

ROHDE BAIER

DEEP DIVE

M&A in der Verteidigungs- industrie

Komplexität meistern, Chancen sichern

Frankfurt | 2026



I. Einleitung

Europa erlebt einen sicherheitspolitischen Strukturbruch. Der Krieg in der Ukraine, Druck aus Russland/China und zunehmende Cyberangriffe treiben Budgets nach oben und rücken Souveränität, Resilienz und industrielle Basis in den Fokus. Parallel entstehen neue Bedarfe (Luftverteidigung, Munition, Cyber/ISR), die mehrjährige Beschaffungswellen auslösen. Die transatlantische Zusammenarbeit über NATO und bilaterale Programme bleibt operativer Anker, während europäische Initiativen die eigene Handlungsfähigkeit stärken sollen. Für Unternehmen heißt das: volle Pipelines, aber auch Engpässe in Lieferketten, Personal und Zertifizierung – und damit Planungs- und Finanzierungsthemen für Deals.

Gleichzeitig kippt das Technologiebild. KI, Autonomie, vernetzte Plattformen, elektronische Kampfführung, sichere Kommunikation und Cyber machen aus klassischen Rüstungsgütern software- und datengetriebene Produkte. Edge-Computing, Sensorfusion und Datenrechte werden wertbestimmend; Zertifizierungszyklen treffen auf agile Releases. Targets mit Software-, Daten- und Subsystem-Kompetenz rücken in den Mittelpunkt – häufig mit Dual-Use-Optionen und ITAR-Sensitivität. Das erhöht den Reiz von Tech-Roll-ups, aber auch die Prüfungsdichte bei IP/IT, Exportkontrolle und Geheimschutz.

Für Investoren entsteht ein seltenes Setup: staatlich abgesicherte Nachfragepfade, Konsolidierungsdruck, Reshoring und eine aktive Förderkulisse. Im fragmentierten europäischen Markt bieten sich stabile Cashflows und echte Skalierungschancen – über Plattformkäufe, Add-ons, Carve-outs von Primes und Nachfolgelösungen im Mittelstand. Relevante Deal-Formen reichen von Minderheiten/JVs bis Buy-and-Build; längere Haltedauern und flexible Instrumente (z. B. Earn-outs, Vendor Loans) gewinnen an Bedeutung. Für PE-Häuser, deren ESG-Mandat Defense zulässt (und deren Appetit für Regulatorik groß genug ist), ist das attraktiv: cashflowstark, planbar, strategisch relevant – bei professioneller Behörden- und Stakeholder-Fähigkeit.



Defense-M&A bietet stabile Cashflows, staatlich abgesicherte Nachfrage und Konsolidierungspotenzial – bei gleichzeitig hoher regulatorischer Komplexität.

Strategisch: Steigende Budgets im Verteidigungssektor schaffen Chancen für M&A. Targets mit Software-, Daten- und Subsystem-Kompetenzen rücken in den Mittelpunkt. Europas Handlungsfähigkeit erfordert Reshoring und Konsolidierung strategischer Industrien.

Der Sektor bleibt zugleich rechtlich anspruchsvoll. Außenwirtschafts- und Investitionskontrolle, Exportkontrolle, Geheimschutz, Vergabe- und Subventionsrecht prägen jede Transaktion – mit Zeit- und Ergebnisunsicherheit. Erfolgreich ist, wer früh regulatorische Pfade plant, Stakeholder gezielt adressiert und Befunde der DD konsequent in SPA-Mechanik übersetzt: Closing Conditions, Efforts-Standards, Long-Stop/Remedies statt pauschaler MAC-Hebel; Lieferkette, Sicherheitsrollen und Day-1-Readiness im Blick. Kurz: Wer Vorbereitung, Risikoallokation und Behördenlogik beherrscht, wandelt Komplexität in planbare Transaktionen – und erschließt resilienten Zugang zu einem wachsenden, aber anspruchsvollen Markt.

II. Regulatorische Rahmenbedingungen für Zielunternehmen

Investitionen in die Verteidigungsindustrie verlangen ein klares Regulatorik-Raster. Defense-Assets agieren zunächst innerhalb eines strengen Regimes der Exportkontrolle: in Deutschland KWKG und AWG, auf EU-Ebene die EU-Dual-Use-VO; bei US-Bezug zusätzlich ITAR/EAR. Je nach Geschäftsmodell kommen Geheimschutz (BMWK-Geheimschutzordnung, VS-Umgang), Cybersicherheit (BSIG, IT-Sicherheitsrecht) sowie Umwelt-/Gefahrstoffregime (Blm-SchG, StrahlenschutzV, SprengG, REACH, ChemG) hinzu. Diese Pflichten wirken projekt-, personen- und produktbezogen – und damit direkt in Transaktionslogik, Closing-Fähigkeit und Day-1-Readiness hinein.

ITAR/EAR und EU-Regime wirken teils extraterritorial; Re-Export, „deemed export“ (Zugriff ausländischer Personen) und Datenübermittlungen sind genehmigungspflichtig. Lizenzen sind oft ziel-/teilnehmerbezogen und müssen bei Gesellschafterwechsel oder Standortverlagerung angepasst/neu beantragt werden. Für Deals heißt das: frühe Lizenz- und Klassifizierungsprüfung, Transfer/Novation-Fähigkeit klären, CPs/Covenants für Lizenzpflege und Clean-Room-Zugänge, damit die Due Diligence nicht selbst zum (Export-) Verstoß wird.

Darüber hinaus erfordert das Arbeiten mit VS-Material geeignete Sicherheitsüberprüfungen und organisatorische Geheimschutz-Compliance; Zugriff während der Due Diligence kann daher nur über cleared personnel und definierte Datenräume erfolgen. Mit NIS-2 (EU, nationale Umsetzung) verschärfen sich Pflichten zu Risikomanagement, Meldepflichten und Lieferketten-Security; KRITIS-Einstufung kann ebenfalls zusätzliche Anforderungen auslösen. In der Praxis ist wichtig, dass hinreichend segmentiert wird (Netze und Datenräume trennen, Access-Reviews), dass belastbare Nachweise vorliegen (ISO 27001 inkl. SoA, Audit- und Pen- Test-Reports, NIS-2-Policies; nicht nur Papier-Compliance) und dass es Incident-Playbooks gibt, die tatsächlich gelebt werden (Detektion → Containment →

Recovery Prozesse, Rollen/ Eskalation und gesetzliche Meldefristen).

Wertvolle Verteidigungsaufträge unterliegen den Anforderungen der GWB/VSVgV, die Transparenz, Gleichbehandlung, Dokumentation voraussetzen. Integritätsanforderungen werden über Antikorruptionsrecht flankiert: deutsches Recht inkl. IntBestG, soweit einschlägig UK Bribery Act und US FCPA. Typische Vertragsfolgen: Audit-/Kündigungsrechte, Blacklisting-Risiken und strenge Flow-Downs entlang der Kette. Die DD muss diese Vorgaben auf Übertragbarkeit, CoC-Zustimmungen bzw. Anzeigepflichten und Kündigungstrigger abklopfen.

Neben NIS-2/ISO 27001 (Security-Standards) greifen Sanktions-/Embargoregime und das LkSG. Erforderlich sind Screenings (End-Use, End-User, Ownership/Control), Monitoring und Remediation-Prozesse für Zulieferer – inklusive vertraglicher Flow-Down-Pflichten, Audit- Rechten und Exit-Klauseln. Geopolitische Abhängigkeiten (kritische Rohstoffe, Drittstaatenrisiken) gehören in eine Sourcing-Risiko-Map; das ist nur mit Onboarding-, Monitoring und Offboarding-Prozess tatsächlich beherrschbar.

Für M&A-Transaktionen gilt: Das Umfeld ist komplex, aber beherrschbar – wenn man früh strukturiert. Zuerst werden die Pflichten systematisch kartiert und die Befunde konsequent in den DD-Scope und die SPA-Mechanik übersetzt: klare Conditions (CPs), definierte Efforts- Standards, Informationsbarrieren/Clean-Team, sowie Lizenz- und Geheimschutz-Covenants; ergänzt um Long-Stop-Regelungen und praktikable Remedies. Parallel ist die Übertragbarkeit staatlicher Verträge, Lizenzen, Genehmigungen und Zertifizierungen abzusichern, Change-of-Control-Klauseln und Förderauflagen sind belastbar zu prüfen und ggf. mit Zustimmungspfaden zu hinterlegen. So wird Regulierung nicht zum Show-Stopper, sondern zur Deal-Design-Komponente – und verschafft im Prozess einen spürbaren Vorsprung.

III. Fusions- und Investitionskontrollverfahren

Ähnlich wie das operative Geschäft der Defense-Unternehmen unterliegen auch M&A-Transaktionen einem besonders komplexen regulatorischen Rahmen. Zu navigieren sind vor allem zwei Regime: die fusionskontrollrechtliche Prüfung und die Kontrolle ausländischer Direktinvestitionen.

Fusionskontrollverfahren

Die Fusionskontrolle stellt sicher, dass Zusammenschlüsse nicht zu einer erheblichen Behinderung wirksamen Wettbewerbs führen. In Deutschland prüft das Bundeskartellamt (BKartA) auf Grundlage des GWB. Eine Anmeldung ist erforderlich, wenn bestimmte Umsatzschwellen überschritten werden: regelmäßig mehr als 500 Mio. € weltweiter Gesamtumsatz aller Beteiligten, davon mehr als 50 Mio. € in Deutschland bei einem Unternehmen und mindestens 17,5 Mio. € weltweiter Umsatz bei einem weiteren. Alternativ kann – insbesondere bei technologie- oder datenbasierten Geschäftsmodellen – die Transaktionswertschwelle greifen. Vollzug ist erst nach Freigabe zulässig; vorzeitiger Vollzug („Gun Jumping“) ist verboten und bußgeldbewehrt.

Das Verfahren ist zweistufig: In Phase I hat das BKartA einen Monat (nicht vier Wochen) Zeit, freizugeben oder in Phase II überzuleiten; dort kann die Prüfung bis zu fünf Monate dauern. Analysiert werden u. a. Marktanteile, Marktzutrittsschranken, Nachfrageseite, potenzielle Wettbewerbsbehinderungen und Effizienzgewinne. Freigaben können mit Auflagen verbunden sein; im Ausnahmefall wird versagt.

Auf EU-Ebene ist bei Zusammenschlüssen von gemeinschaftsweiter Bedeutung die Europäische Kommission nach der EUMR zuständig (typisch: > 5 Mrd. € weltweiter Umsatz; zudem je > 250 Mio. € EU-Umsatz für mindestens zwei Unternehmen). Die Fristen betragen 25 Arbeitstage (Phase I) bzw. 90 Arbeitstage (Phase II) mit Verlängerungsoptionen.

Die Fusionskontrolle ist ausschließlich wettbewerbsrechtlich motiviert; Fragen nationaler Sicherheit und außenwirtschaftlicher Interessen werden gesondert im Investitionskontrollverfahren geprüft und berühren das Kartellverfahren nicht. Gleichwohl weist die Verteidigungsindustrie Besonderheiten auf. Viele Märkte sind hoch spezialisiert, mit wenigen Anbietern für bestimmte Technologien oder Teilsysteme, sodass auch umsatzkleinere Transaktionen Wirkung entfalten können. Zudem agiert der Staat in Teilmärkten faktisch als Monopsonist (ein dominanter Nachfrager; Abgrenzung zum Monopolist=ein dominanter Anbieter). Beschaffungsplanung, mehrjährige Rahmenverträge und verteidigungspolitische Prioritäten prägen daher die wettbewerbliche Marktdefinition ebenso wie die Beurteilung der Wirkungen auf der Nachfrageseite.

Investitionskontrollverfahren

Investitionen in sicherheitsrelevante Unternehmen unterliegen einer strengen Investitionskontrolle – in Deutschland, der EU und den USA. In Deutschland prüft das BMWK nach AWG/AWV. Besonders sensibel sind Beteiligungen an Rüstungsunternehmen, Dual-Use- Herstellern und in Bereichen kritischer Infrastruktur. Im Fokus stehen sicherheitsrelevante Technologien, Versorgungssicherheit und mögliche Einflussnahmen ausländischer Investoren. Bereits Minderheitsbeteiligungen können meldepflichtig sein und eine vertiefte Prüfung auslösen. Das Verfahren ist zweistufig: Vorprüfung mit einer Frist von zwei Monaten, anschließend – falls eröffnet – eine vertiefte Prüfung mit einer verlängerbaren Vier-Monats- Frist.

Auf EU-Ebene koordiniert die EU-Screening-Verordnung (VO (EU) 2019/452) einen unionsweiten Kooperationsmechanismus. Die Entscheidung verbleibt bei den Mitgliedstaaten; die Kommission kann Stellung nehmen und eine vertiefte Prüfung anregen. Gerade bei grenzüberschreitenden Investments in verteidigungs- oder infrastrukturbezogene Unternehmen können diese Abstimmungen die Verfahren verlängern.

In den USA gilt CFIUS als eines der weitreichendsten Regimes. Bereits indirekte US-Bezüge – etwa Standort, Beteiligte oder Zugriff auf sensible Daten/Technologien – können eine Prüfungspflicht begründen. Das Verfahren ist mehrstufig, politisch sensibel und nur begrenzt vorhersehbar; mögliche Ergebnisse reichen von Auflagen über strukturelle Anpassungen bis zum Verbot. Durch FIRRMA wurde der Anwendungsbereich spürbar erweitert.

Konsequenz für Transaktionen: investitionskontrollrechtliche Themen sind früh in Struktur und Zeitplan zu spiegeln (CPs, Efforts-Standards, Long-Stop) und parallel zur Fusionskontrolle zu steuern – insbesondere bei Investments in Technologie, Rüstung, Cybersicherheit oder Infrastruktur.

IV. Transaktionsrechtliche Erfolgsfaktoren im Defense-M&A

M&A-Transaktionen in der Verteidigungsindustrie liegen an der Schnittstelle von Wirtschaft, Sicherheitspolitik und Technologie. Die Regulatorik ist dicht, die Rechtsrisiken vielfältig und die Interessen politisch sensibel. Umso wichtiger ist ein methodisch strukturierter Prozess, der branchenspezifische Risiken früh erkennt, behörden- und stakeholderfähig ist und die rechtliche Absicherung konsequent mitdenkt.

Frühe Vorbereitung, eine transaktionsspezifische Legal Due Diligence (fokussiert auf die richtigen Systeme statt Einzelfälle) und eine klug austarierte Vertragsmechanik. Dazu gehören eine klare Closing-Architektur (FK/IK-CPs, Efforts-Standards, Long-Stop), ein fokussierter Garantien-/Freistellungskatalog und ein professionell gesteuertes Stakeholder- und Behördenmanagement, das Zustimmungen sichert und Auflagen steuerbar hält. Ebenso wichtig ist die Post-Merger-Integration mit Day-1-Readiness – insbesondere bei sicherheitsrelevanten Projekten, VS-Material sowie personenabhängigen Genehmigungen und Zertifizierungen.

Anforderungen an die Legal Due Diligence

Die Legal Due Diligence im Verteidigungssektor folgt eigenen Maßstäben. Neben den klassischen rechtlichen Prüfbereichen liegt der Fokus auf einer tiefgehenden Bewertung der regulatorischen und technologiebezogenen Risikofelder, die in dieser Branche transaktionsentscheidend sind. Weist das Target einen starken Technologiefokus auf, steigen die Anforderungen an die Prüfung von geistigem Eigentum und digitaler Infrastruktur. Ein hoher Anspruch an regulatorische Konformität sollte dabei stets zum Kern der Geschäftsgrundlage gehören.

Im Defense-Tech-Sektor ist IP häufig das zentrale strategische Asset. Entsprechend ist der Prüfgegenstand der Legal DD auszurichten: Patente, Marken, Designs, Urheberrechte – plus relevante Softwarebestandteile, einschließlich Open-Source-Komponenten und

durch Drittsoftware entstehende Rechteketten. Im Mittelpunkt stehen Inhaberschaft und wirtschaftliche Nutzbarkeit der IP-Rechte. Drittbeteiligungen – insbesondere öffentliche Fördergeber oder Kooperationspartner – sind auf Nutzungseinschränkungen zu prüfen (Zugriffsrechte, Nutzungsvorbehalte, Rückforderungsmechanismen, etwa bei EDF/nationaler Förderung). Nationale Sicherheitsinteressen oder eine VS-Einstufung können die Übertragbarkeit erheblich begrenzen. In grenzüberschreitenden Konstellationen erhöht sich die Komplexität zusätzlich, da Exportbeschränkungen, Geheimschutzvorgaben und Informationssicherheitsanforderungen den Datenzugang limitieren und ggf. sicherheitsüberprüftes Personal erfordern.

Unabhängig vom Technologiebezug ist zu prüfen, ob belastbare Systeme die dauerhafte Einhaltung der hohen regulatorischen Anforderungen sicherstellen. Dazu zählen insbesondere Exportkontrollvorgaben, alle erforderlichen Genehmigungen sowie Prozesse zur Einhaltung von Auflagen und Nebenbestimmungen. Arbeiten mit Verschlusssachen oder sicherheitsempfindliche Projekte verlangen passende Zulassungen und Sicherheitsüberprüfungen – etwa nach Maßgabe der Geheimschutzordnung des BMWK oder einschlägiger europäischer Bestimmungen. Sensibel ist auch die Übertragung sicherheitsrelevanter Rollen oder Zugriffsbefugnisse im Rahmen der Transaktion: Nachvollziehbare, organisatorisch verankerte Geheimschutz- Compliance ist regelmäßig Teil der Deal-Strategie. Zunehmend im Fokus steht die Lieferkette: Bezug kritischer Komponenten ist oft mit geopolitischen Risiken, IT-Sicherheitsthemen und regulatorischer Abhängigkeit verbunden. Die DD sollte systematisch erfassen, ob Verbindungen zu sanktionierten Unternehmen/Drittstaaten bestehen und ob LkSG-, NIS-2- sowie branchenspezifische Standards (z. B. NIST SP 800-171, ISO 27001) eingehalten werden – auch bei Subunternehmern und Partnern. Wesentlich ist neben dem Status quo die Prozessqualität: Sind Exportkontroll- und Genehmigungsprozesse formalisiert? Existiert ein funktionierendes Reg-Risikomanagement? Sind Mitarbeitende geschult und ist der Zugang zu genehmigungsrelevanten Informationen geregelt?

Gleichzeitig gilt: Eine vollständige Konformität ist in globalen Lieferketten faktisch selten erreichbar. Für eine seriöse Risikoeinschätzung braucht es Branchenkenntnis, Erfahrungswerte und Urteilsvermögen. Gerade ausländische Zulieferer geben häufig weitreichende Konformitätserklärungen ab – deren Substanz ist nicht immer vollständig verifizierbar. Risiken sind im Gesamtbild zu bewerten; eine rein formalistische Prüfung kann tragfähige Vorhaben blockieren, ohne dass dies aufgrund des materiellen Risikoprofils gerechtfertigt wäre. Gleichwohl sind die Ergebnisse transaktionsentscheidend: Werden systematische Schwächen festgestellt, die Verstöße gegen Exportkontrollvorschriften oder andere wesentliche Anforderungen (z. B. Genehmigungsaufgaben, Geheimschutz- oder Sorgfaltspflichten) wahrscheinlich machen, oder liegt bereits eine deutlich unvollständige Genehmigungslage vor, sind die Grenzen des souveränen Urteilsermessens erreicht – das Risikoprofil muss in die Ratio der Gesamttransaktion eingewertet werden.

Auch die Prüfung der kommerziellen Vertragsstruktur ist im Defense-Bereich von besonderer Bedeutung, da wesentliche Beziehungen häufig auf langfristigen, strategischen und öffentlich- rechtlich geprägten Verträgen beruhen. Im Vordergrund stehen staatliche Rahmen- und Lieferverträge, SLAs, Wartungsverträge sowie weitere Vereinbarungen, die Umsatzsicherheit und Planbarkeit tragen. Für alle wesentlichen Verträge ist zu verifizieren, ob sie wirksam bestehen, rechtlich durchsetzbar und aus Erwerbersicht im Rahmen der Gesamtrechtsnachfolge übertragbar sind. Besondere Aufmerksamkeit gilt Change-of-Control-Klauseln, Kündigungsrechten oder Zustimmungsvorbehalten, die durch die Transaktion ausgelöst werden können.

In öffentlich-rechtlich geprägten Vertragsverhältnissen – etwa bei Behördenaufträgen oder Förderprojekten – ist zusätzlich zu prüfen, ob der Vertrag ordnungsgemäß zustande gekommen ist, ob ein förmliches Vergabeverfahren zugrunde liegt und ob im Falle eines Eigentümerwechsels eine Neuausschreibung oder Genehmigungspflicht droht. Ferner ist zu klären, ob die Zielgesellschaft in laufende Zuwendungs-/Subventionsverhältnisse eingebunden ist; hier kann schon eine nicht anzeigepflichtige Änderung der Eigentümerstruktur Rückforderungen auslösen. Auch vertragliche Rückzahlungs- oder Nachschusspflichten in Projektverbänden sind sorgfältig zu prüfen.

Erfolgreiche Kaufvertragsgestaltung

Die Gestaltung des Kaufvertrags erfordert neben dem klassischen M&A-Handwerkszeug die Berücksichtigung branchenspezifischer regulatorischer, sicherheitsrelevanter und technologischer Anforderungen. Zentrales Element ist ein auf die Branche zugeschnittener Garantien- und Freistellungskatalog, der die Ergebnisse der Legal Due Diligence gezielt aufgreift. Durch das Zusammenspiel einer fundierten Due Diligence und klarer Haftungsallokation lässt sich ein ausgewogener Interessenausgleich im Hinblick auf potenzielle Risiken erreichen.

Sind wesentliche Verträge mit Change-of-Control-Klauseln versehen oder bestehen sonstige Unwägbarkeiten bei wesentlichen Werttreibern, muss dies vertraglich adressiert werden. Dabei ist zu bestimmen, welche Maßnahmen von wem (regelmäßig der Verkäufer) bis wann zu ergreifen sind, um den Fortbestand der Vertragsbeziehung bzw. des Werttreibers zu sichern – und welche Rechtsfolgen eintreten, wenn dies nicht oder nicht fristgerecht gelingt. Solche Regelungen werden typischerweise im Rahmen der Closing Conditions verortet und mit entsprechenden Pflichten hinterlegt.

Angesichts teils erheblicher Zeiträume zwischen Signing und Closing – u.a. wegen investitions-/außenwirtschaftsrechtlicher Prüfungen und regulatorischer Genehmigungen – wird in deutschen M&A-Transaktionen auch häufiger mit MAC- bzw. No-MAC-Klauseln gearbeitet. Material Adverse Change bezeichnet das Instrument, mit dem sich Käufer vom Vertrag lösen können, wenn sich die Zielgesellschaft zwischen Signing und Closing wesentlich nachteilig verändert. Bei der Festlegung von Tatbestand und Rechtsfolgen ist zu berücksichtigen, dass lange Vollzugszeiträume häufig durch Umstände entstehen, die überwiegend dem Verantwortungsbereich des Käufers zugeordnet werden (z. B. Fusionskontrolle aufgrund Käuferstellung oder Investitionskontrolle bei ausländischen Erwerb). Eine ausgewogene Risikoverteilung muss das abbilden und darf nicht pauschal alle Veränderungen der Pre-Closing- Phase dem Verkäufer zurechnen.

Es empfiehlt sich, vertraglich klar zu definieren, welche Veränderungen zwischen Verpflichtungsgeschäft und Vollzug als erheblich gelten und welche Rechtsfolgen daran

anknüpfen. Zentral ist die präzise Bestimmung eines „wesentlichen nachteiligen Ereignisses“, insbesondere im Hinblick auf (i) regulatorische Änderungen (z. B. neue Exportrestriktionen), (ii) den Verlust wesentlicher Aufträge oder Genehmigungen, (iii) Sicherheitszwischenfälle oder (iv) technologische Ausfälle, Störungen oder externe Angriffe. Unbestimmte oder zu weite Formulierungen erhöhen das Streitrisiko. Die Risikoverteilung sollte daher auf das spezifische Geschäftsmodell des Targets zugeschnitten sein und realistische Szenarien adressieren – ohne dem Käufer ein beliebiges Rücktrittsrecht zu eröffnen.

Im Übrigen sind Unternehmenskaufverträge maßgeschneidert auf die Spezifika der jeweiligen Transaktion und sollten gemeinsam mit den einschlägigen Experten erarbeitet werden, um alle relevanten Aspekte rechtssicher zu erfassen.

Stakeholder Management

Aus Verkäufersicht sollte ein besonderer Fokus auf das Stakeholder Management gelegt werden; aus Sicht des Autors keine Kür, sondern Pflicht. Zu Beginn der Transaktionsplanung steht das systematische Mapping mit klaren Prioritäten: SPA-relevante Adressaten – also alle Stellen, deren Zustimmung/Anzeige/Auflage voraussichtlich das Closing bedingt – haben Priorität 1; danach folgen öffentliche Auftraggeber, sicherheitskritische Zulieferer, Kooperationspartner und interne Schlüsselpersonen. Für jede Gruppe werden Zielbild, verantwortliche Person (Owner) und Zeitschiene definiert. Die Milestones orientieren sich an voraussichtlichen Terminen zur Erfüllung von Vollzugsvoraussetzungen, Long-Stop und internen Entscheidungsfenstern; Eskalationspfade sind vorab festzulegen, damit Verzögerungen steuerbar bleiben.

Stakeholder Management findet dabei innerhalb bestehender Compliance- und Governance- Schranken statt: Gun-Jumping ist zu vermeiden, d. h. keine Vorab-Steuerung des Targets und kein Austausch wettbewerbssensibler Informationen außerhalb des Clean-Teams. Operative Informationsbarrieren, abgestufte Disclosure-Levels (insb. VS-/ Exportkontrollbezug) und Joint-Communications-Freigaben sorgen für Konsistenz.

Kommunikation, Q&A und Entscheidungen werden protokolliert; Zuständigkeiten und Vertretungen sind eindeutig geregelt.

Aus dem Mapping folgt dann eine klare Risikoagenda: Verzögerung oder Versagung in Fusions- und Investitionskontrollverfahren, scheiternde Change of Control-Zustimmungen, Rückforderungen in Förderbeziehungen, Abwanderung von „must-keep“-Lieferanten, Leaks oder negative politische Signale sowie widersprüchliche Botschaften. Dem stehen messbare Potenziale gegenüber: ein planbarer Closing-Pfad durch frühzeitige Auflagenklärung, konstruktiv verhandelbare Auflagen/Übergangsregelungen, Sicherung bzw. Verlängerung von Aufträgen, Stabilisierung kritischer Lieferanten und Akzeptanzgewinne bei Behörden und Auftraggebern. Angestrebt wird höchste Transaktionssicherheit sowie Day-1-Readiness des Targets nach Vollzug. Das Interesse der Käuferseite insbesondere an Day-1-Readiness ist legitim, seine Einbindung jedoch rechtlich nur begrenzt möglich (und aus Verkäufersicht gewünscht).

Letztlich findet in jeder Transaktion Stakeholder Management statt. Der Unterschied liegt in der Steuerung: strukturiert & strategisch vs. ad hoc. Nur ein strukturierter und strategischer Weg minimiert Risiken und realisiert Chancen.

V. Unser Fazit

Defense-M&A ist ein zunehmend spannendes Feld. Transaktionen scheitern hier selten am Kapital, sondern an mangelnder Souveränität im Umgang mit Regulatorik und an schwacher Risikoallokation zwischen Käufer und Verkäufer. Das Rezept: Regulatorik, Lieferkette und staatliche Vertragslogik frühzeitig in SPA-Mechanik und ein strategisches Stakeholder-Management übersetzen. Konkret auf die Montagmorgen-Agenda gehören eine Legal DD auf Systemrisiken (Exportkontrolle, Geheimschutz, LkSG/NIS-2, Lieferkette); die Absicherung von Langläufern/Behördenverträgen (Übertragbarkeit, CoC/Zustimmungen, Kündigungsrechte, Abnahmen); eine saubere Closing-Architektur (FK/IK als CPs, klarer Efforts-Standard, Long-Stop/Remedies, Stakeholder-Priorisierung); werttreiberbezogene Garantien/Freistellungen statt Standardkatalog; ein verbindlicher Stakeholder-Plan (Mapping mit Prios, Clean Team, Joint Comms, Approval-Tracker); sowie Day-1-Readiness mit Rollen/Zugriffen (VS/IT), TSAs und festen Kommunikations- und Eskalationspfaden.

Wer diese Punkte früh orchestriert, erschließt im Defense-Tech-Umfeld resilienten Zugang zu einem wachsenden, aber anspruchsvollen Markt – und verwandelt regulatorische Komplexität in planbare Transaktionen.



Defense-M&A scheitert selten am Kapital, sondern an Regulierung, Risikoallokation und Stakeholder-Management.

Einordnung: Entscheidend für erfolgreiche Defense-Transaktionen sind eine saubere Closing-Struktur, regulatorische Vorbereitung und ein strategisches Stakeholder-Management.

ROHDE BAIER

RECHTSANWÄLTE

ROHDE BAIER Rechtsanwälte mit Standorten in Frankfurt am Main und München vereint die Qualität und Erfahrung internationaler Großkanzleien mit wirtschaftlicher Lösungsorientierung, Pragmatismus und umfassender Branchenkenntnis in einer schlagkräftigen Kanzleiboutique.

Das Team von ROHDE BAIER steht Ihnen als Sparringspartner bei Unternehmenstransaktionen sowie allen Themen des Gesellschafts-, Handels- und Immobilienrechts zur Verfügung.

ROHDE BAIER

www.rohdebaier.de

Ansprechpartner



Thorsten Rohde, Mag. iur. (Dublin) ist Gründungspartner von ROHDE BAIER. Er berät nationale und grenzüberschreitende Unternehmenstransaktionen im Wirtschafts- und Gesellschaftsrecht mit besonderem Fokus auf M&A, Private Equity, Venture / Growth Capital sowie Search-Fund-Transaktionen.

Thorsten Rohde, Mag. iur. (Dublin) is a founding partner of ROHDE BAIER and advises national and cross-border corporate transactions in commercial and corporate law with a special focus on M&A, PE, venture / growth capital and search fund transactions.

☎ +49157 850 18 223

✉ beier@rohdebaier.de