THINKTANK
CORPORATE RESILIENCE
OPERATIONAL GUIDE 01

to the Strategic White Paper 02 “Geopolitical Change, AI and Entrepreneurial Options”

- Resilience in Practice -

VSW
Bundesverband

November 2026

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

Foreword

The Operational Guide 01 to Strategic White Paper 02 **provides tools for security, risk and crisis management, business continuity, procurement and compliance as well as resilience management** in the form of various working modules**.**

A total of nine working modules with checklists, analysis tools and the scenario stress test 2027-2030 have been derived from Strategic White Paper 02 “Geopolitical Change, AI and Entrepreneurial Options”. Strategic White Paper 02 contains the strategic assessment for management, executive boards and supervisory boards.

The ThinkTank Corporate Resilience and the VSW Bundesverband

At the interface of business, government and academia, the ThinkTank Corporate Resilience positions itself as a think tank and the VSW Bundesverband as the umbrella organization of the regional security associations of German industry. The aim is to shape resilience as a shared value-creating task, to provide orientation and to strengthen the dialogue between companies, policymakers and public authorities. In doing so, the ThinkTank Corporate Resilience supports the VSW's Vision 2029 of establishing itself as the leading authority for economic protection - as a point of contact, a source of ideas and a platform for knowledge transfer, further education and cooperation.

On behalf of the publisher ThinkTank Corporate Resilience

Prof. Dr. Marc Knoppe Johannes Strümpfel

The White Paper, Operational Guide and Executive Summary are available at:

Publisher:

ThinkTank Corporate Resilience: *Where business and academia think ahead*

The **ThinkTank Corporate Resilience** creates a platform on which strategic trends, geopolitical analyses and future scenarios from the resilience perspective of Chief Security Officers are brought together with the business perspective of CEOs, executive boards, supervisory boards and shareholders. It emerged from the close cooperation between business and academia at Technische Hochschule Ingolstadt in the field of "Value Creation through Corporate Security and Resilience" („Wertschöpfung durch Corporate Security und Resilienz") and is closely linked to the MBA program **Strategy, Global Risk & Security Management (Resilience Management)**.

The ThinkTank was initiated to offer C-suite representatives, Chief Security Officers and other executives from all business areas as well as public authorities a forum for forward-looking thinking and strategic exchange on systemic risks **from a business perspective**.

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 (Head of Group Security, Daimler Truck AG)

Alexander Klotz (Head of Group Security, BMW AG)

Marco Mille (Head of Corporate Security, Siemens AG)

Johannes Strümpfel (Siemens AG; President VSW Bundesverband)

Strategic Foresight Lab

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

in cooperation with the

VSW Bundesverband and the
Advisory Board of the MBA Strategy, Global Risk & Security Management at Technische Hochschule Ingolstadt.

Table of Contents

1 HOW TO USE THIS GUIDE 5

2 CONCRETE IMPACTS ON COMPANIES 7

2.1 Markets 7
2.2 Supply chains 8
2.3 Capital 8
2.4 Talent 9
2.5 Innovation 10
2.6 Raw material and energy supply 10
2.7 Locations and production 11
2.8 Employees, executives and key personnel 12
2.9 Artificial Intelligence 13

3 RISK MULTIPLIERS: WHEN CRISES FUEL EACH OTHER 14

3.1 Possible risk multipliers 14
3.2 Change of perspective: from individual risks to interconnected cascades 16
3.3 The six-point protection approach 16

4 RESILIENCE ARCHITECTURE: CAPABILITY MATURITY CHECK 17

4.1 Eight capabilities of a modern resilience architecture 18
4.2 Artificial Intelligence as a tool in resilience management 19
4.3 From analysis to implementation: first steps 20

5 CRITICAL DEPENDENCIES: DEPENDENCY MAPPING 22

6 SCENARIO STRESS TEST TOOLKIT 2027-2030 25

6.1 Scenario 1 - Large-scale conflict in Europe 26
6.2 Scenario 2 - Escalation in the Taiwan Strait as a geo-economic system shock 28
6.3 Scenario 3 - US-China technological decoupling 30
6.4 Scenario 4 - Strategic fragmentation of the transatlantic partnership 32
6.5 Simultaneity and combination of scenarios 34

7 INTERFACE BETWEEN GOVERNMENT AND BUSINESS 36

7.1 What the state offers 36
7.2 What companies think of it - and where the gaps are 36
7.3 Checklist: business requirements for the state 37
7.4 The shared vision 38

8 REGULATORY AND IMPLEMENTATION ROADMAP 39

8.1 THE OPERATIONAL PLAN FOR GERMANY (OPERATIONSPLAN DEUTSCHLAND, OPLAN DEU) ... 39
8.2 REGULATORY PRESSURE VERSUS ENTREPRENEURIAL ROOM FOR MANEUVER 40
8.3 NINE GAPS IN THE SYSTEM - SELF-DIAGNOSIS 41
8.4 IMPLICATIONS FOR COMPANIES - CONCRETE APPROACHES 42

9 MARKET ENTRY & DIVERSIFICATION 43

9.1 EU SINGLE MARKET 43
9.2 INDIA 43
9.3 SOUTHEAST ASIA (ASEAN) 43
9.4 GULF REGION 43
9.5 BRAZIL AND MERCOSUR 43
9.6 CHECKLIST: STRUCTURAL PREREQUISITES FOR MARKET ENTRY 44

10 OPPORTUNITY AREAS IN DETAIL 45

10.1 DEFENSE & DUAL-USE 45
10.2 INFRASTRUCTURE & ENERGY 45
10.3 DIGITAL SOVEREIGNTY 45
10.4 REGIONAL VALUE CREATION 46

REFERENCES 47

LIST OF ABBREVIATIONS 53

NOTE ON THIS DOCUMENT

1 How to use this guide

This Operational Guide 01 is the practice-oriented companion document to Strategic White Paper 02 “Geopolitical Change, AI and Entrepreneurial Options”. While the strategic white paper brings together the key facts and findings for management, executive boards and supervisory boards, this guide translates the same content into concrete working tools for operational practice. Put simply: Chapter 2 shows where geopolitical change takes effect; Chapter 3 explains why these points of impact reinforce one another; Chapters 4 and 5 describe the capabilities and knowledge a company needs to respond; Chapter 6 tests these capabilities in an emergency; Chapters 7 and 8 place the whole in relation to government and regulation; Chapters 9 and 10 reverse the perspective and show that the same vulnerability analysis is **at the same time a map of entrepreneurial opportunities**.

Target group

Chief Security Officers, corporate security and corporate resilience · Chief Information Security Officers and information security · Risk management and enterprise risk management · Business continuity and crisis management · Procurement and supply chain management · Compliance, legal and regulatory affairs · Strategy and business development.

Structure

The guide is divided into nine modules. Chapter 1 serves as an introduction; Modules 1 to 9 follow in Chapters 2 to 10.

The modules follow a working logic (understanding impacts, analyzing risks, building capabilities, mapping dependencies, testing scenarios, using interfaces with government and regulation, tapping opportunities) and therefore do not follow the chapter sequence of Strategic White Paper 02. Each module can be used independently - for example as the

basis for a workshop, a risk meeting or a tabletop exercise. Where useful, cross-references point to the corresponding summary in Strategic White Paper 02.

Module	Core content
1 - Function-specific measures	Markets, supply chains, capital, talent, innovation, raw material and energy supply, locations and production, employees and executives, Artificial Intelligence
2 - Risk multipliers	Ten possible amplifying factors, self-assessment, six-point protection approach
3 - Resilience architecture	Eight-capability maturity check, assessment scale, AI as a tool, first steps
4 - Critical dependencies	Dependency mapping in nine fields
5 - Scenario stress test 2027-2030	Four scenarios with three escalation levels each, worksheet, combination check
6 - Interface between government and business	National Economic Protection Strategy (Nationale Wirtschaftsschutzstrategie), eleven-point checklist, internal preparation
7 - Regulatory and implementation roadmap	OPLAN DEU, EU regulation, nine-gap diagnosis
8 - Market entry & diversification	Five strategic markets, checklist
9 - Opportunity areas in detail	Defense, infrastructure, digital sovereignty, regional value creation

The content builds on and deepens White Paper 02; sources are listed in the references.

2 Concrete impacts on companies

What companies can do in concrete terms - by dimension

Geopolitical developments affect key business dimensions: markets, supply chains, capital, talent, innovation, raw material and energy supply, and locations and production; in addition, employees as the central asset to be protected, exposed executives and key personnel (Module 1, Chapter 2, Section 2.8) and Artificial Intelligence as a cross-cutting topic (Module 1, Chapter 2, Section 2.9) are considered. For each dimension: first understand why the impact arises, then take targeted countermeasures (cf. Strategic White Paper 02, Chapter 2). The practical examples for each dimension are illustrative and not a binding catalog of measures.

2.1 Markets

Why is it noticeable?

Trade conflicts, sanctions and protectionist measures can make access to important sales markets more difficult or block it entirely. US tariff policy illustrates this in concrete terms: following the political agreement in principle in August 2025, an agreed maximum tariff rate of 15% applies to most EU exports to the United States; the EU implementing rules entered into force on 1 July 2026. At the same time, EU exports of goods to the United States in the first quarter of 2026 were around 30.4% below the previous year's level (Die Bundesregierung 2026c; Eurostat 2026). Political tensions can also lead to a decline in consumer and investment sentiment in affected regions. Companies are faced with the need to adapt their market strategies and possibly to develop new markets or diversify existing ones (Hakobyan, Meleshchuk, Zymek 2023).

What companies can do

- **Market diversification (“de-risking”):** don't put all your eggs in one basket - developing new sales markets reduces dependence on individual regions.
- **Localization:** move production and value creation closer to end customers in order to circumvent trade barriers and better serve local preferences.
- **Scenario planning:** early analysis of potential political opportunities and risks and development of contingency plans for different market scenarios.

Practical example (illustrative): A manufacturer generates 40% of its revenue in a single non-European market. It decides that no single market should grow beyond 25% in the medium term and builds up two replacement markets with local sales partners.

2.2 Supply chains

Why is it noticeable?

Geopolitical tensions can lead to disruptions in global supply chains, whether through trade restrictions, damage to infrastructure or political instability. The COVID-19 pandemic and the war in Ukraine have dramatically highlighted the vulnerability of global supply chains (WTO 2023). Currently, the conflicts in the Middle East in particular demonstrate the vulnerability of global transport and supply networks. Since the start of the military escalation on 28 February 2026, there have been repeated massive restrictions on shipping through the Strait of Hormuz, through which more than a quarter of seaborne oil trade and around a fifth of global LNG trade (EIA 2025) are normally transported. The resulting risks for energy supply, transport and global supply chains extend beyond each military escalation phase and led to considerable upheaval on energy and commodity markets in 2026. Higher energy prices had a direct impact on production, transport and logistics costs worldwide (Euronews 2026a).

What companies can do

- **Ensure a complete situational picture:** monitor relevant developments and carry out scenario planning that addresses, for example, the effects of port closures, airspace closures, sanctions or supply shortages and ensures solutions and alternatives for these disruptions.
- **Build resilience:** establish redundant supplier relationships and inventories at strategic locations.
- **Regionalization and nearshoring:** relocate parts of production or procurement to geographically closer or politically more stable regions.
- **Create transparency:** use technologies to better monitor and trace supply chains in order to identify risks at an early stage.

Practical example (illustrative): An electronics manufacturer finds twelve components in its bill of materials with only one source of supply in East Asia. For the five most revenue-critical components it qualifies a second source; for the rest it increases safety stock to three months.

2.3 Capital

Why is it noticeable?

Geopolitical uncertainty can lead to capital flight, currency fluctuations and rising financing costs. Investment decisions are made more cautiously, and access to international capital markets can become more difficult, particularly in countries considered politically unstable (IMF 2023b).

What companies can do

- **Risk management:** hedge against currency fluctuations and political risks using appropriate financial instruments.
- **Strengthen equity:** a solid equity base makes companies more resilient to external shocks.
- **Diversification of funding sources:** do not rely solely on bank loans but also consider other forms of financing such as bonds or private equity.

Practical example (illustrative): An exporter hedges foreign currency revenues for twelve months, insures political risks in a high-risk market and extends its credit line while conditions are still favorable.

2.4 Talent

Why is it noticeable?

Geopolitical conflicts and tensions can restrict or influence the international mobility of skilled workers. Visa restrictions, travel bans or general uncertainty can make it more difficult to recruit talent globally or to send employees abroad. In addition, regional conflicts can be a reason for employees to flee, which can result in the loss of know-how for the company concerned. Moreover, sentiment toward certain nationalities can affect the integration of international talent (OECD 2021).

What companies can do

- **Local talent development:** greater investment in the training and development of talent in the respective regions.
- **Attractive working conditions:** create an inclusive and attractive working environment in order to attract and retain talent regardless of origin.
- **Values-based corporate culture:** shared values, fairness and a lived security awareness strengthen the loyalty of skilled workers and increase resilience to poaching and external influence.
- **Digital collaboration:** use digital tools to enable international teams to work together effectively even without physical presence.

Practical example (illustrative): A software company with a development center in a crisis region documents critical knowledge, forms tandems with teams in Germany and has a relocation plan ready for employees and their families.

2.5 Innovation

Why is it noticeable?

Geopolitical rivalries can impede the free exchange of knowledge and technologies. Export controls for certain technologies or restrictions on cooperation in research and development can slow down the innovation process or steer it in certain directions (Europäische Kommission 2024).

What companies can do

- **Resilient R&D strategies:** diversify research locations and partners in order to reduce dependencies.
- **Investment in in-house research:** build stronger internal research and development capacities in order to be less dependent on external technology sources.
- **Open innovation with trusted partners:** targeted cooperation with partners from politically stable and reliable regions.

Practical example (illustrative): Before every research cooperation and every licensing deal, a technology company reviews export control and dual-use issues as well as the partner's background and regulates access to key knowledge.

2.6 Raw material and energy supply

Why is it noticeable?

Raw materials and energy are increasingly becoming instruments of geopolitical power. Export restrictions, trade conflicts, sanctions or conflicts along important transport routes can considerably impair the availability of critical raw materials and energy sources. At the same time, supply shortages and rising energy prices lead to higher production, logistics and operating costs. Companies that are highly dependent on individual suppliers, regions or energy sources are particularly vulnerable to geopolitical shocks (WEF 2026; IEA 2022).

What companies can do

- **Diversify sources of supply:** identify and reduce dependencies on individual suppliers, countries or sources of raw materials.
- **Increase security of supply:** build up supply contracts, strategic reserves and alternative sources of supply.
- **Increase energy efficiency:** invest in energy efficiency measures, self-generation and alternative energy sources to reduce external dependencies.

Practical example (illustrative): An energy-intensive plant secures part of its electricity demand through long-term supply contracts and its own photovoltaics and builds up a two-month stock of a critical raw material.

2.7 Locations and production

Why is it noticeable?

Geopolitical developments increasingly influence the attractiveness and operational capability of company locations. In addition to traditional factors such as costs, taxes or infrastructure, political stability, sanctions and regulatory risks, the availability of energy and raw materials and the security of supply chains are gaining in importance. Added to this is access to data centers and AI computing capacity, which is increasingly becoming a location factor for data-intensive development and production. Conflicts, trade restrictions or geopolitical tensions can cause locations to lose their economic advantages or significantly restrict business activities (WEF 2026).

What companies can do

- **Assess locations geopolitically:** base location decisions not only on economic viability but also on resilience and risk criteria. Include political stability, sanctions risks, resource availability and supply chain dependencies in investment and location decisions.
- **Diversify the location portfolio:** distribute critical functions, production capacities and data processing across several regions. Regularly assess the impact of geopolitical crises on production and operating sites and prepare contingency measures, taking into account country-specific restrictions (e.g. relationships: China/Taiwan, USA/Cuba).
- **Create redundancies:** maintain alternative production and backup sites for critical business processes.

Practical example (illustrative): A company with a plant in a region of tension defines thresholds above which production is relocated, keeps tools and production data at a second site and practices the changeover once a year.

2.8 Employees, executives and key personnel

Why is it noticeable?

Employees are every company's central asset to be protected: duty of care, travel and site security, reachability and evacuation concepts, and protection against espionage and approaches by foreign actors concern the entire workforce (cf. Strategic White Paper 02, Chapter 2.3); the specific measures are listed below. Exposed executives and key personnel must be included in the assessment of critical assets. The need for protection is not derived from hierarchy but from function, visibility, threat situation and possible effects on the company's ability to act. To this end, digital and physical exposure factors must be recorded together, possible escalation paths assessed and appropriate organizational, digital, communication and, where necessary, physical measures defined. Digital traces and publicly available information about family members (e.g. partners or children) must also be taken into account if they allow conclusions to be drawn about the whereabouts, routines or movement profiles of protected persons. Corporate security, cybersecurity, communications, human resources, travel security, data protection and close protection must be involved as the situation requires (cf. BfV 2025; BSI 2025).

What companies can do

- **Record exposure:** As a first step, carry out a visibility analysis to establish the current situation: Which digital and physical information increases visibility or predictability? Does the digital footprint of family members allow conclusions to be drawn about the whereabouts, habits or movement profiles of the protected person?
- **Assess risk:** Which function, situation, region, trip, event or corporate activity increases the need for protection?
- **Check escalation:** Can information be used for phishing, reconnaissance, approaches, intimidation or physical threats?
- **Define measures:** Which graduated measures and interfaces are appropriate, and when is a reassessment necessary?
- **Protect the workforce:** define and practice reachability, travel and site security as well as evacuation and repatriation concepts for employees in risk regions.
- **Address deepfake risks:** never issue approvals or payment instructions solely on the basis of a call, voice message or video; establish call-backs via known contact channels and the four-eyes principle.

Note on application:

The assessment is carried out on a case-by-case basis; general threat assumptions as well as operational protection levels or tactical measures are not the subject of this guide.

2.9 Artificial Intelligence

Why is it noticeable?

AI is changing the threat situation directly: attackers use AI to find and exploit vulnerabilities faster, to personalize phishing and social engineering in any language, and to imitate executives or business partners with voice and video forgeries (deepfakes) (BSI 2026a; BSI 2024; NCSC 2025). At the same time, new dependencies are emerging on a few, predominantly non-European providers of AI models, data centers and AI chips (cf. Strategic White Paper 02, Chapter 3). The uncontrolled use of external AI services by employees (“shadow AI”) can lead to the leakage of confidential data. The EU AI Act adds binding requirements for transparency and risk management (Europäische Union 2024c).

What companies can do

- **Establish an AI policy:** which AI services are permitted for which data classes; approval process for new tools.
- **Deepfake-resilient processes:** call-back principle and four-eyes principle for payments, approvals and data releases.
- **Map AI dependencies:** include providers, data center locations and exit options in the dependency mapping (Module 4, Chapter 5).
- **Train employees:** recognize and report AI-supported phishing and deception attempts.

Practical example (illustrative): A medium-sized supplier discovers that sales and development are using freely available AI chatbots with customer data and design documents. First steps: an inventory of the services used, a one-page usage policy, an approved AI tool with data processing in the EU and a short training session on deepfake calls.

3 Risk multipliers: when crises fuel each other

Analysis tool for interconnected crisis cascades

Strategic White Paper 02 (Chapter 2.4) describes how geopolitical risks escalate into cascades via interconnected systems. This module provides the corresponding analysis tool: ten possible risk multipliers and questions for self-assessment.

For companies, the key challenge therefore lies not only in identifying individual risks but in understanding their interactions. A geopolitical escalation can simultaneously increase raw material prices, impair transport routes, intensify sanctions risks and delay investment decisions. It is precisely in these chain reactions that the real vulnerability lies.

Risk multipliers are factors that amplify or accelerate individual events or transfer them to other domains. They do not necessarily trigger crises themselves, but they increase their reach, speed and the complexity of managing them. The following multipliers are a selection and not exhaustive; depending on the industry, location and business model, others may be added.

3.1 Possible risk multipliers

Risk multiplier	Relevance for companies
1. Connectivity of critical systems	The more closely energy, transport, IT, finance, supply chains and communications are coupled, the faster local disruptions can have systemic effects. (Kotzanikolaou, Theoharidou, Gritzalis 2013; Mühlhofer, Bresch, Koks 2024)
2. Geopolitical escalation and sanctions dynamics	Wars, blockades, sanctions and export controls affect prices, supply, regulation, market access and political stability. (IMF 2023b; Hakobyan, Meleshchuk, Zymek 2023)
3. Energy and raw material dependency	High import and concentration dependencies amplify shocks via costs, production, delivery capability and competitiveness. (IEA 2022; OECD 2026)
4. Supply chain and logistics fragility	Bottlenecks in ports, sea routes, intermediate products or transit countries can trigger operational failures far beyond the original point of disruption. (WTO 2023; OECD 2026)

Risk multiplier	Relevance for companies
5. Price and inflation transmission	Geopolitical tensions pass through energy, raw material, agricultural and transport markets to inflation, purchasing power, margins and social stability. (IMF 2023a)
6. Climate and environmental stress	Extreme weather, water stress, crop failures and biodiversity loss intensify existing economic, political and social tensions. (IPCC 2022; Feyen et al. 2020)
7. Social polarization and loss of legitimacy	Supply crises, price increases and uncertainty can exacerbate protests, political instability and governance problems. (OECD 2023; IPCC 2022)
8. Information and disinformation dynamics	Disinformation, loss of trust and targeted influence operations can affect markets, political decisions and corporate reputation. (OECD 2024; Bentzen 2024)
9. Technological vulnerability of critical infrastructures	Cyberattacks, OT/IT failures and digital dependencies can accelerate physical, financial and political crises. (Kotzanikolaou, Theoharidou, Gritzalis 2013; BSI 2025)
10. Governance and response delays	Fragmented responsibilities, weak early warning and slow decisions increase the duration, depth and costs of cascading effects. (OECD 2023)

These risk multipliers show: the greatest challenge lies not in the existence of individual risks but **in their combination**. Energy crises can increase production costs, which inhibits investment, weakens innovative capacity and deepens technological dependencies. Supply chain disruptions can trigger regulatory conflicts, increase financing costs and jeopardize market access. Disinformation can make crisis communication more difficult, undermine trust and influence political responses.

3.2 Change of perspective: from individual risks to interconnected cascades

Traditional risk management, which assesses risks primarily according to the probability of occurrence and the extent of damage of individual events, is of only limited use for systemic geopolitical cascades. What is needed is a more interconnected approach that considers dependencies, trigger points, escalation paths and operational effects together. This does not mean predicting every conceivable crisis - what matters is understanding one's own vulnerability to cascading effects.

Self-assessment questions for risk and security managers

- Which critical functions depend on individual suppliers, regions, technologies, data spaces, transport routes or regulatory prerequisites?
- Where are there concentration risks - single source, single region, single technology?
- Which disruption could affect several business units at the same time?
- Which decisions would have to be made under time pressure - and who makes them?

3.3 The six-point protection approach

Companies can protect themselves effectively if they manage geopolitical risk areas not as a collection of isolated individual risks but as interconnected cascades. A resilience strategy consists of the combination and joint assessment of individual activities, which can be carried out using the six-point protection approach:

1. Early detection
2. Reduction of critical dependencies
3. Robust governance and crisis management
4. Resilient supply chains and technology
5. Due diligence and protection of critical assets
6. Cooperation with trusted partners and public authorities

> *The aim is not to avoid disruptions completely but to be able to identify impacts early, prepare options for action, protect critical functions and remain capable of making decisions and performing under intensified geopolitical conditions.*

4 Resilience architecture: capability maturity check

From a protective function to a strategic management capability

Strategic White Paper 02 (Chapter 1.1) describes how resilience is developing from a downstream protective function into a strategic management capability. This module translates this into a tool: existing risk, security and crisis management approaches are more closely interconnected and made more forward-looking and business-oriented.

Corporate resilience begins with transparency about the company's own critical functions: which products, processes, locations, suppliers, technologies, data spaces, infrastructures and partners are actually indispensable for the ability to act? In other words:

A company's resilience concept must contain and define the absolute lower limit of operational capability in a severe crisis. In doing so, the company's normal value creation is reduced to its minimum, primary value-creating activities. All indispensable value-creating activities are prioritized in order to maintain the most critical value chain - from essential service delivery to securing liquidity - in emergency operation with a minimal use of resources. The aim is to prevent existentially threatening damage to customers and to secure the economic survival of the organization. This approach goes beyond the Minimum Business Continuity Objective (MBCO) according to ISO 22301:2019 and emergency operation according to BSI Standard 200-4 (ISO 2019; ISO 2025; BSI 2023). An example for an SME can be found in Module 3, Chapter 4, Section 4.3.[1]

Only when these dependencies within the value chain are known can priorities be set, protective measures derived and investment decisions robustly justified.

[1] Minimum Business Continuity Objective (MBCO) (ISO 2019; ISO 2025); BSI Standard 200-4 describes how companies can plan such emergency operation (BSI 2023).

4.1 Eight capabilities of a modern resilience architecture

Use the following table as a starting point for an internal maturity workshop: where does your company stand today for each capability - basic, under development or strategically anchored?

Capability	Significance for companies
Geopolitical early detection	Identify strategic trigger points, classify developments and derive options for action at an early stage.
Transparency of critical dependencies	Identify critical suppliers, technologies, data spaces, locations and functions.
Reduction of strategic vulnerabilities	Reduce single-source, single-region and technology dependencies in a targeted manner.
Integrated governance	Link security, BCM, crisis management, cybersecurity, risk, legal, compliance and business more closely.
Scenario and stress test capability	Test the effects of geopolitical escalations on business models, supply chains and critical functions.
Protection of critical assets	Effectively protect employees, data, IP, technologies, key personnel, production capability and sensitive partnerships.
Crisis and decision-making capability	Ensure clear escalation paths, reliable situational pictures and fast decision-making processes.
Cooperation with partners and public authorities	Improve situational pictures, increase responsiveness and secure access to relevant warning and support structures.

Geopolitical early detection requires continuous monitoring of strategic trigger points: political decisions, sanctions, export controls, military escalations, regulatory changes, disinformation campaigns, cyber threats, raw material shortages and changes in critical supply chains. This information must not only be collected but translated into concrete decision-making processes.

Business continuity management, crisis management, corporate security, cybersecurity and enterprise risk management must also be brought together more closely. In a geopolitically fragmented environment, disruptions often occur simultaneously in several

domains: cyberattacks meet supply chain bottlenecks, regulatory uncertainty meets reputational risks, energy prices meet production decisions. Only integrated resilience structures can manage such cascades effectively.

Assessment scale for the maturity workshop

Assess each of the eight capabilities on a three-level scale and record concrete evidence (document, exercise, indicator) for levels 2 and 3. The scale is based on the principles of organizational resilience in ISO 22316:2017 (ISO 2017).

Level	Characteristics	Example: geopolitical early detection
1 - basic	The task is assigned and performed on an ad hoc and person-dependent basis; no fixed processes or indicators.	Individual experts follow the news; information is sent to management by e-mail as needed.
2 – under development	Process, responsibility and tools are defined; regular application, first exercises; results feed into individual decisions.	Monthly situational picture with defined trigger points (e.g. new sanctions or export controls for own intermediate products, freight or energy prices above a defined threshold, military maneuvers or blockades in supply regions); distribution list for procurement, BCM and sales; annual exercise.
3 – strategically anchored	The capability is integrated into strategy and investment processes, underpinned by indicators in management reporting, and regularly exercised and improved.	Early warning indicators are linked to thresholds and action plans; the situational picture is an integral part of executive board meetings and strategic planning.

Workshop result: maturity profile for each capability, prioritized gaps with responsible persons and target dates, reference to the corporate objectives concerned (e.g. delivery capability, margin, market access).

4.2 Artificial Intelligence as a tool in resilience management

Artificial Intelligence (AI) is increasingly becoming an important support tool in security, risk and resilience management. Its particular strength lies in the rapid processing of large amounts of information from different sources and languages. AI can research, structure, analyze, summarize and visualize information and thereby improve the information base for security decisions (BSI 2026a; BSI 2024; NCSC 2025).

In large companies, for example, AI is used in security operations centers to prioritize security-relevant alerts, detect suspicious activities faster or support the evaluation of event data from security information and event management systems. In addition, AI can continuously evaluate publicly available information sources in order to create situational pictures, identify developments early and improve strategic foresight (security intelligence

and foresight). Further fields of application include support for video analysis, monitoring geopolitical developments and identifying risks in supply chains.

AI opens up new opportunities, especially for small and medium-sized enterprises. Organizations that do not have experts for all security-relevant topics can use AI to efficiently evaluate information on threats, geopolitical developments, cyber risks or supply chain disruptions. This enables security managers to cover a broader range of topics and make better-informed decisions without having to employ specialists for every area.

At the same time, AI is no substitute for security managers, risk experts or crisis teams. The technology supports people in gathering and analyzing information but does not assume responsibility for assessments, prioritization or decisions. The quality of the results depends largely on the question asked, the underlying data and the expert review of the results. Human expertise therefore remains indispensable in order to classify AI-generated findings, compare them with company-specific processes and requirements, and derive suitable measures from them.

Limits and risks of use: AI results can be incomplete, outdated or simply wrong; language models sometimes invent plausible-sounding statements or sources (“hallucinations”). Security-relevant evaluations must therefore always be reviewed by experts; this continues to require staff with subject-matter and methodological knowledge. It must also be determined which information may be entered into AI systems (data protection, classified information protection, trade secrets) and where the data is processed. The risks posed by the use of AI on the attacker side are described in Module 1, Chapter 2, Section 2.9.

The greatest added value of AI therefore lies not in replacing human competence but in extending it. It enables security managers to respond more quickly to changes, evaluate more sources of information at the same time and use scarce human resources more effectively.

Link to the resilience architecture: AI mainly supports geopolitical early detection, the transparency of critical dependencies, and crisis and decision-making capability (Module 3, Chapter 4, Section 4.1). A sensible starting point is an AI-supported situational picture for a few clearly defined trigger points, whose results are always reviewed by experts. Risks posed by AI are covered in Module 1, Chapter 2, Section 2.9; opportunities for new business areas in Module 9, Chapter 10, Section 10.3.

4.3 From analysis to implementation: first steps

The following examples show possible first steps. They are deliberately illustrative and not an exhaustive or binding catalog of measures; the starting situation and implementation

differ from company to company. The time horizons follow the guiding question of Strategic White Paper 02: today, in the coming six months and in the long term.

Time horizon	Possible first steps	Result
Immediately (0-3 months)	Appoint a person responsible for resilience; list the ten most important products, customers and suppliers; update emergency contacts and reporting channels (Module 6, Chapter 7); check backups and emergency power for critical systems.	Clarity about what must not fail under any circumstances
Short term (up to 6 months)	Dependency mapping for the most critical processes (Module 4, Chapter 5); run through a scenario as a tabletop exercise (Module 5, Chapter 6); request second sources for single-source parts; maturity self-assessment (Module 3, Chapter 4, Section 4.1).	Prioritized list of the greatest vulnerabilities with responsible persons
Medium term (6-24 months)	Qualify second sources and build up safety stocks; anchor resilience criteria in investment, location and procurement decisions; include the situational picture and indicators in management reporting.	Resilience is part of corporate management, not just of crisis situations

Example: securing minimum value creation (SME, illustrative). A mechanical engineering company with 250 employees determines which services it must maintain even in a severe incident, such as the supply of spare parts and service for its most important existing customers. To this end, it identifies the necessary employees and their deputies, a minimum stock of critical components, an IT emergency mode (e.g. order processing for two weeks without central systems) and a fixed line of communication to customers. In this way, the core of value creation is preserved even if the overall business temporarily collapses.

> *The key question is not whether companies should invest in resilience, but where the greatest vulnerabilities lie and which capabilities need to be built in order to remain functional even under geopolitical pressure.*

5 Critical dependencies: dependency mapping

Nine fields in which modern vulnerability is concentrated

Anyone who wants to build resilience must first understand where their own vulnerabilities lie. Use the following nine fields as a structure for internal dependency mapping - for each field: Where do we stand? What concentration risks exist? Which alternatives do we already have, and which are still missing?

Field	Significance for companies
Energy	Energy is the foundation of industrial capability - price volatility, security of supply and the availability of renewable sources have become strategic variables. Example: review of emergency power supply, including diesel stockpiles, at critical sites such as data centers.
Supply chains	Supply chains have lost their supposed robustness under pandemic conditions and geopolitical tensions; their redesign is one of the key management tasks of the decade. Example: continuous monitoring along supply chains, identification of single-source dependencies, such as for critical components, raw materials and services, and development of alternative suppliers and transport routes.
Digitalization	Digitalization creates efficiency but at the same time generates new dependencies - especially where critical processes are based on external platforms, proprietary software or non-European cloud infrastructure. Example: review of alternative European providers to ensure confidentiality, integrity and availability, development of redundant technologies for critical processes, diversification of critical technologies and competencies in order to limit vendor lock-in and know-how dependencies.
Semiconductors and key components	The concentration of global chip production in a few locations makes semiconductors the geopolitical Achilles' heel of industrial and digital value chains. Example: determination of the availability of critical semiconductors and identification of possible bottlenecks, development of redundant sources of supply, adequate stockpiling.

Field	Significance for companies
Security management	Security is gaining weight as a basic business requirement. Example: integration of security situation information and risk analyses into the company's strategic decisions, provision of the resources required for adequate security measures.
Cloud and data center infrastructure	Increasing geopolitical volatility increases dependence on political developments, creating the risk of unwanted information leakage and impairment of integrity and availability due to regulatory intervention and political decisions. Added to this is the dependence on data center and AI computing capacities, which are concentrated among a few providers and locations. Example: create transparency regarding existing infrastructure, risks and dependencies (multi-cloud strategy), review European or sovereign cloud offerings for particularly sensitive data and applications, regional data storage with local fallback options for business-critical processes, adequate encryption, clear exit and migration strategies.
Cyber technologies	Cyber risks are no longer an isolated IT issue but an integral part of geopolitical conflict situations and must be addressed accordingly at the strategic level. Example: conducting a cyber exercise in which the failure of a central IT or production system is simulated and restoration from secured backups is tested.
Physical security	Sites, production facilities, data centers, logistics hubs and personnel are the physical basis of all other fields. Sabotage, espionage, drone overflights and attacks on critical infrastructure are increasing; companies should know the protection requirements, redundancies and restart times of their critical sites and align them with the requirements of the CER Directive and the German Critical Infrastructure Protection Umbrella Act (KRITIS-Dachgesetz) (cf. BfV 2025; Europäische Union 2022b; Die Bundesregierung 2026b). Example: holistic assessment of the protection requirements of critical sites, including access control, drone detection, video surveillance, redundancies and restart times.
Satellite, navigation and timing services	Many processes depend, often unnoticed, on satellite-based navigation, timing, communication or earth observation - from logistics and fleet management to grid and financial systems and time synchronization in IT and OT. Example: companies should check which critical processes depend on these directly or indirectly and assess failure, impairment and manipulation (jamming, spoofing) as well as available fallback levels.

Guiding questions for the mapping workshop

- Which of these fields are indispensable for our most critical business processes?
- Where do we have single-source or single-region dependencies - and are we even aware of them?
- Which alternatives (diversification, regionalization, nearshoring, friend-shoring, in-house development capacities) have we already built up?
- Who in the company is responsible for continuously updating these dependencies?

> *Resilience is therefore no longer a defensive concept. It is becoming a strategic prerequisite for competitiveness, trust and entrepreneurial capability.*

6 Scenario stress test toolkit 2027-2030

Four equally weighted futures - not forecasts, but planning corridors

> *The scenarios are not forecasts but plausible, deliberately pointed developments based on current geopolitical trends, security policy analyses and known vulnerabilities. The aim is to raise awareness of interactions and systemic effects - not to predict specific events (the ThinkTank's own scenario development). The starting situations reflect the state of analysis as of June 2026; developments in the Middle East since then are taken into account in Module 5, Chapter 6, Section 6.5.*

Worksheet for the stress test

Work through each scenario for each escalation level using this grid. The completed row shows an example for Scenario 2 (Taiwan Strait), level 1, from the perspective of an industrial company.

Escalation	Critical functions	Early indicators / triggers	Impact on objectives	Measures and lead time	Responsible
Example: Scenario 2, level 1	Procurement of semiconductors and electronics; series production	Expansion of military exercises, rising insurance premiums and freight rates, export license requirements	Delivery delays, margin pressure from spot market purchases, contractual penalties	Safety stocks for critical chips (3-6 months), qualify second sources (6-18 months), secure alternative routes contractually	Procurement, BCM, production
Level 1					
Level 2					
Level 3					

Result: for each scenario, a statement as to whether the business model remains viable at each level, which measures must be taken in advance and what lead time is required.

6.1 Scenario 1 - Large-scale conflict in Europe

This scenario describes a plausible but by no means deterministic development in which a combination of intensified hybrid warfare, political fragmentation and regional military escalation could lead to a large-scale conflict in Europe.

6.1.1 STARTING SITUATION (STATE OF ANALYSIS: JUNE 2026)

As a result of the ongoing Russia-Ukraine war, increasing tensions and growing military activity, Europe faces heightened instability in Central and Eastern Europe, shifts in the transatlantic alliance and increasing hybrid threats.

6.1.2 ESCALATION LEVEL 1 - EUROPE UNDER INTENSIFIED HYBRID WARFARE

Russia expands hybrid warfare across Europe and deliberately exploits political fragmentation. Disinformation campaigns, influence operations and activities of state-sponsored actors against critical infrastructure increase (cf. BfV 2025). The main targets are critical infrastructures (electricity, rail, fuel, industrial control systems) for sabotage, economic espionage and cyberattacks - with chronic disruptions in supply chains and logistics.

- Persistent hybrid attacks undermine public trust, weaken EU unity and deepen political fragmentation.
- Declining Western support for Ukraine enables Russia to make military gains.
- Russia uses weakened European coordination to expand its influence (e.g. Odesa, Transnistria, Moldova).

Impact categories: cybersecurity, physical and economic security, business operations and supply chains, workforce and employees.

6.1.3 ESCALATION LEVEL 2 - REGIONAL MILITARY EXPANSION AND FRAGMENTATION OF NATO

Declining Western support enables Russian advances toward Odesa and Transnistria and destabilizes Moldova. The United States could withdraw military forces from Europe and support NATO in the conflict with Russia only minimally or not at all. Russia could initiate limited military activities in the Narva area and/or seek to establish a land bridge to Kaliningrad via the Suwałki Gap by military meansin order to test NATO's responsiveness and cohesion.

- Russian military action in Narva tests NATO unity; the Suwałki Gap is militarily contested and isolates the Baltic states.
- European countries activate defense plans, including partial mobilization and emergency controls of critical infrastructure.
- Hybrid attacks could gradually develop into limited kinetic attacks on critical infrastructure.

- The Baltic crisis escalates into a direct confrontation between NATO and Russia.
- China exploits the commitment of Western forces in Europe to increase pressure on Taiwan and in the South China Sea, and supports Russia economically and technologically (cf. NATO 2024).

Impact categories: cybersecurity, physical and economic security, business operations and supply chains, workforce and employees, government and law, finance and trade.

6.1.4 ESCALATION LEVEL 3 - LARGE-SCALE CONFLICT IN EUROPE AS A RESULT OF THE BALTIC CRISIS

The conflict in Estonia escalates rapidly while Russia blockades and isolates the Baltic states via Belarus and Kaliningrad. A German brigade in Lithuania becomes involved in intensive fighting. European countries activate comprehensive defense plans and switch to a full national defense posture. Drone and missile attacks hit critical logistics hubs and infrastructure throughout Europe and lead to a direct NATO-Russia confrontation.

Impact categories: technology and data, cybersecurity, physical and economic security, government and law, business operations and supply chains, customers, partners and markets, workforce and employees, finance and trade.

Affected system	Potential impact
Energy supply	Rationing, price shocks
Logistics	Border controls, transport failures
Supply chains	Production interruptions
Cyber	Attacks on OT and IT systems
Personnel	Travel restrictions, evacuations
Compliance	Emergency regulations
Finance	Liquidity shortages
Communication	Disinformation

6.1.5 WHAT DOES THIS MEAN FOR GLOBAL COMPANIES?

In addition to traditional business continuity and crisis management approaches, geopolitical early warning mechanisms, scenario planning, resilience investments and the safeguarding of critical functions and dependencies are gaining in importance. Strategically strengthening digital sovereignty, through investment in in-house technology development and the use of trusted European or regional solutions, is becoming a decisive competitive factor and a necessity for business continuity.

6.2 Scenario 2 - Escalation in the Taiwan Strait as a geo-economic system shock

> *A conflict in the Taiwan Strait would not be a regionally limited security event but a global geo-economic system shock with immediate effects on technology, trade, energy, financial markets and corporate resilience.*

This scenario examines a possible escalation of tensions in the Taiwan Strait from ongoing coercive measures and gray-zone activities to a comprehensive military confrontation culminating in a full blockade and open conflict with far-reaching geostrategic and economic consequences.

6.2.1 STARTING SITUATION (STATE OF ANALYSIS: JUNE 2026)

China continues to put pressure on Taiwan with regular incursions into its maritime and air space, large-scale military exercises, cyber operations, economic pressure and diplomatic measures. The Taiwan Strait is one of the most geopolitically sensitive regions in the world, as security, technological and economic interests overlap directly there.

approx. 44%

Taiwan's share of global foundry capacity (2024) - approx. two thirds for advanced processes (16 nm and smaller), over 90% for the most advanced chips below 10 nm (data as of 2019) (TrendForce 2024; SIA/BCG 2021)

6.2.2 ESCALATION LEVEL 1 - INTENSIFICATION OF GRAY-ZONE AND MILITARY PRESSURE

China tries to weaken Taiwan politically without triggering an open war: military pressure through air and sea incursions, cyberattacks, disinformation, espionage, economic pressure, disruption of supply chains and sabotage. Even this phase can have a considerable impact on international financial markets, insurance premiums, shipping costs and investment decisions.

- Intensification of gray-zone measures weakens government, communications, financial systems and public trust.

- Increase in economic pressure on ECFA-related exports (Economic Cooperation Framework Agreement, China-Taiwan trade agreement of 2010), shipping and investor confidence.
- “Red line” events lead to expanded military exercises and possible access controls.

Impact categories: cybersecurity, physical and economic security, business operations and supply chains, workforce and employees.

6.2.3 ESCALATION LEVEL 2 - LIMITED BLOCKADE LEADS TO REGIONAL CRISIS AND GLOBAL DISRUPTION

After unsuccessful gray-zone measures, China switches to a limited blockade focusing on key ports and air routes - a mix of maritime and paramilitary forces, regulatory and economic coercion and targeted disinformation campaigns.

- Control over key ports and air access as well as inspections of maritime traffic.
- Selective incentives for cooperative countries and companies.
- Rising transport risks and delays in global supply chains, especially for semiconductors - as around half of the global container ship fleet passes through the Taiwan Strait (Varley 2022), even limited maritime restrictions can have a considerable impact on global flows of goods.
- Overloading of Taiwan's critical infrastructure; increasing likelihood of secondary effects on international energy, financial and commodity markets.
- If the war against Ukraine has not been settled by then, Russia can exploit the commitment of American forces in the Pacific to increase pressure on Europe.

Impact categories: cybersecurity, physical and economic security, business operations and supply chains, workforce and employees, government and law, finance and trade.

6.2.4 ESCALATION LEVEL 3 - FULL BLOCKADE ESCALATES INTO MILITARY CONFLICT

An incident in the Taiwan Strait initially leads to a quarantine, which escalates into a full blockade and open military conflict. Integrated missile, cyber, air and naval operations aim to secure information, sea and air superiority. China denies companies from countries that support Taiwan access to facilities, data and critical services - with considerable supply chain disruptions and far-reaching business interruptions. Extensive sanctions regimes, export controls and restrictions on data and technology transfers are likely.

A conflict in the Taiwan Strait would at the same time be a technology and data conflict: in addition to physical supply chains, global semiconductor, cloud, AI and communication ecosystems in particular would be affected (cf. Kleinhans, Jha 2025).

Impact categories: cybersecurity, physical and economic security, business operations and supply chains, workforce and employees, government and law, finance and trade, technology and data, customers, partners and markets.

Area	Potential impact
Semiconductors	Production losses
Logistics	Delays and bottlenecks
Shipping	Diversions and cost increases
Energy	Price volatility
Cyber	Attacks on critical systems
Technology	Export controls
Finance	Market disruptions
Data	Access restrictions

6.2.5 WHAT DOES THIS MEAN FOR GLOBAL COMPANIES?

This scenario illustrates the need to systematically identify and regularly review strategic dependencies - in particular semiconductors, critical raw materials, cloud services, maritime transport routes, data flows and access to regional sales and procurement markets. Geopolitical developments in the Taiwan Strait can very quickly turn into global technology, trade and supply chain crises.

6.3 Scenario 3 - US-China technological decoupling

This scenario considers a gradual escalation of the techno-economic rivalry between the United States and China. The focus is not only on technological rivalry but on the increasing fragmentation of global economic, data, financial and technology systems - from increasing compliance pressure to a more comprehensive systemic separation in critical sectors to a crisis-driven rupture.

6.3.1 STARTING SITUATION (STATE OF ANALYSIS: JUNE 2026)

Relations between the United States and China are characterized by structural rivalry and increasing techno-economic decoupling. Competition is increasingly evolving from a trade conflict into systemic competition for technological leadership, economic resilience and geopolitical influence. China is responding with its Export Control Law, the Unreliable Entity List and so-called “blocking” rules.

6.3.2 ESCALATION LEVEL 1 - TIGHTENED COMPLIANCE AND RETALIATORY MEASURES

Relations are evolving from selective separation to more comprehensive compliance friction, increasing operational uncertainty for foreign companies while transaction costs rise significantly. “Dual compliance” becomes a permanent condition: companies increasingly have to operate in parallel in different regulatory and technological ecosystems.

- The United States expands Entity List designations and tightens licensing and monitoring measures along the supply chains for chips, AI and semiconductor equipment (cf. Crosignani et al. 2024).
- China increases pressure through the Unreliable Entity List and measures against extraterritorial regulations, increasing trade and investment risks.
- China tightens export licensing for strategic materials and uses case-by-case decisions as leverage.

Impact categories: cybersecurity, physical and economic security, business operations and supply chains, workforce and employees.

6.3.3 ESCALATION LEVEL 2 - SYSTEMIC DECOUPLING AND CONFLICTS OVER STRATEGIC BOTTLENECKS

Strategic decoupling hardens across key sectors as technology and control measures for critical intermediate products spill over into key industrial ecosystems. Critical minerals become a central weak point, causing production disruptions and cost pressure.

- The United States expands sanctioning instruments and investment bans and accelerates financial fragmentation.
- Requirements for “trusted suppliers” and sourcing from partner countries are expanded; CHIPS regulations further restrict technology partnerships.
- China extends export controls to rare earths and controlled materials, increasing the risk of cascading effects and bottlenecks in strategic sectors.
- Industries that are highly dependent on semiconductors, battery technologies, rare earths, industrial automation and AI applications would be particularly affected.
- The fragmentation of technological systems could also lead to diverging satellite navigation and communication standards, increasing operational complexity and costs for global logistics and data-intensive industries.

Impact categories: cybersecurity, physical and economic security, business operations and supply chains, workforce and employees, government and law, finance and trade.

6.3.4 ESCALATION LEVEL 3 - CRISIS-DRIVEN STRATEGIC RUPTURE

An incident in the Taiwan Strait triggers a rapid escalation of sanctions and export controls between the United States and China, interrupting supply chains for AI computing power and critical minerals. The EU is caught in the crossfire and faces shortages of semiconductors and raw materials as well as significantly rising compliance and operational risks.

Impact categories: technology and data, cybersecurity, physical and economic security, government and law, business operations and supply chains, customers, partners and markets, workforce and employees.

6.3.5 WHAT DOES THIS MEAN FOR GLOBAL COMPANIES?

Companies need operating models that remain functional even under competing US and Chinese compliance regimes, especially for technology, critical intermediate products and cross-border partnerships. Equally important are early warning mechanisms, monitoring of geopolitical trigger points, robust alternatives for strategic materials and more resilience-oriented management.

6.4 Scenario 4 - Strategic fragmentation of the transatlantic partnership

This scenario outlines how transatlantic tensions can gradually condense from political estrangement and selective economic friction into strategic separation in key areas such as trade, technology and defense. The focus is not on the dissolution of the transatlantic partnership but on the increasing fragmentation of previously closely integrated economic, technological and security areas. The question of digital sovereignty becomes a central element of strategic realignment here.

6.4.1 STARTING SITUATION (STATE OF ANALYSIS: JUNE 2026)

Relations between the United States and the EU are strained by growing mistrust and increasing strategic divergence. Disputes in trade, technology and security are increasing, while the EU is expanding its technological sovereignty and the United States is safeguarding its industrial and security policy interests more offensively. Tensions are evident above all in export controls, compliance requirements and legal uncertainties regarding data flows.

6.4.2 ESCALATION LEVEL 1 - GROWING TRANSATLANTIC DIVERGENCE AND REGULATORY FRAGMENTATION

Escalation takes place predominantly via regulatory, technological and economic policy instruments and less via open political confrontation - driven by stricter procurement guidelines, AI-related export controls and legal requirements on data flows.

- **Technology:** selective and symbolic restrictions emerge; the United States introduces throttling or conditional access to certain services.
- **Trade:** political tensions increase, but supply chains persist, while EU competitiveness is weakened by energy costs.
- **Defense:** first tensions within NATO become visible as member states begin to question alignment and long-term commitments.

Impact categories: cybersecurity, physical and economic security, business operations and supply chains, technology and data, government and law.

6.4.3 ESCALATION LEVEL 2 - STRATEGIC SEPARATION IN KEY AREAS

The diverging narratives become entrenched in political practice. Europe accelerates its sovereignty efforts but lags behind US capabilities, reinforcing performance differences and internal fragmentation.

- **Technology:** regulated systems shift to sovereign EU technology stacks, while AI computing capacities are divided to address risks from export controls.
- **Trade:** decoupling focuses on enforceable bottlenecks (e.g. digital customs processes) rather than complete market isolation.
- **Defense:** the US troop presence in Europe and the intensity of intelligence sharing could be reduced or made more dependent on political conditions. This could also restrict access to critical satellite information for companies operating in high-risk regions, which would impair security assessments and operational planning and force companies to invest in alternative sources of information.

Impact categories: cybersecurity, physical and economic security, business operations and supply chains, technology and data, government and law, customers, partners and markets.

6.4.4 ESCALATION LEVEL 3 - PROFOUND TRANSATLANTIC FRAGMENTATION

An isolated shock rapidly escalates relations between the United States and the EU from controlled competition to open economic and security confrontation. Trade, data and technology transfers could be significantly restricted or selectively interrupted; defense and intelligence cooperation loses considerable intensity. Restricted access to advanced US technology forces European companies to use regional technology stacks, increasing costs, complexity and operational risks. This scenario would lead to higher R&D costs, slower innovation cycles and a potential loss of global competitive advantage for

European companies, while at the same time creating considerable demand for software, hardware and cloud services developed in Europe (cf. Europäisches Parlament 2025). Full digital sovereignty becomes a necessity here in order to secure Europe's technological and economic capability and to minimize dependencies.

Impact categories: business operations and supply chains, workforce and employees, technology and data, government and law, physical, cyber and economic security, customers, partners and markets.

6.4.5 WHAT DOES THIS MEAN FOR GLOBAL COMPANIES?

This scenario illustrates that geopolitical risks do not necessarily arise from open conflicts - even regulatory divergence, different technology policies and selective market restrictions can have a considerable impact on global business models. Companies need more regionalized technologies, data and governance structures. Regionalization, technological diversification and resilience-oriented governance structures are therefore gaining considerably in importance. The consistent implementation of digital sovereignty becomes the foundation for future growth and for safeguarding competitiveness in a fragmented global environment.

6.5 Simultaneity and combination of scenarios

The four scenarios are described individually but are not mutually exclusive in reality. They can occur simultaneously, trigger or reinforce one another; the risk multipliers from Module 2, Chapter 3, then act across several scenarios. Examples are shown in the following table; the strategic assessment can be found in Strategic White Paper 02 (Chapter 6). A separate overall scenario is deliberately not developed. However, a stress

test should examine at least one combination of two scenarios; the worksheet at the beginning of this module can be used for this without modification.

Combination	Typical amplifying effect	Test question for the company
Current: Ukraine war + Iran war/Hormuz	Energy and logistics prices rise while defense needs tie up capacities and budgets.	Which cost and delivery commitments to customers can still be honored?
1 + 2: Conflict in Europe + escalation in the Taiwan Strait	Crises in Europe and Asia tie up Western forces simultaneously; Russia and China can exploit each other's crisis for their own purposes (NATO 2024).	Are we prepared for the simultaneous loss of procurement and sales markets in Eastern Europe and East Asia?
1 + 3: Conflict in Europe + US-China decoupling	Energy and raw material shocks meet export controls on chips and rare earths.	Are stocks and second sources sufficient if sources of supply in Europe and Asia fail at the same time?
2 + 3: Taiwan Strait + decoupling	Semiconductor shortage and sanctions regime: replacement sources are scarce and legally restricted at the same time.	Which products can still be manufactured without chips from Taiwan and China?
1 + 4: Conflict in Europe + transatlantic fragmentation	Military pressure with restricted access to US technology, cloud, data and satellite services.	Do communications, cloud and situational picture also work without US services?

7 Interface between government and business

Economic Protection Initiative (Initiative Wirtschaftsschutz): between ambition and implementation

7.1 What the state offers

On 18 March 2026, the German Federal Cabinet (Bundeskabinett) adopted the National Economic Protection Strategy (Nationale Wirtschaftsschutzstrategie) presented by the Federal Ministry of the Interior (Bundesministerium des Innern, BMI) (BMI 2026). The strategic assessment can be found in Strategic White Paper 02, Chapter 5; this module focuses on the specific range of services, the gaps from the companies' perspective and practical use.

Core services are warnings and situational pictures, security advisories, information products, industry-specific discussion groups, regular briefings by authorities and further developed single points of contact. SMEs, start-ups and companies without their own security organization in particular are to be reached more easily - via associations, chambers of industry and commerce (IHKs), digital formats, platforms and social media. In addition, the state is expanding its services on cyber and information security, business continuity, research security, hybrid threats and physical corporate resilience.

7.2 What companies think of it - and where the gaps are

From the perspective of many companies, the National Economic Protection Strategy (Nationale Wirtschaftsschutzstrategie) is an important step in the right direction. Particularly positive is the fact that there is now a cross-departmental political lead for economic protection - exactly this kind of bundling of responsibility, prioritization and political visibility has been demanded by business for years.

The central gap continues to be the fragmentation of government services. Despite progress, it often remains unclear to companies which authority is responsible in which situation, which information should be reported where and what response can realistically be expected. This concerns, for example, drone sightings and drone defense, civil-military cooperation, security-relevant incidents, hybrid situational pictures and reporting channels to the police, the Office for the Protection of the Constitution (Verfassungsschutz), BSI, BBK, the Bundeswehr and state authorities.

It is positive that certain threat areas are increasingly coordinated across authorities - for example in the Joint Counter-Terrorism Centre (Gemeinsames Terrorismusabwehrzentrum, GTAZ), the Joint Centre for Countering Extremism and Terrorism (Gemeinsames Extremismus- und Terrorismusabwehrzentrum, GETZ), the National Cyber Defence Centre (Nationales Cyber-Abwehrzentrum, Cyber-AZ), the Joint

Drone Defence Centre (Gemeinsames Drohnenabwehrzentrum, GDAZ) and now the Joint Centre for Countering Hybrid Threats (Gemeinsames Zentrum zur Abwehr hybrider Bedrohungen, GAZ Hybrid). At the same time, a new problem is emerging: the number of such centers, platforms and dialogue formats is growing faster than their connectivity for business. What ultimately counts for companies is not the internal logic of the authorities but a clear point of access, a shared understanding of the situation and effective interfaces.

Official classified information and sabotage protection is also becoming particularly important in view of hybrid threats, defense-related supply chains, dual-use technologies and sensitive infrastructure services. What is needed is a solution that brings together classified information protection, sabotage protection, economic protection and corporate reality - combined with a legally secure framework for security clearances and pre-employment screenings, which is not yet sufficiently clear, fast and practical.

7.3 Checklist: business requirements for the state

Use the following list to sharpen your own representation of interests vis-à-vis authorities and associations:

- **Create clear responsibilities:** unambiguous contact persons and transparent responsibilities - especially for drones, hybrid threats, civil-military cooperation and security-relevant incidents.
- **Establish a central point of access:** instead of many parallel centers, platforms and dialogue formats, business needs a clear, effective interface with the state.
- **Operationalize the strategy:** the National Economic Protection Strategy (Nationale Wirtschaftsschutzstrategie) must be translated into concrete processes, reporting channels, situational pictures and support services together with security associations and companies.
- **Reduce fragmentation:** government services should be better bundled, coordinated and made easier for companies to use.
- **Improve information flows:** companies need faster, practical and usable situational information, warnings and recommendations for action.
- **Enable legally secure information exchange:** the exchange of classified information between government and business also requires a robust legal basis, clear procedures, defined groups of recipients and practicable protection mechanisms.
- **Involve SMEs in a targeted manner:** small and medium-sized enterprises need low-threshold services, simple reporting channels and concrete support without high bureaucratic hurdles.
- **Develop classified information and sabotage protection in a practical way:** keep it closely linked to economic protection and corporate security.
- **Modernize security clearances:** procedures must become more reliable, faster and better tailored to security-relevant corporate functions.

- **Create legal certainty for pre-employment screenings:** a clear legal framework to adequately protect sensitive functions, key technologies and critical supply chains.
- **Establish a partnership on an equal footing:** government and business should jointly develop situational pictures, standards, exercises and crisis processes - not merely be consulted on an ad hoc basis.

What you should prepare internally

- **Appoint a contact person:** designate a responsible person or function as a single point of contact for security authorities and associations and maintain an up-to-date list of the relevant reporting and contact channels (BSI, BBK, Office for the Protection of the Constitution (Verfassungsschutz), police, state authorities, industry associations).
- **Document reporting channels:** define reporting channels for cyber incidents, drone sightings and suspected sabotage and test them once a year.
- **Formulate needs:** describe your own support needs specifically and submit them jointly via security associations.
- **Clarify personnel security:** coordinate criteria and the legal framework for security clearances and pre-employment screenings with HR, legal and data protection.
- **Use exchange formats:** participate in official situation briefings, discussion groups and exercises.

7.4 The shared vision

> *Business and government see themselves as strategic partners who jointly identify threats early, share situational pictures, clarify responsibilities and practice their response capability. The state contributes insights from the security authorities, coordination capability and legal frameworks; business adds operational proximity, knowledge of critical processes, international supply chains and technological expertise. The aim is an economic protection system that is not activated only in a crisis but permanently creates trust, exchange and joint capability.*

8 Regulatory and implementation roadmap

OPLAN DEU and the European regulatory landscape

Europe is regulating resilience in an increasingly binding but fragmented manner. CER, NIS-2, DORA, the Cyber Resilience Act and the Corporate Sustainability Due Diligence Directive (CSDDD; Directive (EU) 2024/1760) (Europäische Union 2022b; 2022a; 2022c; 2024a; 2024b) show that (cyber) security, resilience, product safety, critical infrastructures and supply chains are becoming central components of corporate security responsibility. At the same time, different speeds of implementation and national specifications in the member states lead to a patchwork of requirements that can result in additional complexity, operational risks and competitive disadvantages for internationally active companies. In addition, the CSDDD has been significantly restricted by the Omnibus I Directive: in future it will apply only to EU companies with more than 5,000 employees and more than EUR 1.5 billion in worldwide turnover, must be transposed by 26 July 2028 and applies from 26 July 2029 (Europäische Union 2026).

> *Those who merely comply reactively with European regulation remain trapped in a catalog of obligations. Those who understand it as a signal of geopolitical, operational and regulatory risks can gain orientation, robustness and capability from it.*

8.1 The Operational Plan for Germany (Operationsplan Deutschland, OPLAN DEU)

The Operational Plan for Germany (Operationsplan Deutschland) aims to ensure a functioning hub for military and civilian logistics and supply in a state of tension or defense (Spannungs- und Verteidigungsfall) (Bundeswehr / Operatives Führungskommando der Bundeswehr 2025; Bundeswehr 2023). Although this results in concrete requirements for business, there is currently no published OPLAN for business. Business cannot prepare for something it does not know.

- Ensuring transport and logistics capacities
- Protection and operation of critical infrastructures
- Provision of services and resources
- Integration into reporting and communication structures

This involvement is clearly addressed in the strategic concept. In operational implementation, however, challenges are emerging (Bundeswehr 2024): different levels of maturity in companies' preparation, limited depth of exercises and practical testing, partly unclear interfaces between government agencies and economic actors, and a lack of standardization of processes and procedures.

> *Key message: the strategic framework exists, but its operational implementation is still incomplete.*

8.2 Regulatory pressure versus entrepreneurial room for maneuver

Relevant developments include European requirements on cyber and digital resilience (NIS-2, Cyber Resilience Act), national regulations for the protection of critical infrastructures (German Critical Infrastructure Protection Umbrella Act [KRITIS-Dachgesetz]) and requirements for supply chain, data and technology sovereignty (Europäische Union 2022a; Europäische Union 2024a; Die Bundesregierung 2026b). This regulation aims to secure minimum standards and reduce systemic risks - but at the same time creates increasing compliance effort, parallel and partly overlapping requirements, different stages of implementation within Europe and uncertainties in interpretation and application.

> *Key message: regulation strengthens resilience selectively, but at the same time creates new complexity and potential inefficiencies (assessment by the ThinkTank; cf. BSI 2026b; Die Bundesregierung 2026a).*

8.3 Nine gaps in the system - self-diagnosis

Where do you see gaps in your own environment, at authorities, at associations or even internally in your own company? (BBK 2024; Bundeswehr 2024; BSI 2026b)

Gap	Description
Coordination gap	Parallel structures and responsibilities without unified leadership in a crisis.
Speed gap	Discrepancy between government decision-making processes and the dynamics of modern threats.
Implementation gap	Strategies and programs have been formulated, but their operational implementation and impact remain limited.
Total defense gap	The interlinking of governmental, economic and societal contributions to resilience is not fully and consistently integrated.
Digital sovereignty gap	High dependence on external technology providers combined with limited European alternatives.
Awareness gap	Security and resilience issues are not yet anchored as a strategic leadership task across the business community.
Regulatory gap	An increasing number of regulations leads to rising requirements but at the same time creates fragmentation and complexity.
Platform gap	There is a lack of integrated, scalable platforms for situational awareness, coordination and exchange between government and business.
Strategic operationalization gap	Overarching resilience concepts and target pictures exist, but their concrete operational implementation often remains unclear.

Taken together, these points show: the resilience architecture exists but is not consistently operationalized, synchronized and effectively integrated (Die Bundesregierung 2023; BBK 2024).

These nine gaps can be traced back to three structural causes: steering and integration deficits (coordination, platform, total defense and strategic operationalization gaps) (Die

Bundesregierung 2025; BBK 2022), speed and implementation deficits (speed and implementation gaps) (Die Bundesregierung 2023; BBK 2024) and sovereignty and capability deficits (digital sovereignty, regulatory and awareness gaps) (Europäische Kommission 2023b; Europäische Kommission 2026; BSI 2026b). The systemic effect is decisive: a lack of coordination reduces the speed of response, low speed exacerbates implementation problems, dependencies make independent action more difficult, and fragmented regulation increases the complexity of additional measures (BBK 2024; Bundeswehr 2024).

8.4 Implications for companies - concrete approaches

1. Build your own situational awareness and early warning systems - do not rely on consistently dependable government steering in a crisis.
2. Independently safeguard critical processes - redundancies and contingency plans that work without external coordination.
3. Develop in-house resilience structures independent of government steering - including clear internal escalation paths.

9 Market entry & diversification

Strategically viable markets in a changed geopolitical environment

Not all markets offer the same stability and growth potential under the changed geopolitical conditions. Five regions stand out as strategically particularly attractive.

9.1 EU single market

Remains a central anchor - despite regulatory complexity, it offers legal certainty, industrial depth and an increasingly sovereignty-oriented industrial policy that specifically strengthens domestic value creation.

9.2 India

Has been the world's most populous country since 2023 (UN DESA 2024), with a growing domestic market, ambitious industrialization goals and deliberate positioning as a strategic actor in the geopolitical competition between Western and emerging power centers, focused on its own economic advantage. The hostilities between India and Pakistan also represent a major factor of uncertainty for European business.

9.3 Southeast Asia (ASEAN)

Benefits from nearshoring effects, young populations and dynamic middle classes that are creating new consumer and industrial markets (FDI inflows in 2024 of approx. USD 226 billion, driven among other things by the restructuring of international supply chains; ASEAN-Sekretariat/UNCTAD 2025).

9.4 Gulf region

Is transforming itself with enormous capital deployment from a resource-based to a knowledge-based economy (IMF 2025). The combination of sovereign wealth funds, infrastructure programs and targeted investment promotion policies creates attractive conditions for internationally oriented companies. Since 2026, however, the region has been exposed to a significantly increased security and supply risk due to the Iran war, attacks on energy infrastructure in the Gulf and repeated massive restrictions on shipping through the Strait of Hormuz (Euronews 2026a).

9.5 Brazil and Mercosur

The interim trade agreement between the EU and Mercosur (Argentina, Brazil, Paraguay, Uruguay) has been provisionally applied since 1 May 2026; tariffs on EU goods are being

gradually reduced (Die Bundesregierung 2026d). As the largest economy in the region, Brazil offers a large industrial and consumer goods market, raw materials and potential for renewable energy. The review of the agreement by the Court of Justice of the EU and the approval of the European Parliament are still pending; in addition, there is political volatility in individual member states.

9.6 Checklist: structural prerequisites for market entry

Developing these markets requires structural prerequisites that should be examined before every market entry decision:

- Infrastructure - local transport, energy and digital infrastructure
- Industrial maturity - existing supplier base and availability of skilled workers
- Degree of digitalization - administrative and approval processes
- Energy availability - security of supply and costs
- Regulatory framework - reliability and planning certainty for investments

These factors are decisive for market entry planning and operational risk management - and should be incorporated into every location or diversification decision derived from Module 4, Chapter 5 (critical dependencies) or Module 5, Chapter 6 (scenario stress test).

10 Opportunity areas in detail

Strategic opportunity areas of the coming years

Geopolitical change not only gives rise to risks - it also opens up substantial entrepreneurial opportunity areas that will attract considerable investment volumes in the coming years. Strategic White Paper 02 (Chapter 7.3) describes which investment programs support these areas; the following sections show where companies can start in concrete terms.

10.1 Defense & dual-use

The growing need for national and collective security is driving investment in a broad spectrum of technologies: software, sensors, communication systems, drone and anti-drone components, robotics, electronics, cyber capabilities, space applications and resilient energy supply for security-critical infrastructures. Mechanical engineering, automotive electronics, embedded systems, Artificial Intelligence, secure networks and manufacturing technology also benefit from the build-up of defense industrial capacities. The dual-use principle - the dual usability of civilian and military technologies - opens up new markets beyond traditional defense structures, especially for medium-sized technology companies.

10.2 Infrastructure & energy

The pressure to transform energy systems and physical infrastructure is enormous: grids, storage technologies, flexibility solutions, electrification infrastructure, industrial efficiency, the hydrogen economy, heating solutions, resilience engineering and local energy availability form an investment spectrum designed to last for decades. In demand are integrated solution providers that master the planning, construction, operation, digitalization and protection of infrastructure systems - including services, components, software and innovative financing models.

10.3 Digital sovereignty

The political and regulatory pressure to keep critical digital technology under European control is creating a growth market for solutions around secure cloud and edge architectures, cybersecurity, OT security, data spaces, trustworthy AI, embedded electronics, semiconductor applications and sovereign operating platforms. This field is particularly attractive where regulatory requirements, security needs and industrial applicability converge - a constellation that is increasingly becoming the norm in Europe.

AI as an opportunity area: Artificial Intelligence offers its own opportunities: sovereign AI infrastructure and computing capacities in Europe, AI-supported security and resilience services (e.g. situational picture, supply chain monitoring) and trustworthy, compliant AI applications for industry and public administration, for which the EU AI Act creates a common legal framework (Europäische Union 2024c).

10.4 Regional value creation

The intelligent reorganization of production, service and supply networks in line with geopolitical realities is more than logistics optimization - it is strategic positioning. European customer proximity, regional supply, local service capability, short decision-making paths and scalable platforms are becoming competitive advantages that increasingly outweigh the traditional cost advantages of global sourcing.

> *Companies that systematically integrate delivery capability, security standards, regulatory compliance and resistance to disruption into their value propositions and business models create sustainable differentiation - regardless of which geopolitical scenario ultimately unfolds.*

References

ASEAN-Sekretariat; UNCTAD (2025): ASEAN Investment Report 2025: Foreign direct investment and supply chain development. Jakarta: ASEAN Secretariat. Available at: https://unctad.org/publication/asean-investment-report-2025 (accessed 30 September 2026).

BBK - Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2022): Deutsche Strategie zur Stärkung der Resilienz gegenüber Katastrophen. [German Strategy for Strengthening Resilience to Disasters]. Decision of the Federal Government of 13 July 2022. Available at: https://www.bbk.bund.de/DE/Themen/Nationale-Kontaktstelle-Sendai-Rahmenwerk/Resilienzstrategie/resilienz-strategie_node.html (accessed 16 June 2026).

BBK - Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2024): Umsetzungsplan der Deutschen Strategie zur Stärkung der Resilienz gegenüber Katastrophen. [Implementation Plan of the German Strategy for Strengthening Resilience to Disasters]. Available at: https://www.bbk.bund.de/SharedDocs/Downloads/DE/Mediathek/Publikationen/Sendai-Katrima/umsetzungsplan-resilienzstrategie.pdf?__blob=publicationFile&v=6 (accessed 16 June 2026).

Bentzen, Naja (2024): Online information manipulation and information integrity. European Parliamentary Research Service (EPRS), Briefing PE 762.416. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/762416/EPRS_BRI%282024%29762416_EN.pdf (accessed 16 June 2026).

BfV - Bundesamt für Verfassungsschutz (2025): Spionage, Cyberangriffe & Co. Bedrohungen durch fremde Nachrichtendienste. [Espionage, Cyberattacks & Co. Threats from Foreign Intelligence Services]. January 2025. Available at: https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/spionage-und-proliferationsabwehr/2025-01-spionage-cyberangriffe-und-co.pdf?__blob=publicationFile&v=3 (accessed 17 June 2026).

BMI - Bundesministerium des Innern (2026): Nationale Wirtschaftsschutzstrategie. [National Economic Protection Strategy]. Cabinet decision of 18 March 2026. Available at: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/sicherheit/BMI26004-nationale-wirtschaftsschutzstrategie.pdf?__blob=publicationFile&v=5 (accessed 4 November 2026).

BSI - Bundesamt für Sicherheit in der Informationstechnik (2023): BSI-Standard 200-4: Business Continuity Management. Version 1.0, published on 14 June 2023. Bonn: BSI; book edition: Cologne: Reguvis Fachmedien. Available at: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_4.pdf?__blob=publicationFile&v=8 (accessed 4 November 2026).

BSI - Bundesamt für Sicherheit in der Informationstechnik (2024): KI und gegenwärtige Cyberbedrohungen. [AI and Current Cyber Threats]. Threat intelligence blog post of 11 September 2024. Available at: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Threat-Intelligence/Blogeintraege/KI_gegenwaertige-Cyberbedrohungen.html (accessed 26 October 2026).

BSI - Bundesamt für Sicherheit in der Informationstechnik (2025): Die Lage der IT-Sicherheit in Deutschland 2025. [The State of IT Security in Germany 2025]. Available at: https://medien.bsi.bund.de/lagebericht/de/ (accessed 17 June 2026).

BSI - Bundesamt für Sicherheit in der Informationstechnik (2026a): KI-Modelle revolutionieren den Umgang mit Sicherheitslücken. [AI Models Are Revolutionizing the Handling of Security Vulnerabilities]. 8 May

2026. Available at: https://www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Blog/KI-Modelle_neue_Zeitrechnung_260508.html (accessed 17 June 2026).

BSI - Bundesamt für Sicherheit in der Informationstechnik (2026b): NIS-2 in Zahlen. [NIS-2 in Figures]. Available at: https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/NIS-2-in-Zahlen/nis-2-in-zahlen.html (accessed 26 October 2026).

Bundeswehr (2023): Operationsplan Deutschland: Wie verteidigen wir unser Land? [Operational Plan for Germany: How Do We Defend Our Country?] 14 November 2023. Available at: https://www.bundeswehr.de/de/selbstverstaendnis/geschichte-bundeswehr/territoriales-fuehrungskommando-der-bundeswehr/operationsplan-deutschland-5703688 (accessed 16 June 2026).

Bundeswehr (2024): Stresstest für den Operationsplan Deutschland. [Stress Test for the Operational Plan for Germany]. 26 November 2024. Available at: https://www.bundeswehr.de/de/organisation/operatives-fuehrungskommando-der-bundeswehr/stresstest-operationsplan-deutschland-5863010 (accessed 16 June 2026).

Bundeswehr / Operatives Führungskommando der Bundeswehr (2025): Gesamtverteidigung: Alles über den Operationsplan Deutschland. [Total Defense: All about the Operational Plan for Germany]. Available at: https://www.bundeswehr.de/de/organisation/operatives-fuehrungskommando-der-bundeswehr/auftrag-und-aufgaben/operationsplan-deutschland (accessed 16 June 2026).

Crosignani, Matteo; Han, Lina; Macchiavelli, Marco; Silva, André F. (2024): Securing Technological Leadership? The Cost of Export Controls on Firms (original title: Geopolitical Risk and Decoupling: Evidence from U.S. Export Controls). Federal Reserve Bank of New York Staff Reports, No. 1096, April 2024, revised February 2025. DOI: 10.59576/sr.1096. Available at: https://www.newyorkfed.org/research/staff_reports/sr1096 (accessed 30 September 2026).

Die Bundesregierung (2023): Nationale Sicherheitsstrategie - Integrierte Sicherheit für Deutschland. [National Security Strategy - Integrated Security for Germany]. 14 June 2023. Available at: https://www.bundesregierung.de/breg-de/aktuelles/nationale-sicherheitsstrategie-2195890 (accessed 16 June 2026).

Die Bundesregierung (2025): Deutschland bekommt einen Nationalen Sicherheitsrat. [Germany Gets a National Security Council]. Cabinet decision of 27 August 2025. Available at: https://www.bundesregierung.de/breg-de/aktuelles/kabinett-sicherheitsrat-2381492 (accessed 26 October 2026).

Die Bundesregierung (2026a): Maßnahmen für mehr Cybersicherheit. [Measures for More Cybersecurity]. Available at: https://www.bundesregierung.de/breg-de/aktuelles/massnahmen-bundesregierung-cybersicherheit-2432652 (accessed 16 June 2026).

Die Bundesregierung (2026b): Schutz kritischer Infrastruktur gestärkt (KRITIS-Dachgesetz). [Protection of Critical Infrastructure Strengthened (KRITIS Umbrella Act)]. 17 March 2026. Available at: https://www.bundesregierung.de/breg-de/aktuelles/kritis-dachgesetz-2383682 (accessed 16 June 2026).

Die Bundesregierung (2026c): Fragen und Antworten zur EU-US-Zolleinigung. [Questions and Answers on the EU-US Tariff Agreement]. Available at: https://www.bundesregierung.de/breg-de/service/fragen-und-anworten/faq-eu-us-zolleinigung-2340924 (accessed 20 October 2026).

Die Bundesregierung (2026d): EU-MERCOSUR-Abkommen vorläufig in Kraft. [EU-MERCOSUR Agreement Provisionally in Force]. Available at: https://www.bundesregierung.de/breg-de/aktuelles/mercosur-auf-dem-weg-2398594 (accessed 23 October 2026).

EIA - U.S. Energy Information Administration (2025): Amid regional conflict, the Strait of Hormuz remains critical oil chokepoint. Today in Energy, June 2025. Available at: https://www.eia.gov/todayinenergy/detail.php?id=65504 (accessed 30 September 2026).

Euronews (2026a): Was die Sperrung der Straße von Hormus für Ölpreise, Gas und Europa bedeutet. [What the Closure of the Strait of Hormuz Means for Oil Prices, Gas and Europe]. 1 April 2026. Available at: https://de.euronews.com/my-europe/2026/04/01/strasse-von-hormus-oelpreise-europa (accessed 30 September 2026).

Europäische Kommission (2023b): European Economic Security Strategy. 20 June 2023. Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3358 (accessed 16 June 2026).

Europäische Kommission (2024): Commission proposes new initiatives to strengthen economic security. Press release IP/24/363, 24 January 2024. Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_24_363; print version: https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_24_363/IP_24_363_EN.pdf (accessed 4 November 2026).

Europäische Kommission (2026): Strengthening Europe's tech sovereignty. News item of 3 June 2026. Available at: https://commission.europa.eu/news-and-media/news/strengthening-europes-tech-sovereignty-2026-06-03_en (accessed 26 October 2026).

Europäische Union (2022a): Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive). Available at: https://eur-lex.europa.eu/eli/dir/2022/2555/oj (accessed 16 June 2026).

Europäische Union (2022b): Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities (CER Directive). Available at: https://eur-lex.europa.eu/eli/dir/2022/2557/oj (accessed 29 September 2026).

Europäische Union (2022c): Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector (DORA). Available at: https://eur-lex.europa.eu/eli/reg/2022/2554/oj (accessed 29 September 2026).

Europäische Union (2024a): Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act). Available at: https://eur-lex.europa.eu/eli/reg/2024/2847/oj (accessed 16 June 2026).

Europäische Union (2024b): Directive (EU) 2024/1760 of the European Parliament and of the Council of 13 June 2024 on corporate sustainability due diligence (CSDDD). Available at: https://eur-lex.europa.eu/eli/dir/2024/1760/oj (accessed 29 September 2026).

Europäische Union (2024c): Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (AI Act). Available at: https://eur-lex.europa.eu/eli/reg/2024/1689/oj (accessed 19 October 2026).

Europäische Union (2026): Directive (EU) 2026/470 of the European Parliament and of the Council amending, inter alia, Directive (EU) 2024/1760 (Omnibus I). Published in the Official Journal on 26 February 2026, in force since 18 March 2026. Available at: https://eur-lex.europa.eu/eli/dir/2026/470/oj (accessed 30 September 2026).

Europäisches Parlament (2025): European Software and Cyber Dependencies. Study commissioned by the ITRE Committee, written by Gineikyte-Kanclere, Vaida; Eggert, Militsa; Skiotyte, Goda (Visionary Analytics), PE 778.576, December 2025. Available at:

https://www.europarl.europa.eu/RegData/etudes/STUD/2025/778576/ECTI_STU%282025%29778576_EN.pdf (accessed 17 June 2026).

Eurostat (2026): Exports to US dropped by 30% year-on-year in Q1 2026. Eurostat News, 28 May 2026. Available at: https://ec.europa.eu/eurostat/en/web/products-eurostat-news/w/ddn-20260528-1 (accessed 2 November 2026).

Feyen, Erik; Utz, Robert; Zuccardi Huertas, Igor; Bogdan, Olena; Moon, Jisung (2020): Macro-Financial Aspects of Climate Change. World Bank Policy Research Working Paper 9109. Available at: https://documents1.worldbank.org/curated/en/223161579009566321/pdf/Macro-Financial-Aspects-of-Climate-Change.pdf (accessed 16 June 2026).

Hakobyan, Shushanik; Meleshchuk, Sergii; Zymek, Robert (2023): Divided We Fall: Differential Exposure to Geopolitical Fragmentation in Trade. IMF Working Paper No. 2023/270. Available at: https://www.imf.org/en/publications/wp/issues/2023/12/22/divided-we-fall-differential-exposure-to-geopolitical-fragmentation-in-trade-542842 (accessed 16 June 2026).

IEA - International Energy Agency (2022): World Energy Outlook 2022. Paris: IEA. Available at: https://www.iea.org/reports/world-energy-outlook-2022 (accessed 16 June 2026).

IMF - International Monetary Fund (2023a): World Economic Outlook, October 2023: Navigating Global Divergences. Washington, D.C.: IMF. Available at: https://www.imf.org/en/publications/weo/issues/2023/10/10/world-economic-outlook-october-2023 (accessed 16 June 2026).

IMF - International Monetary Fund (2023b): Global Financial Stability Report, April 2023, Chapter 3: Geopolitics and Financial Fragmentation: Implications for Macro-Financial Stability (chapter authors: Catalán, Mario; Tsuruga, Tomohiro et al.). Washington, D.C.: IMF. Available at: https://www.imf.org/en/publications/gfsr/issues/2023/04/11/global-financial-stability-report-april-2023 (accessed 30 September 2026).

IMF - International Monetary Fund (2025): Regional Economic Outlook: Middle East and Central Asia, May 2025 - Charting a Path through the Haze. Washington, D.C.: IMF. ISBN 9798229007771. Available at: https://www.bookstore.imf.org/books/regional-economic-outlook-middle-east-and-central-asia-may-2025-charting-a-path-through-the-haze (accessed 4 November 2026).

IPCC (2022): Climate Change 2022: Impacts, Adaptation and Vulnerability. Contribution of Working Group II to the Sixth Assessment Report of the Intergovernmental Panel on Climate Change. Available at: https://www.ipcc.ch/report/ar6/wg2/ (accessed 16 June 2026).

ISO - International Organization for Standardization (2017): ISO 22316:2017 Security and resilience - Organizational resilience - Principles and attributes. Geneva: ISO. Available at: https://www.iso.org/standard/50053.html (accessed 4 November 2026).

ISO - International Organization for Standardization (2019): ISO 22301:2019 Security and resilience - Business continuity management systems - Requirements, including Amendment 1:2024 (Climate action changes). Geneva: ISO. Available at: https://www.iso.org/standard/75106.html (accessed 4 November 2026).

ISO - International Organization for Standardization (2025): ISO 22300:2025 Security and resilience - Vocabulary. Geneva: ISO. Available at: https://www.iso.org/standard/85749.html (accessed 4 November 2026).

Kleinhans, Jan-Peter; Jha, Sabhyata (2025): The chip landscape: Geographical distribution of wafer fabrication capacity. OECD Science, Technology and Industry Policy Papers, 30 November 2025.

Paris: OECD Publishing. DOI: 10.1787/02dbd028-en. Available at: https://www.oecd.org/en/publications/the-chip-landscape_02dbd028-en.html (accessed 30 September 2026).

Kotzanikolaou, Panayiotis; Theoharidou, Marianthi; Gritzalis, Dimitris (2013): Cascading Effects of Common-Cause Failures in Critical Infrastructures. In: Critical Infrastructure Protection VII. IFIP AICT, Vol. 417, pp. 171-182. DOI: 10.1007/978-3-642-45330-4_12. Available at: https://inria.hal.science/hal-01456884/file/978-3-642-45330-4_12_Chapter.pdf (accessed 16 June 2026).

Mühlhofer, Evelyn; Bresch, David N.; Koks, Elco E. (2024): Infrastructure failure cascades quintuple risk of storm and flood-induced service disruptions across the globe. In: One Earth, 7(4), pp. 714-729. Available at: https://www.cell.com/one-earth/fulltext/S2590-3322%2824%2900139-8 (accessed 16 June 2026).

NATO (2024): Washington Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Washington, D.C., 10 July 2024. Press Release 2024 001. Available at: https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/07/10/washington-summit-declaration (accessed 4 November 2026).

NCSC - National Cyber Security Centre (2025): Impact of AI on cyber threat from now to 2027. London: NCSC. Available at: https://www.ncsc.gov.uk/sites/default/files/pdfs/publication/impact-ai-cyber-threat-now-2027.pdf (accessed 17 June 2026).

OECD (2021): International Migration Outlook 2021. Paris: OECD Publishing. Available at: https://www.oecd.org/en/publications/international-migration-outlook-2021_29f23e9d-en.html (accessed 16 June 2026).

OECD (2023): Building Trust and Reinforcing Democracy - Action Plans. OECD Public Governance Committee at Ministerial Level, document GOV/PGC/MIN(2022)4; adopted at the ministerial meeting in Luxembourg on 18 November 2022, published 2023. Available at: https://one.oecd.org/document/gov/pgc/min%282022%294/en/pdf (accessed 16 June 2026).

OECD (2024): Facts not Fakes: Tackling Disinformation, Strengthening Information Integrity. Paris: OECD Publishing. DOI: 10.1787/d909ff7a-en. Available at: https://doi.org/10.1787/d909ff7a-en (accessed 30 September 2026).

OECD (2026): Global value and supply chains; Resilient supply chains. OECD topic pages. Available at: https://www.oecd.org/en/topics/global-value-and-supply-chains.html and https://www.oecd.org/en/topics/resilient-supply-chains.html (accessed 16 June 2026).

SIA/BCG - Semiconductor Industry Association; Boston Consulting Group (2021): Strengthening the Global Semiconductor Supply Chain in an Uncertain Era. April 2021. Available at: https://www.semiconductors.org/strengthening-the-global-semiconductor-supply-chain-in-an-uncertain-era/ (accessed 29 September 2026).

TrendForce (2024): Foundry Capacity Market Share of Advanced Process to Decline in Taiwan, Korea until 2027, While US on the Rise. 14 May 2024. Available at: https://www.trendforce.com/news/2024/05/14/insights-trendforce-foundry-capacity-market-share-of-advanced-process-to-decline-in-taiwan-korea-until-2027-while-us-on-the-rise/ (accessed 30 September 2026).

UN DESA - United Nations, Department of Economic and Social Affairs (2024): World Population Prospects 2024. Available at: https://population.un.org/wpp/ (accessed 29 September 2026).

Varley, Kevin (2022): Taiwan Tensions Raise Risks in One of Busiest Shipping Lanes. Bloomberg, 2 August 2022. Available at: https://www.bloomberg.com/news/articles/2022-08-02/taiwan-tensions-raise-risks-in-one-of-busiest-shipping-lanes (accessed 30 September 2026).

WEF - World Economic Forum (2026): Global Value Chains Outlook 2026: Orchestrating Corporate and National Agility. In cooperation with Kearney, 19 January 2026. Available at: https://www.weforum.org/publications/global-value-chains-outlook-2026-orchestrating-corporate-and-national-agility/ (accessed 29 September 2026).

WTO - World Trade Organization (2023): World Trade Report 2023: Re-globalization for a secure, inclusive and sustainable future. Geneva: WTO. Available at: https://www.wto.org/english/res_e/publications_e/wtr23_e.htm (accessed 30 September 2026).

List of Abbreviations

ASEAN	Association of Southeast Asian Nations
BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (Federal Office of Civil Protection and Disaster Assistance)
BCM	Business Continuity Management
BfV	Bundesamt für Verfassungsschutz (Federal Office for the Protection of the Constitution)
BMI	Bundesministerium des Innern (Federal Ministry of the Interior)
BSI	Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security)
CER	Critical Entities Resilience (Directive (EU) 2022/2557)
CSDDD	Corporate Sustainability Due Diligence Directive (Directive (EU) 2024/1760)
DORA	Digital Operational Resilience Act (Regulation (EU) 2022/2554)
ECFA	Economic Cooperation Framework Agreement (China-Taiwan, 2010)
EU	European Union
R&D	Research and development
FDI	Foreign Direct Investment
IEA	International Energy Agency
IMF	International Monetary Fund
IP	Intellectual Property
IPCC	Intergovernmental Panel on Climate Change
IT	Information technology
AI	Artificial Intelligence
SMEs	Small and medium-sized enterprises
KRITIS	Critical infrastructure (Kritische Infrastrukturen)
LNG	Liquefied Natural Gas
MBCO	Minimum Business Continuity Objective
NATO	North Atlantic Treaty Organization
NCSC (UK)	National Cyber Security Centre

NCSC (USA)	National Counterintelligence and Security Center
NIS-2	Directive (EU) 2022/2555 on network and information security
nm	Nanometer (unit for the feature size of semiconductors)
OECD	Organisation for Economic Co-operation and Development
OPLAN DEU	Operationsplan Deutschland (Operational Plan for Germany)
OT	Operational Technology
THI	Technische Hochschule Ingolstadt
VSW	Verband für Sicherheit in der Wirtschaft, Bundesverband e.V. (VSW Bundesverband)
WEF	World Economic Forum
WTO	World Trade Organization

Your opinion matters to us!

FAQ & feedback on the white paper

Do you have any questions or suggestions?

Use our feedback questionnaire or contact our ThinkTank directly. Your input is valuable and can make a decisive contribution to making future publications even more practical and relevant.

Visit our FAQs to find answers to frequently asked questions and to explore the topic in greater depth.

👉 **Contact & feedback**

Operational Guide 01 to White Paper 02 - ThinkTank Corporate Resilience, November 2026