



# THINKTANK CORPORATE RESILIENCE WHITEPAPER

---

**Wirtschaftliche Folgen hybrider Bedrohungen für Unternehmen und  
ihre Wertschöpfungsketten – Wie muss sich die Wirtschaft jetzt  
vorbereiten?**

**- Hybride Kriegsführung als strategische Herausforderung  
für die deutsche Wirtschaft -**

**VSW**  
Bundesverband

Dezember 2025



## **Vorwort**

### **Sicherheit als wirtschaftliche Rahmenbedingung**

Hybride Bedrohungen prägen zunehmend den unternehmerischen Alltag. Cyberangriffe, Sabotage, Desinformation und geopolitische Handelshemmnisse wirken direkt auf Geschäftsmodelle, Wertschöpfungsketten und strategische Entscheidungen. Sicherheit ist damit keine Randbedingung mehr, sondern eine zentrale wirtschaftliche Voraussetzung.

### **Verwundbarkeit vernetzter Volkswirtschaften**

Deutschland und Europa sind als exportorientierte, hochvernetzte Wirtschaftsräume besonders anfällig für Störungen. Geopolitische Eskalationen, Systemkonkurrenz und eine fragmentierte Weltwirtschaft haben die Planbarkeit von Märkten nachhaltig verändert. Angriffe auf kritische Infrastrukturen und wirtschaftsrelevante Spionage nehmen zu.

### **Vom Weckruf zur Strategie**

Der „Operationsplan Deutschland“ hat viele Unternehmen sensibilisiert. Punktuelle Reaktionen reichen jedoch nicht aus. Entscheidend ist die strategische Einordnung sicherheitsrelevanter Risiken: Was ist geschäftskritisch – und wie bleibt das Unternehmen dauerhaft handlungsfähig?

### **Sicherheit als Wettbewerbsfaktor**

Hybride Bedrohungen verursachen jährlich Schäden in dreistelliger Milliardenhöhe und beeinflussen Investitionen, Innovation und Wettbewerbsfähigkeit. Dennoch wird Sicherheit häufig noch als Kosten- oder Compliance-Thema behandelt – nicht als Faktor für Wertschöpfung und Unternehmenswert.

### **Resilienz als Führungsaufgabe**

Dieses Whitepaper betrachtet Sicherheit konsequent aus Sicht der Unternehmensführung. Resilienz wird als strategische Aufgabe verstanden, die Governance, Wertschöpfung und Entscheidungsstrukturen gleichermaßen betrifft.

### **Zusammenarbeit schafft Resilienz**

Resilienz entsteht nicht isoliert. Sie erfordert den strukturierten Austausch zwischen Wirtschaft, Staat und Sicherheitsbehörden sowie den Abbau von Silos und den Aufbau von Vertrauen.

## Ziel dieses Whitepapers

Das Whitepaper unterstützt Entscheidungsträgerinnen und Entscheidungsträger dabei, Resilienz systematisch als Wettbewerbs- und Wertschöpfungsfaktor zu verankern und Sicherheit strategisch zu steuern.

## Der ThinkTank Corporate Resilience und der VSW als Plattform der Verantwortung

An dieser Schnittstelle positionieren sich der **ThinkTank Corporate Resilience als Denkfabrik** und der **VSW Bundesverband als Netzwerk der Verantwortung**. Ziel ist es, Sicherheit 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

## 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“ entstanden und eng mit dem MBA-Programm **Strategy, Global Risk & Security Management** verbunden.

Initiiert wurde der ThinkTank von Sven Dawson, Florian Haacke, Alexander Klotz, Marco Mille, Johannes Strümpfel und Prof. Dr. Marc Knoppe, um C-Suite-Vertreter, Chief Security Officers und 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, Dr. Ing. h.c. F. Porsche 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), Florian Haacke (Dr. Ing. h.c. F. Porsche AG), Linda Joana Hagen (ProSiebenSat.1 Media SE), Reiner F. Hindel (Siemens AG), Thomas Kiele-Dunsche (Daimler Truck AG), Matthew Kish (Siemens AG), Gereon Klein (RWE AG), Alexander Klotz (BMW AG), Prof. Dr. Marc Knoppe (THI), Florian Mayer (Lidl Stiftung & Co. KG), Dr. Terry Daniel Meincke (Siemens AG), Marco Mille (Siemens AG), Kevin Pukat (Lidl Stiftung & Co. KG), Thomas Seisler (Dr. Ing. h.c. F. Porsche AG), Katharina Stocker (BMW AG), Johannes Strümpfel (Siemens AG & VSW Bundesverband), Victoria Ulbricht (Siemens AG), Steffi van den Broek (BMW AG), Stefan van de Wetering (Airbus Defence and Space GmbH)

**in Kooperation mit dem**

**VSW-Bundesverband und dem**

**Beirat MBA Strategy, Global Risk & Security Management der Technische Hochschule Ingolstadt.**

## Ihre Meinung ist uns wichtig!

### FAQ & Feedback zum Whitepaper

Die Herausforderungen hybrider Kriegsführung betreffen uns alle: Wirtschaft, Wissenschaft und Gesellschaft. Um gemeinsam tragfähige Lösungen zu entwickeln, möchten wir Ihre Perspektive einbeziehen.

Haben Sie Fragen oder Anregungen?

Nutzen Sie unseren Feedback-Fragebogen oder kontaktieren Sie direkt unseren Think-tank. 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](#)

# Inhaltsverzeichnis

|   |           |
|---|-----------|
| <b>Executive Summary .....</b>  | <b>8</b>  |
| <b>1 Operationsplan Deutschland im Kontext der Wirtschaft.....</b>  | <b>10</b> |
| 1.1 OPLAN Deutschland: Operationsplan der Bundeswehr für Landes- und Bündnisverteidigung.....                             | 10        |
| 1.2 Zivil-Militärische Zusammenarbeit (ZMZ): Strukturen zur Kooperation zwischen Wirtschaft, Behörden und Bundeswehr..... | 10        |
| 1.3 KRITIS: Kritische Dienstleister und Infrastrukturen mit besonderer Bedeutung für die Versorgung der Bevölkerung.....  | 10        |
| 1.4 Europäische Dimension.....  | 12        |
| 1.5 Zustimmungsfall, Spannungsfall, Verteidigungsfall und Bündnisfall .....   | 13        |
| 1.6 Unternehmensrollen im Kontext der Gesamtverteidigung.....   | 13        |
| <b>2 Szenarien – Auswirkung auf Geschäftsmodelle .....</b>  | <b>15</b> |
| 2.1 Hybride Bedrohungslage .....  | 15        |
| 2.2 Eskalationsdynamik und Risikoverlauf .....  | 16        |
| 2.3 Strategische Rolle Deutschlands.....  | 17        |
| 2.4 Handlungsimplicationen für Unternehmen .....  | 18        |
| <b>3 Strategische Handlungsfelder für Unternehmen – Kritische Erfolgsfaktoren....</b>                                     | <b>19</b> |
| 3.1 Energie & Rohstoffversorgung .....  | 19        |
| 3.2 Lieferketten & Logistik .....   | 20        |
| 3.3 Interne Infrastruktur .....   | 22        |
| 3.4 Länder- und Standortperspektive .....   | 23        |
| 3.5 Produkte und Dienstleistungen.....  | 24        |
| 3.6 Märkte & Kundenverhalten .....  | 26        |
| 3.7 Cyber, Kommunikations- und Betriebssysteme.....   | 27        |
| 3.8 Personal & Arbeitsfähigkeit .....   | 29        |
| 3.9 Recht & Governance - Staatliche Steuerung & Regulierung.....  | 30        |
| 3.10 Finanzen & Liquidität .....  | 32        |
| 3.11 Technologie & Innovation .....   | 34        |
| 3.12 Ökologie & Nachhaltigkeit .....  | 35        |
| 3.13 Internationale Verflechtungen & Geopolitik .....   | 37        |
| 3.14 Kooperation & Netzwerke.....   | 39        |
| 3.15 Krisenkommunikation - Kommunikationsmatrix (intern/extern) - Stakeholderkommunikation.....                           | 41        |
| 3.16 Monitoring & Frühwarnsystem.....   | 43        |

|          |  |           |
|----------|--|-----------|
| <b>4</b> | <b>Handlungsempfehlungen</b>   | <b>46</b> |
| 4.1      | Corporate Resilience Framework (CRF)                                       | 46        |
| 4.2      | Rolle von CEO & C-Suite  | 47        |
| 4.3      | Governance, Compliance & Operating Model                                   | 48        |
| 4.3.1    | Governance-Struktur  | 48        |
| 4.3.2    | Reporting & Resilienz-Dashboard  | 48        |
| 4.4      | Rolle von Corporate Security   | 50        |
| 4.4.1    | Strategische Aufgaben von Corporate Security                               | 50        |
| 4.4.2    | Operative Aufgaben von Corporate Security                                  | 51        |
| 4.5      | Resilienz-Maßnahmenprogramm  | 51        |
| 4.5.1    | Sofortprogramm (0-30 Tage)   | 51        |
| 4.5.2    | Stabilisierungsprogramm (30 – 180 Tage)                                    | 52        |
| 4.5.3    | Technische Resilienz   | 52        |
| 4.5.4    | Operative Resilienz (Lieferketten, Märkte, Ressourcen)                     | 53        |
| 4.5.5    | Kooperationen & Netzwerke  | 53        |
| <b>5</b> | <b>Branchenbeispiele im Kontext des OPLAN Deutschland</b>                  | <b>54</b> |
| 5.1      | Lebensmittelindustrie & Logistik   | 54        |
| 5.2      | Automobilindustrie   | 55        |
| 5.3      | Energiebranche   | 56        |
| 5.4      | Kultur & Medien  | 57        |
| 5.5      | Luft- und Raumfahrtindustrie   | 59        |
| 5.6      | Sicherheitsdienstleister & Private Security - Auswirkungen auf Unternehmen | 62        |
| <b>6</b> | <b>Zentrale Fragen der Industrie im Kontext des OP-Plan DEUTSCHLAND</b>    | <b>65</b> |
| 6.1      | Strukturelle Defizite  | 65        |
| 6.2      | Energieversorgung & Priorisierung  | 65        |
| 6.3      | Mobilmachung & Rechtlicher Rahmen  | 66        |
| 6.4      | Lieferketten, Märkte & Transport   | 66        |
| 6.5      | Cyber-Security & Informationslage  | 66        |
| 6.6      | Staatliche Inanspruchnahme, Haftung & Entschädigung                        | 67        |
| 6.7      | Kommunikation, Behörden & Governance                                       | 67        |
| 6.8      | KRITIS, Priorisierung & Schutz   | 67        |
| 6.9      | Regionale & Operative Umsetzung  | 68        |
| 6.10     | Ergänzende Grundsatzfragen   | 68        |

|  |           |
|--|-----------|
| <b>7 Ansprechpartner und Netzwerke .....</b>                           | <b>69</b> |
| <b>Anhang: Auszüge rechtlicher Rahmen &amp; Checklisten.....</b>       | <b>70</b> |
| Anhang 1: Personal und Arbeitsfähigkeit .....                          | 70        |
| Anhang 2: Governance.....  | 71        |
| Anhang 3: Finanzen & Liquidität.....                                   | 72        |
| Anhang 4: Checkliste Strategische Aufgaben von Corporate Security..... | 73        |
| Anhang 5: Checkliste Operative Aufgaben von Corporate Security .....   | 74        |
| <b>Literatur .....</b>   | <b>75</b> |
| <b>Abkürzungsverzeichnis .....</b>                                     | <b>79</b> |

## Executive Summary

Dieses Whitepaper analysiert die **ökonomische Dimension hybrider Bedrohungen** und deren Auswirkungen auf die Stabilität von Unternehmen, globalen Wertschöpfungsketten und kritischen Infrastrukturen. Es beleuchtet die betriebswirtschaftlichen, organisatorischen und unternehmensstrategischen Herausforderungen infolge dieser hybriden Kriegsführung. Der Operationsplan Deutschland (OPLAN DEU) ist ein Element der Rahmenrichtlinien für Gesamtverteidigung (RRGV) (BMI 2024) und steckt die regulatorischen Anforderungen im Kontext der zivilen- und militärischen Verteidigung ab. Der OPLAN DEU fokussiert hierbei auf drei<sup>1</sup> von sieben Säulen der Gesamtverteidigung und stellt das Bindeglied zwischen ziviler- und militärischer Verteidigung dar (BMI 2024).

Hybride Bedrohungen (Bundestag 2025a, 2025b, 2024a, 2024b, NATO 2025b, Sperling 2025) – eine orchestrierte Kombination aus militärischen, nicht-militärischen und wirtschaftlichen Instrumenten – haben sich zu einem **zentralen Risikofaktor für die Unternehmensresilienz und Wertschöpfung** europäischer Unternehmen entwickelt. Sie umfassen insbesondere:

- Cyberangriffe (z. B. Ransomware, Industriespionage, Angriffe auf ERP- und Produktionssysteme),
- Physische Störungen (z. B. Sabotage an Energie- und Logistiknetzen, Drohnenaktivitäten, Brand- und Stromanschläge),
- Spionage (z. B. Ausspähversuche, Innentäter, Drohnenüberflüge),
- Desinformation und ökonomische Einflussnahme zur Destabilisierung von Märkten, Mitarbeitenden und Gesellschaft.

Diese hybriden Operationen zielen auf die Erosion von Vertrauen, Stabilität und Versorgungssicherheit ab. Der **volkswirtschaftliche Schaden** durch Cyberangriffe, Wirtschafts- und Industriespionage sowie Sabotage wird allein in Deutschland auf **über 289 Milliarden Euro jährlich** geschätzt (Bitkom 2025).

Unternehmen sehen sich dadurch einer neuen Verantwortung ausgesetzt: Sie müssen ihre Abhängigkeiten, Verwundbarkeiten und kritischen Schnittstellen zu staatlicher Infrastruktur kennen, bewerten und absichern. Der OPLAN DEU definiert erstmals konkrete Erwartungen an die Wirtschaft – von der Sicherstellung kritischer Prozesse über logistische

---

<sup>1</sup> 3 Säulen OPLAN DEU: Zivile Verteidigung: 1.Unterstützung der Streitkräfte; Militärische Verteidigung: 2.Heimatschutz/ Nationale territoriale Verteidigung, 3.Operationsbasis/ Drehscheibe Deutschland

Unterstützung bis zur Cyber- und Kommunikationssicherheit im Spannungs- und Verteidigungsfall.

### Zentrale Handlungsfelder der Wirtschaft

- **Cyber- und Lieferkettenresilienz stärken**  
Diversifizierung von Energie-, Rohstoff- und Logistikbeziehungen zur Reduktion geopolitischer Abhängigkeiten; Aufbau redundanter IT- und Kommunikationssysteme; regelmäßige Schwachstellenanalysen und Stresstests.
- **Hybride Bedrohungen im Risikomanagement verankern**  
Systematische Integration hybrider Szenarien in Risiko- und Business-Continuity-Management (BCM); Modellierung indirekter Abhängigkeiten (z. B. Cloud-Dienstleister, KRITIS-Betreiber).
- **Kooperation und Zivil-Militärische Zusammenarbeit (ZMZ)**  
Institutionalisierung gemeinsamer Frühwarnsysteme, Lagebilder und Krisenmechanismen zwischen Wirtschaft, Bundeswehr, Behörden und Branchenverbänden; aktive Vorbereitung auf Unterstützungsanforderungen nach OPLAN DEU.
- **Governance- und Compliance-Strukturen anpassen**  
Ausrichtung auf EU- und NATO-Rahmenwerke (NIS2, Cyber Resilience Act, Strategic Compass, Military Mobility); Aufbau eines unternehmensweiten Resilienz-Governance-Frameworks.

### Wirtschaftliche Verantwortung in der Gesamtverteidigung

**Die Resilienz der Wirtschaft ist heute nicht nur eine betriebswirtschaftliche, sondern eine sicherheitspolitische Kernaufgabe.** Unternehmen übernehmen eine aktive Rolle in der gesamtstaatlichen Sicherheitsarchitektur, indem sie kritische Dienstleistungen, Infrastruktur und Know-how auch unter Krisenbedingungen aufrechterhalten.

Dieses Whitepaper gibt Anregungen, wie Unternehmensleitungen ihre Organisationen auf die Eskalationsstufen „Hybride Kriegsführung, Zustimmung-, Spannungs-, Verteidigungs- und Bündnisfall“ vorbereiten, wie sie operative Kontinuität und rechtliche Konformität sichern – und wie **Resilienz als strategischer Wettbewerbsfaktor** etabliert werden kann.

Nur durch gezielte Investitionen in Resilienz, Kooperation und Prävention bleibt die deutsche und europäische Wirtschaft auch unter den Bedingungen hybrider Bedrohungen handlungsfähig. **Resilienz ist damit kein Kostenfaktor, sondern ein zentraler Wertschöpfungstreiber im Zeitalter der systemischen Unsicherheit.**

# 1 Operationsplan Deutschland im Kontext der Wirtschaft

## 1.1 OPLAN Deutschland: Operationsplan der Bundeswehr für Landes- und Bündnisverteidigung.

Der OPLAN DEU, der nicht öffentlich verfügbar ist und als Verschlussache gilt, bildet ein zentrales militärische Element für die Landes- und Bündnisverteidigung. Er definiert die operative Verzahnung zwischen den militärischen Kräften der Bundeswehr und den zivilen Unterstützungsstrukturen des Staates und der Wirtschaft (BMI 2024).

Deutschland nimmt dabei eine Drehscheibenrolle innerhalb Europas ein: Im Verteidigungs- oder Bündnisfall müssen innerhalb von sechs Monaten bis zu 800.000 alliierte Soldaten und rund 200.000 Fahrzeuge über deutsches Territorium verlegt, versorgt und geschützt werden. Dies erfordert eine enge Kooperation zwischen staatlichen Institutionen, Bundeswehr, Wirtschaft und Zivilgesellschaft – insbesondere in den Bereichen Transport, Energie, Logistik, Instandhaltung, Kommunikation, medizinische Versorgung und Recht.

Der OPLAN DEU markiert damit eine neue Phase gesamtstaatlicher Verteidigungsplanung, in der zivile Resilienz als Teil der nationalen Sicherheit verstanden wird.

## 1.2 Zivil-Militärische Zusammenarbeit (ZMZ): Strukturen zur Kooperation zwischen Wirtschaft, Behörden und Bundeswehr.

Die Zivil-Militärische Zusammenarbeit (ZMZ) – international als *Civil-Military Cooperation (CIMIC)* bezeichnet – beschreibt die systematische Kooperation zwischen Bundeswehr, Behörden, Wirtschaft und Zivilgesellschaft (BBK 2025c, BMVg 2023, Grünbuch 2025). Im Frieden konzentriert sich ZMZ auf Katastrophenhilfe und Unterstützung der zivilen Infrastruktur (z. B. Hochwasserhilfe, technische Unterstützung). Im Spannungs-, Verteidigungs- oder Bündnisfall hingegen dient sie der Unterstützung der Streitkräfte zur Erfüllung ihres militärischen Auftrags, etwa durch Bereitstellung von Ressourcen, Logistik oder Personal.

**Für Unternehmen bedeutet dies**, dass sie im Krisenfall zu Partnern der staatlichen Sicherheitsarchitektur werden – mit klar definierten Aufgaben, Meldewegen und Prioritäten.

## 1.3 KRITIS: Kritische Dienstleister und Infrastrukturen mit besonderer Bedeutung für die Versorgung der Bevölkerung.

Kritische Infrastrukturen (KRITIS) sind Einrichtungen und Unternehmen, deren Ausfall oder Beeinträchtigung zu erheblichen Versorgungsengpässen, Störungen der öffentlichen Sicherheit oder wirtschaftlichen Schäden führen würde (BBK 2025a, 2025b, 2021).

Dazu zählen insbesondere Sektoren wie Energie, Wasser, Ernährung, Transport, Informationstechnologie, Gesundheit, Finanzen, Verwaltung und Medien.

KRITIS-Betreiber<sup>2</sup> stehen im Fokus hybrider Bedrohungen und militärischer Planungen. Sie gelten als erste Ziele möglicher Sabotageakte oder Cyberangriffe, da ihre Lähmung unmittelbare Auswirkungen auf die gesellschaftliche und militärische Handlungsfähigkeit hätte. Dementsprechend ist ihre Resilienz gesetzlich verpflichtend, u. a. durch das IT-Sicherheitsgesetz 2.0, die NIS2-Richtlinie und den EU-Cyber Resilience Act (BMI 2023b, BSI 2024; EU-Commission 2025, 2022a, 2022b).

KRITIS ist in 10 Sektoren eingeteilt und bildet die Grundlage von Staat und Wirtschaft zum Schutz Kritischer Infrastrukturen:



Sektoren und Branchen KRITIS (BBK 2025b)

<sup>2</sup> Ein Unternehmen oder eine Organisation, die eine Kritische Infrastruktur (KRITIS) betreibt und damit für die Versorgung der Bevölkerung mit lebenswichtigen Gütern und Dienstleistungen verantwortlich ist (BBK 2025a).

## 1.4 Europäische Dimension

Der OPLAN DEU ist fest eingebettet in die europäische Sicherheitsarchitektur und ergänzt die strategischen Initiativen der NATO und der Europäischen Union. Zentrale Referenzrahmen sind der EU Strategic Compass, die NIS2-Richtlinie, der Cyber Resilience Act sowie das Programm Military Mobility (EU-Commission 2025, 2022a, 2022b; NATO 2025a, 2024). Diese Instrumente verdeutlichen:

- Resilienz wird europäischer Standard. Sicherheits- und Meldepflichten werden EU-weit harmonisiert.
- Energie- und Rohstoffströme werden im Krisenfall supranational koordiniert.
- Transportkorridore können militärisch priorisiert oder temporär umgewidmet werden.
- Industrie wird sicherheitspolitischer Akteur – insbesondere durch Dual-Use-Technologien und Rüstungskooperationen.

### **Damit wird deutlich:**

Die europäische Wirtschaft ist künftig integraler Bestandteil einer Gesamtverteidigungspolitik, die Sicherheit, Wettbewerbsfähigkeit und Nachhaltigkeit strategisch miteinander verknüpft (Bafa 2021, BMI 2024, EU-Commission 2025).

## 1.5 Zustimmungsfall, Spannungsfall, Verteidigungsfall und Bündnisfall

Zur Einordnung und Erklärung von Zustimmungsfall, Spannungsfall, Verteidigungsfall und Bündnisfall gibt die nachfolgende Tabelle einen kurzen Überblick.

|                      | Zustimmungsfall<br>(Art. 80a GG)   | Spannungsfall<br>(Art. 80a GG)  | Verteidigungsfall<br>(Art. 115a GG)   | Bündnisfall<br>(NATO Art. 5 /<br>Art. 87a GG)                     |
|----------------------|--|---|---|---|
| Auslöser             | Einfache Mehrheit im Bundestag; Aktivierung einzelner Sicherstellungsbefugnisse. | Bedrohung der BRD; Feststellung mit Kanzlermehrheit.                        | Militärischer Angriff auf BRD oder deutsche Truppen im Ausland; schwerer Terror- oder Cyberangriff. | Angriff auf NATO-Mitglied löst Beistandspflicht aus.              |
| Mehrheitserfordernis | Einfache Mehrheit  | Kanzlermehrheit   | Zweidrittelmehrheit Bundestag + Zustimmung Bundesrat  | NATO-Beschluss (national politisch bestätigt)                     |
| Rechtsfolgen         | Aktivierung einzelner Sicherstellungsbefugnisse.                                 | Vollständige Aktivierung Sicherstellungsgesetze; mögliche Wehrpflicht.      | Universelle Wehrpflicht; erweiterte Exekutivbefugnisse.   | Militärische oder zivile Unterstützung des angegriffenen Staates. |
| Typische Anlässe     | Politische Krisen, internationale Entwicklungen.                                 | Drohende militärische Konflikte oder staatliche/terroristische Bedrohungen. | Angriff auf BRD oder deutsche Kräfte; Terror- oder Cyberangriffe.                                   | Angriff auf NATO-Partner durch Staat oder Terrororganisation.     |

## 1.6 Unternehmensrollen im Kontext der Gesamtverteidigung

Unternehmen übernehmen im Spannungs- und Verteidigungsfall eine aktive Funktion innerhalb der gesamtstaatlichen Sicherheitsarchitektur.

Ihre Aufgaben gehen weit über Krisenmanagement hinaus und reichen von der Versorgungssicherung bis zur Unterstützung militärischer und ziviler Strukturen.

Zentrale Rollen sind:

- **Aufrechterhaltung** kritischer Prozesse und Dienstleistungen (z. B. Energie, Produktion, Versorgung).
- **Bereitstellung** logistischer, technischer und personeller Kapazitäten für militärische und zivile Zwecke.

- **Mitwirkung an Cyberabwehr und Kommunikationssicherheit**, insbesondere zum Schutz von Unternehmens- und Kundennetzwerken.
- **Unterstützung der Zivilgesellschaft**, etwa durch Versorgung, Unterkünfte oder technische Hilfe.

## Fazit

Unternehmen werden zu **systemrelevanten Partnern im nationalen Resilienzverbund** – an der Schnittstelle von Wirtschaft, Staat und Gesellschaft. Dies erfordert eine vorausschauende Planung, klare Zuständigkeiten und eine regelmäßige Abstimmung mit Behörden, Kammern und der Bundeswehr. Darauf muss sich die Wirtschaft vorbereiten, denn bereits die **aktuelle Lage hybrider Bedrohungen** verschärft nicht nur das globale Wettbewerbsumfeld, sondern **gefährdet auch die deutsche und europäische Wettbewerbsfähigkeit** – insbesondere in Bezug auf Wertschöpfungsketten, Lieferfähigkeit und Innovationskraft.

Damit dies gelingt, **braucht es Investitionsanreize**, staatliche Förderprogramme und klare regulatorische Rahmenbedingungen, die Resilienz nicht als zusätzliche Belastung, sondern als **strategische Zukunftsaufgabe und Innovationschance** begreifen. Gleichzeitig ist die **Politik vielerorts noch zu weit von der Realität und den Handlungszwängen der Unternehmen entfernt**, wodurch notwendige Entscheidungen verzögert oder unzureichend getroffen werden. Wirtschafts- und Sicherheitspolitik müssen daher zusammen gedacht werden: **Resiliente Unternehmensstrukturen sind heute ebenso ein sicherheits- wie ein industriepolitisches Ziel.**

Es gilt, die technologische Führungsrolle sowie die wirtschaftliche Stärke Deutschlands und Europas nicht nur aus unternehmerischer Perspektive zu sichern, sondern auch im Interesse der europäischen Sicherheit, Stabilität und Unabhängigkeit.

## 2 Szenarien – Auswirkung auf Geschäftsmodelle

### 2.1 Hybride Bedrohungslage

Die europäische Sicherheitsarchitektur steht vor einer dauerhaften Belastungsprobe und befindet sich in einer sicherheitspolitischen Übergangsphase, die durch hybride Bedrohungen, geopolitische Spannungen und eine zunehmende Verflechtung von zivilen und militärischen Aufgaben gekennzeichnet ist. Deutschland gilt dabei aufgrund seiner wirtschaftlichen Bedeutung und zentralen Lage als **Schlüsselziel hybrider Einflussnahmen** (EU-Commission 2023, Sperling 2025) .

Hybride Aktivitäten – darunter Wegwerfagenten, Ausspähversuche, Cyberangriffe auf staatliche und industrielle Ziele, gezielte Desinformationskampagnen, Drohnenüberflüge über kritische Infrastruktur, Industriespionage und Spionage durch verdeckte Agentennetze – sind inzwischen Bestandteil einer kontinuierlichen Einflussstrategie Russlands gegen Deutschland und seine europäischen Partner (Edwards & Seidenstein 2025, NATO 2025b, Sperling 2025).

**Das Ziel:** die Destabilisierung westlicher Gesellschaften und wirtschaftlicher Strukturen (BfV 2025a, 2025b), die Erosion gesellschaftlicher Kohäsion und die Schwächung politischer Entscheidungsfähigkeit sowie die Beeinträchtigung wirtschaftlicher Stabilität, ohne die Schwelle eines offenen Konflikts zu überschreiten.

Die Bundeswehr und ihre Partnerinstitutionen gehen von einer Vier-Stufen-Systematik aus: Frieden – Hybride Kriegsführung – Krise – Krieg (BMVg 2023).

Nach Einschätzung der Bundesregierung und führender Nachrichtendienste befindet sich Deutschland „nicht mehr im Frieden, aber noch nicht im Krieg“, sondern im Stadium einer hybriden Bedrohungslage (Bundeskanzleramt 2023; BfV 2025a, 2025b) – der oben beschriebenen Phase der militärisch-hybriden Intensivierung (Bundeskanzleramt 2023; BMVg 2023, Hartmann 2025, Grünbuch ZMZ 4.0 2025).

Europäische Nationen und die NATO reagieren auf diese Bedrohung mit verstärkten Abschreckungsmaßnahmen, erhöhten Verteidigungsausgaben, militärischer Modernisierung und erweiterten gemeinsamen Übungen. Deutschland leistet hierbei einen signifikanten Beitrag, indem es seine Cyberabwehr stärkt, Fähigkeiten zur Abwehr hybrider Bedrohungen ausbaut und seine Verteidigungsbudgets erhöht (Sperling 2025). Russische Geheimdienste intensivieren derweil ihre Spionageaktivitäten, um kritische Infrastrukturen und verteidigungsrelevante Einrichtungen zu identifizieren und für potenzielle Sabotageakte vorzubereiten (BfV 2025b). Diese kontinuierliche Eskalationsspirale in der Grauzone der hybriden Kriegsführung erfordert von den europäischen Nationen und insbesondere auch von den europäischen Unternehmen die Entwicklung neuer Abwehrmaßnahmen (EEAS 2024).

Die inhärente Gefahr dieser " Militärisch-Hybriden Intensivierung" liegt in ihrem Risiko, einen schleichenden Übergang zu einem weiteren Szenario 2: Militärische Eskalation, einem russischen Angriff auf ein NATO-Gebiet, zu initiieren. Eine persistente Belastung

durch hybride Operationen kann zu einer Degradation der kollektiven Widerstandsfähigkeit und einer wahrgenommenen Fragmentierung der europäischen Sicherheitsallianzen führen (Kather 2024). Es könnte zu einer internen Zerrüttung der NATO durch den Austritt von Mitgliedstaaten wie der Slowakei und Ungarn kommen, was eine gefährliche Sicherheitslücke in Zentraleuropa schaffen würde. In einem solchen Kontext würden die derzeitigen hybriden Operationen nicht mehr primär der Störung dienen, sondern auf eine Maximierung der Zerstörung und **die gezielte Lahmlegung kritischer Infrastrukturen in Deutschland und anderen NATO-Ländern** (Metis 2024, Edwards & Seidenstein 2025).

Ein Übergang zu Szenario 2 würde die Eskalation von der hybriden Kriegsführung zu einer konventionellen militärischen Konfrontation bedeuten, beispielsweise durch eine koordinierte Militäroperation in den baltischen Staaten, die darauf abzielt, den strategisch wichtigen Suwalki-Korridor zwischen Litauen und Polen zu erobern. Dies würde eine direkte Bedrohung für das NATO-Territorium darstellen und den "Bündnisfall" auslösen (Pöhlmann 2025).

**Für Unternehmen resultiert daraus** eine strukturelle Gefährdung ihrer gesamten Wertschöpfungsketten, da hybride Angriffe nicht nur operative Engpässe und Qualitätsverluste verursachen, sondern auch strategische Vermögenswerte wie Innovationsfähigkeit, Marktpositionen und geistiges Eigentum nachhaltig beeinträchtigen können.

## 2.2 Eskalationsdynamik und Risikoverlauf

Die Strategie der „militärisch-hybriden Intensivierung“ nutzt gezielt die „Grauzone“ zwischen Frieden und Krieg, um westliche Systeme zu überlasten.

Zu den beobachtbaren Mustern zählen:

- Cyber- und Informationsoperationen, die gezielt Unternehmensnetzwerke und Lieferketten adressieren (BSI 2024).
- Physische Sabotageakte gegen Energie-, Transport- oder Kommunikationsinfrastrukturen.
- Manipulation von Märkten und Desinformation, um öffentliche Meinung und Investitionsentscheidungen zu beeinflussen.
- Zielgerichtete Angriffe auf Resilienzstrukturen, z. B. auf Sicherheitsbehörden oder Forschungszentren.

Die Gefahr besteht im schleichenden Übergang von dieser hybriden Phase zu einer offenen militärischen Eskalation, etwa durch Zwischenfälle an der NATO-Ostflanke (SWP 2025, 2024). Ein Angriff auf NATO-Gebiet würde nach Artikel 5 des Nordatlantikvertrags den Bündnisfall auslösen und Deutschland unmittelbar in die operative Gesamtverteidigung einbinden (Metis 2024, NATO 2025a, 2024).

## 2.3 Strategische Rolle Deutschlands

Als größte europäische Volkswirtschaft und logistische Drehscheibe der NATO trägt Deutschland im Ernstfall eine **zentrale operative Verantwortung** (BMI 2024).

Diese Rolle **wirkt sich unmittelbar auf die Industrie aus** – insbesondere auf Unternehmen mit kritischer Infrastruktur, verteidigungsrelevanter Produktion oder transnationalen Lieferketten.

### **Folgende ökonomische Auswirkungen sind zu erwarten:**

- Erhöhte Nachfrage nach sicherheitsrelevanten Gütern (z. B. Energie, Logistik, Kommunikation, IT-Sicherheit).
- Engpässe und Unterbrechungen in globalen Lieferketten durch militärische Priorisierung oder Sanktionen.
- Stärkere Regulierung und rechtliche Verpflichtungen zur Unterstützung staatlicher Verteidigungsaufgaben.
- Wachsende Bedrohungslage im Cyber-Raum, einschließlich Angriffen auf industrielle Steuerungssysteme und Cloud-Infrastrukturen.
- Reputations- und Marktveränderungen durch gesellschaftliche Polarisierung oder Fehlinformation.

Diese **Faktoren beeinflussen direkt Geschäftsmodelle**, Marktstrategien und Investitionsentscheidungen. Unternehmen müssen die Schnittstelle zwischen Wirtschaft und Sicherheitspolitik aktiv in ihre strategische Planung integrieren.

Diese umfassende Mobilisierung und die damit verbundenen logistischen und sicherheitspolitischen Anforderungen hätten weitreichende Konsequenzen für deutsche Unternehmen. Sie wären direkt betroffen durch eine erhöhte Nachfrage nach bestimmten Gütern und Dienstleistungen, stünden aber auch vor verschärften Sicherheitsanforderungen, potenziellen Lieferkettenstörungen und einer Zunahme von Cyberbedrohungen, was aktuell bereits täglich zu verzeichnen ist (Bundeswehr 2025).

Die fortgesetzte und präzise Analyse dieser Übergangsphasen ist daher von kritischer Bedeutung für die Risikobewertung und die Entwicklung adäquater Präventions- und Reaktionsstrategien. Es ist von entscheidender Bedeutung, die Mechanismen und Indikatoren dieser potenziellen Eskalation genau zu verstehen.

## 2.4 Handlungsimplicationen für Unternehmen

Die **fortgesetzte Eskalation hybrider Bedrohungen** erfordert von der **Wirtschaft eine Neubewertung von Risiko- und Resilienzmanagement** im Kontext der individuellen Wertschöpfung.

Folgende strategische Implikationen sind zentral:

- **Integration von Sicherheits- und Resilienzstrategien** in Unternehmensgovernance- und ESG-Strukturen.
- **Aufbau widerstandsfähiger Lieferketten** mit regionalen Redundanzen („Dual Sourcing“, Nearshoring).
- **Erhöhung der Cyber-Resilienz** durch Segmentierung, Notfallübungen und Abstimmung mit BSI, CERT-Bund und Behörden.
- **Einrichtung von Frühwarn- und Lagebildsystemen** zur Erkennung geopolitischer und wirtschaftlicher Risiken.
- **Stärkere Vernetzung mit staatlichen Strukturen** (ZMZ, IHK, KRITIS-Cluster) für Krisenreaktionen.

Unternehmen, die frühzeitig entsprechende Governance- und Sicherheitsmechanismen implementieren, schaffen einen entscheidenden Wettbewerbsvorteil: **Resilienz wird zum ökonomischen Erfolgsfaktor.**

## 3 Strategische Handlungsfelder für Unternehmen – Kritische Erfolgsfaktoren

### 3.1 Energie & Rohstoffversorgung

#### Relevanz

Energie ist die zentrale Voraussetzung für Produktion, Logistik sowie Kommunikation – und damit Rückgrat jeder industriellen Wertschöpfung. Im Spannungs- oder Verteidigungsfall können staatliche Eingriffe, Rationierungen, Priorisierungen oder Sabotageakte erhebliche Auswirkungen auf die Unternehmenshandlungsfähigkeit haben. Deutschland bleibt in hohem Maße abhängig von importierten Energieträgern und kritischen Rohstoffen; zugleich gelten Energie- und Rohstoffströme als strategische Zielobjekte hybrider Einflussnahme (BMWK 2024a, 2024b; BNetzA 2025, 2024).

#### Zentrale Risiken

- Versorgungsunterbrechungen: Blackouts, Cyber-Angriffe, physische Sabotage oder Ausfall von Umspannwerken und Pipelines.
- Rationierungen & staatliche Priorisierungen: Energieträger und Treibstoffe werden für Streitkräfte, KRITIS-Sektoren und Behörden priorisiert.
- Abhängigkeit von Importen: Verwundbarkeit durch geopolitische oder logistische Engpässe (Gas, Öl, seltene Erden, Metalle).
- Kosten- und Preisrisiken: Volatile Märkte, Transportkostensteigerungen.
- Fehlende Resilienz in der Eigenversorgung: Unzureichende Redundanzen, fehlende Notstrom- oder Speicherkapazitäten.

#### Strategische Ziele

- Aufrechterhaltung der Betriebs- und Produktionsfähigkeit durch belastbare Energie- und Rohstoffversorgung in Krisen- und Verteidigungslagen.
- Reduktion von Abhängigkeiten durch Aufbau alternativer, regionaler und dezentraler Energiequellen.
- Sicherstellung der Energieversorgung kritischer Systeme (IT, Kommunikation, Sicherheit, Produktion).
- Frühzeitige Einbindung in nationale Versorgungsprioritäten und Zuteilungsmechanismen (BMWE, BNetzA, ZMZ).
- Schutz der eigenen Energieinfrastruktur vor physischen und Cyber-Angriffen.
- Integration von Energie-Resilienz in Business Continuity und Krisenmanagement.

## Kritische Maßnahmen & Governance

- Notfall- und Resilienzplanung:  
Aufbau von Notfallplänen für Energieausfälle inkl. Redundanzen, Prioritäten und Entscheidungswegen; regelmäßige Simulationen („Blackout-Drills“).
- Dezentrale Eigenversorgung:  
Investition in Photovoltaik-, Batterie- und Biogas-Kapazitäten; Aufbau lokaler Speicher- und Dieselreserven zur Überbrückung von Versorgungsengpässen.
- Schnittstellen zu Behörden:  
Aktive Abstimmung mit Netzbetreibern, BNetzA, BMWI und ZMZ-Stellen über Melde- und Priorisierungsverfahren im Krisenfall.
- Cyber- und physische Sicherheit:  
Härtung von Leittechnik- und OT-Systemen; physische Sicherung von Trafostationen, Tankanlagen, Energiezentralen; 24/7-Monitoring.
- Diversifizierung von Bezugsquellen:  
Aufbau redundanter Liefer- und Transportstrukturen für Energie- und Rohstoffe, inkl. strategischer Partnerschaften mit europäischen Anbietern.
- Energie-Effizienz und Reserven:  
Reduktion des Energiebedarfs durch Effizienzmaßnahmen; Schaffung betrieblicher „Krisenreserven“ für priorisierte Prozesse.
- Regelmäßige Stresstests:  
Durchführung von Energie-Stresstests und Krisenübungen mit internen und externen Partnern zur Validierung von Redundanzen und Entscheidungswegen.

## 3.2 Lieferketten & Logistik

### Relevanz

Globale Lieferketten bilden das Rückgrat industrieller Produktion und Wertschöpfung. Ihre Komplexität und internationale Verflechtung machen sie jedoch hochgradig verwundbar – insbesondere im Spannungs- oder Verteidigungsfall.

Militärische Priorisierungen von Transportwegen, Exportbeschränkungen oder Engpässe bei Treibstoff und Personal können zu massiven Störungen führen. Deutschland ist als Logistikdrehscheibe Europas besonders exponiert (BMI 2024, Hartmann 2025).

### Zentrale Risiken

- Unterbrechung internationaler Lieferketten durch militärische Priorisierung, Sanktionen oder Infrastrukturverluste.
- Engpässe in Transport & Personal: Ausfall von Lkw-Fahrern, Bahn- und Hafenlogistik; eingeschränkte Luftfrachtkapazitäten.
- Single-Source-Abhängigkeiten: Konzentration kritischer Komponenten auf wenige Lieferanten oder Regionen.

- Cyber- und Sabotagerisiken entlang der Transportkette (Tracking-Systeme, Hafensteuerungen, OT-Netze).
- Ressourcenverknappung & Preisschocks durch Energie- oder Rohstoffkrisen.

### **Strategische Ziele**

- Aufrechterhaltung der Liefer- und Transportfähigkeit auch bei militärischer Priorisierung oder Infrastrukturausfällen.
- Reduzierung von Abhängigkeiten durch Diversifizierung von Lieferanten, Transportwegen und Regionen.
- Stärkung der Transparenz und Steuerungsfähigkeit entlang der gesamten Supply Chain (Tier-1 bis Tier-n).
- Integration von Lieferkettenrisiken in das unternehmensweite Business Continuity Management (BCM) und Krisenmanagement.
- Bevorratung kritischer Materialien und Produkte zur Überbrückung von Disruptionen.
- Etablierung abgestimmter Prozesse mit Behörden, ZMZ-Strukturen und Netzbetreibern.

### **Kritische Maßnahmen & Governance**

- Risikotransparenz & Priorisierung:  
Systematische Analyse von Abhängigkeiten (Tier-1 bis Tier-n); Identifikation von Single Points of Failure; Entwicklung einer dynamischen Risiko-Heatmap.
- Diversifizierung & Regionalisierung:  
Aufbau von Dual-Sourcing-Strategien, Nearshoring europäischer Lieferketten, Nutzung regionaler Hub-Strukturen („Hub-and-Spoke-Modelle“).
- Krisenfähige Logistik:  
Abschluss von Rahmenverträgen mit alternativen Carriern und Spediteuren; Planung redundanter Transportkorridore; Festlegung militärischer und ziviler Prioritäten mit Behörden.
- Koordination mit Staat & Militär:  
Frühe Abstimmung mit ZMZ-Stellen, Bundeswehr-LogCom und BMVg zur Nutzung militärisch relevanter Infrastruktur und zur Vermeidung von Zielkonflikten.
- Sicherheits- & Cyberhärtung:  
Absicherung logistischer IT-Systeme (z. B. ERP, Tracking, Port-Management); physischer Schutz kritischer Umschlagplätze.
- Resilienztests & Übungen:  
Durchführung regelmäßiger Lieferketten-Stresstests, Szenarioanalysen und gemeinsamer Übungen mit Partnern und Behörden.

### 3.3 Interne Infrastruktur

#### Relevanz

Eigene Standorte und Anlagen sind das physische Fundament der Wertschöpfung. Sie sichern Produktion, Logistik, Forschung und Kommunikation. Im Spannungs- oder Verteidigungsfall werden industrielle Standorte sowohl strategisch als auch symbolisch zu Zielobjekten hybrider Angriffe — etwa durch Sabotage, Drohnenüberflüge, Ausspähung oder Cyberzugriffe auf Gebäudesteuerungen. Zudem können regionale Operationspläne (OPLAN DEU, Landesverteidigungskonzepte) die Verfügbarkeit von Flächen, Energie und Personal einschränken (BMVg 2023; BMI 2024, 2023b).

#### Zentrale Risiken

- Physische Sabotage und Spionage: Drohnenaufklärung, Manipulation an Versorgungsleitungen oder Zutrittssystemen.
- Interne Abhängigkeiten: Globale Konzernnetzwerke und interne Lieferstrukturen als Risiko bei Standortausfall.
- Regionale Einschränkungen: Militärische Nutzung oder Priorisierung von Verkehrswegen, Energie- und Kommunikationsinfrastruktur.
- Soziale Risiken: Einflussnahme auf Mitarbeitende, gesellschaftliche Spannungen, Desinformation in Standortregionen.
- Unzureichende Schutzkonzepte: Fehlende Redundanz, Sicherheitszonen oder Überwachungssysteme.

#### Strategische Ziele

- Sicherstellung der Betriebsfähigkeit kritischer Standorte im Krisen- oder Verteidigungsfall.
- Physische und organisatorische Resilienz für Schlüsselstandorte und Mitarbeitende aufbauen.
- Reduzierung interner Abhängigkeiten durch regionale Redundanzen und Ausweichkapazitäten.
- Früherkennung und Abwehr hybrider Bedrohungen an und um Unternehmensstandorte.
- Integration der Standortresilienz in die Gesamt-Governance (Security, BCM, Facility, HR, IT).

#### Kritische Maßnahmen & Governance

- Standortklassifizierung:  
Identifikation und Priorisierung kritischer Produktions-, Logistik- und Führungsstandorte nach nationaler, wirtschaftlicher und verteidigungspolitischer Relevanz (KRITIS-Definition, DIN SPEC 14027).

- **Physische Schutzmaßnahmen:**  
Verstärkung von Zutritts-, Video-, Perimeter- und Drohnenschutzsystemen; Integration von Sicherheits-Monitoring in zentrale Leitstellen.
- **Redundanz & Ausweichplanung:**  
Aufbau alternativer Standorte oder „Hot Sites“ für Produktion, Datenverarbeitung und Krisensteuerung.
- **Sicherheits- und Lageübungen:**  
Regelmäßige Standortübungen zu Sabotage, Ausfall, Evakuierung und Notbetrieb; Einbindung regionaler Behörden und ZMZ-Strukturen.
- **Monitoring & Frühwarnung:**  
Einsatz von Sensorik, Drohnenerkennung und OSINT-Monitoring zur Erkennung potenzieller Bedrohungen im Umfeld von Anlagen.
- **Sicherheits-Governance:**  
Festlegung von Verantwortlichkeiten im Zusammenspiel von Corporate Security, Facility Management, IT und Business Continuity.

### 3.4 Länder- und Standortperspektive

#### Relevanz

**Multinationale Unternehmen agieren in einem komplexen Umfeld aus unterschiedlichen nationalen Sicherheits-, Rechts- und Krisenregelungen.** Im Spannungs- oder Verteidigungsfall greifen nationale Gesetze (z. B. Sicherheits-, Energiesicherungs- und Arbeitssicherstellungsgesetze) parallel zu europäischen und NATO-Vorgaben. Fehlende Harmonisierung, unterschiedliche Eskalationsstufen und divergierende Kommunikations- und Entscheidungswege können die Unternehmenshandlungsfähigkeit erheblich beeinträchtigen.

Für international tätige Unternehmen ist daher ein einheitliches, länderübergreifendes Krisen- und Sicherheitsmanagement essenziell (EU-Commission 2025, 2022a; NATO 2024).

#### Zentrale Risiken

- Abweichende nationale Sicherheits- und Krisenvorgaben (z. B. Aktivierung von Mobilmachungs- oder Meldepflichten).
- Fehlende Harmonisierung mit EU-, NATO- und Partnerstaatenregelwerken.
- Unklare Zuständigkeiten zwischen nationalen Landesgesellschaften, Behörden und Headquarters.
- Inkonsistente Kommunikation über Länder- und Rechtssystemgrenzen hinweg.
- Reputations- und Haftungsrisiken bei Nichteinhaltung nationaler Sicherheits- oder Compliance-Pflichten.

## Strategische Ziele

- Etablierung eines einheitlichen, international abgestimmten Krisen- und Notfallmanagements.
- Sicherstellung rechtlicher und regulatorischer Konformität an allen nationalen und internationalen Standorten.
- Harmonisierung sicherheitsrelevanter Standards und Prozesse im Einklang mit EU-, NATO- und nationalen Anforderungen.
- Konsistente Kommunikation und Entscheidungswege zwischen Headquarters, Tochtergesellschaften und Behörden.
- Integration von Standort- und Länderrisiken in das zentrale Risikomanagement und Business Continuity Framework.

## Kritische Maßnahmen & Governance

- Harmonisierung & Standardisierung:  
Entwicklung einheitlicher Krisen-, Sicherheits- und Kommunikationsrichtlinien für alle Länderorganisationen (inkl. Eskalations- und Freigabeprozesse).
- Governance-Framework:  
Aufbau einer zentralen, international abgestimmten Sicherheits-Governance mit klaren Rollen (HQ, Landesgesellschaften, Behörden).
- Rechts- und Compliance-Monitoring:  
Regelmäßige Prüfung nationaler Sicherheits- und Krisengesetze; Integration in das Compliance-Management-System.
- Länderübergreifende Krisenübungen:  
Durchführung gemeinsamer Krisenübungen mit internationalen Standorten, Behörden und ZMZ-Strukturen.
- Kommunikationsarchitektur:  
Sicherstellung redundanter, international synchronisierter Kommunikationskanäle; Definition klarer Melde- und Entscheidungswege.
- Berücksichtigung geopolitischer Risiken:  
Bewertung der Sicherheitslage in relevanten Ländern (z. B. NATO-Ostflanke, Indo-Pazifik) im Rahmen strategischer Standortentscheidungen.

## 3.5 Produkte und Dienstleistungen

### Relevanz

Im Spannungs- oder Verteidigungsfall werden Produkte und Dienstleistungen nicht nur nach wirtschaftlichen, sondern nach sicherheits- und versorgungspolitischen Kriterien priorisiert. **Unternehmen mit systemrelevanten oder Dual-Use-Produkten können staatlicher Steuerung, Meldepflichten oder Produktionsauflagen unterliegen.**

Eine frühzeitige Bewertung der Systemrelevanz und des Dual-Use-Potenzials ist daher entscheidend, um Handlungs-, Liefer- und Planungssicherheit zu wahren (Bafa 2021, BMWK 2024a, 2024b; EU-Commission 2022).

## Zentrale Risiken

- Produktionsunterbrechungen durch Ressourcenknappheit, Energieausfälle oder staatliche Eingriffe.
- Staatliche Steuerung und Priorisierung (z. B. Fertigung für Bundeswehr oder kritische Infrastrukturen).
- Verlust von Flexibilität durch Umwidmung von Produktionskapazitäten oder Exportrestriktionen.
- Rechtliche Risiken durch fehlende Klassifizierung von Dual-Use-Gütern.
- Abhängigkeit von Vorprodukten und sensiblen Lieferanten mit sicherheitsrelevanten Schnittstellen.

## Strategische Ziele

- Sicherstellung der kontinuierlichen Bereitstellung systemkritischer Produkte und Dienstleistungen.
- Frühzeitige Identifikation und Bewertung sicherheitsrelevanter und Dual-Use-Produkte.
- Aufrechterhaltung der Produktionsfähigkeit trotz staatlicher Eingriffe oder Ressourceneinschränkungen.
- Flexibilisierung des Geschäftsmodells zur Anpassung an behördliche Priorisierungsvorgaben.
- Integration der Produkt- und Service-Resilienz in Business Continuity, Supply Chain und Risiko-Management.

## Kritische Maßnahmen & Governance

- Systemrelevanz-Analyse:  
Bewertung des Portfolios nach Kritikalität (KRITIS-Bezug, sicherheitspolitische Bedeutung, zivile und militärische Nutzung).
- Dual-Use-Compliance:  
Prüfung bestehender Export- und Handelsbeschränkungen; Aufbau klarer Klassifizierungs- und Meldeprozesse (nach EU-Dual-Use-VO 2021/821).
- Produktions- und Ressourcenplanung:  
Entwicklung von Notfall-Produktionsplänen mit Priorisierungen und Reserven für kritische Güter.
- Abstimmung mit Behörden:  
Etablierung fester Kommunikationswege mit BMWF, BMVg und ZMZ-Stellen zur Koordination von Produktionskapazitäten im Krisenfall.
- Governance & Reporting:  
Integration produktbezogener Resilienzindikatoren in die Unternehmenssteuerung (z.B. Produktionsfähigkeit, Materialverfügbarkeit, staatliche Steuerungsfähigkeit).
- Forschung & Innovation:  
Förderung sicherheitsrelevanter Innovationen mit europäischem Mehrwert (z.B. über EDF, IPCEI, Horizon Europe).

## 3.6 Märkte & Kundenverhalten

### Relevanz

Krisen, Spannungs- oder Verteidigungsfälle verändern Nachfrage, Kaufkraft und Marktstrukturen tiefgreifend. Lieferkettenstörungen, Energieknappheit, Inflation, Exportverbote oder **militärische Priorisierungen führen zu Disruptionen in Angebot und Nachfrage**, die sich direkt auf Absatzmärkte und Kundenbeziehungen auswirken. Unternehmen müssen in der Lage sein, Marktdynamiken zu antizipieren und Strategien flexibel anzupassen (IFW 2024; IMF 2024, OECD 2025).

### Zentrale Risiken

- Nachfrageeinbrüche oder Nachfrageschocks durch Kaufkraftverlust oder staatliche Eingriffe.
- Verschiebung von Marktprioritäten zugunsten sicherheits- oder versorgungsrelevanter Güter.
- Verlust internationaler Absatzmärkte infolge von Sanktionen, Konflikten oder Logistikeinschränkungen.
- Reputationsrisiken bei Geschäftsbeziehungen in geopolitisch sensiblen Regionen.
- Konsumentenverhalten unter Krisenstress: steigende Sensibilität für Preis, Herkunft und Versorgungssicherheit.

### Strategische Ziele

- Aufrechterhaltung der wirtschaftlichen Handlungsfähigkeit durch flexible Markt- und Produktstrategien.
- Früherkennung von Markt- und Nachfrageverschiebungen zur proaktiven Anpassung von Produktion und Vertrieb.
- Absicherung zentraler Absatzmärkte durch geografische Diversifizierung und strategische Partnerschaften.
- Stärkung der Kundenbindung durch Vertrauen, Versorgungssicherheit und klare Krisenkommunikation.
- Integration von Marktrisiken in strategische Planung, Krisenmanagement und Business Continuity.

### Kritische Maßnahmen & Governance

- Marktszenarien & Frühwarnsysteme:  
Aufbau kontinuierlicher Markt- und Umfeldanalysen zur Erkennung geopolitischer, regulatorischer und sozialer Trendänderungen.
- Diversifizierung der Absatzstruktur:  
Entwicklung alternativer Märkte innerhalb der EU oder befreundeter Partnerstaaten („Friend-Shoring“).

- **Kundenmanagement & Kommunikation:**  
Transparente Information über Lieferfähigkeit, Versorgungslage und Priorisierungen im Krisenfall.
- **Vertrags- und Risikoabsicherung:**  
Aufnahme von Force-Majeure-, Liefergarantie- und Priorisierungsklauseln in Schlüsselkundenverträge.
- **Innovations- und Produktstrategie:**  
Fokussierung auf Produkte mit hoher Krisenresistenz (z.B. Energieeffizienz, Sicherheit, Versorgung, Digitalisierung).
- **Resilienz-Monitoring:**  
Integration marktbezogener Kennzahlen in das Risikomanagement (z.B. Absatzresilienz, Kundenstabilität, Nachfragevolatilität).

### 3.7 Cyber, Kommunikations- und Betriebssysteme

#### Relevanz

**IT-, Kommunikations- und Betriebssysteme sind die neuralgischen Punkte moderner Unternehmensresilienz.** In hybriden Konflikten sind Cyberangriffe, Desinformation, Spionage und Sabotage die bevorzugten Mittel, um kritische Infrastrukturen und Wertschöpfungsketten zu destabilisieren. Mit Inkrafttreten der NIS2-Richtlinie und des EU Cyber Resilience Act (CRA) sind Unternehmen zudem gesetzlich verpflichtet, digitale Systeme widerstandsfähig, meldefähig und sicher zu gestalten. Ein Ausfall zentraler IT-, OT- oder Kommunikationssysteme gefährdet unmittelbar die Führungs-, Steuerungs- und Produktionsfähigkeit — und damit die nationale und wirtschaftliche Sicherheit.

#### Zentrale Risiken

- Cyberangriffe auf ERP-, Produktions- und Steuerungssysteme (IT/OT), häufig über Lieferketten oder kompromittierte Drittanbieter.
- Datenverlust oder Manipulation durch Ransomware, Spionage oder Sabotage.
- Abhängigkeit von Cloud-Dienstleistern außerhalb der EU (fehlende Datensouveränität).
- Kommunikationsausfälle bei Unterbrechung öffentlicher Netze, Internet oder Mobilfunk.
- Störungen kritischer Anbieter (z.B. AWS, Microsoft, Google) mit Kaskadeneffekten auf gesamte Industrien.
- Fehlende Integration von Cyberlage, Krisenkommunikation und Business Continuity.

#### Strategische Ziele

- Sicherstellung der Funktionsfähigkeit kritischer IT-, Kommunikations- und Betriebssysteme im Krisen- und Verteidigungsfall.
- Stärkung der Cyber-Resilienz durch mehrschichtige Schutz-, Erkennungs- und Wiederherstellungsmaßnahmen.

- Aufbau autarker Kommunikations- und Entscheidungsfähigkeit bei Ausfall öffentlicher Netze oder Cloud-Infrastrukturen.
- Sicherstellung von Datenhoheit und Systemzugriff in geopolitischen Krisen oder bei staatlichen Eingriffen.
- Etablierung einer klaren Governance für Cyber- und Informationssicherheit (Einbindung von CSO, CISO, CIO und BCM).
- Einbindung in staatliche und internationale Lagebilder (BSI, CERT-Bund, NATO-Cyber Command, EU-CSIRT-Network).

### **Kritische Maßnahmen & Governance**

- Technische Resilienzmaßnahmen:  
Aufbau redundanter und segmentierter Netzwerkstrukturen (Zero Trust Architecture).  
Einführung autarker Kommunikationssysteme (Satellit, Out-of-Band, Kurzwelle).  
Offline-fähige Backups geschäftskritischer Daten und Systeme.
- Melde- und Kooperationspflichten:  
Implementierung der NIS2- und CRA-Anforderungen inkl. 24-h-Meldepflicht bei Sicherheitsvorfällen.  
Aufbau direkter Kommunikationskanäle zu BSI, CERT-Bund und europäischen CSIRT-Netzwerken.
- Cyber-Lagebild & Krisenintegration:  
Verankerung von Cyber- und IT-Lagebildern in Krisenstäben und Business Continuity Management (BCM).  
Nutzung staatlicher und kommerzieller Threat-Intelligence-Plattformen (BSI, NATO MISP, EU-SOCTA).
- Training & Resilienztests:  
Durchführung regelmäßiger Cyber- und Wiederherstellungsübungen inkl. physischer Angriffsszenarien.  
Integration von Red-Team-Tests, Tabletop-Exercises und Blackout-Szenarien in den BCM-Zyklus.
- Rechts- & Vertragsmanagement:  
Überprüfung von Cloud- und IT-Verträgen auf Krisen- und Zugriffsklauseln; Sicherung von Notfallzugängen und Datensouveränität.

## 3.8 Personal & Arbeitsfähigkeit

### Relevanz

Mitarbeitende sind die kritische Ressource jeder unternehmerischen und gesellschaftlichen Resilienz. Im Spannungs-, Verteidigungs- oder Bündnisfall greifen rechtliche Verpflichtungen (z. B. Art. 12 GG, Arbeitssicherstellungsgesetz (ASG), Zivilschutz- und Ersatzdienstgesetze)<sup>3</sup>, die eine staatliche Verfügung über Arbeitskräfte zulassen. Parallel führen Sicherheitslagen, Evakuierungen, Mobilmachung oder psychische Belastung zu erheblichen Ausfällen und Effizienzverlusten. Unternehmen müssen daher sowohl rechtlich planbar als auch organisatorisch resilient aufgestellt sein, um trotz Personalabzug, Mobilmachung oder Krisendruck arbeitsfähig zu bleiben.

### Zentrale Risiken

- Personalabzug durch Einberufung von Reservisten oder Verpflichtung zu zivilen Schutzdiensten (z.B. THW, Feuerwehr, Zivilschutz).
- Arbeitsausfälle infolge von Evakuierungen, Schutzmaßnahmen oder familiären Verpflichtungen.
- Überlastung und psychische Erschöpfung durch Dauerkrisen und hohe Sicherheitsanforderungen.
- Sicherheitsrisiken durch Desinformation, ideologische Beeinflussung oder illoyales Verhalten.
- Fehlende Rollen- und Vertretungsstrukturen bei Schlüsselpersonal.
- Mangelnde Transparenz über Verteidigungs- oder Zivilschutzpflichten innerhalb der Belegschaft.

### Strategische Ziele

- Sicherstellung der Mindestbesetzung / Arbeitsfähigkeit in allen kritischen Prozessen.
- Aufbau von Wissens- und Funktionsredundanz zur Absicherung der Wertschöpfung.
- Transparenz über Reservistenstatus, Ehrenämter und Einsatzpflichten unter Wahrung des Datenschutzes.
- Sicherstellung des Mitarbeiterschutzes, inkl. Evakuierungs-, Fürsorge- und psychologischer Unterstützungsmaßnahmen.
- Rechtliche Planbarkeit durch Abstimmung mit Behörden (z.B. BMAS, BMVg, ZMZ-Strukturen).
- Förderung einer resilienten Unternehmenskultur, die Loyalität, Fürsorge und Eigenverantwortung stärkt.

---

<sup>3</sup> Auszüge zum rechtlichen Rahmen oder Regularien finden sich im Anhang 1.

## Kritische Maßnahmen & Governance

- Rollen- und Mindestbesetzungsplanung:  
Definition kritischer Funktionen und Personalbedarfe pro Standort und Prozess.
- Reservisten- und Ehrenamtsmanagement:  
Einrichtung einer vertraulichen Selbstauskunft unter Wahrung der DSGVO; Kooperation mit Initiativen wie „Arbeitgeber und Reserve“ (BMVg).
- Freistellungs- und Rückkehrvereinbarungen:  
Regelungen zur Rückkehrpflicht und Arbeitsplatzsicherung nach Reservisteneinsätzen oder Zivilschutzeinbindung.
- Cross-Training & Wissensmanagement:  
Aufbau redundanter Kompetenzen und Stellvertretermodelle in Schlüsselprozessen.
- Psychologische & soziale Resilienz:  
Einführung von Care- und Employee-Assistance-Programmen, psychologischer Krisenhilfe, Schulungen für Führungskräfte im Umgang mit Belastungssituationen.
- Rechtliche & organisatorische Vorsorge:  
Prüfung der Unternehmenspflichten aus ASG (§ 3), Zivildienstgesetz (§ 79 ZDG) und Arbeitsschutzgesetz.  
Abstimmung mit Katastrophenschutzbehörden und ZMZ-Koordinatoren zur Sicherstellung der Arbeitsfähigkeit in Verteidigungsfällen.
- Krisenübungen & Szenarien:  
Durchführung regelmäßiger Tabletop-Übungen mit Behörden (z.B. ZMZ, BSI, Katastrophenschutz), Einbindung von Personal- und Kommunikationsstrukturen.

## 3.9 Recht & Governance - Staatliche Steuerung & Regulierung

### Relevanz

**Im Spannungs- oder Verteidigungsfall tritt eine Vielzahl von Sicherstellungs- und Steuerungsmechanismen in Kraft, die tief in Unternehmensprozesse eingreifen.**

Ziel des Staates ist die Aufrechterhaltung der Landes- und Bündnisverteidigung – dies schließt die Steuerung von Produktion, Lieferketten, Energie, Personal und Kommunikation ein. Für Unternehmen bedeutet dies: Rechtssicherheit, Governance und Compliance werden zu entscheidenden Resilienzfaktoren.

### Zentrale Risiken

- Verpflichtung zur Bereitstellung von Gütern und Dienstleistungen für Streitkräfte oder Zivilverteidigung.
- Produktionsauflagen und Eingriffe in Lieferketten, z.B. Priorisierung militärischer Aufträge.
- Versicherungslücken (Krieg, Terror, Cyberangriffe) und daraus resultierende Kostenrisiken.
- Rechtliche Unsicherheiten bei staatlicher Inanspruchnahme oder Mobilmachung.

- Haftungsrisiken für Geschäftsleitung bei Nichterfüllung staatlicher Verpflichtungen.
- Neue Compliance-Anforderungen durch nationale und europäische Sicherheitsgesetzgebung (NIS2, KRITIS-Dachgesetz, Verteidigungswirtschaftsverordnung)<sup>4</sup>.

### Strategische Ziele

- Rechtssicherheit in Spannungs-, Verteidigungs- und Bündnisfällen.
- Etablierung klarer Governance-Strukturen mit definierten Rollen, Verantwortlichkeiten und Entscheidungswegen.
- Verankerung der Sicherheits- und Verteidigungsverpflichtungen in Corporate Policies.
- Sicherstellung der Compliance gegenüber nationalen und internationalen Rechtsrahmen.
- Transparente Kosten- und Entschädigungsmechanismen bei staatlichen Eingriffen.
- Integration rechtlicher und regulatorischer Resilienz in das Enterprise Risk Management (ERM).

### Kritische Maßnahmen & Governance

- Board Ownership:  
Verankerung von Sicherheit, Krisenrecht und Resilienz in der Verantwortung der höchsten Managementebene (C-Level, Aufsichtsrat und Eigentümer)
- Governance-Struktur:  
Einrichtung eines **Resilience & Compliance Steering Committee auf Vorstandsebene** mit Schnittstellen zu Corporate Security, IT, Legal, Finance, HR und Supply Chain.
- Regelwerke & Richtlinien:  
Erstellung einer **Resilience & Crisis Policy** mit definierten Eskalationswegen, Freigabeprozessen und Dokumentationspflichten.
- Rechtliche Prüfung:  
Externe Gutachten zu Verpflichtungen aus Sicherstellungs-, Arbeits- und Wirtschaftsgesetzen (z.B. ASG, LV/BV-Gesetze)<sup>5</sup>.
- Vertragsmanagement:  
Prüfung von Verträgen auf Force-Majeure-, Lieferpriorisierungs- und Kostenerstattungsklauseln.
- Versicherungsschutz:  
Erweiterung bestehender Policen auf Krieg, Terror, Cyber, Betriebsunterbrechung und politische Risiken.

---

<sup>4</sup> Auszüge zum rechtlichen Rahmen oder Regularien finden sich im Anhang 2.

<sup>5</sup> Auszüge zum rechtlichen Rahmen oder Regularien finden sich im Anhang 1.

- Compliance & Training:  
Schulung von Führungskräften zu rechtlichen Pflichten und Haftungsrisiken im Spannungsfall.
- Dokumentation & Nachweisführung:  
Vorbereitung von Standardformularen, Meldeschienen und Nachweisprotokollen (z.B. zur Erfüllung staatlicher Anforderungen).

### 3.10 Finanzen & Liquidität

#### Relevanz

**In sicherheitspolitischen Krisen geraten Finanzmärkte, Kapitalströme und Kreditmechanismen unter erheblichen Druck.** Zahlungssysteme können eingeschränkt, Versicherungen teilweise wirkungslos und Kapitalflüsse durch Sanktionen oder staatliche Eingriffe blockiert werden. Unternehmen müssen deshalb **ihre finanzielle Resilienz proaktiv sichern**, um auch bei Marktstillstand, Energiekrise oder Cybervorfall **liquide zu bleiben** und operative Kontinuität zu gewährleisten. Finanzmanagement wird damit zu einem **strategischen Bestandteil der Unternehmenssicherheit**.

#### Zentrale Risiken

- Liquiditätsengpässe infolge von Produktionsausfällen, Kreditkürzungen oder Lieferstopps.
- Zahlungsausfälle bei Kunden und Lieferanten durch wirtschaftliche Instabilität.
- Zusammenbruch des Kapitalmarkts oder Zahlungssysteme (TARGET2, SWIFT, SEPA).
- Versicherungslücken (Krieg, Terror, Cyber) und eingeschränkte Schadensregulierung.
- Inflation, Zinsschocks und Währungsvolatilität durch geopolitische Spannungen.
- Fehlende Planbarkeit von Entschädigungen oder Kostenübernahmen bei staatlichen Eingriffen.

#### Strategische Ziele

- Sicherstellung der Liquidität für mindestens 3-6 Monate Krisenbetrieb.
- Aufrechterhaltung des Zahlungsverkehrs auch bei Ausfall zentraler Systeme.
- Reduzierung finanzieller Abhängigkeiten von einzelnen Banken, Versicherern oder Ländern.
- Integration von Finanzrisiken in das Krisen- und Business-Continuity-Management.
- Schaffung von Transparenz über Förder- und Absicherungsmechanismen auf EU-, Bundes- und Landesebene.
- Absicherung der Unternehmenswerte gegen geopolitische, operative und makroökonomische Schocks.

## Kritische Maßnahmen & Governance

- Liquiditätsmanagement & Stresstests:  
Aufbau von Liquiditäts- und Cash-Reserven für mehrere Szenarien; tägliches Monitoring zentraler Finanzkennzahlen.
- Finanzielle Redundanz:  
Nutzung mehrerer Banken und alternativer Zahlungsdienstleister; Vorbereitung auf Offline-Zahlungen (z.B. manuelle Buchungen, Notkonten).
- Kreditlinien & Notfallfinanzierung:  
Frühzeitige Abstimmung mit Banken über Krisenlinien, Bürgschaften und Avale; Aufbau interner Liquiditätspools.
- Versicherungsschutz:  
Prüfung und Erweiterung bestehender Policen auf Krieg, Terror, Cyber, Lieferketten- und Betriebsunterbrechungsrisiken.
- Förder- und Sicherungsinstrumente:  
Nutzung von EU-Programmen (*InvestEU Crisis Response, Resilience and Recovery Facility*) und nationalen Mechanismen (KfW-Krisenkredite, Bürgschaften).
- Finanz-Compliance & Dokumentation:  
Einrichtung von Notfallfreigabeprozessen und Nachweisstrukturen zur Kostenverfolgung und staatlichen Entschädigung<sup>6</sup>.
- Board Reporting:  
Integration von Finanz- und Liquiditätsrisiken in das Enterprise Risk Management (ERM) und monatliche Berichterstattung an CEO/CFO.

## Empfohlene Governance-Verankerung

- Verantwortlichkeit beim CFO / CRO, eingebunden in Krisenstab und BCM.
- Aufbau eines Financial Resilience Playbooks (Kreditlinien, Ansprechpartner, Genehmigungswege).
- Regelmäßige Liquiditäts- und Versicherungsreviews (Quartalsbasis).
- Integration in OPLAN-relevante Planungsprozesse für Energie-, Lieferketten- und Sicherheitsfunktionen.

---

<sup>6</sup> Hinweise zu Finanzierungs- und Unterstützungsprogrammen der Wirtschaft finden sich im Anhang 3.

## 3.11 Technologie & Innovation

### Relevanz

Technologische Unabhängigkeit ist ein zentraler Pfeiler nationaler und unternehmerischer Resilienz. **Abhängigkeiten von außereuropäischen Schlüsseltechnologien** – insbesondere im Bereich Halbleiter, KI, Cloud-Infrastruktur, Kommunikations- und Raumfahrt-technologien – **gefährden im Krisenfall sowohl Betriebssicherheit als auch strategische Handlungsfähigkeit**. Der EU Chips Act, der Cyber Resilience Act (CRA) und das Programm Key Digital Technologies (KDT JU) bilden die regulatorische Basis für eine europäische technologische Souveränität, die Unternehmen aktiv in ihre Sicherheitsarchitektur integrieren müssen.

### Zentrale Risiken

- Lieferstopps und Exportbeschränkungen für kritische Technologien (z.B. Halbleiter, Sensorik, Software).
- Abhängigkeit von nicht-europäischen Anbietern (z.B. US-Clouds, asiatische Halbleiter, KI-Plattformen).
- Cyberrisiken durch Manipulation von Hard- oder Softwarekomponenten.
- Technologielücken in europäischen Wertschöpfungsketten (z.B. bei Verteidigungs-, Raumfahrt- oder Energiesystemen).
- Sanktions- oder Lizenzrisiken bei Nutzung von Dual-Use-Technologien in Drittstaaten.
- Verzögerte Innovationszyklen durch regulatorische Unsicherheit und fehlende europäische Skalierungsfähigkeit.

### Strategische Ziele

- Sicherstellung der technologischen Souveränität durch Stärkung europäischer Schlüsseltechnologien.
- Diversifizierung und Lokalisierung kritischer Innovations- und Produktionspartner.
- Integration von Dual-Use-Technologien in Forschung, Entwicklung und industrielle Umsetzung.
- Schutz geistigen Eigentums (IP) und kritischer Entwicklungsdaten durch eigene Sicherheitsarchitektur.
- Kooperation mit europäischen Innovationsclustern (EDA, ESA, EU-Defence Innovation Scheme).
- Frühzeitige Einbindung technologischer Risiken in das Unternehmens- und Sicherheitsrisikomanagement.

### Kritische Maßnahmen & Governance

- Technologie-Mapping:  
Identifikation von Schlüsseltechnologien, deren Lieferketten und Abhängigkeiten (z.B. Halbleiter, KI-Modelle, Cloud, Quantencomputing, Raumfahrt).

- **Souveränitätsstrategie:**  
Entwicklung einer internen Roadmap zur Reduzierung nicht-europäischer Abhängigkeiten und Förderung lokaler Innovationspartnerschaften.
- **Kooperation & Förderung:**  
Teilnahme an EU-Programmen (*Horizon Europe, EDF, Key Digital Technologies Joint Undertaking*).  
Nutzung nationaler Fördermechanismen (z.B. BMBF-„Souveräne IT“).
- **Schutz & Sicherheit:**  
Integration von ITAR/EAR-Konformität, Cybersecurity-by-Design und Know-how-Schutz in Entwicklungsprozesse.
- **Dual-Use-Governance:**  
Bewertung von Forschungsprojekten hinsichtlich sicherheitsrelevanter Anwendungen, Exportkontrolle und ethischer Compliance.
- **Technologie-Resilienztests:**  
Überprüfung der Wiederanlaufzeiten kritischer Systeme bei Ausfall von Zulieferern oder Softwareplattformen.
- **IP-Security & Innovationsschutz:**  
Einrichtung sicherer Entwicklungsumgebungen, insbesondere für verteidigungsnahe oder sicherheitskritische Anwendungen.

### Politisch-strategische Einordnung

**Technologische Resilienz ist kein rein wirtschaftliches Thema, sondern Teil der europäischen Sicherheitsarchitektur.** Die EU fördert gezielt den Aufbau eigener Wertschöpfungsketten in sicherheitsrelevanten Bereichen (Halbleiter, Raumfahrt, Quanten- und Energietechnologien). Unternehmen sind gefordert, Innovationen nicht nur marktgetrieben, sondern sicherheitsbewusst zu gestalten – als Bestandteil einer „*Corporate Sovereignty Strategy*“ im Sinne der nationalen und europäischen Resilienz.

## 3.12 Ökologie & Nachhaltigkeit

### Relevanz

**Nachhaltigkeit bleibt auch im Spannungs- und Verteidigungsfall ein verpflichtendes strategisches Ziel.** Allerdings geraten Unternehmen zunehmend in Zielkonflikte zwischen Versorgungssicherheit, Energieeffizienz und CO<sub>2</sub>-Reduktion. Die EU-Taxonomie, der Green Deal Industrial Plan, die Corporate Sustainability Reporting Directive (CSRD) und nationale Klimagesetze schreiben Nachhaltigkeitsverpflichtungen auch in Krisenzeiten fort. Damit wird Nachhaltigkeit zu einem Kernbestandteil der Sicherheitsarchitektur – ökologisch, ökonomisch und sozial.

## Zentrale Risiken

- Zielkonflikte zwischen Versorgungssicherheit und Klimazielen (z.B. Reaktivierung fossiler Energien).
- Ressourcenverknappung (Wasser, seltene Erden, Recyclingmaterialien).
- Lieferabhängigkeiten von nicht nachhaltigen Zulieferketten außerhalb der EU.
- Regulatorische Risiken bei Nichterfüllung von ESG-Verpflichtungen (Bußgelder, Reputationsschäden).
- Reputationsverlust durch wahrgenommene Abkehr von Nachhaltigkeitszielen in Krisenzeiten.
- Physische Klimarisiken (z.B. Hitzewellen, Extremwetter) mit unmittelbarem Einfluss auf Produktion und Logistik.

## Strategische Ziele

- Aufrechterhaltung der ESG-Konformität auch in Krisen- und Verteidigungsszenarien.
- Integration von Nachhaltigkeit in die Resilienzstrategie – „Sustainable Security“ (Knoppe 2025).
- Sicherstellung der Versorgung mit kritischen Ressourcen unter ökologischen und sozialen Kriterien.
- Förderung energieeffizienter und emissionsarmer Produktionsprozesse trotz Krisenanforderungen.
- Aufbau geschlossener Stoff- und Energiekreisläufe (Circular Economy).
- Verankerung ökologischer Aspekte in Krisen- und Notfallplanung (z.B. Ersatzbeschaffung, Standortstrategie).

## Kritische Maßnahmen & Governance

- Nachhaltigkeits-Resilienzprogramm:  
Integration von ESG-Parametern in das Risikomanagement, Business Continuity und Sicherheitsstrategie.
- Kreislaufwirtschaft & Ressourcenmanagement:  
Aufbau von Recyclingstrukturen und Wiederverwertungssystemen, um Materialabhängigkeiten zu verringern.
- Klimarisikomanagement:  
Einbindung physischer Klimarisiken (Hitze, Dürre, Sturm) in Standort- und Produktionsentscheidungen.
- ESG-Compliance & Berichtspflichten:  
Sicherstellung der Berichtsfähigkeit nach CSRD/ESRS, auch bei gestörter Datenerhebung oder Krisenbetrieb.
- Green-Procurement-Strategie:  
Priorisierung nachhaltiger Zulieferer und Vertragsklauseln zur ökologischen und sozialen Mindestperformance.

- Energiemanagement & Eigenversorgung:  
Ausbau von Photovoltaik, Batteriespeichern, Biogas und Wasserstoff, um Versorgungssicherheit und CO<sub>2</sub>-Reduktion zu kombinieren.
- Stakeholder-Kommunikation:  
Transparente Darstellung von Zielkonflikten (z.B. temporärer Energieverbrauch fossiler Quellen) im ESG-Reporting.

### **Politisch-strategische Einordnung**

Nachhaltigkeit ist nicht nur Klimaschutz, sondern strategische Resilienzpolitik. Der EU-Green-Deal betont die Verzahnung von Dekarbonisierung, Rohstoffsoveränität und Krisenfestigkeit. Unternehmen, die Nachhaltigkeit als Teil ihrer Sicherheitsstrategie begreifen, sichern sich regulatorische Akzeptanz, gesellschaftliches Vertrauen und langfristige Wettbewerbsfähigkeit. ESG ist damit kein „weiches“ Thema (Knoppe 2025), sondern eine Voraussetzung für nationale und unternehmerische Wehrfähigkeit.

## **3.13 Internationale Verflechtungen & Geopolitik**

### **Relevanz**

Globale Wertschöpfung und geopolitische Stabilität sind zunehmend miteinander verflochten. Spannungen zwischen Großmächten, Sanktionen, Rohstoffnationalismus und der zunehmende Einsatz wirtschaftlicher Mittel als geopolitisches Instrument machen Unternehmen zu strategischen Akteuren in einer neuen Sicherheitsökonomie. Internationale Kooperationen, Partnernetzwerke und Produktionsverlagerungen werden damit Teil der Resilienzarchitektur moderner Industrieunternehmen.

### **Zentrale Risiken**

- Sanktions- und Exportrestriktionen (z.B. Russland, China, Iran), die Lieferketten und Absatzmärkte unterbrechen.
- Politisch motivierte Handelshemmnisse (Zölle, Technologiebeschränkungen, Lizenzpflichten).
- Abhängigkeit von geopolitisch instabilen Regionen bei Energie, Rohstoffen oder Vorprodukten.
- Verlagerung strategischer Allianzen (z.B. BRICS+, Indo-Pacific-Allianzen).
- Konkurrenz staatlich subventionierter Märkte (z.B. USA: Inflation Reduction Act; China: State Industrial Strategy).
- Zunahme hybrider Einflussaktivitäten über internationale Tochtergesellschaften, Lieferanten oder Logistikrouten.
- Fragmentierung multilateraler Systeme (WTO, UN) und Verlust verlässlicher Schlichtungsmechanismen.

## Strategische Ziele

- Stärkung wirtschaftlicher und politischer Handlungsfreiheit durch Diversifizierung globaler Wertschöpfungsketten.
- Minimierung geopolitischer Abhängigkeiten von kritischen Märkten, Partnern und Technologien.
- Etablierung eines geopolitischen Frühwarnsystems zur Bewertung und Steuerung internationaler Risiken.
- Integration geopolitischer Szenarien in Business-, Risiko- und Investitionsentscheidungen.
- Kooperation innerhalb sicherheitspolitisch verlässlicher Räume (EU, NATO, G7, „like-minded nations“).
- Schutz internationaler Tochtergesellschaften, Datenflüsse und Vermögenswerte vor staatlichen Zugriffen oder Enteignungen.

## Kritische Maßnahmen & Governance

- Geopolitisches Risikomanagement:  
Einrichtung eines „GeoRisk-Boards“ unter Einbindung von Corporate Security, Strategy und Risk Management.
- Friendshoring-Strategie:  
Neuordnung der Lieferketten in politisch stabile Regionen („Resilient Supply Zones“) innerhalb von EU, EWR und NATO-Partnerstaaten.
- Diversifizierung & Regionalisierung:  
Ausbau europäischer Fertigungs- und Beschaffungsstandorte (Nearshoring, Dual Sourcing).
- Sanktions- und Exportkontroll-Compliance:  
Systematische Prüfung nach EU-, US- und nationalem Recht (ITAR, EAR, BAFA).
- Schutz ausländischer Assets:  
Vertragsklauseln und Versicherungsschutz gegen politische Risiken, Enteignung und staatliche Eingriffe (z.B. PRI-Versicherungen, MIGA-Deckungen).
- Globale Lageanalyse:  
Nutzung von Regierungs- und Nachrichtendienst-Lagebildern (AA, BMVg, NATO Strat-Com, EEAS, EU INTCEN).
- Koordination internationaler Krisenreaktionen:  
Enge Abstimmung zwischen Unternehmensstandorten, Auslandsvertretungen und nationalen Krisenstäben (AA-Krisenzentrum, ZMZ).
- Sicherheitsarchitektur in Drittstaaten:  
Bewertung politischer Stabilität, Rechtssicherheit und Sicherheitslage vor Investitionen oder Expansionen.

## Politisch-strategische Einordnung

**Der OPLAN DEU ist in europäische und transatlantische Sicherheitsstrukturen eingebettet.** Parallel entwickeln EU-Staaten eigene nationale OPLAN-Konzepte (z.B. Frankreich: *Plan ORSEC Défense*, Polen: *Plan Obronny RP*, Schweden: *Totalförsvarsplanen*). Diese Programme verdeutlichen die Verschmelzung von wirtschaftlicher Leistungsfähigkeit und nationaler Verteidigungsfähigkeit.

Unternehmen mit internationaler Präsenz werden daher Teil einer gesamtstaatlichen Resilienzplanung – sie müssen ihre globalen Liefer-, Energie- und Informationsnetze so gestalten, dass sie auch im geopolitischen Stressfall stabil bleiben. Der Fokus verschiebt sich von „Just-in-Time“ zu „**Just-in-Case**“, von Effizienz zu strategischer Autonomie.

## 3.14 Kooperation & Netzwerke

### Relevanz

Resilienz entsteht durch Vernetzung – **kein Unternehmen übersteht eine Krise isoliert.** Die Fähigkeit, in Krisen und Verteidigungsfällen schnell, abgestimmt und vertrauensvoll mit Behörden, Partnern und Branchenakteuren zu agieren, ist entscheidend für Stabilität und Handlungsfähigkeit. Der Aufbau solcher Netzwerke wird zunehmend als Bestandteil der nationalen Sicherheitsarchitektur verstanden.

Kooperationen zwischen Industrie, Staat, Bundeswehr und Verbänden bilden das Rückgrat für eine funktionierende Gesamtverteidigung. Programme wie die Zivil-Militärische Zusammenarbeit (ZMZ) oder die KRITIS-Allianzen des Bundes fördern bereits heute diese Verflechtung – sie müssen jedoch auf Unternehmensebene aktiv operationalisiert werden.

### Zentrale Risiken

- Fehlende Koordination zwischen Unternehmen, Behörden und militärischen Stellen.
- Informationsdefizite und parallele Lagebilder („Informationssilos“).
- Mangelnde Einbindung in Krisenkommunikation und staatliche Meldekettten.
- Fehlende Vernetzung mit regionalen ZMZ-Stellen und Katastrophenschutzbehörden.
- Abhängigkeit von informellen Kontakten statt strukturierter Kooperationen.
- Fehlende Integration von Industrieinteressen in staatliche Krisenplanung (z.B. Energie, Transport, Personal).

### Strategische Ziele

- Institutionalisierte Kooperation mit Behörden, Bundeswehr, IHKs und Branchenverbänden.
- Etablierung belastbarer Resilienznetzwerke entlang der gesamten Wertschöpfungskette.

- Abstimmung von Krisen- und Notfallplänen mit staatlichen Stellen und regionalen ZMZ-Kommandos.
- Aufbau gemeinsamer Lage- und Informationsstrukturen (z.B. CERTs, Krisenplattformen, BSI-Meldewege).
- Förderung einer Sicherheits- und Resilienzkultur über Branchengrenzen hinweg.
- Koordinierte Kommunikation im Krisenfall (One-Voice-Policy zwischen Unternehmen, Behörden und Medien).

### Kritische Maßnahmen & Governance

- Teilnahme an Resilienznetzwerken:  
Mitgliedschaft in KRITIS-Allianzen, Branchenverbänden (BDI, Bitkom, VCI, VSW), IHK-Netzwerken und staatlichen Resilienzprogrammen.
- Zivil-Militärische Zusammenarbeit (ZMZ):  
Aufbau von Kontaktstrukturen zu regionalen ZMZ-Stäben der Bundeswehr, gemeinsame Übungen und Austausch im Krisenfall.
- Schnittstellenmanagement:  
Einrichtung klarer Melde- und Kommunikationswege zu BMI, BSI, BMWV, BBK, THW, Katastrophenschutz, CERT-Bund und Landesbehörden.
- Kooperationsvereinbarungen:  
Entwicklung bilateraler oder sektorübergreifender Abkommen zur gegenseitigen Unterstützung (z.B. Versorgung, Transport, IT-Support).
- Krisenübungen & Szenarien:  
Regelmäßige Teilnahme an länder- und branchenübergreifenden Übungen (z.B. LÜKEX, EU-CIP-Exercises).
- Informationssicherheit & Vertrauen:  
Nutzung sicherer Kommunikationsplattformen für vertraulichen Austausch (z.B. VS-NfD-konforme Kanäle).
- Wissensaustausch & Lessons Learned:  
Teilnahme an Resilienz-Foren, Branchenaustausch und wissenschaftlichen Kooperationen mit Forschungseinrichtungen.

### Politisch-strategische Einordnung

**Kooperation ist ein Sicherheitsfaktor.** Die Bundesregierung hat mit der Nationalen Sicherheitsstrategie (Bundeskanzleramt 2023), der KRITIS-Verordnung (BMI 2023b), dem OPLAN DEU und dem Gesetz zur Stärkung der Resilienz im Bevölkerungsschutz (BMI 2023a) die Grundlage geschaffen, um Unternehmen systematisch in den nationalen Resilienzverbund einzubinden. Industrie, Staat und Gesellschaft sollen damit integriert statt sequenziell handeln – präventiv, abgestimmt und verbindlich.

Unternehmen, die ihre Kooperationsfähigkeit als Teil ihrer Sicherheitsstrategie begreifen, erhöhen nicht nur ihre eigene Krisenfestigkeit, sondern tragen unmittelbar zur Verteidigungs- und Wettbewerbsfähigkeit des Landes bei.

### 3.15 Krisenkommunikation - Kommunikationsmatrix (intern/extern) - Stakeholderkommunikation

#### Relevanz

In einer hybriden Bedrohungslage entscheidet Kommunikation über Vertrauen, Legitimität und Stabilität. **Unternehmen stehen im Spannungsfall stärker im öffentlichen Fokus** – sie sind Teil der öffentlichen Sicherheitsarchitektur und Träger gesellschaftlicher Verantwortung. Transparente, konsistente und glaubwürdige Kommunikation wird damit zu einem strategischen Resilienzfaktor.

**Gleichzeitig steigen die Risiken:** Desinformationskampagnen, manipulative Narrative und gezielte Diskreditierungen in sozialen Medien können die Reputation eines Unternehmens innerhalb von Stunden massiv beschädigen. Daher muss Krisenkommunikation nicht nur reaktiv, sondern präventiv, koordiniert und sicherheitsintegriert ausgestaltet werden.

#### Zentrale Risiken

- Vertrauensverlust durch fehlende oder widersprüchliche Kommunikation.
- Reputationsschäden infolge von Intransparenz, Fehlmeldungen oder Fehlinformationen.
- Desinformation und Informationskrieg gegen Unternehmen (Deepfakes, Social Media Manipulation, Trollnetzwerke).
- Unkoordinierte Sprecherrollen und mangelnde Abstimmung zwischen Unternehmensbereichen.
- Fehlende Integration in staatliche Kommunikationsstrukturen (BMI, BBK, MoWaS).
- Überlastung von Kommunikationskanälen im Krisenfall.

#### Strategische Ziele

- Sicherung von Vertrauen bei Mitarbeitenden, Kunden, Behörden und Öffentlichkeit.
- Einheitliche, abgestimmte Kommunikation nach dem One-Voice-Prinzip.
- Wahrung der Informationshoheit durch aktive und glaubwürdige Krisenkommunikation.
- Integration in nationale Kommunikations- und Warnsysteme (z.B. MoWaS, BSI-Meldesysteme).
- Frühzeitige Erkennung und Bekämpfung von Desinformation.
- Transparente Darstellung der gesellschaftlichen Rolle und Verantwortung des Unternehmens.

## Kritische Maßnahmen & Governance

- **Krisenkommunikationshandbuch:**  
Definition von Rollen, Sprecherrechten, Eskalationswegen, Freigabeprozessen und Kommunikationskanälen.
- **Kommunikationsmatrix:**  
Klare Zuständigkeiten für interne und externe Stakeholder (Vorstand, HR, Kunden, Medien, Behörden, Zulieferer, externe Dienstleister).
- **Desinformationsabwehr:**  
Monitoring sozialer Medien, Identifizierung manipulativer Inhalte, enge Zusammenarbeit mit Behörden und Plattformbetreibern.
- **Stakeholder-Dialoge:**  
Regelmäßiger Austausch mit Behörden, Verbänden, Medien und Mitarbeitenden zur Vertrauensbildung.
- **One-Voice-Policy:**  
Einheitliche Botschaften - abgestimmt zwischen Kommunikation, Corporate Security, HR, Legal und Vorstand.
- **Training & Mediensimulation:**  
Regelmäßige Schulungen und Kamera-/Interviewtrainings für Pressesprecher und Führungskräfte.
- **Psychosoziale Kommunikation:**  
Unterstützung der Belegschaft in Krisen durch empathische, glaubwürdige und lösungsorientierte Ansprache.
- **Sichere Kommunikationskanäle:**  
Nutzung redundanter Systeme (z.B. Satellit, Kurzwelle, gesicherte Intranetlösungen).

## Politisch-strategische Einordnung

### **Krisenkommunikation ist kein PR-Thema, sondern Sicherheitskommunikation.**

Sie muss in die gesamtstaatliche Kommunikationsarchitektur eingebettet sein – insbesondere in die Informationskanäle von BBK, BMI, BSI und Bundeswehr (ZMZ).

Das Modulare Warnsystem (MoWaS) dient dabei als zentrale Schnittstelle für vertrauenswürdige Information und Krisenwarnung. Unternehmen sollten sich frühzeitig in diese Kommunikationsflüsse integrieren, um konsistente Lagebilder und abgestimmte Botschaften zu gewährleisten.

In hybriden Konflikten gilt: „**Wer die Kommunikation kontrolliert, kontrolliert die Wahrnehmung.**“ Ein glaubwürdiger, verantwortungsvoller Kommunikationsstil stärkt nicht nur die Reputation, sondern auch die gesellschaftliche Resilienz – ein Beitrag zur Gesamtverteidigung.

## 3.16 Monitoring & Frühwarnsystem

### Relevanz

**Frühzeitige Information entscheidet über Handlungsspielräume.** In einer Zeit geopolitischer Instabilität, zunehmender Cyberbedrohungen und hybrider Einflussoperationen ist ein belastbares Frühwarnsystem der zentrale Baustein strategischer Resilienz. Es ermöglicht Unternehmen, Risiken proaktiv zu erkennen, zu bewerten und steuernd einzugreifen, bevor kritische Schwellen erreicht werden.

Corporate Security ist bestens qualifiziert hier eine Schlüsselrolle zu übernehmen: Als Schnittstelle zwischen Staat, Wirtschaft, Nachrichtendiensten und internen Fachbereichen koordiniert sie die Gesamtlagebeurteilung, integriert externe und interne Informationsquellen und leitet Entscheidungen für Management und Krisenstäbe ab.

### Zentrale Risiken

- Fehlende Integration von Lageinformationen aus staatlichen, privaten und internen Quellen.
- Verzögerte Erkennung sicherheitsrelevanter Trends (z.B. Cyberangriffe, Sabotage, geopolitische Eskalationen).
- Informationssilos und mangelnde Bewertungskompetenz im Unternehmen.
- Fehlende Abstimmung mit Behörden (BSI, ZMZ, CERT-Bund).
- Unzureichende Indikatoren zur Früherkennung von Versorgungs-, Personal- oder Infrastrukturrisiken.
- Fehlende Verbindung zwischen strategischem Risiko-Reporting und operativem Lagebild.

### Strategische Ziele

- Etablierung eines integrierten Lagebildsystems, das sicherheitsrelevante Informationen aus allen Quellen zusammenführt.
- Proaktive Früherkennung und Bewertung von Risiken im politischen, technologischen, physischen und digitalen Umfeld.
- Sicherstellung der Entscheidungsfähigkeit von Vorstand und Krisenstab durch aktuelle, verlässliche und konsolidierte Informationen.
- Nahtlose Anbindung an nationale und europäische Warn- und Informationsstrukturen (BSI, CERT, BBK, NATO, EU).
- Verankerung eines permanenten Frühwarnprozesses in der Governance der Corporate Security.

## Kritische Maßnahmen & Governance

- Einrichtung eines zentralen Lagezentrums (Security Intelligence Hub):  
Zusammenführung und Auswertung aller sicherheitsrelevanten Informationen (Cyber, Geo, Industrie, Personal, Security, Supply Chain).
- Staatliche Informationsschnittstellen:  
Direkte Anbindung an
  - BSI (Cyberwarnungen, CERT-Bund),
  - BMI / BBK (Krisen- und Bevölkerungsschutz),
  - BMVg / ZMZ (Zivil-Militärische Zusammenarbeit),
  - AA-Krisenzentrum / EU INTCEN (geopolitische Lagebilder).
- Private Intelligence-Dienste:  
Nutzung kommerzieller Anbieter für Cyber Threat Intelligence, OSINT, Satellitendaten und geopolitische Analysen.
- Internes Lagebild:  
Integration von Daten aus IT-Sicherheitsüberwachung, Werkschutz, Lieferkettenmonitoring, Personalverfügbarkeit und Facility Management.
- Kritische Partnerbewertung:  
Identifikation und Kategorisierung von Geschäftspartnern, Dienstleistern und Lieferanten nach Kritikalität („Single Points of Failure“).
- Frühwarnindikatoren (KPIs & Thresholds):  
Definition messbarer Frühwarnsignale (z.B. Lieferverzögerungen, Anomalien in Cyberlogs, regionale Eskalationsmeldungen).
- Reporting & Decision Support:  
Tägliche, wöchentliche oder anlassbezogene Lageberichte für CSO, CRO, CEO und Krisenstäbe.
- Automatisierung & KI-Nutzung:  
Einsatz von KI-gestützter Trendanalyse und Mustererkennung für Risikoentwicklungen (Cyber, Geo, Energie, Lieferkette).
- Kooperation mit Behörden:  
Teilnahme an branchenübergreifenden Sicherheits- und Lagebriefings (BSI-Allianz für Cyber-Sicherheit, BDI-Sicherheitsnetzwerke, ZMZ-Übungen).

## Politisch-strategische Einordnung

**Ein funktionierendes Frühwarnsystem ist nicht nur operativ, sondern strategisch systemrelevant.** Es schließt die Informationslücke zwischen Staat und Wirtschaft – ein zentrales Ziel der nationalen Sicherheitsstrategie (Bundeskanzleramt 2023) und des OPLAN DEU. Unternehmen, die über eigene Lagebild- und Analysekapazitäten verfügen, tragen aktiv zur nationalen Resilienz bei.

Im Zusammenspiel mit den Behörden entsteht eine Public-Private Intelligence-Struktur, die

- Risiken schneller erkennt,
- operative Reaktionszeiten verkürzt und
- staatliche Entscheidungsprozesse unterstützt.

Damit kann sich Corporate Security zur **Frühwarninstanz der Unternehmensführung** entwickeln – ein entscheidender Faktor für Sicherheit, Wettbewerbsfähigkeit und gesamtgesellschaftliche Stabilität.

## 4 Handlungsempfehlungen

Unternehmensresilienz (Corporate Resilience) kann nicht allein im operativen Tagesgeschäft entstehen – sie erfordert strategische Führung und gelebte Verantwortung auf der obersten Führungsebene. Die Zeichen sind unmissverständlich: geopolitische Unsicherheit, hybride Bedrohungen und verschärfte Regulierung. Resilienz ist längst keine freiwillige Kür mehr, sondern Pflichtaufgabe für Aufsichtsrat, Vorstand und Geschäftsführung - im Konzern ebenso wie im Mittelstand. Der OPLAN DEU verdeutlicht den Paradigmenwechsel: Die Wirtschaft ist integraler Bestandteil der nationalen Sicherheitsarchitektur. Die Konsequenz ist klar: **Resilienz ist Chefsache.**

**Resilienz ist die neue Wettbewerbsfähigkeit** - ein handfester Wettbewerbsvorteil und zentraler Erfolgsfaktor. Die Fähigkeit, auch unter Druck handlungs- und lieferfähig zu bleiben, wird zum zentralen Maßstab unternehmerischer Exzellenz. Wer in Krisen lieferfähig bleibt, gewinnt seine Aufträge, die Wettbewerber verlieren. Wer transparent kommuniziert, bindet langfristig Kunden und Investoren. Strategische Weitsicht, operative Vorbereitung und glaubwürdige Kommunikation **zahlen direkt auf die Bottom Line ein** – auf Umsatz, Gewinn, Marke, Reputation, finanzielle Stabilität sowie Unternehmenswert – und machen Unternehmen zum verlässlichen Partner in ihrer Rolle als systemrelevante Akteure der nationalen Sicherheit.

Investitionen in strategische und operative Resilienzmaßnahmen sind Investitionen in Geschäftskontinuität, robuste Geschäftsmodelle und langfristige Ertragskraft. Resiliente Unternehmen sichern ihre Position unter den globalen Technologie- und Innovationsführern. **Es ist Zeit zu handeln – jetzt, nicht erst morgen.**

### 4.1 Corporate Resilience Framework (CRF)

Der Corporate Resilience Framework (CRF) definiert die strategischen Verantwortlichkeiten, Governance-Strukturen und operativen Maßnahmen, die erforderlich sind, um die Handlungsfähigkeit eines Unternehmens in Krisen-, Spannungs- und Verteidigungsfällen zu sichern. **Er unterstützt kleine wie große Unternehmen dabei**, sich gegen hybride Bedrohungen und geopolitische Herausforderungen zu wappnen und **ein unternehmens-individuelles Resilienz-System aufzubauen**. Hierzu gliedert sich der Corporate Resilience Framework (CFR) in vier Ebenen:

- Strategische Führung durch CEO & C-Suite
- Governance, Compliance & Operating Model
- Corporate Security Organisation (CSO-Office)
- Resilienz-Maßnahmenprogramm (strategisch & operativ)

## 4.2 Rolle von CEO & C-Suite

Die Unternehmensführung trägt die Gesamtverantwortung für Resilienz, Sicherheit und Funktionsfähigkeit des Unternehmens. Sie legt den strategischen Rahmen fest und steuert Prioritäten, Ressourcen und Entscheidungen.

- Resilienz- und Risikoanalyse initiieren:  
Ganzheitliche Bewertung aller Unternehmensbereiche (Energie, Lieferkette, Personal, IT, Kommunikation, Finanzen).
- Verankerung in der Unternehmensstrategie:  
Resilienz und Sicherheit als feste Komponenten von ESG, Nachhaltigkeit und Governance-Berichtspflichten (CSRD).
- Einrichtung eines „Resilience Steering Committee“ zur bereichsübergreifenden Steuerung auf Vorstandsebene (CEO, CSO, CFO, CISO, HR).
- Strategische Verantwortung verankern:  
Zuständigkeiten auf Vorstandsebene (CEO, CFO, COO, CSO, CISO) definieren
- Strategische Investitionen in Resilienz priorisieren:  
Aufbau redundanter Systeme, Schutz kritischer Infrastruktur, Diversifizierung von Lieferketten, Stärkung der Cyberabwehr.
- Wertschöpfungskette unter Verteidigungsbedingungen prüfen:  
Stärkung der Widerstandsfähigkeit von Wertschöpfungsketten und betriebsrelevanten Kernprozessen, Entwicklung eines *Business Model im Spannungsfall* – nicht zu verwechseln mit BCM-Normalbetrieb.
- Kooperation mit Staat und Bundeswehr institutionalisieren:  
Teilnahme an ZMZ-Strukturen, KRITIS-Allianzen und behördlichen Lagebriefings.
- Krisenübungen auf Vorstandsebene:  
Regelmäßige Tabletop-Übungen mit realistischen Szenarien (z. B. Blackout, Cyberangriff, Lieferausfall).

### 4.3 Governance, Compliance & Operating Model

Dieser Abschnitt definiert Strukturen, Prozesse und Werkzeuge, mit denen Resilienz gesteuert, gemessen und weiterentwickelt wird. Governance schafft Klarheit über Verantwortlichkeiten, Berichtswege und Entscheidungslogiken.

#### 4.3.1 GOVERNANCE-STRUKTUR

- Aufbau eines Governance- und Compliance-Rahmens Spannungsfall – Definition von Rollen, Eskalationswegen, Meldepflichten und Haftungsgrenzen.
- Verankerung klarer Entscheidungs-, Eskalations- und Berichtslinien zwischen operativer Ebene und Vorstand.
- Enge Verzahnung mit IT-Security, HR, Supply Chain, Facility Management und Kommunikation.
- Sicherstellung der rechtlichen Konformität mit relevanten Vorgaben (Arbeitssicherstellungsgesetz, KRITIS-Verordnung, BSI-Gesetz, NIS2).
- Dokumentation von Entscheidungswegen und Risikobewertungen zur Nachweisführung gegenüber Aufsichtsbehörden und Versicherern.

#### 4.3.2 REPORTING & RESILIENZ-DASHBOARD

Ein transparentes, datenbasiertes Reporting schafft Steuerungs- und Entscheidungsfähigkeit. Es verknüpft operative Resilienzmaßnahmen mit strategischer Unternehmensführung und dokumentiert die Wirksamkeit der getroffenen Vorkehrungen.

- Reporting-Framework:  
Entwicklung eines standardisierten Resilienz-Reportings (Krisenstatus, Risiken, Maßnahmen, Trends),  
Monatliche Berichterstattung an Vorstand, Aufsichtsrat und zuständige Behörden.  
Integration in bestehende Governance- und Audit-Prozesse (Risikomanagement, Compliance, ESG, CSRD)
- Resilienz-Dashboard:  
Etablierung eines KPI-gestützten Dashboards zur laufenden Bewertung. Berichterstattung an Vorstand und Aufsichtsrat über Bedrohungslage, Maßnahmenstatus und Resilienzwirkung.
- Kennzahlen (KPIs):  
Energieautarkiegrad, Wiederanlaufzeit kritischer Systeme (Recovery Time Objective), Cybervorfallreaktionszeit, Personalverfügbarkeit in Schlüsselprozessen, Lieferfähigkeit bei Infrastrukturfähigkeit

- Berichterstattung im Geschäftsbericht:  
Integration eines *Resilience Index* als Steuerungsgröße – analog zu ESG-Kriterien (ökonomisch, ökologisch, sozial, sicherheitspolitisch).
- Review & Lessons Learned:
  - Nach jeder Übung und jedem Vorfall Evaluation der Wirksamkeit, Anpassung der Strategien und Prozesse,
  - Nachbereitung aller Krisen, Übungen und Sicherheitsvorfälle („After Action Review“).
  - Dokumentation von Erkenntnissen und Integration in Richtlinien, Schulungen und Prozesse;
  - Systematische Anpassung des Resilienz-Frameworks an neue Bedrohungslagen und regulatorische Anforderungen.  
Regelmäßige Überprüfung der Wirksamkeit des Corporate Resilience Frameworks
- Externe Transparenz & ESG-Integration
  - Berücksichtigung sicherheits- und resilienzrelevanter Aspekte in ESG- und Nachhaltigkeitsberichten (CSRD).
  - Nutzung des Resilience Index als ergänzende Steuerungsgröße neben ökonomischen Kennzahlen.
  - Offenlegung relevanter Sicherheits- und Risikomaßnahmen gegenüber Stakeholdern (Behörden, Investoren, Öffentlichkeit).

## 4.4 Rolle von Corporate Security

Corporate Security ist eine **wesentliche strategische Säule der Unternehmensresilienz** (Knoppe 2025, 2024). Sie gewährleistet den Schutz von Menschen, Werten sowie Informationen und stellt die Verbindung zwischen staatlicher Sicherheitsarchitektur<sup>7</sup> und betrieblicher Resilienzsteuerung her. Corporate Security ist die zentrale Einheit zur Bewertung strategischer Resilienzfaktoren und liefert potenzielle Szenarien (z.B. geopolitische Risiko- und Erfolgsfaktoren in den Wertschöpfungsketten), die die Bottom Line der Unternehmen nachhaltig beeinflussen können. Daher eignet sich Corporate Security als zentrale Resilienzplattform, um unternehmensweite Resilienzprozesse zu entwickeln, zu steuern und die Handlungs- und Wertschöpfungsfähigkeit der Unternehmen auch unter Krisen und hybriden Bedrohungen zu ermöglichen.

### 4.4.1 STRATEGISCHE AUFGABEN VON CORPORATE SECURITY<sup>8</sup>

- Aufbau des Resilience Steering Committees und Verankerung der CSO-Funktion.
- Strategische Szenarientwicklung mit Bezug zu geopolitischen, technologischen und wirtschaftlichen Veränderungen (Entscheidungsgrundlagen für die Geschäftsleitung).
- Entwicklung und Umsetzung einer integrierten Resilienz- und Sicherheitsstrategie für den Krisen- und Verteidigungsfall.
- Aufbau und Betrieb eines integrierten Resilienz- und Informationssystems zur Lagebildführung, Bedrohungsanalyse und Frühwarnung.
- Abwehr von Spionage, Sabotage und hybriden Angriffen, einschließlich Cyber-, Desinformations- und Insider-Bedrohungen.
- Design-to-Resilience: Integration von Resilienz- und Sicherheitsaspekten in alle Geschäftsprozesse.
- Schutz und Aufrechterhaltung der Funktionsfähigkeit kritischer Standorte, Systeme und Prozesse (physisch, digital, personell).
- Einrichtung klarer Kommunikationswege in Krisen: interne und externe Eskalationsmatrix (Management, Behörden, Partner).
- Steuerung und Priorisierung sicherheitsrelevanter Ressourcen in Abstimmung mit Vorstand und Behörden.

---

<sup>7</sup> z.B. BMI, BMW, BMVg, Nachrichtendienste, KRITIS-Netzwerken etc.

<sup>8</sup> Checkliste siehe Anhang 4

#### 4.4.2 OPERATIVE AUFGABEN VON CORPORATE SECURITY<sup>9</sup>

- Lagebildführung und Unterstützung der Krisenkommunikation und Sicherstellung konsistenter Informationen im Sinne des One-Voice-Prinzips.
- Schnittstellenmanagement zu Behörden, Bundeswehr, NATO-Partnern Nachrichtendiensten und Sicherheitsnetzwerken.
- Standortsicherung: Schutz kritischer Standorte, Anlagen und Mitarbeiter.
- Mitarbeitersicherheit (z.B. Evakuierung).
- Sicherheitskulturförderung, Awareness und Training im gesamten Unternehmen.
- Schulung und Sensibilisierung aller Mitarbeitenden im Bereich Sicherheitsbewusstsein, Verhalten in Krisen und Resilienz.
- Regelmäßige Audits und Übungen, um Wirksamkeit und Reaktionsfähigkeit zu überprüfen.

#### 4.5 Resilienz-Maßnahmenprogramm

Dieser Abschnitt bündelt alle operativen und technischen Maßnahmen, die zur Stabilisierung, Absicherung und Wiederherstellungsfähigkeit beitragen. Strategische Resilienz-Programme sichern die Handlungsfähigkeit des Unternehmens in Krisen, Spannungs- oder Verteidigungsfällen. Sie überbrücken operative Ausfälle, stabilisieren kritische Prozesse und stellen sicher, dass Energie, IT, Lieferketten und Kommunikation auch unter staatlicher Steuerung oder Infrastrukturengpässen funktionsfähig bleiben.

Zeithorizont: 30 bis 180 Tage nach Eintritt einer Krise.

##### 4.5.1 SOFORTPROGRAMM (0-30 TAGE)

- **Aufbau eines unternehmensweiten Krisenstabs:**  
Klare Rollen, klare Kommunikationsmatrix (intern/extern) und Entscheidungsprozesse; Anbindung an Behördenstrukturen (BSI, ZMZ, BBK).
- **Sicherung kritischer Prozesse:**  
Energieversorgung, IT-Betrieb, Kommunikation, Transportlogistik.
- **Reservisten- und Notfallpersonalmanagement:**  
Erfassung von Schlüsselpersonal, Freistellungsregeln und Mindestbesetzungsplänen. Sicherstellung der Mindestbesetzung und Handlungsfähigkeit auf allen Ebenen.

---

<sup>9</sup> Checkliste siehe Anhang 5

- **Kommunikation & Informationsfluss:**  
One-Voice-Prinzip etablieren; Kommunikationshandbuch und Freigabeprozesse festlegen.
- **Kontaktaufnahme mit Behörden:**  
Registrierung in regionalen ZMZ-Strukturen, Austausch mit Katastrophenschutz, IHK, BBK. KRITIS-Netzwerken

#### 4.5.2 STABILISIERUNGSPROGRAMM (30 – 180 TAGE)

- **Redundante Energie- und IT-Systeme:**  
Aufbau alternativer Energiequellen, Notstrom, Backup-Rechenzentren, Offline-Betriebsfähigkeit.
- **Lieferketten & Märkte diversifizieren:**  
Dual Sourcing, Nearshoring, Bevorratung kritischer Materialien, Absicherung von Transportwegen.
- **Cyber-Resilienz erhöhen:**  
Zero-Trust-Architektur, Netzwerksegmentierung, Notfallkommunikation, Cyberübungen.
- **Szenarienplanung:**  
Entwicklung von Krisen- und Verteidigungsszenarien inkl. Markt-, Personal- und Kommunikationsdimension.
- **Governance-Rahmen etablieren:**  
Klare Zuständigkeiten, Eskalationspfade, Compliance- und Haftungsbewertung (z. B. Arbeitssicherstellungsgesetz, KRITIS-Verordnung).
- **Lagerhaltung & Versorgung:**  
Bevorratung kritischer Produkte und Materialien für 30–90 Tage.
- **Branchenkooperationen:**  
Vernetzung mit Partnern zur wechselseitigen Absicherung in Krisenfällen.

#### 4.5.3 TECHNISCHE RESILIENZ

- Aufbau redundanter Energie- und IT-Systeme zur Aufrechterhaltung des Betriebs im Inselmodus (Notstrom, Offline-IT, unabhängige Datennetze).
- Implementierung autarker Kommunikationsinfrastrukturen (Satellit, Kurzwelle, Out-of-Band-Systeme) für Führungs- und Meldefähigkeit.
- Etablierung von Backup-Rechenzentren und segmentierten Netzwerken, um Betriebsfähigkeit trotz externer Cyber- oder Infrastrukturausfälle zu gewährleisten.

- Integration von Energie- und IT-Notfallplänen in das Business-Continuity- und Krisenmanagement.

#### **4.5.4 OPERATIVE RESILIENZ (LIEFERKETTEN, MÄRKTE, RESSOURCEN)**

- Diversifizierung und Regionalisierung von Lieferketten und Absatzmärkten; Aufbau regionaler Backup-Strukturen zur Reduzierung von Abhängigkeiten.
- Einrichtung von Lagerbeständen und Bevorratungsstrategien für kritische Materialien, Ersatzteile und Betriebsmittel (Horizont: 30–90 Tage).
- Anpassung von Markt- und Produktstrategien an geopolitische und sicherheitsrelevante Veränderungen.
- Durchführung regelmäßiger Stresstests für Lieferfähigkeit unter realistischen Krisenszenarien.

#### **4.5.5 KOOPERATIONEN & NETZWERKE**

- Institutionalisierung von Partnerschaften mit staatlichen Stellen (BSI, ZMZ, BBK, Bundeswehr, IHK).
- Teilnahme an branchenübergreifenden Sicherheits- und Resilienznetzwerken („alle statt einer“).
- Förderung von gegenseitiger Unterstützung zwischen Unternehmen, insbesondere bei Logistik, Energieversorgung und IT-Infrastruktur.
- Regelmäßige Krisen- und Kommunikationsübungen mit Behörden und Partnern.

## 5 Branchenbeispiele im Kontext des OPLAN Deutschland

Die Branchenbeispiele basieren auf der aktuellen Situation der militärisch-hybriden Intensivierung und deren Bedeutung für die industrielle Wertschöpfung. Flankierend wirken weitere internationale Handelsrestriktionen, Lieferengpässe und internationale Zölle, die wirtschaftliche Wertschöpfung deutscher und europäischer Unternehmen verschärfen. Erste Auswirkungen sind bereits in der Wirtschaft zu spüren. An dieser Stelle werden nur einige der wichtigsten Industrien exemplarisch dargestellt, da eine detaillierte Auflistung aller Branchen den Rahmen dieses Whitepapers sprengen würde.

### 5.1 Lebensmittelindustrie & Logistik

Die hybride Bedrohung durch Russland stellt für die Lebensmittelindustrie und die allgemeine Lebensmittelversorgung eine vielschichtige Herausforderung dar. Eine Eskalation könnte weitreichende wirtschaftliche Folgen haben.

#### Herausforderungen

Schon während der Covid-19 Pandemie kam es vor allem zu logistischen Engpässen. Gerade durch hybride Bedrohungen oder eine Ausweitung des Konflikts drohen sich diese durch militärische Priorisierung oder Sabotage zu verschärfen. Dies würde zu erheblichen Verzögerungen in der gesamten Wertschöpfungskette führen, was sich vor allem in der Versorgung der Bevölkerung durch eine stark eingeschränkte Warenverfügbarkeit äußert. Verstärkt wird dies durch Fluchtbewegungen oder Einberufung von Reservisten ausgelösten Mangel an Personal, vor allem in den Bereichen Landwirtschaft, Logistik und Vertrieb. Dies hat eine direkte Auswirkung auf den Betrieb von Filialen, Logistikzentren und Transportflotten.

Neben den direkten Auswirkungen auf den Lebensmitteleinzelhandel wird vor allem die Verfügbarkeit von Rohstoffen einen unmittelbaren Effekt auf die Versorgung haben. Durch gestörten internationalen Handel, Sanktionen oder Exportverbote können Rohstoffe für die Lebensmittelproduktion nur sehr eingeschränkt oder gar nicht verfügbar sein. Die extreme Unsicherheit und die drohenden Engpässe werden in der Bevölkerung zu verstärkten Hamsterkäufen führen, was die angespannte Warenverfügbarkeit weiter verschärft und zu einer ungleichen Verteilung innerhalb der Bevölkerung führen kann.

#### Fazit

All diese Faktoren würden maßgeblich zu drastisch steigenden Lebensmittelpreisen beitragen. Engpässe, erhöhte Produktionskosten und Transportrisiken würden direkt an die Verbraucher weitergegeben, was die Lebenshaltungskosten massiv erhöht und die Kaufkraft der Haushalte mindert.

## 5.2 Automobilindustrie

Die Automobilbranche zählt in Deutschland zu den umsatzstärksten und beschäftigungsintensivsten Branchen. Hunderttausende Mitarbeitende arbeiten bei Herstellern, Zulieferern und Dienstleistern entlang einer komplexen Wertschöpfungskette. Aufgrund ihrer hohen wirtschaftlichen und gesellschaftlichen Bedeutung stellt die Automobilindustrie ein attraktives Ziel hybrider Einfluss- und Angriffsformen dar. Durch gezielte Störungen der Produktion oder die Verbreitung von Desinformation lassen sich erhebliche wirtschaftliche Schäden verursachen und gleichzeitig Verunsicherung in der Bevölkerung erzeugen. Unternehmen entlang der gesamten Lieferkette müssen sich daher frühzeitig auf ein breites Spektrum potenzieller Sicherheitsvorfälle einstellen – von Cyberangriffen, Spionage und Ausspähung über Sabotage bis hin zu Desinformationskampagnen und physischen Anschlägen.

Die Zuverlässigkeit der Lieferkette ist wesentlicher Bestandteil der Aufrechterhaltung der Produktion. Ausfälle führten hier in der Vergangenheit zu Beeinträchtigungen bis hin zum Produktionsausfall.

### Herausforderungen

Die deutsche Automobilbranche bezieht viele Teile aus Osteuropa, unter anderem aus Polen. Eine Ausweitung des Szenarios zwischen der NATO und Russland auf Polen hätte weitreichende Folgen auf die gesamte deutsche Automobilindustrie und deren Zulieferer, unter anderem durch die Beeinträchtigung der dortigen Märkte und Lieferketten.

Viele Teile, wie elektronische Steuergeräte (ECUs), Hochvolt (HV)-Batterieteile, Sensorik sowie Karosserieteile, werden dort produziert und nach Deutschland geliefert. Ein Konflikt würde die Produktion beeinflussen und Transportwege sowie Logistikprozesse im äußersten Falle ganz blockieren. Just-in-Time und Just-in-Sequence Prozesse in Deutschland wären ohne Redundanzen und funktionierenden BCM-Prozesse gefährdet.

Polen ist ein Absatzmarkt, auch für Elektrofahrzeuge (EVs) und Plug-in-Hybride (PHEVs). Ein militärischer Konflikt würde die Kaufkraft für Automobile beeinträchtigen. Hinzu kommen mögliche Exportverbote in Konfliktregionen, auch für sensible Technologien, die in Fahrzeugteilen verbaut sind.

**Schon im Vorfeld eines Konflikts** könnten sich Energie- und damit Produktionspreise drastisch erhöhen, die Preise für die Versorgung der ansässigen Zulieferer mit Rohstoffen wie Lithium, Kobalt und Nickel würde ebenso steigen.

Letztlich würde auch die Investition in Forschung von Zukunftstechnologien wie autonomes Fahren und Digitalisierung von Fahrzeugen stagnieren oder ganz ausbleiben, was sich nachhaltig im globalen Wettbewerb auswirkt.

## Fazit

Die Automobilindustrie sollte bereits jetzt ihre Standort- und Cybersicherheitsmaßnahmen gezielt ausbauen und das Krisenmanagement umfassend weiterentwickeln. Dazu gehören die regelmäßige Aktualisierung von Notfall- und Reaktionsplänen, praxisnahe Schulungen und Übungen sowie der Aufbau alternativer Zuliefer- und Logistikstrukturen. Viele dieser Maßnahmen erfordern einen zeitlichen Vorlauf, etwa die Qualifizierung und Integration neuer Zulieferer im Falle eines Ausfalls durch hybride oder militärische Einwirkungen. Nur durch frühzeitige Vorbereitung kann die Branche ihre Widerstandsfähigkeit gegenüber komplexen Bedrohungslagen stärken.

## 5.3 Energiebranche

Die Energiebranche zählt zu den kritischen Infrastrukturen (KRITIS) und nimmt eine zentrale Rolle in der gesamtstaatlichen Verteidigungsplanung im Rahmen des OPLAN DEU ein. Energieerzeuger und Netzbetreiber tragen maßgeblich zur Versorgungssicherheit bei und stellen potenzielle Ziele für hybride Angriffe dar.

Verschlechtert sich die Sicherheitslage weiter, ohne dass es zu offenen Kampfhandlungen kommt, steigt die Bedrohung durch Cyberangriffe, Sabotageakte und gezielte Desinformationskampagnen. Energieunternehmen sind daher gefordert, ihre Resilienz in mehreren Bereichen zu stärken. Dazu gehört die priorisierte Versorgung, also die Sicherstellung der Energiezufuhr für z.B. militärische Einrichtungen, Krankenhäuser und andere kritische Infrastrukturen. Ergänzend müssen erhöhte Sicherheitsmaßnahmen getroffen werden, etwa durch zusätzliche physische und digitale Schutzvorkehrungen wie Zugangskontrollen, Netzsegmentierung und ein kontinuierliches 24/7-Monitoring.

## Herausforderungen

Auch die Krisenorganisation spielt eine entscheidende Rolle: Unternehmen müssen gegebenenfalls an Lagebesprechungen teilnehmen, behördliche Weisungen zügig umsetzen und benötigen daher interne Krisenstäbe zur Koordination dieser Maßnahmen. Für den Notfallbetrieb ist die Vorhaltung von Ersatzstromkapazitäten sowie eine ausgeprägte Blackout-Resilienz erforderlich. Im Rahmen des Business Continuity Managements müssen insbesondere Personal- und Ressourcenausfälle berücksichtigt werden. Schlüsselpersonal kann für militärische oder Blaulichtaufgaben abgezogen werden, ebenso können LKW-Fahrer, Ausrüstung oder Flächen vom Militär angefordert werden. Unternehmen sind daher angehalten, Verfügbarkeiten zu ermitteln und Ersatzkapazitäten sowie flexible Logistiklösungen einzuplanen.

## Fazit

Der OPLAN DEU verdeutlicht, dass Energieversorgung nicht nur eine wirtschaftliche, sondern auch eine sicherheitspolitische Aufgabe ist. Unternehmen müssen ihre Notfall- und Krisenpläne regelmäßig aktualisieren, ihr Personal entsprechend schulen und in

technische, digitale sowie organisatorische Resilienz investieren, um auch bei Personalausfällen und Ressourcenengpässen handlungsfähig zu bleiben.

Besonders herausfordernd ist im Bereich der Stromversorgung das Zusammenspiel zwischen den verschiedenen Akteuren; Erzeuger, Übertragungsnetzbetreiber, Verteilnetzbetreiber und Bundesnetzagentur. Dieses muss geübt werden, um im Bedarfsfall adäquat reagieren und Stromausfälle begrenzen bzw. die Versorgung schnell wiederherstellen zu können.

Hinzu kommt, dass alle Erzeuger und Netzbetreiber wirtschaftlich selbstständige Unternehmen sind, die Maßnahmen nur im Rahmen gesetzlicher Vorgaben und unter Berücksichtigung von Wirtschaftlichkeitsfaktoren umsetzen können.

## 5.4 Kultur & Medien

Der Sektor Kultur und Medien ist Teil der kritischen Infrastrukturen (KRITIS) und spielt eine zentrale Rolle für die gesellschaftliche Resilienz, Meinungsbildung und Identitätsstiftung, insbesondere im Spannungs- und Verteidigungsfall. Kulturelle Einrichtungen, Medienhäuser und journalistische Akteure sind nicht nur Träger demokratischer Werte, sondern können auch Ziel hybrider Bedrohungen sein.

Bei einer erheblichen Verschlechterung der Sicherheitslage ohne offene Kampfhandlungen steigt die Bedrohungslage für Kultur- und Medieneinrichtungen erheblich. Die Angriffe erfolgen vor allem im digitalen Raum, über Desinformation und gezielte Destabilisierung der öffentlichen Meinung.

### Herausforderungen

- Desinformationskampagnen: Verbreitung prorussischer Narrative über soziale Medien, Deepfakes und manipulierte Inhalte zur Spaltung der Gesellschaft
- Physische- oder Cyberangriffe auf Rundfunk- und Medienhäuser
- Zielgerichtete Angriffe auf Kulturgüter: Sabotage oder digitale Löschung von Kulturerbe (z. B. digitale Archive, Mediatheken)
- Einschränkung journalistischer Arbeit: Behinderung oder gezielte Diskreditierung von Medienschaffenden

## Rolle des Modularen Warnsystems (MoWaS)<sup>10</sup>

- Verbreitung verlässlicher Informationen zur Warnung der Bevölkerung: MoWaS wird genutzt, um Warnmeldungen, Verhaltensempfehlungen und Klarstellungen über Radio, Fernsehen, Apps (z. B. NINA) und Cell Broadcast zu verbreiten.
- Koordination mit Rundfunk- und Medienhäusern: Öffentlich-rechtliche sind verpflichtet und private Sender angehalten, MoWaS-Meldungen zu übernehmen und redaktionell einzuordnen, um die Bevölkerung zu warnen.
- Risiko: Manipulation oder Überlastung von MoWaS-Schnittstellen durch Cyberangriffe könnte die Glaubwürdigkeit staatlicher Kommunikation gefährden.

## Fazit

Im Verteidigungsfall wird der Sektor Kultur und Medien Teil der gesamtstaatlichen Verteidigungsarchitektur. Die Anforderungen steigen erheblich, insbesondere im Bereich der Informationshoheit, Kulturgutsicherung und gesellschaftlichen Resilienz.

- Aufrechterhaltung der Berichterstattung: Medienhäuser müssen trotz möglicher Evakuierungen, Stromausfällen oder Personalengpässen senden können. Ausgebildetes Personal, für Berichterstattungen aus Krisen- und Kriegsgebieten.
- Bekämpfung von Desinformation: Staatliche Stellen und Medien müssen eng kooperieren, um Falschinformationen schnell zu identifizieren und zu entkräften.
- Kulturelle Resilienz stärken: Kulturangebote (z. B. Musik, Theater, Literatur) können zur Stabilisierung der Bevölkerung beitragen.
- Schutz kultureller Einrichtungen: Museen, Theater, Archive und Denkmäler sowie Rundfunk- und Medienhäuser müssen gegen physische Angriffe oder Plünderungen gesichert werden
- Zentrale Warn- und Informationsplattform: MoWaS wird ggf. zur primären Schnittstelle für staatliche Kommunikation mit der Bevölkerung.
- Integration mit Kultur- und Medienakteuren: Kommunikationspartner wie Telekommunikationsanbieter oder Medienunternehmen erhalten über MoWaS aktuelle Lageinformationen und Handlungsempfehlungen zur Kommunikation.

---

<sup>10</sup> Das **Modulare Warnsystem (MoWaS)** ist das zentrale technische System, über das in Deutschland offizielle Warnmeldungen zu Gefahrenlagen verbreitet werden. Es wird vom Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) betrieben (siehe [https://www.bbk.bund.de/DE/Warnung-Vorsorge/Warnung-in-Deutschland/MoWaS/mowas\\_node.html](https://www.bbk.bund.de/DE/Warnung-Vorsorge/Warnung-in-Deutschland/MoWaS/mowas_node.html)).

- Erweiterung der Reichweite: Nutzung von Kurzwellenradio, Lautsprecherfahrzeugen, Cell Broadcast, Warn-Apps und digitalen Anzeigetafeln zur Sicherstellung der Informationsverbreitung bei Ausfall klassischer Medien.

Der Sektor Kultur und Medien ist nicht nur Träger von Information und Identität, sondern auch ein strategisches Ziel hybrider Bedrohungen. Die Sicherung kultureller Einrichtungen, die Gewährleistung unabhängiger Berichterstattung und die Verteidigung gegen Desinformation sind sicherheitspolitische Aufgaben. MoWaS spielt dabei eine Schlüsselrolle als vertrauenswürdiger Kommunikationskanal zwischen Staat, Medien und Bevölkerung.

## 5.5 Luft- und Raumfahrtindustrie

Die Luft- und Raumfahrtindustrie zählt zu den wirtschaftlich bedeutendsten Hochtechnologiebranchen Europas. Sie verbindet hohe Wertschöpfungstiefe, langfristige Innovationszyklen und globale Exportmärkte mit kritischen Infrastrukturen für Kommunikation, Navigation und Logistik. Als dualer Sektor (zivil/militärisch) ist sie zugleich zentral für technologische Souveränität und für die industrielle Resilienz Deutschlands und Europas. Zu den industriellen Kernbereichen zählen:

- Transport- und Aufklärungsflotten sowie deren Betrieb und Wartung (Air Mobility, ISR),
- Satelliten- und Kommunikationssysteme,
- zivile und militärische Flughäfen als logistische Knotenpunkte,
- Fertigungs- und Wartungsbetriebe (OEMs, MROs, Zulieferer),
- europäische Raumfahrtprogramme (Galileo, Copernicus, IRIS<sup>2</sup>) sowie
- industrielle Schlüsselakteure (z.B. Airbus, OHB, MT Aerospace, Safran, Thales Alenia).

### Herausforderungen

Die Branche ist global eingebunden, forschungsintensiv und von Zulieferern mit extrem hoher Spezialisierung abhängig. Entsprechend groß ist ihre Verwundbarkeit gegenüber geopolitischen, technologischen und logistischen Disruptionen. Wesentliche Belastungsfaktoren sind:

- Cyber- und Sabotageangriffe auf Produktions-, Steuerungs- und Satellitensysteme
- Ausfall kritischer Zulieferer und Logistikketten (Titan, Elektronik, Software)
- Energie- und Kommunikationsengpässe bei Betrieb von Werken, Flughäfen und Bodenstationen
- Angriffe auf Flughäfen oder Luftraum-Infrastruktur (z.B. GPS-Störungen, Drohnen)

- Spionage gegen Hochtechnologie und geheime Entwicklungsprogramme
- Politische Abhängigkeiten bei globalen Lieferketten (z.B. Titan aus Russland, Komponenten aus Asien)
- Exportrestriktionen und Sanktionen bei militärisch relevanten Technologien
- Ausfälle von Satelliteninfrastruktur durch Cyberangriffe oder Kollisionen im Orbit
- Verlust von Fachpersonal durch Mobilmachung, Evakuierung oder Überlastung
- Drohnen- und GPS-Interferenzaktionen im Umfeld kritischer Flughäfen oder Testgelände.
- Desinformation gegen Rüstungs- und Luftfahrtkonzerne („Kriegsprofiteure“, „Militärintdustrie“).
- Sabotageversuche gegen Energie- und Kommunikationsknoten, insbesondere an Standorten mit militärischer oder dualer Funktion.
- Störungen von Datenverbindungen zu Satelliten und Bodenkontrollzentren.

Für Unternehmen bedeutet dies: steigender Bedarf an Diversifizierung, strategischer Redundanz und resilienten Partnerschaften innerhalb Europas.

Im Krisen- oder Verteidigungsfall wird die Branche unmittelbarer Bestandteil der gesamtstaatlichen Sicherheits- und Versorgungsketten. Wirtschaftlich entscheidend sind:

- Bereitstellung militärischer Transportkapazitäten (Truppen, Material, Verwundete).
- Aufrechterhaltung des Flug- und Wartungsbetriebs unter erhöhten Sicherheitsbedingungen.
- Beteiligung an Satelliten-, Kommunikations- und Aufklärungssystemen für NATO und EU.
- Priorisierung von Energie- und Ersatzteilversorgung für militärische Flotten und Raumfahrtinfrastruktur.
- Integration ziviler Luftfahrtbetriebe in militärische Lufttransportlogistik (Host Nation Support).
- Verpflichtungen nach Arbeitssicherstellungsgesetz (ASG) für technisches und flugbetriebliches Personal.
- Sicherstellung der Flug- und Betriebssicherheit bei gleichzeitiger militärischer Nutzung ziviler Infrastruktur

- Schutz von Weltrauminfrastruktur (Satelliten, Bodenstationen, Datenleitungen)
- Kontinuität der Lieferketten bei hochspezialisierten Zulieferern
- Gewährleistung von Cyber-, Geheim- und Spionageschutz in internationalen Kooperationen
- Resiliente Energie- und Kommunikationsversorgung für Produktions- und Kontrollstandorte
- Koordination mit Behörden, BMVg, BMWI, BSI, DLR und NATO-Agenturen
- Akzeptanz und Vertrauen der Öffentlichkeit in militärisch-zivile Nutzung

### **Fazit**

Für Management und Eigentümer ergibt sich daraus ein unmittelbarer Einfluss auf Geschäftskontinuität, Vertragserfüllung, Lieferfähigkeit und Unternehmensreputation. Die Resilienz der Luft- und Raumfahrtindustrie beeinflusst unmittelbar die wirtschaftliche Wettbewerbsfähigkeit und technologische Zukunftsfähigkeit Europas. Ein wirtschaftlich widerstandsfähiger Luft- und Raumfahrtsektor erhöht nicht nur die Sicherheit Europas, sondern schützt zugleich Wertschöpfung, Innovationskraft und langfristige Marktpositionierung seiner Unternehmen. Nur durch vorausschauende Investitionen, robuste Lieferketten und koordinierte Kooperation zwischen Industrie, Staat und europäischen Partnern kann die Luft- und Raumfahrtindustrie ihre Rolle als wirtschaftliches Rückgrat und Innovationstreiber Europas langfristig sichern.

## 5.6 Sicherheitsdienstleister & Private Security - Auswirkungen auf Unternehmen

Sicherheitsdienstleister stellen für viele Unternehmen im Normalbetrieb einen wesentlichen Bestandteil der Standort- und Veranstaltungssicherheit dar. Im Spannungs- und Verteidigungsfall kann ihre Verfügbarkeit jedoch erheblich eingeschränkt sein. Grund dafür sind die Regelungen der Sachleistungs-, Sicherstellungs- und Vorsorgegesetze sowie mögliche staatliche Dienstverpflichtungen. **Sicherheitsdienstleister können dadurch teilweise oder vollständig abgezogen** und staatlich für höher priorisierte Schutzaufgaben eingesetzt werden – insbesondere im Bereich kritischer und verteidigungsrelevanter Infrastruktur. Obwohl die Bewachung solcher Objekte grundsätzlich von Polizei und Heimatschutzkräften vorgesehen ist, ist deren Personalumfang begrenzt. Daher ist mit einer staatlichen Inanspruchnahme privater Sicherheitskräfte zu rechnen. Unternehmen müssen folglich bereits im Frieden einkalkulieren, dass externe Bewachungsleistungen im Krisenfall nur eingeschränkt oder gar nicht mehr verfügbar sind.

### Herausforderungen

Privatwirtschaftliche Standorte – auch solche mit hohen Sicherheitsanforderungen – könnten im Verteidigungsfall nur eingeschränkt geschützt werden. Unternehmen müssen daher frühzeitig Strukturen schaffen, um Personal, kritische Prozesse und Immobilien eigenständig zu sichern.

| Bereich                          | Mögliche Einschränkung   | Rechtsgrundlage / Begründung                     |
|----------------------------------|--|--|
| Personalverfügbarkeit            | Sicherheitskräfte können einberufen oder dienstverpflichtet werden → Personal fällt aus.                     | Wehrpflichtrecht / § 13 ZSKG                     |
| Priorisierung von Schutzobjekten | Staat priorisiert kritische Infrastruktur → Bewachung privatwirtschaftlicher Liegenschaften wird nachrangig. | Sicherheits- und Verteidigungsplanung des Bundes |
| Vertragslage                     | Private Bewachungsverträge können eingeschränkt oder zeitweise ausgesetzt werden.                            | Überragendes öffentliches Interesse              |
| Staatlicher Zugriff              | Polizei/Bundeswehr können Bewachungsaufgaben übernehmen oder anordnen.                                       | GG Art. 87a, Wehr- und Polizeirecht              |
| Material- und Logistikengpässe   | Schutzausstattung und Fahrzeuge können knapp oder staatlich priorisiert werden.                              | Sicherstellungsgesetze                           |

## Fazit

Da externe Sicherheitsdienstleister im Krisenfall nur eingeschränkt verfügbar sind, ist der Aufbau eines internen Reserveteams sinnvoll. Ziel ist die minimal erforderliche Sicherung systemkritischer Standorte. Dieses Team kann aus folgenden Gruppen bestehen:

- Corporate-Security-Personal (aus weniger kritischen Bereichen)
- Mitarbeitenden mit militärischer oder behördlicher Vorverwendung (soweit nicht dienstverpflichtungsgefährdet)
- technisch geschultem Personal (Facility Management, Technik)

Zur Reduzierung des Risikos eines vollständigen Wegfalls externer Dienstleister können Unternehmen prüfen:

- Vertragliche Regelungen zur Einsatzpflicht im Krisenfall, soweit rechtlich möglich
- Einsatz ausländischer Sicherheitsdienstleister, deren Personal schwerer dienstverpflichtbar sein könnte
- jedoch Abwägung von Sicherheitsrisiken, höheren Kosten und potenziellen Einflussmöglichkeiten des Herkunftsstaates
- Absprachen zwischen Unternehmen und Staat, insbesondere bei verteidigungsrelevanter Infrastruktur, um Abzüge zu vermeiden oder Unterstützung durch Territorialkräfte zu erhalten

**Bewertung:** Auslandspersonal kann potenzielle Verfügbarkeit erhöhen, erhöht aber Wirtschafts- und Spionagerisiken. Eine betriebliche Priorisierung stellt sicher, dass knappe Sicherheitsressourcen zielgerichtet eingesetzt werden können.

| Kategorie                     | Bedeutung   | Beispiele  | Bewachungspriorität                        |
|-------------------------------|---|--|--|
| <b>A</b><br>systemkritisch    | Unverzichtbar für Produktion oder sicherheitsrelevante Leistungen | Rechenzentrum, Produktionskern, F&E mit Schutzbedarf | Sehr hoch (intern + extern + Behörden)     |
| <b>B</b><br>betriebsnotwendig | Für Betrieb relevant, aber reduzierbar                            | Verwaltungsgebäude, Ersatzlager                      | Mittel (eingeschränkte Bewachung)          |
| <b>C</b><br>nachrangig        | Temporär stilllegbar  | Gästehäuser, Schulungszentren                        | Niedrig (technische Sicherung ausreichend) |

Ergänzend sollten technische Systeme verstärkt werden, um den Wegfall von Personal teilweise zu kompensieren:

- resiliente Zutrittskontrollsysteme
- verstärkte Videoüberwachung und Sensorik
- semi-autonome Überwachungssysteme (Drohnen, Robotik)
- redundante Energieversorgung (Generatoren, Netzersatzanlagen) für kritische Systeme

Sicherheitsdienstleister sind im Friedensbetrieb verlässliche Partner, im Spannungs- oder Verteidigungsfall jedoch nur eingeschränkt verfügbar. Für Unternehmen entsteht dadurch ein **strategisches Risiko für Standortsicherheit, Betriebsfähigkeit und Know-how-Schutz**.

Durch interne Reservekapazitäten, Priorisierung, technische Redundanzen und frühzeitige Abstimmung mit Staat und externen Dienstleistern lässt sich dieses Risiko signifikant reduzieren und die betriebliche Resilienz nachhaltig stärken.

## 6 Zentrale Fragen der Industrie im Kontext des OP-Plan DEUTSCHLAND

Die deutsche Wirtschaft sieht sich mit zunehmender Unsicherheit über ihre Rolle, Verantwortung und Rechte innerhalb des OPLAN DEU im Kontext der Gesamtverteidigung konfrontiert. Viele Unternehmen, insbesondere Betreiber kritischer Infrastrukturen (KRITIS) und exportorientierte Industrien, erkennen erhebliche Informationsdefizite über rechtliche, organisatorische und operative Abläufe im Spannungs-, Verteidigungs- oder Bündnisfall.

Die folgenden Fragen, die aus verschiedenen Industrieverbänden, Sicherheitsnetzwerken und Unternehmensdialogen hervorgegangen sind, verdeutlichen den **strukturellen Orientierungsbedarf** zwischen Staat, Wirtschaft und Bundeswehr. Sie lassen sich in zehn Themenfelder gliedern.

### 6.1 Strukturelle Defizite

Fünf übergeordnete Problemfelder prägen derzeit die Industrieperspektive:

- Unklare Priorisierungen und Zuständigkeiten – insbesondere bei Energie, Transport, Personal und Cyberabwehr.
- Fehlende Transparenz rechtlicher Mechanismen – etwa bei Mobilmachung, Weisungsbefugnissen und Meldepflichten.
- Unzureichende Kommunikationsstrukturen – zwischen Unternehmen, Behörden, Bundeswehr und Ländern.
- Lückenhafte Koordination bei Cyber-, KRITIS- und Lieferkettenrisiken.
- Fehlende Regelungen für Entschädigung und Haftung bei staatlicher Inanspruchnahme.

Empfohlen wird daher die Einrichtung eines „**Industrieforums OPLAN DEU**“ als ständiges Koordinations- und Dialoggremium zwischen Bundesregierung, Bundeswehr, Industrieverbänden und Schlüsselunternehmen.

### 6.2 Energieversorgung & Priorisierung

- Wie erfolgt die Priorisierung der Energie- und Treibstoffversorgung im Spannungs- oder Verteidigungsfall?
- Welche Sektoren gelten als priorisiert, und nach welchen Kriterien erfolgt die Einstufung?
- Gibt es Zuteilungsquoten oder Kontingente für Industrie, KRITIS- und Verteidigungsunternehmen?

- Wer koordiniert die Verteilung von Energie und Rohstoffen zwischen ziviler Wirtschaft und Bundeswehr?
- Wie werden Unternehmen informiert und eingebunden, sobald Priorisierungsmaßnahmen greifen?
- Welche Ausnahmeregelungen oder Notfallmechanismen gelten bei drohendem Produktionsstopp?

### **6.3 Mobilmachung & Rechtlicher Rahmen**

- Wie sind die Mobilmachungsregelungen für Unternehmen und Mitarbeitende ausgestaltet?
- Welche rechtlichen Verpflichtungen ergeben sich aus den Eskalationsstufen (Zustimmungs-, Spannungs-, Verteidigungs-, Bündnisfall)?
- Wie wird mit Reservisten und Schlüsselpersonal in sicherheitsrelevanten Unternehmen verfahren?
- Welche Gesetze greifen, wenn die NATO militärisch reagiert, ohne dass Deutschland den Verteidigungsfall erklärt?
- Welche Behörden besitzen Weisungsbefugnis gegenüber Unternehmen, und wie werden Entscheidungen kommuniziert?

### **6.4 Lieferketten, Märkte & Transport**

- Bestehen Liefer- oder Transportprioritäten zugunsten der Bundeswehr oder NATO, die zivile Unternehmen betreffen?
- Welche Transportkorridore werden militärisch reserviert, und wie erfolgt Koordination und Entschädigung?
- Welche staatlichen Mechanismen zur Kostenerstattung gibt es bei Nutzung ziviler Kapazitäten?
- Wie kann Planungssicherheit für Lieferketten und Absatzmärkte gewährleistet werden?

### **6.5 Cyber-Security & Informationslage**

- Wie erfolgt die Meldung und Unterstützung bei Cyberangriffen – über BSI, CERT-Bund, ZMZ-Stellen oder Länder?
- Wie können Unternehmen in staatliche Lagebilder (Cyber- und Hybride Bedrohungen) integriert werden?

- Welche Meldepflichten und Informationskanäle gelten im Spannungs- oder Verteidigungsfall?
- Wie werden klassifizierte Informationen sicher an Industriepartner weitergegeben?
- Welche staatlichen Mechanismen gegen Desinformation existieren, die gezielt Unternehmen angreifen?

## **6.6 Staatliche Inanspruchnahme, Haftung & Entschädigung**

- Nach welchen Kriterien werden Standorte oder Ressourcen für militärische Zwecke herangezogen?
- Wie wird die Kostenerstattung oder Entschädigung bei staatlicher Nutzung geregelt?
- Welche Standardverfahren oder Antragswege existieren (BBK, BMVg, Länder)?
- Wie werden Haftungsfragen und Versicherungsschutz behandelt, wenn Unternehmen auf Weisung handeln?

## **6.7 Kommunikation, Behörden & Governance**

- Gibt es eine zentrale Anlaufstelle für Unternehmen, um Fragen zum OPLAN DEU zu klären?
- Besteht eine Koordinationsstelle Wirtschaft–Bundeswehr oder ein nationales Resilienz-Sekretariat?
- Welche Rolle übernehmen ZMZ-Stellen in der direkten Wirtschaftskommunikation?
- Wie erfolgt die Befehlskette und Eskalation zwischen Bund, Ländern und Wirtschaft?
- Gibt es ein zentrales Informationsportal oder Lage-Dashboard, über das Weisungen, Priorisierungen und Lagen kommuniziert werden?

## **6.8 KRITIS, Priorisierung & Schutz**

- Wie werden Unternehmen als KRITIS-, verteidigungswichtig oder verteidigungsrelevant eingestuft?
- Welche Behörde informiert über diese Kategorisierung und daraus entstehende Pflichten?
- Welche Schutz- und Fördermechanismen bestehen für diese Unternehmen (z.B. Sicherheitsbegleitung, Förderprogramme)?
- Wie werden staatliche Resilienzprogramme (KRITIS-Dachgesetz, NIS2, Cyber Resilience Act) koordiniert und kommuniziert?

## 6.9 Regionale & Operative Umsetzung

- Wo befinden sich die Convoy Support Centers (CSCs), und welche Rolle spielen sie für Industrie und Logistik?
- Welche operativen Auswirkungen ergeben sich für Unternehmen in ihrer Umgebung (Sicherheitsauflagen, Zugang, Nutzung)?
- Wie werden Unternehmen in regionale OPLAN-Umsetzungsstrukturen eingebunden?

## 6.10 Ergänzende Grundsatzfragen

- Wie wird der Daten- und Geheimschutz bei wachsender zivil-militärischer Kooperation gewährleistet?
- Wie werden europäische Mechanismen (NATO, EU, Strategic Compass, Military Mobility) national integriert?
- Wie werden KMU ohne eigene Sicherheitsorganisation unterstützt?
- Welche Rolle übernehmen Wirtschaftsverbände (BDI, VCI, Bitkom, BDLI etc.) in der Koordination?
- Wie wird sichergestellt, dass Resilienzmaßnahmen wirtschaftlich tragfähig bleiben?
- Wie werden gemeinsame Übungen und Planspiele zwischen Wirtschaft, Behörden und Bundeswehr institutionalisiert?

### Fazit:

Die Industriefragen zeigen deutlich: Zwischen Staat, Wirtschaft und Bundeswehr bestehen erhebliche Koordinations-, Kommunikations- und Rechtslücken. Eine verbindliche, transparente Struktur – **etwa durch ein Industrieforum OPLAN DEU oder eine Task Force Wirtschaft & Resilienz** – ist erforderlich, um Planungssicherheit, Handlungskompetenz und Vertrauen herzustellen. Nur durch institutionalisierte Zusammenarbeit lässt sich die Funktionsfähigkeit der deutschen Wirtschaft im Spannungs- und Verteidigungsfall sichern.

## 7 Ansprechpartner und Netzwerke

| Institution  | Zuständigkeit   |
|--|---|
| <b>BMI</b>   | Innere Sicherheit, Gesamtkoordination der Zivilverteidigung |
| <b>BMVg / Bundeswehr (ZMZ)</b>   | Militärische Unterstützung, Host Nation Support             |
| <b>BBK</b>   | Bevölkerungsschutz, KRITIS-Koordination                     |
| <b>BSI (Bundesamt für Sicherheit in der Informationstechnik) / CERT-Bund</b> | Cyberlage, Angriffserkennung, Meldewesen                    |
| <b>BMWE</b>  | Wirtschaftliche Steuerung, Industriekoordination            |
| <b>IHK / BDI / Branchenverbände</b>  | Informationsweitergabe, Austausch mit Unternehmen           |
| <b>THW / Länder / Katastrophenschutzbehörden</b>                             | Operative Unterstützung im Krisenfall                       |
| <b>VSW</b>   |   |
| <b>ZMZ-Strukturen der Bundeswehr / regionale Ansprechpartner</b>             |   |

## Anhang: Auszüge rechtlicher Rahmen & Checklisten

### Anhang 1: Personal und Arbeitsfähigkeit

| <b>Gesetz / Rahmen</b>                  | <b>Inhalt / Bedeutung</b>  |
|---|--|
| Art. 12 GG                              | Pflicht zu militärischem oder zivilem Dienst im Verteidigungsfall.                                   |
| Arbeitssicherstellungsgesetz (ASG, § 3) | Staatliche Sicherstellung von Arbeitsleistungen für Zwecke der Verteidigung.                         |
| Zivildienstgesetz (§ 79 ZDG)            | Möglichkeit der Heranziehung bislang zurückgestellter Personen im Spannungs- oder Verteidigungsfall. |
| Katastrophenschutzgesetz & ZMZ-Doktrin  | Zusammenarbeit zwischen Wirtschaft, Behörden und Bundeswehr im Zivilschutz.                          |

## Anhang 2: Governance

| Gesetz / Rahmen                                  | Inhalt / Bedeutung  |
|--|---|
| <b>Grundgesetz (Art. 80a, 115a)</b>              | Definition von Spannungs- und Verteidigungsfall, Aktivierung von Sicherstellungsgesetzen. |
| <b>Arbeitssicherstellungsgesetz (ASG)</b>        | Staatliche Sicherstellung von Arbeitsleistungen für Verteidigungszwecke (§§ 1–3).         |
| <b>Verteidigungswirtschaftsverordnung (VWiV)</b> | Regelung staatlicher Eingriffe in Produktions- und Lieferprozesse.                        |
| <b>Sicherstellungs- und Versorgungsgesetze</b>   | Steuerung kritischer Ressourcen (Energie, Ernährung, Transport).                          |
| <b>NIS2 / KRITIS-Dachgesetz</b>                  | EU-weiter Rahmen zur Gewährleistung digitaler und physischer Resilienz.                   |
| <b>BGB / HGB</b>                                 | Haftungsfragen bei staatlicher Inanspruchnahme und Force-Majeure-Situationen.             |

## Anhang 3: Finanzen & Liquidität

| <b>Ebene</b>          | <b>Mechanismus / Institution</b>                                      | <b>Relevanz</b>  |
|-----------------------|---|--|
| <b>EU</b>             | <i>InvestEU / RRF / Solidarity Mechanism</i>                          | Unterstützt Unternehmen bei Wiederaufbau und Krisenfinanzierung. |
| <b>Bund</b>           | <i>KfW-Krisenprogramme, Bürgschaften BMWF / BMF</i>                   | Stützt Liquidität bei staatlich anerkannten Krisenlagen.         |
| <b>EZB / BaFin</b>    | <i>Liquidity Coverage Ratio (LCR), Counter-Cyclical Buffer (CCyB)</i> | Flexibilisierung von Kapitalpuffern im Krisenmodus.              |
| <b>Versicherungen</b> | <i>Krieg- und Terror-Ausschlüsse</i>                                  | Prüfung von Deckungslücken und Nachverhandlung erforderlich.     |

## Anhang 4: Checkliste Strategische Aufgaben von Corporate Security

### Resilienz-Governance

- 0 Aufbau eines Resilience Steering Committee auf Vorstandsebene
- 0 Verankerung der CSO-Funktion
- 0 Definition der unternehmensweiten Resilienzstrategie für Krisen-, Stress- und Verteidigungsfälle

### Strategische Frühaufklärung & Szenarien (Corporate Foresight Security)

- 0 Entwicklung eines mehrdimensionalen Szenariomodells (Geopolitik, Technologie, Cyber, Supply Chain, Regulierung)
- 0 Ableitung strategischer Handlungsoptionen für Geschäftsführung, Portfoliosteuerung und Standortpriorisierung
- 0 Bewertung der Resilienzfähigkeit aller Geschäftsbereiche, Wertschöpfungsstufen und kritischen Assets

### Design-to-Resilience

- 0 Integration von Resilienzprinzipien in Produktentwicklung, Standortsicherheit, Supply-Chain-Design, IT-Architektur und Personalprozesse
- 0 Sicherstellung, dass zentrale Produkte, Programme und Lieferketten unter Stress, Krisen oder feindlichem Einfluss stabil funktionieren

### Integriertes Sicherheits- und Lagebildsystem

- 0 Aufbau eines gesamtunternehmerischen Lagebilds aus Cyber, Physical, Geo, Personal, Business Continuity, Intelligence, Lieferkette
- 0 Einführung eines Frühwarn- und Analyseprogramms, das strategische Trends und Bedrohungen in faktenbasierte Steuerungsimpulse übersetzt

### Schutz vor komplexen Bedrohungen

- 0 Entwicklung eines Verteidigungsmodells zur Abwehr hybrider Angriffe: Cyberoperationen, Desinformation, Insider, Spionage, Sabotage, Lieferkettengriffe
- 0 Aufbau eines intelligence-gestützten Sicherheitsprogramms (inkl. strategischer Kooperationen mit Behörden, Partnern, NATO-Strukturen)

### Strategische Kommunikationsarchitektur (Crisis & Influence Management)

- 0 Sicherstellung einer einheitlichen, souveränen und glaubwürdigen Kommunikationslinie gegenüber Behörden, Investoren, Mitarbeitenden und Öffentlichkeit
- 0 Aufbau eines OPLAN-DEU-kompatiblen Eskalations- und Freigabeprozesses

### Ressourcenpriorisierung und Entscheidungsunterstützung

- 0 Steuerung von Ressourcen, Budgets und kritischen Fähigkeiten auf Basis strategischer Risiken und Unternehmensprioritäten
- 0 Entscheidungsunterstützung für Geschäftsführung, Vorstand und Aufsichtsrat in sicherheitsrelevanten und geopolitischen Fragestellungen

## Anhang 5: Checkliste Operative Aufgaben von Corporate Security

### Lagebildführung & Krisenbetrieb

- 0 Betrieb eines integrierten Operation Centers für Lagebild, Monitoring und Reaktion.
- 0 Sicherstellung des One-Voice-Prinzips in Kommunikation und Entscheidungsfindung.
- 0 Unterstützung des Krisenstabs durch faktenbasierte Analytik und fachliche Bewertung.

### Behörden- und Netzwerkmanagement

- 0 Kontinuierliche Koordination mit Behörden, Bundeswehr, Geheimdiensten, NATO-Partnern, KRITIS-Netzwerken, Industrieverbänden.
- 0 Betreuung aller Schnittstellen gemäß den Anforderungen des OPLAN DEU, einschließlich Mobilmachung, Transport, Energie, Schutz kritischer Assets.

### Schutz von Standorten, Systemen und Personal

- 0 Physische Sicherheit, Zutrittssteuerung, Perimeterschutz, Besuchermanagement.
- 0 Globale Arbeitnehmersicherheit inkl. Reise-, Evakuierungs- und Expat-Schutzprogrammen.
- 0 Schutz sensibler Standorte und Fertigungsketten.

### Cyber-, Informations- und Geheimschutz

- 0 Operative Abwehrmaßnahmen gegen Spionage, Datenabfluss, Sabotage, Social Engineering.
- 0 Umsetzung des Geheimschutzes gemäß nationalen Vorgaben (GHB, Sicherheitsüberprüfungen).
- 0 Enge Verzahnung von physischer Sicherheit, OT-Security und Cyberabwehr.

### Übungen, Audits & Sicherheitskultur

- 0 Regelmäßige Übungen (Stress-/Red-Team-Übungen, Behördenübungen, Mobilmachungstests).
- 0 Schulung aller Mitarbeitenden zur Stärkung der Sicherheits- und Resilienzkultur.

## Literatur

1. **Bafa (2021)**. Die neue EU-Dual-Use-Verordnung (Verordnung (EU) 2021/821). [https://www.bafa.de/SharedDocs/Downloads/DE/Aussenwirtschaft/afk\\_merkblatt\\_eu-dual-use-vo.pdf?\\_\\_blob=publicationFile&v=2](https://www.bafa.de/SharedDocs/Downloads/DE/Aussenwirtschaft/afk_merkblatt_eu-dual-use-vo.pdf?__blob=publicationFile&v=2) zuletzt aufgerufen am 11.12.2025
2. **BBK (2025a)**. Kritische Infrastrukturen [https://www.bbk.bund.de/DE/Themen/Kritische-Infrastrukturen/kritische-infrastrukturen\\_node.html?utm\\_source=chatgpt.com](https://www.bbk.bund.de/DE/Themen/Kritische-Infrastrukturen/kritische-infrastrukturen_node.html?utm_source=chatgpt.com) zuletzt aufgerufen am 11.12.2025
3. **BBK (2025b)**. Sektoren und Branchen. [https://www.bbk.bund.de/DE/Themen/Kritische-Infrastrukturen/Sektoren-Branchen/sectoren-branchen\\_node.html](https://www.bbk.bund.de/DE/Themen/Kritische-Infrastrukturen/Sektoren-Branchen/sectoren-branchen_node.html) zuletzt aufgerufen am 11.12.2025
4. **BBK (2025c)**. Zivil-Militärische Zusammenarbeit (ZMZ). [https://www.bbk.bund.de/SharedDocs/Downloads/DE/Krisenmanagement/zmz-flyer.pdf?\\_\\_blob=publicationFile&v=5](https://www.bbk.bund.de/SharedDocs/Downloads/DE/Krisenmanagement/zmz-flyer.pdf?__blob=publicationFile&v=5) zuletzt aufgerufen am 11.12.2025
5. **BBK (2021)**. Bundesamt für Bevölkerungsschutz und Katastrophenhilfe. Definitionen von Schutzziele für Kritische Infrastrukturen. Forschung im Bevölkerungsschutz, Band 28. [https://www.bbk.bund.de/SharedDocs/Downloads/DE/KRITIS/definition\\_von\\_schutzzielen\\_fuer\\_kritis.pdf?\\_\\_blob=publicationFile&v=4](https://www.bbk.bund.de/SharedDocs/Downloads/DE/KRITIS/definition_von_schutzzielen_fuer_kritis.pdf?__blob=publicationFile&v=4) zuletzt aufgerufen am 11.12.2025
6. **BfV (2025a)**. Bundesamt für Verfassungsschutz. Verfassungsschutzbericht 2024 [https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/verfassungsschutzberichte/2025-06-10-verfassungsschutzbericht-2024.pdf?\\_\\_blob=publicationFile&v=4&utm\\_source=chatgpt.com](https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/verfassungsschutzberichte/2025-06-10-verfassungsschutzbericht-2024.pdf?__blob=publicationFile&v=4&utm_source=chatgpt.com) zuletzt aufgerufen am 11.12.2025
7. **BfV (2025b)**. Bundesamt für Verfassungsschutz. Gefährdung durch russische Spionage, Sabotage und Desinformation. [https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/spionage-und-proliferationsabwehr/2025-05-gefaehrdungen-durch-russische-spionage-sabotage-und-desinformation.pdf?\\_\\_blob=publicationFile&v=5](https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/spionage-und-proliferationsabwehr/2025-05-gefaehrdungen-durch-russische-spionage-sabotage-und-desinformation.pdf?__blob=publicationFile&v=5) zuletzt aufgerufen am 11.12.2025
8. **Bitkom (2025)**. Studie Wirtschaftsschutz 2025 (DE) [https://www.bitkom.org/Bitkom/Publikationen/Studie-Wirtschaftsschutz?utm\\_source=chatgpt.com](https://www.bitkom.org/Bitkom/Publikationen/Studie-Wirtschaftsschutz?utm_source=chatgpt.com) zuletzt aufgerufen am 11.12.2025
9. **BMI (2024)**. Rahmenrichtlinien für die Gesamtverteidigung – Gesamtverteidigungsrichtlinien – (RRGV). [https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/sicherheit/RRGV.pdf?\\_\\_blob=publicationFile&v=4](https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/sicherheit/RRGV.pdf?__blob=publicationFile&v=4) zuletzt aufgerufen am 11.12.2025
10. **BMI (2023a)**. Deutsche Strategie zur Stärkung der Resilienz gegenüber Katastrophen. [https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/BMI22017-resilienz-katastrophen.pdf?\\_\\_blob=publicationFile&v=3](https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/BMI22017-resilienz-katastrophen.pdf?__blob=publicationFile&v=3) zuletzt aufgerufen am 11.12.2025
11. **BMI (2023b)**. Bundesministerium des Innern. Positionspapier „KRITIS-Dachgesetz“ [https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/stellungnahmen/kritis-dg/stn-up-kritis.pdf?\\_\\_blob=publicationFile&v=3](https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/stellungnahmen/kritis-dg/stn-up-kritis.pdf?__blob=publicationFile&v=3) zuletzt aufgerufen am 11.12.2025
12. **BMVg (2023)**. Verteidigungspolitische Richtlinien 2023 Bundesministerium der Verteidigung zuletzt aufgerufen am 11.12.2025
13. **BMWK (2024a)**. Bundesministerium für Wirtschaft und Klimaschutz. Bundesbericht Energieforschung 2024 Energie- und Rohstoffsicherheitsanalysen. <https://www.bundeswirtschaftsministerium.de/Redaktion/DE/Publikationen/Energie/240716-bundesbericht-energieforschung-2024.html> zuletzt aufgerufen am 11.12.2025
14. **BMWK (2024b)**. Bundesministerium für Wirtschaft und Klimaschutz. Systementwicklungsstrategie 2024 [https://www.bundeswirtschaftsministerium.de/Redaktion/DE/Publikationen/Klimaschutz/2024-systementwicklungsstrategie.pdf?\\_\\_blob=publicationFile&v=10](https://www.bundeswirtschaftsministerium.de/Redaktion/DE/Publikationen/Klimaschutz/2024-systementwicklungsstrategie.pdf?__blob=publicationFile&v=10) zuletzt aufgerufen am 11.12.2025

15. **BNetzA (2025)**. Bundesnetzagentur Monitoringbericht 2025.  
<https://data.bundesnetzagentur.de/Bundesnetzagentur/SharedDocs/Mediathek/Monitoringberichte/MonitoringberichtEnergie2025.pdf> zuletzt aufgerufen am 11.12.2025
16. **BNetzA (2024)**. Bundesnetzagentur Monitoringbericht 2024.  
<https://data.bundesnetzagentur.de/Bundesnetzagentur/SharedDocs/Mediathek/Monitoringberichte/MonitoringberichtEnergie2024.pdf> zuletzt aufgerufen am 11.12.2025
17. **BSI (2024)**. Bundesamt für Sicherheit in der Informationstechnik. Die Lage der IT-Sicherheit in Deutschland 2024.  
[https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2024.pdf?\\_\\_blob=publicationFile&v=5](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2024.pdf?__blob=publicationFile&v=5) zuletzt aufgerufen am 11.12.2025
18. **Bundeskanzleramt (2023)**. Integrierte Sicherheit für Deutschland. Nationale Sicherheitsstrategie.  
<https://www.nationalesicherheitsstrategie.de/Sicherheitsstrategie-DE.pdf> zuletzt aufgerufen am 11.12.2025
19. **Bundestag (2025a)**. Fragen zur Notwendigkeit eines umfassenden Lagebilds zu Sabotage, Spionage und Desinformation. Drucksache 21/995  
<https://dserver.bundestag.de/btd/21/009/2100995.pdf> zuletzt aufgerufen am 11.12.2025
20. **Bundestag (2025b)**. Hybride Angriffe und Desinformation im Vorfeld der Bundestagswahl. Drucksache 20/14595  
<https://dserver.bundestag.de/btd/20/145/2014595.pdf> zuletzt aufgerufen am 11.12.2025
21. **Bundestag (2024a)**. Umsetzung Nationale Sicherheitsstrategie. Drucksache 20/13542  
<https://dserver.bundestag.de/btd/20/135/2013542.pdf> zuletzt aufgerufen am 11.12.2025
22. **Bundestag (2024b)**. Bericht zur Risikoanalyse für den Zivilschutz 2023.  
<https://dserver.bundestag.de/btd/20/104/2010476.pdf> zuletzt aufgerufen am 11.12.2025
23. **Bundeswehr (2025)**. Operationsplan Deutschland  
<https://www.bundeswehr.de/resource/blob/5920008/5eb62255741addec3f38d49a443d0282/booklet-operationsplan-deutschland-data.pdf> zuletzt aufgerufen am 11.12.2025
24. **DIN SPEC 14027 (2024)**. Geschäftsplan: Corporate Security - Anforderungen zur Stärkung physischer Resilienz von Organisationen  
<https://www.din.de/de/forschung-und-innovation/din-spec/alle-geschaeftsplaene/wdc-beuth.din21:382621796/pdf-3562598> zuletzt aufgerufen am 11.12.2025
25. **Edwards, C.; Seidenstein, N. (2025)**. The Scale of Russian Sabotage Operations Against Europe's Critical Infrastructure. IISS. The International Institute for Strategic Studies.  
<https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2025/08/pub25-095-the-scale-of-russian-sabotage-operations.pdf> zuletzt aufgerufen am 11.12.2025
26. **EEAS (2024)**. Strategic Compass: ANNUAL PROGRESS REPORT on the Implementation of the Strategic Compass for Security and Defence.  
[https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1\\_en](https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en) zuletzt aufgerufen am 11.12.2025
27. **EU-Commission 2025**. Commission Staff Working Document on Military Mobility. COM (2025) 847 final.  
[https://transport.ec.europa.eu/document/download/c925bad5-7d13-4551-bfaa-03152dd468dd\\_en?filename=SWD\\_2025\\_847.pdf](https://transport.ec.europa.eu/document/download/c925bad5-7d13-4551-bfaa-03152dd468dd_en?filename=SWD_2025_847.pdf) zuletzt aufgerufen am 11.12.2025
28. **EU-Commission (2023)**. European Commission, Joint Research Centre (JRC) (2023). Hybrid Threats : A Comprehensive Resilience Ecosystem  
[https://www.hybridcoe.fi/wp-content/uploads/2023/04/CORE\\_comprehensive\\_resilience\\_ecosystem.pdf](https://www.hybridcoe.fi/wp-content/uploads/2023/04/CORE_comprehensive_resilience_ecosystem.pdf) zuletzt aufgerufen am 11.12.2025
29. **EU-Commission (2022a)** Cyber Resilience Act (2022). EU-Commission. Regulation (EU) 2024/2847.  
<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R2847> zuletzt aufgerufen am 11.12.2025
30. **EU-Commission (2022b)**. NIS2 Directive: securing network and information systems. Directive 2022/2555.

- [https://digital-strategy.ec.europa.eu/en/policies/nis2-directive?utm\\_source=chatgpt.com](https://digital-strategy.ec.europa.eu/en/policies/nis2-directive?utm_source=chatgpt.com) zuletzt aufgerufen am 11.12.2025
31. **Grünbuch ZMZ 4.0 (2025)**. Bubendorfer-Licht, S.; Eckert, L.; Hahn, A.; Krings, G.; Schäfer, I. Zivil-Militärische Zusammenarbeit 4.0 im militärischen Krisenfall. Eine Situationsbeschreibung, Analyse und Handlungsempfehlungen.  
[https://zoes-bund.de/wp-content/uploads/2025/03/250306\\_Gruenbuch\\_ZMZ\\_digital.pdf](https://zoes-bund.de/wp-content/uploads/2025/03/250306_Gruenbuch_ZMZ_digital.pdf) zuletzt aufgerufen am 11.12.2025
  32. **Hartmann, J. (2025)**. DGAP Policy Brief Nr. 15 Juni 2025. Hybride Kriegsführung. Lehren zur Stärkung der europäischen Handlungsfähigkeit  
[https://dgap.org/system/files/article\\_pdfs/15\\_DGAP%20Policy%20Brief%20Hybride%20Kriegsfuehrung%203.pdf](https://dgap.org/system/files/article_pdfs/15_DGAP%20Policy%20Brief%20Hybride%20Kriegsfuehrung%203.pdf) zuletzt aufgerufen am 11.12.2025
  33. **IFW (2024)**. Kiel Institute For The World Economy. Economic Outlook. No. 119(2024/Q4)  
[https://www.kielinstitut.de/fileadmin/Dateiverwaltung/IfW-Publications/fis-import/78097681-d900-4bfe-9428-838e8b4ff77e-KKB\\_119\\_2024-Q4\\_Welt\\_EN.pdf?utm\\_source=chatgpt.com](https://www.kielinstitut.de/fileadmin/Dateiverwaltung/IfW-Publications/fis-import/78097681-d900-4bfe-9428-838e8b4ff77e-KKB_119_2024-Q4_Welt_EN.pdf?utm_source=chatgpt.com) zuletzt aufgerufen am 11.12.2025
  34. **IMF (2024)**. World Economic Outlook. Policy Pivot, Rising Threats.  
<https://www.imf.org/-/media/files/publications/weo/2024/october/english/text.pdf> zuletzt aufgerufen am 11.12.2025
  35. **Kather, T. (2024)**. Nachgefragt. Wenn Russland die Nato angreifen würde, werden wir einen anderen Krieg sehen.  
<https://www.bundeswehr.de/de/meldungen/nachgefragt-nato-verteidigungsbuendnis-5809526> zuletzt aufgerufen am 11.12.2025
  36. **Knoppe, M. (2025)**. Corporate Security als nachhaltiger Wertschöpfungsfaktor. In: Knoppe, M. (eds) Nachhaltige Wirtschaftskonzepte. SDG - Forschung, Konzepte, Lösungsansätze zur Nachhaltigkeit. Springer Gabler, Wiesbaden.  
[https://doi.org/10.1007/978-3-658-47879-7\\_1](https://doi.org/10.1007/978-3-658-47879-7_1)
  37. **Knoppe (2024)**. Disruption und Wertschöpfung der Unternehmenssicherheit. In: Knoppe, M. (eds) Unternehmerische Wertschöpfung neu aufstellen. Springer Gabler, Wiesbaden.  
[https://doi.org/10.1007/978-3-658-42270-7\\_1](https://doi.org/10.1007/978-3-658-42270-7_1)
  38. **Metis (2024)**. Universität der Bundeswehr Metis Studie Nr. 42 (Tsetsos, K., 2024). Szenarien russischer Einflussnahme bis 2030. Hybride Einwirkung Russlands auf die EU/NATO-Ostflanke  
[https://metis.unibw.de/assets/pdf/metis-studie42-2024\\_12-rus\\_ostflanke.pdf](https://metis.unibw.de/assets/pdf/metis-studie42-2024_12-rus_ostflanke.pdf) zuletzt aufgerufen am 11.12.2025
  39. **NATO (2025a)**. Collective defence and Article 5.  
<https://www.nato.int/en/what-we-do/introduction-to-nato/collective-defence-and-article-5> zuletzt aufgerufen am 11.12.2025
  40. **NATO (2025b)**. Virtual Manipulation Brief  
<https://stratcomcoe.org/pdfs/?file=/publications/download/VMB-Final-5aa5d.pdf?zoom=page-fit> zuletzt aufgerufen am 11.12.2025
  41. **NATO (2024)**. Resilience, civil preparedness and Article 3.  
[https://www.nato.int/en/what-we-do/deterrence-and-defence/resilience-civil-preparedness-and-article-3?utm\\_source=chatgpt.com](https://www.nato.int/en/what-we-do/deterrence-and-defence/resilience-civil-preparedness-and-article-3?utm_source=chatgpt.com) zuletzt aufgerufen am 11.12.2025
  42. **OECD (2025)**. OECD Economic Outlook. Resilient Growth but with Increasing Fragilities Volume 2025/2, N.118.  
[https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/12/oecd-economic-outlook-volume-2025-issue-2\\_413f7d0a/9f653ca1-en.pdf](https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/12/oecd-economic-outlook-volume-2025-issue-2_413f7d0a/9f653ca1-en.pdf) zuletzt aufgerufen am 11.12.2025
  43. **Pöhlmann, M. (2025)**. Der Suwałki-Korridor. ZMSBw (Publikation / Opus).  
[https://opus4.kobv.de/opus4-zmsbw/files/861/AK38\\_Suwalki\\_Poehlmann\\_2025.pdf](https://opus4.kobv.de/opus4-zmsbw/files/861/AK38_Suwalki_Poehlmann_2025.pdf) zuletzt aufgerufen am 11.12.2025
  44. **Sperling, N. (2025)**. Hybride Bedrohungen. Die Bedrohung durch Russland im Cyber- und Informationsraum.  
[https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum/aktuelles/bedrohung-russland-cyber-informationsraum-5981306?utm\\_source=chatgpt.com](https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum/aktuelles/bedrohung-russland-cyber-informationsraum-5981306?utm_source=chatgpt.com) zuletzt aufgerufen am 11.12.2025

45. **SWP (2025)**. Polens Sicherheitspolitik: amerikanische Ungewissheit und europäisches Moment. Die Zweifel an den USA wachsen.  
[https://www.swp-berlin.org/publications/products/aktuell/2025A24\\_PolensSicherheitspolitik.pdf](https://www.swp-berlin.org/publications/products/aktuell/2025A24_PolensSicherheitspolitik.pdf) zuletzt aufgerufen am 11.12.2025
46. **SWP (2024)**. Die Neuvermessung der amerikanisch-europäischen Sicherheitsbeziehungen. Von Zeitwende zu Zeitwende. SWP-Studie 2024/S 15.  
[https://www.swp-berlin.org/publications/products/studien/2024S15\\_sicherheitsbeziehungen\\_usa\\_europa.pdf](https://www.swp-berlin.org/publications/products/studien/2024S15_sicherheitsbeziehungen_usa_europa.pdf) zuletzt aufgerufen am 11.12.2025

## Abkürzungsverzeichnis

### Abkürzung Bedeutung

|           |  |
|-----------|--|
| AA        | Auswärtiges Amt  |
| ASG       | Arbeitssicherstellungsgesetz                           |
| BDI       | Bundesverband der Deutschen Industrie                  |
| BBK       | Bundesamt für Bevölkerungsschutz und Katastrophenhilfe |
| BMF       | Bundesministerium der Finanzen                         |
| BMI       | Bundesministerium des Innern und für Heimat            |
| BMVg      | Bundesministerium der Verteidigung                     |
| BMWE      | Bundesministerium für Wirtschaft und Energie           |
| BCM       | Business Continuity Management                         |
| BNetzA    | Bundesnetzagentur                                      |
| BSI       | Bundesamt für Sicherheit in der Informationstechnik    |
| CERT-Bund | Computer Emergency Response Team des Bundes            |
| CSIRT     | Computer Security Incident Response Team               |
| CRF       | Corporate Resilience Framework                         |
| CSRD      | Corporate Sustainability Reporting Directive           |
| EDA       | European Defence Agency                                |
| EDF       | European Defence Fund                                  |
| ESG       | Environmental, Social, Governance                      |
| EU INTCEN | EU Intelligence and Situation Centre                   |
| ISR       | Intelligence, Surveillance, Reconnaissance             |
| ITAR/EAR  | US Exportkontrollrecht                                 |
| KRITIS    | Kritische Infrastrukturen                              |
| LCR       | Liquidity Coverage Ratio                               |
| MoWaS     | Modulares Warnsystem des Bundes                        |
| MRO       | Maintenance, Repair & Overhaul                         |
| NIS2      | EU-Richtlinie zur Netz- und Informationssicherheit     |
| OT        | Operational Technology                                 |
| OPLAN DEU | Operationsplan Deutschland                             |
| PHEV      | Plug-In Hybrid Electric Vehicle                        |
| RRF       | Recovery and Resilience Facility (EU)                  |
| VWiV      | Verteidigungswirtschaftsverordnung                     |
| ZMZ       | Zivil-Militärische Zusammenarbeit                      |
| ZSKG      | Zivilschutz- und Katastrophenhilfegesetz               |

Haben Sie Fragen oder Anregungen?

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

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



**Kontakt & Feedback**

Whitepaper 01 ThinkTank Corporate Resilience, 12.12.2025