenswerte hiergegen zu schützen, ist seit jeher die primäre Verantwortung der Industrie. Dies geschieht im besten Fall präventiv. Da es infolge der Komplexität möglicher Szenarien jedoch keine 100-prozentige Sicherheit geben kann, ist im Ernstfall die frühzeitige Begrenzung von Schäden entscheidend. Infolgedessen wächst neben der Prävention der Stellenwert eines international handlungsfähigen Krisenmanagements.

Global Player und größere Mittelstandsunternehmen verfügen über professionelle Sicherheitsabteilungen. Diese bilden mit ihrem Know-how und internationalen Sicherheitsnetzwerken den Grundpfeiler für die Sicherheit in der deutschen Wirtschaft und der kritischen Infrastrukturen. Ein nach wie vor hoher Handlungsbedarf im Bereich des Wirtschaftsschutzes existiert vor allem bei kleinen und mittelständischen Unternehmen (KMU). Hier gilt es, die Unternehmen für Gefährdungen und Sicherheitsrisiken zu sensibilisieren. Zusätzlich ist das erforderliche Wissen

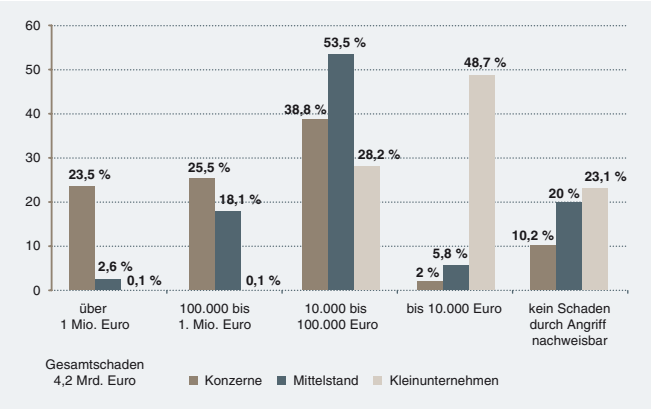
1 Quellen: SiFo-Studie 09/10 »Know-how-Schutz in Baden Württemberg«; CorporateTrust »Industriespionage 2012«

Gründe für das Unterlassen von Strafanzeigen



Quelle: SiFo-Studie 2009/10

Schäden durch Wirtschaftsspionage nach Unternehmensgröße in Deutschland im Jahr 2011



Quelle: Corporate Trust 2012

für die Identifizierung von Sicherheitsrisiken und die Umsetzung eines geeigneten Präventions- und Krisenmanagements gemeinsam durch Staat und Industrie zu stärken.

Eine vertrauensvolle Zusammenarbeit zwischen Industrie und Staat erfordert entsprechende Kenntnisse in den Unternehmen über behördliche Abläufe und Unterstützungsmöglichkeiten. Befragungen zeigen, dass acht von zehn Unternehmen von einer Anzeige entsprechender Sicherheitsvorkommnisse absehen, da sie mögliche Konsequenzen nicht abschätzen können. Sie befürchten, im Kontext der staatlichen Ermittlungen mit einem öffentlichen Reputationsverlust, Regressforderungen seitens der Kunden und ggf. strafrechtlichen Folgen konfrontiert zu werden.

Politik und Staat sind daher gefordert, bedarfsgerechte Unterstützungsangebote sowie vertrauensbildende Maßnahmen noch stärker als bisher anzubieten. Das Spektrum der Hilfestellung muss vom Austausch sicherheitsrelevanter Informationen bis hin zu einem pragmatischen Zusammenwirken beim internationalen Krisenmanagement reichen. Zusätzlich ist die Sensibilisierung von Öffentlichkeit und Unternehmen für Fragen des Wirtschaftsschutzes zu intensivieren.

1.4 Fehlende Kohärenz bei staatlichen Unterstützungsmaßnahmen

Zwar existieren mit dieser Zielsetzung eine Vielzahl an staatlichen und privaten Wirtschaftsschutzinitiativen auf Bundes- und Landesebene, jedoch fehlt ihnen ein abgestimmter, kohärenter Handlungsrahmen. Auch die für eine vertrauliche und freiwillige Kooperation notwendigen rechtlichen Grundlagen sind außerhalb des Geheim- und vorbeugenden Sabotageschutzes unklar oder erschweren einen Austausch. Daher findet eine Zusammenarbeit oftmals nur auf informeller Ebene statt.

Kontakt- und Austauschmöglichkeiten brauchen feste, eindeutige Ansprechpartner und Zuständigkeiten. Die föderale Sicherheitsarchitektur unseres Landes wird diesem Anspruch nur teilweise gerecht. Vor allem wenn es im Ernstfall auf zügiges Handeln ankommt, führen nicht immer eindeutige Zuständigkeiten und unterschiedliche Verfahrensabläufe zu einem immensen Zeit- und Verwaltungsaufwand.

Für international tätige Unternehmen stellen darüber hinaus die unterschiedlichen Vorschriften und Verfahren in den jeweiligen Staaten in und außerhalb der EU eine Herausforderung für die Unternehmenssicherheit dar. Die Anpassung und Umsetzung der nationalen Regularien ist aufwendig, zeitintensiv und somit kostspielig. Ziel der Politik muss es sein, durch eine Harmonisierung der gesetzlichen Regelungen zumindest auf EU-Ebene das Sicherheitsniveau in der Industrie zu stärken.

2. Handlungsempfehlungen

2.1 Ausarbeitung eines »Nationalen Konzepts für Wirtschaftsschutz«

Eine nachhaltige Stärkung des Wirtschaftsschutzes in Deutschland – und davon ausstrahlend in der EU – erfordert ein gemeinsames Sicherheitsverständnis und gemeinsame, klare Zielsetzungen von Politik und Industrie. Es gilt, aus diesen geeignete Unterstützungsmaßnahmen abzuleiten und kohärent in den föderalen Sicherheitsstrukturen umzusetzen. In einem regelmäßigen Turnus sind Zielsetzungen und Maßnahmen auf ihre Aktualität und Zielerreichung hin zu evaluieren und ggf. anzupassen. Dieser Prozess muss gemeinsam mit der Industrie in einem »Nationalen Konzept für Wirtschaftsschutz« festgeschrieben werden. Synergien mit bestehenden (Teil-)Strategien, wie z. B. der nationalen Cybersicherheitsstrategie oder UP-KRITIS, sind – soweit sie den Wirtschaftsschutz tangieren – gezielt herzustellen und auszunutzen.

BDI-Forderungen:
Ausarbeitung eines nationalen Konzepts für Wirtschaftsschutz mit folgenden zu beachtenden Eckpunkten:

- Entwicklung eines gemeinsamen Grundverständnisses zu Inhalt und Umfang des Wirtschaftsschutzes bei Politik, Behörden und Industrie.
- Intensivere Kooperation von Staat und Industrie bei der freiwilligen Lagebilderstellung, bei Prävention und Krisenmanagement.
- Schaffung klarer rechtlicher Rahmenbedingungen für die freiwillige Kooperation und den Austausch von Staat und Industrie im Wirtschaftsschutz.
- Harmonisierung gesetzlicher Sicherheitsbestimmungen zwischen den Ländern sowie zwischen den Mitgliedsstaaten der EU.
- Schaffung klarer Zuständigkeiten und zentraler Ansprechpartner bei den Sicherheitsbehörden.
- Ausweitung der Kapazitäten und Ressourcen staatlicher Sicherheitsbehörden zur Unterstützung der Sicherheit der deutschen Industrie.
- Stärkung eines adäquaten Sicherheitsbewusstseins in Unternehmen und Gesellschaft.

2.2 Gründung einer Dachinitiative »Allianz für Wirtschaftsschutz«

Die Ausarbeitung, Koordinierung, Umsetzung und Evaluierung des »Nationalen Konzepts für Wirtschaftsschutz« kann nur in einem gemeinsamen und partnerschaftlichen Zusammenwirken auf Augenhöhe von Industrie und Politik gelingen. Dafür bedarf es eines institutionalisierten Kooperationsrahmens.

Zu diesem Zweck fordert der BDI die Bundesregierung auf, mit den Spitzenorganisationen der deutschen Wirtschaft eine dauerhafte Dachinitiative, eine »Allianz für Wirtschaftsschutz«, ins Leben zu rufen. Für die Umsetzung des »Nationalen Konzepts für Wirtschaftsschutz« sollte die Initiative weiteren Partnern auf Landesebene offen stehen.

BDI-Forderungen:
Gründung einer Dachinitiative »Allianz für Wirtschaftsschutz« zur Ausarbeitung und Umsetzung des nationalen Wirtschaftsschutzkonzepts durch Industrie und Politik.

2.3 Benennung einer zentralen Ansprechstelle für Wirtschaftsschutzfragen

Die komplexe Thematik »Wirtschaftsschutz« berührt eine Vielzahl von Zuständigkeitsbereichen bei Ressorts und Behörden. Für die Ausarbeitung und Umsetzung eines »Nationalen Konzepts für Wirtschaftsschutz« ist die Zusammenarbeit dieser staatlichen Stellen zu koordinieren und über eine zentrale staatliche Ansprechstelle auf ministerieller Ebene mit der Industrie abzustimmen.

BDI-Forderungen:
Benennung einer zentralen Ansprechstelle für Wirtschaftsschutzfragen bei der Bundesregierung.

II. IT- und Cybersicherheit erhöhen

1. Ausgangslage und Herausforderungen

1.1 Digitale Vernetzung: Rückgrat der modernen Informationsgesellschaft

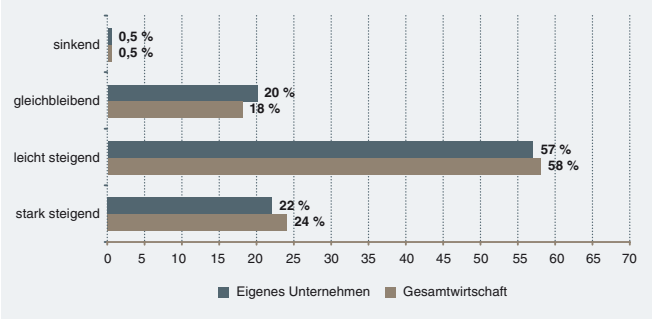
Es gibt in der globalisierten Welt heute keine Infrastruktur mehr, keinen Prozess in Wirtschaft und Politik, der ohne IT-Systeme funktioniert: Informations- und Kommunikationstechnologien sind Treiber der volkswirtschaftlichen Produktivitätssteigerung. Sie beeinflussen und prägen alle Sektoren der Wirtschaft und der Gesellschaft.

Die deutsche Industrie macht sich gerade auf den Weg in die 4. Industrielle Revolution: Wertschöpfungsketten werden digitalisiert, virtualisiert und miteinander vernetzt. Künftig können Fabriken, Unternehmen und ganze Wertschöpfungsnetzwerke in nahezu Echtzeit gesteuert werden. Die vertikale Vernetzung eingebetteter Systeme mit betriebswirtschaftlichen Prozessen bietet neben ganz neuen Geschäftsmodellen erhebliche Optimierungspotentiale in Produktion, Logistik und Vermarktung. Das gilt branchenübergreifend für sämtliche Industriebranchen in Deutschland. Dieser Prozess ist noch längst nicht zu Ende.

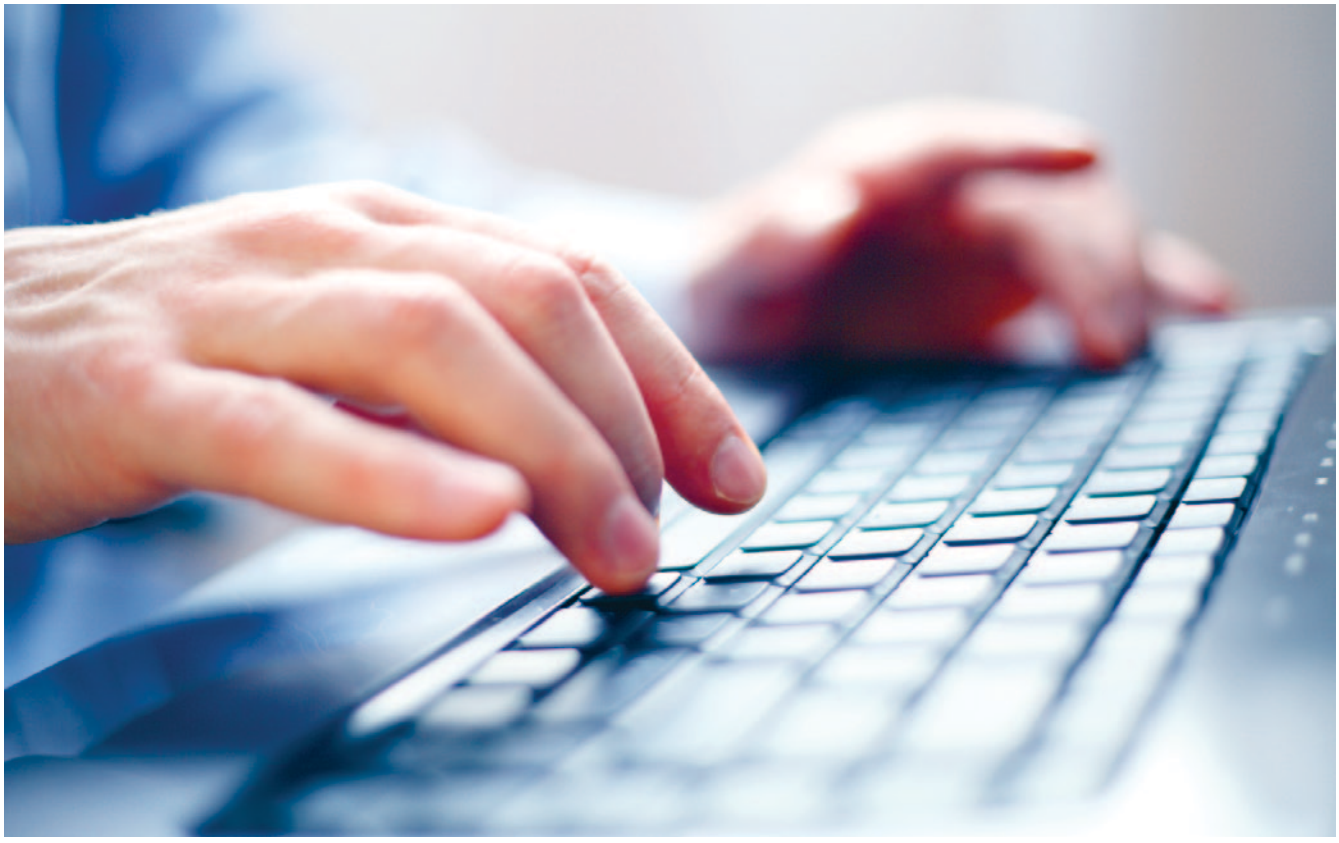
1.2 Umfassende Vernetzung birgt auch Risiken

Doch neben den unbestreitbaren Vorteilen und Synergien einer umfassenden Vernetzung stehen auch Risiken und Gefahren: Das Aufbrechen der Firmengrenzen, die Verflechtung mit Zulieferern, Dienstleistern und die starke Nutzung drahtloser Kommunikation erleichtern Angriffe auf IT-Systeme im Unternehmen.

Vergleich: Entwicklung der Cyberbedrohungen für die Wirtschaft und die Unternehmen



Quelle: BDI-Umfrage 2011



Fast täglich werden Fälle von Cyberkriminalität bekannt. Die Gefahr und der potentielle Schaden digitaler Angriffe sind enorm. Zeitlich unabhängig und grenzüberschreitend greifen kriminelle Organisationen und ausländische Nachrichtendienste zusammen deutsche IT-Strukturen an. Daten werden oftmals unentdeckt entwendet, manipuliert oder ausgespäht, technische Systeme sabotiert. Laut Bundeskriminalamt steigt die Rate der Cyberkriminalität jedes Jahr um bis zu 20 %.

Die Ausfälle bei den Unternehmen aufgrund von Cyberangriffen haben weitreichende Folgen: Allein in Deutschland werden die jährlichen Schäden für die Industrie im zweistelligen Milliardenbereich veranschlagt.

Diese Erkenntnisse sind nicht neu. Neu ist aber die Art und Weise, wie Unternehmen Cyberangriffen ausgesetzt sind, mit welcher Geschwindigkeit neue Viren entstehen und verbreitet werden: Alle zwei Sekunden wird ein neues Schadprogramm entwickelt. Angriffe werden heute gezielt durchgeführt und richten sich auf Unternehmen, Staaten oder das Militär.

Die Sicht der deutschen Industrie auf die aktuelle Cyberbedrohung wird nicht zuletzt aus einer Umfrage des BDI bei über 500 Unternehmen deutlich: Gefragt, wie sie die Bedrohungslage für ihre Unternehmen einschätzen, antworteten 75 % der Befragten mit »hoch«. Zudem gehen die Unternehmen davon aus, dass sich diese Lage in den nächsten Jahren noch deutlich verschärfen wird.

1.3 Hohes Eigeninteresse der Unternehmen an sicheren IT-Systemen

Die deutsche Industrie hat ein hohes Eigeninteresse, die Funktionsfähigkeit und Verfügbarkeit ihrer IT-Systeme nachhaltig abzusichern. Sie hat deshalb auf die stetig steigende Cyber-Bedrohungslage mit einer Vielzahl an freiwilligen Maßnahmen reagiert: Das Sicherheitsniveau wird kontinuierlich verbessert und unterliegt regelmäßigen Audits.

In einigen Branchen – wie der Telekommunikations- und Versicherungsbranche – bestehen bereits heute verschiedene und umfängliche gesetzliche Melde- und Transparenzverpflichtungen auf nationaler Ebene, denen die Unternehmen nachkommen. Im Rahmen des Umsetzungsplans KRITIS (UP KRITIS) zum Schutz der kritischen Infrastrukturen gibt es in einigen Branchen etablierte und gut funktionierende Meldeprozesse, sowohl gegenüber staatlichen Behörden als auch zwischen Unternehmen. Der Austausch der Wirtschaft untereinander wird bereits heute praktiziert – sowohl bilateral als auch im CERT-Verbund.

2. Handlungsempfehlungen

2.1 Prävention durch Aufklärung

Aufklärung über Risiken und Prävention sind das wirksamste Mittel, um IT-Strukturen vor Cyber-Angriffen abzusichern. Nur wer rechtzeitig über die Gefahrenpotenziale informiert ist, kann geeignete Gegenmaßnahmen einleiten. Dazu gehört, die Aufmerksamkeit der Unternehmen für mögliche Gefahren im Bereich Cybersicherheit zu stärken und rechtzeitig über Gefahrenpotentiale zu informieren, um geeignete Maßnahmen zu ergreifen. Wir sind davon überzeugt: Wer gut kommuniziert und proaktiv handelt, ist anderen einen Schritt voraus. Zwar gibt es keine absolute Sicherheit, wir können aber die Hürden für Angreifer höher legen.

Hier sieht sich der BDI in der Pflicht, seine Mitglieder und Unternehmen auf mögliche Risiken hinzuweisen und über Gefahren aufzuklären. Wir tun dies bereits sehr intensiv über unsere BDI-Kanäle. Insbesondere mittelständische Unternehmen müssen wir stärker erreichen.

BDI-Forderungen:

- Schaffung eines Sicherheitsbewusstseins bei Unternehmen und privaten Akteuren.
- Verbesserung des Risikomanagements der IT-Systeme in den Unternehmen:
  IT-Sicherheit muss als Mittel zur Erkennung und Minimierung von Geschäftsrisiken einen entsprechenden Stellenwert erhalten.[2]
- Ausbau der Beratungsangebote des BSI für Unternehmen und Bevölkerung.
- Umsetzung von branchenübergreifenden Mindestanforderungen für IT-Sicherheit.

2.2 Enge Kooperation zwischen Staat, Industrie und Gesellschaft

Cybersicherheit ist eine gesamtgesellschaftliche Aufgabe. Die nachhaltige Stärkung der IT-Sicherheit von Infrastrukturen muss ein gemeinsames Ziel von Industrie, Politik und Gesellschaft sein. Das beinhaltet die Akzeptanz von Sicherheitstechnik in der Öffentlichkeit und der Politik. Der Staat sollte den Rahmen schaffen und sicherstellen, dass die Abwehr von Angriffen zeitgemäß ist. Unternehmen sollten ihre IT-Systeme sicherer machen und ihre Mitarbeiter in dem Bereich sensibilisieren. Dabei ist dem Grundsatz der Selbstregulierung der Vorzug zu gewähren.

Eine schnelle Ansprech- und Reaktionsmöglichkeit ist für die Unternehmen von großer Bedeutung. Vor diesem Hintergrund begrüßt der BDI den Ausbau der bestehenden CERT-Strukturen ausdrücklich und setzt sich für eine enge Vernetzung von Industrie, Forschung und Sicherheitsbehörden auf allen Ebenen ein, um einen nachhaltigen Schutz vor Cyberangriffen zu gewährleisten.

BDI-Forderungen:

- Cybersicherheit als gesamtgesellschaftliche Aufgabe betrachten.
- Staat und Industrie müssen gemeinsam Verantwortung für eine verbesserte IT-Sicherheit übernehmen.
- Strukturierte, enge Zusammenarbeit zwischen Industrie und Sicherheitsbehörden sowie zwischen Unternehmen intensivieren, wie z. B. im Rahmen der Cybersicherheitsstrategie der Bundesregierung (Nationaler Cybersicherheitsrat, Cyberabwehrzentrum, Allianz für Cybersicherheit, Task Force IT-Sicherheit für die Wirtschaft).
- Verantwortung des Staates als Pionieranwender im Bereich IT-Sicherheit.

2.3 Freiwilligkeit vor Meldepflicht

Für ein vollständiges Lagebild brauchen wir einen freiwilligen Lösungsansatz der Industrie, um Erkenntnisgewinn und Reaktionsmöglichkeit für alle zu erhöhen. Dafür ist es notwendig, dass Unternehmen, Behörden und Nutzer Cyberangriffe freiwillig und anonym melden. Dieses Meldesystem muss durch ein Verständnis der Notwendigkeit und nicht durch regulatorischen Zwang entstehen. Ziel muss es sein, die richtige Balance zwischen Sicherheitsinteressen einerseits und unternehmerischen Freiheiten andererseits zu finden.

Aus dieser Überzeugung heraus ist die deutsche Industrie der Meinung: Eine gesetzliche Meldepflicht, wie sie disku-

2 Durch die Internetvernetzung in den Unternehmen hat die Frage von bewusster Anonymität bzw. bewusstem Umgang mit Teilen der eigenen Identität eine neue und zuvor nie gekannte Komplexitätsstufe erreicht. Im Internet wird regelmäßig mit (Teil-)Identitäten gespielt. Hierbei können und sollen Identitätsmanager helfen und die Technik transparent machen. Dies kann von der einfachen Passwort- und Zugangsverwaltung bis hin zum umfassenden situationsbezogenen Pseudonymmanagement gehen. Ziel ist stets die Vereinfachung der Internetkommunikation, ohne dass hiermit eine Verringerung der Sicherheit und des Datenschutzes einhergeht.

tiert wird, ist nicht der richtige Weg. Deshalb setzt sich der BDI in Berlin und Brüssel gegen eine bürokratische, nicht zielführende Regulierung und gesetzliche Meldeverpflichtung von Cybervorfällen für die Industrie ein.

Der BDI ist grundsätzlich der Auffassung, dass die freiwillige und vertrauensvolle Arbeit zwischen Industrie und Politik sowie Sicherheitsbehörden zu stärken ist. Bundesregierung und Behörden haben gemeinsam mit der Industrie erfolgsversprechende, freiwillige Initiativen ins Leben gerufen. Ein gutes Beispiel ist die »Allianz für Cybersicherheit«. Politik und Industrie arbeiten hier Hand in Hand beim Schutz vor Cyberangriffen. In konkreten Fällen kann so sehr schnell und effizient ein breites Netzwerk aktiviert werden. Unternehmen haben die Möglichkeit, Angriffe freiwillig und anonym an das Bundesamt für Sicherheit in der Informationstechnik (BSI) zu melden. Deutschland ist mit der Einführung eines Meldesystems für IT-Sicherheitsvorfälle internationaler Vorreiter. Die Bundesregierung sollte jetzt alles daran setzen, zunächst diese gemeinsame Initiative zum Erfolg zu führen, bevor sie zusätzliche gesetzliche Maßnahmen auf den Weg bringt.

BDI-Forderungen:
- Richtige Balance zwischen Sicherheitsinteressen einerseits und unternehmerischer Freiheit andererseits finden.
- Bereits existierende, gut funktionierende, freiwillige Meldewege weiter ausbauen.
- Politisch geforderte, zusätzliche gesetzliche Meldepflichten ablehnen.

2.4 Internationale Zusammenarbeit ausbauen

Im internationalen Kontext ist es wichtig, dass der öffentliche und private Sektor zur Erkennung und Abwehr von Bedrohungen zusammenarbeiten. Der BDI begrüßt, dass das Thema Cybersicherheit in zahlreichen internationalen Prozessen, Foren und Gremien verankert ist, wie z. B. im Europarat, in der OECD/APEC, in der OSZE, in den VN, in der NATO, der EU und der G8/G20. Dabei gilt es zu beachten, dass die Initiativen auf nationaler Ebene immer auch im europäischen und internationalen Kontext stringent sind. Doppelregulierung muss in jedem Fall vermieden werden.

Die Harmonisierung von international einheitlichen Standards ist entscheidend: Das Vertrauen in die Datensicherheit – insbesondere im Umgang mit sensiblen und unternehmenswichtigen Daten – erweist sich im Wettbewerb als entscheidender Pluspunkt. Aufgrund des hohen Niveaus der Datensicherheit hat Deutschland einen Standortvorteil, den es zu bewahren und weiter zu entwickeln gilt.

Deutschland ist als Exportnation darauf angewiesen, stabile und verlässliche Rahmenbedingungen auf Auslandsmärkten vorzufinden. Daher ist die Dringlichkeit für eine ressortübergreifende, stringente Technologieaußenpolitik zur Durchsetzung deutscher Interessen in nationalen Märkten der europäischen Union, als auch in internationalen Märkten zu formulieren. Dazu gehört, auch die IT-Sicherheitsforschung, im Sinne der Stärkung des Wirtschaftsstandortes Deutschlands, auf den relevanten Auslandmärkten strukturiert zu befördern.

BDI-Forderungen:
- Internationale Zusammenarbeit im Bereich Cybersicherheit weiter ausbauen.
- Hohe deutsche Sicherheitsstandards mit den internationalen Standards kompatibel machen: Keine nationalen Sonderwege bei der Regulierung/Standardisierung.
- Stabile und verlässliche Rahmenbedingungen auf Auslandsmärkten befördern.
- Notwendige prüffähige Mindeststandards für die Industrie werden benötigt. Somit muss eine Unterstützung von industriellen Zertifizierungs- und Prüfstellen erfolgen. Hieraus ergeben sich Entwicklungschancen für neue nationale IKT-Produkte.
- Wirksamkeit des länderübergreifenden Krisenmanagements in regelmäßigen Übungen testen.
- International einheitliche Strafverfolgung von Cyber-Kriminalität ausbauen.

III. Schutz internationaler Handels- und Logistikketten gewährleisten

1. Ausgangslage und Herausforderungen

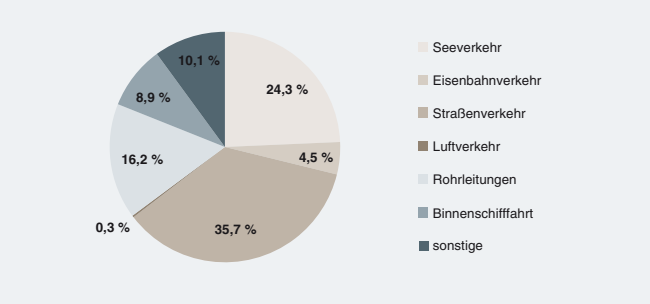
1.1 Die Bedeutung sicherer Handels- und Logistikketten für die deutsche Industrie

Handels- und Logistikketten sind die Pulsadern unserer global vernetzten Wirtschaft. Hochkomplexe und in der Regel zeitkritische Logistikprozesse zu Land, Wasser und in der Luft ermöglichen erst, dass Güter jeglicher Art rechtzeitig und effizient ihr Ziel erreichen. Ihr Funktionieren ist eine Grundvoraussetzung für eine international arbeitsteilige Wertschöpfung und damit ein entscheidender Faktor für die Wettbewerbsfähigkeit der deutschen Industrie. Der Schutz der internationalen Logistikketten und Infrastrukturen gegen zunehmende und vielschichtige Sicherheitsbedrohungen wie Terrorismus, organisierte Kriminalität oder Katastrophenszenarien liegt im nationalen Interesse Deutschlands und der EU.

1.2 Heterogene Sicherheitsanforderungen

Handels- und Logistikketten kombinieren in der Regel unterschiedliche Transportarten, -mittel, -wege und -infrastrukturen, deren jeweilige Sicherheitsrisiken und Gefahrenpotentiale signifikant variieren. Allgemein pauschale Sicherheitslösungen für sämtliche Logistikprozesse sind daher weder möglich, noch zielführend, soll der reibungslose Warenverkehr nicht unnötig und kostentreibend unterbrochen werden. Sicherheitsmaßnahmen müssen daher stets risikobasiert an den jeweiligen Prozessabläufen und Sicherheitsrisiken einzelner Logistikketten ausgerichtet werden. Es gilt unbedingt, ein Gleichgewicht zwischen den eingesetzten Sicherheitsverfahren und dem freien Handelsverkehr sicherzustellen.

Anteil der Verkehrsträger an der Güterbeförderungsmenge im deutschen Außenhandel in %



Quelle: DESTATIS

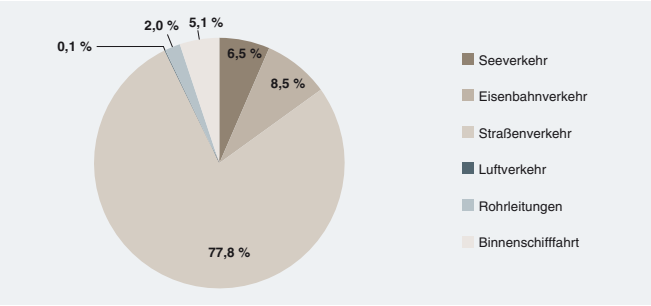
1.3 Fehlende Kohärenz bei Sicherheitsregularien und -standards

Um den heterogenen Sicherheitsanforderungen gerecht zu werden, wurden in der Vergangenheit gemeinsam durch Wirtschaft und Politik eine Vielzahl freiwilliger Sicherheitsregime, Standards und ergänzender staatlicher Sicherheitsregularien für die unterschiedlichen Logistikbereiche entwickelt und umgesetzt. Diese ermöglichen in Deutschland und der EU ein im internationalen Vergleich hohes Sicherheitsniveau. Die Sicherheitsregime, -regularien und Standards sind jedoch unzureichend aufeinander abgestimmt, ihre Umsetzung erfolgt in den EU-Mitgliedsstaaten uneinheitlich. Das gilt im stärkeren Maße auch für den internationalen Warenverkehr mit Drittstaaten. Dadurch entstehen der deutschen Industrie jedes Jahr ein enormer bürokratischer Mehraufwand und hohe Kosten.

1.4 Grenzüberschreitende Zusammenarbeit mit Strafverfolgungs-, Zoll- und Sicherheitsbehörden

Die deutsche Wirtschaft hat ein hohes Eigeninteresse, seine Güter und Einrichtungen gegen den Zugriff und Einfluss Dritter zu schützen, und übernimmt bereits seit jeher die primäre Verantwortung für die Sicherheit ihrer Logistikprozesse. Sie ist dabei auf die grenzüberschreitende Flankierung durch Politik und Strafverfolgungs-, Zoll- und Sicherheitsbehörden angewiesen. Das gilt insbesondere bei Vorkommnissen der Gefahrenabwehr, die grundsätzlich in die staatliche Zuständigkeit fallen. Es ist nicht möglich, eine 100-prozentige end-to-end Security zu erzielen. Bei der Gefahrenprävention und beim Krisenmanagement ist es daher umso wichtiger, dass Behörden und Unternehmen auf internationaler Ebene eng miteinander kooperieren. Trotz vielfältiger Unterstützungsmaßnahmen fehlt jedoch ein kohärenter Handlungsrahmen.

Anteile der Verkehrsmittel an der Güterbeförderung 2011 im Inland in %



Quelle: DESTATIS

BDI

2. Handlungsempfehlungen

2.1 Verbesserung der internationalen Sicherheitskooperationen

Das Thema Sicherheit in der Handels- und Logistikkette bedarf einer europäischen bzw. internationalen Betrachtung, da grenzüberschreitende Verkehre auf diesem Gebiet die Regel sind. Den steigenden Sicherheitsherausforderungen für unsere komplexen Logistikketten und -infrastrukturen kann daher nur in einem gemeinsamen, internationalen Ansatz von Wirtschaft und Politik wirksam begegnet werden. Die Politik muss hierfür in Abstimmung mit der Wirtschaft geeignete Rahmenbedingungen schaffen und ggf. erweitern. Freiwillige, risikobasierte und sinnvoll aufeinander abgestimmte Sicherheitsmaßnahmen, die den Anforderungen des zeitlich hochsensiblen Logistikgeschäfts gerecht werden, sind verpflichtenden regulatorischen Eingriffen in jedem Fall vorzuziehen.

BDI-Forderungen

- Verbesserung der grenzüberschreitenden Zusammenarbeit und des Informationsaustauschs zwischen Strafverfolgungs-, Zoll- und Sicherheitsbehörden auf europäischer und internationaler Ebene einerseits und der Wirtschaft andererseits.
- Gemeinsamer Aufbau und Weiterentwicklung von freiwilligen Sicherheits- und Notfallmaßnahmen (grenzüberschreitend) auf Grundlage internationaler Mindeststandards und bewährter betrieblicher Unternehmenskonzepte zum Krisenmanagement unter Wahrung der Zuständigkeits- und Verantwortungsbereiche von Staat und Industrie.
- Etablierung bzw. Ausbau länderübergreifender Expertengremien; Arbeitsprozess zur Evaluierung erfolgreicher Maßnahmen und ggf. freiwillige, gemeinsame Umsetzung durch Politik und Industrie.
- Gemeinsame Schulungs- und Sensibilisierungsprogramme für Mitarbeiter durch Behörden und Unternehmen; EU-weite Anerkennung entsprechender Qualifizierungen.

2.2 Weiterentwicklung internationaler Sicherheitsstandards

International anerkannte und harmonisierte Sicherheitsstandards bilden die Grundlage für einen sicheren und nahtlosen Warenverkehr im Rahmen grenzüberschreitender Handels- und Logistikketten. Sie können unnötige Doppelungen von Sicherheitsprozessen vermeiden, die nur eine zusätzliche Last für die Wirtschaftsbeteiligten bedeuten, ohne einen Mehrwert für die Transportsicherheit zu haben.

Sicherheitsstandards sollten dabei auf bestehenden, freiwilligen Zertifizierungen und Regularien aufbauen und diese integrieren. So gibt es beispielsweise mit der AEO-F/S im EU-Zollrecht, die europaweit Anwendung findet und darüber hinaus teilweise international, u. a. in USA und Japan anerkannt ist, TAPA oder der ISO 28.000 bereits Best Practices, die eine ausreichende Möglichkeiten zur Gewährleistung eines guten Sicherheitsstandards bieten. Die zugrunde liegenden Rechtsvorschriften sind flexibel und bieten einen hinreichenden Gestaltungsspielraum für eine Vertiefung und Weiterentwicklung.

Weitere verpflichtende Sicherheitsregularien sind weder notwendig noch zielführend.

Grundsätzlich sind auch hier risikobasierte und abgestufte Kontroll- und Sicherheitslösungen pauschalen Lösungen vorzuziehen. Eine differenzierte Betrachtung von Sicherheitsmaßnahmen ist erforderlich, um den unterschiedlichen Strukturen, Geschäftsmodellen sowie Sicherheitskulturen der unterschiedlichen Verkehrssysteme Rechnung zu tragen.

BDI-Forderungen

- Schaffung und Ausbau international anerkannter Standards auf Grundlage bestehender, freiwilliger Zertifizierungen und Regularien.
- Integration bestehender Zertifizierungen und Regularien in ein EU-weit harmonisiertes, international anerkanntes strategisches Sicherheitskonzept.
- Globale Harmonisierung oder zumindest gegenseitige Anerkennung der europäischen Sicherheitsverfahren mit Drittstaaten (Ermöglichung eines internationalen »One-Stop-Shop«-Ansatzes)
- Ausstattung der Sicherheitsbehörden mit ausreichenden Kapazitäten und Ressourcen sowie gegenseitige Anerkennung geeigneter Kontrollmethoden zur Vermeidung zeitlicher Engpässe bei Logistikprozessen.

IV. Rahmenbedingungen der Sicherheits- und Verteidigungsindustrie (SVI) verbessern

1. Ausgangslage und Herausforderungen

1.1 Die Bedeutung der Sicherheits- und Verteidigungsindustrie (SVI)

Deutschland ist ein souveräner Staat mit nationalen Interessen und internationaler Verantwortung. Unsere Nachbarn und Partner erwarten von Deutschland die Übernahme von Verantwortung – nicht nur im Rahmen der Finanz- und Haushaltskrise, sondern auch in der Außen- und Sicherheitspolitik. Zur Wahrnehmung und Gestaltung der daraus resultierenden Aufgaben gehören neben einer verantwortungsvollen Außenpolitik auch leistungsfähige Streit- und Sicherheitskräfte.

Die deutsche SVI ist Bestandteil der nationalen Sicherheitsvorsorge und leistet einen wichtigen Beitrag für die Bündnis- und Sicherheitsarchitektur. Ihr kommt der Status einer strategischen Schlüsselindustrie zu, deren Fähigkeiten es national durch die Schaffung geeigneter Rahmenbedingungen zu erhalten und weiterzuentwickeln gilt.

1.2 Markt- und Industriestrukturen

Die SVI sicherte im Jahr 2011 rund 220.000 Arbeitsplätze in Deutschland. Der Wert der produzierten Güter betrug im gleichen Zeitraum insgesamt 22,6 Mrd. Euro, die Exportquote lag bei 44 %.[3]

Die volkswirtschaftliche Bedeutung der SVI geht jedoch deutlich über die branchenspezifischen Eckdaten zu Beschäftigten und Produktionswerten hinaus: Mit einer internen Forschungs- und Entwicklungsquote (FuE) von 19,1 %[4] ist sie eine der innovativsten Industriebranchen Deutschlands. Über hohe Impuls- und Ausstrahlungswirkungen auch auf andere Industriesektoren[5] ist sie ein Innovationsmotor für das Industrieland Deutschland. Auch international nimmt sie eine technologische Spitzenstellung ein.

Die SVI-Märkte werden international von staatlichen Nachfragern geprägt und aufgrund jeweiliger nationaler sicherheits- und wirtschaftspolitischer Interessen stark reguliert. Subventionen und Staatsbeteiligungen, Reexport-Vorschriften, Offset-Verpflichtungen, nationale Zulassungs-, Prüfungs- oder Zertifizierungsanforderungen oder Wettbewerber ausschließende Beschaffungsverfahren: Die Liste der wettbewerbsverzerrenden, protektionistischen Regularien und Instrumente ist lang. Die resultierende Marktfragmentierung in Europa führt zu Ineffizienz im Beschaffungsprozess, mangelnder Interoperabilität der Streitkräfte sowie zur allgemeinen Verschwendung von Ressourcen.

1.3 Sinkende Beschaffungsbudgets in Deutschland und Europa

Im Kontext der Finanz- und Haushaltskrise werden derzeit in vielen westlichen Volkswirtschaften die Budgets noch stärker als bisher reduziert. Außerdem werden die Sicherheits- und Streitkräfte in Deutschland und Europa weiterhin verkleinert, Fähigkeitsanforderungen verändert und vereinbarte Beschaffungsstückzahlen im Nachhinein reduziert. Die deutsche SVI steht vor der Herausforderung, auf diese veränderte Marktsituation im Inland und in Europa Antworten finden zu müssen.

1.4 Beschaffung in Deutschland

Die veränderten Fähigkeitsanforderungen an Streit- und Sicherheitskräfte führen zu neuen Beschaffungsbedarfen – oftmals jedoch nur in sehr geringen Stückzahlen. Erkannte Fähigkeitslücken sollen zudem möglichst kurzfristig und kostengünstig geschlossen werden. Ein Weg hierfür ist die Beschaffung bereits marktverfügbarer Systeme und von Dual-Use-Technologien (sogenannte COTS-[6]/MOTS-[7] oder Kauflösungen). Unter den derzeitigen Rahmenbedingungen können diese von der deutschen SVI nur begrenzt vorgehalten werden. Diese Art der Beschaffung kann mittelfristig zu einem Verlust von Schlüsseltechnologien und -kompetenzen in Deutschland und zur Schaffung sicherheitspolitischer Abhängigkeiten führen.

Die Modernisierung der Beschaffungsprozesse in Deutschland – vor allem der neue Ausrüstungs- und Nutzungsprozess des BMVg – bietet allerdings die Chance, diesen drohenden Kompetenzverlust in der SVI abzuwenden. Dies setzt vor allem praxisorientiertere Beschaffungsvorgänge voraus, die von Beginn an im engen Austausch mit der deutschen SVI gestaltet werden. Eine für die Industrie rechtssichere Umsetzung dieser Beschaffungsprozesse ist zwingend notwendig.

3 Quelle: WifOR-Studie 2012 »Quantifizierung der volkswirtschaftlichen Bedeutung der Sicherheits- und Verteidigungsindustrie für den deutschen Wirtschaftsstandort«
4 Interne FuE-Quote: unternehmensinterne FuE-Ausgaben im Verhältnis zur Bruttowertschöpfung; Quelle: WifOR-Studie 2012
5 Zum Vergleich: die durchschnittliche FuE-Quote der deutschen Wirtschaft von 2007 bis 2010 lag bei 2,1 %; Quelle: WifOR-Studie 2012

6 commercial off-the-shelf
7 military off the shelf

1.5 Europäischer Beschaffungsmarkt

Im Rahmen der Gemeinsamen Außen- und Sicherheitspolitik (GASP) und der Europäischen Sicherheits- und Verteidigungspolitik (ESVP) gibt es seit Anfang der 90er Jahre Bestrebungen, die Schaffung eines europäischen Beschaffungsmarktes für Rüstungsgüter und Sicherheitstechnologien voranzutreiben. Mit der Gründung der European Defence Agency (EDA) und der Umsetzung des »Defence-Package« wurden u. a. die Voraussetzungen für eine »European Defence Technological and Industrial Base« geschaffen. Deren Potentiale werden bisher noch nicht ausreichend ausgeschöpft. So sind die europäischen SVI-Märkte weiterhin geprägt durch nationale Eigeninteressen, die sich in den massiven wettbewerbsverzerrenden Rahmenbedingungen, etwa in Form von Staatsbeteiligungen und damit verbundenen Subventionen oder Kompensationsgeschäften, widerspiegeln.

1.6 Globale Märkte/Exporte

Der nationale Bedarf von Bundeswehr und Behörden sowie Organisationen mit Sicherheitsaufgaben reicht für den Technologie- und Kompetenzerhalt in den deutschen Unternehmen bei weitem nicht aus. Dem Export kommt somit eine zentrale Bedeutung zu. Ein wichtiger Referenzkunde für die deutsche SVI ist die Bundeswehr.

Auf den Exportmärkten steht die deutsche SVI im intensiven Wettbewerb mit Anbietern aus Europa, den USA, Russland und weiteren Staaten, die für ihre Exportaktivitäten massive, organisierte politische und wirtschaftliche Unterstützung ihrer jeweiligen Regierung erhalten. International wird Rüstungsexportpolitik wesentlich stärker als in Deutschland im Verbund eigener außen- und sicherheitspolitischer sowie wirtschaftlicher Interessen gesehen.

1.7 Forschung und Technologie (F&T)

Die hohe Innovationskraft der deutschen Industrie ist der Schlüssel für ihre internationale Wettbewerbsfähigkeit. Die Unternehmen der SVI investieren im Durchschnitt 19 % ihrer Umsätze in die Forschung und Technologieentwicklung und nehmen damit national und international eine Spitzenstellung ein. Als High-Tech-Industrie ist die SVI auf qualifizierte Mitarbeiter angewiesen. Daher ist sie von dem steigenden Fachkräftemangel im Industrieland Deutschland besonders betroffen. Infolge nicht ausreichend qualifizierter Bewerber bleiben immer mehr Stellen dauerhaft vakant – mit steigender Tendenz. Insbesondere in naturwissenschaftlich-technischen Fächern fehlen Nachwuchskräfte. Diese Situation gefährdet langfristig die Innovations- und damit die Wettbewerbsfähigkeit der deutschen SVI.

2. Handlungsempfehlungen

2.1 SVI ist strategischer Bestandteil der nationalen Sicherheitsvorsorge

Sicherheitspolitik hat zwingend auch eine industriepolitische Komponente. Diese gilt es bei der Definition nationaler sicherheitspolitischer Interessen zu berücksichtigen. Während andere Staaten ihre nationalen Interessen auf Grundlage und dem Verständnis einer vernetzten Außen-, Sicherheits- und Industriepolitik festgelegt haben, werden diese Bereiche in Deutschland überwiegend ressortspezifisch betrachtet.

BDI-Forderungen:

- Führung eines Dialogs mit Politik, Industrie und Gesellschaft zur strategischen Bedeutung der SVI für die nationale Sicherheitspolitik.
- Ressortübergreifende Definition nationaler Interessen als Grundlage für eine aktive Mitgestaltung außen- und sicherheitspolitischer Prozesse in Europa und im internationalen Staatengefüge.
- Ableitung konkreter verbundener sicherheits- und industriepolitischer Interessen.

2.2 Stärkung und Erhalt der Innovationskraft und des Know-hows

Forschung von heute entscheidet über den wirtschaftlichen und technologischen Erfolg von morgen. Forschung und Entwicklung sind das Fundament der technologischen Spitzenstellung der SVI und ihres Erfolges auf den europäischen- und weltweiten Märkten und ermöglichen es, auf künftige sicherheitspolitische Herausforderungen bedarfsgerecht reagieren zu können.

Mit ihrer Forschung trägt die deutsche SVI zusätzlich zum wirtschaftlichen Wachstum und zur Innovationsfähigkeit anderer Branchen bei. Damit sichert sie jetzt und zukünftig Arbeitsplätze und Steuereinnahmen im Industrieland Deutschland.

BDI-Forderungen

- Bereitschaft, Zukunftstechnologien zu fördern.
- Stärkung öffentlicher Ressort-/Auftragsforschung.
- Stärkung der militärischen Forschungsförderung und Ausbau von Schnittstellen zu zivilen Förderprogrammen, um Transfer-Potenziale seitens der Unternehmen gezielt nutzen zu können.
- Sicherung des Fachkräftenachwuchses durch bedarfsgerechte Ausbildung und Weiterqualifizierung insbesondere in MINT-Berufen/Fächern.

2.3 Förderung des Außenhandels

Um die Versorgungssicherheit der nationalen Streitkräfte gewährleisten und ihre Schlüsseltechnologien und -kompetenzen erhalten zu können, ist die deutsche SVI auf den Export ihrer Produkte angewiesen.

BDI-Forderungen

- Strategische und ressortübergreifende Verankerung von Rüstungsexporten als Bestandteil einer modernen deutschen Außen-, Sicherheits- und Wirtschaftspolitik.
- Wahrung der Geschäftsgeheimnisse und Sicherheitsinteressen der Unternehmen der SVI sowie ihrer internationalen Kunden und Zulieferer im Genehmigungsverfahren.
- Abbau von Marktzugangsbarrieren (z. B. Off-Set-Verpflichtungen) und Wettbewerbsverzerrungen (insbesondere in EU und bei Rahmenabkommen zu grenzüberschreitenden Güterverkehr), sowie Schaffung eines »Level Playing Field«.

2.4 Beschaffung national und EU-weit

Um den Herausforderungen durch die Begrenzung der Haushaltsmittel einerseits und den Einsatzanforderungen von Bundeswehr und Sicherheitsbehörden andererseits gerecht zu werden, bedarf es innovativer Ansätze sowohl bezüglich der Beschaffung, als auch bezüglich der zukünftigen Finanzierung. Dies betrifft auch den Bereich der Zertifizierungs- und Zulassungsbestimmungen. So sollte z. B. ein gemeinsames Verständnis darüber entwickelt werden, inwieweit ordnungsrechtliche Anwendungen aus dem zivilen Zulassungsbereich bei militärischen Ausrüstungsgegenständen berücksichtigt werden müssen. Dazu ist ein enges, frühzeitiges Zusammenwirken von Industrie und Staat erforderlich.

Zugleich ist unter der erkennbar zunehmenden Einflussnahme der EU eine Standardisierung, Zertifizierung und Harmonisierung von Bau- und Zulassungsverfahren auf europäischer Ebene Voraussetzung für eine weiterhin wettbewerbsfähige deutsche wie auch gesamteuropäische Verteidigungsindustrie. Dies gilt auch für die politische Harmonisierung von Beschaffungsbedarfen (HMR – Harmonization of Requirements, HoD – Harmonization of Demand) zwischen den einzelnen nationalen Bedarfsträgern auf EU-Ebene mit dem Ziel, den Mitteleinsatz bei zukünftigen Großprogrammen zu optimieren. Bei Erreichen dieser verschiedenen Harmonisierungsziele wäre der zukünftige Ressourceneinsatz insgesamt effizienter, die Einsatzfähigkeit, Interoperabilität und Verfügbarkeit sichergestellt und die globale Wettbewerbsfähigkeit der Industrie erhöht. Gerade in Zeiten knapper Finanzmittel und im Bemühen, den Ausrüstungs- und Nutzungsprozess zu optimieren, erscheinen diese Maßnahmen als Mittel der Wahl. Auftraggeber und Auftragnehmer würden gleichermaßen profitieren.

BDI-Forderungen:

- Konsequente Umsetzung des neuen Ausrüstungs- und Nutzungsprozesses unter Einbeziehung der Industrie.
- Ausbau kooperativer Modelle zwischen Bundeswehr und Industrie sowie Weiterentwicklung langfristiger Partnerschaften in der Systembetreuung.
- Übernahme nichthoheitlicher Aufgaben durch die Industrie in den Bereichen Ausbildung, Betrieb, Wartung und Instandsetzung.
- Im Rahmen des »Defence Package«: Erhöhung der Transparenz hinsichtlich der europaweiten Umsetzung.
- EU-weite und internationale Harmonisierung technischer Prüf-, Zertifizierungs- und Zulassungsverfahren.
- EU-weite Harmonisierung von Beschaffungsbedarfen zwischen den nationalen Bedarfsträgern.

Impressum

Stand: Juni 2013

Herausgeber:
Bundesverband der Deutschen Industrie e.V. (BDI)
Abteilung Sicherheit und Rohstoffe
Breite Straße 29
D-10178 Berlin
T: 030 2028-0
www.bdi.eu

Redaktion:
Mattias Wachter, Abteilungsleiter
Felix Esser, Referent Sicherheit
Deborah Klein, Referentin Sicherheit und Rohstoffe

Kontaktdaten:
Bundesverband der Deutschen Industrie e.V. (BDI)
Abteilung Sicherheit und Rohstoffe
T: 030 2028-1495
F: 030 2028-2495
M: f.esser@bdi.eu

Layout und Druck:
DCM Druck Center Meckenheim GmbH
www.druckcenter.de

Fotos:
Cover: © chris-m / fotolia.com
Seite 9: © strixcode / fotolia.com
Seite 12: © amaze646 / fotolia.com
Seite 13: © Günter Menzl / fotolia.com
Seite 15: © Volodymyr Kyrylyuk / fotolia.com