STIFTERVERBAND

ANALYSE

SICHERHEITS- UND VERTEIDIGUNGS-FORSCHUNG NEU DENKEN

Innovationskraft für Souveränität und Wertschöpfung

Mit analytischer Unterstützung von:

McKinsey & Company

INHALT

Diese Analyse basiert auf einer Vielzahl von Quellen, darunter auch Analysen von McKinsey & Company. Der Stifterverband ist verantwortlich für die Schlussfolgerungen und Ableitungen aus diesen Recherchen.

EXECUTIVE SUMMARY

Forschung und Innovation im Bereich der Sicherheit können für Deutschland einen doppelten Nutzen bringen: Sie stärken Verteidigungsfähigkeit, Resilienz und technologische Souveränität und fördern gleichzeitig neue Ideen, Produktivität und wirtschaftliche Leistung. Die Hebelwirkung ist enorm: Erkenntnisse aus den USA zeigen, dass Investitionen in Verteidigungsforschung unter den richtigen Voraussetzungen langfristig eine 1,7- bis 2-fache Wirkung auf die gesamte Wirtschaft entfalten können. Für Deutschland würde sich dieser Multiplikatoreffekt langfristig in ein zusätzliches Wirtschaftswachstum von 22 Milliarden Euro jährlich übersetzen.

Die vorliegende Analyse zeigt, dass wesentliche Voraussetzungen für die Realisierung dieses Potenzials darin liegen, dass Investitionen in die Forschung ausreichend hoch und die Rahmenbedingungen für ein nahtloses Ineinandergreifen von Sicherheit und Innovation vorhanden sind. Auch wenn die USA und andere Länder – wie Israel und Südkorea – zeigen, dass verteidigungsbezogene Forschung und Entwicklung über ihren unmittelbaren Sicherheitszweck hinaus Wirkung entfalten können, müssen Deutschland und Europa die dort erprobten Konzepte an ihre eigenen Sicherheits- und Innovationssysteme anpassen. Eine besondere Rolle bei der besseren Verzahnung der beiden Politikbereiche Sicherheit und Verteidigung auf der einen sowie Forschungs- und Innovationspolitik auf der anderen Seite spielen parlamentarische Kontrolle, rechtsstaatliche Verfahren, verantwortungsvolle Exportregeln, die Aufgabenverteilung von Bund und Ländern sowie die Zusammenarbeit in Europa. Ziel ist entsprechend nicht die Entwicklung eines militärisch geprägten Innovationssystems, sondern ein verantwortungsvoll geregeltes Modell, das zivile und sicherheitsbezogene Entwicklungen miteinander verbindet – mit klaren Anforderungen, Forschungsfragen, die für verschiedene Technologien offen sind, der Bereitstellung von Risikokapital, Erprobung, Anschlussinvestitionen und einer breiten Umsetzung in der Industrie.

Die vorliegende Analyse untersucht die deutsche sicherheitsbezogene Forschungslandschaft auf Basis von Interviews mit Expertinnen und Experten aus den Bereichen Wirtschaft, Wissenschaft, Politik und sicherheitsnahen Institutionen. Ergänzend wurden Daten der Startup-Datenbank startupdetector zur Analyse von Start-up-Aktivitäten herangezogen. Im Zentrum steht die Frage, inwiefern sie im Sinne eines produktiven Innovationsökosystems mit Staat, Wirtschaft und Startups aufgestellt ist. Wesentliche Erkenntnisse aus dieser Analyse sind:

- **Innovationsfähigkeit als Sicherheitsfaktor** – Die Fähigkeit, technologische Entwicklungen schnell zu verstehen und anzuwenden ist ein entscheidender Faktor für die sicherheitspolitische Handlungsfähigkeit.
- **Strukturelle Defizite im Innovationssystem** – Trotz einer starken Basis in Forschung, Industrie und einer wachsenden Start-up-Landschaft im Sicherheitsbereich zeigen sich strukturelle Brüche im deutschen System. Die mangelnde systematische Verknüpfung zwischen den vorhandenen Stärken und den konkreten Bedarfen von Sicherheit und Verteidigung gilt als größte Hürde.
- **Vier zentrale Engpässe** – Hemmnisse, die eine effektive Nutzung der Potenziale verhindern:
    1. Zielsetzung: Es fehlt an einer klaren und technologieoffenen Übersetzung von Sicherheitsbedarfen in strategische Prioritäten.
    2. Finanzierung: Die Finanzierung ist lückenhaft und unterstützt den Übergang von der Forschung und Demonstration zur Erprobung, Beschaffung und industriellen Skalierung nicht systematisch.
    3. Kooperation: Die Zusammenarbeit zwischen Wissenschaft, Wirtschaft, Staat und Sicherheitsakteuren ist unzureichend, was den Transfer von wissenschaftlichen Potenzialen in anwendungsfähige Lösungen behindert.
    4. Talente und Kultur: Unklare rechtliche und ethische Rahmenbedingungen sowie administrative Hürden führen zu Unsicherheit und hemmen das Engagement in der sicherheitsrelevanten Forschung.

Insgesamt zeigt die Analyse, dass die zentrale Herausforderung in Deutschland nicht ein Mangel an Potenzialen ist, sondern die unzureichende und fragmentierte Nutzung dieser Potenziale. Die vorhandenen

Stärken in Wissenschaft und Wirtschaft werden nicht effektiv mit den sicherheitsrelevanten Anforderungen verbunden, was die Entfaltung einer vollen sicherheitspolitischen und wirtschaftlichen Wirkung verhindert.

Methodik:

Grundlagen der Ergebnisse dieser Analyse:

- **Qualitative Interviews mit Expertinnen und Experten**: Qualitative Interviews mit 11 Expertinnen und Experten aus deutschen Hochschulen, die im Sicherheitskontext forschen und lehren, deutschen Defence Tech Start-ups, Wirtschaftsinstituten, Forschungseinrichtungen sowie dem sicherheits- und verteidigungspolitischen Umfeld. Alle Daten wurden im vierten Quartal 2025 erhoben.
- **Übertragung eines empirisch belegten ökonometrischen Modells zu langfristigen Wachstumseffekten militärischer FuE-Ausgaben (Forschung und Entwicklung) in den USA (*Multiplikatoreffekte*) auf den deutschen Kontext:** Dazu wurde der zugrundeliegende Innovationsprozess in vier aufeinander aufbauende Stufen zerlegt: strategische Ambition, Förder- und Programmmechanismen, Forschungspool und -cluster sowie Technologietransfer und Skalierung. Die Stufen wurden entsprechend ihrer Bedeutung für die gesamtwirtschaftliche Wertschöpfung gewichtet – mit höherem Gewicht für die späten Stufen, da der Großteil der gesamtwirtschaftlichen Wirkung erst durch die erfolgreiche Überführung von Innovationen in marktfähige Produkte und deren breite zivile Anwendung entsteht. Für jede Innovationsstufe wurde Deutschland anhand internationaler Indikatoren mit den USA verglichen. Daraus wurde abgeleitet, welcher Anteil der im US-Modell beobachteten Wirkung unter deutschen Rahmenbedingungen realisierbar erscheint. Die gewichtete Zusammenführung dieser stufenspezifischen Bewertungen bildet die Grundlage für die Ableitung des deutschen Multiplikators.
- **Analyse der Hochschullandschaft**: In die Analyse der Hochschullandschaft wurden 419 Hochschulen in Deutschland einbezogen. Für die Analyse wurde ein kategoriengeleitetes Vorgehen gewählt. Zunächst wurden drei analytische Sphären definiert: die militärische Kernforschung, die technologische Sicherheitssphäre sowie die nicht-technische Sicherheitssphäre. Diesen drei Kategorien wurden anschließend einschlägige Studienbereiche zugeordnet. Auf dieser Grundlage erfolgte eine systematische Sichtung der Webseiten aller deutschen Universitäten. Dabei wurde für jede Universität erfasst, ob Studiengänge angeboten werden, die einer der drei Peripherien zugeordnet werden können. Wurde mindestens ein Studiengang identifiziert, der der militärischen Kernforschung oder der technologischen Sicherheitsperipherie zuzurechnen ist, wurde die betreffende Universität der entsprechenden Kategorie zugeordnet. Auf diese Weise konnte sichtbar gemacht werden, an welchen Universitäten sicherheits- und militärrelevante Studienangebote in den definierten Bereichen institutionell verankert sind.
- **Start-up-Analyse:** Die Analyse basiert auf einem regelbasierten Klassifikationsansatz zur Identifikation sicherheitsrelevanter Organisationen in Deutschland. Als Datengrundlage wurden insbesondere Daten über Start-ups genutzt und mit weiteren Informationen über Hochschulen und außeruniversitäre Forschungseinrichtungen angereichert. Die Klassifikation kombiniert formale Merkmale wie WZ-Codes (Wirtschaftszweig-Codes) mit inhaltlichen Signalen aus Keywords, Kurzbeschreibungen und weiteren Kontextangaben, um Organisationen verschiedenen Sicherheitsstufen zuzuordnen.

1. SICHERHEIT ALS INNOVATIONSAGENDA: WIE FORSCHUNG EINEN DOPPELTEN NUTZEN ENTFALTET

1.1 Doppelte Dividende: Sicherheit und Wertschöpfung

Die vorliegende Analyse bekräftigt Erkenntnisse und Erfahrungen aus Ländern wie USA oder Israel: Sicherheitsrelevante Forschung und Innovation stärken Verteidigungsfähigkeit, Resilienz und technologische Souveränität. Wo es gelingt, Forschung in Anwendung, Erprobung und Skalierung zu überführen, können daraus zusätzlich Innovations- und Wertschöpfungseffekte entstehen. Diese *doppelte Dividende* entsteht über Spillover-Effekte: Wissen, Technologien und Kompetenzen werden über ihren ursprünglichen Anwendungskontext hinaus nutzbar. Im Fokus stehen Technologien an der Schnittstelle von zivilen, behördlichen und verteidigungsbezogenen Anwendungen.

Dabei sollte jedoch nicht jede Form der Diffusion als Selbstzweck verstanden werden: Gerade bei Dual-Use-Technologien ist entscheidend, mögliche zivile, sicherheitsbehördliche und militärische Anschlussverwendungen früh mitzudenken und verantwortungsvoll zu steuern. Diese Analyse spricht von Dual Use, Mehrfachnutzung und zivil-militärischer Anschlussfähigkeit. Ziel ist dabei nicht, zivile Forschung zu militarisieren, sondern sicherheitsrelevante Potenziale, Risiken und Anwendungsmöglichkeiten frühzeitig zu erkennen und verantwortbar zu organisieren. Auch wenn diese Begriffe auf der Sachebene lediglich beschreiben, dass Wissen und Technologien flexibel für unterschiedliche Zwecke eingesetzt werden können, birgt diese Vielseitigkeit in der Praxis oft komplexe Zielkonflikte – etwa bei der Exportkontrolle, beim Wissensschutz oder durch generelle Missbrauchsrisiken. Umso wichtiger ist es, Dual-Use-Potenziale weder zu idealisieren noch pauschal zu problematisieren, sondern ihre Nutzung durch klare ethische sowie rechtliche Leitplanken und verlässliche Kontrollstrukturen von Beginn an sicher und verantwortungsvoll zu steuern. Dual Use beschreibt also ein Möglichkeitsfeld, nicht bereits dessen normative Bewertung.

Aus ökonomischer Sicht stellt sich die Frage, ob zusätzliche staatliche Ausgaben für Forschung und Entwicklung (FuE) neben ihrem eigentlichen sicherheits- und verteidigungspolitischen Zweck auch der Gesamtwirtschaft zugutekommen. Entscheidend ist dabei die Art der Investition: Während der reine Kauf bestehender Systeme oder laufende Betriebskosten vor allem kurzfristig wirken, kann technologieoffene FuE langfristig die Produktivität steigern. Dies gelingt, wenn sie neue Technologien hervorbringt, private Investitionen anstößt, industrielle Skalierung fördert und breite zivile Märkte eröffnet. Ob diese Effekte jedoch tatsächlich eintreten, hängt maßgeblich davon ab, ob eine zivile Anschlussnutzung rechtlich, politisch und gesellschaftlich vertretbar ist.

Wie erheblich diese Wirkung sein kann, zeigt internationale Evidenz (Antolin-Diaz und Surico, 2025). Für die USA werden im Bereich der verteidigungsbezogenen FuE langfristige Multiplikatoren von 1,7 bis 2,0 beschrieben – das heißt, jeder zusätzliche Euro kann dort langfristig 1,70 bis 2,00 Euro an gesamtwirtschaftlicher Wertschöpfung auslösen. Dieser internationale Befund ist nicht als direkte Blaupause zu lesen: Er verweist auf mögliche Wirkungen unter bestimmten institutionellen Bedingungen, sagt aber noch nichts darüber aus, wie diese Wirkungen in einem deutschen oder europäischen Ordnungsrahmen verantwortungsvoll hergestellt werden können.

Ein Blick auf die zugrundeliegenden Wirkmechanismen zeigt, dass trotz qualifizierter Fachkräfte und exzellenter Forschung dieser Multiplikatoreffekt und die damit verbundene doppelte Dividende hierzulande bislang weitgehend ausbleiben dürften. Der Grund hierfür liegt in strukturellen Brüchen in der Innovationskette, die wie ein Trichter funktioniert. Auf dem Weg von der Forschungsinvestition bis zur kommerzialisierten Technologie verliert das deutsche System auf jeder Stufe an Wirkungskraft. Bereits zu Beginn reduziert eine fehlende strategische Ambition das Startpotenzial: Die für die Analyse durchgeführten Interviews zeigen, dass anstelle disruptiver Hochtechnologien häufig die inkrementelle Verbesserung bestehender Systeme priorisiert wird, oft gepaart mit einer stark beschaffungsorientierten und bürokratischen Fördermechanik. Die zentrale Wachstumsbremse liegt jedoch am Ende dieser Kette, beim Technologietransfer in die zivile Realwirtschaft. Eine historisch gewachsene, fragmentierte Innovationslandschaft sowie Defizite in der

Skalierungsfinanzierung durch ein vergleichsweise geringes Risikokapital verhindern, dass sicherheitsrelevante Forschung erfolgreich in zivile Anwendungen mündet. Hinzu kommt, dass technologische Diffusion gerade im Dual-Use-Bereich nicht nur eine Frage der ökonomischen Anschlussfähigkeit ist, sondern auch von klaren Regeln, Verantwortung und belastbaren Governance-Strukturen abhängt.

Diese kumulierten Schwächen senken die wirtschaftliche Hebelwirkung der staatlichen Investitionen in Deutschland erheblich. Auf Basis der vorliegenden Analyse der deutschen sicherheitsbezogenen Forschungslandschaft ist davon auszugehen, dass der aktuelle Multiplikator für verteidigungsbezogene FuE in Deutschland lediglich einen Wert von 0,9 erreicht. Die investierten Mittel spielen ihre eigenen Kosten an zusätzlicher Wertschöpfung also nicht wieder ein. Wie signifikant das ökonomische Potenzial tatsächlich ist, zeigt ein Gegenentwurf: Würde Deutschland seine verteidigungsbezogenen Forschungsinvestitionen auf das Benchmark-Niveau der USA von 0,36 Prozent des Bruttoinlandsprodukts (BIP) anheben und durch konsequente Reformen ebenfalls einen Multiplikator von 1,7 erreichen, ergäbe sich daraus ein langfristiger gesamtwirtschaftlicher Wachstumsimpuls von mehr als 22 Milliarden Euro jährlich. Dieses Szenario ist jedoch keine bloße Rechengröße. Es veranschaulicht vielmehr, was ein leistungsfähigeres Innovationssystem unter bestimmten Bedingungen bewirken könnte.

Die Effekte treten zudem nicht automatisch ein. Die für die Analyse durchgeführten Interviews identifizierten Hemmnisse zeigen, dass eine reine Budgeterhöhung die strukturellen Herausforderungen in Deutschland nicht lösen wird. Eine Steigerung dieser Hebelwirkung lässt sich vor allem durch die gezielte Stärkung der Übergänge im Innovationsprozess erreichen. Nur wenn bestehende Schnittstellen durch eine engere Kooperation der Akteure in Politik, Forschung und (ziviler) Privatwirtschaft verbessert werden, kann sicherheitsrelevante FuE ihr Potenzial in Form von branchenübergreifenden Produktivitätssteigerungen und zusätzlicher Wertschöpfung bestmöglich entfalten.

Die Übertragung des US-Modells auf Deutschland stößt aufgrund unterschiedlicher Systemstrukturen an Grenzen. Entscheidend ist, die dort wirksamen Mechanismen in ein eigenes, für Deutschland funktionierendes Innovationssystem zu übersetzen. Dabei kommt dem Staat als primärer Bedarfsträger eine zentrale Rolle als Weichensteller zu: Indem er klare Sicherheits- und Verteidigungsbedarfe definiert, Forschungsfragen technologieoffen stellt und disruptive Forschung strategisch priorisiert, ebnet er den Weg für private Anschlussfinanzierungen und die spätere industrielle Skalierung.

Diese Logik wird besonders sichtbar an Technologien, die zivile, sicherheitsbehördliche und militärische Anwendungen verbinden. Kommerzielle Satellitendaten fließen heute in militärische Lagebilder ein. Zivile Kleindrohnen sind für das Kriegsgeschehen in der Ukraine relevant. Beide Beispiele zeigen, dass sicherheitsrelevante Innovation immer häufiger dort entsteht, wo zivile Technologieentwicklung, militärische Bedarfe und neue Anwendungskontexte zusammenfallen. Zugleich zeigen sie, dass gerade solche Konvergenzen nicht nur Chancen eröffnen, sondern auch Fragen von Regulierung, Kontrolle und Verantwortung aufwerfen.

Sicherheit muss deshalb als Innovationsagenda begriffen werden: nicht als Militarisierung ziviler Forschung, sondern als Fähigkeit, sicherheitsrelevante Potenziale, Risiken und Anwendungsmöglichkeiten frühzeitig zu erkennen und verantwortbar in Forschung, Testfelder und skalierbare Anwendungen zu übersetzen.

1.2 Sicherheit breiter denken

Die für die Analyse durchgeführten Interviews bekräftigen: Der potenzielle Nutzen sicherheitsrelevanter Forschung lässt sich nur erzielen, wenn Sicherheit breit verstanden wird. Krieg in Europa, hybride Bedrohungen, Angriffe auf kritische Infrastrukturen und technologische Abhängigkeiten zeigen, dass Sicherheit nicht mehr allein militärische Verteidigungsfähigkeit meint. Sie betrifft die Handlungsfähigkeit von Staat, Wirtschaft und Gesellschaft insgesamt.

Sicherheit umfasst heute weit mehr als klassische Verteidigung: Auch die Verlässlichkeit von Energieversorgung, Kommunikationsnetzen oder Gesundheitswesen in Krisenzeiten ist eine essenzielle Frage der Resilienz. Aus diesem Grund arbeitet diese Analyse mit dem Begriff der sicherheitsrelevanten Forschung und Innovation. Dies schließt gezielt solche FuE-Aktivitäten, Transfers und Anwendungen ein, die neben der militärischen Handlungsfähigkeit auch kritische Infrastrukturen, die technologische Souveränität sowie die gesamtstaatliche Widerstandskraft stärken.

Diese Rahmung orientiert sich eng am Wissenschaftsrat, der sicherheitsrelevante Forschung als elementaren Beitrag zur inneren und äußeren Sicherheit sowie zur gesamtgesellschaftlichen Resilienz versteht und zeitgleich einen professionelleren Umgang mit potenziellen Wissensrisiken einfordert (Wissenschaftsrat 2025). Die vorliegende Untersuchung zeigt, dass sicherheitsrelevante FuE weit über die klassische Verteidigungsforschung hinausgehen sollte, ohne die militärische Verteidigungsfähigkeit dabei zu vernachlässigen.

1.3 Von Dual Use zu Bedarfsübersetzung: Warum der Nutzungskontext entscheidet

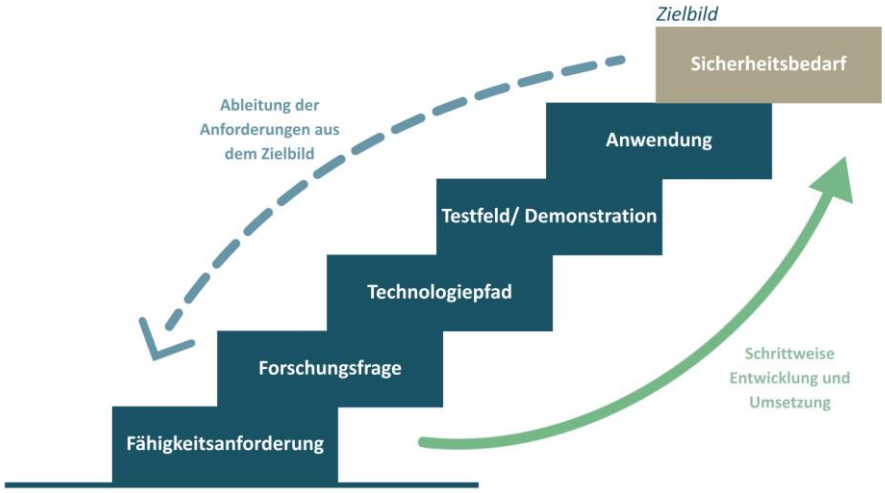
Die Erweiterung des Sicherheitsbegriffs spiegelt den technologischen Wandel wider. Schlüsseltechnologien wie KI oder Sensorik sind heute inhärent dual-use-fähig. Nicht die Technologie an sich, sondern erst ihr konkreter Nutzungskontext entscheidet darüber, ob sie zivil, behördlich oder militärisch eingesetzt wird.

Wer Forschung, Förderung und Transfer strikt entlang der alten Trennung zwischen zivil und militärisch organisiert, begrenzt in vielen Feldern die Möglichkeit, sicherheitsrelevante Bedarfe, technologische Entwicklungen und zivile Anschlussfähigkeit sinnvoll zusammenzuführen und schafft dadurch häufig doppelte Forschungsaufwände. Das behindert den Austausch, verhindert gemeinsame Lernprozesse und verzögert den Weg in die Praxis. Es geht also um einen rechtlich, ethisch und demokratisch abgesicherten Wissenstransfer zwischen den Sektoren. Wissenschaftsfreiheit, Ergebnisoffenheit und die Unabhängigkeit der Grundlagenforschung bleiben dabei strikt gewahrt. Ebenso setzt ein solcher Ansatz klare Grenzen, sobald Anwendungen rechtlich, ethisch oder politisch nicht gewollt sind.

Die für die Analyse geführten Interviews mit Expertinnen und Experten entlang der gesamten Wertschöpfungskette machen deutlich, dass die zentrale Herausforderung darin besteht, Sicherheits- und Verteidigungsbedarfe systematisch in Forschungs- und Innovationsanforderungen zu übersetzen. Bislang stehen häufig entweder abstrakte Sicherheitsziele oder konkrete technologische Einzelvorhaben im Vordergrund. Dazwischen fehlt ein strukturierter Prozess, der Bedrohungs- und Risikolagen, Fähigkeitsanforderungen, Forschungsfragen, Technologiepfade, Testfelder, Finanzierung und spätere Anwendung einbezieht.

Eine innovationsorientierte Sicherheitsstrategie beginnt nicht bei der Frage, welche einzelne Technologie gefördert werden soll, sondern bei den Problemen, die gelöst werden müssen. Für Verteidigungsforschung ist dieser Punkt besonders relevant. Abbildung 1 zeigt, wie militärische Fähigkeitsbedarfe früher und klarer in Forschungs- und Innovationsfragen übersetzt werden können, ohne den Lösungsweg vorschnell technologisch zu verengen. Ein solches Vorgehen schafft laut der vorliegenden Analyse mehr Raum für neue Technologien, Start-ups, wissenschaftliche Ansätze und disruptive Innovationen. Gleichzeitig gilt diese Logik ebenso für zivile Sicherheitsverantwortliche, Länder, Kommunen, Betreiber kritischer Infrastrukturen oder Industrieunternehmen. Die Aufgabe besteht darin, diese unterschiedlichen Bedarfe sichtbar, vergleichbar und anschlussfähig zu machen.

Abbildung 1: Bedarfsorientierter Innovationsprozess in der Verteidigungsinnovation



Quelle: Eigene Darstellung.

2. DEUTSCHLANDS AUSGANGSLAGE: VIEL POTENZIAL, WENIG VERBINDUNG

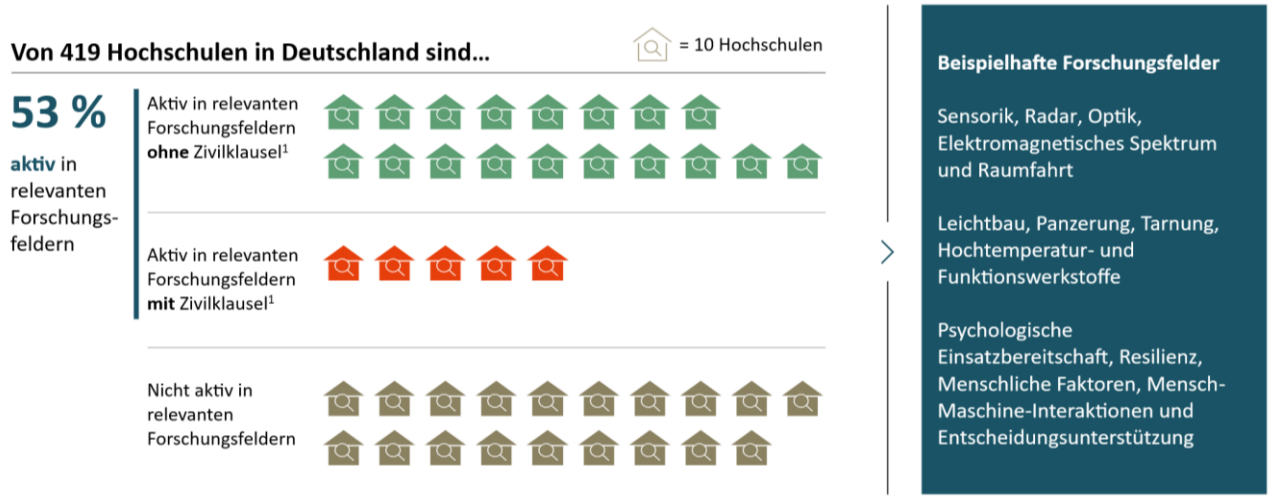
2.1 Breite Basis: Hochschulen, Industrie und Start-ups als Ausgangspunkt

Die vorliegende Analyse bestätigt: Deutschland verfügt über eine breite Ausgangsbasis für sicherheitsrelevante Forschung und Innovation: leistungsfähige Hochschulen, außeruniversitäre Forschung, industrielle Kompetenzen, innovative Unternehmen und ein wachsendes Start-up-Ökosystem. Das Problem liegt daher nicht im Fehlen einzelner Kompetenzen, sondern in ihrer systematischen Verbindung mit Sicherheits- und Verteidigungsbedarfen, Transferstrukturen, Testfeldern, Finanzierung und späterer Anwendung.

Besonders relevant ist dabei Deutschlands starke zivile Forschungs- und Entwicklungsbasis. Viele sicherheitsrelevante Schlüsseltechnologien entstehen heute nicht ausschließlich in militärischen Kontexten, sondern in zivilen Innovationsfeldern. Dazu zählen etwa künstliche Intelligenz, Sensorik, Raumfahrt, Robotik, Cybertechnologien, neue Materialien, Energie- und Antriebstechnologien oder resiliente Kommunikationssysteme. Werden hier Wege zur Mehrfachnutzung gleich zu Beginn berücksichtigt, kann diese zivile FuE-Basis zu einem Aktivierungspotenzial für sicherheitsrelevante Innovationen werden.

Auch die Hochschullandschaft bietet hierfür eine relevante Grundlage. Eine Analyse der 419 Hochschulen in Deutschland hinsichtlich ihrer Lehr- und Forschungsaktivität in sicherheitsrelevanten Feldern zeigt, dass mehr als die Hälfte der Hochschulen in Forschungsfeldern aktiv ist, die für Dual-Use- und sicherheitsrelevante Anwendungen nutzbar sind. Damit besteht ein wissenschaftliches Potenzial, das stärker für Sicherheits-, Resilienz- und Verteidigungsfragen aktiviert werden kann.

Abbildung 2: In sicherheitsrelevanten Forschungsfeldern aktive Hochschule



[1] Eine Zivilklausel ist eine Selbstverpflichtung von Hochschulen und Forschungseinrichtung, ihre Forschung und Lehre ausschließlich für friedliche und zivile Zwecke zu betreiben
Quelle: Eigene Darstellung. Analyse basierend auf Daten von: Centrum für Hochschulentwicklung (CHE), TU9-Allianz, Initiative Hochschulen für den Frieden.

Auch im Start-up-Ökosystem gewinnt das Feld sicherheits- und verteidigungsrelevanter Technologien an Dynamik. Das Interesse von Kapitalgebern an Defense Tech hat in den vergangenen Jahren deutlich zugenommen. Eine Analyse der Daten von PitchBook Data, Inc. zeigt, das Gesamtvolumen entsprechender Start-up-Deals in Europa stieg von rund 511 Millionen US-Dollar im Zeitraum 2018 bis 2021 auf mehr als 5 Milliarden US-Dollar im Zeitraum 2022 bis 2025 – eine Verzehnfachung innerhalb weniger Jahre. Diese Dynamik verdeutlicht, dass sicherheitsrelevante Technologien zunehmend als eigenständiges Innovations- und Wachstumsfeld wahrgenommen werden.

Zugleich ist das Ökosystem in Deutschland regional verteilt und technologisch heterogen. Diese Verteilung ist ambivalent: Sie zeigt Potenzial an vielen Standorten, erschwert aber strategische Bündelung, schnelle Vernetzung und klare Transferpfade. Für die Analyse ist dabei wichtig, das Start-up-Ökosystem nicht nur als engen Defense-Tech-Sektor zu verstehen. Neben Start-ups mit klarem Verteidigungsfokus existiert ein breiteres Feld angrenzender Dual-Use- und Sicherheitstechnologien. Dazu gehören etwa Cybersecurity, Sensorik, KI, Robotik, Raumfahrt, Energie, Materialien, resiliente Infrastrukturen und industrielle Sicherheit.

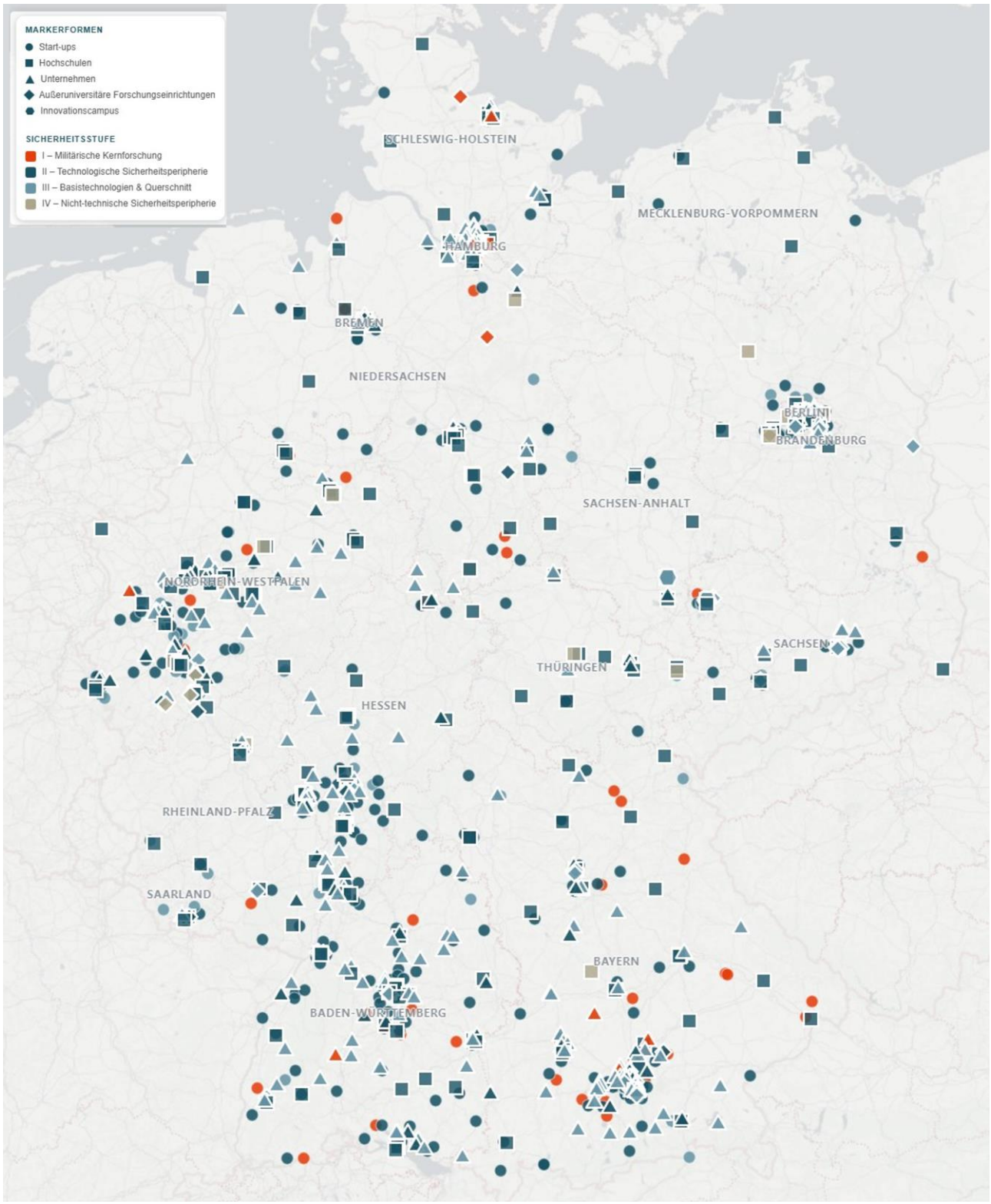
Diese Unterscheidung ist für Deutschland besonders relevant. Start-ups mit engem Verteidigungsfokus konzentrieren sich stärker in einzelnen Clustern. Das breitere Feld angrenzender Dual-Use- und Sicherheitstechnologien ist dagegen stärker über Hochschul-, Industrie- und Technologieregionen verteilt. Dadurch entsteht ein dezentrales Innovationspotenzial, das wissenschaftliche Exzellenz, industrielle Anwendungsnähe und unternehmerische Dynamik verbinden kann.

Die zentrale Diagnose lautet daher: Deutschland verfügt über relevante Voraussetzungen für sicherheitsrelevante Forschung und Innovation, aber noch nicht über ein ausreichend verbundenes Innovationssystem.

2.2 Fragmentierung: viel Aktivität, zu wenig Verbindung

Die fragmentierte Landschaft von Sicherheitsforschung und -innovation ist Ausgangspunkt der weiteren Analyse. In Deutschland gibt es zahlreiche Aktivitäten an Hochschulen und außeruniversitären Forschungseinrichtungen, bei Unternehmen, Start-ups, Behörden, bundeswehrnahen Strukturen sowie auf Ebene von Ländern und Regionen. Wie untenstehende Grafik zeigt, gibt es eine wachsende Zahl regionaler Zentren für Verteidigung, Dual Use und Sicherheit. Das Thema gewinnt in den Bundesländern an Bedeutung. Diese Entwicklung ist ein wichtiges Signal.

Abbildung 3: Sicherheitsrelevante Forschung und Innovation in Deutschland



Quelle: Eigene Darstellung. Die Karte zeigt die dezentrale Verteilung sicherheitsrelevanter Forschungs-, Innovations- und Anwendungspotenziale in Deutschland. Sie macht sichtbar, dass zahlreiche Aktivitäten bestehen, diese aber bislang nur begrenzt zu einem strategisch verbundenen Ökosystem verdichtet sind.

Die Karte verdeutlicht die zentrale Ambivalenz des deutschen Systems: Sicherheitsrelevante Potenziale verteilen sich räumlich, institutionell und technologisch über ein breites Spektrum. Diese Dezentralität ist keineswegs Nachteil; sie kann auch Ausdruck eines vielfältigen Wissenschafts-, Industrie- und Innovationssystems sein. Zum Problem wird sie jedoch, wenn Bedarfe, Forschung, Förderung, Testfelder, Beschaffung, Finanzierung und Skalierung nicht ineinandergreifen, weil Vernetzung, Sichtbarkeit oder kritische Masse

fehlen. Dann entstehen Brüche entlang der Innovationskette. Entscheidend ist daher, dezentrale Stärken über regionale Profile, klare Schnittstellen und nationale Leitplanken mit konkreten Sicherheits- und Resilienzbedarfen zu verbinden.

3. VIER ENGPÄSSE AUF DEM WEG VON FORSCHUNG ZU WIRKUNG

Kapitel 2 zeigt, dass Deutschland zwar über viele sicherheitsrelevante Potenziale verfügt, diese jedoch räumlich, institutionell und technologisch breit verteilt sind. Da diese Dezentralität an sich keinen Nachteil darstellt, analysiert Kapitel 3 nun vier zentrale Hemmnisse, die verhindern können, dass aus dieser Vielfalt eine durchgängige Innovationskette erwächst. Diese Barrieren leiten sich aus Erkenntnissen zu leistungsfähigen Innovationssystemen in anderen Sektoren sowie Interviews mit Expertinnen und Experten (siehe Infobox) ab. Aus den Fachgesprächen kristallisieren sich vier erfolgskritische Dimensionen für ein Innovationsökosystem mit Schlagkraft heraus: Zielsetzung und Rahmenbedingungen, Finanzierung, Kooperation und Vernetzung sowie Talente und Kultur.

(A) **Zielsetzung und Rahmenbedingungen** bestimmen die strategische Richtung, etwa durch klare Innovations- und Sicherheitsstrategien, definierte Fähigkeitsprofile und eine entsprechend ausgerichtete Beschaffung.
(B) **Finanzierung** entscheidet über Schlagkraft und Risikologik, insbesondere durch ausreichende Mittel in allen Phasen – von der Grundlagenforschung bis zur Skalierung von Start-ups.
(C) **Kooperation und Vernetzung** prägen die Umsetzungsgeschwindigkeit, etwa durch systematische Zusammenarbeit von Staat, Wissenschaft und Wirtschaft.
(D) **Talente und Kultur** sichern die nachhaltige Innovationsfähigkeit, beispielsweise durch funktionierenden Talenttransfer und Offenheit gegenüber sicherheitsrelevanten Technologien.

Stimmen aus den Interviews: drei wiederkehrende Muster
Die Interviews mit Akteuren aus Wissenschaft, Wirtschaft, Start-ups und sicherheitsnahen Institutionen verdeutlichen die in Kapitel 3 beschriebenen Engpässe. Drei Muster treten besonders hervor:

- **Missionsprofile klarer kommunizieren:** Mehrere Interviewte wünschen sich eine klarere staatliche Kommunikation zu sicherheits- und verteidigungsrelevanten Bedarfen. Die Bedarfslagen seien häufig bekannt, würden aber noch nicht ausreichend in Missionsprofile, Forschungsfragen und Innovationsprioritäten übersetzt.
- **Strategischer planen, nicht nur kurzfristig optimieren:** Die Interviewten kritisieren, dass Innovations- und Beschaffungslogiken zu häufig auf kurzfristige Anforderungen oder die Optimierung einzelner Aufgaben ausgerichtet seien. Für sicherheitsrelevante Innovation brauche es stärker voraus-schauende Planung und einen klareren Fokus auf Umsetzung.
- **Strategischer planen, nicht nur kurzfristig optimieren:** Die Interviewten kritisieren, dass Innovations- und Beschaffungslogiken zu häufig auf kurzfristige Anforderungen oder die Optimierung einzelner Aufgaben ausgerichtet seien. Für sicherheitsrelevante Innovation brauche es stärker voraus-schauende Planung und einen klareren Fokus auf Umsetzung

Die Praxisbeobachtungen aus den Interviews verweisen auf eine breitere Frage von Handlungssicherheit und verdeutlichen, dass eine engere Zusammenarbeit neuer, grundlegender Spielregeln bedarf. Das Spannungsfeld zwischen wissenschaftlicher Freiheit, sicherheitsrelevanter Forschung und notwendiger Geheimhaltung muss dafür aktiv bewältigt werden. Wissenschaft braucht Offenheit, Veröffentlichungen und Nachvollziehbarkeit; Verteidigungsakteure benötigen Vertraulichkeit, Zugriffskontrolle und Verschwiegenheitsvereinbarungen. Kooperation gelingt daher über abgestufte Modelle: offene Forschung, geschützte

Testumgebungen, kontrollierter Datenaustausch und klare Regeln für Veröffentlichungen, geistiges Eigentum, Exportkontrolle und Sicherheitsprüfung.

Die identifizierten Engpässe in den vier Dimensionen wirken nicht isoliert, sondern verstärken sich gegenseitig. Ohne klare Zielbilder bleibt Finanzierung unscharf; ohne anschlussfähige Finanzierung bleiben Prototypen stecken; ohne Kooperation entstehen keine Transferpfade; ohne gemeinsame Sprache und Handlungssicherheit werden vorhandene Talente nicht ausreichend mobilisiert. Zusammengenommen bilden diese Faktoren ein Innovationsökosystem, dessen vier zentrale Wirkungsdimensionen und ihre gegenseitige Abhängigkeit in der untenstehenden Abbildung visualisiert werden.

Abbildung 4: Vier Dimensionen eines Innovationsökosystems für Deutschland

Quelle: Stifterverband, eigene Darstellung.

3.1 Zielsetzung und Rahmenbedingungen

Der erste identifizierte Engpass liegt in der Übersetzung von Bedarfen in Prioritäten. Heute entstehen sicherheits- und verteidigungsrelevante Bedarfe an unterschiedlichen Stellen: in Ressorts, bei Sicherheitsbehörden und Bundeswehr, in Förderprogrammen, in Länderinitiativen, in Forschungseinrichtungen und bei Unternehmen. Die Experteninterviews zeigen, dass diese Perspektiven jedoch noch nicht systematisch genug zusammengeführt werden. Der bislang fehlende Abgleich zwischen Bedarfen, Fähigkeiten und Innovationsplänen unterstreicht deshalb die Notwendigkeit eines stärker strukturierten Austauschs zwischen Wissenschaft, Sicherheitsverantwortlichen und Politik. Hier setzt der Vorschlag des Wissenschaftsrats (Wissenschaftsrat 2025) an, ein Strategisches Dialogforum für Vertreterinnen und Vertreter aus Wissenschaft und Sicherheitspolitik einzurichten. In einem solchen Forum könnten multidisziplinäre Risikoanalysen erarbeitet und sicherheitspolitische Szenarien entworfen werden sowie darauf aufbauend sicherheitsrelevante Forschungsbedarfe systematisch identifiziert, abgeleitet und so beschrieben werden, dass Erprobung und Anwendung direkt daran anknüpfen können.

Deutschland verfügt über relevante Forschungsaktivitäten, industrielle Kompetenzen und sicherheitsbezogene Bedarfe. Diese werden jedoch noch nicht systematisch genug zusammengeführt. Häufig fehlt ein Prozess, der klärt, welche Fähigkeiten benötigt werden, welche Forschungsfragen sich daraus ergeben und über welche Test- und Anwendungspfade Ergebnisse in die Praxis gelangen.

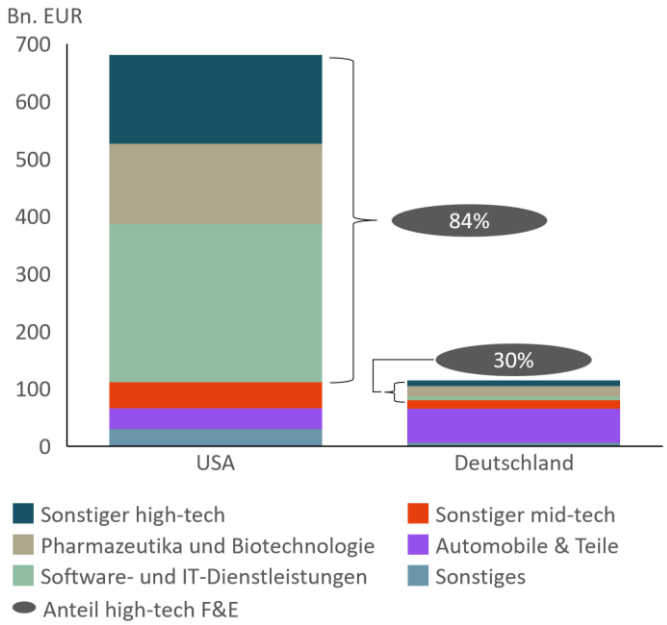
Gerade für sicherheits- und verteidigungsrelevante Innovationen ist diese Übersetzungsleistung entscheidend. Wenn Bedarfe zu abstrakt bleiben, fehlt Orientierung für Wissenschaft, Unternehmen und Start-ups. Werden sie dagegen zu früh als konkrete Produkt- oder Komponentenanforderungen formuliert, verengt sich der Lösungsraum. Innovationsfreundliche Zielsetzung beschreibt daher Problem und Zielbild klar, hält den technologischen Lösungsweg aber offen.

Diese fehlende gemeinsame Ausrichtung trifft auf eine Innovationslandschaft, die stärker durch bestehende industrielle Stärken geprägt ist als durch eine breite Ausrichtung auf Spitzentechnologie, wie

Abbildung 4 zeigt. Der vergleichsweise geringe Anteil unternehmerischer Forschungsausgaben in diesen Hochtechnologiebereichen erklärt die sicherheitsrelevante Innovationslücke in der folgenden Abbildung zwar nicht allein, deutet aber auf ein Umfeld hin, in dem sich neue, technologieübergreifende Entwicklungen schwerer verbreiten und vergrößern lassen. Die Folge ist ein System, das vorhandene Stärken eher nebeneinander bestehen lässt, statt sie gezielt zu bündeln. Umso wichtiger ist daher ein strategischer Rahmen, der Anforderungen in Forschungsfragen, Kooperationsformate und konkrete Anwendungswege übersetzt.

Abbildung 5: Deutschland in der *Mid-Tech-Falle*

Business-FuE-Ausgaben (Business enterprise R&D expenditure (BERD)) nach Tech-Level (Top 2.000 Unternehmen), 2024



Quellen: BMFTR, European Commission, EU Industrial R&D Scoreboard 2025, ifo (2024), IMF World Economic Outlook , OECD, OECD, Sachverständigenrat (2025). Die Abbildung ordnet die deutsche Innovationslandschaft im Vergleich zu stärker hightechorientierten Innovationssystemen ein. Für die vorliegende Analyse dient sie als Hintergrund: Sicherheitsrelevante Forschung und Innovation benötigen strategische Orientierung gerade dort, wo neue technologische Entwicklungen und Dual-Use-Anwendungen nicht automatisch aus bestehenden industriellen Prozessen entstehen.

3.2 Finanzierung

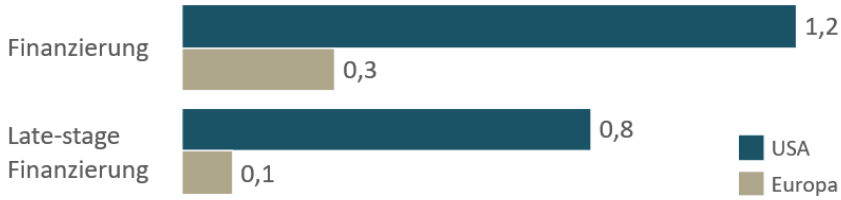
Der zweite identifizierte Engpass betrifft die Finanzierung. Sicherheitsrelevante Forschung und Innovation benötigen eine Finanzierungskette, die von Grundlagenforschung über Prototypen und Demonstration bis zu Erprobung, Beschaffung und industrieller Skalierung reicht. In Deutschland bestehen gerade an diesen Übergängen Lücken. Viele technologische Ansätze entstehen in Forschungsprojekten, erreichen aber nicht die Entwicklungsreife, die für Einsatz, Markteintritt oder Skalierung notwendig wäre.

Staatlich finanzierte verteidigungsbezogene FuE ist in Deutschland vergleichsweise gering unterlegt. Der Anteil, der im Einzelplan 14 des Bundeshaushaltes dafür ausgewiesen ist, liegt bei rund 0,08 Prozent des BIP, gegenüber 0,36 Prozent in den USA. Im Bundeshaushalt 2025 sind im Einzelplan 14 rund 1,2 Milliarden Euro für Forschung, Entwicklung und Erprobung vorgesehen; das entspricht etwa 2 Prozent des Verteidigungshaushalts. Die Zahlen zeigen die begrenzte finanzielle Basis, erklären die Skalierungslücke aber nicht allein.

Hinzu kommt eine private Skalierungslücke. Gerade Deep-Tech- und Defense-Tech-Innovationen sind kapitalintensiv, risikoreich und oft durch lange Entwicklungszeiten geprägt. Ob aus Prototypen einsatzfähige oder marktfähige Lösungen werden, hängt daher auch von privater Anschlussfinanzierung ab. Die Abbildung zur Finanzierung von Deep-Tech-Start-ups zeigt auf Basis von Daten von Pitchbook, dass die

Kapitalverfügbarkeit in den USA deutlich höher ist als in Europa. Das gilt besonders in späteren Finanzierungsphasen, in denen technologische Ansätze zur Marktreife oder Einsatzfähigkeit gebracht werden müssen.

Abbildung 6: Finanzierung von Deep-Tech-Start-ups
in Prozent des BIP, pro Region



Quellen: Dealroom, ifo, McKinsey, McKinsey, McKinsey. Die Abbildung zeigt die Finanzierungslücke zwischen Europa und den USA im Deep-Tech-Bereich. Für sicherheitsrelevante Innovationen ist diese Lücke besonders relevant, weil viele Technologien lange Entwicklungszeiten, hohe Anfangsinvestitionen und unsichere Anwendungsmärkte aufweisen.

Die Analysen auf Basis der Pitchbook-Daten zeigen, das Kapital in diesem Bereich stammt derzeit vor allem aus drei Quellen: spezialisierte Investoren für Verteidigung und komplexe Technologien, größere europäische und transatlantische Wagniskapitalfonds sowie strategische Industrieakteure. Diese Entwicklung wird angetrieben durch steigende Verteidigungsetats, die sicherheitspolitische Neubewertung von Dual-Use-Technologien und neue europäische sowie NATO-bezogene Finanzierungs- und Validierungsinitiativen. Für Deutschland bleibt entscheidend, ob dieser Kapitalfluss auch in späteren Finanzierungsrunden, beim Aufbau der Produktion und bei der staatlichen Beschaffung ankommt.

Damit bleibt die kritische Übergangsphase zwischen Forschung, Demonstration und Skalierung ein zentraler Engpass. Ökonomischer Mehrwert entsteht erst dann, wenn Forschungsergebnisse erfolgreich in die Anwendung überführt, weiterfinanziert und industriell skaliert werden. Finanzierung ist deshalb nicht nur eine Frage der Mittelhöhe, sondern der Anschlussfähigkeit zwischen öffentlicher Förderung, privatem Kapital und späterer Beschaffung. Genau hier entscheidet sich, ob sicherheitsrelevante FuE zum Multiplikator wird oder in der Lücke zwischen Prototyp, Erprobung und Skalierung stecken bleibt.

Auch bei der privaten Wachstumsfinanzierung zeigt sich ein struktureller Abstand zu den USA. Diese verfügen über eine deutlich höhere Kapitaltiefe, insbesondere in den kapitalintensiven Deep-Tech- und Defense-Tech-Feldern. Entsprechend konzentriert sich auch ein großer Teil des NATO-weiten Risikokapitals für Verteidigungstechnologien in den USA, während der europäische Anteil deutlich geringer ausfällt. Diese Vergleiche unterstreichen, dass der deutsche Engpass nicht nur bei der öffentlichen Förderung liegt, sondern auch bei der privaten Anschlussfinanzierung für Wachstum, Industrialisierung und Marktzugang.

3.3 Kooperation und Vernetzung

Der dritte identifizierte Engpass betrifft Kooperation und Vernetzung. Deutschland verfügt über eine Vielzahl relevanter Akteure: Hochschulen, außeruniversitäre Forschung, Start-ups, Mittelstand und Großindustrie, ebenso wie Sicherheitsverantwortliche, Länder, Kommunen und Kapitalgeber. Die Experteninterviews unterstreichen, dass das eigentliche Problem kein Mangel an Akteuren, sondern deren fehlende Verknüpfung untereinander ist.

Die fehlenden Schnittstellen werden besonders an den Übergängen zwischen Technology Readiness Levels (TRL) sichtbar. Deutschland ist in frühen Forschungs- und Entwicklungsphasen gut aufgestellt. Schwieriger ist der Übergang in höhere Reifestufen, insbesondere in Demonstration, realitätsnahe Erprobung, Systemintegration, Zertifizierung, Beschaffungsfähigkeit und Skalierung.

Technology Readiness Levels und Transferlücken

Der Technology Readiness Level (TRL) ist ein international gebräuchliches Modell zur Bewertung des technologischen Reifegrads einer Innovation. Entwickelt wurde es ursprünglich von der NASA.

Technology Readiness Levels beschreiben den technologischen Reifegrad einer Innovation von grundlegender Forschung bis zum operativen Einsatz. Für sicherheitsrelevante Forschung ist vor allem der Übergang von TRL 6 bis 8 kritisch: Prototypen müssen unter realitätsnahen Bedingungen demonstriert, in Systeme integriert und für Anwendung, Beschaffung oder Skalierung qualifiziert werden. Genau hier entstehen in Deutschland häufig Transferlücken.

Die Skala umfasst neun Stufen:

- TRL 1: Beobachtung grundlegender Prinzipien
- TRL 2: Formulierung eines Technologiekonzepts
- TRL 3: Experimenteller Nachweis der Machbarkeit (Proof of Concept)
- TRL 4: Validierung im Laborumfeld
- TRL 5: Validierung in relevanter, anwendungsnaher Umgebung
- TRL 6: Demonstration eines Prototyps unter realistischen Bedingungen
- TRL 7: Systemprototyp im Einsatzumfeld
- TRL 8: Abgeschlossenes, qualifiziertes System
- TRL 9: Einsatzfähiges, bewährtes System im operativen Betrieb

Typische Erfolgsfaktoren entlang der TRL-Stufen sind:

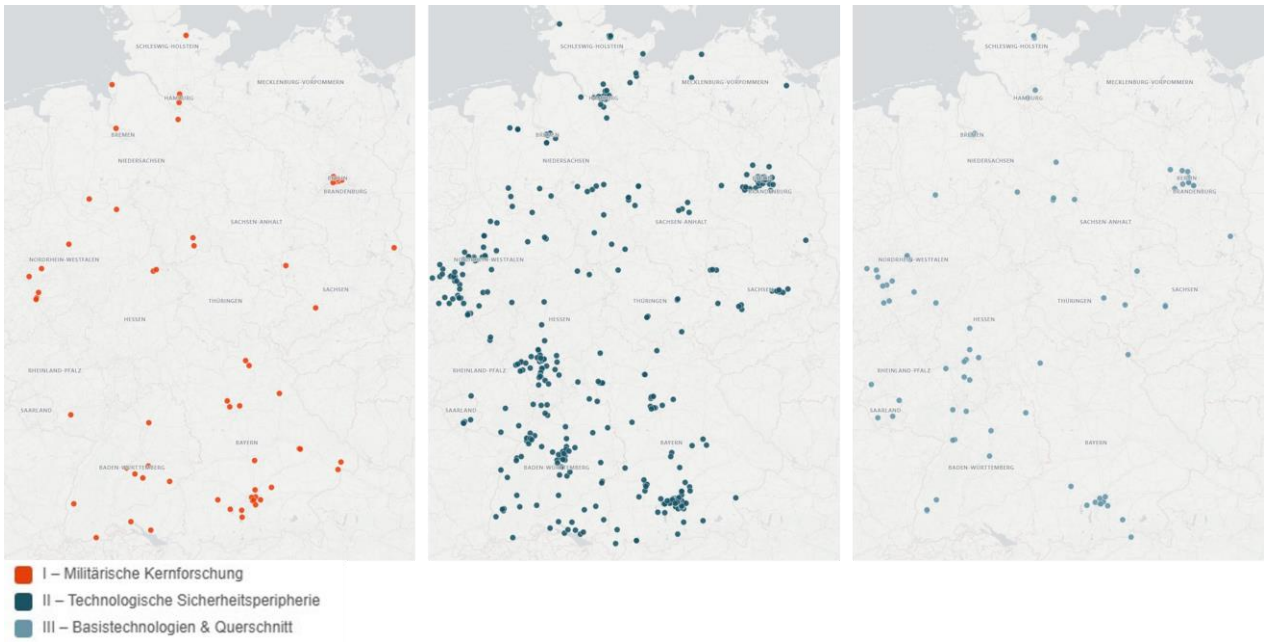
- TRL 1-3 (Forschung): Wissenschaftliche Exzellenz, interdisziplinäre Kompetenz, Zugang zu Laborinfrastruktur, ausreichende Frühphasenfinanzierung.
- TRL 4-6 (Demonstration): Technische Integrationsfähigkeit, Systemengineering-Kompetenz, realitätsnahe Testumgebungen, enge Kooperation zwischen Forschung und Industrie.
- TRL 7-9 (Einführung und Skalierung): Industrielle Produktionsfähigkeit, Qualitätssicherung, Zertifizierungs- und Zulassungsprozesse, Marktzugang beziehungsweise Beschaffungsintegration.

Höhere TRL-Stufen erfordern mehr als wissenschaftliche Exzellenz. Sie brauchen Testumgebungen, Anwenderfeedback, Systemengineering, regulatorische Klärung, industrielle Kapazitäten, Finanzierung und Beschaffungsnähe. Diese Voraussetzungen entstehen nur durch frühe und dauerhafte Zusammenarbeit zwischen Wissenschaft, Wirtschaft, Staat, Sicherheitsverantwortlichen und Kapitalgebern. Ohne solche Schnittstellen bleiben Technologien in Laboren, Pilotprojekten oder Einzelinitiativen stecken.

Die Transferlücke zeigt sich auch in quantitativen Indikatoren zur zivilen Nachnutzung von Dual-Use-Technologien. Laut einer JRC-Studie der Europäischen Kommission liegt der Anteil von Patenten mit potenziellem zivilem Nutzen an allen Defense-Patenten in Deutschland deutlich unter dem US-Wert; auch die inländische zivile Weiterverwendung solcher Technologien fällt geringer aus. Dual-Use-Patente machen laut der Studie hierzulande lediglich 24,1 Prozent aller Defense-Patente aus – in den USA sind es 63,9 Prozent. Ein ähnliches Bild zeigt sich bei der über Patentzitationen gemessenen inländischen zivilen Weiterverwendung: Hier stehen 36 Prozent in Deutschland 76 Prozent in den USA gegenüber. Diese Befunde deuten darauf hin, dass sicherheits- und verteidigungsnahe Technologien in Deutschland seltener in zivile Folgeinnovationen, industrielle Prozesse und neue Märkte diffundieren.

Die Grafik zur räumlichen Verteilung sicherheitsnaher Start-ups in Deutschland (siehe Abbildung 7) zeigt insbesondere in der technologischen Sicherheitsperipherie keine klare Spezialisierung. Während sich Start-ups mit eindeutigem Defense-Fokus stärker auf einzelne Cluster konzentrieren, sind angrenzende sicherheitsrelevante und Dual-Use-fähige Felder breiter verteilt. Für die Innovationslogik ist daher entscheidend, ob diese Innovatoren Zugang zu Anwendern, Testfeldern, Kapital und industrieller Skalierung finden.

Abbildung 7: Start-ups im deutschen Raum nach Sicherheitsnähe



Quelle: Stifterverband, eigene Darstellung. Die Abbildung zeigt, dass sich Start-ups je nach Sicherheitsnähe unterschiedlich über den deutschen Raum verteilen. Diese Verteilung bildet einen wichtigen Ausgangspunkt für die regionale Standortlogik der Fallanalysen in Kapitel 4.

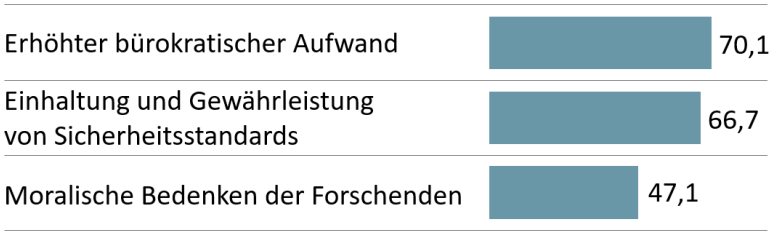
Kooperation und Vernetzung sind damit keine ergänzenden Faktoren, sondern Voraussetzung für Umsetzungsgeschwindigkeit, Skalierungsfähigkeit und Spillover-Potenzial. Je besser Bedarfe, Forschung, Anwendung und Finanzierung verbunden sind, desto höher ist die Wahrscheinlichkeit, dass sicherheitsrelevante Innovationen auch zivile Wirkung entfalten.

3.4 Talente und Kultur

Der vierte identifizierte Engpass bezieht sich auf Talente und Kultur. Wie aus Fachgesprächen hervorgeht, verfügt Deutschland über starke Forschungsressourcen, qualifizierte Fachkräfte und relevante technologische Kompetenzen, deren sicherheitspolitisches und wirtschaftliches Potenzial jedoch noch nicht ausreichend ausgeschöpft wird. Der Engpass lässt sich nicht allein auf individuelle Einstellungen zurückführen, sondern resultiert, wie Abbildung 7 zeigt, aus fehlender Handlungssicherheit, administrativen Hürden, hohen Sicherheitsanforderungen und kulturellen Unsicherheiten im Umgang mit sicherheits- und verteidigungsbezogener Forschung.

Gerade Letztere wiegen laut der Interviewten schwer, denn sicherheitsrelevante Forschung ist in Deutschland historisch besonders sensibel. Ethische und moralische Bedenken, bürokratische Anforderungen, Sicherheitsstandards und Zivilklauseln beeinflussen die Bereitschaft von Forschenden und Einrichtungen maßgeblich, sich in diesem Feld zu engagieren. Dass genau diese Faktoren als zentrale Herausforderungen wahrgenommen werden, belegen auch aktuelle Befunde aus dem Hochschul-Barometer (siehe Abbildung°8). Solche Bedenken sollten dabei jedoch nicht als bloße Hemmnisse verstanden werden, sondern als Ausdruck legitimer Verantwortung in Wissenschaft und Forschung. Ein tragfähiger Umgang damit setzt daher nicht auf ihre Relativierung, sondern auf klare Verfahren: transparente Governance, ethische Reflexion, verlässliche rechtliche Rahmenbedingungen, den Schutz der Wissenschaftsfreiheit und Formate, in denen Chancen, Risiken und Grenzen sicherheitsrelevanter Forschung nachvollziehbar abgewogen werden können.

Abbildung 8: Zentrale Herausforderungen bei sicherheitsrelevanter Forschung
Angaben der Hochschulleitungen; in Prozent



Quelle: Hochschul-Barometer 2025. Die Abbildung zeigt zentrale Hürden, die Hochschulen und Forschungseinrichtungen bei sicherheitsrelevanter Forschung wahrnehmen. Sie verweist darauf, dass kulturelle und institutionelle Barrieren nicht nur Einstellungsfragen sind, sondern auch administrative und regulatorische Dimensionen haben.

Diese Befunde des Hochschul-Barometers verdeutlichen, dass die Debatte um Talente und Kultur nicht auf individuelle Einstellungen verengt werden sollte. Entscheidend sind ebenso verlässliche institutionelle Rahmenbedingungen, Forschungssicherheit und Handlungssicherheit. Zivilklauseln wirken in diesem Zusammenhang nicht als Hauptbarriere, sind aber sichtbarer Bestandteil einer breiteren Unsicherheit im Umgang mit sicherheits- und verteidigungsbezogener Forschung.

Aus den vier Engpässen wird deutlich: Der zentrale Hebel liegt nicht in einzelnen zusätzlichen Maßnahmen, sondern im strategischen Zusammenspiel von Zielsetzung, Finanzierung, Kooperation und Kultur. Erst wenn diese Dimensionen ineinandergreifen, können aus Forschung konkrete Anwendungen, aus Prototypen skalierbare Lösungen und aus sicherheitsrelevanten Technologien breitere Spillover-Effekte entstehen.

4. REGIONALE PROFILE ENTWICKELN UND HEMMNISSE ABBAUEN

Regionale Standortprofile können helfen, die in Kapitel 3 beschriebenen Engpässe praktisch zu überwinden. Experten betonen in Gespräche mehrfach, dass sicherheitsrelevante Forschung und Innovation dort besonders wirksam werden, wo konkrete Bedarfe, wissenschaftliche Kompetenzen, industrielle Fähigkeiten, Anwender und Testfelder zusammenkommen. Die dezentrale Struktur des deutschen Innovationssystems muss deshalb nicht als Defizit verstanden werden. Sie kann vielmehr der Ausgangspunkt für eine produktive Spezialisierung sein, wenn regionale Profile mit nationalen Prioritäten, Testfeldern, Finanzierung und Wegen in die breite Anwendung verbunden werden.

Sicherheitsrelevante Forschung als Standortstrategie zu verstehen bedeutet, regionale Profile aus vorhandenen Stärken und konkreten Bedarfen abzuleiten. Entscheidend ist nicht, neue Ökosysteme künstlich aufzubauen oder überall dieselben Strukturen zu fördern. Ausgangspunkt können vorhandene Stärken sein: Hochschulen und Forschungseinrichtungen, industrielle Kompetenzen, kritische Infrastrukturen, Start-up-Aktivitäten und reale Anwendungskontexte. Werden diese Stärken sichtbar profiliert und gezielt verbunden, können Regionen ihre eigene Standortdynamik erzeugen und zusätzliche Talente, Start-ups, Kapital und Anwendungspartner anziehen.

Zwei Beispiele illustrieren diese Logik: Hamburg und die maritime Küstenregion stehen für einen länderübergreifenden maritimen Innovationsraum, in dem Hafen, Logistik, maritime Wirtschaft, Energieinfrastruktur, Digitalisierung und Sicherheit zusammenlaufen. Nordrhein-Westfalen steht dagegen weniger für ein enges Defense-Tech-Cluster als für einen industriellen Skalierungsraum, in dem Forschung, Start-ups und digitale Technologien auf starke industrielle Anwender, Energie- und Infrastrukturakteure sowie Mittelstand und Großunternehmen treffen.

Die regionalen Profile wurden methodisch aus drei Perspektiven abgeleitet: erstens aus der eigenen Analyse der räumlichen Verteilung sicherheitsnaher Start-ups und sicherheitsrelevanter Technologiefelder, zweitens aus der kartierten Hochschul-, Forschungs- und Industriekompetenz sowie den qualitativen

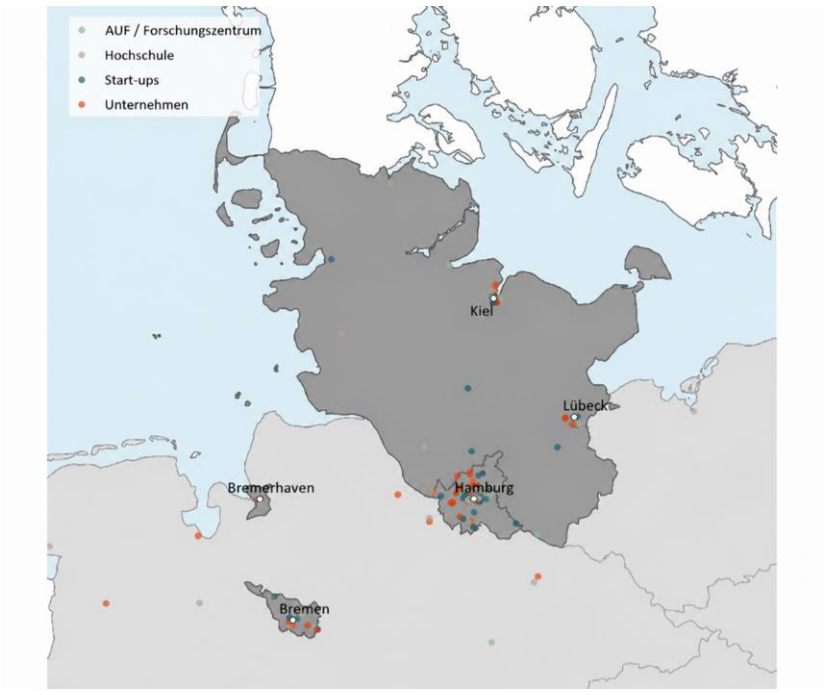
Hinweisen aus den für die Analyse durchgeführten Interviews und drittens aus der Spiegelung mit bestehenden regionalen und nationalen Innovationsstrategien. Die Beispiele sind daher nicht als vollständige Bestandsaufnahme aller Akteure zu lesen, sondern als verdichtete Standortlogiken. Sie zeigen, wie vorhandene Stärken, reale Anwendungskontexte und strategische Innovationsfelder in sicherheitsrelevante Innovationspfade übersetzt werden können.

4.1 Hamburg und die maritime Küstenregion: Synergien durch überlappende Ökosysteme

Hamburg und die maritime Küstenregion repräsentieren ein Profil, in dem zivile Infrastruktur, maritime Sicherheit und Verteidigungsfähigkeit eng ineinandergreifen. Im Zentrum steht die Resilienz maritimer Infrastruktur: Hafen, Logistik, Energie- und Datenflüsse sind wirtschaftlich kritisch und sicherheitsrelevant, weil die Region zugleich globaler Logistikstandort, maritimer Wirtschaftsraum und Anwendungsraum für vernetzte Mobilitäts-, Energie- und Sicherheitslösungen ist. Dieses Profil knüpft an die länderübergreifende Innovationsstrategie der Metropolregion Hamburg an, die die Schnittpunkte der Innovationsstrategien der beteiligten Länder herausarbeitet und ein überregionales Innovations- und Kooperationssystem entwickeln will. Für die sicherheitsrelevante Standortlogik besonders anschlussfähig sind die dort beschriebenen Leuchtturmthemen, Digitalisierung und KI sowie nachhaltige und smarte Energiesysteme.

Die Kompetenzbasis liegt entsprechend nicht in einem einzelnen Sektor, sondern in der Überlagerung von Hafen- und Logistikfunktionen, maritimer Industrie, Forschung, Transferstrukturen, Start-ups und operativen Anwendern. Beispielhafte Akteure sind das Maritime Cluster Norddeutschland, Hafen- und Logistikakteure, maritime Forschungs- und Transfereinrichtungen wie Fraunhofer CML, DLR-Institute, die Hamburger Universitäten, Unternehmen aus Schifffahrt, Zulieferung und kombinierten Verkehren sowie Kommunen und Sicherheitsbehörden in der Küstenregion.

Abbildung 9: Ökosystem sicherheitsrelevanter Forschung und Innovation in Hamburg und maritimer Küstenregion



Quelle: Stifterverband, eigene Darstellung. Die Abbildung bündelt zentrale Akteursgruppen und Kompetenzfelder des maritimen regionalen Profils: Hafen und Logistik, maritime Wirtschaft, Werften und Marineschiffbau, maritime Zulieferer und Systemintegratoren, Hochschulen und Forschungseinrichtungen, Start-ups, öffentliche Anwender sowie Länder, Kommunen und Sicherheitsbehörden. Sie visualisiert damit eine Standortlogik, in der zivile Infrastruktur, maritime Sicherheit, Digitalisierung und industrielle Anwendung zusammengeführt werden können.

Daraus kann ein Innovationsmechanismus entstehen, der auf der konsequenten Mehrfachnutzung beruht: Lösungen für maritime Lagebilder, den Schutz kritischer Infrastruktur, autonome Systeme oder Resilienz können zivile und verteidigungsbezogene Anwendungen zugleich bedienen. Entscheidend ist, diese Schnittstellen durch Testfelder, Anwenderkontakte und gemeinsame Bedarfsdefinitionen systematisch zu organisieren. Plausible Übertragungseffekte liegen in resilienter Logistik, maritimer Sicherheit, Infrastrukturmanagement und industrieller Anwendung. Dieses Beispiel zeigt, wie Sicherheitsbedarfe und wirtschaftliche Wettbewerbsfähigkeit in einem gemeinsamen Innovationsraum verbunden werden können.

Greifbar wird diese Logik an einem maritimen Lagebildsystem zum Schutz kritischer Infrastruktur über und unter Wasser. Sensoren an Hafenanlagen, unbemannte Über- und Unterwassersysteme, Schiffsidentifikations- und Satellitendaten, sichere Kommunikationskanäle sowie KI-basierte Anomalieerkennung könnten zusammengeführt werden, um ungewöhnliche Bewegungen, Störungen oder Sabotagerisiken frühzeitig zu erkennen. Die Maritime Forschungsstrategie 2025 des Bundes beschreibt hierfür zentrale Innovationspfade: neue Sensortechnologien, autonome Plattformen, multisensorielle Datenfusion, integrierte Lagebilder, Risiko- und Bedrohungsanalysen in Echtzeit, Cyber-Resilienz und Zustandsüberwachung maritimer Strukturen.

Hinter einem solchen System steht ein Verbund aus Infrastrukturbetreibern, Hafen- und Logistikunternehmen, maritimen Technologieanbietern, Forschungseinrichtungen, Sicherheitsbehörden sowie kommunalen und Landesakteuren. Zivil stärkt ein solcher Innovationspfad Hafensicherheit, Logistik, Verkehrsleitung, Energieinfrastruktur und Infrastrukturmanagement; sicherheitsbezogen trägt er zum Schutz von Seekabeln, Offshore-Anlagen, Hafenräumen und maritimen Versorgungswegen bei. Das Beispiel zeigt, warum die Küstenregion nicht nur Forschungsstandort, sondern auch Test- und Anwendungsraum für sicherheitsrelevante Mehrfachnutzung ist.

4.2 Nordrhein-Westfalen: Innovationspipeline für industrielle Skalierung

Nordrhein-Westfalen steht für ein Profil, in dem sicherheitsrelevante Forschung vor allem über industrielle Anwendung und Skalierung wirksam werden kann. Im Mittelpunkt steht industrielle Resilienz: Energieversorgung, Cybersecurity, Produktionsfähigkeit und robuste Lieferketten sind sicherheitspolitisch relevant, weil sie wirtschaftliche Leistungsfähigkeit und gesellschaftliche Stabilität absichern. NRW ist ein industriell geprägter Innovationsstandort und rückt in seiner Innovationsstrategie unter anderem innovative Werkstoffe und intelligente Produktion, vernetzte Mobilität und Logistik, Energie und innovatives Bauen sowie Schlüsseltechnologien der Zukunft und IKT in den Mittelpunkt.

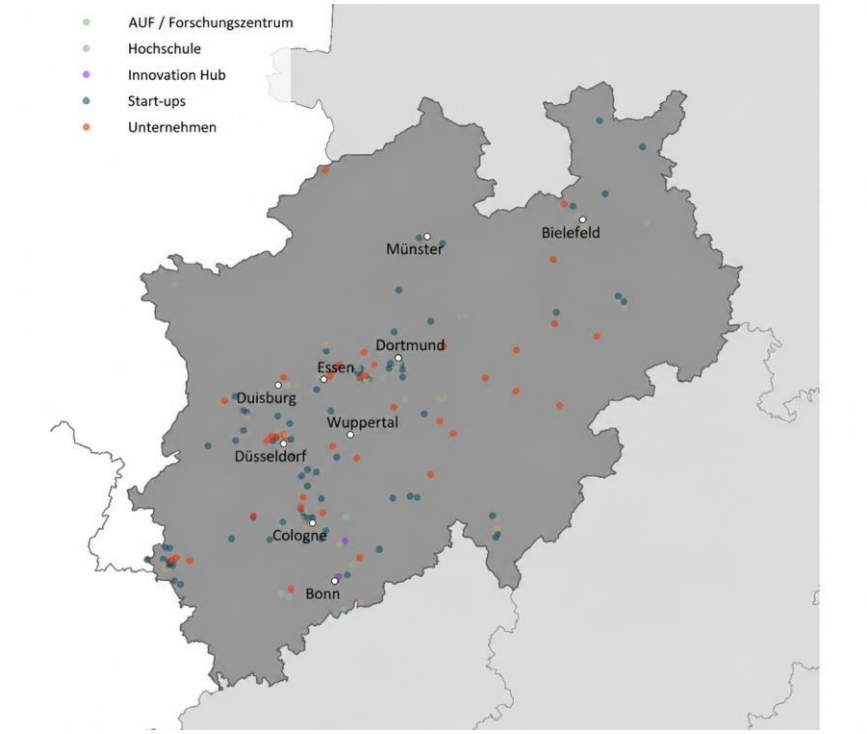
NRW strebt in seiner Innovationsstrategie keine Verengung auf einzelne Branchen oder Technologien an, sondern stellt innovative Herausforderungen in den Mittelpunkt. Digitalisierung, Nachhaltigkeit, Resilienz und neue Geschäftsmodelle werden als Querschnittsthemen über alle Innovationsfelder hinweg verstanden. Damit bietet NRW ein plausibles Profil für sicherheitsrelevante Innovationen, die nicht primär aus militärischer Forschung entstehen, sondern aus der Verbindung von industrieller Anwendung, Energie- und Infrastruktursystemen, Cybersecurity, KI, Robotik, Dateninfrastrukturen, Hochschulen, Forschungseinrichtungen, Start-ups und Mittelstand.

Für Nordrhein-Westfalen lässt sich diese Logik an einem vernetzten Schutzsystem für die Widerstandskraft industrieller Energie- und Produktionsanlagen zeigen. Sensortechnik, digitale Zwillinge, KI-gestützte Angriffserkennung und Notfallsteuerung könnten genutzt werden, um Energieflüsse, Produktionsanlagen und Lieferketten auch bei Cyberangriffen, Sabotage oder Versorgungsschocks funktionsfähig zu halten. Hinter einem solchen Schutzsystem stünde ein Verbund aus industriellen Anwendern wie thyssenkrupp, Energie- und Netzinfrastrukturakteuren wie RWE und Amprion, die RWTH Aachen als forschungsstarke Hochschule sowie digitalen Sicherheitsakteuren wie dem Bundesamt für Sicherheit in der Informationstechnik in Bonn. Dadurch lässt sich der Innovationspfad nicht nur technologisch, sondern auch anwendungsnah begründen:

Forschung, industrielle Nachfrage, Energieinfrastruktur und Cybersicherheitskompetenz kommen in einem regionalen Skalierungsraum zusammen.

Im zivilen Bereich stärkt dies die industrielle Produktivität, die Energiesicherheit und robuste Wertschöpfungsketten; im Sicherheitsbereich erhöht es das Durchhaltevermögen kritischer Industrie- und Versorgungsstrukturen. Nordrhein-Westfalen bietet dafür reale industrielle Testumgebungen, wachstumsstarke Unternehmen, Akteure der Energiewirtschaft und eine dichte Forschungslandschaft.

Abbildung 10: Ökosystem sicherheitsrelevanter Forschung und Innovation in Nordrhein-Westfalen



Quelle: Eigene Darstellung. Die Abbildung bündelt zentrale Akteursgruppen und Kompetenzfelder des nordrhein-westfälischen Profils: Hochschulen und außeruniversitäre Forschung, Industrie und Mittelstand, Energie- und Infrastrukturakteure, IT- und Cybersecurity-Kompetenzen, Start-ups, Cluster und digitale Hubs, Kommunen und Regionen, Testfelder, Reallabore sowie Förder- und Kapitalgeber. Sie visualisiert damit eine Standortlogik, in der sicherheitsrelevante Forschung vor allem über industrielle Anwendung, Resilienz und Skalierung Wirkung entfalten kann.

Daraus kann ein Innovationsmechanismus entstehen, der Forschung und Start-ups mit industrieller Anwendung verbindet: Neue Lösungen können in realen industriellen Kontexten erprobt, integriert und skaliert werden. Entscheidend ist der Übergang vom Prototyp in die industrielle Nutzung. Plausible Übertragungseffekte liegen in der Produktivität, robusteren Wertschöpfungsketten, Energie- und Cybersicherheit sowie neuen industriellen Anwendungen. Das Beispiel zeigt, wie sicherheitsrelevante Forschung wirtschaftliche Breite erreichen kann.

5. ZUSAMMENFASSENDE ANALYSE DER SYSTEMISCHEN ARCHITEKTUR UND STRATEGISCHEN ARBEITSTEILUNG

Die regionalen Fälle machen deutlich: Sicherheitsrelevante Forschung und Innovation brauchen Orte, an denen Bedarfe, Kompetenzen und Anwendung zusammenkommen. Regionale Standortprofile können helfen, die Fragmentierung des deutschen Systems in eine Stärke umzuwandeln. Voraussetzung dafür ist jedoch, dass die regionale Spezialisierung nicht isoliert bleibt, sondern mit nationalen Prioritäten, Förderlogiken und Transferstrukturen verbunden wird.

Damit verschiebt sich der Blick auf die Lösungsebene. Es geht nicht nur darum, einzelne Programme aufzulegen oder bestehende Fördermittel zu erhöhen. Entscheidend ist ein systemischer Ansatz: klare Zielsetzung, skalierungsfähige Finanzierung, institutionalisierte Kooperation, gemeinsame Sprache und eine Governance, die Bund, Länder, Regionen, Wissenschaft, Wirtschaft und Sicherheitsverantwortliche zusammenführt.

Die Analyse des deutschen sicherheitsrelevanten Innovationssystems zeigt, dass dezentrale Vielfalt und technologische Potenziale derzeit häufig fragmentiert bleiben. Anhand regionaler Beispiele (wie in Hamburg, der Küstenregion oder Nordrhein-Westfalen) sowie internationaler Modelle (wie DARPA, NATO DIANA oder UK DASA) lässt sich analytisch ableiten, dass Innovationskraft maßgeblich von einer durchgängigen „Verbindungsarchitektur“ abhängt. In Deutschland weist diese Architektur derzeit signifikante strukturelle Lücken auf. Die Untersuchung identifiziert dabei fünf zentrale Befunde entlang der Innovationskette:

5.1 Fehlen einer durchgängigen Rollenverteilung in der Innovationskette

Die Analyse stellt fest, dass eine strategische Arbeitsteilung über alle föderalen und zivilen Ebenen hinweg – von der Bedarfsdefinition bis zur Marktdurchdringung – aktuell nicht flächendeckend existiert. Die Funktionen der einzelnen Akteure (Bund, Länder, Kommunen, Wissenschaft, Wirtschaft, Anwender und Kapitalgeber) greifen nicht nahtlos ineinander. Die unzureichende Verzahnung von Forschung, Testfeldern, Finanzierung und industrieller Skalierung verhindert die Entstehung systemischer Hebelwirkungen.

5.2 Defizite bei der technologieoffenen Bedarfsübersetzung

Die Untersuchung zeigt eine strukturelle Schwäche in der Übersetzung von Sicherheits- und Verteidigungsbedarfen in Forschungs- und Innovationsprioritäten. Das aktuelle System tendiert dazu, sich zu früh auf spezifische Produkte festzulegen, anstatt Probleme, Fähigkeitslücken und Zielbilder technologieoffen zu beschreiben. Ein strategisches Portfolio, das Beschaffung und Förderung als Orientierung dient, ohne den Lösungsraum vorzeitig zu verengen, ist bislang nicht etabliert.

5.3 Strukturelle Brüche in der Finanzierung bei der Skalierung

Ein zentrales Ergebnis der Untersuchung sind die diskontinuierlichen Übergänge in der Finanzierungskette. Während bestehende Förderlogiken frühe Forschungsphasen abdecken, bricht die Finanzierung beim Übergang zu Demonstration, realitätsnaher Erprobung, Zertifizierung und Beschaffung häufig ab. Die derzeitige öffentliche Finanzierung ist nicht systematisch darauf ausgerichtet, das für die späten Entwicklungsphasen und die Marktreife zwingend erforderliche private Anschlusskapital zu mobilisieren.

5.4 Unzureichende Vernetzung der Transferpfade

Die Analyse diagnostiziert unzureichend institutionalisierte Schnittstellen zwischen Wissenschaft, Staat, Wirtschaft und Kapitalgebern. Es mangelt der Untersuchung zur Folge an belastbaren, wiederholbaren Übergängen von der Forschungsfrage bis zum industriellen Integrationsprojekt. Zudem wird festgestellt, dass europäische Programme (wie EDF oder NATO Innovation Fund) national nicht systematisch genug als Erprobungsräume und Skalierungshebel eingebunden werden.

5.5 Friktionen durch mangelnde Handlungssicherheit (Talente und Kultur)

Die Analyse beobachtet eine ausgeprägte sektorale Trennung: Den Akteuren aus Forschung, Verwaltung, Sicherheitsbehörden und Start-ups fehlt es oftmals an einer gemeinsamen „Sprache“ sowie an personeller Mobilität zwischen den Sektoren. Darüber hinaus identifiziert die Untersuchung unklare Regeln für Verantwortung, Forschungssicherheit und Wissensschutz als wesentliche Ursache für fehlende Handlungssicherheit. Diese regulatorische und ethische Unsicherheit wirkt als Barriere für eine stärkere Öffnung der Wissenschaft hin zu sicherheitsrelevanten Fragestellungen.

6. FAZIT: VOM FORSCHUNGSPOTENZIAL ZUR SICHERHEITSPOLITISCHEN WIRKUNG

Deutschland startet nicht bei null. Die Voraussetzungen für sicherheitsrelevante Forschung und Innovation sind besser, als die Debatte oft vermuten lässt: starke Talente, leistungsfähige Hochschulen, produktive Spitzenforschung, eine breite industrielle Basis und eine wachsende Start-up-Landschaft im Sicherheitsbereich. Der Engpass ist nicht das fehlende Potenzial, sondern die Nutzung.

Genau darin liegt die strategische Aufgabe. Die Bestandsaufnahme macht deutlich, wie entscheidend es für Deutschland ist, vorhandene Stärken konsequent mit sicherheitsrelevanten Bedarfen zu verbinden. Dafür ist ein enges Ineinandergreifen von Forschung, Förderung, Testfeldern, Beschaffung, privatem Kapital und der breiten Umsetzung in der Industrie erforderlich, damit aus wissenschaftlicher Exzellenz sicherheitspolitische Wirkung und wirtschaftliche Wertschöpfung entstehen.

Die doppelte Dividende ist möglich, wenn das System stimmt. Sicherheitsrelevante FuE kann die Verteidigungsfähigkeit, die Resilienz und die technologische Souveränität stärken und zugleich Innovation, Produktivität und Wachstum fördern. Dafür braucht Deutschland keine Kopie eines ausländischen Modells, sondern ein eigenes System, das zur starken zivilen Forschungsbasis, zur industriellen Struktur und zur föderalen Ordnung des Landes passt.

Der Zeitpunkt erhöht den Handlungsdruck. Sicherheits- und verteidigungspolitische Fragen werden breiter diskutiert, und die Bereitschaft, in Sicherheit zu investieren, nimmt zu. Gerade diese veränderte Debattenlage verlangt jedoch eine besonders sorgfältige, transparente und verantwortliche Priorisierung. Sicherheitsrelevante Forschung darf dabei weder pauschal mit Militarisierung gleichgesetzt noch als innovationspolitisches Allheilmittel behandelt werden. Entscheidend ist, Potenziale, Risiken, Zielkonflikte und Grenzen frühzeitig sichtbar zu machen und in demokratisch legitimierten Verfahren verantwortbar in Forschung, Anwendung und Skalierung zu übersetzen.

Die Weiterentwicklung entsteht deshalb nicht durch einzelne Programme oder höhere Budgets allein. Sie entsteht durch politische Weichenstellungen, die vorhandene Exzellenz mobilisieren, Innovationsökosysteme stärken und zugleich klare Regeln für Verantwortung, Wissenschaftsfreiheit und zulässige Anwendungskontexte sichern. Es ist nicht erforderlich, die sicherheitsrelevante Forschung in Deutschland neu zu erfinden. Vielmehr gilt es, sie in einem verlässlichen, rechtsstaatlich abgesicherten und transparent priorisierten Ordnungsrahmen besser zu aktivieren, zu verbinden und wirksam zu machen.

LITERATURVERZEICHNIS

Antolin-Diaz, Juan, and Paolo Surico (2025): The Long-Run Effects of Government Spending. American Economic Review 115 (7): 2376–2413. DOI: 10.1257/aer.20231278

Bitkom e.V. (2025): DefTech Report 2025: Einblicke und Forderungen für den DefTech- und Dual-Use Standort Deutschland. URL: https://www.bitkom.org/sites/main/files/2025-04/deftech-report.pdf. Abgerufen am 17.06.2026.

Bunde, Nicolas, Nina Czernich, Oliver Falck und Clemens Fuest (2020): Europäische öffentliche Güter: Was lässt sich vom US-amerikanischen ARPA-System für die Förderung von Sprunginnovationen in Europa lernen? ifo Forschungsbericht 117. URL: https://www.ifo.de/DocDL/ifo_Forschungsbericht_117_Sprunginnovationen.pdf. Abgerufen am 17.06.2026.

Bundesministerium für Forschung, Technologie und Raumfahrt (BMFTR) (2025): 18 Milliarden Euro für die Hightech Agenda Deutschland. Kurzmeldung; Berlin. URL: https://www.bmftr.bund.de/SharedDocs/Kurzmeldungen/DE/2025/09/260925-haushalt-26-1-lesung.html. Abgerufen am 17.06.2026.

Bundesministerium für Wirtschaft und Energie (2018): Maritime Forschungsstrategie 2025. Berlin.

Bundesverband der Deutschen Industrie e.V. (BDI) (2024): „Dual Use“ Forschungsförderung. Positionspapier. URL: https://bdi.eu/de/publications/dual-use-forschungsfoerderung. Abgerufen am 17.06.2026.

Burk, Marian und Hetze, Pascal (2025): Hochschul-Barometer 2025: Lage und Entwicklung der Hochschulen aus Sicht ihrer Leitungen. Stifterverband für die Deutsche Wissenschaft e.V.; Essen. URL: https://www.hochschul-barometer.de/sites/barometer/files/2025-12/hochschul-barometer_2025.pdf. Abgerufen am 17.06.2026.

Caviggioli, Federico, De Marco, Antonio und Scellato, Giuseppe (2018): Assessing the innovation capability of EU companies in developing dual use technologies, Joint Research Centre (JRC), European Commission.

Dealroom.co (2025): The State of Defence Tech 2025. URL: https://content.dealroom.co/uploaded/2025/09/State-of-Defence-Tech-2025-Dealroom-Resilience.pdf?x17682. Abgerufen am 17.06.2026.

Deutscher Bundestag, Wissenschaftliche Dienste (2024): Wehrtechnische Forschung in ausgewählten Ländern: Finanzen, Verantwortlichkeiten, Verfahren. Sachstand WD 2 - 3000 - 050/24. URL: https://www.bundestag.de/resource/blob/1032720/4ec2c18ad1aa3ee397241bf58e418947/WD-2-050-24-pdf.pdf. Abgerufen am 17.06.2026.

Dietrich, Anita, Florian Dorn, Clemens Fuest, Daniel Gros, Giorgio Presidente, Philipp-Leo Mengel und Jean Tirole (2024): Europe's Middle-Technology Trap. EconPol Forum 25 (4): 32–39. URL: https://www.ifo.de/DocDL/econpol-forum-2024-4-dorn-fuest-etal-innovation.pdf. Abgerufen am 17.06.2026.

Erntell, Hannes, Berger-de León, Markus, Flötotto, Max, Bout, Stéphane, Henz, Tobias und Olanrewaju, Tunde (2025): Europe's deep-tech engine could spur $1 trillion in economic growth. McKinsey & Company. URL: https://www.mckinsey.com/capabilities/business-building/our-insights/europes-deep-tech-engine-could-spur-1-trillion-in-economic-growth. Abgerufen am 17.06.2026.

Europäische Kommission (2025): EU Defence Industry Transformation Roadmap: Unleashing Disruptive Innovation for Defence Readiness. COM(2025) 845 final; Brüssel. URL: https://defence-industry-space.ec.europa.eu/document/download/513de692-d08c-40cc-80c3-cb6611ace178_en?filename=EU-Defence-Industry-Transformation-Roadmap.pdf. Abgerufen am 17.06.2026.

Exchange-Rates.org (2025): Euro (EUR) To US Dollar (USD) Exchange Rate History for 2025. Online-Datenbank. URL: https://www.exchange-rates.org/exchange-rate-history/eur-usd-2025. Abgerufen am 17.06.2026.

Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e. V. (2025): Verteidigungsforschung in der Zeitenwende. Positionspapier zur Bundestagswahl 2025.

Gallo, Marcy E. (2026): Defense Primer: Research, Development, Test, and Evaluation. Congress.gov. URL: https://www.congress.gov/crs-product/IF10553. Abgerufen am 17.06.2026.

German Council of Economic Experts (2025): Structural Change in Germany: Productivity, Regional Aspects and the Labour Market. National Productivity Report 2025, Chapter 4. URL: https://www.sachverstaendigenrat-wirtschaft.de/fileadmin/dateiablage/gutachten/fg2025/2025_National_Productivity_Report.pdf. Abgerufen am 17.06.2026.

GovInfo (2025): 6. Research and Development. URL: https://www.govinfo.gov/content/pkg/BUDGET-2025-PER/pdf/BUDGET-2025-PER-3-3.pdf. Abgerufen am 17.06.2026.

Initiative Hochschulen für den Frieden – Ja zur Zivilklausel! (2024): Liste aktueller Zivilklauseln sortiert nach dem Datum ihres Bestehens. URL: http://zivilklausel.de/index.php/bestehende-zivilklauseln. Abgerufen am 17.06.2026.

International Monetary Fund (IMF) (2025): World Economic Outlook Databases. Datenbank. URL: https://www.imf.org/en/publications/sprolls/world-economic-outlook-databases. Abgerufen am 17.06.2026.

Joint Research Centre (JRC), Europäische Kommission (2025): 2025 Industrial Research & Development Investment Scoreboard. Datenbank. URL: https://iri.jrc.ec.europa.eu/data. Abgerufen am 17.06.2026.

Metropolregion Hamburg / Prognos AG (2022): Länderübergreifende Innovationsstrategie für die Metropolregion Hamburg. Ein Projekt der Zukunftsagenda.

Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen (2021): Regionale Innovationsstrategie des Landes Nordrhein-Westfalen 2021–2027.

OECD (2025): Gross domestic spending on R&D. URL: https://www.oecd.org/en/data/indicators/gross-domestic-spending-on-r-d.html. Abgerufen am 17.06.2026.

OECD (2025): Government budget allocations for R&D. OECD Data Explorer. URL: https://data-explorer.oecd.org/vis?fs[0]=Topic,1%7CScience%252C%20technology%20and%20innovation%23INT%23%7CResearch%20and%20development%20%28R%26D%29%23INT_RD%23&pg=0&fc=Topic&bp=true&snb=9&vw=tb&df[ds]=dsDisseminateFinalDMZ&df[id]=DSD_RDS_GOV%40DF_GBARD_NABS07&df[ag]=OECD.STI.STP&df[vs]=1.0&dq=DEU%2BFRA%2BGBR%2BUSA.A..NABS14%2B_T...USD_PPP%2BXDC.Q%2BV&pd=2015,&to[TIME_PERIOD]=false. Abgerufen am 17.06.2026.

Richter, Gérard, Flötotto, Max, Schumacher, Thomas und Henz, Tobias (2025): Orchestrating Europe's deep-tech funding. McKinsey & Company. URL: https://www.mckinsey.de/publikationen/finanzierung-von-deep-tech-in-europa. Abgerufen am 17.06.2026.

U.S. Department of War (2024): Department of Defense Releases the President's Fiscal Year 2025 Defense Budget. Pressemitteilung. URL: https://www.war.gov/News/Releases/Release/Article/3703410/department-of-defense-releases-the-presidents-fiscal-year-2025-defense-budget/. Abgerufen am 17.06.2026.

Wissenschaftsrat (2025): Wissenschaft und Sicherheit in Zeiten weltpolitischer Umbrüche. Positionspapier; Köln. DOI:10.57674/9tr5-kn29

Worldometer (2026): United States Population. Online-Datenbank. URL: https://www.worldometers.info/world-population/us-population/. Abgerufen am 17.06.2026.

Impressum

Sicherheits- und Verteidigungsforschung neu denken – Innovationskraft für Souveränität und Wertschöpfung.

Herausgeber
Stifterverband für die Deutsche Wissenschaft e.V.
Baedekerstraße 1. 45128 Essen
T 0201 8401-0 . mail@stifterverband.de
www.stifterverband.org

Inhaltliche Leitung Stifterverband
Dr. Volker Meyer-Guckel, Generalsekretär, Stifterverband
Andrea Frank, Stellvertretende Generalsekretärin, Stifterverband
Inhaltliche Leitung McKinsey
Prof. Dr. Julia Klier, Senior Partner, McKinsey & Company
Dr. Björn Münstermann, Senior Partner, McKinsey & Company
Dr. Julian Kirchherr, Partner, McKinsey & Company
Katharina Wagner, Associate Partner, McKinsey & Company
Projektteam Stifterverband
Maik Gebert, Dr. Pascal Hetze, Dr. Svetoslava Antonova-Baumann, Marian Burk, Dr. Frauke Stehr, Simone Höfer, Johanna Guttenberger
Projektteam McKinsey
Dr. Björn Saß, Rebecca Blum, Dr. Robin Seibert, Julio Carrascu-Grau, Andreas Renner, Isabel Backes, Henrik Förster

Veröffentlicht
Juli 2026

Zitationshinweis
Stifterverband für die Deutsche Wissenschaft: Sicherheits- und Verteidigungsforschung neu denken - Innovationskraft für Souveränität und Wertschöpfung. Essen, 2026.