THINKTANK
CORPORATE RESILIENCE
OPERATIVER LEITFADEN 01

zum strategischen Whitepaper 02 „Geopolitischer Wandel, KI und unternehmerische Optionen“

- Resilienz in der Praxis -

VSW
Bundesverband

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

Oktober 2026

Vorwort

Der operative Leitfaden 01 zum strategischen Whitepaper 02 **liefert Werkzeuge für Sicherheits-, Risiko- und Krisenmanagement, Business Continuity, Einkauf und Compliance sowie Resilience Management** in Form verschiedener Arbeitsmodule**.**

Insgesamt neun Arbeitsmodule mit Checklisten, Analyseinstrumenten und dem Szenario-Stresstest 2027-2030 wurden aus dem strategischen Whitepaper 02 „Geopolitischer Wandel, KI und unternehmerische Optionen“ abgeleitet. Im strategischen Whitepaper 02 ist die strategische Einordnung für Geschäftsführung, Vorstand und Aufsichtsrat enthalten.

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

1 WIE SIE DIESEN LEITFADEN NUTZEN 5

2 KONKRETE WIRKUNGEN AUF UNTERNEHMEN 7

2.1 MÄRKTE 7
2.2 LIEFERKETTEN 8
2.3 KAPITAL 8
2.4 TALENTE 9
2.5 INNOVATION 10
2.6 ROHSTOFF- UND ENERGIEVERSORGUNG 10
2.7 STANDORTE UND PRODUKTION 11
2.8 MITARBEITENDE, FÜHRUNGSKRÄFTE UND SCHLÜSSELPERSONEN 12
2.9 KÜNSTLICHE INTELLIGENZ 13

3 RISIKOMULTIPLIKATOREN: WENN SICH KRISEN GEGENSEITIG BEFEUERN 14

3.1 MÖGLICHE RISIKOMULTIPLIKATOREN 14
3.2 PERSPEKTIVWECHSEL: VON EINZELRISIKEN ZU VERNETZTEN KASKADEN 16
3.3 DER SECHS-PUNKTE-SCHUTZANSATZ 16

4 RESILIENZARCHITEKTUR: FÄHIGKEITEN-REIFEGRADCHECK 17

4.1 ACHT FÄHIGKEITEN EINER MODERNEN RESILIENZARCHITEKTUR 18
4.2 KÜNSTLICHE INTELLIGENZ ALS WERKZEUG IM RESILIENZMANAGEMENT 19
4.3 VON DER ANALYSE ZUR UMSETZUNG: ERSTE SCHRITTE 21

5 KRITISCHE ABHÄNGIGKEITEN: DEPENDENCY-MAPPING 22

6 SZENARIO-STRESSTEST-TOOLKIT 2027-2030 25

6.1 SZENARIO 1 - GROß ANGELEGTER KONFLIKT IN EUROPA 26
6.2 SZENARIO 2 - ESKALATION IN DER TAIWANSTRAßE ALS GEOÖKONOMISCHER SYSTEMSCHOCK 28
6.3 SZENARIO 3 - US-CHINA TECHNOLOGISCHE ENTKOPPLUNG 31
6.4 SZENARIO 4 - STRATEGISCHE FRAGMENTIERUNG DER TRANSATLANTISCHEN PARTNERSCHAFT 33
6.5 GLEICHZEITIGKEIT UND KOMBINATION DER SZENARIEN 35

7 SCHNITTSTELLE STAAT-WIRTSCHAFT 37

7.1 WAS DER STAAT ANBIETET 37
7.2 WAS UNTERNEHMEN DAVON HALTEN - UND WO DIE GAPS LIEGEN 37
7.3 CHECKLISTE: ANFORDERUNGEN DER WIRTSCHAFT AN DEN STAAT 38
7.4 DIE GEMEINSAME VISION 39

8 REGULATORIK- UND UMSETZUNGSFAHRPLAN 40

8.1 DER OPERATIONSPLAN DEUTSCHLAND (OPLAN DEU) 40
8.2 REGULATORISCHER DRUCK VERSUS UNTERNEHMERISCHER HANDLUNGSSPIELRAUM 41
8.3 NEUN LÜCKEN IM SYSTEM - SELBSTDIAGNOSE 42
8.4 IMPLIKATIONEN FÜR UNTERNEHMEN - KONKRETE HANDLUNGSANSÄTZE 43

9 MARKTEINTRITT & DIVERSIFIZIERUNG 44

9.1 EU-BINNENMARKT 44
9.2 INDIEN 44
9.3 SÜDOSTASIEN (ASEAN) 44
9.4 GOLFREGION 44
9.5 BRASILIEN UND MERCOSUR 45
9.6 CHECKLISTE: STRUKTURELLE VORAUSSETZUNGEN FÜR DEN MARKTEINTRITT 45

10 CHANCENFELDER IM DETAIL 46

10.1 VERTEIDIGUNG & DUAL-USE 46
10.2 INFRASTRUKTUR & ENERGIE 46
10.3 DIGITALE SOUVERÄNITÄT 46
10.4 REGIONALE WERTSCHÖPFUNG 47

LITERATURVERZEICHNIS 48

ABKÜRZUNGSVERZEICHNIS 54

1 Wie Sie diesen Leitfaden nutzen

Dieser Operative Leitfaden 01 ist das praxisorientierte Begleitdokument zum Strategischen Whitepaper 02 „Geopolitischer Wandel, KI und unternehmerische Optionen“. Während das strategische Whitepaper die zentralen Fakten und Befunde für Geschäftsführung, Vorstand und Aufsichtsrat bündelt, übersetzt dieser Leitfaden dieselben Inhalte in konkrete Arbeitsinstrumente für die operative Praxis. Einfach ausgedrückt: Kapitel 2 zeigt, wo geopolitischer Wandel ansetzt; Kapitel 3 erklärt, warum sich diese Ansatzpunkte gegenseitig verstärken; Kapitel 4 und 5 beschreiben, welche Fähigkeiten und welches Wissen ein Unternehmen braucht, um dem zu begegnen; Kapitel 6 prüft diese Fähigkeiten im Ernstfall; Kapitel 7 und 8 verorten das Ganze im Verhältnis zu Staat und Regulierung; Kapitel 9 und 10 drehen die Perspektive um und zeigen, dass dieselbe Verwundbarkeitsanalyse zugleich eine Landkarte unternehmerischer Chancen ist.

Zielgruppe

Chief Security Officers, Unternehmenssicherheit und Corporate Resilience · Chief Information Security Officers und Informationssicherheit · Risikomanagement und Enterprise Risk Management · Business Continuity und Krisenmanagement · Einkauf und Lieferkettenmanagement · Compliance, Legal und Regulatory Affairs · Strategie und Business Development.

Aufbau

Der Leitfaden gliedert sich in neun Module. Kapitel 1 dient als Einführung; die Module 1 bis 9 folgen in den Kapiteln 2 bis 10.

Die Module folgen einer Arbeitslogik (Wirkungen verstehen, Risiken analysieren, Fähigkeiten aufbauen, Abhängigkeiten kartieren, Szenarien testen, Schnittstellen zu Staat und Regulierung nutzen, Chancen erschließen) und daher nicht der Kapitelfolge des Strategischen Whitepapers 02. Jedes Modul kann eigenständig genutzt werden - etwa als Grundlage für einen Workshop, eine Risikositzung oder ein Tabletop-Format. Wo sinnvoll,

verweisen Querverweise auf die entsprechende Kurzfassung im Strategischen Whitepaper 02.

Modul	Kerninhalt
1 - Funktionsspezifische Maßnahmen	Märkte, Lieferketten, Kapital, Talente, Innovation, Rohstoff- und Energieversorgung, Standorte und Produktion, Mitarbeitende und Führungskräfte, Künstliche Intelligenz
2 - Risikomultiplikatoren	Zehn mögliche Verstärkerfaktoren, Selbstcheck, Sechs-Punkte-Schutzansatz
3 - Resilienzarchitektur	Acht-Fähigkeiten-Reifegradcheck, Bewertungsskala, KI als Werkzeug, erste Schritte
4 - Kritische Abhängigkeiten	Dependency-Mapping in neun Feldern
5 - Szenario-Stresstest 2027-2030	Vier Szenarien mit je drei Eskalationsstufen, Arbeitsblatt, Kombinationsprüfung
6 - Schnittstelle Staat-Wirtschaft	Wirtschaftsschutzstrategie, Elf-Punkte-Checkliste, interne Vorbereitung
7 - Regulatorik- und Umsetzungsfahrplan	OPLAN DEU, EU-Regulierung, Neun-Lücken-Diagnose
8 - Markteintritt & Diversifizierung	Fünf strategische Märkte, Checkliste
9 - Chancenfelder im Detail	Verteidigung, Infrastruktur, digitale Souveränität, regionale Wertschöpfung

Die Inhalte bauen auf dem Whitepaper 02 auf und vertiefen es; die Quellen sind im Literaturverzeichnis ausgewiesen.

2 Konkrete Wirkungen auf Unternehmen

Was Unternehmen konkret tun können - je Dimension

Geopolitische Entwicklungen wirken auf zentrale unternehmerische Dimensionen: Märkte, Lieferketten, Kapital, Talente, Innovation, Rohstoff- und Energieversorgung sowie Standorte und Produktion; ergänzend werden Mitarbeitende als zentrales Schutzgut sowie exponierte Führungskräfte und Schlüsselpersonen (Modul 1, Kapitel 2, Abschnitt 2.8) und Künstliche Intelligenz als Querschnittsthema (Modul 1, Kapitel 2, Abschnitt 2.9) betrachtet. Für jede Dimension gilt: Zunächst verstehen, warum die Wirkung entsteht, dann gezielt gegensteuern (vgl. Strategisches Whitepaper 02, Kapitel 2). Die Praxisbeispiele je Dimension sind illustrativ und kein verbindlicher Maßnahmenkatalog.

2.1 Märkte

Warum spürbar?

Handelskonflikte, Sanktionen und protektionistische Maßnahmen können den Zugang zu wichtigen Absatzmärkten erschweren oder ganz blockieren. Die US-Zollpolitik zeigt dies konkret: Nach der politischen Grundsatzeinigung im August 2025 gilt für die meisten EU-Exporte in die USA ein vereinbarter Höchstzollsatz von 15 %; die EU-seitigen Regelungen zur Umsetzung traten am 01.07.2026 in Kraft. Zeitgleich lagen die EU-Warenausfuhren in die USA im ersten Quartal 2026 rund 30,4 % unter dem Vorjahreswert (Die Bundesregierung 2026c; Eurostat 2026). Politische Spannungen können zudem zu einem Rückgang der Konsum- und Investitionsbereitschaft in betroffenen Regionen führen. Unternehmen sehen sich mit der Notwendigkeit konfrontiert, ihre Marktstrategien anzupassen und möglicherweise neue Märkte zu erschließen oder bestehende zu diversifizieren (Hakobyan, Meleshchuk, Zymek 2023).

Was Unternehmen tun können

- **Marktdiversifizierung („De-risking“):** nicht alle Eier in einen Korb legen - die Erschließung neuer Absatzmärkte reduziert die Abhängigkeit von einzelnen Regionen.
- **Lokalisierung:** Produktion und Wertschöpfung näher an den Endkunden verlagern, um Handelsbarrieren zu umgehen und lokale Präferenzen besser zu bedienen.
- **Szenarioplanung:** frühzeitige Analyse potenzieller politischer Chancen und Risiken sowie Entwicklung von Notfallplänen für verschiedene Marktszenarien.

Praxisbeispiel (illustrativ): Ein Hersteller erzielt 40 % seines Umsatzes in einem einzigen außereuropäischen Markt. Er legt fest, dass kein Einzelmarkt mittelfristig über 25 % wachsen soll, und baut zwei Ersatzmärkte mit lokalen Vertriebspartnern auf.

2.2 Lieferketten

Warum spürbar?

Geopolitische Spannungen können zu Unterbrechungen in globalen Lieferketten führen, sei es durch Handelsbeschränkungen, Infrastrukturschäden oder politische Instabilität. Die COVID-19-Pandemie und der Krieg in der Ukraine haben die Anfälligkeit globaler Lieferketten drastisch vor Augen geführt (WTO 2023). Aktuell zeigen insbesondere die Konflikte im Nahen Osten die Verwundbarkeit globaler Transport- und Liefernetzwerke. Seit Beginn der militärischen Eskalation am 28.02.2026 kam es wiederholt zu massiven Einschränkungen des Schiffsverkehrs durch die Straße von Hormus, durch die normalerweise mehr als ein Viertel des seegestützten Ölhandels und rund ein Fünftel des weltweiten LNG-Handels (EIA 2025) transportiert werden. Die daraus entstandenen Risiken für Energieversorgung, Transport und globale Lieferketten wirken über die jeweilige militärische Eskalationsphase hinaus und führten 2026 zu erheblichen Verwerfungen auf den Energie- und Rohstoffmärkten. Höhere Energiepreise wirkten sich unmittelbar auf Produktions-, Transport- und Logistikkosten weltweit aus (Euronews 2026a).

Was Unternehmen tun können

- **Vollständiges Lagebild sicherstellen:** Relevante Sachverhalte monitoren und Szenarioplanung betreiben, die sich bspw. mit den Auswirkungen von Hafenschließungen, Luftraumsperren, Sanktionen oder Versorgungsengpässen auseinandersetzt und Lösungsansätze sowie Alternativen für diese Beeinträchtigungen sicherstellt.
- **Resilienz aufbauen:** Aufbau redundanter Lieferantenbeziehungen und Lagerhaltung an strategischen Standorten.
- **Regionalisierung und Nearshoring:** Teile der Produktion oder Beschaffung in geografisch näher gelegene oder politisch stabilere Regionen verlagern.
- **Transparenz schaffen:** Einsatz von Technologien zur besseren Überwachung und Rückverfolgbarkeit von Lieferketten, um Risiken frühzeitig zu erkennen.

Praxisbeispiel (illustrativ): Ein Elektronikfertiger findet in seiner Stückliste zwölf Bauteile mit nur einer Bezugsquelle in Ostasien. Für die fünf umsatzkritischsten qualifiziert er eine Zweitquelle, für die übrigen erhöht er den Sicherheitsbestand auf drei Monate.

2.3 Kapital

Warum spürbar?

Geopolitische Unsicherheiten können zu Kapitalflucht, Währungsschwankungen und einem Anstieg der Finanzierungskosten führen. Investitionsentscheidungen werden

vorsichtiger getroffen, und der Zugang zu internationalen Kapitalmärkten kann sich erschweren, insbesondere in Ländern, die als politisch instabil gelten (IMF 2023b).

Was Unternehmen tun können

- **Risikomanagement:** Absicherung gegen Währungsschwankungen und politische Risiken durch entsprechende Finanzinstrumente.
- **Eigenkapital stärken:** eine solide Eigenkapitalbasis macht Unternehmen widerstandsfähiger gegenüber externen Schocks.
- **Diversifizierung der Finanzierungsquellen:** nicht nur auf Bankkredite setzen, sondern auch andere Finanzierungsformen wie Anleihen oder Private Equity in Betracht ziehen.

Praxisbeispiel (illustrativ): Ein Exporteur sichert Fremdwährungserlöse für zwölf Monate ab, versichert politische Risiken in einem Hochrisikomarkt und erweitert seine Kreditlinie, solange die Konditionen noch günstig sind.

2.4 Talente

Warum spürbar?

Geopolitische Konflikte und Spannungen können die internationale Mobilität von Fachkräften einschränken oder beeinflussen. Visa-Beschränkungen, Reiseverbote oder eine allgemeine Unsicherheit können es erschweren, Talente global zu rekrutieren oder Mitarbeitende ins Ausland zu entsenden. Darüber hinaus können regionale Konflikte einen Fluchtgrund für Mitarbeitende darstellen, wodurch Know-how für das betroffene Unternehmen verloren gehen kann. Zudem kann die Stimmung gegenüber bestimmten Nationalitäten die Integration internationaler Talente beeinflussen (OECD 2021).

Was Unternehmen tun können

- **Lokale Talententwicklung:** stärkere Investition in Ausbildung und Entwicklung von Talenten in den jeweiligen Regionen.
- **Attraktive Arbeitsbedingungen:** Schaffung eines inklusiven und attraktiven Arbeitsumfelds, um Talente unabhängig von ihrer Herkunft anzuziehen und zu halten.
- **Wertebasierte Unternehmenskultur:** Gemeinsame Werte, Fairness und gelebtes Sicherheitsbewusstsein stärken die Bindung von Fachkräften und erhöhen die Widerstandsfähigkeit gegenüber Abwerbung und Einflussnahme von außen.
- **Digitale Zusammenarbeit:** Nutzung digitaler Tools, um internationale Teams auch ohne physische Präsenz effektiv zusammenarbeiten zu lassen.

Praxisbeispiel (illustrativ): Ein Softwarehaus mit Entwicklungszentrum in einer Krisenregion dokumentiert kritisches Wissen, bildet Tandems mit Teams in Deutschland und hält einen Relocation-Plan für Mitarbeitende und ihre Familien bereit.

2.5 Innovation

Warum spürbar?

Geopolitische Rivalitäten können den freien Austausch von Wissen und Technologien behindern. Exportkontrollen für bestimmte Technologien oder Beschränkungen bei der Zusammenarbeit in Forschung und Entwicklung können den Innovationsprozess verlangsamen oder in bestimmte Richtungen lenken (Europäische Kommission 2024).

Was Unternehmen tun können

- **Resiliente F&E-Strategien:** Diversifizierung von Forschungsstandorten und -partnern, um Abhängigkeiten zu reduzieren.
- **Investition in eigene Forschung:** stärkere interne Forschungs- und Entwicklungskapazitäten aufbauen, um weniger von externen Technologiequellen abhängig zu sein.
- **Open Innovation mit vertrauenswürdigen Partnern:** gezielte Zusammenarbeit mit Partnern aus politisch stabilen und verlässlichen Regionen.

Praxisbeispiel (illustrativ): Ein Technologieunternehmen prüft vor jeder Forschungskooperation und jedem Lizenzgeschäft Exportkontroll- und Dual-Use-Fragen sowie den Hintergrund des Partners und regelt den Zugriff auf Schlüsselwissen.

2.6 Rohstoff- und Energieversorgung

Warum spürbar?

Rohstoffe und Energie entwickeln sich zunehmend zu geopolitischen Machtinstrumenten. Exportbeschränkungen, Handelskonflikte, Sanktionen oder Konflikte entlang wichtiger Transportwege können die Verfügbarkeit kritischer Rohstoffe und Energieträger erheblich beeinträchtigen. Gleichzeitig führen Versorgungsengpässe und steigende Energiepreise zu höheren Produktions-, Logistik- und Betriebskosten. Unternehmen mit einer hohen Abhängigkeit von einzelnen Lieferanten, Regionen oder Energieträgern sind dabei besonders anfällig für geopolitische Schocks (WEF 2026; IEA 2022).

Was Unternehmen tun können

- **Beschaffungsquellen diversifizieren:** Abhängigkeiten von einzelnen Lieferanten, Ländern oder Rohstoffquellen identifizieren und reduzieren.
- **Versorgungssicherheit erhöhen:** Lieferverträge, strategische Reserven und alternative Bezugsquellen aufbauen.
- **Energieeffizienz steigern:** Investitionen in Energieeffizienzmaßnahmen, Eigenversorgung und alternative Energieträger zur Reduzierung externer Abhängigkeiten.

Praxisbeispiel (illustrativ): Ein energieintensiver Betrieb sichert einen Teil seines Strombedarfs über langfristige Lieferverträge und eigene Photovoltaik und legt für einen kritischen Rohstoff einen Bestand für zwei Monate an.

2.7 Standorte und Produktion

Warum spürbar?

Geopolitische Entwicklungen beeinflussen zunehmend die Attraktivität und Betriebsfähigkeit von Unternehmensstandorten. Neben klassischen Faktoren wie Kosten, Steuern oder Infrastruktur gewinnen politische Stabilität, Sanktions- und Regulierungsrisiken, die Verfügbarkeit von Energie und Rohstoffen sowie die Sicherheit von Lieferketten an Bedeutung. Hinzu kommt der Zugang zu Rechenzentren und KI-Rechenkapazität, der für datenintensive Entwicklung und Produktion zunehmend zum Standortfaktor wird. Konflikte, Handelsbeschränkungen oder geopolitische Spannungen können dazu führen, dass Standorte ihre wirtschaftlichen Vorteile verlieren oder Geschäftsaktivitäten erheblich eingeschränkt werden (WEF 2026).

Was Unternehmen tun können

- **Standorte geopolitisch bewerten:** Standortentscheidungen nicht nur nach Wirtschaftlichkeit, sondern auch nach Resilienz- und Risikokriterien treffen. Politische Stabilität, Sanktionsrisiken, Ressourcenverfügbarkeit und Lieferkettenabhängigkeiten in Investitions- und Standortentscheidungen einbeziehen.
- **Standortportfolio diversifizieren:** Kritische Funktionen, Produktionskapazitäten und Datenverarbeitung auf mehrere Regionen verteilen. Auswirkungen geopolitischer Krisen auf Produktions- und Betriebsstandorte regelmäßig bewerten und Notfallmaßnahmen vorbereiten unter Berücksichtigung länderspezifischer Einschränkungen (bspw. Verhältnis: China/Taiwan, USA/Kuba).
- **Redundanzen schaffen:** Alternative Produktions- und Ausweichstandorte für kritische Geschäftsprozesse vorhalten.

Praxisbeispiel (illustrativ): Ein Unternehmen mit Werk in einer Spannungsregion definiert Schwellenwerte, ab denen Produktion verlagert wird, hält Werkzeuge und Fertigungsdaten an einem zweiten Standort vor und übt die Umstellung einmal jährlich.

2.8 Mitarbeitende, Führungskräfte und Schlüsselpersonen

Warum spürbar?

Mitarbeitende sind das zentrale Schutzgut jedes Unternehmens: Fürsorgepflicht, Reise- und Standortsicherheit, Erreichbarkeits- und Evakuierungskonzepte sowie der Schutz vor Ausspähung und Anbahnung betreffen die gesamte Belegschaft (vgl. Strategisches Whitepaper 02, Kapitel 2.3); die konkreten Maßnahmen stehen unten. Bei der Bewertung kritischer Assets sind exponierte Führungskräfte und Schlüsselpersonen einzubeziehen. Der Schutzbedarf ist nicht aus der Hierarchie, sondern aus Funktion, Sichtbarkeit, Bedrohungslage und möglichen Auswirkungen auf die Handlungsfähigkeit des Unternehmens abzuleiten. Hierzu sind digitale und physische Expositionsfaktoren gemeinsam zu erfassen, mögliche Eskalationspfade zu bewerten und angemessene organisatorische, digitale, kommunikative sowie erforderlichenfalls physische Maßnahmen festzulegen. Dabei sind auch digitale Spuren und öffentlich verfügbare Informationen von Familienangehörigen (z. B. Partnern oder Kindern) zu berücksichtigen, sofern hierdurch Rückschlüsse auf Aufenthaltsorte, Routinen oder Bewegungsprofile von Schutzpersonen möglich werden. Corporate Security, Cybersecurity, Communications, Personalorganisation, Travel Security, Datenschutz und Personenschutz sind lagegerecht einzubinden (vgl. BfV 2025; BSI 2025).

Was Unternehmen tun können

- **Exponierung erfassen:** Als ersten Schritt eine Sichtbarkeitsanalyse durchführen, um den Ist-Stand zu erfassen: Welche digitalen und physischen Informationen erhöhen Sichtbarkeit oder Vorhersehbarkeit? Sind über den digitalen Footprint von Familienangehörigen Rückschlüsse auf Aufenthaltsorte, Gewohnheiten oder Bewegungsprofile der Schutzperson möglich?
- **Risiko bewerten:** Welche Funktion, Lage, Region, Reise, Veranstaltung oder Unternehmensaktivität erhöht den Schutzbedarf?
- **Eskalation prüfen:** Können Informationen für Phishing, Ausforschung, Annäherung, Einschüchterung oder physische Gefährdung genutzt werden?
- **Maßnahmen festlegen:** Welche abgestuften Maßnahmen und Schnittstellen sind angemessen, und wann ist eine Neubewertung erforderlich?
- **Belegschaft absichern:** Erreichbarkeit, Reise- und Standortsicherheit sowie Evakuierungs- und Rückholkonzepte für Mitarbeitende in Risikoregionen festlegen und beüben.
- **Deepfake-Risiken adressieren:** Freigaben und Zahlungsanweisungen nie allein auf Basis von Anruf, Sprachnachricht oder Video erteilen; Rückruf über bekannte Kontaktwege und Vier-Augen-Prinzip festlegen.

Anwendungshinweis:

Die Bewertung erfolgt einzelfallbezogen; pauschale Gefährdungsannahmen sowie operative Schutzstufen oder taktische Maßnahmen sind nicht Gegenstand des Leitfadens.

2.9 Künstliche Intelligenz

Warum spürbar?

KI verändert die Bedrohungslage unmittelbar: Angreifer nutzen KI, um Schwachstellen schneller zu finden und auszunutzen, Phishing und Social Engineering in jeder Sprache zu personalisieren und mit Stimm- und Videofälschungen (Deepfakes) Führungskräfte oder Geschäftspartner zu imitieren (BSI 2026a; BSI 2024; NCSC 2025). Zugleich entstehen neue Abhängigkeiten von wenigen, überwiegend außereuropäischen Anbietern von KI-Modellen, Rechenzentren und KI-Chips (vgl. Strategisches Whitepaper 02, Kapitel 3). Die unkontrollierte Nutzung externer KI-Dienste durch Mitarbeitende („Schatten-KI“) kann zum Abfluss vertraulicher Daten führen. Mit der KI-Verordnung der EU kommen verbindliche Anforderungen an Transparenz und Risikomanagement hinzu (Europäische Union 2024c).

Was Unternehmen tun können

- **KI-Leitlinie festlegen:** welche KI-Dienste für welche Datenklassen zugelassen sind; Freigabeprozess für neue Werkzeuge.
- **Deepfake-resiliente Prozesse:** Rückrufprinzip und Vier-Augen-Prinzip für Zahlungen, Freigaben und Datenherausgaben.
- **KI-Abhängigkeiten kartieren:** Anbieter, Rechenzentrumsstandorte und Exit-Optionen in das Dependency-Mapping (Modul 4, Kapitel 5) aufnehmen.
- **Mitarbeitende schulen:** KI-gestützte Phishing- und Täuschungsversuche erkennen und melden.

Praxisbeispiel (illustrativ): Ein mittelständischer Zulieferer stellt fest, dass Vertrieb und Entwicklung frei verfügbare KI-Chatbots mit Kundendaten und Konstruktionsunterlagen nutzen. Erste Schritte: Bestandsaufnahme der genutzten Dienste, eine einseitige Nutzungsrichtlinie, ein freigegebenes KI-Werkzeug mit Datenverarbeitung in der EU und eine kurze Schulung zu Deepfake-Anrufen.

3 Risikomultiplikatoren: Wenn sich Krisen gegenseitig befeuern

Analyseinstrument für vernetzte Krisenkaskaden

Wie sich geopolitische Risiken über vernetzte Systeme zu Kaskaden verstärken, beschreibt das Strategische Whitepaper 02 (Kapitel 2.4). Dieses Modul liefert das Analyseinstrument dazu: zehn mögliche Risikomultiplikatoren und Fragen für den Selbstcheck.

Für Unternehmen liegt die zentrale Herausforderung deshalb nicht allein in der Identifikation einzelner Risiken, sondern im Verständnis ihrer Wechselwirkungen. Eine geopolitische Eskalation kann gleichzeitig Rohstoffpreise erhöhen, Transportwege beeinträchtigen, Sanktionsrisiken verschärfen und Investitionsentscheidungen verzögern. Genau in diesen Kettenreaktionen liegt die eigentliche Verwundbarkeit.

Risikomultiplikatoren sind Faktoren, die Einzelereignisse verstärken, beschleunigen oder in andere Domänen übertragen. Sie lösen Krisen nicht zwingend selbst aus, erhöhen aber deren Reichweite, Geschwindigkeit und Steuerungskomplexität. Die folgenden Multiplikatoren sind eine Auswahl und nicht abschließend; je nach Branche, Standort und Geschäftsmodell können weitere hinzukommen.

3.1 Mögliche Risikomultiplikatoren

Risikomultiplikator	Unternehmensrelevanz
1. Konnektivität kritischer Systeme	Je enger Energie, Transport, IT, Finanzen, Lieferketten und Kommunikation gekoppelt sind, desto schneller können lokale Störungen systemische Auswirkungen entfalten. (Kotzanikolaou, Theoharidou, Gritzalis 2013; Mühlhofer, Bresch, Koks 2024)
2. Geopolitische Eskalation und Sanktionsdynamik	Kriege, Blockaden, Sanktionen und Exportkontrollen wirken auf Preise, Versorgung, Regulierung, Marktzugang und politische Stabilität. (IMF 2023b; Hakobyan, Meleshchuk, Zymek 2023)
3. Energie- und Rohstoffabhängigkeit	Hohe Import- und Konzentrationsabhängigkeiten verstärken Schocks über Kosten, Produktion, Lieferfähigkeit und Wettbewerbsfähigkeit. (IEA 2022; OECD 2026)

Risikomultiplikator	Unternehmensrelevanz
4. Lieferketten- und Logistikfragilität	Engpässe in Häfen, Seewegen, Vorprodukten oder Transitländern können operative Ausfälle weit über den ursprünglichen Störungsort hinaus auslösen. (WTO 2023; OECD 2026)
5. Preis- und Inflationsübertragung	Geopolitische Spannungen schlagen über Energie-, Rohstoff-, Agrar- und Transportmärkte auf Inflation, Kaufkraft, Margen und soziale Stabilität durch. (IMF 2023a)
6. Klima- und Umweltstress	Extremwetter, Wasserstress, Ernteausfälle und Biodiversitätsverluste verstärken bestehende wirtschaftliche, politische und gesellschaftliche Spannungen. (IPCC 2022; Feyen et al. 2020)
7. Soziale Polarisierung und Legitimationsverlust	Versorgungskrisen, Preissteigerungen und Unsicherheit können Proteste, politische Instabilität und Governance-Probleme verschärfen. (OECD 2023; IPCC 2022)
8. Informations- und Desinformationsdynamiken	Desinformation, Vertrauensverlust und gezielte Einflussoperationen können Märkte, politische Entscheidungen und Unternehmensreputation beeinflussen. (OECD 2024; Bentzen 2024)
9. Technologische Verwundbarkeit kritischer Infrastrukturen	Cyberangriffe, OT-/IT-Ausfälle und digitale Abhängigkeiten können physische, finanzielle und politische Krisen beschleunigen. (Kotzanikolaou, Theoharidou, Gritzalis 2013; BSI 2025)
10. Governance- und Reaktionsverzögerungen	Fragmentierte Zuständigkeiten, schwache Frühwarnung und langsame Entscheidungen erhöhen Dauer, Tiefe und Kosten von Kaskadeneffekten. (OECD 2023)

Diese Risikomultiplikatoren zeigen: Die größte Herausforderung liegt nicht in der Existenz einzelner Risiken, sondern **in deren Kombination**. Energiekrisen können Produktionskosten erhöhen, was Investitionen hemmt, Innovationsfähigkeit schwächt und technologische Abhängigkeiten vertieft. Lieferkettenstörungen können regulatorische Konflikte auslösen, Finanzierungskosten erhöhen und Marktzugang gefährden. Desinformation kann Krisenkommunikation erschweren, Vertrauen untergraben und politische Reaktionen beeinflussen.

3.2 Perspektivwechsel: von Einzelrisiken zu vernetzten Kaskaden

Klassisches Risikomanagement, das Risiken primär nach Eintrittswahrscheinlichkeit und Schadenshöhe einzelner Ereignisse bewertet, reicht für systemische geopolitische Kaskaden nur eingeschränkt aus. Erforderlich ist ein stärker vernetzter Ansatz, der Abhängigkeiten, Triggerpunkte, Eskalationspfade und operative Auswirkungen gemeinsam betrachtet. Das bedeutet nicht, jede denkbare Krise vorherzusagen - entscheidend ist, die eigene Verwundbarkeit gegenüber Kaskadeneffekten zu verstehen.

Selbstcheck-Fragen für Risiko- und Sicherheitsverantwortliche

- Welche kritischen Funktionen hängen von einzelnen Lieferanten, Regionen, Technologien, Datenräumen, Transportwegen oder regulatorischen Voraussetzungen ab?
- Wo bestehen Konzentrationsrisiken - Single-Source, Single-Region, Single-Technology?
- Welche Störung könnte mehrere Geschäftsbereiche gleichzeitig treffen?
- Welche Entscheidungen müssten unter Zeitdruck getroffen werden - und wer trifft sie?

3.3 Der Sechs-Punkte-Schutzansatz

Unternehmen können sich wirksam schützen, wenn sie geopolitische Risikofelder nicht als Sammlung isolierter Einzelrisiken, sondern als vernetzte Kaskaden managen. Eine Resilienzstrategie setzt sich aus der Kombination und gemeinsamen Bewertung von Einzelaktivitäten zusammen, was mit Hilfe des Sechs-Punkte-Schutzansatzes erfolgen kann:

1. Früherkennung
2. Reduktion kritischer Abhängigkeiten
3. Robuste Governance und Krisensteuerung
4. Belastbare Lieferketten- und Technologieresilienz
5. Due Diligence und Schutz kritischer Assets
6. Kooperation mit vertrauenswürdigen Partnern und Behörden

> *Nicht die vollständige Vermeidung von Störungen ist das Ziel, sondern die Fähigkeit, Auswirkungen früh zu erkennen, Handlungsoptionen vorzubereiten, kritische Funktionen zu schützen und unter verschärften geopolitischen Bedingungen entscheidungs- und leistungsfähig zu bleiben.*

4 Resilienzarchitektur: Fähigkeiten-Reifegradcheck

Von der Schutzfunktion zur strategischen Managementfähigkeit

Wie sich Resilienz von einer nachgelagerten Schutzfunktion zu einer strategischen Managementfähigkeit entwickelt, beschreibt das Strategische Whitepaper 02 (Kapitel 1.1). Dieses Modul übersetzt das in ein Werkzeug: Bestehende Risiko-, Sicherheits- und Krisenmanagementansätze werden enger vernetzt, vorausschauender und geschäftsnäher ausgerichtet.

Unternehmensresilienz beginnt mit Transparenz über die eigenen kritischen Funktionen: Welche Produkte, Prozesse, Standorte, Lieferanten, Technologien, Datenräume, Infrastrukturen und Partner sind für die Handlungsfähigkeit tatsächlich unverzichtbar? Mit anderen Worten:

Das Resilienzkonzept eines Unternehmens muss die absolute Untergrenze der Betriebsfähigkeit in einer schweren Krise enthalten und definieren. Dabei wird die normale Wertschöpfung des Unternehmens auf seine minimalen, primären Wertschöpfungsaktivitäten reduziert. Alle unverzichtbaren Wertschöpfungsaktivitäten werden fokussiert, um bei einem Minimalansatz von Ressourcen die kritischste Wertschöpfungskette - von der essenziellen Leistungserbringung bis zur Liquiditätssicherung - im Notbetrieb aufrechtzuerhalten. Das Ziel besteht darin, existenzbedrohende Schäden von Kunden abzuwenden und das wirtschaftliche Überleben der Organisation zu sichern. [1]Dieser Ansatz geht über das Minimum Business Continuity Objective (MBCO) nach ISO 22301:2019 und den Notbetrieb nach BSI-Standard 200-4 hinaus (ISO 2019; ISO 2025; BSI 2023). Ein Beispiel für ein KMU enthält Modul 3, Kapitel 4, Abschnitt 4.3.

Erst wenn diese Abhängigkeiten innerhalb der Wertschöpfungskette bekannt sind, lassen sich Prioritäten setzen, Schutzmaßnahmen ableiten und Investitionsentscheidungen belastbar begründen.

[1] Minimum Business Continuity Objective (MBCO) (ISO 2019; ISO 2025); der BSI-Standard 200-4 beschreibt, wie Unternehmen einen solchen Notbetrieb planen könnten (BSI 2023).

4.1 Acht Fähigkeiten einer modernen Resilienzarchitektur

Nutzen Sie die folgende Tabelle als Ausgangspunkt für einen internen Reifegrad-Workshop: Wo steht Ihr Unternehmen je Fähigkeit heute - grundlegend vorhanden, im Aufbau, oder strategisch verankert?

Fähigkeit	Bedeutung für Unternehmen
Geopolitische Früherkennung	Strategische Triggerpunkte erkennen, Entwicklungen einordnen und frühzeitig Handlungsoptionen ableiten.
Transparenz kritischer Abhängigkeiten	Kritische Lieferanten, Technologien, Datenräume, Standorte und Funktionen identifizieren.
Reduktion strategischer Verwundbarkeiten	Single-Source-, Single-Region- und Technologieabhängigkeiten gezielt reduzieren.
Integrierte Governance	Security, BCM, Crisis Management, Cybersecurity, Risk, Legal, Compliance und Business enger verzahnen.
Szenario- und Stresstestfähigkeit	Auswirkungen geopolitischer Eskalationen auf Geschäftsmodelle, Lieferketten und kritische Funktionen testen.
Schutz kritischer Assets	Mitarbeitende, Daten, IP, Technologien, Schlüsselpersonen, Produktionsfähigkeit und sensible Partnerschaften wirksam schützen.
Krisen- und Entscheidungsfähigkeit	Klare Eskalationswege, belastbare Lagebilder und schnelle Entscheidungsprozesse sicherstellen.
Kooperation mit Partnern und Behörden	Lagebilder verbessern, Reaktionsfähigkeit erhöhen und Zugang zu relevanten Warn- und Unterstützungsstrukturen sichern.

Geopolitische Früherkennung erfordert ein kontinuierliches Monitoring strategischer Triggerpunkte: politische Entscheidungen, Sanktionen, Exportkontrollen, militärische Eskalationen, regulatorische Veränderungen, Desinformationskampagnen, Cyberbedrohungen, Rohstoffengpässe und Veränderungen in kritischen Lieferketten. Diese Informationen müssen nicht nur gesammelt, sondern in konkrete Entscheidungsprozesse übersetzt werden.

Auch Business Continuity Management, Crisis Management, Corporate Security, Cybersecurity und Enterprise Risk Management müssen enger zusammengeführt werden.

In einem geopolitisch fragmentierten Umfeld entstehen Störungen häufig gleichzeitig in mehreren Domänen: Cyberangriffe treffen auf Lieferkettenengpässe, regulatorische Unsicherheit auf Reputationsrisiken, Energiepreise auf Produktionsentscheidungen. Nur integrierte Resilienzstrukturen können solche Kaskaden wirksam steuern.

Bewertungsskala für den Reifegrad-Workshop

Bewerten Sie jede der acht Fähigkeiten auf einer dreistufigen Skala und halten Sie für Stufe 2 und 3 einen konkreten Nachweis fest (Dokument, Übung, Kennzahl). Die Skala lehnt sich an die Prinzipien organisationaler Resilienz der ISO 22316:2017 an (ISO 2017).

Stufe	Merkmale	Beispiel: Geopolitische Früherkennung
1 - grundlegend vorhanden	Aufgabe ist benannt, wird anlassbezogen und personenabhängig wahrgenommen; keine festen Prozesse oder Kennzahlen.	Einzelne Fachleute verfolgen Nachrichtenlage; Informationen gehen bei Bedarf per E-Mail an die Geschäftsführung.
2 - im Aufbau	Prozess, Verantwortlichkeit und Werkzeuge sind definiert; regelmäßige Anwendung, erste Übungen; Ergebnisse fließen in einzelne Entscheidungen ein.	Monatliches Lagebild mit definierten Triggerpunkten (z. B. neue Sanktionen oder Exportkontrollen für eigene Vorprodukte, Fracht- oder Energiepreise über einem festgelegten Schwellenwert, Militärmanöver oder Blockaden in Lieferregionen); Verteiler für Einkauf, BCM und Vertrieb; jährliche Übung.
3 - strategisch verankert	Fähigkeit ist in Strategie- und Investitionsprozesse integriert, mit Kennzahlen im Management-Reporting unterlegt und wird regelmäßig beübt und verbessert.	Frühwarnindikatoren sind mit Schwellenwerten und Maßnahmenplänen hinterlegt; Lagebild ist fester Bestandteil der Vorstandssitzung und der Strategieplanung.

Ergebnis des Workshops: Reifegradprofil je Fähigkeit, priorisierte Lücken mit Verantwortlichen und Zieltermin, Bezug zu den betroffenen Unternehmenszielen (z. B. Lieferfähigkeit, Marge, Marktzugang).

4.2 Künstliche Intelligenz als Werkzeug im Resilienzmanagement

Künstliche Intelligenz (KI) entwickelt sich zunehmend zu einem wichtigen Unterstützungsinstrument im Sicherheits-, Risiko- und Resilienzmanagement. Ihre besondere Stärke liegt in der schnellen Verarbeitung großer Informationsmengen aus unterschiedlichen Quellen und Sprachen. KI kann Informationen recherchieren, strukturieren, analysieren, zusammenfassen und visualisieren und dadurch die Informationsgrundlage für Sicherheitsentscheidungen verbessern (BSI 2026a; BSI 2024; NCSC 2025).

In großen Unternehmen wird KI beispielsweise in Sicherheitsleitstellen (Security Operations Centers) eingesetzt, um sicherheitsrelevante Meldungen zu priorisieren, verdächtige Aktivitäten schneller zu erkennen oder die Auswertung von Ereignisdaten aus

Systemen des Security Information and Event Managements zu unterstützen. Darüber hinaus kann KI kontinuierlich öffentlich verfügbare Informationsquellen auswerten, um Lagebilder zu erstellen, Entwicklungen frühzeitig zu erkennen und die strategische Vorausschau (Security Intelligence und Foresight) zu verbessern. Weitere Anwendungsfelder sind die Unterstützung bei der Videoanalyse, die Beobachtung geopolitischer Entwicklungen sowie die Identifikation von Risiken in Lieferketten.

Besonders für kleine und mittlere Unternehmen eröffnet KI neue Möglichkeiten. Organisationen, die nicht über Experten für alle sicherheitsrelevanten Themengebiete verfügen, können KI nutzen, um Informationen zu Bedrohungen, geopolitischen Entwicklungen, Cyberrisiken oder Lieferkettenstörungen effizient auszuwerten. Dadurch können Sicherheitsverantwortliche ein breiteres Themenspektrum abdecken und fundiertere Entscheidungen treffen, ohne für jedes Fachgebiet eigene Spezialisten vorhalten zu müssen.

Gleichzeitig ist KI kein Ersatz für Sicherheitsmanager, Risikoexperten oder Krisenstäbe. Die Technologie unterstützt Menschen bei der Informationsgewinnung und Analyse, übernimmt jedoch nicht die Verantwortung für Bewertungen, Priorisierungen oder Entscheidungen. Die Qualität der Ergebnisse hängt wesentlich von der Fragestellung, den zugrundeliegenden Daten sowie der fachlichen Überprüfung der Resultate ab. Menschliche Expertise bleibt daher unverzichtbar, um KI-generierte Erkenntnisse einzuordnen, mit unternehmensspezifischen Prozessen und Vorgaben abzugleichen sowie daraus geeignete Maßnahmen abzuleiten.

Grenzen und Risiken der Nutzung: KI-Ergebnisse können unvollständig, veraltet oder schlicht falsch sein; Sprachmodelle erfinden mitunter plausibel klingende Aussagen oder Quellen („Halluzinationen“). Sicherheitsrelevante Auswertungen müssen daher immer fachlich geprüft werden; dafür braucht es weiterhin Personal mit Fach- und Methodenkenntnis. Zudem ist festzulegen, welche Informationen in KI-Systeme eingegeben werden dürfen (Datenschutz, Geheimschutz, Geschäftsgeheimnisse) und wo die Daten verarbeitet werden. Die Risiken durch den Einsatz von KI auf Angreiferseite beschreibt Modul 1, Kapitel 2, Abschnitt 2.9.

Der größte Mehrwert von KI liegt somit nicht im Ersatz menschlicher Kompetenz, sondern in deren Erweiterung. Sie ermöglicht es Sicherheitsverantwortlichen, schneller auf Veränderungen zu reagieren, mehr Informationsquellen gleichzeitig zu bewerten und knappe personelle Ressourcen wirksamer einzusetzen.

Bezug zur Resilienzarchitektur: KI unterstützt vor allem die geopolitische Früherkennung, die Transparenz kritischer Abhängigkeiten und die Krisen- und Entscheidungsfähigkeit (Modul 3, Kapitel 4, Abschnitt 4.1). Ein sinnvoller Einstieg ist ein KI-gestütztes Lagebild für wenige, klar definierte Triggerpunkte, dessen Ergebnisse stets fachlich geprüft werden. Risiken durch KI behandelt Modul 1, Kapitel 2, Abschnitt 2.9, Chancen für neue Geschäftsfelder Modul 9, Kapitel 10, Abschnitt 10.3.

4.3 Von der Analyse zur Umsetzung: erste Schritte

Die folgenden Beispiele zeigen mögliche erste Schritte. Sie sind bewusst illustrativ und kein abschließender oder verbindlicher Maßnahmenkatalog; Ausgangslage und Umsetzung unterscheiden sich je nach Unternehmen. Die Zeithorizonte folgen der Leitfrage des Strategischen Whitepapers 02: heute, in den kommenden sechs Monaten und langfristig.

Zeithorizont	Mögliche erste Schritte	Ergebnis
Sofort (0-3 Monate)	Verantwortliche Person für Resilienz benennen; die zehn wichtigsten Produkte, Kunden und Lieferanten auflisten; Notfallkontakte und Meldewege (Modul 6, Kapitel 7) aktualisieren; Backups und Notstrom kritischer Systeme prüfen.	Klarheit, was auf keinen Fall ausfallen darf
Kurzfristig (bis 6 Monate)	Dependency-Mapping für die kritischsten Prozesse (Modul 4, Kapitel 5); ein Szenario als Tabletop-Übung durchspielen (Modul 5, Kapitel 6); Zweitquellen für Single-Source-Teile anfragen; Reifegrad-Selbsteinschätzung (Modul 3, Kapitel 4, Abschnitt 4.1).	Priorisierte Liste der größten Verwundbarkeiten mit Verantwortlichen
Mittelfristig (6-24 Monate)	Zweitquellen qualifizieren und Sicherheitsbestände aufbauen; Resilienzkriterien in Investitions-, Standort- und Einkaufsentscheidungen verankern; Lagebild und Kennzahlen ins Management-Reporting aufnehmen.	Resilienz ist Teil der Unternehmenssteuerung, nicht nur des Krisenfalls

Beispiel: Mindestwertschöpfung sichern (KMU, illustrativ). Ein Maschinenbauer mit 250 Beschäftigten legt fest, welche Leistungen er auch im schweren Störfall aufrechterhalten muss, etwa Ersatzteilversorgung und Service für die wichtigsten Bestandskunden. Dafür bestimmt er die nötigen Mitarbeitenden und ihre Vertretungen, einen Mindestbestand kritischer Komponenten, einen IT-Notbetrieb (z. B. Auftragsabwicklung für zwei Wochen ohne zentrale Systeme) und eine feste Kommunikationslinie zu den Kunden. So bleibt der Kern der Wertschöpfung erhalten, auch wenn das Gesamtgeschäft vorübergehend einbricht.

> *Die zentrale Frage lautet nicht, ob Unternehmen in Resilienz investieren sollten, sondern wo die größten Verwundbarkeiten liegen und welche Fähigkeiten aufgebaut werden müssen, um auch unter geopolitischem Druck funktionsfähig zu bleiben.*

5 Kritische Abhängigkeiten: Dependency-Mapping

Neun Felder, in denen sich moderne Verwundbarkeit konzentriert

Wer Resilienz aufbauen will, muss zunächst verstehen, wo die eigenen Verwundbarkeiten liegen. Nutzen Sie die folgenden neun Felder als Struktur für ein internes Dependency-Mapping - je Feld: Wo stehen wir? Welche Konzentrationsrisiken bestehen? Welche Alternativen haben wir bereits, welche fehlen noch?

Feld	Bedeutung für Unternehmen
Energie	Energie ist das Fundament industrieller Handlungsfähigkeit - Preisvolatilität, Versorgungssicherheit und die Verfügbarkeit erneuerbarer Quellen sind strategische Variablen geworden. Beispiel: Prüfung der Notstromversorgung, inkl. Dieselbevorratung, an kritischen Standorten wie Rechenzentren.
Lieferketten	Lieferketten haben ihre vermeintliche Robustheit unter Pandemiebedingungen und geopolitischen Spannungen eingebüßt; ihre Neugestaltung ist eine der zentralen Managementaufgaben der Dekade. Beispiel: Ständiges Monitoring entlang der Lieferketten, Identifikation von Single-Source-Abhängigkeiten, wie bei kritischen Bauteilen, Rohstoffen und Services sowie Aufbau alternativer Lieferanten und Transportwege.
Digitalisierung	Digitalisierung schafft Effizienz, erzeugt aber gleichzeitig neue Abhängigkeiten - insbesondere dort, wo kritische Prozesse auf externe Plattformen, proprietäre Software oder nicht-europäische Cloudinfrastruktur aufsetzen. Beispiel: Prüfung alternativer europäischer Provider zur Sicherstellung von Vertraulichkeit, Integrität und Verfügbarkeit sowie Aufbau redundanter Technologien für kritische Prozesse, Diversifizierung kritischer Technologien und Kompetenzen, um Vendor-Lock-in und Know-how-Abhängigkeiten zu begrenzen.
Halbleiter und Schlüsselkomponenten	Die Konzentration der globalen Chipproduktion auf wenige Standorte macht Halbleiter zur geopolitischen Achillesferse industriell-digitaler Wertschöpfungsketten. Beispiel: Ermittlung der Verfügbarkeit kritischer Halbleiter und Erkennung möglicher Engpässe, Aufbau redundanter Bezugsquellen, angemessene Bevorratung.

Feld	Bedeutung für Unternehmen
Sicherheitsmanagement	Sicherheit gewinnt als unternehmerische Grundanforderung an Gewicht. Beispiel: Integration von Sicherheitslageinformationen und Risikoanalysen in strategische Entscheidungen des Unternehmens, Bereitstellung der erforderlichen Ressourcen für adäquate Sicherheitsmaßnahmen.
Cloud- und Rechenzentrumsinfrastruktur	Durch zunehmende geopolitische Volatilität steigt die Abhängigkeit von politischen Entwicklungen, dadurch entsteht das Risiko eines ungewollten Informationsabflusses, Beeinträchtigung der Integrität und Verfügbarkeit aufgrund regulatorischer Eingriffe und politischer Entscheidungen. Hinzu kommt die Abhängigkeit von Rechenzentrums- und KI-Rechenkapazitäten, die sich auf wenige Anbieter und Standorte konzentrieren. Beispiel: Transparenz herstellen bezüglich der bestehenden Infrastruktur, Risiken und Abhängigkeiten (Multi-Cloud-Strategie), Prüfung europäischer bzw. souveräner Cloud-Angebote für besonders schützenswerte Daten und Anwendungen, regionale Datenhaltung mit lokalen Rückfalloptionen für geschäftskritische Prozesse, adäquate Verschlüsselung, klare Exit- und Migrationsstrategien.
Cybertechnologien	Cyberrisiken sind kein isoliertes IT-Thema mehr, sondern integraler Bestandteil geopolitischer Konfliktlagen und müssen entsprechend auf strategischer Ebene adressiert werden. Beispiel: Durchführung einer Cyberübung, bei der der Ausfall eines zentralen IT- oder Produktionssystems simuliert und die Wiederherstellung aus gesicherten Backups getestet wird.
Physische Sicherheit	Standorte, Produktionsanlagen, Rechenzentren, Logistikknoten und Personal sind die physische Grundlage aller übrigen Felder. Sabotage, Ausspähung, Drohnenüberflüge und Angriffe auf kritische Infrastrukturen nehmen zu; Unternehmen sollten Schutzbedarf, Redundanzen und Wiederanlaufzeiten ihrer kritischen Standorte kennen und mit den Anforderungen aus CER-Richtlinie und KRITIS-Dachgesetz abgleichen (vgl. BfV 2025; Europäische Union 2022b; Die Bundesregierung 2026b). Beispiel: Ganzheitliche Bewertung des Schutzbedarfs kritischer Standorte einschließlich Zutrittsschutz, Drohnendetektion, Videoüberwachung, Redundanzen und Wiederanlaufzeiten.

Feld	Bedeutung für Unternehmen
Satelliten-, Navigations- und Zeitdienste	Viele Prozesse hängen unbemerkt von satellitengestützter Navigation, Zeitgebung, Kommunikation oder Erdbeobachtung ab - von Logistik und Flottensteuerung über Netz- und Finanzsysteme bis zur Zeitsynchronisation in IT und OT. Beispiel: Unternehmen sollten prüfen, welche kritischen Prozesse unmittelbar oder mittelbar davon abhängen, und Ausfall, Beeinträchtigung, Manipulation (Jamming, Spoofing) sowie verfügbare Rückfallebenen bewerten.

Leitfragen für den Mapping-Workshop

- Welche dieser Felder sind für unsere kritischsten Geschäftsprozesse unverzichtbar?
- Wo haben wir Single-Source- oder Single-Region-Abhängigkeiten - und sind uns diese überhaupt bekannt?
- Welche Alternativen (Diversifizierung, Regionalisierung, Nearshoring, Friend-Shoring, eigene Entwicklungskapazitäten) haben wir bereits aufgebaut?
- Wer im Unternehmen trägt die Verantwortung, diese Abhängigkeiten laufend zu aktualisieren?

> *Resilienz ist damit kein defensives Konzept mehr. Sie wird zu einer strategischen Voraussetzung für Wettbewerbsfähigkeit, Vertrauen und unternehmerische Handlungsfähigkeit.*

6 Szenario-Stresstest-Toolkit 2027-2030

Vier gleichwertige Zukünfte - keine Prognosen, sondern Planungskorridore

> *Die Szenarien stellen keine Prognosen dar, sondern plausible, bewusst zugespitzte Entwicklungen auf Basis aktueller geopolitischer Trends, sicherheitspolitischer Analysen und bekannter Verwundbarkeiten. Ziel ist die Sensibilisierung für Wechselwirkungen und systemische Auswirkungen - nicht die Vorhersage konkreter Ereignisse (eigene Szenarioentwicklung des ThinkTank). Die Ausgangslagen geben den Analysestand vom Juni 2026 wieder; die seither eingetretene Entwicklung im Nahen Osten ist in Modul 5, Kapitel 6, Abschnitt 6.5 berücksichtigt.*

Arbeitsblatt für den Stresstest

Bearbeiten Sie jedes Szenario je Eskalationsstufe mit diesem Raster. Die ausgefüllte Zeile zeigt ein Beispiel für Szenario 2 (Taiwanstraße), Stufe 1, aus Sicht eines Industrieunternehmens.

Eskalation	Kritische Funktionen	Frühindikatoren / Trigger	Auswirkung auf Ziele	Maßnahmen und Vorlaufzeit	Zuständig
Beispiel: Szenario 2, Stufe 1	Beschaffung von Halbleitern und Elektronik; Serienproduktion	Ausweitung von Militär-übungen, steigende Versicherungsprämien und Frachtraten, Exportgenehmigungspflichten	Lieferverzug, Margendruck durch Spotmarktkäufe, Vertragsstrafen	Sicherheits-bestände für kritische Chips (3-6 Monate), Zweitquellen qualifizieren (6-18 Monate), Alternativrouten vertraglich sichern	Einkauf, BCM, Produktion
Stufe 1					
Stufe 2					
Stufe 3					

Ergebnis: für jedes Szenario eine Aussage, ob das Geschäftsmodell auf jeder Stufe tragfähig bleibt, welche Maßnahmen vorab getroffen werden müssen und welche Vorlaufzeit dafür nötig ist.

6.1 Szenario 1 - Groß angelegter Konflikt in Europa

Dieses Szenario beschreibt eine plausible, jedoch keineswegs deterministische Entwicklung, in der eine Kombination aus intensivierter hybrider Kriegsführung, politischer Fragmentierung und regionaler militärischer Eskalation zu einem groß angelegten Konflikt in Europa führen könnte.

6.1.1 AUSGANGSLAGE (STAND DER ANALYSE: JUNI 2026)

Europa sieht sich infolge des andauernden Russland-Ukraine-Krieges, zunehmender Spannungen und wachsender militärischer Aktivitäten mit erhöhter Instabilität in Mittel- und Osteuropa, Verschiebungen in der transatlantischen Allianz und zunehmenden hybriden Bedrohungen konfrontiert.

6.1.2 ESKALATIONSSTUFE 1 - EUROPA UNTER INTENSIVIERTER HYBRIDER KRIEGSFÜHRUNG

Russland weitet hybride Kriegsführung in ganz Europa aus und nutzt die politische Fragmentierung gezielt aus. Desinformationskampagnen, Einflussoperationen sowie Aktivitäten staatlich unterstützter Akteure gegen kritische Infrastruktur nehmen zu (vgl. BfV 2025). Hauptziele sind kritische Infrastrukturen (Strom, Schiene, Treibstoff, industrielle Steuerungssysteme) für Sabotage, Wirtschaftsspionage und Cyberangriffe - mit chronischen Störungen in Lieferketten und Logistik.

- Anhaltende hybride Angriffe untergraben das öffentliche Vertrauen, schwächen die EU-Einheit und vertiefen politische Fragmentierung.
- Nachlassende westliche Unterstützung für die Ukraine ermöglicht Russland militärische Fortschritte.
- Russland nutzt geschwächte europäische Koordination zur Ausweitung seines Einflusses (z. B. Odessa, Transnistrien, Moldau).

Auswirkungskategorien: Cybersecurity, physische und wirtschaftliche Sicherheit, Geschäftsabläufe und Lieferketten, Belegschaft und Mitarbeitende.

6.1.3 ESKALATIONSSTUFE 2 - REGIONALE MILITÄRISCHE EXPANSION UND FRAGMENTIERUNG DER NATO

Nachlassende westliche Unterstützung ermöglicht russische Vorstöße nach Odessa und Transnistrien und destabilisiert Moldau. Die USA könnten militärische Kräfte aus Europa abziehen und unterstützen die NATO im Konflikt mit Russland nur minimal bis gar nicht. Russland könnte begrenzte militärische Aktivitäten im Raum Narva initiieren und/oder über die Suwałki-Lücke eine Landbrücke nach Kaliningrad mit militärischen Mitteln herstellen wollen, um die Reaktionsfähigkeit und Geschlossenheit der NATO zu testen.

- Russische Militäraktionen in Narva testen die Einheit der NATO; die Suwałki-Lücke wird militärisch umkämpft und isoliert die baltischen Staaten.

- Europäische Länder aktivieren Verteidigungspläne, einschließlich Teilmobilisierung und Notfallkontrollen kritischer Infrastruktur.
- Hybride Angriffe könnten sich schrittweise zu begrenzten kinetischen Angriffen gegen kritische Infrastrukturen entwickeln.
- Die baltische Krise eskaliert zu einer direkten Konfrontation zwischen NATO und Russland.
- China nutzt die Bindung westlicher Kräfte in Europa, um den Druck auf Taiwan und im Südchinesischen Meer zu erhöhen, und stützt Russland wirtschaftlich und technologisch (vgl. NATO 2024).

Auswirkungskategorien: Cybersecurity, physische und wirtschaftliche Sicherheit, Geschäftsabläufe und Lieferketten, Belegschaft und Mitarbeitende, Regierung und Recht, Finanzen und Handel.

6.1.4 ESKALATIONSSTUFE 3 - GROß ANGELEGTER KONFLIKT IN EUROPA INFOLGE DER BALTISCHEN KRISE

Der Konflikt in Estland eskaliert schnell, während Russland über Belarus und Kaliningrad die baltischen Staaten blockiert und isoliert. Eine deutsche Brigade in Litauen gerät in intensive Gefechte. Europäische Länder aktivieren umfassende Verteidigungspläne und wechseln in eine vollständige nationale Verteidigungshaltung. Drohnen- und Raketenangriffe treffen kritische Logistikdrehscheiben und Infrastruktur in ganz Europa und führen zu einer direkten NATO-Russland-Konfrontation.

Auswirkungskategorien: Technologie und Daten, Cybersecurity, physische und wirtschaftliche Sicherheit, Regierung und Recht, Geschäftsabläufe und Lieferketten, Kunden, Partner und Märkte, Belegschaft und Mitarbeitende, Finanzen und Handel.

Betroffenes System	Potenzielle Auswirkung
Energieversorgung	Rationierung, Preisschocks
Logistik	Grenzkontrollen, Transportausfälle
Lieferketten	Produktionsunterbrechungen
Cyber	Angriffe auf OT- und IT-Systeme
Personal	Reisebeschränkungen, Evakuierungen
Compliance	Notfallregulierungen
Finanzen	Liquiditätsengpässe
Kommunikation	Desinformation

6.1.5 WAS BEDEUTET DAS FÜR GLOBALE UNTERNEHMEN?

Neben klassischen Business-Continuity- und Krisenmanagementansätzen gewinnen insbesondere geopolitische Frühwarnmechanismen, Szenarioplanung, Resilienzinvestitionen sowie die Absicherung kritischer Funktionen und Abhängigkeiten an Bedeutung. Die strategische Stärkung der digitalen Souveränität, durch Investitionen in eigene Technologieentwicklung und die Nutzung vertrauenswürdiger europäischer oder regionaler Lösungen, wird zu einem entscheidenden Wettbewerbsfaktor und einer Notwendigkeit für die Geschäftskontinuität.

6.2 Szenario 2 - Eskalation in der Taiwanstraße als geoökonomischer Systemschock

> *Ein Konflikt in der Taiwanstraße wäre kein regional begrenztes Sicherheitsereignis, sondern ein globaler geoökonomischer Systemschock mit unmittelbaren Auswirkungen auf Technologie, Handel, Energie, Finanzmärkte und Unternehmensresilienz.*

Dieses Szenario untersucht eine mögliche Eskalation der Spannungen in der Taiwanstraße von anhaltenden Zwangsmaßnahmen und Grauzonenaktivitäten hin zu einer umfassenden militärischen Konfrontation, die in einer vollständigen Blockade und offenem Konflikt mit weitreichenden geostrategischen und wirtschaftlichen Folgen mündet.

6.2.1 AUSGANGSLAGE (STAND DER ANALYSE: JUNI 2026)

China übt weiterhin Druck auf Taiwan aus, mit regelmäßigem Eindringen in See- und Lufträume, groß angelegten Militärübungen, Cyberoperationen, wirtschaftlichem Druck und diplomatischen Maßnahmen. Die Taiwanstraße zählt zu den geopolitisch sensibelsten Regionen der Welt, da sich dort sicherheitspolitische, technologische und wirtschaftliche Interessen unmittelbar überlagern.

rd. 44 %

Anteil Taiwans an der weltweiten Foundry-Kapazität (2024) - rd. zwei Drittel bei fortgeschrittenen Prozessen (16 nm und kleiner), über 90 % bei modernsten Chips unter 10 nm (Datenstand 2019) (TrendForce 2024; SIA/BCG 2021)

6.2.2 ESKALATIONSSTUFE 1 - INTENSIVIERUNG VON GRAUZONEN- UND MILITÄRDRUCK

China versucht, Taiwan politisch zu schwächen, ohne einen offenen Krieg auszulösen: militärischer Druck durch Luft- und Seevorstöße, Cyberangriffe, Desinformation, Spionage, wirtschaftlicher Druck, Störungen von Lieferketten und Sabotage. Bereits diese Phase kann erhebliche Auswirkungen auf internationale Finanzmärkte, Versicherungsprämien, Schifffahrtskosten und Investitionsentscheidungen entfalten.

- Intensivierung von Grauzonenmaßnahmen schwächt Regierung, Kommunikation, Finanzsysteme und öffentliches Vertrauen.
- Ausweitung wirtschaftlichen Drucks auf ECFA (Economic Cooperation Framework Agreement, Handelsabkommen China-Taiwan von 2010)-bezogene Exporte, Schifffahrt und Investorenvertrauen.
- „Rote Linien“-Ereignisse führen zu erweiterten Militärübungen und möglicher Zugangskontrolle.

Auswirkungskategorien: Cybersecurity, physische und wirtschaftliche Sicherheit, Geschäftsabläufe und Lieferketten, Belegschaft und Mitarbeitende.

6.2.3 ESKALATIONSSTUFE 2 - BEGRENZTE BLOCKADE FÜHRT ZU REGIONALER KRISE UND GLOBALER STÖRUNG

Nach erfolglosen Grauzonenmaßnahmen wechselt China zu einer begrenzten Blockade mit Fokus auf Schlüsselhäfen und Luftwegen - eine Mischung aus maritimen und

paramilitärischen Kräften, regulatorischem und wirtschaftlichem Zwang sowie gezielten Desinformationskampagnen.

- Kontrolle über zentrale Häfen und Luftzugänge sowie Inspektionen im Seeverkehr.
- Selektive Anreize für kooperative Länder und Unternehmen.
- Steigende Transportrisiken und Verzögerungen in globalen Lieferketten, insbesondere bei Halbleitern - da rund die Hälfte der weltweiten Containerschiffsflotte die Taiwanstraße passiert (Varley 2022), können bereits begrenzte maritime Einschränkungen erhebliche Auswirkungen auf globale Warenströme haben.
- Überlastung kritischer Infrastruktur Taiwans; steigende Wahrscheinlichkeit sekundärer Auswirkungen auf internationale Energie-, Finanz- und Rohstoffmärkte.
- Ist der Krieg gegen die Ukraine dann nicht beigelegt, kann Russland die Bindung amerikanischer Kräfte im Pazifik nutzen, um den Druck auf Europa zu erhöhen.

Auswirkungskategorien: Cybersecurity, physische und wirtschaftliche Sicherheit, Geschäftsabläufe und Lieferketten, Belegschaft und Mitarbeitende, Regierung und Recht, Finanzen und Handel.

6.2.4 ESKALATIONSSTUFE 3 - VOLLBLOCKADE ESKALIERT IN MILITÄRISCHEN KONFLIKT

Ein Zwischenfall in der Taiwanstraße führt zunächst zu einer Quarantäne, die in eine vollständige Blockade und einen offenen militärischen Konflikt eskaliert. Integrierte Raketen-, Cyber-, Luft- und Marineoperationen zielen auf die Sicherung von Informations-, See- und Lufthoheit ab. China verwehrt Unternehmen aus Ländern, die Taiwan unterstützen, den Zugang zu Einrichtungen, Daten und kritischen Dienstleistungen - mit erheblichen Lieferkettenstörungen und weitreichenden Betriebsunterbrechungen. Umfangreiche Sanktionsregime, Exportkontrollen sowie Einschränkungen des Daten- und Technologietransfers sind wahrscheinlich.

Ein Konflikt in der Taiwanstraße wäre zugleich ein Technologie- und Datenkonflikt: Neben physischen Lieferketten wären insbesondere globale Halbleiter-, Cloud-, KI- und Kommunikationsökosysteme betroffen (vgl. Kleinhans, Jha 2025).

Auswirkungskategorien: Cybersecurity, physische und wirtschaftliche Sicherheit, Geschäftsabläufe und Lieferketten, Belegschaft und Mitarbeitende, Regierung und Recht, Finanzen und Handel, Technologie und Daten, Kunden, Partner und Märkte.

Bereich	Potenzielle Auswirkung
Halbleiter	Produktionsausfälle
Logistik	Verzögerungen und Engpässe
Schifffahrt	Umleitungen und Kostensteigerungen
Energie	Preisvolatilität
Cyber	Angriffe auf kritische Systeme
Technologie	Exportkontrollen
Finanzen	Marktverwerfungen
Daten	Zugriffsrestriktionen

6.2.5 WAS BEDEUTET DAS FÜR GLOBALE UNTERNEHMEN?

Dieses Szenario verdeutlicht die Notwendigkeit, strategische Abhängigkeiten systematisch zu identifizieren und regelmäßig zu überprüfen - insbesondere Halbleiter, kritische Rohstoffe, Cloud-Dienste, maritime Transportwege, Datenflüsse sowie den Zugang zu regionalen Absatz- und Beschaffungsmärkten. Geopolitische Entwicklungen in der Taiwanstraße können sich innerhalb kürzester Zeit zu globalen Technologie-, Handels- und Lieferkettenkrisen entwickeln.

6.3 Szenario 3 - US-China technologische Entkopplung

Dieses Szenario betrachtet eine schrittweise Eskalation der techno-ökonomischen Rivalität zwischen den USA und China. Im Mittelpunkt steht nicht allein die technologische Rivalität, sondern die zunehmende Fragmentierung globaler Wirtschafts-, Daten-, Finanz- und Technologiesysteme - von zunehmendem Compliance-Druck über eine umfassendere systemische Trennung in kritischen Sektoren bis zu einem krisengetriebenen Bruch.

6.3.1 AUSGANGSLAGE (STAND DER ANALYSE: JUNI 2026)

Die Beziehungen zwischen den USA und China sind durch strukturelle Rivalität und zunehmende techno-ökonomische Entkopplung geprägt. Der Wettbewerb entwickelt sich zunehmend von einem Handelskonflikt zu einer systemischen Konkurrenz um technologische Führerschaft, wirtschaftliche Resilienz und geopolitischen Einfluss. China reagiert mit seinem Exportkontrollgesetz, der Liste unzuverlässiger Unternehmen und sogenannten „Blocking“-Regeln.

6.3.2 ESKALATIONSSTUFE 1 - VERSCHÄRFTE COMPLIANCE UND VERGELTUNGSMAßNAHMEN

Die Beziehungen entwickeln sich von selektiver Trennung hin zu umfassenderen Compliance-Reibungen, was die operative Unsicherheit für ausländische Unternehmen erhöht, während Transaktionskosten deutlich steigen. „Dual Compliance“ wird zum Dauerzustand: Unternehmen müssen zunehmend parallel in unterschiedlichen regulatorischen und technologischen Ökosystemen operieren.

- Die USA erweitern Entity-List-Einstufungen und verschärfen Genehmigungs- sowie Überwachungsmaßnahmen entlang der Lieferketten für Chips, KI und Halbleiterausrüstung (vgl. Crosignani et al. 2024).
- China erhöht den Druck durch die Liste unzuverlässiger Unternehmen und Maßnahmen gegen extraterritoriale Vorschriften, wodurch Handels- und Investitionsrisiken steigen.
- China verschärft Exportgenehmigungen für strategische Materialien und nutzt Einzelfallentscheidungen als Hebelinstrument.

Auswirkungskategorien: Cybersecurity, physische und wirtschaftliche Sicherheit, Geschäftsabläufe und Lieferketten, Belegschaft und Mitarbeitende.

6.3.3 ESKALATIONSSTUFE 2 - SYSTEMISCHE ENTKOPPLUNG UND KONFLIKTE UM STRATEGISCHE ENGPÄSSE

Die strategische Entkopplung verhärtet sich über zentrale Sektoren hinweg, da Technologie- und Kontrollmaßnahmen für kritische Vorprodukte auf zentrale industrielle Ökosysteme übergreifen. Kritische Mineralien werden zu einer zentralen Schwachstelle, wodurch Produktionsstörungen und Kostendruck entstehen.

- Die USA weiten sanktionierende Instrumente und Investitionsverbote aus und beschleunigen die finanzielle Fragmentierung.
- Anforderungen an „vertrauenswürdige Lieferanten“ und Beschaffung aus Partnerstaaten werden ausgeweitet; CHIPS-Regelwerke schränken Technologiepartnerschaften weiter ein.
- China erweitert Exportkontrollen auf seltene Erden und kontrollierte Materialien, wodurch das Risiko von Kaskadeneffekten und Engpässen in strategischen Sektoren steigt.

- Besonders betroffen wären Branchen mit hoher Abhängigkeit von Halbleitern, Batterietechnologien, Seltenen Erden, industrieller Automatisierung sowie KI-Anwendungen.
- Die Fragmentierung technologischer Systeme könnte auch zu divergierenden Satellitennavigations- und Kommunikationsstandards führen, was die operative Komplexität und Kosten für globale Logistik und datenintensive Branchen erhöht.

Auswirkungskategorien: Cybersecurity, physische und wirtschaftliche Sicherheit, Geschäftsabläufe und Lieferketten, Belegschaft und Mitarbeitende, Regierung und Recht, Finanzen und Handel.

6.3.4 ESKALATIONSSTUFE 3 - KRISENGETRIEBENE STRATEGISCHE ZÄSUR

Ein Vorfall in der Taiwanstraße löst eine schnelle Eskalation von Sanktionen und Exportkontrollen zwischen den USA und China aus, wodurch Lieferketten für KI-Rechenleistung und kritische Mineralien unterbrochen werden. Die EU gerät zwischen die Fronten und sieht sich mit Halbleiter- und Rohstoffengpässen sowie deutlich steigenden Compliance- und operativen Risiken konfrontiert.

Auswirkungskategorien: Technologie und Daten, Cybersecurity, physische und wirtschaftliche Sicherheit, Regierung und Recht, Geschäftsabläufe und Lieferketten, Kunden, Partner und Märkte, Belegschaft und Mitarbeitende.

6.3.5 WAS BEDEUTET DAS FÜR GLOBALE UNTERNEHMEN?

Unternehmen benötigen Betriebsmodelle, die auch unter konkurrierenden US- und chinesischen Compliance-Regimen funktionsfähig bleiben, insbesondere bei Technologie, kritischen Vorprodukten und grenzüberschreitenden Partnerschaften. Ebenso wichtig sind Frühwarnmechanismen, das Monitoring geopolitischer Triggerpunkte, belastbare Alternativen bei strategischen Materialien und eine stärker resilienzorientierte Steuerung.

6.4 Szenario 4 - Strategische Fragmentierung der transatlantischen Partnerschaft

Dieses Szenario skizziert, wie sich transatlantische Spannungen schrittweise von politischer Entfremdung und selektiver wirtschaftlicher Reibung zu einer strategischen Trennung in zentralen Bereichen wie Handel, Technologie und Verteidigung verdichten können. Im Vordergrund steht nicht die Auflösung der transatlantischen Partnerschaft, sondern die zunehmende Fragmentierung bislang eng integrierter Wirtschafts-, Technologie- und Sicherheitsräume. Die Frage der digitalen Souveränität wird hier zu einem zentralen Element der strategischen Neuausrichtung.

6.4.1 AUSGANGSLAGE (STAND DER ANALYSE: JUNI 2026)

Die Beziehungen zwischen den USA und der EU sind durch wachsendes Misstrauen und zunehmende strategische Divergenz belastet. Streitfragen in Handel, Technologie und

Sicherheit nehmen zu, während die EU ihre technologische Souveränität ausbaut und die USA ihre industrie- und sicherheitspolitischen Interessen offensiver absichern. Spannungen zeigen sich vor allem über Exportkontrollen, Compliance-Vorgaben und rechtliche Unsicherheiten bei Datenflüssen.

6.4.2 ESKALATIONSSTUFE 1 - WACHSENDE TRANSATLANTISCHE DIVERGENZEN UND REGULATORISCHE FRAGMENTIERUNG

Die Eskalation erfolgt überwiegend über regulatorische, technologische und wirtschaftspolitische Instrumente und weniger über offene politische Konfrontationen - getrieben durch strengere Beschaffungsrichtlinien, KI-bezogene Exportkontrollen und gesetzliche Vorgaben zu Datenströmen.

- **Technologie:** selektive und symbolische Einschränkungen entstehen; die USA führen Drosselungen oder bedingten Zugang zu bestimmten Dienstleistungen ein.
- **Handel:** politische Spannungen nehmen zu, aber Lieferketten bestehen fort, während die Wettbewerbsfähigkeit der EU durch Energiekosten geschwächt wird.
- **Verteidigung:** erste Spannungen innerhalb der NATO werden sichtbar, da Mitgliedstaaten beginnen, Ausrichtung und langfristige Verpflichtungen zu hinterfragen.

Auswirkungskategorien: Cybersecurity, physische und wirtschaftliche Sicherheit, Geschäftsabläufe und Lieferketten, Technologie und Daten, Regierung und Recht.

6.4.3 ESKALATIONSSTUFE 2 - STRATEGISCHE TRENNUNG IN SCHLÜSSELBEREICHEN

Die divergierenden Narrative verfestigen sich in politischer Praxis. Europa beschleunigt Souveränitätsbestrebungen, liegt jedoch hinter den US-Fähigkeiten zurück, was Leistungsunterschiede und interne Fragmentierung verstärkt.

- **Technologie:** regulierungspflichtige Systeme verlagern sich auf souveräne EU-Technologie-Stacks, während KI-Rechenkapazitäten aufgeteilt werden, um Risiken durch Exportkontrollen zu adressieren.
- **Handel:** die Entkopplung konzentriert sich auf durchsetzbare Engpässe (z. B. digitale Zollprozesse) statt auf eine vollständige Marktabschottung.
- **Verteidigung:** die US-Truppenpräsenz in Europa sowie die Intensität des nachrichtendienstlichen Austauschs könnten reduziert oder stärker an politische Bedingungen geknüpft werden. Dies könnte auch den Zugang zu kritischen Satelliteninformationen für Unternehmen, die in Hochrisikoregionen tätig sind, einschränken, was Sicherheitsbewertungen und die operative Planung beeinträchtigen und Unternehmen zwingen würde, in alternative Informationsquellen zu investieren.

Auswirkungskategorien: Cybersecurity, physische und wirtschaftliche Sicherheit, Geschäftsabläufe und Lieferketten, Technologie und Daten, Regierung und Recht, Kunden, Partner und Märkte.

6.4.4 ESKALATIONSSTUFE 3 - TIEFGREIFENDE TRANSATLANTISCHE FRAGMENTIERUNG

Ein isolierter Schock eskaliert die Beziehungen zwischen den USA und der EU rasch von kontrolliertem Wettbewerb zu einer offenen wirtschafts- und sicherheitspolitischen Konfrontation. Handels-, Daten- und Technologietransfers könnten erheblich eingeschränkt oder selektiv unterbrochen werden; die Verteidigungs- und Geheimdienstkooperation verliert deutlich an Intensität. Eingeschränkter Zugang zu fortgeschrittener US-Technologie zwingt europäische Unternehmen zur Nutzung regionaler Technologie-Stacks, wodurch Kosten, Komplexität und operative Risiken steigen. Dieses Szenario würde zu höheren F&E-Kosten, langsameren Innovationszyklen und einem potenziellen Verlust des globalen Wettbewerbsvorteils für europäische Unternehmen führen, während es gleichzeitig eine erhebliche Nachfrage nach in Europa entwickelter Software, Hardware und Cloud-Diensten schafft (vgl. Europäisches Parlament 2025). Die vollständige digitale Souveränität wird hier zur Notwendigkeit, um die technologische und wirtschaftliche Handlungsfähigkeit Europas zu sichern und Abhängigkeiten zu minimieren.

Auswirkungskategorien: Geschäftsabläufe und Lieferketten, Belegschaft und Mitarbeitende, Technologie und Daten, Regierung und Recht, physische, Cybersecurity und wirtschaftliche Sicherheit, Kunden, Partner und Märkte.

6.4.5 WAS BEDEUTET DAS FÜR GLOBALE UNTERNEHMEN?

Dieses Szenario verdeutlicht, dass geopolitische Risiken nicht zwangsläufig aus offenen Konflikten entstehen - bereits regulatorische Divergenzen, unterschiedliche Technologiepolitiken und selektive Marktbeschränkungen können erhebliche Auswirkungen auf globale Geschäftsmodelle entfalten. Unternehmen benötigen stärker regionalisierte Technologien, Daten- und Governance-Strukturen. Regionalisierung, technologische Diversifizierung und resilienzorientierte Governance-Strukturen gewinnen dadurch erheblich an Bedeutung. Die konsequente Umsetzung digitaler Souveränität wird hier zum Fundament für zukünftiges Wachstum und die Sicherung der Wettbewerbsfähigkeit in einem fragmentierten globalen Umfeld.

6.5 Gleichzeitigkeit und Kombination der Szenarien

Die vier Szenarien sind als Einzelszenarien beschrieben, schließen sich in der Realität aber nicht aus. Sie können gleichzeitig eintreten, sich gegenseitig auslösen oder verstärken; die Risikomultiplikatoren aus Modul 2, Kapitel 3, wirken dann über mehrere Szenarien hinweg. Beispiele zeigt die folgende Tabelle; die strategische Einordnung enthält das Strategische Whitepaper 02 (Kapitel 6). Ein eigenes Gesamtszenario wird bewusst nicht gebildet. Ein Stresstest sollte jedoch mindestens eine Kombination aus zwei

Szenarien prüfen; das Arbeitsblatt zu Beginn dieses Moduls lässt sich dafür unverändert nutzen.

Kombination	Typischer Verstärkungseffekt	Prüffrage für das Unternehmen
Aktuell: Ukraine-Krieg + Iran-Krieg/Hormus	Energie- und Logistikpreise steigen, während Verteidigungsbedarf Kapazitäten und Haushalte bindet.	Welche Kosten- und Lieferzusagen gegenüber Kunden sind dann noch haltbar?
1 + 2: Konflikt in Europa + Eskalation in der Taiwanstraße	Krisen in Europa und Asien binden westliche Kräfte gleichzeitig; Russland und China können die Krise des jeweils anderen für eigene Ziele nutzen (NATO 2024).	Sind wir auf den gleichzeitigen Ausfall von Bezugs- und Absatzmärkten in Osteuropa und Ostasien vorbereitet?
1 + 3: Konflikt in Europa + US-China-Entkopplung	Energie- und Rohstoffschocks treffen auf Exportkontrollen für Chips und seltene Erden.	Reichen Bestände und Zweitquellen, wenn Bezugsquellen in Europa und Asien zugleich ausfallen?
2 + 3: Taiwanstraße + Entkopplung	Halbleiterausfall und Sanktionsregime: Ersatzquellen sind knapp und zugleich rechtlich eingeschränkt.	Welche Produkte lassen sich ohne Chips aus Taiwan und China noch fertigen?
1 + 4: Konflikt in Europa + transatlantische Fragmentierung	Militärischer Druck bei eingeschränktem Zugang zu US-Technologie, Cloud-, Daten- und Satellitendiensten.	Funktionieren Kommunikation, Cloud und Lagebild auch ohne US-Dienste?

7 Schnittstelle Staat-Wirtschaft

Initiative Wirtschaftsschutz: zwischen Anspruch und Umsetzung

7.1 Was der Staat anbietet

Am 18.03.2026 hat das Bundeskabinett die vom Bundesministerium des Innern (BMI) vorgelegte Nationale Wirtschaftsschutzstrategie beschlossen (BMI 2026). Die strategische Einordnung findet sich im Strategischen Whitepaper 02, Kapitel 5; dieses Modul konzentriert sich auf das konkrete Leistungsangebot, die Lücken aus Unternehmenssicht und die praktische Nutzung.

Kernleistungen sind Warnungen und Lagebilder, Sicherheitshinweise, Informationsprodukte, branchenspezifische Gesprächskreise, regelmäßige Behördenbriefings sowie weiterentwickelte Single Points of Contact. Besonders KMU, Start-ups und Unternehmen ohne eigene Sicherheitsorganisation sollen einfacher erreicht werden - über Verbände, IHKs, digitale Formate, Plattformen und soziale Medien. Ergänzend baut der Staat Angebote zu Cyber- und Informationssicherheit, Business Continuity, Forschungssicherheit, hybriden Bedrohungen und physischer Unternehmensresilienz aus.

7.2 Was Unternehmen davon halten - und wo die Gaps liegen

Aus Sicht vieler Unternehmen ist die Nationale Wirtschaftsschutzstrategie ein wichtiger Schritt in die richtige Richtung. Besonders positiv bewertet wird, dass es nun einen ressortübergreifenden politischen Verantwortlichen für Wirtschaftsschutz gibt - genau eine solche Bündelung von Zuständigkeit, Priorisierung und politischer Sichtbarkeit wurde von der Wirtschaft seit Jahren gefordert.

Der zentrale Gap liegt weiterhin in der Fragmentierung staatlicher Leistungen. Trotz Fortschritten bleibt für Unternehmen häufig unklar, welche Behörde in welcher Lage zuständig ist, welche Informationen wohin gemeldet werden sollen und welche Reaktion realistisch erwartet werden kann. Das betrifft etwa Drohnensichtungen und Drohnenabwehr, zivil-militärische Zusammenarbeit, sicherheitsrelevante Vorfälle, hybride Lagebilder oder Meldewege zu Polizei, Verfassungsschutz, BSI, BBK, Bundeswehr und Landesbehörden.

Positiv ist, dass bestimmte Bedrohungsfelder zunehmend behördenübergreifend koordiniert werden - etwa im Gemeinsamen Terrorismusabwehrzentrum, im Gemeinsamen Extremismus- und Terrorismusabwehrzentrum, im Nationalen Cyber-Abwehrzentrum, im Gemeinsamen Drohnenabwehrzentrum und nun im Gemeinsamen Zentrum zur Abwehr hybrider Bedrohungen. Zugleich entsteht ein neues Problem: Die Zahl solcher Zentren, Plattformen und Gesprächsformate wächst schneller als ihre

Anschlussfähigkeit für die Wirtschaft. Für Unternehmen zählt am Ende nicht die interne Behördenlogik, sondern ein klarer Zugangspunkt, ein gemeinsames Lageverständnis und handlungsfähige Schnittstellen.

Besondere Bedeutung gewinnt zudem der amtliche Geheim- und Sabotageschutz angesichts hybrider Bedrohungen, verteidigungsnaher Lieferketten, Dual-Use-Technologien und sensibler Infrastrukturleistungen. Erforderlich ist eine Lösung, die Geheimschutz, Sabotageschutz, Wirtschaftsschutz und Unternehmensrealität zusammenführt - verbunden mit einem rechtssicheren Rahmen für Sicherheitsüberprüfungen und Pre-Employment-Screenings, der heute noch nicht ausreichend klar, schnell und praxistauglich ist.

7.3 Checkliste: Anforderungen der Wirtschaft an den Staat

Nutzen Sie die folgende Liste, um die eigene Interessenvertretung gegenüber Behörden sowie Verbänden zu schärfen:

- **Klare Zuständigkeiten schaffen:** eindeutige Ansprechpartner und transparente Verantwortlichkeiten - insbesondere bei Drohnen, hybriden Bedrohungen, zivil-militärischer Zusammenarbeit und sicherheitsrelevanten Vorfällen.
- **Einen zentralen Zugangspunkt etablieren:** statt vieler paralleler Zentren, Plattformen und Gesprächsformate braucht die Wirtschaft eine klare, handlungsfähige Schnittstelle zum Staat.
- **Strategie operationalisieren:** die Wirtschaftsschutzstrategie muss gemeinsam mit Sicherheitsverbänden und Unternehmen in konkrete Prozesse, Meldewege, Lagebilder und Unterstützungsangebote übersetzt werden.
- **Fragmentierung reduzieren:** staatliche Leistungen sollten besser gebündelt, abgestimmt und für Unternehmen einfacher nutzbar gemacht werden.
- **Informationsflüsse verbessern:** Unternehmen benötigen schnellere, praxisnahe und verwertbare Lageinformationen, Warnhinweise und Handlungsempfehlungen.
- **Rechtssicheren Informationsaustausch ermöglichen:** für den Austausch auch klassifizierter Informationen zwischen Staat und Wirtschaft braucht es eine belastbare rechtliche Grundlage, klare Verfahren, definierte Empfängerkreise und praktikable Schutzmechanismen.
- **KMU gezielt einbinden:** kleine und mittlere Unternehmen brauchen niedrigschwellige Angebote, einfache Meldewege und konkrete Unterstützung ohne hohe bürokratische Hürden.
- **Geheim- und Sabotageschutz praxisnah weiterentwickeln:** eng mit Wirtschaftsschutz und Unternehmenssicherheit verbunden halten.
- **Sicherheitsüberprüfungen modernisieren:** Verfahren müssen verlässlicher, schneller und besser auf sicherheitsrelevante Unternehmensfunktionen zugeschnitten werden.

- **Rechtssicherheit für Pre-Employment-Screenings schaffen:** ein klarer rechtlicher Rahmen, um sensible Funktionen, Schlüsseltechnologien und kritische Lieferketten angemessen zu schützen.
- **Partnerschaft auf Augenhöhe etablieren:** Staat und Wirtschaft sollten gemeinsam Lagebilder, Standards, Übungen und Krisenprozesse entwickeln - nicht nur punktuell konsultiert werden.

Was Sie intern vorbereiten sollten

- **Ansprechpartner benennen:** eine verantwortliche Person oder Funktion als Single Point of Contact für Sicherheitsbehörden und Verbände festlegen und eine aktuelle Liste der relevanten Melde- und Kontaktwege pflegen (BSI, BBK, Verfassungsschutz, Polizei, Landesbehörden, Branchenverbände).
- **Meldewege dokumentieren:** Meldewege für Cybervorfälle, Drohnensichtungen und Sabotageverdacht festlegen und einmal jährlich testen.
- **Bedarfe formulieren:** eigene Unterstützungsbedarfe konkret beschreiben und über Sicherheitsverbände gebündelt einbringen.
- **Personalsicherheit klären:** Kriterien und rechtlichen Rahmen für Sicherheitsüberprüfungen und Pre-Employment-Screenings mit Personal, Recht und Datenschutz abstimmen.
- **Austausch nutzen:** an behördlichen Lagebriefings, Gesprächskreisen und Übungen teilnehmen.

7.4 Die gemeinsame Vision

> *Wirtschaft und Staat verstehen sich als strategische Partner, die Bedrohungen frühzeitig gemeinsam erkennen, Lagebilder teilen, Zuständigkeiten klären und Reaktionsfähigkeit praktisch einüben. Der Staat bringt sicherheitsbehördliche Erkenntnisse, Koordinierungsfähigkeit und rechtliche Rahmenbedingungen ein; die Wirtschaft ergänzt operative Nähe, Kenntnis kritischer Prozesse, internationale Lieferketten und technologische Expertise. Ziel ist ein Wirtschaftsschutzsystem, das nicht erst im Krisenfall aktiviert wird, sondern dauerhaft Vertrauen, Austausch und gemeinsame Handlungsfähigkeit schafft.*

8 Regulatorik- und Umsetzungsfahrplan

OPLAN Deutschland und die europäische Regulierungslandschaft

Europa reguliert Resilienz zunehmend verbindlich, aber fragmentiert. CER, NIS-2, DORA, der Cyber Resilience Act und die EU-Lieferkettenrichtlinie (CSDDD) (Europäische Union 2022b; 2022a; 2022c; 2024a; 2024b) zeigen, dass (Cyber-)Sicherheit, Widerstandsfähigkeit, Produktsicherheit, kritische Infrastrukturen und Lieferketten zu zentralen Bestandteilen unternehmerischer Sicherheitsverantwortung werden. Gleichzeitig führen unterschiedliche Umsetzungsgeschwindigkeiten und nationale Konkretisierungen in den Mitgliedstaaten zu einem Flickenteppich an Anforderungen, der für international tätige Unternehmen zu zusätzlicher Komplexität, operativen Risiken und Wettbewerbsnachteilen führen kann. Die CSDDD wurde zudem durch die Omnibus-I-Richtlinie deutlich eingeschränkt: Sie gilt künftig nur für EU-Unternehmen mit mehr als 5.000 Beschäftigten und über 1,5 Mrd. Euro weltweitem Umsatz, ist bis 26.07.2028 umzusetzen und ab 26.07.2029 anzuwenden (Europäische Union 2026).

> *Wer europäische Regulierung nur reaktiv erfüllt, bleibt im Pflichtenkatalog gefangen. Wer sie als Signalgeber für geopolitische, operative und regulatorische Risiken versteht, kann daraus Orientierung, Robustheit und Handlungsfähigkeit gewinnen.*

8.1 Der Operationsplan Deutschland (OPLAN DEU)

Der Operationsplan Deutschland zielt darauf ab, im Spannungs- und Verteidigungsfall eine funktionierende Drehscheibe für militärische und zivile Logistik sowie Versorgung sicherzustellen (Bundeswehr / Operatives Führungskommando der Bundeswehr 2025; Bundeswehr 2023). Für die Wirtschaft ergeben sich daraus zwar konkrete Anforderungen - aktuell existiert jedoch kein veröffentlichter OPLAN für die Wirtschaft. Die Wirtschaft kann sich nicht auf etwas vorbereiten, was sie nicht kennt.

- Sicherstellung von Transport- und Logistikkapazitäten
- Schutz und Betrieb kritischer Infrastrukturen
- Bereitstellung von Dienstleistungen und Ressourcen
- Integration in Melde- und Kommunikationsstrukturen

In der strategischen Konzeption ist diese Einbindung klar adressiert. In der operativen Umsetzung zeigen sich jedoch Herausforderungen (Bundeswehr 2024): unterschiedliche Reifegrade in der Vorbereitung von Unternehmen, begrenzte Übungstiefe und praktische Erprobung, teilweise unklare Schnittstellen zwischen staatlichen Stellen und wirtschaftlichen Akteuren sowie fehlende Standardisierung von Prozessen und Abläufen.

> *Kernaussage: Der strategische Rahmen ist vorhanden, seine operative Durchdringung ist jedoch noch unvollständig.*

8.2 Regulatorischer Druck versus unternehmerischer Handlungsspielraum

Relevante Entwicklungen umfassen europäische Vorgaben zur Cyber- und Digitalresilienz (NIS-2, Cyber Resilience Act), nationale Regelwerke zum Schutz kritischer Infrastrukturen (KRITIS-Dachgesetz) sowie Anforderungen an Lieferketten-, Daten- und Technologiesouveränität (Europäische Union 2022a; Europäische Union 2024a; Die Bundesregierung 2026b). Diese Regulierung verfolgt das Ziel, Mindeststandards zu sichern und systemische Risiken zu reduzieren - erzeugt aber gleichzeitig steigenden Compliance-Aufwand, parallel laufende, teilweise überlappende Anforderungen, unterschiedliche Umsetzungsstände innerhalb Europas und Unsicherheiten bei Auslegung und Anwendung.

> *Kernaussage: Regulierung stärkt Resilienz punktuell, erzeugt jedoch gleichzeitig neue Komplexität und potenzielle Ineffizienzen (Einschätzung des ThinkTank; vgl. BSI 2026b; Die Bundesregierung 2026a).*

8.3 Neun Lücken im System - Selbstdiagnose

Wo sehen Sie Lücken in Ihrem eigenen Umfeld, bei Behörden, bei Verbänden, oder sogar intern im eigenen Unternehmen? (BBK 2024; Bundeswehr 2024; BSI 2026b)

Lücke	Beschreibung
Koordinationslücke	Parallel bestehende Strukturen und Zuständigkeiten ohne einheitliche Führung im Krisenfall.
Geschwindigkeitslücke	Diskrepanz zwischen staatlichen Entscheidungsprozessen und der Dynamik moderner Bedrohungen.
Umsetzungslücke	Strategien und Programme sind formuliert, ihre operative Durchdringung und Wirkung bleiben jedoch begrenzt.
Gesamtverteidigungslücke	Die Verzahnung von staatlichen, wirtschaftlichen und gesellschaftlichen Resilienzbeiträgen ist nicht vollständig konsistent integriert.
Digitale Souveränitätslücke	Hohe Abhängigkeit von externen Technologieanbietern bei gleichzeitig begrenzten europäischen Alternativen.
Bewusstseinslücke	Sicherheits- und Resilienzfragen sind in der Breite der Wirtschaft noch nicht flächendeckend als strategische Führungsaufgabe verankert.
Regulierungslücke	Zunehmende Regelwerke führen zu steigenden Anforderungen, erzeugen jedoch gleichzeitig Fragmentierung und Komplexität.
Plattformlücke	Es fehlt an integrierten, skalierbaren Plattformen für Lagebild, Koordination und Austausch zwischen Staat und Wirtschaft.
Strategische Operationalisierungslücke	Übergeordnete Resilienzvorstellungen und Zielbilder sind vorhanden, ihre konkrete operative Umsetzung bleibt jedoch oft unklar.

In ihrer Gesamtheit zeigen diese Punkte: Die Resilienzarchitektur ist vorhanden, aber nicht durchgängig operationalisiert, synchronisiert und wirksam integriert (Die Bundesregierung 2023; BBK 2024).

Diese neun Lücken lassen sich auf drei strukturelle Ursachen zurückführen: Steuerungs- und Integrationsdefizite (Koordinations-, Plattform-, Gesamtverteidigungs- und Strategische Operationalisierungslücke) (Die Bundesregierung 2025; BBK 2022), Geschwindigkeits- und Umsetzungsdefizite (Geschwindigkeits- und Umsetzungslücke) (Die Bundesregierung 2023; BBK 2024) sowie Souveränitäts- und Fähigkeitsdefizite (Digitale Souveränitäts-, Regulierungs- und Bewusstseinslücke) (Europäische Kommission 2023b; Europäische Kommission 2026; BSI 2026b). Entscheidend ist der systemische Effekt: Fehlende Koordination reduziert die Geschwindigkeit der Reaktion, geringe Geschwindigkeit verstärkt Umsetzungsprobleme, Abhängigkeiten erschweren eigenständige Handlungsfähigkeit, und fragmentierte Regulierung erhöht die Komplexität zusätzlicher Maßnahmen (BBK 2024; Bundeswehr 2024).

8.4 Implikationen für Unternehmen - konkrete Handlungsansätze

1. Aufbau eigener Lagebilder und Frühwarnsysteme - nicht auf durchgehend verlässliche staatliche Steuerung im Krisenfall vertrauen.
2. Eigenständige Sicherstellung kritischer Prozesse - Redundanzen und Notfallpläne, die ohne externe Koordination funktionieren.
3. Entwicklung unternehmensinterner Resilienzstrukturen unabhängig von staatlicher Steuerung - inklusive klarer interner Eskalationswege.

9 Markteintritt & Diversifizierung

Strategisch tragfähige Märkte im veränderten geopolitischen Umfeld

Nicht alle Märkte bieten unter den veränderten geopolitischen Bedingungen gleichermaßen Stabilität und Wachstumspotenzial. Fünf Regionen ragen als strategisch besonders attraktiv heraus.

9.1 EU-Binnenmarkt

Bleibt ein zentraler Anker - trotz regulatorischer Komplexität bietet er Rechtssicherheit, industrielle Tiefe und eine zunehmend souveränitätsorientierte Industriepolitik, die gezielt heimische Wertschöpfung stärkt.

9.2 Indien

Ist seit 2023 das bevölkerungsreichste Land der Welt (UN DESA 2024) mit wachsendem Binnenmarkt, ambitionierten Industrialisierungszielen und einer bewussten Positionierung als strategischer Akteur im geopolitischen Wettbewerb zwischen westlichen und aufstrebenden Machtzentren mit Fokus auf den eigenen wirtschaftlichen Vorteil. Auch die Feindseligkeiten zwischen Indien und Pakistan stellen einen hohen Unsicherheitsfaktor für die europäische Wirtschaft dar.

9.3 Südostasien (ASEAN)

Profitiert von Nearshoring-Effekten, jungen Bevölkerungen und dynamischen Mittelschichten, die neue Konsum- und Industriemärkte entstehen lassen (FDI-Zuflüsse 2024 rd. 226 Mrd. US-Dollar, getragen u. a. vom Umbau internationaler Lieferketten; ASEAN-Sekretariat/UNCTAD 2025).

9.4 Golfregion

Transformiert sich mit enormem Kapitaleinsatz von rohstoffbasierter zu wissensbasierter Wirtschaft (IMF 2025). Die Verbindung von Staatsfonds, Infrastrukturprogrammen und gezielter Ansiedlungspolitik schafft attraktive Bedingungen für international ausgerichtete Unternehmen. Seit 2026 ist die Region allerdings durch den Iran-Krieg, Angriffe auf Energieinfrastruktur am Golf und wiederholte massive Einschränkungen des Schiffsverkehrs durch die Straße von Hormus einem deutlich erhöhten Sicherheits- und Lieferrisiko ausgesetzt (Euronews 2026a).

9.5 Brasilien und Mercosur

Das Interims-Handelsabkommen zwischen der EU und dem Mercosur (Argentinien, Brasilien, Paraguay, Uruguay) wird seit dem 1. Mai 2026 vorläufig angewendet; Zölle auf EU-Waren werden schrittweise abgebaut (Die Bundesregierung 2026d). Brasilien als größte Volkswirtschaft der Region bietet einen großen Industrie- und Konsumgütermarkt, Rohstoffe und Potenzial für erneuerbare Energien. Offen bleiben die Prüfung des Abkommens durch den EuGH und die Zustimmung des Europäischen Parlaments; hinzu kommt die politische Volatilität einzelner Mitgliedsstaaten.

9.6 Checkliste: strukturelle Voraussetzungen für den Markteintritt

Die Erschließung dieser Märkte setzt strukturelle Voraussetzungen voraus, die vor jeder Markteintrittsentscheidung geprüft werden sollten:

- Infrastruktur - Verkehrs-, Energie- und Digitalinfrastruktur vor Ort
- Industrielle Reife - vorhandene Zulieferbasis und Fachkräfteverfügbarkeit
- Digitalisierungsgrad - Verwaltungs- und Genehmigungsprozesse
- Energieverfügbarkeit - Versorgungssicherheit und Kosten
- Regulierungsrahmen - Verlässlichkeit und Planungssicherheit für Investitionen

Diese Faktoren sind entscheidend für die Markteintrittsplanung und das operative Risikomanagement - und sollten in jede Standort- oder Diversifizierungsentscheidung einfließen, die aus Modul 4, Kapitel 5 (kritische Abhängigkeiten) oder Modul 5, Kapitel 6 (Szenario-Stresstest) abgeleitet wird.

10 Chancenfelder im Detail

Strategische Chancenfelder der kommenden Jahre

Aus dem geopolitischen Wandel entstehen nicht nur Risiken - er eröffnet zugleich substanzielle unternehmerische Chancenfelder, die in den kommenden Jahren erhebliche Investitionsvolumina auf sich vereinen werden. Welche Investitionsprogramme diese Felder tragen, beschreibt das Strategische Whitepaper 02 (Kapitel 7.3); die folgenden Abschnitte zeigen, wo Unternehmen konkret ansetzen können.

10.1 Verteidigung & Dual-Use

Der wachsende Bedarf an nationaler und kollektiver Sicherheit treibt Investitionen in ein breites Technologiespektrum: Software, Sensorik, Kommunikationssysteme, Drohnen- und Anti-Drohnen-Komponenten, Robotik, Elektronik, Cyber-Kapazitäten, Raumfahrtanwendungen sowie resiliente Energieversorgung für sicherheitskritische Infrastrukturen. Auch Maschinenbau, Automotive Electronics, Embedded Systems, Künstliche Intelligenz, sichere Netzwerke und Fertigungstechnik profitieren vom Aufbau verteidigungsindustrieller Kapazitäten. Das Dual-Use-Prinzip - die Doppelnutzbarkeit ziviler und militärischer Technologien - eröffnet insbesondere mittelständischen Technologieunternehmen neue Märkte jenseits klassischer Rüstungsstrukturen.

10.2 Infrastruktur & Energie

Der Transformationsdruck auf Energiesysteme und physische Infrastruktur ist enorm: Netze, Speichertechnologien, Flexibilitätslösungen, Elektrifizierungsinfrastruktur, Industrieeffizienz, Wasserstoffwirtschaft, Wärmelösungen sowie Resilienz-Engineering und standortnahe Energieverfügbarkeit bilden ein Investitionsspektrum, das auf Jahrzehnte ausgelegt ist. Gefragt sind integrierte Lösungsanbieter, die Planung, Bau, Betrieb, Digitalisierung und Absicherung von Infrastruktursystemen beherrschen - inklusive Services, Komponenten, Software und innovativer Finanzierungsmodelle.

10.3 Digitale Souveränität

Der politische und regulatorische Druck, kritische Digitaltechnologie unter europäischer Kontrolle zu halten, schafft einen Wachstumsmarkt für Lösungen rund um sichere Cloud- und Edge-Architekturen, Cybersecurity, OT-Sicherheit, Datenräume, vertrauenswürdige KI, Embedded Electronics, Halbleiteranwendungen und souveräne Betriebsplattformen. Besonders attraktiv ist dieses Feld dort, wo regulatorische Anforderungen, Sicherheitsbedarf und industrielle Anwendbarkeit zusammentreffen - eine Konstellation, die in Europa zunehmend zur Norm wird.

KI als Chancenfeld: Für Künstliche Intelligenz ergeben sich eigene Chancen: souveräne KI-Infrastruktur und Rechenkapazitäten in Europa, KI-gestützte Sicherheits- und Resilienzdienstleistungen (z. B. Lagebild, Lieferkettenmonitoring) sowie vertrauenswürdige, regelkonforme KI-Anwendungen für Industrie und Verwaltung, für die die KI-Verordnung der EU einen gemeinsamen Rechtsrahmen schafft (Europäische Union 2024c).

10.4 Regionale Wertschöpfung

Die intelligente Neuordnung von Produktions-, Service- und Liefernetzwerken entlang geopolitischer Realitäten ist mehr als Logistikoptimierung - sie ist strategische Positionierung. Europäische Kundennähe, regionale Zulieferung, lokale Servicefähigkeit, kurze Entscheidungswege und skalierbare Plattformen werden zu Wettbewerbsvorteilen, die klassische Kostenvorteile globaler Beschaffung zunehmend überwiegen.

> *Unternehmen, die Lieferfähigkeit, Sicherheitsstandard, regulatorische Konformität und Störungsresistenz systematisch in ihre Leistungsversprechen und Geschäftsmodelle integrieren, schaffen nachhaltige Differenzierung - unabhängig davon, welches geopolitische Szenario sich letztlich entfaltet.*

Literaturverzeichnis

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 (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).

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).

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).

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).

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 (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 (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 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 (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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

Abkürzungsverzeichnis

ASEAN	Association of Southeast Asian Nations
BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
BCM	Business Continuity Management
BfV	Bundesamt für Verfassungsschutz
BMI	Bundesministerium des Innern
BSI	Bundesamt für Sicherheit in der Informationstechnik
CER	Critical Entities Resilience (Richtlinie (EU) 2022/2557)
CSDDD	Corporate Sustainability Due Diligence Directive (Richtlinie (EU) 2024/1760)
DORA	Digital Operational Resilience Act (Verordnung (EU) 2022/2554)
ECFA	Economic Cooperation Framework Agreement (China-Taiwan, 2010)
EU	Europäische Union
F&E	Forschung und Entwicklung
FDI	Foreign Direct Investment (ausländische Direktinvestitionen)
IEA	International Energy Agency
IMF	International Monetary Fund
IP	Intellectual Property (geistiges Eigentum)
IPCC	Intergovernmental Panel on Climate Change
IT	Informationstechnik
KI	Künstliche Intelligenz
KMU	Kleine und mittlere Unternehmen
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)
OECD	Organisation for Economic Co-operation and Development
OPLAN DEU	Operationsplan Deutschland
OT	Operational Technology
THI	Technische Hochschule Ingolstadt
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**