THINKTANK
CORPORATE RESILIENCE
WHITEPAPER 02

Geopolitischer Wandel, KI und unternehmerische Optionen

- Szenarien, Herausforderungen und neue Chancenfelder für die Wirtschaft -

VSW
Bundesverband

LEAD. SECURE. SHAPE RESILIENCE
THI
MBA STRATEGY, GLOBAL RISK AND SECURITY MANAGEMENT

Oktober 2026

Vorwort

Mit dem vorliegenden Whitepaper 02 setzt der **ThinkTank Corporate Resilience** die Arbeit fort, die mit dem ersten Whitepaper[1] im Dezember 2025 begonnen wurde. Seither hat sich die geopolitische Lage weiter verschärft: Handelskonflikte, technologische Blockbildung, sicherheitspolitische Spannungen und die rasante Entwicklung Künstlicher Intelligenz prägen zunehmend den unternehmerischen Alltag. Daraus entstehen neue Chancen, aber auch zusätzliche Verwundbarkeiten für Unternehmen in Deutschland und Europa.

Dieses Whitepaper ordnet die Entwicklungen strategisch ein und übersetzt sie in konkrete Handlungsoptionen für unternehmerische Entscheidungsprozesse.

Zwei Dokumente: Strategisches Whitepaper 02 und Operativer Leitfaden 01

Das Ziel dieses Whitepapers ist es, einen belastbaren Orientierungsrahmen für strategische Entscheidungen in einem zunehmend volatilen, geopolitisch geprägten und KI-getriebenen Umfeld zu geben und nicht, zukünftige Entwicklungen vorherzusagen.

Dieses Whitepaper analysiert, wie sich geopolitische Rahmenbedingungen und KI-Entwicklungen auf Unternehmen in Deutschland und Europa auswirken - und was dies für Führung, Strategie, Resilienz und operative Handlungsfähigkeit bedeutet.

Damit die zentralen Erkenntnisse auf unterschiedlichen Entscheidungsebenen wirksam werden, gliedert sich die Veröffentlichung in zwei Dokumente:

- ein **Strategisches Whitepaper** - dieses Dokument -, das die wichtigsten Fakten, Befunde und Handlungsimplikationen für strategische Entscheidungen kompakt darstellt, insbesondere für Geschäftsführung, Vorstand und Aufsichtsrat;

- den **Operativen Leitfaden 01** zum Whitepaper 02 als Begleitdokument, das vertiefende Analysen, Checklisten, Szenario-Stresstests und Arbeitsinstrumente für Unternehmenssicherheit, Informationssicherheit, Risiko-, Krisen- und Business-Continuity-Management, Corporate Resilience, Einkauf, Compliance und weitere relevante Funktionen bereitstellt.

[1] ThinkTank Corporate Resilience (2025): Wirtschaftliche Folgen hybrider Bedrohungen für Unternehmen und ihre Wertschöpfungsketten – Wie muss sich die Wirtschaft jetzt vorbereiten; https://www.vsw-bundesverband.de/wp-content/uploads/Whitepaper_01_ThinkTank_CorporateResilience.pdf

Der ThinkTank Corporate Resilience und der VSW Bundesverband

An der Schnittstelle von Wirtschaft, Staat und Wissenschaft positionieren sich der ThinkTank Corporate Resilience als Denkfabrik und der VSW Bundesverband als Dachverband der regionalen Sicherheitsverbände der Wirtschaft. Ziel ist es, Resilienz als gemeinsame wertschöpfende Aufgabe zu gestalten, Orientierung zu geben und den Dialog zwischen Unternehmen, Politik und Behörden zu stärken. Dabei unterstützt der ThinkTank Corporate Resilience die Vision 2029 des VSW, sich als führende Instanz für Wirtschaftsschutz - Ansprechpartner, Impulsgeber und Plattform für Wissenstransfer, Weiterbildung und Kooperation - zu etablieren.

Für den Herausgeber ThinkTank Corporate Resilience

Prof. Dr. Marc Knoppe Johannes Strümpfel

Whitepaper, Operativer Leitfaden und Executive Summary finden Sie unter:

Herausgeber:

ThinkTank Corporate Resilience: *Wo Wirtschaft und Wissenschaft vorausdenken*

Der **ThinkTank Corporate Resilience** schafft eine Plattform, auf der strategische Trends, geopolitische Analysen und Zukunftsszenarien aus der Resilienzperspektive von Chief Security Officers mit der Business-Sicht von CEOs, Vorständen, Aufsichtsräten und Anteilseignern zusammengeführt werden. Er ist aus der engen Zusammenarbeit zwischen Wirtschaft und Wissenschaft an der Technischen Hochschule Ingolstadt im Bereich „Wertschöpfung durch Corporate Security und Resilienz“ entstanden und eng mit dem MBA-Programm **Strategy, Global Risk & Security Management (Resilience Management)** verbunden.

Initiiert wurde der ThinkTank, um C-Suite-Vertretern, Chief Security Officers und weiteren Führungskräften aller Unternehmensbereiche sowie Behörden ein Forum für zukunftsorientiertes Denken sowie den strategischen Austausch über systemische Risiken **aus wirtschaftlicher Sicht** zu bieten.

Executive Council ThinkTank Corporate Resilience

Prof. Dr. Marc Knoppe (Business School, Technische Hochschule Ingolstadt)

Sven Dawson (Head of Corporate Security, Airbus Defence and Space GmbH)

Stefan Engelbrecht (Chief Security Officer, RWE AG)

Florian Haacke (Leiter Konzernsicherheit, Daimler Truck AG)

Alexander Klotz (Leiter Konzernsicherheit, BMW AG)

Marco Mille (Leiter Unternehmenssicherheit, Siemens AG)

Johannes Strümpfel (Siemens AG; Präsident VSW Bundesverband)

Strategic Foresight Lab

Sven Dawson (Airbus Defence and Space GmbH), Stefan Engelbrecht (RWE AG), Jan Grimser (BMW AG), Gunnar Groß (Airbus Commercial), Linda Joana Hagen (ProSiebenSat.1 Media SE), Stela Häusler (Siemens AG), Thomas Kiele-Dunsche (Daimler Truck AG), Matthew Kish (Siemens AG), Gereon Klein (RWE AG), Prof. Dr. Marc Knoppe (THI), Dr. Terry Daniel Meincke (Siemens AG), Marco Mille (Siemens AG), Thomas Seisler (Securitas), Katharina Stocker (BMW AG), Philipp Stockfisch (BMW AG), Johannes Strümpfel (Siemens AG & VSW Bundesverband), Leonie Wichert (Siemens AG)

in Kooperation mit dem

VSW Bundesverband und dem
Beirat MBA Strategy, Global Risk & Security Management der Technischen Hochschule Ingolstadt.

Inhaltsverzeichnis

Executive Summary **5**

1 Das Ende der geopolitischen Komfortzone **6**

1.1 Vom Globalisierungsgewinner zur resilienzorientierten Unternehmenssteuerung 6

2 Multidimensionale Kraftfelder: Die neuen Spielregeln für Unternehmen **7**

2.1 Eine fragmentierte Weltordnung 7

2.2 Konkrete Wirkung auf Unternehmen 8

2.3 Mitarbeitende, Führungskräfte und Schlüsselpersonen im Kontext der multidimensionalen Kraftfelder 9

2.4 Wenn Krisen sich gegenseitig befeuern: Risikomultiplikatoren 9

3 Technologie und Innovation als geopolitisches Schlachtfeld **10**

4 Die strategische Resilienzlücke der Unternehmen in Deutschland und Europa **13**

4.1 Vier Konfliktsysteme im wirtschaftlichen Stresstest 13

4.2 Fallstudie Ukraine: Wirtschaftliche Resilienz unter Kriegsbedingungen 15

4.3 Internationaler Vergleich: Strategische Differenzen und strukturelle Lücken 17

4.4 Die systemische Resilienzlücke: Anspruch trifft Realität 18

4.5 Was das für die Unternehmen bedeutet 19

5 Initiative Wirtschaftsschutz: Staat als Partner mit Mehrwert? **20**

6 Geopolitische Szenarien 2027-2030 ..... **21**

7 Unternehmensrelevante Implikationen und Chancenfelder **23**

7.1 Potenziell strategisch tragfähige Märkte 23

7.2 Neun kritische Abhängigkeiten 24

7.3 Vier Chancenfelder mit Zukunftspotenzial 24

8 Fazit: Kernbotschaften für die Unternehmensführung **25**

9 Weiterführend: Der Operative Leitfaden 01 ..... **26**

Ansprechpartner und Netzwerke **27**

Literaturverzeichnis **28**

Abkürzungsverzeichnis **36**

Executive Summary

Deutschland zwischen Globalisierung und Resilienzökonomie

Die neue Logik wirtschaftlicher Wettbewerbsfähigkeit

Die geopolitischen Rahmenbedingungen, auf denen das deutsche Erfolgsmodell der Globalisierungsära beruhte, verändern sich grundlegend. Entwicklungen, die lange als vorübergehende Störungen wahrgenommen wurden, erweisen sich zunehmend als Ausdruck eines strukturellen Wandels: Freihandel, stabile Lieferketten, verlässliche Partnerschaften und berechenbare Märkte können nicht länger als dauerhaft gesichert vorausgesetzt werden.

Deutschland und Europa stehen damit vor einer grundlegenden strategischen Neuausrichtung. Wirtschaftliche Wettbewerbsfähigkeit wird künftig stärker durch Resilienz, Diversifikation, technologische Souveränität, den wirksamen Einsatz von KI und strategische Handlungsfähigkeit geprägt.

Drei zentrale Erkenntnisse

- **Wettbewerb wird zunehmend geopolitisch geprägt.** Das exportorientierte, globalisierungsgetriebene Geschäftsmodell Deutschlands steht unter systemischem Anpassungsdruck. Märkte fragmentieren, Abhängigkeiten werden zur strategischen Verwundbarkeit, und wirtschaftlicher Wettbewerb wird zunehmend durch geopolitische Rahmenbedingungen, technologische Blockbildung und KI-getriebene Entwicklungen beeinflusst.
- **Die Resilienzlücke von Unternehmen wird sichtbarer**. Im Vergleich zu führenden Volkswirtschaften zeigt Deutschland strukturelle Herausforderungen bei Entscheidungsgeschwindigkeit, Digitalisierung, Energieunabhängigkeit, KI-Fähigkeiten und strategischer Fokussierung. Für Unternehmen wird daraus die Aufgabe, kritische Abhängigkeiten, operative Verwundbarkeiten und fehlende Anpassungsfähigkeit systematisch zu identifizieren und zu reduzieren.
- **Die Transformation eröffnet neue strategische Chancenfelder.** Verteidigung und Dual-Use, Infrastruktur und Energie, digitale Souveränität einschließlich Künstlicher Intelligenz sowie regionale Wertschöpfung zählen zu den prägenden strategischen Chancenfeldern der kommenden Jahre. Unternehmen, die frühzeitig in Resilienz, technologische Fähigkeiten und neue Partnerschaften investieren, können daraus nachhaltige Wettbewerbsvorteile ableiten.

Leitfrage für jedes Unternehmen:

Welche Entscheidungen müssen heute, in den kommenden sechs Monaten und langfristig getroffen werden, um kritische Verwundbarkeiten zu reduzieren und das eigene Geschäftsmodell resilient, wettbewerbsfähig und anpassungsfähig aufzustellen?

1 Das Ende der geopolitischen Komfortzone

1.1 Vom Globalisierungsgewinner zur resilienzorientierten Unternehmenssteuerung

Jahrzehntelang profitierte Deutschland, wie kaum ein anderes Land, von der Globalisierung. Offene Märkte, stabile Lieferketten, internationale wirtschaftliche Verflechtungen sowie eine weitgehend verlässliche politische und sicherheitspolitische Ordnung dienten als stabiler Rahmen unternehmerischen Handelns. Diese Rahmenbedingungen ermöglichten Unternehmen ein hohes Maß an Planbarkeit, Effizienz und internationaler Skalierung. Heute stoßen traditionelle Optimierungsansätze, die primär auf Effizienz, Kostensenkung und globale Arbeitsteilung ausgerichtet sind, an ihre Grenzen und vernachlässigen innovative Chancen. Risiken, die früher als externe Ausnahme betrachtet wurden, entwickeln sich zu dauerhaften Einflussgrößen strategischer Unternehmenssteuerung.

Unternehmen müssen daher davon ausgehen, dass geopolitische Volatilität, technologische Machtkonkurrenz, KI-getriebene Disruptionen und zunehmende staatliche Eingriffe in Märkte keine temporären Störungen, sondern **dauerhafte Planungsparameter** darstellen. Wirtschaftliche Effizienz bleibt ein zentraler Wettbewerbsfaktor, wird jedoch zunehmend durch Sicherheits-, Souveränitäts- und Resilienzerfordernisse ergänzt.

> Resilienz bezeichnet in diesem Kontext die Fähigkeit von Unternehmen, kritische Erfolgsziele auch unter widrigen Bedingungen aufrechtzuerhalten, Störungen zu widerstehen, sich schnell von Disruptionen zu erholen und sich so anzupassen, dass langfristige Leistungsfähigkeit und Stabilität gestärkt werden.

Resilienz entwickelt sich damit von einer klassischen Risiko- und Schutzfunktion zu einem strategischen Wettbewerbsfaktor. Unternehmen mit resilienten Lieferketten, belastbaren digitalen Infrastrukturen und hoher Anpassungsfähigkeit können Marktchancen schneller nutzen, regulatorische Anforderungen besser erfüllen und ihre operative Leistungsfähigkeit auch unter Krisenbedingungen aufrechterhalten. Laut Global Value Chains Outlook 2026 gaben 74 % der befragten Führungskräfte an, Resilienz als Wachstumstreiber zu betrachten (WEF 2026).

Ein „Zurück“ zu den bisherigen sicherheitspolitischen Annahmen erscheint wenig realistisch. Nicht nur einzelne Krisen haben sich verschärft; vielmehr hat sich der Rahmen unternehmerischen Handelns strukturell verändert. Unternehmen stehen zunehmend vor Zielkonflikten zwischen kurzfristiger Effizienz und langfristiger Widerstandsfähigkeit. Die Diversifizierung von Lieferanten, der Aufbau redundanter Kapazitäten, die Absicherung kritischer Technologien oder die stärkere regionale Ausrichtung von Wertschöpfungsketten erhöhen häufig zunächst die Kosten. Gleichzeitig reduzieren sie die Anfälligkeit gegenüber geopolitischen Krisen, Handelskonflikten, Cyberangriffen, technologischen Abhängigkeiten und regulatorischen Eingriffen.

Resilienz wird damit zu einer Managemententscheidung, die Risiken, Chancen und Unternehmensziele ganzheitlich miteinander verbinden muss.

Die zentrale Herausforderung besteht nicht darin, geopolitische Entwicklungen und KI-Dynamiken exakt vorherzusagen. Entscheidend ist vielmehr, strategische und operative Fähigkeiten so auszurichten, dass Unternehmen auch unter volatilen Rahmenbedingungen handlungsfähig bleiben und ihre Geschäftsziele erreichen können. Resilienz ist damit kein Gegenentwurf zu wirtschaftlicher Leistungsfähigkeit, sondern eine wesentliche Voraussetzung für nachhaltige Wettbewerbsfähigkeit, Innovationsfähigkeit und Wachstum.

Für die oberste Managementebene stellt sich deshalb die Frage, wie Corporate Resilience organisatorisch verankert, mit Strategie und Governance verbunden und in kritische Wertschöpfungsprozesse integriert werden kann.

2 Multidimensionale Kraftfelder: Die neuen Spielregeln für Unternehmen

Geopolitik war lange vor allem eine Angelegenheit von Außenministerien, Nachrichtendiensten und sicherheitspolitischen Strategieabteilungen. Heute wirkt sie unmittelbar auf Unternehmensentscheidungen. Kein Unternehmen ist mehr geopolitisch neutral: Auch Unternehmen ohne direkte politische Exponierung sind betroffen, wenn Marktzugang, Energiepreise, Datenflüsse, Lieferketten oder Technologiezugang politisch beeinflusst, reguliert, begrenzt oder anderweitig konditioniert werden.

Weitere Kraftfelder wie Klimawandel, zunehmende Umweltbelastungen, die Verknappung kritischer Ressourcen wie Wasser sowie weitere ökologische, demografische und gesellschaftliche Trends, etwa die Gestaltung globaler Migration mit ihren Chancen und Herausforderungen, beeinflussen die Rahmenbedingungen unternehmerischen Handelns in erheblichem Maße. Diese Faktoren stehen nicht isoliert nebeneinander, sondern wirken vielfach aufeinander ein und entfalten in Kombination mit geopolitischen Entwicklungen zusätzliche Dynamiken, Risiken und Chancen. In Summe bilden sie einen wesentlichen Teil des strategischen Risiko- und Chancenumfelds, das Unternehmen bei der Entwicklung langfristiger Resilienz- und Zukunftsfähigkeitsstrategien berücksichtigen müssen.

2.1 Eine fragmentierte Weltordnung

Der Aufstieg Chinas als wirtschaftlicher, technologischer und politischer Akteur verändert die bisher stark US-geprägte internationale Ordnung. China und Indien sowie weitere aufstrebende Staaten versuchen, ihren Einflussbereich auszubauen. Sichtbar wird dies unter anderem an Formaten wie BRICS, die weniger als geschlossenes Gegenmodell, sondern vielmehr als Ausdruck einer wachsenden Bereitschaft zu alternativen Macht- und Wirtschaftsbeziehungen zu verstehen sind.

Gleichzeitig wird die NATO durch die stärkere Pazifik-Fokussierung der US-Außenpolitik unter Anpassungsdruck gesetzt, während sich die EU-Bestrebungen nach größerer strategischer Autonomie verstärken (Rat der Europäischen Union 2022; Europäische Kommission, Hoher Vertreter 2025). Für Unternehmen bedeutet das: Marktzugang hängt zunehmend nicht mehr allein von der eigenen Wettbewerbsfähigkeit ab, sondern auch von politischen Rahmenbedingungen, regulatorischen Vorgaben und strategischen Allianzen. Dies führt zu einem Wettbewerb um Ressourcen, Technologien, Standards, industrielle Wertschöpfung und geopolitischen Einfluss (vgl. Mearsheimer 2014; Die Bundesregierung 2023; Münchner Sicherheitskonferenz 2026; Merz 2026).

2.2 Konkrete Wirkung auf Unternehmen

Dimension	Konkrete Auswirkung
Märkte	Marktzugang wird politisch konditioniert; Exportkontrollen und Sanktionen schließen Wirtschaftsräume.
Lieferketten	Single-Source-Abhängigkeiten werden zum Existenzrisiko; Nearshoring ist strategisch zu betrachten, nicht nur kostengetrieben.
Kapital	Geopolitisches Risiko wird eingepreist; ESG- und geopolitische Compliance-Anforderungen überlagern sich.
Talente	Fachkräftezuwanderung wird politisch reguliert; Standortentscheidungen erhalten eine geopolitische Dimension.
Innovation	Technologietransfer wird beschränkt; IP-Schutz und Dual-Use-Kontrollen nehmen zu.
Rohstoff- und Energieversorgung	Rohstoffe und Energie werden geopolitisch instrumentalisiert; Lieferengpässe und Preissteigerungen erhöhen Kosten und verstärken Standort- sowie Lieferantenrisiken.
Standorte und Produktion	Standortattraktivität wird durch geopolitische Stabilität geprägt; Sanktions-, Ressourcen- und Lieferkettenrisiken beeinflussen die langfristige Betriebsfähigkeit.

Tabelle 1: Konkrete Wirkung geopolitischer Entwicklungen auf Unternehmen. Quelle: eigene Darstellung auf Basis von Hakobyan, Meleshchuk, Zymek 2023; WTO 2023; IMF 2023b; OECD 2021; Europäische Kommission 2024; IEA 2022; WEF 2026

Eine funktionsspezifische Übersicht mit konkreten Handlungsoptionen für Märkte, Lieferketten, Kapital, Talente, Innovation, Rohstoff- und Energieversorgung, Standorte

und Produktion, Mitarbeitende und Führungskräfte sowie Künstliche Intelligenz findet sich im Operativen Leitfaden 01, Modul 1, Kapitel 2.

2.3 Mitarbeitende, Führungskräfte und Schlüsselpersonen im Kontext der multidimensionalen Kraftfelder

Zentrales Schutzgut jedes Unternehmens sind seine Mitarbeitenden: Fürsorgepflicht, Reise- und Standortsicherheit, Erreichbarkeits- und Evakuierungskonzepte sowie der Schutz vor Ausspähung und Anbahnung betreffen die gesamte Belegschaft (vgl. BfV 2025). Darüber hinaus gilt: Führungskräfte und Schlüsselpersonen können durch ihre Funktion, Sichtbarkeit und Entscheidungsverantwortung einer erhöhten digitalen und physischen Exponierung unterliegen. Öffentlich verfügbare Informationen, digitale Spuren sowie Termin- und Reisedaten können zusammengeführt und für Phishing, Ausforschung, Einflussnahme, gezielte Annäherung oder physische Bedrohungen genutzt werden. Dabei können auch digitale Spuren und öffentlich verfügbare Informationen von Familienangehörigen, insbesondere von Partnern oder Kindern, Rückschlüsse auf Aufenthaltsorte, Routinen oder Bewegungsprofile exponierter Personen ermöglichen. Hinzu kommen KI-gestützte Stimm- und Videofälschungen (Deepfakes): Schon kurze öffentlich verfügbare Ton- oder Videoaufnahmen können genügen, um Führungskräfte täuschend echt zu imitieren, zu diskreditieren oder erpressbar zu machen (vgl. BSI 2024; NCSC 2025).

Der Schutz exponierter Personen ist daher als Bestandteil der Unternehmensresilienz - abhängig von Sicherheitslage, Funktion und Risiko - zu berücksichtigen. Maßnahmen müssen verhältnismäßig sein und Sicherheitsinteressen, Persönlichkeitsrechte sowie die notwendige Sichtbarkeit und Handlungsfähigkeit von Führung in Einklang bringen.

Fazit: Digitale und physische Exponierung von Führungskräften und Schlüsselpersonen ist als zusammenhängendes Unternehmensrisiko zu bewerten sowie verhältnismäßig zu adressieren.

2.4 Wenn Krisen sich gegenseitig befeuern: Risikomultiplikatoren

Geopolitische Risiken wirken selten isoliert. Ihre besondere Relevanz entsteht dort, wo einzelne Störungen über Energie, Logistik, Daten, Kapitalmärkte, Lieferketten, Regulierung, gesellschaftliche Stabilität und Klima in andere Systeme übertragen werden. Dadurch können aus zunächst begrenzten Ereignissen komplexe Wirkungsketten entstehen, die mit klassischen Einzelrisikoansätzen nicht mehr beherrschbar sind (Kotzanikolaou, Theoharidou, Gritzalis 2013; Mühlhofer, Bresch, Koks 2024).

Ein Cyberangriff kann Produktionsprozesse unterbrechen, Lieferverpflichtungen gefährden, regulatorische Meldepflichten auslösen, Reputationsschäden erzeugen und finanzielle Auswirkungen nach sich ziehen. Genau in diesen Kettenreaktionen liegt die eigentliche Verwundbarkeit für die Erreichung von Unternehmenszielen.

Unternehmen können sich wirksam schützen, wenn sie geopolitische Risikofelder nicht als Sammlung isolierter Einzelrisiken, sondern als vernetztes System begreifen, managen und als wesentliches Element ihrer Wertschöpfung verstehen.

Eine fortschrittliche Resilienzstrategie kombiniert mindestens sechs Bausteine: (1) Früherkennung, (2) Reduktion kritischer Abhängigkeiten, (3) robuste Governance und Krisensteuerung, (4) belastbare Lieferketten- und Technologieresilienz, (5) Due Diligence und Schutz kritischer Assets sowie (6) Kooperation mit vertrauenswürdigen Partnern und Behörden. Die vollständige Analyse der Risikomultiplikatoren inklusive Selbstcheck-Fragen findet sich im Operativen Leitfaden 01, Modul 2, Kapitel 3.



Abbildung 1: Geopolitisch bedeutsame Risikofelder und zugeordnete Risikomultiplikatoren. Eigene Darstellung.

3 Technologie und Innovation als geopolitisches Schlachtfeld

Mit der Verschiebung der globalen Machtstrukturen kommt der **technologischen Entwicklung** eine neue, zentrale Rolle zu. **Technologie** ist nicht länger ausschließlich ein Treiber wirtschaftlichen Fortschritts, sondern wird zunehmend zum entscheidenden Faktor geopolitischer Machtprojektion, wirtschaftlicher Wettbewerbsfähigkeit und sicherheitspolitischer Handlungsfähigkeit.

Im Zentrum dieses Wettbewerbs stehen wenige, aber systemkritische **Technologiefelder**: **Künstliche Intelligenz**, **Halbleitertechnologien** sowie **digitale Infrastrukturen, Cloud-Ökosysteme, Datenräume** und **Plattformen.** Wie schnell eine Schwachstelle in weit verbreiteter Basissoftware zu einem breiten Risiko für Unternehmen werden kann, zeigten zuletzt die als „PHP2Shell“ bekannt gewordenen zwei kritischen Schwachstellen in der Laufzeitumgebung der Skriptsprache PHP, die am 21. Oktober 2026 veröffentlicht wurden und zahlreiche Webanwendungen weltweit potenziell betrafen (BSI 2026c).

Vor diesem Hintergrund gewinnt das Konzept der **digitalen Souveränität einschließlich KI-Fähigkeiten** an Bedeutung. Staaten und Unternehmen stehen zunehmend vor der Frage, inwieweit sie ihre technologischen Grundlagen kontrollieren oder von externen

Akteuren abhängig sind. Diese Abhängigkeiten betreffen etwa den Zugang zu **Cloud-Infrastrukturen**, die Nutzung proprietärer Softwarelösungen oder die Kontrolle über kritische Datenbestände (JRC 2025; Europäische Kommission 2025; Europäisches Parlament 2025). Gleichzeitig führt der Versuch, technologische Souveränität zu sichern, zu neuen Regulierungen und Eingriffen, die ihrerseits die unternehmerische Flexibilität beeinflussen können (Europäische Kommission 2023a).

Ein zentrales verbindendes Element dieser Entwicklungen ist der **Cyberraum**. **Cyber** wird zunehmend als strategisches Instrument genutzt, das wirtschaftliche, politische und sicherheitspolitische Dimensionen miteinander verknüpft. Aktivitäten im **Cyberraum** reichen von Wirtschaftsspionage über Sabotage bis hin zu gezielten Einflussoperationen und ergänzen dabei Angriffe in der physischen Sphäre (BfV 2025; BfV 2026). Für Unternehmen bedeutet dies, dass **Cyberrisiken** nicht mehr isoliert als IT-Thema betrachtet werden können, sondern als integraler Bestandteil geopolitischer Konfliktlagen verstanden und entsprechend auf strategischer Ebene - insbesondere als Teil eines präventiven und ganzheitlich ausgerichteten Wirtschaftsschutzes - adressiert werden müssen (BSI 2025; BSI 2024).

Künstliche Intelligenz verstärkt diese Entwicklung in beide Richtungen: Angreifer nutzen KI, um Schwachstellen schneller zu finden, Phishing und Social Engineering zu personalisieren und mit Stimm- und Videofälschungen (Deepfakes) Führungskräfte oder Geschäftspartner zu imitieren; auf Verteidigerseite verkürzt KI die Zeit für Erkennung und Reaktion (BSI 2026a; BSI 2024; NCSC 2025). Zugleich entsteht eine neue Abhängigkeit: Leistungsfähige KI-Modelle, Rechenzentren und KI-Chips konzentrieren sich auf wenige, überwiegend außereuropäische Anbieter und unterliegen Exportkontrollen (Kleinhans, Jha 2025; Crosignani et al. 2024). Für Unternehmen ist KI damit zugleich Produktivitätshebel, Angriffsfläche und strategische Abhängigkeit. Ihre Ergebnisse ersetzen zudem keine fachliche Prüfung, da KI fehlerhafte oder erfundene Aussagen liefern kann („Halluzinationen“). Risiken und Gegenmaßnahmen beschreibt der Operative Leitfaden 01 in Modul 1, Kapitel 2, Abschnitt 2.9, den Einsatz als Werkzeug in Modul 3, Kapitel 4, Abschnitt 4.2 und Chancen in Modul 9, Kapitel 10, Abschnitt 10.3.

Exemplarisch lässt sich diese Entwicklung am **Beispiel Chinas** verdeutlichen. Die chinesische Technologieoffensive ist in umfassenden Plänen und Programmen verankert. Seit den 1990er-Jahren verbindet Peking Langfristplanung mit nationaler Industrie- und Sicherheitsstrategie; unter Xi Jinping wurde technologische Eigenständigkeit noch stärker als strategisches Leitmotiv verankert (Eigner 2025; Zenglein, Holzmann 2019). Meilensteine dieser Planungen sind im Schaubild aufgeführt.



Abbildung 2: Meilensteine der chinesischen Technologie- und Innovationsstrategie. Eigene Darstellung auf Basis von Eigner (2025), Wübbeke et al. (2016) sowie Zenglein, Holzmann (2019).

Diese Strategiepläne verdeutlichen Chinas Ambition, bis 2049, dem 100. Jahrestag der Gründung der Volksrepublik China, zur führenden Industrie- und Technologiemacht aufzusteigen. Technologische Innovation wird in der offiziellen Rhetorik der Kommunistischen Partei Chinas (KPCh) als Schlüssel zur nationalen Revitalisierung und zum globalen Einfluss bezeichnet (Eigner 2025; Wübbeke et al. 2016; Zenglein, Holzmann 2019). Im Westen sorgten diese Programme früh für Aufmerksamkeit: „Made in China 2025“ etwa galt als industriepolitische Offensive auf dem Weg zur Technologieführerschaft und führte zu erheblichen Gegenmaßnahmen, darunter Exportkontrollen auf kritische Technologien (Zenglein, Holzmann 2019; U.S. Department of State 2025; Crosignani et al. 2024).

Technologiepolitik wird staatlicherseits heute oft gezielt eingesetzt, um eigene Abhängigkeiten zu reduzieren und gleichzeitig Einfluss auf internationale Wertschöpfungsketten auszuüben; westliche Sicherheitsbehörden warnen dabei

insbesondere vor staatlich flankiertem Wissens- und Technologietransfer in strategischen Zukunftsfeldern (ODNI/NCSC 2025; BfV 2024). Für Unternehmen ergibt sich daraus die Notwendigkeit, strategische Entscheidungen nicht nur unter wirtschaftlichen, sondern auch unter geopolitischen Gesichtspunkten zu bewerten.

Die Konsequenzen für Unternehmen sind weitreichend. Technologische Entscheidungen werden zunehmend zu sicherheitsrelevanten und geopolitischen Entscheidungen. Die Auswahl von Partnern, Technologien und Märkten ist eng mit Fragen der Resilienz und strategischen Positionierung eines Unternehmens und seiner Wertschöpfung verknüpft. Unternehmen müssen daher ihre technologischen Abhängigkeiten systematisch analysieren, Risiken diversifizieren und gleichzeitig ihre Fähigkeit stärken, kritische Technologien zu schützen und weiterzuentwickeln (Kleinhans, Jha 2025; Europäische Kommission 2025).

Zusammenfassend zeigt sich: Technologie ist zu einem zentralen Austragungsort geopolitischer Konkurrenz geworden. Für Unternehmen bedeutet dies, dass Innovation nicht mehr nur unter Effizienz- und Wachstumsaspekten betrachtet werden kann, sondern integraler Bestandteil einer umfassenden Strategie ist, die wirtschaftliche, sicherheitspolitische und geopolitische Dimensionen miteinander verbindet (Europäische Kommission 2023b; BSI 2025).

4 Die strategische Resilienzlücke der Unternehmen in Deutschland und Europa

Deutschland verfügt über eine leistungsfähige industrielle Basis, technologisches Know-how und erhebliche wirtschaftliche Ressourcen. Die Anforderungen an wirtschaftliche Wettbewerbsfähigkeit und unternehmerische Widerstandsfähigkeit haben sich jedoch grundlegend verändert. In einer Welt, die Anpassungsfähigkeit, digitale und technologische Souveränität, eine resiliente Energieversorgung und geopolitische Handlungsfähigkeit zunehmend voraussetzt, treten strukturelle Verwundbarkeiten deutlicher hervor. Diese betreffen insbesondere strategische Abhängigkeiten, technologische Fähigkeiten und die Fähigkeit, auf externe Störungen schnell und wirksam zu reagieren.

4.1 Vier Konfliktsysteme im wirtschaftlichen Stresstest

Der russische Angriffskrieg gegen die Ukraine, der Krieg der USA und Israels gegen den Iran, die Spannungen in der Taiwanstraße sowie die restriktive Zoll- und Handelspolitik der USA sind Ausdruck unterschiedlicher geopolitischer Konfliktdynamiken und stellen die wirtschaftliche Resilienz deutscher und europäischer Unternehmen auf die Probe. Besonders deutlich wird dies an den erheblichen Einschränkungen des Schiffsverkehrs

durch die Straße von Hormus und ihren Auswirkungen auf Energieversorgung, Transportkosten und internationale Lieferketten.

Konfliktsystem	Risiko für Unternehmen	Chance für Unternehmen
Russland - Ukraine	Energie- und Rohstoffschocks, gestörte osteuropäische Lieferketten, steigende Sicherheitsanforderungen sowie mögliche Auswirkungen höherer Verteidigungsausgaben auf öffentliche Haushalte und Investitionsprioritäten.	Beschleunigter Aufbau einer diversifizierten und resilienteren Energieversorgung (LNG, Erneuerbare, Wasserstoff); Wachstum der Verteidigungsindustrie; Beteiligung am Wiederaufbau der Ukraine (Wiederaufbaubedarf rund 588 Mrd. US-Dollar über die kommenden zehn Jahre, Stand Dezember 2025; World Bank et al. 2026).
Iran - USA	Höhere Ölpreise und Transportkosten; erhebliche Beeinträchtigungen strategischer Seehandelsrouten, insbesondere der Straße von Hormus, sowie mittelbare Auswirkungen auf weitere internationale Transportverbindungen; Planungsunsicherheit für Exporteure.	Diversifizierung von Energie- und Handelsbeziehungen; Entwicklung alternativer Transportwege und resilienterer Logistiknetzwerke; zusätzliche Nachfrage nach Energieeffizienz-, Infrastruktur- und Sicherheitstechnologien.
China - Taiwan	Potenziell weitreichende Störungen globaler Halbleiter- und Technologielieferketten mit erheblichen Auswirkungen auf exportorientierte Industrien; China war 2025 erneut Deutschlands wichtigster Handelspartner gemessen am gesamten Warenhandelsumsatz (Destatis 2026).	Ausbau europäischer Halbleiterkapazitäten (European Chips Act, Verordnung (EU) 2023/1781); gezieltes De-Risking; Diversifizierung technologischer Abhängigkeiten, Stärkung regionaler Wertschöpfungsketten und Nearshoring

Konfliktsystem	Risiko für Unternehmen	Chance für Unternehmen
USA - EU (Zoll- und Handelspolitik)	US-Zollregelungen mit einem vereinbarten allgemeinen Höchstzollsatz von 15 % für die meisten EU-Waren (politische Grundsatzeinigung im August 2025; EU-seitige Regelungen zur Umsetzung in Kraft seit 01.07.2026), produktspezifischen Ausnahmen und höheren Sonderzöllen insbesondere im Stahl- und Aluminiumbereich sowie wiederholte Drohungen mit Zusatzzöllen (Die Bundesregierung 2026c); die EU-Warenausfuhren in die USA lagen zeitgleich im ersten Quartal 2026 rund 30,4 % unter dem Vorjahreswert (Eurostat 2026). Planungsunsicherheit für Exporte und Investitionen.	Diversifizierung in Wachstumsmärkte (u. a. Indien, ASEAN) und Nutzung von EU-Freihandelsabkommen; lokale Wertschöpfung in den USA zur Reduktion handelspolitischer Risiken, soweit wirtschaftlich und strategisch sinnvoll; Stärkung des EU-Binnenmarkts.

Tabelle 2: Konfliktsysteme im wirtschaftlichen Stresstest: Risiken und Chancen für Unternehmen. Eigene Darstellung.

4.2 Fallstudie Ukraine: Wirtschaftliche Resilienz unter Kriegsbedingungen

Mit Beginn der groß angelegten russischen Invasion im Februar 2022 war die Ukraine mit massiven Angriffen auf kritische Infrastruktur, erheblichen wirtschaftlichen Verwerfungen und weitreichenden Bevölkerungsbewegungen konfrontiert. Bereits im Herbst 2022 wurden erhebliche Teile der Energieinfrastruktur beschädigt; über 2022/23 war rund die Hälfte der Stromerzeugungskapazität besetzt, zerstört oder beschädigt (IEA 2024). Ende 2025 waren rund 3,7 Millionen Menschen innerhalb der Ukraine vertrieben, während sich etwa 5,9 Millionen Geflüchtete im Ausland aufhielten (IOM 2026; UNHCR 2026). Diese Bevölkerungsbewegungen beeinträchtigten die Verfügbarkeit von Arbeitskräften und die wirtschaftliche Leistungsfähigkeit erheblich. Die unmittelbare Folge des Krieges war ein Rückgang des realen Bruttoinlandsprodukts um 28,8 % im Jahr 2022 (Staatlicher Statistikdienst der Ukraine 2026)

Bemerkenswert ist die Anpassungs- und Widerstandsfähigkeit, die Teile der ukrainischen Wirtschaft trotz fortdauernder Kriegshandlungen entwickelten: Bereits 2023 verzeichnete das Land ein Wirtschaftswachstum von rund 5,5 % (Staatlicher Statistikdienst der Ukraine 2026), allerdings ausgehend von einem stark gesunkenen Produktionsniveau. Zur wirtschaftlichen Stabilisierung trugen unter anderem internationale Finanzhilfen, staatliche Unterstützungsmaßnahmen und die staatlich unterstützte Verlagerung von Unternehmen

in sicherere Landesteile bei. Unterschiedliche Anpassungsmechanismen zeigten sich insbesondere in der IT-Wirtschaft (Remotearbeit, Verlagerung von Dienstleistungen), der Landwirtschaft (Anpassung von Absatz- und Transportwegen), der Verteidigungsindustrie (Ausbau inländischer Produktionskapazitäten), dem Bauwesen (Reparatur und Wiederherstellung beschädigter Infrastruktur) sowie im Energiesektor (dezentrale Erzeugung und Wiederherstellung kritischer Versorgungskapazitäten).

Kennzahl	Wert
Einbruch des realen BIP 2022	-28,8 %
Stromerzeugungskapazität 2022/23: besetzt, zerstört oder beschädigt	rund 50 %
Binnenflüchtlinge / Flüchtlinge im Ausland	3,7 Mio. / 5,9 Mio.
Wirtschaftswachstum 2023 (reales BIP, gegenüber 2022)	≈ +5,5 %

Tabelle 3: Kennzahlen der Fallstudie Ukraine. Quellen siehe Text.

Vier strategische Erkenntnisse für Unternehmen:

1. Institutionelle und operative Flexibilität ermöglichen die Anpassung kritischer Geschäftsprozesse selbst unter extremen Störungsbedingungen.

2. Digitale Fähigkeiten und dezentrale Betriebsmodelle können die Kontinuität wesentlicher Unternehmensfunktionen unterstützen.

3. Die Absicherung kritischer Wertschöpfungsketten, Schlüsseltechnologien und Versorgungsstrukturen reduziert systemische Verwundbarkeiten.

4. Klare Zuständigkeiten, kurze Entscheidungswege und eine enge Zusammenarbeit zwischen Staat und Wirtschaft stärken die Reaktions- und Anpassungsfähigkeit.

4.3 Internationaler Vergleich: Strategische Differenzen und strukturelle Lücken

Strategische Dimension	Referenzländer und Befund
Entscheidungsgeschwindigkeit	Dänemark/Estland: fortgeschrittene Verwaltungsdigitalisierung und datenbasierte Verwaltungsprozesse. USA: gezielte industriepolitische Investitionsanreize durch den CHIPS and Science Act. Deutschland steht vor der Herausforderung, Genehmigungsverfahren zu beschleunigen und administrative Prozesse effizienter zu gestalten.
Strategische Investitionsfähigkeit	USA und China setzen umfangreiche staatliche Förder- und industriepolitische Instrumente in KI, Halbleiter, Energie und Elektromobilität ein. Deutschland steht vor der Herausforderung, bestehende industriepolitische Prioritäten konsequent umzusetzen, Investitionen zu mobilisieren und strategische Schlüsseltechnologien gezielt zu stärken.
Innovation & Digitalisierung	USA (Silicon Valley/Wagniskapital), China (Skalierung digitaler Geschäftsmodelle), Estland (Verwaltungsdigitalisierung), Israel (Deep-Tech). Deutschland verfügt über eine leistungsfähige Forschungs- und Industrielandschaft, weist jedoch insbesondere bei der Skalierung junger Technologieunternehmen und der Verfügbarkeit von Wachstumskapital strukturelle Herausforderungen auf.
Fachkräfte & Arbeitsmarkt	Kanada/Australien (punktebasierte Zuwanderung), Singapur (gezielte Gewinnung internationaler Fachkräfte). Deutschland steht vor der Aufgabe, Fachkräftegewinnung, Anerkennungsverfahren und internationale Mobilität effizienter zu gestalten.
Resilienz und Effizienz	Schweiz/Norwegen/Finnland (Krisenvorsorge), Japan/Südkorea (strategische Vorratshaltung und Versorgungssicherheit), USA (Rückverlagerung kritischer Kapazitäten). Deutschland steht vor der Herausforderung, strategische Abhängigkeiten bei Energie, kritischen Rohstoffen, Halbleitern und ausgewählten internationalen Lieferketten systematisch zu bewerten und gezielt zu reduzieren.

Tabelle 4: Internationaler Vergleich strategischer Differenzen und ausgewählter struktureller Herausforderungen. Eigene Darstellung.

Das strategische Ziel: eine innovationsstarke, technologisch leistungsfähige und widerstandsfähige Volkswirtschaft, die digitale Technologien und KI produktiv nutzt, über verlässlichen Zugang zu Investitions- und Wachstumskapital verfügt und kritische externe Abhängigkeiten gezielt begrenzt, ohne die Vorteile internationaler Arbeitsteilung aufzugeben.

Erfolgsfaktor Europa: Deutschland ist als Einzelstaat ein bedeutender wirtschaftlicher und politischer Akteur, dessen strategischer Handlungsspielraum durch eine starke und handlungsfähige Europäische Union erheblich erweitert wird. Als größte Volkswirtschaft der EU kommt Deutschland eine besondere Rolle dabei zu, die wirtschaftliche Stärke des europäischen Binnenmarktes, technologische Innovationsfähigkeit und gemeinsame strategische Handlungsfähigkeit weiterzuentwickeln.

Für Unternehmen eröffnet ein leistungsfähiger europäischer Wirtschaftsraum zusätzliche Möglichkeiten zur Skalierung, Diversifizierung, technologischen Kooperation und Absicherung strategischer Abhängigkeiten. Die gemeinsame europäische Handlungsfähigkeit entwickelt sich damit zu einem wesentlichen Faktor für Wettbewerbsfähigkeit und unternehmerische Resilienz.

4.4 Die systemische Resilienzlücke: Anspruch trifft Realität

Deutschland verfolgt das Ziel, die Resilienz von Staat, Wirtschaft und Gesellschaft systematisch zu stärken - u. a. durch die Nationale Sicherheitsstrategie, den Nationalen Sicherheitsrat und den Operationsplan Deutschland (OPLAN DEU) (Die Bundesregierung 2023; Die Bundesregierung 2025; Bundeswehr 2023). Der Anspruch ist klar formuliert: Resilienz soll gesamtstaatlich und gesamtgesellschaftlich verstanden und in enger Kooperation mit der Wirtschaft umgesetzt werden.

Für die Wirtschaft existiert bislang jedoch kein umfassend öffentlich zugängliches Gesamtbild der konkreten Anforderungen und Unterstützungsleistungen im Spannungs- und Verteidigungsfall. Der OPLAN DEU ist als militärisches Planungsdokument geheim eingestuft; zugleich bestehen bereits Informationsangebote, Kooperationsstrukturen und vertragliche Vereinbarungen mit ausgewählten Unternehmen. Für die Breite der Wirtschaft bleibt damit die Herausforderung, ihre potenzielle Rolle und die daraus resultierenden betrieblichen Anforderungen frühzeitig und hinreichend konkret zu erfassen (vgl. Bundeswehr 2024).

Zwischen diesem Anspruch und der flächendeckenden operativen Umsetzung bestehen weiterhin strukturelle Herausforderungen. Zwar wurden wichtige strategische und institutionelle Grundlagen geschaffen, ihre ressortübergreifende, föderale und wirtschaftsbezogene Operationalisierung bleibt jedoch eine zentrale Aufgabe.

Im aktuellen System lassen sich aus Sicht des ThinkTank neun potenzielle strukturelle Lücken beziehungsweise Handlungsfelder unterscheiden (eigene Analyse des ThinkTank

auf Basis von BBK 2024; Bundeswehr 2024; BSI 2026b), die sich drei übergeordneten Problemdimensionen zuordnen lassen:

Problemdimension	Zugehörige Lücken
Steuerung und Integration	Koordinationslücke · Plattformlücke · Gesamtverteidigungslücke · Operationalisierungslücke auf strategischer Ebene
Geschwindigkeit und Umsetzung	Geschwindigkeitslücke · Umsetzungslücke
Souveränität, Fähigkeiten und regulatorische Kohärenz	Digitale Souveränitätslücke · Regulierungslücke · Bewusstseinslücke

Tabelle 5: Systematisierung potenzieller Resilienzlücken nach drei Problemdimensionen. Eigene Analyse des ThinkTank.

Entscheidend ist der systemische Effekt:

Fehlende Koordination kann die Geschwindigkeit der Reaktion verringern, verzögerte Entscheidungen können Umsetzungsprobleme verstärken, Abhängigkeiten erschweren eigenständige Handlungsfähigkeit, und fragmentierte Regulierung erhöht die Komplexität der Vorsorge und Krisenbewältigung. Die Resilienzlücke ist damit nicht allein als Summe einfacher Defizite zu verstehen. Ihre besondere Tragweite entsteht durch Wechselwirkungen, gegenseitige Verstärkung und mögliche Kaskadeneffekte zwischen den verschiedenen Handlungsfeldern.

4.5 Was das für die Unternehmen bedeutet

- Begrenzte Planbarkeit staatlicher Unterstützung im Krisenfall - Entscheidungswege, Zuständigkeiten und Priorisierungen sind für Unternehmen nicht durchgehend frühzeitig und konsistent erkennbar. Umfang und Zeitpunkt staatlicher Unterstützung können daher nicht vorausgesetzt werden.
- Struktureller Zeitnachteil gegenüber Bedrohungsakteuren: Die langsamere Reaktionsgeschwindigkeit institutioneller Systeme verschiebt den Handlungsspielraum zugunsten schnellerer, adaptiverer Akteure.
- Implizite Verlagerung von Resilienzverantwortung auf die Unternehmen selbst - in der Praxis bedeutet das: Aufbau eigener Lagebilder und Frühwarnsysteme, eigenständige Sicherstellung kritischer Prozesse und unternehmensinterne Resilienzstrukturen unabhängig von staatlicher Steuerung.

Implikation: Unternehmen werden zu wesentlichen Akteuren gesamtwirtschaftlicher Resilienz. Ihre Fähigkeit, kritische Leistungen auch unter außergewöhnlichen Belastungen

aufrechtzuerhalten, trägt unmittelbar zur Stabilität der eigenen Wertschöpfungsketten und wirtschaftlichen Versorgungsstrukturen bei.

Kern jeder unternehmerischen Resilienzstrategie ist daher eine definierte Mindestwertschöpfung: Unternehmen sollten festlegen, welche minimalen Wertschöpfungsaktivitäten sie auch in einer schweren Krise mindestens erbringen müssen, um Kunden zu halten und die Liquidität zu sichern, und welche Mitarbeitenden, Vorprodukte, Systeme und Standorte dafür unverzichtbar sind. Die Minimum Business Continuity Objectives (MBCO) definieren bereits ein akzeptables Mindestleistungsniveau während einer Störung. Eine strategische Resilienzbetrachtung ergänzt diesen Ansatz insbesondere durch die Berücksichtigung längerfristiger geopolitischer Krisen, systemischer Abhängigkeiten und strategischer Unternehmensziele (ISO 2019; ISO 2025; BSI 2023). Hinweise zur ersten Umsetzung enthält der Operative Leitfaden 01, Modul 3, Kapitel 4.

Der vollständige Überblick über die relevanten sicherheitspolitischen Planungsgrundlagen und regulatorischen Anforderungen (OPLAN DEU, NIS-2, DORA, Cyber Resilience Act und KRITIS-Dachgesetz) sowie eine Selbstdiagnose-Checkliste zu allen neun Lücken finden sich im Operativen Leitfaden 01, Modul 7, Kapitel 8.

5 Initiative Wirtschaftsschutz: Staat als Partner mit Mehrwert?

Am 18.03.2026 hat das Bundeskabinett die vom Bundesministerium des Innern vorgelegte Nationale Wirtschaftsschutzstrategie beschlossen (BMI 2026). Sie positioniert den Staat als Partner und Unterstützer, nicht als Ersatz unternehmerischer Eigenverantwortung: Unternehmen bleiben für ihre Sicherheit selbst verantwortlich, erhalten aber gezielte Unterstützung durch Lageinformationen, Prävention, Beratung und bessere Zugänge zu Sicherheitsbehörden.

Positiv bewertet die Wirtschaft insbesondere, dass es nun einen ressortübergreifenden politischen Verantwortlichen für Wirtschaftsschutz gibt. Der zentrale Misfit liegt jedoch weiterhin in der Fragmentierung staatlicher Leistungen: Für Unternehmen bleibt häufig unklar, welche Behörde in welcher Lage zuständig ist und welche Reaktion realistisch erwartet werden kann. Die Zahl an Zentren, Plattformen und Gesprächsformaten wächst schneller als ihre Anschlussfähigkeit an die Wirtschaft.

Für die Unternehmensführung folgt daraus, dass Wirtschaftsschutz stärker als strategischer Erfolgsfaktor verstanden werden muss - nicht nur als Schutzfunktion, sondern als Voraussetzung für Resilienz, Wettbewerbsfähigkeit und Handlungsfähigkeit. Ziele wie Wachstum, Innovation, internationale Geschäftstätigkeit und Versorgungssicherheit lassen sich nachhaltiger verfolgen, wenn Risiken durch Spionage, Sabotage, Cyberangriffe, geopolitische Spannungen und hybride Bedrohungen frühzeitig erkannt und wirksam gesteuert werden. Die engere Zusammenarbeit mit staatlichen Stellen bietet dabei die Chance, Lagebilder, Prävention und Krisenreaktion gezielter in die Unternehmensstrategie zu integrieren.

In der Wirtschaftsschutzstrategie wird zudem als Ziel formuliert, die Leistungsangebote der Sicherheitsbehörden weiterzuentwickeln und stärker am Bedarf der Unternehmen auszurichten. Daraus folgt für die Wirtschaft die Aufgabe, eigene Unterstützungsbedarfe klar zu definieren, zu priorisieren und gebündelt einzubringen.

Sicherheitsverbände übernehmen dabei eine wichtige Schnittstellenfunktion: Sie können Anforderungen aus der Unternehmenspraxis konsolidieren, gegenüber staatlichen Stellen artikulieren und so dazu beitragen, dass Beratungs-, Informations- und Unterstützungsleistungen passgenauer, praxisnäher und wirksamer ausgestaltet werden.

Die gemeinsame Vision: Wirtschaft und Staat verstehen sich als strategische Partner, die Bedrohungen frühzeitig gemeinsam erkennen, Lagebilder teilen, Zuständigkeiten klären und Reaktionsfähigkeit praktisch einüben - von der Prävention über die Früherkennung bis zur Bewältigung konkreter Sicherheitslagen.

Die vollständige Anforderungsliste der Wirtschaft an den Staat (u. a. klare Zuständigkeiten, ein zentraler Zugangspunkt, rechtssicherer Informationsaustausch, praxisnahe Sicherheitsüberprüfungen) findet sich im Operativen Leitfaden 01, Modul 6, Kapitel 7, ergänzt um Hinweise, was Unternehmen intern vorbereiten sollten.

6 Geopolitische Szenarien 2027-2030

Szenarien sind keine Prognosen. Sie sind Denkwerkzeuge - strukturierte Beschreibungen möglicher Zukünfte, die helfen, strategische Entscheidungen unter Unsicherheit zu treffen. Die vier folgenden Szenarien sind nicht nach Eintrittswahrscheinlichkeit gewichtet; welches Szenario sich wie entwickelt, hängt von politischen Entscheidungen, technologischen Entwicklungen und geopolitischen Schocks ab, die heute nicht vorhersehbar sind.

Der strategische Wert liegt nicht im Vorhersagen der Zukunft, sondern in der Frage: Ist unser Geschäftsmodell unter allen vier Szenarien überlebensfähig? Wenn nicht - was muss sich ändern?

Szenario	Kernaussage für Unternehmen
1. Groß angelegter Konflikt in Europa	Hybride Kriegsführung, NATO-Fragmentierung und eine mögliche baltische Krise treffen kritische Infrastruktur, Lieferketten, Cybersicherheit und Mitarbeitende - auch Unternehmen, die selbst keine Konfliktpartei sind.
2. Eskalation in der Taiwanstraße	Ein geoökonomischer Systemschock: Auf Taiwan entfallen rd. 44 % der weltweiten Foundry-Kapazität, rd. zwei Drittel der Kapazität für fortgeschrittene Prozesse (Strukturgröße 16 Nanometer (nm) und kleiner; TrendForce 2024) sowie über 90 % der Kapazität für modernste Chips unter 10 nm (Datenstand 2019; SIA/BCG 2021). Bereits Grauzonenmaßnahmen wirken auf Finanzmärkte, Versicherungsprämien und Schifffahrtskosten.
3. US-China technologische Entkopplung	„Dual Compliance“ wird zum Dauerzustand. Exportkontrollen, Investitionsprüfungen und Listenregime entwickeln sich zu dauerhaften Instrumenten strategischer Machtprojektion - Effizienzlogik wird durch Sicherheits- und Souveränitätslogik ergänzt.
4. Fragmentierung der transatlantischen Partnerschaft	Regulatorische Divergenz statt offener Konfrontation: europäische Unternehmen benötigen zunehmend regionalisierte Technologie-, Daten- und Governance-Strukturen.

Tabelle 6: Geopolitische Szenarien 2027-2030 im Überblick. Eigene Darstellung.

Die vollständigen Eskalationsstufen, Frühindikatoren und Wirkungsanalysen für alle vier Szenarien - als Grundlage für einen Stresstest des eigenen Geschäftsmodells - enthält der Operative Leitfaden 01, Modul 5, Kapitel 6.

Die Szenarien sind als Einzelszenarien beschrieben, schließen sich aber nicht aus: Sie können gleichzeitig oder in Kombination eintreten und sich gegenseitig verstärken. Akteure können eine Krise in einer anderen Region zudem gezielt für eigene Ziele nutzen; China gilt nach Einschätzung der NATO als wesentlicher Ermöglicher der russischen Kriegsführung gegen die Ukraine, insbesondere durch die Unterstützung der russischen Verteidigungsindustrie (NATO 2024).

Das Jahr 2026 zeigt die wirtschaftliche Relevanz paralleler Konflikte: Der fortdauernde Krieg in der Ukraine und der Krieg der USA und Israels gegen Iran sowie die erheblichen Einschränkungen des Schiffsverkehrs durch die Straße von Hormus belasten Energiepreise, Logistik und wirtschaftliche Planbarkeit gleichzeitig. Ein Stresstest sollte

daher auch kombinierte Eskalationsverläufe aus mindestens zwei Szenarien berücksichtigen (Operativer Leitfaden 01, Modul 5, Kapitel 6, Abschnitt 6.5).

7 Unternehmensrelevante Implikationen und Chancenfelder

Die geopolitischen Verwerfungen der Gegenwart sind keine vorübergehenden Störungen, die sich durch operative Anpassungen überbrücken lassen. Die Veränderungen sind weit mehr als nur kurzfristige Markt- und Lieferkettenstörungen. Sie stellen neue Anforderungen an die strategische Führung - mit unmittelbaren Implikationen für Strategie, Organisationsstrukturen, Kapitalallokation und Partnerschaftsmodelle. Vorstände und Geschäftsführungen stehen vor der Aufgabe, Geschäftsmodelle, Marktpositionierungen und Investitionsprioritäten regelmäßig unter veränderten geopolitischen Rahmenbedingungen zu überprüfen: Welche Produkte und Märkte sind unter Berücksichtigung technologischer Verschiebungen einschließlich KI-getriebener Entwicklungen und technologischer Abhängigkeiten, politischer Rahmenbedingungen und der Ressourcenverfügbarkeit langfristig tragfähig?

7.1 Potenziell strategisch tragfähige Märkte

EU-Binnenmarkt: zentraler Anker mit einem weitgehend harmonisierten Rechtsrahmen, industrieller Tiefe und zunehmend auf strategische Autonomie und technologische Wettbewerbsfähigkeit ausgerichteter Industriepolitik.

Indien: seit 2023 bevölkerungsreichstes Land der Welt (UN DESA 2024) mit wachsendem Binnenmarkt und Positionierung als strategisch autonomer Akteur zwischen westlichen und aufstrebenden Machtzentren. Spannungen mit Pakistan können regionale Sicherheits-, Investitions- und Lieferkettenrisiken erhöhen.

Südostasien (ASEAN): profitiert von Nearshoring-Effekten, jungen Bevölkerungen und dynamischen Mittelschichten (FDI-Zuflüsse 2024 rd. 226 Mrd. US-Dollar, getragen u. a. vom Umbau internationaler Lieferketten; ASEAN-Sekretariat/UNCTAD 2025).

Golfregion: Transformation von rohstoff- zu wissensbasierter Wirtschaft mit erheblichem Kapitaleinsatz (IMF 2025); seit 2026 allerdings durch den Iran-Krieg, Angriffe auf Energieinfrastruktur am Golf und die massive Beeinträchtigung des Schiffsverkehrs durch die Straße von Hormus mit deutlich erhöhtem Sicherheits- und Versorgungsrisiko (Euronews 2026a).

Brasilien und Mercosur: Das Interims-Handelsabkommen zwischen der EU und dem Mercosur (Argentinien, Brasilien, Paraguay, Uruguay) wird seit dem 1. Mai 2026 vorläufig angewendet und baut Zölle schrittweise ab (Die Bundesregierung 2026d); die Region verbindet Rohstoff-, Agrar- und Energiepotenzial mit bedeutenden Industrie- und Absatzmärkten. Während das Interims-Handelsabkommen bereits vorläufig angewendet wird, steht der vollständige Abschluss des umfassenderen Partnerschaftsabkommens weiterhin aus (Prüfung durch den EuGH, ausstehende Zustimmung des Europäischen Parlaments).

7.2 Neun kritische Abhängigkeiten

Energie · Lieferketten · Digitalisierung · Halbleiter & Schlüsselkomponenten · Sicherheit (IT, politische Stabilität, Compliance) · Cloud- und Rechenzentrumsinfrastruktur · Cybertechnologien · Physische Sicherheit · Satelliten-, Navigations- und Zeitdienste. Eine vertiefte Analyse je Feld inklusive Leitfragen zur eigenen Abhängigkeitslage findet sich im Operativen Leitfaden 01, Modul 4, Kapitel 5.

Beispiel (illustrativ): Ein mittelständischer Hersteller steuert seine Produktion über eine Software, die in der Cloud eines außereuropäischen Anbieters läuft, bezieht Leiterplatten aus nur einer Region in Ostasien und stützt seine Logistik auf GNSS-Ortung und -Zeitstempel. Er ist damit in drei Feldern zugleich verwundbar (Cloud, elektronische Komponenten, Satellitendienste); fällt eines aus, steht im ungünstigen Fall die gesamte Wertschöpfung. Ein Dependency-Mapping macht solche Kopplungen sichtbar, bevor sie im Ernstfall zu operativen Störungen führen.

Als Leitprinzip für resiliente Geschäftsmodelle gilt: Souveränität, Handlungsfähigkeit, strategische Robustheit.

7.3 Vier Chancenfelder mit Zukunftspotenzial

Chancenfeld	Kern der Chance
Verteidigung & Dual-Use	Wachsender Bedarf an nationaler und kollektiver Sicherheit treibt Investitionen in Software, Sensorik, Robotik, Cybersicherheit und resiliente Energieversorgung - auch für mittelständische Technologieunternehmen.
Infrastruktur & Energie	Netze, Speicher, Wasserstoff und Resilienz-Engineering bilden ein auf Jahrzehnte angelegtes Investitionsspektrum für integrierte Lösungsanbieter.
Digitale Souveränität	Politischer und regulatorischer Druck schafft einen Wachstumsmarkt für sichere Cloud-/Edge-Architekturen, Cybersecurity und vertrauenswürdige KI „made in Europe“; KI selbst wird zum Wachstumsfeld, etwa für souveräne KI-Infrastruktur und KI-gestützte Sicherheitsdienstleistungen.
Regionale Wertschöpfung	Kunden zahlen zunehmend nicht nur für das Produkt, sondern für Lieferfähigkeit, Sicherheitsstandard, regulatorische Konformität und Störungsresistenz.

Tabelle 7: Vier Chancenfelder mit Zukunftspotenzial. Eigene Darstellung.

Diese Chancenfelder sind keine spekulativen Zukunftsbilder, sondern bereits heute durch politische Investitionsprogramme, regulatorische Weichenstellungen und veränderte

Nachfragemuster unterlegt: etwa durch das Sondervermögen Infrastruktur und Klimaneutralität mit bis zu 500 Mrd. Euro für zusätzliche Investitionen, deren Bewilligung im Zeitraum 2025-2036 vorgesehen ist und die unter anderem dem Ziel der Klimaneutralität bis 2045 dienen (SVIKG 2025), die NATO-Zusage von 5 % des BIP bis 2035, aufgeteilt in mindestens 3,5 % für klassische Verteidigungsausgaben und bis zu 1,5 % für weitere verteidigungs- und sicherheitsbezogene Investitionen, etwa in kritische Infrastruktur, Netzsicherheit, zivile Vorsorge und Innovation (NATO 2025), das EU-Instrument SAFE mit Darlehen von bis zu 150 Mrd. Euro für gemeinsame Verteidigungsbeschaffung (Rat der Europäischen Union 2025) sowie das europäische Chips-Gesetz (Europäische Union 2023). Unternehmen, die jetzt handeln, sichern sich strukturelle Vorteile.

8 Fazit: Kernbotschaften für die Unternehmensführung

Vom Lagebild zur Entscheidung - die Leitfrage lautet: Welche Entscheidungen müssen Unternehmen heute, in den kommenden sechs Monaten und langfristig treffen, um resilient, wettbewerbsfähig und anpassungsfähig zu bleiben? Die folgenden sieben Kernbotschaften fassen zusammen, worauf es aus strategischer Sicht der Unternehmensführung jetzt ankommt.

1. Geopolitik ist kein Randthema mehr, sondern eine zentrale strategische Führungsaufgabe - mit direkter Wirkung auf Märkte, Lieferketten, Kapital, Talente, Innovation, Rohstoffe und Energie sowie Standorte.

2. Die Resilienzlücke Deutschlands ist real und messbar - bei Entscheidungsgeschwindigkeit, Digitalisierung, Energieunabhängigkeit und strategischer Fokussierung.

3. Der Staat baut Unterstützungsstrukturen auf (Nationale Wirtschaftsschutzstrategie, OPLAN DEU), doch deren operative Durchdringung ist noch unvollständig - Unternehmen sollten nicht auf durchgehend verlässliche staatliche Steuerung im Krisenfall bauen.

4. Unternehmen werden zu wesentlichen Akteuren gesamtwirtschaftlicher Resilienz - mit der Konsequenz, eigene Lagebilder, Frühwarnsysteme und Resilienzstrukturen aufzubauen.

5. Vier geopolitische Szenarien 2027-2030 (Europa-Konflikt, Taiwan-Eskalation, US-China-Entkopplung, transatlantische Fragmentierung) sollten als Stresstest für das eigene Geschäftsmodell dienen.

6. Neun kritische Abhängigkeiten - Energie, Lieferketten, Digitalisierung, Halbleiter, Sicherheit, Cloud und Rechenzentren, Cyber, physische Sicherheit, Satellitendienste - bestimmen die eigentliche Verwundbarkeit und sollten systematisch kartiert werden.

7. Der geopolitische Wandel eröffnet vielfältige Chancen: Verteidigung & Dual-Use, Infrastruktur & Energie, digitale Souveränität inklusive KI-Anwendungen für die

europäische Industrie, insbesondere für den Maschinenbau, und regionale Wertschöpfung sind die strategischen Chancenfelder der kommenden Jahre.

Das Ziel ist nicht, zukünftige Entwicklungen exakt vorherzusagen, sondern einen belastbaren Orientierungsrahmen für strategische Entscheidungen in einem zunehmend volatilen geopolitischen Umfeld unternehmensspezifisch bereitzustellen.

9 Weiterführend: Der Operative Leitfaden 01

Der begleitende „Operative Leitfaden 01“ übersetzt die in diesem Dokument zusammengefassten strategischen Erkenntnisse und Handlungsimplikationen in konkrete Arbeitsinstrumente für die operative Praxis: funktionsspezifische Maßnahmenkataloge einschließlich des Schutzes von Mitarbeitenden und exponierten Führungskräften sowie der Risiken durch KI, mögliche Risikomultiplikatoren, ein Reifegradcheck für die Resilienzarchitektur mit dreistufiger Bewertungsskala sowie Hinweise zum Einsatz von KI und illustrative erste Schritte für die Umsetzung, das Dependency-Mapping in neun Feldern, den Szenario-Stresstest 2027-2030 mit Arbeitsblatt und Kombinationsprüfung, die Anforderungscheckliste an den Staat sowie den regulatorischen Fahrplan (OPLAN DEU, NIS-2, DORA, Cyber Resilience Act, KRITIS-Dachgesetz), Markteintrittskriterien und Chancenfelder im Detail. Die Module des Leitfadens folgen dabei einer Arbeitslogik (Wirkungen verstehen, Risiken analysieren, Fähigkeiten aufbauen, Abhängigkeiten kartieren, Szenarien testen, Schnittstellen zu Staat und Regulierung nutzen, individuelle Chancen erschließen) und daher nicht der Kapitelfolge dieses Whitepapers.

Ansprechpartner und Netzwerke

Institution	Zuständigkeit
VSW Bundesverband	Netzwerk der Verantwortung für Wirtschaftsschutz; Vision 2029 als führende Instanz für Wirtschaftsschutz - Ansprechpartner, Impulsgeber und Plattform für Wissenstransfer, Weiterbildung und Kooperation.
ThinkTank Corporate Resilience	Denkfabrik für strategische Trends, geopolitische Analysen und Zukunftsszenarien; Kontakt über das Feedback-Formular (siehe Vorwort).
Beirat MBA Strategy, Global Risk & Security Management (THI)	Wissenschaftliche Anbindung an die Technische Hochschule Ingolstadt; Programmberatung und Forschungskooperation.

Literaturverzeichnis

Das Verzeichnis enthält die Quellen des Strategischen Whitepapers und des Operativen Leitfadens 01.

ASEAN-Sekretariat; UNCTAD (2025): ASEAN Investment Report 2025: Foreign direct investment and supply chain development. Jakarta: ASEAN Secretariat. Verfügbar unter: https://unctad.org/publication/asean-investment-report-2025 (Zugriff: 30.09.2026).

BBK - Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2022): Deutsche Strategie zur Stärkung der Resilienz gegenüber Katastrophen. Beschluss der Bundesregierung vom 13.07.2022. Verfügbar unter: https://www.bbk.bund.de/DE/Themen/Nationale-Kontaktstelle-Sendai-Rahmenwerk/Resilienzstrategie/resilienz-strategie_node.html (Zugriff: 16.06.2026).

BBK - Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2024): Umsetzungsplan der Deutschen Strategie zur Stärkung der Resilienz gegenüber Katastrophen. Verfügbar unter: https://www.bbk.bund.de/SharedDocs/Downloads/DE/Mediathek/Publikationen/Sendai-Katrima/umsetzungsplan-resilienzstrategie.pdf?__blob=publicationFile&v=6 (Zugriff: 16.06.2026).

Bentzen, Naja (2024): Online information manipulation and information integrity. European Parliamentary Research Service (EPRS), Briefing PE 762.416. Verfügbar unter: https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/762416/EPRS_BRI%282024%29762416_EN.pdf (Zugriff: 16.06.2026).

BfV - Bundesamt für Verfassungsschutz (2024): Verfassungsschutzbericht 2024. Veröffentlicht am 10.06.2025. Verfügbar unter: https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/verfassungsschutzberichte/2025-06-10-verfassungsschutzbericht-2024.pdf?__blob=publicationFile&v=4 (Zugriff: 17.06.2026).

BfV - Bundesamt für Verfassungsschutz (2025): Spionage, Cyberangriffe & Co. Bedrohungen durch fremde Nachrichtendienste. Januar 2025. Verfügbar unter: https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/spionage-und-proliferationsabwehr/2025-01-spionage-cyberangriffe-und-co.pdf?__blob=publicationFile&v=3 (Zugriff: 17.06.2026).

BfV - Bundesamt für Verfassungsschutz (2026): Cyberangriffe - Gefahren, Risiken und Schutz vor staatlich gesteuerten Attacken. Februar 2026. Verfügbar unter: https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/cyberabwehr/2026-02-cyberangriffe.html (Zugriff: 17.06.2026).

BMI - Bundesministerium des Innern (2026): Nationale Wirtschaftsschutzstrategie. Kabinettsbeschluss vom 18.03.2026. Verfügbar unter: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/sicherheit/BMI26004-nationale-wirtschaftsschutzstrategie.pdf?__blob=publicationFile&v=5 (Zugriff: 04.11.2026).

BSI - Bundesamt für Sicherheit in der Informationstechnik (2023): BSI-Standard 200-4: Business Continuity Management. Version 1.0, veröffentlicht am 14.06.2023. Bonn: BSI; Buchausgabe: Köln: Reguvis Fachmedien. Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_4.pdf?__blob=publicationFile&v=8 (Zugriff: 04.11.2026).

BSI - Bundesamt für Sicherheit in der Informationstechnik (2024): KI und gegenwärtige Cyberbedrohungen. Threat-Intelligence-Blogeintrag vom 11.09.2024. Verfügbar unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-

Sicherheitslage/Analysen-und-Prognosen/Threat-Intelligence/Blogeintraege/KI_gegenwaertige-Cyberbedrohungen.html (Zugriff: 26.10.2026).

BSI - Bundesamt für Sicherheit in der Informationstechnik (2025): Die Lage der IT-Sicherheit in Deutschland 2025. Verfügbar unter: https://medien.bsi.bund.de/lagebericht/de/ (Zugriff: 17.06.2026).

BSI - Bundesamt für Sicherheit in der Informationstechnik (2026a): KI-Modelle revolutionieren den Umgang mit Sicherheitslücken. 08.05.2026. Verfügbar unter: https://www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Blog/KI-Modelle_neue_Zeitrechnung_260508.html (Zugriff: 17.06.2026).

BSI - Bundesamt für Sicherheit in der Informationstechnik (2026b): NIS-2 in Zahlen. Verfügbar unter: https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/NIS-2-in-Zahlen/nis-2-in-zahlen.html (Zugriff: 26.10.2026).

BSI - Bundesamt für Sicherheit in der Informationstechnik (2026c): PHP: Kritische Schwachstellen bedrohen Webanwendungen weltweit. Cybersicherheitswarnung BITS-H 2026-297981-1032, Version 1.0, 21.10.2026. Verfügbar unter: https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Cybersicherheitswarnungen/DE/2026/2026-297981-1032.pdf?__blob=publicationFile&v=2 (Zugriff: 23.10.2026).

Bundeswehr (2023): Operationsplan Deutschland: Wie verteidigen wir unser Land? 14.11.2023. Verfügbar unter: https://www.bundeswehr.de/de/selbstverstaendnis/geschichte-bundeswehr/territoriales-fuehrungskommando-der-bundeswehr/operationsplan-deutschland-5703688 (Zugriff: 16.06.2026).

Bundeswehr (2024): Stresstest für den Operationsplan Deutschland. 26.11.2024. Verfügbar unter: https://www.bundeswehr.de/de/organisation/operatives-fuehrungskommando-der-bundeswehr/stresstest-operationsplan-deutschland-5863010 (Zugriff: 16.06.2026).

Bundeswehr / Operatives Führungskommando der Bundeswehr (2025): Gesamtverteidigung: Alles über den Operationsplan Deutschland. Verfügbar unter: https://www.bundeswehr.de/de/organisation/operatives-fuehrungskommando-der-bundeswehr/auftrag-und-aufgaben/operationsplan-deutschland (Zugriff: 16.06.2026).

Crosignani, Matteo; Han, Lina; Macchiavelli, Marco; Silva, André F. (2024): Securing Technological Leadership? The Cost of Export Controls on Firms (ursprünglicher Titel: Geopolitical Risk and Decoupling: Evidence from U.S. Export Controls). Federal Reserve Bank of New York Staff Reports, Nr. 1096, April 2024, revidiert Februar 2025. DOI: 10.59576/sr.1096. Verfügbar unter: https://www.newyorkfed.org/research/staff_reports/sr1096 (Zugriff: 30.09.2026).

Destatis - Statistisches Bundesamt (2026): China im Jahr 2025 wieder wichtigster Handelspartner Deutschlands. Pressemitteilung Nr. 056 vom 20.02.2026. Verfügbar unter: https://www.destatis.de/DE/Presse/Pressemitteilungen/2026/02/PD26_056_51.html (Zugriff: 29.09.2026).

Die Bundesregierung (2023): Nationale Sicherheitsstrategie - Integrierte Sicherheit für Deutschland. 14.06.2023. Verfügbar unter: https://www.bundesregierung.de/breg-de/aktuelles/nationale-sicherheitsstrategie-2195890 (Zugriff: 16.06.2026).

Die Bundesregierung (2025): Deutschland bekommt einen Nationalen Sicherheitsrat. Kabinettsbeschluss vom 27.08.2025. Verfügbar unter: https://www.bundesregierung.de/breg-de/aktuelles/kabinett-sicherheitsrat-2381492 (Zugriff: 26.10.2026).

Die Bundesregierung (2026a): Maßnahmen für mehr Cybersicherheit. Verfügbar unter: https://www.bundesregierung.de/breg-de/aktuelles/massnahmen-bundesregierung-cybersicherheit-2432652 (Zugriff: 16.06.2026).

Die Bundesregierung (2026b): Schutz kritischer Infrastruktur gestärkt (KRITIS-Dachgesetz). 17.03.2026. Verfügbar unter: https://www.bundesregierung.de/breg-de/aktuelles/kritis-dachgesetz-2383682 (Zugriff: 16.06.2026).

Die Bundesregierung (2026c): Fragen und Antworten zur EU-US-Zolleinigung. Verfügbar unter: https://www.bundesregierung.de/breg-de/service/fragen-und-anworten/faq-eu-us-zolleinigung-2340924 (Zugriff: 20.10.2026).

Die Bundesregierung (2026d): EU-MERCOSUR-Abkommen vorläufig in Kraft. Verfügbar unter: https://www.bundesregierung.de/breg-de/aktuelles/mercosur-auf-dem-weg-2398594 (Zugriff: 23.10.2026).

EIA - U.S. Energy Information Administration (2025): Amid regional conflict, the Strait of Hormuz remains critical oil chokepoint. Today in Energy, Juni 2025. Verfügbar unter: https://www.eia.gov/todayinenergy/detail.php?id=65504 (Zugriff: 30.09.2026).

Eigner, Leo (2025): Chinas Vision für Wissenschaft und Technologie. CSS Analysen zur Sicherheitspolitik, Nr. 364, Juli 2025. Zürich: Center for Security Studies, ETH Zürich. Verfügbar unter: https://ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse364-DE.pdf (Zugriff: 17.06.2026).

Euronews (2026a): Was die Sperrung der Straße von Hormus für Ölpreise, Gas und Europa bedeutet. 01.04.2026. Verfügbar unter: https://de.euronews.com/my-europe/2026/04/01/strasse-von-hormus-oelpreise-europa (Zugriff: 30.09.2026).

Europäische Kommission (2023a): Commission Recommendation on critical technology areas for the EU's economic security for further risk assessment with Member States. C(2023) 6689 final. Verfügbar unter: https://defence-industry-space.ec.europa.eu/system/files/2023-10/C_2023_6689_1_EN_ACT_part1_v8.pdf (Zugriff: 17.06.2026).

Europäische Kommission (2023b): Europäische Strategie für wirtschaftliche Sicherheit. 20.06.2023. Verfügbar unter: https://ec.europa.eu/commission/presscorner/detail/de/ip_23_3358 (Zugriff: 16.06.2026).

Europäische Kommission (2024): Commission proposes new initiatives to strengthen economic security. Pressemitteilung IP/24/363, 24.01.2024. Verfügbar unter: https://ec.europa.eu/commission/presscorner/detail/en/ip_24_363; Druckfassung: https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_24_363/IP_24_363_EN.pdf (Zugriff: 04.11.2026).

Europäische Kommission (2025): Cloud Sovereignty Framework. Version 1.2.1, Oktober 2025. Verfügbar unter: https://commission.europa.eu/document/download/09579818-64a6-4dd5-9577-446ab6219113_en?filename=Cloud-Sovereignty-Framework.pdf (Zugriff: 17.06.2026).

Europäische Kommission (2026): Strengthening Europe's tech sovereignty. Meldung vom 03.06.2026. Verfügbar unter: https://commission.europa.eu/news-and-media/news/strengthening-europes-tech-sovereignty-2026-06-03_en (Zugriff: 26.10.2026).

Europäische Kommission; Hoher Vertreter der Union für Außen- und Sicherheitspolitik (2025): Gemeinsames Weißbuch zur europäischen Verteidigung - Bereitschaft 2030. JOIN(2025) 120 final,

19.03.2025. Verfügbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52025JC0120 (Zugriff: 05.11.2026).

Europäische Union (2022a): Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS-2-Richtlinie). Verfügbar unter: https://eur-lex.europa.eu/eli/dir/2022/2555/oj (Zugriff: 16.06.2026).

Europäische Union (2022b): Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die Resilienz kritischer Einrichtungen (CER-Richtlinie). Verfügbar unter: https://eur-lex.europa.eu/eli/dir/2022/2557/oj (Zugriff: 29.09.2026).

Europäische Union (2022c): Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor (DORA). Verfügbar unter: https://eur-lex.europa.eu/eli/reg/2022/2554/oj (Zugriff: 29.09.2026).

Europäische Union (2023): Verordnung (EU) 2023/1781 des Europäischen Parlaments und des Rates vom 13. September 2023 zur Schaffung eines Rahmens für Maßnahmen zur Stärkung des europäischen Halbleiter-Ökosystems (Chips-Gesetz). Verfügbar unter: https://eur-lex.europa.eu/eli/reg/2023/1781/oj (Zugriff: 29.09.2026).

Europäische Union (2024a): Verordnung (EU) 2024/2847 des Europäischen Parlaments und des Rates vom 23. Oktober 2024 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen (Cyber Resilience Act). Verfügbar unter: https://eur-lex.europa.eu/eli/reg/2024/2847/oj (Zugriff: 16.06.2026).

Europäische Union (2024b): Richtlinie (EU) 2024/1760 des Europäischen Parlaments und des Rates vom 13. Juni 2024 über die Sorgfaltspflichten von Unternehmen im Hinblick auf Nachhaltigkeit (CSDDD, „EU-Lieferkettenrichtlinie“). Verfügbar unter: https://eur-lex.europa.eu/eli/dir/2024/1760/oj (Zugriff: 29.09.2026).

Europäische Union (2024c): Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (KI-Verordnung). Verfügbar unter: https://eur-lex.europa.eu/eli/reg/2024/1689/oj (Zugriff: 19.10.2026).

Europäische Union (2026): Richtlinie (EU) 2026/470 des Europäischen Parlaments und des Rates zur Änderung u. a. der Richtlinie (EU) 2024/1760 (Omnibus I). Veröffentlicht im Amtsblatt am 26.02.2026, in Kraft seit 18.03.2026. Verfügbar unter: https://eur-lex.europa.eu/eli/dir/2026/470/oj (Zugriff: 30.09.2026).

Europäisches Parlament (2025): European Software and Cyber Dependencies. Studie im Auftrag des ITRE-Ausschusses, verfasst von Gineikyte-Kanclere, Vaida; Eggert, Militsa; Skiotyte, Goda (Visionary Analytics), PE 778.576, Dezember 2025. Verfügbar unter: https://www.europarl.europa.eu/RegData/etudes/STUD/2025/778576/ECTI_STU%282025%29778576_EN.pdf (Zugriff: 17.06.2026).

Eurostat (2026): Exports to US dropped by 30% year-on-year in Q1 2026. Eurostat News, 28.05.2026. Verfügbar unter: https://ec.europa.eu/eurostat/en/web/products-eurostat-news/w/ddn-20260528-1 (Zugriff: 02.11.2026).

Feyen, Erik; Utz, Robert; Zuccardi Huertas, Igor; Bogdan, Olena; Moon, Jisung (2020): Macro-Financial Aspects of Climate Change. World Bank Policy Research Working Paper 9109. Verfügbar unter: https://documents1.worldbank.org/curated/en/223161579009566321/pdf/Macro-Financial-Aspects-of-Climate-Change.pdf (Zugriff: 16.06.2026).

Hakobyan, Shushanik; Meleshchuk, Sergii; Zymek, Robert (2023): Divided We Fall: Differential Exposure to Geopolitical Fragmentation in Trade. IMF Working Paper Nr. 2023/270. Verfügbar unter: https://www.imf.org/en/publications/wp/issues/2023/12/22/divided-we-fall-differential-exposure-to-geopolitical-fragmentation-in-trade-542842 (Zugriff: 16.06.2026).

IEA - International Energy Agency (2022): World Energy Outlook 2022. Paris: IEA. Verfügbar unter: https://www.iea.org/reports/world-energy-outlook-2022 (Zugriff: 16.06.2026).

IEA - International Energy Agency (2024): Ukraine's Energy Security and the Coming Winter. Paris: IEA. Verfügbar unter: https://www.iea.org/reports/ukraines-energy-security-and-the-coming-winter (Zugriff: 30.09.2026).

IMF - International Monetary Fund (2023a): World Economic Outlook, October 2023: Navigating Global Divergences. Washington, D.C.: IMF. Verfügbar unter: https://www.imf.org/en/publications/weo/issues/2023/10/10/world-economic-outlook-october-2023 (Zugriff: 16.06.2026).

IMF - International Monetary Fund (2023b): Global Financial Stability Report, April 2023, Kapitel 3: Geopolitics and Financial Fragmentation: Implications for Macro-Financial Stability (Kapitelautoren: Catalán, Mario; Tsuruga, Tomohiro et al.). Washington, D.C.: IMF. Verfügbar unter: https://www.imf.org/en/publications/gfsr/issues/2023/04/11/global-financial-stability-report-april-2023 (Zugriff: 30.09.2026).

IMF - International Monetary Fund (2025): Regional Economic Outlook: Middle East and Central Asia, May 2025 - Charting a Path through the Haze. Washington, D.C.: IMF. ISBN 9798229007771. Verfügbar unter: https://www.bookstore.imf.org/books/regional-economic-outlook-middle-east-and-central-asia-may-2025-charting-a-path-through-the-haze (Zugriff: 04.11.2026).

IOM - International Organization for Migration (2026): Ukraine Internal Displacement Report. General Population Survey, Round 22, Januar 2026 (Datenstand Dezember 2025: 3.712.000 Binnenvertriebene). IOM Displacement Tracking Matrix. Verfügbar unter: https://dtm.iom.int/reports/ukraine-internal-displacement-report-general-population-survey-round-22-january-2026 (Zugriff: 04.11.2026).

IPCC (2022): Climate Change 2022: Impacts, Adaptation and Vulnerability. Contribution of Working Group II to the Sixth Assessment Report of the Intergovernmental Panel on Climate Change. Verfügbar unter: https://www.ipcc.ch/report/ar6/wg2/ (Zugriff: 16.06.2026).

ISO - International Organization for Standardization (2017): ISO 22316:2017 Security and resilience - Organizational resilience - Principles and attributes. Genf: ISO. Verfügbar unter: https://www.iso.org/standard/50053.html (Zugriff: 04.11.2026).

ISO - International Organization for Standardization (2019): ISO 22301:2019 Security and resilience - Business continuity management systems - Requirements, einschließlich Amendment 1:2024 (Climate action changes). Genf: ISO. Verfügbar unter: https://www.iso.org/standard/75106.html (Zugriff: 04.11.2026).

ISO - International Organization for Standardization (2025): ISO 22300:2025 Security and resilience - Vocabulary. Genf: ISO. Verfügbar unter: https://www.iso.org/standard/85749.html (Zugriff: 04.11.2026).

JRC - Joint Research Centre (2025): Open but Not Powerless: Towards a Common Understanding of EU Digital Sovereignty. Science for Policy Brief. Verfügbar unter: https://publications.jrc.ec.europa.eu/repository/bitstream/JRC144908/JRC144908_01.pdf (Zugriff: 17.06.2026).

Kleinhans, Jan-Peter; Jha, Sabhyata (2025): The chip landscape: Geographical distribution of wafer fabrication capacity. OECD Science, Technology and Industry Policy Papers, 30.11.2025. Paris: OECD Publishing. DOI: 10.1787/02dbd028-en. Verfügbar unter: https://www.oecd.org/en/publications/the-chip-landscape_02dbd028-en.html (Zugriff: 30.09.2026).

Kotzanikolaou, Panayiotis; Theoharidou, Marianthi; Gritzalis, Dimitris (2013): Cascading Effects of Common-Cause Failures in Critical Infrastructures. In: Critical Infrastructure Protection VII. IFIP AICT, Bd. 417, S. 171-182. DOI: 10.1007/978-3-642-45330-4_12. Verfügbar unter: https://inria.hal.science/hal-01456884/file/978-3-642-45330-4_12_Chapter.pdf (Zugriff: 16.06.2026).

Mearsheimer, John J. (2014): The Tragedy of Great Power Politics. Updated Edition (Erstauflage 2001). New York: W. W. Norton & Company. ISBN 978-0-393-34927-6.

Merz, Friedrich (2026): Rede von Bundeskanzler Friedrich Merz auf der Münchner Sicherheitskonferenz am 13. Februar 2026. Verfügbar unter: https://www.bundesregierung.de/breg-en/federal-government/speech-munich-security-conference-2407298 (Zugriff: 23.10.2026).

Mühlhofer, Evelyn; Bresch, David N.; Koks, Elco E. (2024): Infrastructure failure cascades quintuple risk of storm and flood-induced service disruptions across the globe. In: One Earth, 7(4), S. 714-729. Verfügbar unter: https://www.cell.com/one-earth/fulltext/S2590-3322%2824%2900139-8 (Zugriff: 16.06.2026).

Münchner Sicherheitskonferenz (2026): Munich Security Report 2026: Under Destruction. München, Februar 2026. Verfügbar unter: https://securityconference.org/en/publications/munich-security-report (Zugriff: 23.10.2026).

NATO (2024): Washington Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Washington, D.C., 10.07.2024. Press Release 2024 001. Verfügbar unter: https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/07/10/washington-summit-declaration (Zugriff: 04.11.2026).

NATO (2025): The Hague Summit Declaration. Erklärung der Staats- und Regierungschefs, Den Haag, 25.06.2025. Verfügbar unter: https://www.nato.int/cps/en/natohq/official_texts_236705.htm (Zugriff: 30.09.2026).

NCSC - National Cyber Security Centre (2025): Impact of AI on cyber threat from now to 2027. London: NCSC. Verfügbar unter: https://www.ncsc.gov.uk/sites/default/files/pdfs/publication/impact-ai-cyber-threat-now-2027.pdf (Zugriff: 17.06.2026).

ODNI/NCSC - Office of the Director of National Intelligence, National Counterintelligence and Security Center (2025): Safeguarding Western Tech Startups: Exploitation of International Pitch Competitions. 04.09.2025. Verfügbar unter: https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/NCSC_SOF_2025-09-04_SafeguardingWesternTechStartups.pdf (Zugriff: 17.06.2026).

OECD (2021): International Migration Outlook 2021. Paris: OECD Publishing. Verfügbar unter: https://www.oecd.org/en/publications/international-migration-outlook-2021_29f23e9d-en.html (Zugriff: 16.06.2026).

OECD (2023): Building Trust and Reinforcing Democracy - Action Plans. OECD Public Governance Committee at Ministerial Level, Dokument GOV/PGC/MIN(2022)4; beschlossen beim Ministertreffen in Luxemburg am 18.11.2022, veröffentlicht 2023. Verfügbar unter: https://one.oecd.org/document/gov/pgc/min%282022%294/en/pdf (Zugriff: 16.06.2026).

OECD (2024): Facts not Fakes: Tackling Disinformation, Strengthening Information Integrity. Paris: OECD Publishing. DOI: 10.1787/d909ff7a-en. Verfügbar unter: https://doi.org/10.1787/d909ff7a-en (Zugriff: 30.09.2026).

OECD (2026): Global value and supply chains; Resilient supply chains. OECD-Themenseiten. Verfügbar unter: https://www.oecd.org/en/topics/global-value-and-supply-chains.html und https://www.oecd.org/en/topics/resilient-supply-chains.html (Zugriff: 16.06.2026).

Rat der Europäischen Union (2022): Ein Strategischer Kompass für Sicherheit und Verteidigung. Angenommen am 21.03.2022, Pressemitteilung. Verfügbar unter: https://www.consilium.europa.eu/en/press/press-releases/2022/03/21/a-strategic-compass-for-a-stronger-eu-security-and-defence-in-the-next-decade/ (Zugriff: 26.10.2026).

Rat der Europäischen Union (2025): Instrument für Sicherheitsmaßnahmen für Europa (SAFE). In Kraft seit 29.05.2025. Verfügbar unter: https://www.consilium.europa.eu/de/policies/safe/ (Zugriff: 30.09.2026).

SIA/BCG - Semiconductor Industry Association; Boston Consulting Group (2021): Strengthening the Global Semiconductor Supply Chain in an Uncertain Era. April 2021. Verfügbar unter: https://www.semiconductors.org/strengthening-the-global-semiconductor-supply-chain-in-an-uncertain-era/ (Zugriff: 29.09.2026).

Staatlicher Statistikdienst der Ukraine (2026): Bruttoinlandsprodukt der Ukraine, Jahreswerte 2022 und 2023 nach regulärer Revision (reales BIP 2022: -28,8 %; 2023: +5,5 %). Kyjiw: Derschstat. Vorläufiger Wert 2023 (+5,3 %): Pressemitteilung „The preliminary estimate of the GDP for 2023 was made“, 28.03.2024, verfügbar unter: https://stat.gov.ua/en/news/preliminary-estimate-gdp-2023-was-made; Revision auf +5,5 % (2025) berichtet u. a. von Kyiv Post: https://www.kyivpost.com/post/50412 (Zugriff: 04.11.2026).

SVIKG (2025): Gesetz zur Errichtung eines Sondervermögens Infrastruktur und Klimaneutralität vom 30.09.2025 (BGBl. 2025 I Nr. 230). Verfügbar unter: https://www.gesetze-im-internet.de/svikg/BJNR0E60A0025.html (Zugriff: 30.09.2026).

TrendForce (2024): Foundry Capacity Market Share of Advanced Process to Decline in Taiwan, Korea until 2027, While US on the Rise. 14.05.2024. Verfügbar unter: https://www.trendforce.com/news/2024/05/14/insights-trendforce-foundry-capacity-market-share-of-advanced-process-to-decline-in-taiwan-korea-until-2027-while-us-on-the-rise/ (Zugriff: 30.09.2026).

U.S. Department of State (2025): Report to Congress on U.S.-Origin Technology that the Chinese Communist Party (CCP) is Using in the Military-Civil Fusion (MCF) Strategy of the PRC. 27.08.2025. Verfügbar unter: https://www.state.gov/wp-content/uploads/2025/08/Report-U.S.-Technology-in-the-Military-Civil-Fusion-Strategy-Revision-Accessible-8.27.2025.pdf (Zugriff: 17.06.2026).

UN DESA - United Nations, Department of Economic and Social Affairs (2024): World Population Prospects 2024. Verfügbar unter: https://population.un.org/wpp/ (Zugriff: 29.09.2026).

UNHCR (2026): Ukraine Refugee Situation. Operational Data Portal (dynamisch); Datenstand Ende Dezember 2025: rund 5,9 Mio. weltweit erfasste Geflüchtete aus der Ukraine. Verfügbar unter: https://data.unhcr.org/en/situations/ukraine (Zugriff: 04.11.2026).

Varley, Kevin (2022): Taiwan Tensions Raise Risks in One of Busiest Shipping Lanes. Bloomberg, 02.08.2022. Verfügbar unter: https://www.bloomberg.com/news/articles/2022-08-02/taiwan-tensions-raise-risks-in-one-of-busiest-shipping-lanes (Zugriff: 30.09.2026).

WEF - World Economic Forum (2026): Global Value Chains Outlook 2026: Orchestrating Corporate and National Agility. In Zusammenarbeit mit Kearney, 19.01.2026. Verfügbar unter:

https://www.weforum.org/publications/global-value-chains-outlook-2026-orchestrating-corporate-and-national-agility/ (Zugriff: 29.09.2026).

World Bank; Government of Ukraine; European Union; United Nations (2026): Ukraine - Fifth Rapid Damage and Needs Assessment (RDNA5): February 2022 - December 2025. Bericht, 23.02.2026; Datenstand 31.12.2025 (Wiederaufbau- und Erholungsbedarf 587,7 Mrd. US-Dollar für 2026-2035). Verfügbar unter: https://documents1.worldbank.org/curated/en/099022026094036395/pdf/P514499-22f93f3a-4278-42bc-b907-db9553d12069.pdf; begleitende Pressemitteilung: https://www.worldbank.org/en/news/press-release/2026/02/23/updated-ukraine-recovery-and-reconstruction-needs-assessment-released (Zugriff: 04.11.2026).

WTO - World Trade Organization (2023): World Trade Report 2023: Re-globalization for a secure, inclusive and sustainable future. Genf: WTO. Verfügbar unter: https://www.wto.org/english/res_e/publications_e/wtr23_e.htm (Zugriff: 30.09.2026).

Wübbeke, Jost; Meissner, Mirjam; Zenglein, Max J.; Ives, Jaqueline; Conrad, Björn (2016): Made in China 2025: The making of a high-tech superpower and consequences for industrial countries. MERICS Papers on China Nr. 2, Dezember 2016. Berlin: Mercator Institute for China Studies. Verfügbar unter: https://merics.org/en/report/made-china-2025 (Zugriff: 17.06.2026).

Zenglein, Max J.; Holzmann, Anna (2019): Evolving Made in China 2025: China's industrial policy in the quest for global tech leadership. MERICS Papers on China Nr. 8, Juli 2019. Berlin: Mercator Institute for China Studies. Verfügbar unter: https://merics.org/sites/default/files/2020-04/MPOC_8_MadeinChina_2025_final_3.pdf (Zugriff: 26.10.2026).

Abkürzungsverzeichnis

ASEAN	Association of Southeast Asian Nations
BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
BfV	Bundesamt für Verfassungsschutz
BMI	Bundesministerium des Innern
BRICS	Staatengruppe Brasilien, Russland, Indien, China, Südafrika (erweitert)
BSI	Bundesamt für Sicherheit in der Informationstechnik
DORA	Digital Operational Resilience Act (Verordnung (EU) 2022/2554)
ESG	Environmental, Social, Governance (Umwelt, Soziales, Unternehmensführung)
EU	Europäische Union
FDI	Foreign Direct Investment (ausländische Direktinvestitionen)
GNSS	Global Navigation Satellite System
IEA	International Energy Agency
IMF	International Monetary Fund
IOM	International Organization for Migration
IP	Intellectual Property (geistiges Eigentum)
IT	Informationstechnik
JRC	Joint Research Centre der EU-Kommission
KI	Künstliche Intelligenz
KMU	Kleine und mittlere Unternehmen
KPCh	Kommunistische Partei Chinas
KRITIS	Kritische Infrastrukturen
LNG	Liquefied Natural Gas
MBCO	Minimum Business Continuity Objective (Mindestbetriebsfähigkeit nach ISO 22301)
NATO	North Atlantic Treaty Organization
NCSC (UK)	National Cyber Security Centre
NCSC (USA)	National Counterintelligence and Security Center

NIS-2	Richtlinie (EU) 2022/2555 zur Netz- und Informationssicherheit
nm	Nanometer (Maß für die Strukturgröße von Halbleitern)
ODNI	Office of the Director of National Intelligence
OECD	Organisation for Economic Co-operation and Development
OPLAN DEU	Operationsplan Deutschland
SAFE	Security Action for Europe (EU-Instrument für Verteidigungsbeschaffung)
SVIKG	Gesetz zur Errichtung eines Sondervermögens Infrastruktur und Klimaneutralität
THI	Technische Hochschule Ingolstadt
UNHCR	Hoher Flüchtlingskommissar der Vereinten Nationen
VC	Venture Capital
VSW	Verband für Sicherheit in der Wirtschaft, Bundesverband e.V. (VSW Bundesverband)
WEF	World Economic Forum
WTO	World Trade Organization

Ihre Meinung ist uns wichtig!

FAQ & Feedback zum Whitepaper

Haben Sie Fragen oder Anregungen?

Nutzen Sie unseren Feedback-Fragebogen oder kontaktieren Sie direkt unseren ThinkTank. Ihre Impulse sind wertvoll und können entscheidend dazu beitragen, zukünftige Veröffentlichungen noch praxisnäher und relevanter zu gestalten.

Besuchen Sie unsere FAQs, um Antworten auf häufige Fragen zu erhalten und sich tiefer in das Thema einzuarbeiten.

👉 **Kontakt & Feedback**

Whitepaper 02 - ThinkTank Corporate Resilience, Oktober 2026