Defense M&A

Besonderheiten von Unternehmenstransaktionen im Sicherheits- und Verteidigungssektor

von

Prof. Dr. Daniel Graewe, LL.M.
Rechtsanwalt, Hamburg

Fachmedien Recht und Wirtschaft | dfv Mediengruppe | Frankfurt am Main

Alle im Buch verwendeten Begriffe verstehen sich geschlechterneutral. Aus Gründen der besseren Lesbarkeit wird auf eine geschlechtsspezifische Differenzierung verzichtet – entsprechende Begriffe gelten im Sinne der Gleichbehandlung grundsätzlich für alle Geschlechter. Die verkürzte Sprachform hat lediglich redaktionelle Gründe und beinhaltet keine Wertung.

Bibliografische Information der Deutschen Nationalbibliothek

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

ISBN 978-3-8005-2089-3

dfv Mediengruppe

© 2026 Deutscher Fachverlag GmbH, Fachmedien Recht und Wirtschaft, Mainzer Landstraße 251, 60326 Frankfurt am Main, buchverlag@ruw.de

www.ruw.de

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlages unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Satzkonvertierung: Lichtsatz Michael Glaese GmbH, 69502 Hemsbach

Druck und Verarbeitung: Beltz Bad Langensalza GmbH, 99947 Bad Langensalza

Vorwort

Mergers & Acquisitions (M&A)-Transaktionen im Sicherheits- und Verteidigungssektor haben seit dem russischen Angriffskrieg gegen die Ukraine im Jahr 2022 erheblich an Bedeutung gewonnen. Der Aufbau verteidigungsindustrieller Fähigkeiten, die Finanzierung von Defense-Tech-Unternehmen, die Konsolidierung etablierter Anbieter und die Öffnung ziviler Technologieunternehmen für sicherheitsrelevante Anwendungen haben einen Transaktionsmarkt entstehen lassen, der sich mit den Kategorien klassischer Unternehmenstransaktionen allein nicht vollständig erfassen lässt.

Das Anliegen dieses Buches ist transaktionspraktisch. Es will zeigen, wie die Besonderheiten des Sicherheits- und Verteidigungssektors in Strategie, Dealstruktur, Käufer- und Target-Screening, Datenraum, Due Diligence, Bewertung, Finanzierung, Vertragsgestaltung, Closing und Post-Merger-Integration übersetzt werden können. Im Mittelpunkt steht nicht die isolierte Darstellung einzelner Rechtsgebiete, sondern ihre Wirkung auf den M&A-Prozess.

Damit ist zugleich die Grenze des Buches beschrieben. Es ist kein Kommentar zum Außenwirtschaftsrecht, kein Handbuch zur Exportkontrollklassifizierung, kein Vergaberechtskommentar oder Geheimschutzhandbuch und keine vollständige Darstellung des US-amerikanischen ITAR- oder EAR-Regimes. Es soll sich vielmehr der Frage widmen: Was folgt daraus für die Strukturierung, Prüfung, Absicherung und Integration einer Defense-M&A-Transaktion? Fallbeispiele, Checklisten und Vertragsbausteine sollen schließlich helfen, typische Bruchstellen früh zu erkennen und in konkrete Transaktionsmechanik zu übersetzen. Denn eine erfolgreiche Defense-M&A-Transaktion entsteht dort, wo wirtschaftliche Transaktionslogik und sicherheitsrechtliche Realität von Beginn an zusammengeführt werden.

Mein besonderer Dank gilt Herrn Rechtsreferendar Max-Justus Hinkel für seine wertvolle Unterstützung bei der Erstellung des Manuskripts.

Hamburg, im Herbst 2026 *Der Autor*

Geleitwort

Noch vor wenigen Jahren fand die Sicherheits- und Verteidigungsindustrie als Branche in Deutschland kaum öffentliche Aufmerksamkeit. Heute wissen wir, wie falsch dies war. Die Erhaltung von Frieden und öffentlicher Sicherheit ist keineswegs mehr selbstverständlich. Sie erfordert vollumfängliche Abschreckungs- und Verteidigungsfähigkeit, die wiederum nur mit entsprechender Ausstattung unserer Streitkräfte und Organe der inneren Sicherheit erreichbar ist.

Während wir uns bis 2022 schwertaten, jährlich mehr als 1,5 % unseres Bruttoinlandsprodukts für Verteidigung auszugeben, haben wir uns im Sommer 2025 vorgenommen, unsere Verteidigungsausgaben bis 2029 auf 3,5 % zu erhöhen. Weitere 1,5 % des Bruttoinlandsprodukts wollen wir zudem für die Ertüchtigung unserer militärisch relevanten Infrastruktur ausgeben. Dies sind gewaltige Summen, die bis zu 40 % unseres Bundeshaushaltes ausmachen werden.

Schon seit Beginn des Ukraine-Krieges im Februar 2022, erst recht aber seit der Lockerung der Schuldenbremse für Verteidigungsausgaben im März 2025 ist in der Sicherheits- und Verteidigungsindustrie eine enorme Dynamik zu verzeichnen, um die ihr gesetzten neuen Beschaffungsziele pünktlich zu erreichen. Teilweise muss der Output an bekannten Produkten bis zum Zehnfachen der früher abzuliefernden Stückzahlen erhöht werden. Es müssen aber auch neue Produkte konzipiert und für eine jederzeit zu startende Hochleistungsproduktion vorbereitet werden. Dies alles muss einhergehen mit hoher Innovations-Agilität und der Fähigkeit, sich ständig an technologische Weiterentwicklungen anpassen zu können.

Viele Startups und Scaleups haben sich herausgebildet, die sich mit ihren Produktideen einen Platz unter den Lieferanten unserer Streitkräfte und Sicherheitsorgane erobern wollen. Dabei findet ein Austausch von Ressourcen zwischen den Branchen statt. Insbesondere zieht die Sicherheits- und Verteidigungsindustrie viele personelle und sachliche Ressourcen aus Bereichen an, die bisher im engeren oder weiteren Sinne für den Automobilsektor tätig waren. Angesichts dieser höchst dynamischen Entwicklung, die sich in den kommenden Jahren weiter fortsetzen wird, bekommen M&A-Transaktionen mit einem sicherheits- und verteidigungsindustriellen Background naturgemäß große Bedeutung. Genau hierzu liefert das vorliegende Buch einen wichtigen Leitfaden für die Praxis.

Um es auf den Punkt zu bringen: Nicht von ungefähr haben viele westliche Länder – darunter auch Deutschland – bestimmte Fähigkeiten im Bereich ihrer Sicherheits- und Verteidigungsindustrie zu sog. „sovereign technologies“ erklärt, also zu Schlüsseltechnologien der nationalen Sicherheit. Dafür spielt es eine er-

hebliche Rolle, wem die betreffenden Unternehmen gehören, und welche Menschen von diesen Technologien Kenntnis haben und über sie im Positiven wie im Negativen verfügen können. „Acquisition“ schließt im Bereich der Sicherheits- und Verteidigungsindustrie immer auch die Frage ein, wer der Erwerber ist, und ob er mit möglichen Rücksichten auf nationale Sicherheitsaspekte kompatibel ist. Daher sind M&A-Transaktionen im Bereich der Sicherheits- und Verteidigungsindustrie immer speziell. Es ist das Verdienst dieses Buches und seines Autors Daniel Graewe, auf die Besonderheiten von M&A im Sicherheits- und Verteidigungsbereich einen ebenso umfassenden wie praxistauglichen Blick zu ermöglichen.

Dr. Hans Christoph Atzpodien, Hauptgeschäftsführer
Bundesverband der Deutschen Sicherheits- und Verteidigungsindustrie (BDSV)

Inhaltsverzeichnis

Vorwort VII

Geleitwort IX

Abkürzungsverzeichnis XV

1. Einführung 1
- 1.1 Defense M&A 1
- 1.2 Marktentwicklungen im Rüstungsbereich 4
- 1.3 Dealtypen im Defense M&A 7
  - 1.3.1 Erwerb eines klassischen Rüstungsunternehmens 8
  - 1.3.2 Erwerb eines Defense-Tech- oder Softwareunternehmens 8
  - 1.3.3 Erwerb eines Dual-Use-Unternehmens 9
  - 1.3.4 Carve-out eines sicherheitsrelevanten Geschäftsbereichs 9
  - 1.3.5 Minderheitsbeteiligung und Joint Venture 10
  - 1.3.6 Erwerb durch Finanzinvestoren 10
  - 1.3.7 Erwerb durch zivile Industrieunternehmen 11
  - 1.3.8 Public-to-Private, Börsenstruktur und kapitalmarktorientierte Defense-Transaktionen 11
  - 1.3.9 Distressed Defense M&A 12
  - 1.3.10 Bedeutung der Dealtypologie für die Transaktionspraxis 12

2. Regulatorische Landkarte 15
- 2.1 Wichtige Bereiche 15
  - 2.1.1 Investitionskontrolle nach AWG/AWV 15
  - 2.1.2 Europäische FDI-Screening-Dimension 17
  - 2.1.3 Fusionskontrolle 17
  - 2.1.4 Exportkontrolle und Dual-Use 19
  - 2.1.5 Kriegswaffenkontrolle 20
  - 2.1.6 ITAR und EAR 20
  - 2.1.7 Sanktionen, Embargos und Integrität des Geschäftsmodells 21
  - 2.1.8 Geheimschutz und Verschlusssachen 21
  - 2.1.9 Cybersecurity und IT-Sicherheit 25
  - 2.1.10 Vergaberecht und staatliche Kundenverträge 26
- 2.2 Überleitung in die Transaktionsstruktur 27

3. Transaktionsphasen 29
- 3.1 Prä-Akquisitionsphase 29
  - 3.1.1 Strategieentwicklung 31
  - 3.1.2 Defense Fit 32

3.1.3 Regulatorische Vorprüfung 33
3.1.4 Organisation und Steuerung 34
3.1.5 Markt- und Targetscreening 35
3.1.6 Kritische Faktoren 37
3.1.6.1 Fähigkeits- und Transaktionsentscheidung 37
3.1.6.2 Anforderungsprofil und Screening im Defense-Sektor 40
3.1.6.3 Steuerung von Informationszugang und Kundenkommunikation 42
3.1.6.4 Einsatz externer Berater 47
3.2 Transaktionsphase 51
3.2.1 Kontaktaufnahme 53
3.2.2 Due Diligence 56
3.2.2.1 Prüfung von Unterlagen 57
3.2.2.2 Q&A-Prozess und Management Interviews 61
3.2.2.3 IP, technische Daten und staatliche Nutzungsrechte . . 63
3.2.3 Unternehmensbewertung 66
3.2.3.1 Bewertungsverfahren 68
3.2.3.2 Bewertungsfolgen von IP- und Technical-Data-Rechten 71
3.2.4 Finanzierung 72
3.2.4.1 Defense-spezifische Anforderungen an die Finanzierbarkeit 73
3.2.4.2 Eigenkapital, Fremdkapital und hybride Finanzierungsinstrumente 74
3.2.4.3 Kreditgeberprüfung und Defense-spezifische Finanzierungsbedingungen 75
3.2.4.4 Informationszugang der Finanzierer 76
3.2.4.5 Sicherheiten und ihre Verwertbarkeit 77
3.2.4.6 Finanzierungssicherheit zwischen Signing und Closing 78
3.2.4.7 Verkäuferperspektive und Prüfung der Käuferfinanzierung 79
3.2.4.8 Post-Closing-Liquidität und Finanzierung der Integration 80
3.2.4.9 Verzahnung von Finanzierung, Regulierung und Unternehmenskaufvertrag 81
3.2.5 Vertragsverhandlungen 82
3.2.5.1 Vertragsverhandlungen im Defense-Sektor 82
3.2.5.2 Defense-spezifische Risikozuordnung im SPA 83

3.2.5.3 Zeit zwischen Signing und Closing 87
3.2.6 EXKURS: Reputation, Nachhaltigkeit und Kommunikation . 89
3.2.6.1 Reputation 89
3.2.6.2 Nachhaltigkeit 90
3.2.6.3 Kommunikation 90
3.2.7 Gremienentscheidung und Business Judgment Rule 91
3.2.8 Kritische Faktoren 96
3.2.8.1 Sorgfältige Due Diligence, Informationsgrenzen und Deal Breaker 97
3.2.8.2 Defense-spezifische Unternehmensbewertung und vollzugssichere Finanzierung 99
3.2.8.3 Verhandlungsführung und Übersetzung der Risiken in die Vertragsmechanik 101
3.2.8.4 Fusionskontrolle, Clean Team und Vermeidung von Gun Jumping 103
3.2.8.5 Kundenakzeptanz, Erwerbereignung und integrierte Deal-Governance 105
3.3 Integrationsphase 107
3.3.1 Integrationsstrategie 109
3.3.2 Integrationskonzeption 111
3.3.3 Integrationsdurchführung 112
3.3.4 Integrationscontrolling 113
3.3.5 Kritische Faktoren 115
3.3.5.1 Integrationslogik und Integrationstiefe richtig bestimmen 116
3.3.5.2 Geschwindigkeit, Reihenfolge und Kontrollpunkte der Integration 120
3.3.5.3 Kundenvertrauen und Schlüsselpersonen sichern 124
3.3.5.4 IT-, Daten- und Sicherheitsarchitektur kontrolliert integrieren 129
3.3.5.5 Governance, Verantwortlichkeit und laufende Erfolgskontrolle 133
3.4 Woran Defense-M&A-Transaktionen scheitern 138

4. Die Rolle der künstlichen Intelligenz 147
4.1 Datenklassen vor Tool-Auswahl 147
4.2 Kritische Einsatzbereiche 149
4.3 Target- und Marktscreening 150
4.4 Unternehmensbewertung 151
4.5 Due Diligence 151

4.6 Management Decision 152

5. Handreichungen für die Praxis 153
5.1 Transaktionsfahrplan 153
5.1.1 Ziel, Funktion und Mindestinhalt 153
5.1.2 Muster-Transaktionsfahrplan 153
5.2 Due-Diligence-Anforderungsliste 170
5.3 Musterklauseln 182
5.3.1 Non-Disclosure Agreement (NDA) 183
5.3.2 Letter of Intent (LoI) 192
5.3.3 Musterklauseln im Kaufvertrag 201
5.3.4 Closing Memorandum 215
5.4 Interviewleitfaden für Management Interviews 224
5.4.1 Vorbereitung der Interviews 225
5.4.2 Durchführung der Interviews 225
5.4.2.1 Geschäftsleitung 226
5.4.2.2 Operative Themen 229
5.4.2.2.1 Vertrieb 230
5.4.2.2.2 Forschung & Entwicklung 232
5.4.2.2.3 Exportkontrollbeauftragter 234
5.4.2.2.4 IT 235
5.4.2.2.5 Compliance 237
5.4.2.2.6 Öffentliches Auftragsmanagement 239
5.4.3 Dokumentation der Interviews 241
5.4.4 Auswertung und Folgemaßnahmen 242

6. Schlussbemerkungen 245

Stichwortverzeichnis 247

3. Transaktionsphasen

Der nachfolgende Transaktionsprozess folgt zwar dem klassischen Ablauf von Prä-Akquisition, Transaktionsphase und Post-Merger-Integration. Im Defense M&A bilden diese Phasen aber keine bloß chronologische Abfolge, sondern auch aufeinander aufbauende Risikofilter. In jeder Phase ist zu prüfen, ob wirtschaftliche Transaktionslogik, regulatorische Zulässigkeit, Informationsschutz, staatliche Kundenakzeptanz und operative Fortführbarkeit noch zusammenpassen. Wird ein Deal Breaker sichtbar, muss deshalb nicht nur ein einzelner Prozessschritt angepasst werden. Gegebenenfalls ist die gesamte Deal-Hypothese neu zu bewerten.

3.1 Prä-Akquisitionsphase

Die Prä-Akquisitionsphase ist im Defense-Sektor die **erste regulatorische Filterstufe** der Transaktion. Bereits vor der ersten Ansprache muss geklärt werden, ob Target, Erwerber, Eigentümerstruktur, Finanzierung, Kundenbasis, Datenlage und Integrationsfähigkeit überhaupt transaktionsfähig sind. Die entscheidende Frage lautet nicht nur, ob ein Unternehmen strategisch interessant ist. Zu prüfen ist ebenso, ob der Erwerb investitionskontrollrechtlich, exportkontrollrechtlich, geheimschutzrechtlich, kundenbezogen und operativ darstellbar erscheint. Professionelle Vorbereitung bedeutet im Defense M&A deshalb, eine Deal-Hypothese nicht allein nach Markt, Synergien, Kaufpreis und Finanzierung zu formulieren. Sie muss zugleich die regulatorische Vollzugsfähigkeit, den zulässigen Informationszugang, die Akzeptanz staatlicher Kunden, die Fortführung wesentlicher Genehmigungen und die spätere Integrationsfähigkeit berücksichtigen. Wer diese Fragen erst in der Due Diligence stellt, hat häufig bereits Zeit, Verhandlungsmacht und Handlungsspielraum verloren.

Innerhalb der Prä-Akquisitionsphase stehen vier Arbeitsstränge im Mittelpunkt: die strategische Zielsetzung, die Definition des Defense Fit, die regulatorische Vorprüfung und die Organisation des Informationszugangs. Der Käufer muss klären, welche sicherheitsrelevante Fähigkeit er erwerben will, welche Targets hierfür überhaupt in Betracht kommen, welche Erwerber- oder Finanzierungsstruktur regulatorisch tragfähig ist und ob ein normaler Datenraum, ein gestufter Datenraum oder ein Clean-Team-Modell erforderlich wird. Strategie, Screening und Regulatory Workstream laufen damit von Beginn an parallel.

Auch auf Verkäuferseite ist die Vorbereitung wichtig. Der Verkäufer muss das Zielunternehmen transaktionsfähig machen. Dazu gehören die Abgrenzung des

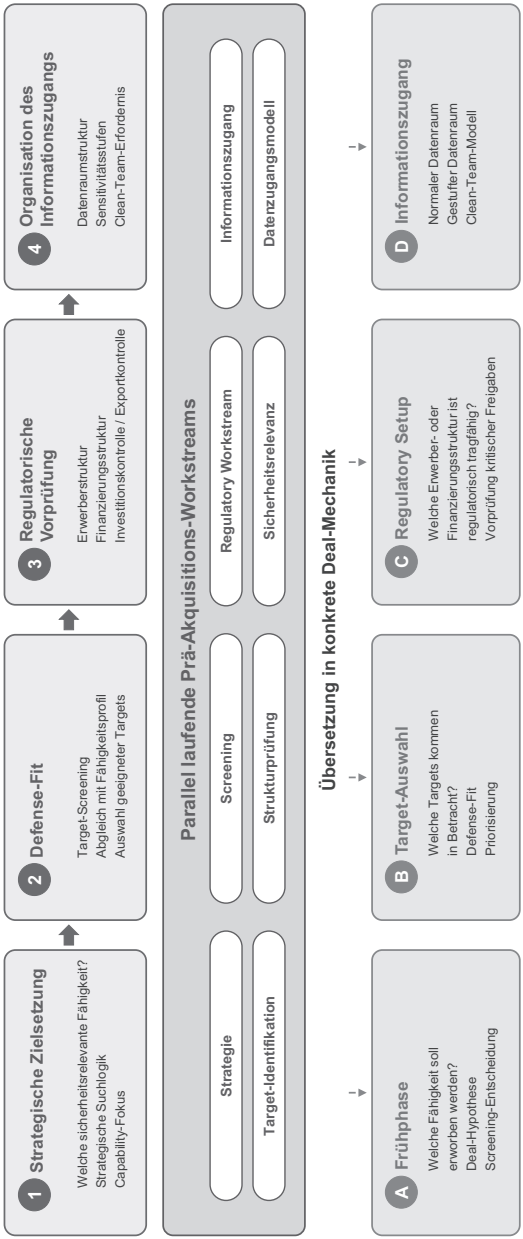


Abbildung 2: Prä-Akquisitionsphase

Verkaufsgegenstands, die Prüfung von Genehmigungen, VS- und Exportkontrollthemen, die Strukturierung des Datenraums, die Vorbereitung staatlicher Kundenkommunikation, die Analyse von Change-of-Control-Rechten sowie gegebenenfalls eine weiterführende Vendor Due Diligence. Bei Carve-outs kommt hinzu, dass der Verkäufer eine operativ und regulatorisch fortführbare Einheit erst schaffen muss.

3.1.1 Strategieentwicklung

M&A-Transaktionen sind auch im Defense-Sektor kein Selbstzweck. Sie müssen aus der Unternehmensstrategie abgeleitet werden. Die Strategieentwicklung beginnt daher mit einer **doppelten Analyse**. Einerseits sind Markt, Technologie, Kunden, Programme und Fähigkeitslücken zu bewerten. Andererseits ist zu prüfen, ob die angestrebte Transaktion unter Defense-Bedingungen tatsächlich durchführbar ist.

Die Entscheidung für eine Akquisition ist im Defense-Sektor nur eine von mehreren strategischen Optionen. Gerade bei sicherheitsrelevanten Technologien kann eine Kooperation, ein Joint Venture, eine Minderheitsbeteiligung, ein Entwicklungsvertrag oder eine Make-Strategie geeigneter sein als eine Vollakquisition. Entscheidend ist nicht nur, welche Option wirtschaftlich attraktiv erscheint, sondern welche Option regulatorisch zulässig, informationsschutzrechtlich beherrschbar, kundenakzeptiert und integrationsfähig ist. Vor der finalen Entscheidung müssen die wirtschaftlichen Grundlagen, die regulatorische Machbarkeit, die Alternativen zur Akquisition, die Finanzierungsstruktur, die Organentscheidung und mögliche Sonderinteressen dokumentiert werden. Parallel dazu sind bei kapitalmarktorientierten Unternehmen Vorkehrungen zur Einhaltung der **Marktmissbrauchsverordnung** zu treffen. Schließlich ist zu prüfen, ob die Einbeziehung externer Berater erforderlich ist, diese ordnungsgemäß ausgewählt wurden und geeignete Vereinbarungen mit diesen getroffen wurden.

Auf Käuferseite beginnt die Akquisitionsstrategie mit einem **Anforderungsprofil**, das nicht nur Marktposition, Technologie, Umsatz, EBITDA und mögliche Synergien beschreibt. Es muss auch Defense-Kriterien enthalten: Produkte und Güterklassifizierung, staatliche Kunden, Exporthistorie, VS-Relevanz, ITAR/EAR-Bezug, Cybersecurity, Preisrecht, Lieferketten, Schlüsselpersonen und Integrationsgrenzen. Das Screening darf deshalb nicht nur kommerziell erfolgen. Es muss früh zwischen strategisch attraktiven und regulatorisch realistisch erwerbbaren Targets unterscheiden. M&A-Berater, Rechtsberater und technische Experten sollten in diesem Stadium so eingebunden werden, dass Teaser, Informations-

memorandum, erste Ansprache und Datenraumstrategie keine sensiblen Informationen unzulässig offenlegen.

Auf Verkäuferseite steht hingegen nicht die Akquisitionsstrategie, sondern die Herstellung von **Transaktionsfähigkeit** im Vordergrund. Der Verkäufer muss prüfen, welche Käufer regulatorisch in Betracht kommen, welche Informationen überhaupt offengelegt werden dürfen, ob ein Carve-out erforderlich ist, welche Genehmigungen, Kundenconsents, VS-Strukturen, Exportkontrollprozesse, Transitional Services Agreements und IP-Rechte für einen stabilen Übergang benötigt werden. Teaser, Informationsmemorandum, NDA, LoI, MoU und Non-binding Offer behalten ihre organisatorische Funktion. Im Defense-Sektor müssen sie aber zusätzlich die Grenzen des Informationszugangs, die regulatorische Vorprüfung, die Behörden- und Kundenkommunikation sowie die zulässige Einbindung von Beratern, Finanzierern und KI-Tools abbilden.

3.1.2 Defense Fit

Der Defense Fit beschreibt, ob ein Zielunternehmen nicht nur wirtschaftlich attraktiv, sondern in das sicherheits-, technologie- und kundenbezogene Profil des Erwerbers passt. Er ist enger als der allgemeine Strategic Fit und zugleich breiter als eine regulatorische Prüfung. Ein Target kann über eine attraktive Technologie verfügen und dennoch ungeeignet sein, wenn Programme, Kundenbindungen, Sicherheitsanforderungen oder Lieferketten mit dem Geschäftsmodell des Käufers nicht vereinbar sind. Die Prüfung soll deshalb früh klären, ob die Transaktion eine tatsächlich nutzbare und fortführbare Verteidigungsfähigkeit schafft.

Ausgangspunkt ist der **Capability Fit**. Zu bestimmen ist, welche konkrete Fähigkeit erworben werden soll, etwa Sensorik, unbemannte Systeme, Software, Cybersecurity, Kommunikation, Instandhaltung oder eine kritische Produktionskapazität. Anschließend ist zu prüfen, ob das Target diese Fähigkeit tatsächlich beherrscht oder lediglich einzelne Komponenten, Entwicklungsprojekte oder personengebundene Kenntnisse besitzt. Maßgeblich sind Technologiereife, Skalierbarkeit, Produktionsfähigkeit, Zertifizierungen, IP- und Datenrechte sowie die Abhängigkeit von Schlüsselpersonen, Unterauftragnehmern und staatlich finanzierten Programmen. Hinzu tritt der **Customer and Programme Fit**. Geschäftsmodelle im Defense-Sektor werden häufig durch langfristige Beschaffungsprogramme, nationale Sicherheitsinteressen und enge Beziehungen zu öffentlichen Auftraggebern geprägt. Zu untersuchen ist, ob Produkte und Leistungen des Targets in bestehende Plattformen, Programme und Vertriebswege des Erwerbers passen, ob Kundenkonflikte entstehen und ob staatliche Auftraggeber einen Eigentümerwechsel akzeptieren würden. Ebenso ist zu prüfen, ob die

Akquisition die Position als Hauptauftragnehmer stärkt oder neue Abhängigkeiten von Systemhäusern, Behörden oder einzelnen Programmen begründet.

Der **Operational Fit** betrifft die Fähigkeit, das Target nach Vollzug stabil fortzuführen und sinnvoll einzubinden. Zu bewerten sind Standorte, Produktionsmittel, Personal, Sicherheitsorganisation, Qualitätsmanagement, Cybersecurity, Lieferketten und der Zugang zu geschützten Informationen. Eine vollständige Integration kann sich verbieten, wenn nationale Abschottung, Security-Ring-Fencing, getrennte IT-Systeme oder eigenständige Governance-Strukturen erforderlich bleiben. Deshalb ist früh festzulegen, ob Vollintegration, kontrollierte Autonomie, Minderheitsbeteiligung, Joint Venture oder Kooperation realistisch ist.

Schließlich ist der **Cultural and Compliance Fit** zu prüfen. Belastbare Prozesse für Exportkontrolle, Geheimschutz, Sanktionen, öffentliche Aufträge, Preisrecht und staatliche Kunden sind Teil der operativen Substanz des Targets. Schwächen können nicht nur Haftungsrisiken begründen, sondern die Verwendbarkeit der erworbenen Fähigkeiten infrage stellen. Ergebnis sollte ein dokumentiertes **Defense-Fit-Profil** sein, das Muss-Kriterien, tolerierbare Abweichungen, Integrationsgrenzen und Deal Breaker festhält. Erst dann lässt sich beurteilen, ob die Akquisition oder eine alternative Kooperationsform den geeigneteren Weg darstellt.

3.1.3 Regulatorische Vorprüfung

Die regulatorische Vorprüfung soll vor Beginn eines aufwendigen Erwerbsprozesses klären, ob die Transaktion grundsätzlich vollzugsfähig erscheint und welche rechtlichen Rahmenbedingungen den Prozess bestimmen. Sie ersetzt weder die Due Diligence noch die spätere Detailprüfung. Ihre Funktion liegt darin, Deal Breaker, Genehmigungserfordernisse, Vollzugsverbote, Informationsgrenzen und zeitkritische Behördenverfahren früh zu identifizieren. Ausgangspunkt sind Target, Erwerber, mittelbare Eigentümer, Finanzierung, Erwerbsquote und Kontrollrechte.

Im Mittelpunkt steht regelmäßig die **Investitionskontrolle**. Zu prüfen ist, ob eine sektorübergreifende oder sektorspezifische Prüfung nach AWG und AWV oder ein Verfahren in anderen Jurisdiktionen ausgelöst wird. Relevant sein können neben dem unmittelbaren Erwerber auch mittelbare Beteiligungen, atypische Kontrollrechte, Fondsstrukturen und die Herkunft der Finanzierung. Früh zu bewerten sind Meldepflichten, Prüfungsfristen, Untersagungsrisiken sowie mögliche Auflagen oder Zugriffsbegrenzungen.

Parallel ist die **fusionskontrollrechtliche Zuständigkeit** zu bestimmen. Neben der deutschen und europäischen Fusionskontrolle können Anmeldungen in weiteren Staaten erforderlich sein. Bei staatlich beeinflussten oder aus Drittstaaten fi-

nanzierten Erwerbern ist außerdem die EU-Verordnung über drittstaatliche Subventionen zu prüfen. Die Zeitpläne müssen mit Investitionskontrolle, Finanzierung und Long-Stop-Date abgestimmt werden. Auch ein materiell unproblematischer Zusammenschluss kann scheitern, wenn Vollzugsverbote übersehen werden.

Ein weiterer Schwerpunkt liegt auf **Exportkontrolle, Sanktionen und Kriegswaffenrecht**. Produkte, Software, Technologie und Entwicklungsdaten sind vorläufig als Rüstungsgüter, Dual-Use-Güter oder nicht gelistete Güter einzuordnen. Zu prüfen sind Genehmigungen, ITAR-/EAR-Bezüge, Reexportbeschränkungen, Endverbleibspflichten, Embargos sowie personen- und unternehmensbezogene Sanktionen. Die Prüfung muss auch den Transaktionsprozess erfassen, weil bereits die Offenlegung technischer Daten an ausländische Erwerber, Berater oder Finanzierer einen kontrollierten Technologietransfer darstellen kann.

Hinzu kommen Geheimschutz, Cybersecurity, Vergaberecht, Preisrecht und staatliche Kundenverträge. Zu klären ist, ob Verschlusssachen betroffen sind, welche Sicherheitsfreigaben bestehen, ob Change-of-Control-Klauseln oder Zustimmungserfordernisse eingreifen und ob Genehmigungen nach Vollzug fortbestehen. Entscheidend ist nicht nur, ob der Anteilserwerb zulässig ist, sondern ob das Target unter der neuen Eigentümerstruktur weiterhin Aufträge erfüllen, Informationen verarbeiten und Genehmigungen nutzen kann.

Das Ergebnis sollte in einer **regulatorischen Roadmap** mit Ampelbewertung festgehalten werden. Für jedes Themenfeld sind Genehmigungspflicht, erwartete Dauer, Risikoniveau und mögliche Mitigationsmaßnahmen zu dokumentieren. Bei kritischen Befunden sind Strukturvarianten zu entwickeln, etwa eine geringere Beteiligungsquote, beschränkte Governance-Rechte, Ring-Fencing oder ein Carve-out. Die Vorprüfung wird damit zur Grundlage für Zeitplan, Transaktionsstruktur, Closing Conditions und die Entscheidung über die Fortführung des Prozesses.

3.1.4 Organisation und Steuerung

Organisation und Steuerung müssen im Defense M&A über die klassische M&A-Projektorganisation hinausgehen. Neben Legal, Financial, Tax, Commercial und Technical Due Diligence ist ein eigener **Regulatory Workstream** erforderlich. Dieser Workstream bündelt Investitionskontrolle, Exportkontrolle, Fusionskontrolle, Sanktionen, Geheimschutz, Cybersecurity, Vergabe, Preisrecht, staatliche Kundenverträge und Kommunikationssteuerung. Er muss nicht nur prüfen, sondern laufend entscheiden helfen, welche Informationen offengelegt werden dürfen, welche Behördenkontakte erforderlich sind, welche Closing Conditions zwingend sind und welche Integration nach Closing zulässig ist.

Käuferseitig ist möglichst früh ein **interdisziplinäres Deal Team** einzurichten. Neben M&A, Recht, Steuern, Finanzen und operativen Fachbereichen sollten Exportkontrolle, Compliance, Cybersecurity, Informationssicherheit, Geheimschutz, Public Affairs, staatliche Kundenverantwortliche und Integrationsexperten eingebunden werden. Die Verantwortlichkeiten für die einzelnen Workstreams müssen klar festgelegt werden. Ohne diese Governance droht, dass wirtschaftliche, rechtliche, technische und sicherheitsrelevante Prüfungen nebeneinander herlaufen und nicht aufeinander abgestimmt sind.

Externe Berater sind im Defense M&A nicht nur kapazitätsbezogene Unterstützung, sondern häufig Voraussetzung für Transaktionsfähigkeit. Neben M&A-Beratern, Transaktionsanwälten, Wirtschaftsprüfern und Steuerberatern werden regelmäßig Spezialisten für Außenwirtschaftsrecht, Exportkontrolle, ITAR/EAR, Geheimschutz, Cybersecurity, technische Produktprüfung und staatliche Kundenkommunikation benötigt. Das Akquisitionscontrolling des Erwerbers muss deshalb nicht nur Budget, Zeitplan und Arbeitspakete überwachen, sondern auch die Gültigkeit der regulatorischen Deal-Annahmen: Erwerberfähigkeit, Genehmigungsbedarf, Datenraumfreigaben, Kundenconsents, Finanzierungsbedingungen und Integrationsgrenzen.

Auch verkäuferseitig reicht die allgemeine Transaktionszuständigkeit nicht aus. Die verkaufsvorbereitende Organisation muss sicherstellen, dass der Verkaufsprozess selbst keine regulatorischen Verstöße auslöst. Dazu gehören ein kontrollierter Datenraum, eine vorab definierte Käuferansprache, ein abgestimmter Umgang mit staatlichen Kunden, eine Prüfung von Exportkontrolle und Geheimschutz vor Offenlegung technischer Informationen, klare Zuständigkeiten für Behördenkontakte sowie ein Carve-out- und TSA-Konzept, wenn der Verkaufsgegenstand nicht stand-alone-fähig ist. Auch verkäuferseitig ist die Einbindung externer Dienstleister kein bloßes Effizienzthema. Sie dient der kontrollierten Herstellung von Transaktionsfähigkeit. Externe Berater sollten insbesondere prüfen, welche Informationen in welcher Form offengelegt werden dürfen, welche Käufer regulatorisch in Betracht kommen, ob ein **Vendor-DD-Bericht** sensible Informationen ersetzen kann, welche Kunden vor Closing einzubeziehen sind und ob ein Carve-out oder TSA-Modell regulatorisch tragfähig sind.

3.1.5 Markt- und Targetscreening

Bevor ein Erstkontakt stattfindet, müssen potenzielle Targets oder Käufer nicht nur strategisch, sondern auch regulatorisch vorgefiltert werden. **Screening** bedeutet im Defense M&A die systematische Prüfung von **Defense Fit, Regulatory Fit, Information Fit und Integration Fit**. Auf Käuferseite geht es um die

Frage, welche sicherheitsrelevante Fähigkeit erworben werden soll und welche Targets überhaupt genehmigungsfähig, finanzierbar und integrierbar erscheinen. Auf Verkäuferseite geht es um die Frage, welche Erwerber regulatorisch akzeptabel sind und welchen Interessenten sensible Informationen überhaupt zugänglich gemacht werden dürfen.

Ausgangspunkt des Screening-Prozesses bleibt eine **Long List**. Im Defense-Sektor darf diese Liste aber nicht nur nach Markt, Umsatz, Technologie und Synergiepotenzial erstellt werden. Sie muss auch klassische Rüstungsunternehmen, Defense-Tech-Anbieter, Dual-Use-Unternehmen, zivile Plattformanbieter, kritische Zulieferer und mögliche Kooperationspartner anhand sicherheitsrelevanter Fähigkeit, staatlichen Kunden, Genehmigungslage, Exportkontrollnähe, IP-/Datenprofil und Integrationsfähigkeit erfassen. Bereits auf Long List-Ebene sollten offensichtliche Ausschlussgründe dokumentiert werden, etwa Sanktionsbezug, Hochrisikoländer, fehlende Käuferfähigkeit oder absehbare Unvereinbarkeit mit Investitionskontrolle und Kundenakzeptanz.

Das **First Screening** dient dann nicht nur der Verdichtung auf kommerziell interessante Kandidaten, sondern der Eliminierung regulatorisch unrealistischer Optionen. Zu prüfen sind insbesondere AWG/AWV-Relevanz, Dual-Use- oder Kriegswaffennähe, ITAR/EAR-Bezug, Verschlusssachen, staatliche Kundenverträge, Preisrechtsrisiken, Cybersecurity, Finanzierbarkeit und mögliche Integrationsgrenzen. Im **Second Screening** werden die verbleibenden Kandidaten vertieft analysiert. Ziel ist nicht zwingend die kleinste Short List, sondern eine belastbare Auswahl derjenigen Targets oder Käufer, mit denen vorvertragliche Gespräche ohne unkontrollierte Offenlegung sensibler Informationen geführt werden können.

Fallbeispiel:
Mercedes-Benz / Tytan – wenn zivile Plattformen verteidigungsnah werden

Die geplante Kooperation zwischen Mercedes-Benz und Tytan Technologies zeigt, wie durchlässig die Grenze zwischen ziviler Industrie und Verteidigungsmarkt geworden ist. Im Fokus steht ein mobiles Drohnenabwehrsystem, bei dem Fahrzeuge wie die G-Klasse und der Sprinter als Plattformen für Sensorik, Startvorrichtungen und Abwehrdrohnen genutzt werden sollen. Berichtet wurde, dass Mercedes-Benz modifizierte Fahrzeuge bereitstellen will; konkrete Investitions- oder Zeitplandetails wurden zunächst nicht genannt.

Für Defense M&A ist dieser Fall weniger wegen einer klassischen Unternehmenstransaktion interessant, sondern wegen seiner strategischen Logik. Unternehmen, die bislang nicht als Rüstungsunternehmen wahrgenommen wurden,

können über Plattformen, Software, Sensorik, Fahrzeuge, Energieversorgung, Kommunikation oder industrielle Fertigung plötzlich verteidigungsnahe Relevanz gewinnen. Damit erweitert sich der Screening-Raum erheblich. Ein potenzielles Target muss nicht bereits Waffen oder Munition herstellen, um für Defense M&A relevant zu sein. Es kann genügen, dass seine Technologie, Plattform oder Produktionsfähigkeit militärisch nutzbar wird.

Für Käufer bedeutet das: Screening-Kriterien müssen breiter werden. Neben klassischen Rüstungsunternehmen sind Dual-Use-Anbieter, Softwareunternehmen, Plattformhersteller, Elektronikunternehmen, Raumfahrt- und Sensorikunternehmen, Mobilitätsanbieter und industrielle Spezialzulieferer zu betrachten. Gleichzeitig entstehen neue regulatorische Fragen. Wird aus einem zivilen Produkt durch militärische Nutzung ein exportkontrollrechtlich sensibles Gut? Welche Rolle spielt der Endnutzer? Müssen technische Daten, Software oder Komponenten neu klassifiziert werden? Entstehen Reputationsrisiken oder neue Kundenrestriktionen? Der Fall zeigt auch, dass Kooperation, Joint Venture, Minderheitsbeteiligung oder Lieferpartnerschaft eine Alternative zur Vollakquisition sein können. Gerade wenn ein ziviler Konzern zunächst Marktzugang, Technologiebeitrag oder Plattformnutzung erproben will, kann eine Kooperation regulatorisch und strategisch sinnvoller sein als ein sofortiger Unternehmenskauf.

3.1.6 Kritische Faktoren

Der Erfolg der Prä-Akquisitionsphase hängt im Defense M&A vor allem von vier Faktoren ab: einer bewussten Fähigkeits- und Transaktionsentscheidung, einem defense-spezifischen Anforderungsprofil, einer angemessenen Steuerung von Informationszugang und Kundenkommunikation sowie der frühen Einbindung von Beratern.

3.1.6.1 Fähigkeits- und Transaktionsentscheidung

Opportunistische Transaktionen sind im Defense-Sektor besonders riskant – und daher auch eher selten. Ein Unternehmen kann wirtschaftlich attraktiv erscheinen, über hohe Auftragsbestände und interessante Technologien verfügen und dennoch kein geeignetes Akquisitionsziel sein. Das Target kann regulatorisch nicht oder nur unter erheblichen Auflagen erwerbbar, schwer finanzierbar, aus Sicht öffentlicher Kunden nicht akzeptabel oder wegen Geheimschutz- und Exportkontrollvorgaben faktisch nicht integrierbar sein. Die Verfügbarkeit eines Targets darf deshalb nicht zum Ausgangspunkt der Strategie werden.