THINKTANK
CORPORATE RESILIENCE
WHITE PAPER 02

Geopolitical Change, AI and Entrepreneurial Options

- Scenarios, Challenges and New Opportunity Areas for Business -

VSW
Bundesverband

November 2026

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

Foreword

With this White Paper 02, the **ThinkTank Corporate Resilience** continues the work that began with the first white paper in December 2025. Since then, the geopolitical situation has deteriorated further: trade conflicts, the formation of technology blocs, security tensions and the rapid development of Artificial Intelligence increasingly shape day-to-day business. This creates new opportunities, but also additional vulnerabilities for companies in Germany and Europe.[1]

This white paper places these developments in a strategic context and translates them into concrete options for corporate decision-making.

Two documents: Strategic White Paper 02 and Operational Guide 01

The aim of this white paper is to provide a robust frame of reference for strategic decisions in an increasingly volatile, geopolitically shaped and AI-driven environment, not to predict future developments.

This white paper analyzes how geopolitical conditions and AI developments affect companies in Germany and Europe - and what this means for leadership, strategy, resilience and operational capability.

To make the key findings effective at different decision-making levels, the publication is divided into two documents:

- a **Strategic White Paper** - this document - which concisely presents the most important facts, findings and implications for strategic decisions, in particular for management, executive boards and supervisory boards;

- the **Operational Guide 01** to White Paper 02 as a companion document that provides in-depth analyses, checklists, scenario stress tests and working tools for corporate security, information security, risk, crisis and business continuity management, corporate resilience, procurement, compliance and other relevant functions.

[1] ThinkTank Corporate Resilience (2025): Wirtschaftliche Folgen hybrider Bedrohungen für Unternehmen und ihre Wertschöpfungsketten – Wie muss sich die Wirtschaft jetzt vorbereiten [Economic consequences of hybrid threats for companies and their value chains - how business must prepare now]; https://www.vsw-bundesverband.de/wp-content/uploads/Whitepaper_01_ThinkTank_CorporateResilience.pdf

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

Executive Summary 5

1 The End of the Geopolitical Comfort Zone 6

1.1 From Globalization Winner to Resilience-Oriented Corporate Management 6

2 Multidimensional Force Fields: The New Rules of the Game for Companies 7

2.1 A Fragmented World Order 7

2.2 Concrete Impact on Companies 8

2.3 Employees, Executives and Key Personnel in the Context of the Multidimensional Force Fields 8

2.4 When Crises Fuel Each Other: Risk Multipliers 9

3 Technology and Innovation as a Geopolitical Battlefield 10

4 The Strategic Resilience Gap of Companies in Germany and Europe 13

4.1 Four Conflict Systems in an Economic Stress Test 13

4.2 Case Study Ukraine: Economic Resilience under Wartime Conditions 15

4.3 International Comparison: Strategic Differences and Structural Gaps 17

4.4 The Systemic Resilience Gap: Ambition Meets Reality 18

4.5 What This Means for Companies 19

5 Economic Protection Initiative (Initiative Wirtschaftsschutz): The State as a Partner with Added Value? 20

6 Geopolitical Scenarios 2027-2030 21

7 Business-Relevant Implications and Opportunity Areas 23

7.1 Potentially Strategically Viable Markets 23

7.2 Nine Critical Dependencies 24

7.3 Four Opportunity Areas with Future Potential 24

8 Conclusion: Key Messages for Corporate Management 25

9 Further Reading: Operational Guide 01 26

Contacts and Networks 27

References 28

List of Abbreviations 36

Executive Summary

Germany between Globalization and the Resilience Economy

The New Logic of Economic Competitiveness

The geopolitical conditions on which Germany's successful model of the globalization era was based are changing fundamentally. Developments that were long perceived as temporary disruptions are increasingly proving to be the expression of structural change: free trade, stable supply chains, reliable partnerships and predictable markets can no longer be assumed to be permanently secured.

Germany and Europe therefore face a fundamental strategic realignment. In the future, economic competitiveness will be shaped more strongly by resilience, diversification, technological sovereignty, the effective use of AI and strategic agility.

Three key findings

- **Competition is increasingly shaped by geopolitics.** Germany's export-oriented, globalization-driven business model is under systemic pressure to adapt. Markets are fragmenting, dependencies are becoming strategic vulnerabilities, and economic competition is increasingly influenced by geopolitical conditions, technology bloc formation and AI-driven developments.
- **Companies' resilience gap is becoming more visible**. Compared with leading economies, Germany faces structural challenges in decision-making speed, digitalization, energy independence, AI capabilities and strategic focus. For companies, this results in the task of systematically identifying and reducing critical dependencies, operational vulnerabilities and a lack of adaptability.
- **The transformation opens up new strategic opportunity areas.** Defense and dual-use, infrastructure and energy, digital sovereignty including Artificial Intelligence, and regional value creation are among the defining strategic opportunity areas of the coming years. Companies that invest early in resilience, technological capabilities and new partnerships can derive sustainable competitive advantages from this.

Guiding question for every company:

Which decisions must be made today, in the coming six months and in the long term to reduce critical vulnerabilities and make the company's business model resilient, competitive and adaptable?

1 The End of the Geopolitical Comfort Zone

1.1 From Globalization Winner to Resilience-Oriented Corporate Management

For decades, Germany benefited from globalization like hardly any other country. Open markets, stable supply chains, international economic interdependence and a largely reliable political and security order provided a stable framework for business activity. These conditions gave companies a high degree of predictability, efficiency and international scalability. Today, traditional optimization approaches focused primarily on efficiency, cost reduction and the global division of labor are reaching their limits and neglect innovative opportunities. Risks that used to be regarded as external exceptions are becoming permanent factors in strategic corporate management.

Companies must therefore assume that geopolitical volatility, technological power rivalry, AI-driven disruption and increasing state intervention in markets are not temporary disruptions but **permanent planning parameters**. Economic efficiency remains a key competitive factor, but is increasingly complemented by security, sovereignty and resilience requirements.

> In this context, resilience refers to the ability of companies to maintain critical success objectives even under adverse conditions, to withstand disruptions, to recover quickly from them and to adapt in a way that strengthens long-term performance and stability.

Resilience is thus evolving from a traditional risk and protection function into a strategic competitive factor. Companies with resilient supply chains, robust digital infrastructures and a high degree of adaptability can seize market opportunities faster, meet regulatory requirements more effectively and maintain their operational performance even in crises. According to the Global Value Chains Outlook 2026, 74% of the executives surveyed regard resilience as a growth driver (WEF 2026).

A “return” to previous security policy assumptions appears unrealistic. It is not only individual crises that have intensified; rather, the framework of business activity has changed structurally. Companies increasingly face trade-offs between short-term efficiency and long-term resilience. Diversifying suppliers, building redundant capacity, safeguarding critical technologies or regionalizing value chains often increase costs at first. At the same time, they reduce vulnerability to geopolitical crises, trade conflicts, cyberattacks, technological dependencies and regulatory intervention.

Resilience thus becomes a management decision that must link risks, opportunities and corporate objectives holistically.

The key challenge is not to predict geopolitical developments and AI dynamics precisely. Rather, what matters is aligning strategic and operational capabilities so that companies remain capable of acting and can achieve their business objectives even under volatile

conditions. Resilience is therefore not the opposite of economic performance, but an essential prerequisite for sustainable competitiveness, innovative capacity and growth.

For top management, the question therefore arises as to how corporate resilience can be anchored organizationally, linked to strategy and governance, and integrated into critical value creation processes.

2 Multidimensional Force Fields: The New Rules of the Game for Companies

For a long time, geopolitics was primarily a matter for foreign ministries, intelligence services and security policy planning units. Today, it has a direct impact on corporate decisions. No company is geopolitically neutral any longer: even companies without direct political exposure are affected when market access, energy prices, data flows, supply chains or access to technology are politically influenced, regulated, restricted or otherwise made conditional.

Other force fields such as climate change, increasing environmental pressures, the scarcity of critical resources such as water, and further ecological, demographic and social trends, for example the management of global migration with its opportunities and challenges, have a considerable influence on the conditions for business activity. These factors do not exist in isolation but frequently interact and, in combination with geopolitical developments, create additional dynamics, risks and opportunities. Taken together, they form a substantial part of the strategic risk and opportunity environment that companies must take into account when developing long-term resilience and future viability strategies.

2.1 A Fragmented World Order

The rise of China as an economic, technological and political actor is changing the international order, which has so far been strongly shaped by the United States. China and India as well as other emerging countries are seeking to expand their spheres of influence. This is evident, among other things, in formats such as BRICS, which should be understood less as a closed counter-model and more as an expression of a growing willingness to pursue alternative power and economic relationships.

At the same time, NATO is coming under pressure to adapt as US foreign policy focuses more strongly on the Pacific, while the EU's efforts to achieve greater strategic autonomy are intensifying (Rat der Europäischen Union 2022; Europäische Kommission, Hoher Vertreter 2025). For companies, this means that market access increasingly depends not only on their own competitiveness but also on political conditions, regulatory requirements and strategic alliances. This leads to competition for resources, technologies, standards, industrial value creation and geopolitical influence (cf. Mearsheimer 2014; Die Bundesregierung 2023; Münchner Sicherheitskonferenz 2026; Merz 2026).

2.2 Concrete Impact on Companies

Dimension	Concrete impact
Markets	Market access becomes politically conditional; export controls and sanctions close off economic areas.
Supply chains	Single-source dependencies become an existential risk; nearshoring must be viewed strategically, not only from a cost perspective.
Capital	Geopolitical risk is priced in; ESG and geopolitical compliance requirements overlap.
Talent	Skilled immigration is politically regulated; location decisions acquire a geopolitical dimension.
Innovation	Technology transfer is restricted; IP protection and dual-use controls are increasing.
Raw material and energy supply	Raw materials and energy are used as geopolitical instruments; supply bottlenecks and price increases raise costs and amplify location and supplier risks.
Locations and production	The attractiveness of locations is shaped by geopolitical stability; sanctions, resource and supply chain risks affect long-term operational capability.

Table 1: Concrete impact of geopolitical developments on companies. Source: own presentation based on Hakobyan, Meleshchuk, Zymek 2023; WTO 2023; IMF 2023b; OECD 2021; Europäische Kommission 2024; IEA 2022; WEF 2026

A function-specific overview with concrete options for action for markets, supply chains, capital, talent, innovation, raw material and energy supply, locations and production, employees and executives, and Artificial Intelligence can be found in Operational Guide 01, Module 1, Chapter 2.

2.3 Employees, Executives and Key Personnel in the Context of the Multidimensional Force Fields

Every company's central asset to be protected is its employees: 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. BfV 2025). In addition, executives and key personnel may be subject to increased digital and physical exposure due to their function, visibility and decision-making responsibility. Publicly available

information, digital traces and appointment and travel data can be combined and used for phishing, reconnaissance, influence operations, targeted approaches or physical threats. Digital traces and publicly available information about family members, in particular partners or children, can also allow conclusions to be drawn about the whereabouts, routines or movement profiles of exposed persons. In addition, there are AI-generated voice and video forgeries (deepfakes): even short publicly available audio or video recordings can be enough to imitate executives deceptively realistically, discredit them or expose them to blackmail (cf. BSI 2024; NCSC 2025).

The protection of exposed persons must therefore be considered as part of corporate resilience, depending on the security situation, function and risk. Measures must be proportionate and balance security interests, personal rights and the necessary visibility and agility of leadership.

Conclusion: The digital and physical exposure of executives and key personnel must be assessed as an interrelated corporate risk and addressed proportionately.

2.4 When Crises Fuel Each Other: Risk Multipliers

Geopolitical risks rarely act in isolation. Their particular relevance arises where individual disruptions are transmitted to other systems via energy, logistics, data, capital markets, supply chains, regulation, social stability and climate. As a result, initially limited events can give rise to complex chains of effects that can no longer be managed with traditional single-risk approaches (Kotzanikolaou, Theoharidou, Gritzalis 2013; Mühlhofer, Bresch, Koks 2024).

A cyberattack can interrupt production processes, jeopardize delivery obligations, trigger regulatory reporting obligations, cause reputational damage and have financial consequences. It is precisely in these chain reactions that the real vulnerability for achieving corporate objectives lies.

Companies can protect themselves effectively if they understand and manage geopolitical risk areas not as a collection of isolated individual risks but as an interconnected system, and regard this as an essential element of their value creation.

An advanced resilience strategy combines at least six building blocks: (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, and (6) cooperation with trusted partners and public authorities. The full analysis of risk multipliers including self-assessment questions can be found in Operational Guide 01, Module 2, Chapter 3.



Figure 1: Geopolitically significant risk areas and associated risk multipliers. Own presentation.

3 Technology and Innovation as a Geopolitical Battlefield

With the shift in global power structures, **technological development** is taking on a new, central role. **Technology** is no longer solely a driver of economic progress but is increasingly becoming the decisive factor for geopolitical power projection, economic competitiveness and security policy capability.

At the center of this competition are a few but systemically critical **technology fields**: **Artificial Intelligence**, **semiconductor technologies** as well as **digital infrastructures, cloud ecosystems, data spaces** and **platforms.** How quickly a vulnerability in widely used basic software can become a broad risk for companies was most recently demonstrated by two critical vulnerabilities in the runtime environment of the PHP scripting language, known as “PHP2Shell”, which were published on 21 October 2026 and potentially affected numerous web applications worldwide (BSI 2026c).

Against this background, the concept of **digital sovereignty including AI capabilities** is gaining importance. States and companies are increasingly faced with the question of the extent to which they control their technological foundations or depend on external actors. These dependencies concern, for example, access to **cloud infrastructures**, the use of proprietary software solutions or control over critical data (JRC 2025; Europäische Kommission 2025; Europäisches Parlament 2025). At the same time, efforts to secure technological sovereignty are leading to new regulations and interventions, which in turn can affect corporate flexibility (Europäische Kommission 2023a).

A key unifying element of these developments is **cyberspace**. **Cyber** is increasingly being used as a strategic instrument that links economic, political and security dimensions. Activities in **cyberspace** range from economic espionage and sabotage to targeted influence operations, complementing attacks in the physical sphere (BfV 2025; BfV 2026). For companies, this means that **cyber risks** can no longer be regarded in isolation as an IT issue but must be understood as an integral part of geopolitical conflict situations and

addressed accordingly at the strategic level - in particular as part of preventive and holistic economic protection (BSI 2025; BSI 2024).

Artificial Intelligence reinforces this development in both directions: attackers use AI to find vulnerabilities faster, personalize phishing and social engineering, and imitate executives or business partners with voice and video forgeries (deepfakes); on the defender side, AI shortens detection and response times (BSI 2026a; BSI 2024; NCSC 2025). At the same time, a new dependency is emerging: powerful AI models, data centers and AI chips are concentrated among a few, predominantly non-European providers and are subject to export controls (Kleinhans, Jha 2025; Crosignani et al. 2024). For companies, AI is therefore at once a productivity lever, an attack surface and a strategic dependency. Moreover, its results do not replace expert review, as AI can produce incorrect or fabricated statements (“hallucinations”). Operational Guide 01 describes risks and countermeasures in Module 1, Chapter 2, Section 2.9, its use as a tool in Module 3, Chapter 4, Section 4.2 and opportunities in Module 9, Chapter 10, Section 10.3.

This development can be illustrated using the **example of China**. The Chinese technology offensive is anchored in comprehensive plans and programs. Since the 1990s, Beijing has combined long-term planning with national industrial and security strategy; under Xi Jinping, technological self-reliance has been anchored even more firmly as a strategic guiding principle (Eigner 2025; Zenglein, Holzmann 2019). Milestones of these plans are shown in the figure.



Figure 2: Milestones of China's technology and innovation strategy. Own presentation based on Eigner (2025), Wübbeke et al. (2016) and Zenglein, Holzmann (2019).

These strategic plans illustrate China's ambition to become the leading industrial and technological power by 2049, the 100th anniversary of the founding of the People's Republic of China. In the official rhetoric of the Chinese Communist Party (CCP), technological innovation is described as the key to national rejuvenation and global influence (Eigner 2025; Wübbeke et al. 2016; Zenglein, Holzmann 2019). These programs attracted attention in the West early on: “Made in China 2025”, for example, was regarded as an industrial policy offensive on the path to technological leadership and led to significant countermeasures, including export controls on critical technologies (Zenglein, Holzmann 2019; U.S. Department of State 2025; Crosignani et al. 2024).

Today, governments often use technology policy deliberately to reduce their own dependencies while at the same time exerting influence on international value chains; Western security authorities warn in particular of state-backed transfer of knowledge and technology in strategic future fields (ODNI/NCSC 2025; BfV 2024). For companies, this

results in the need to evaluate strategic decisions not only from an economic but also from a geopolitical perspective.

The consequences for companies are far-reaching. Technological decisions are increasingly becoming security-relevant and geopolitical decisions. The choice of partners, technologies and markets is closely linked to questions of resilience and the strategic positioning of a company and its value creation. Companies must therefore systematically analyze their technological dependencies, diversify risks and at the same time strengthen their ability to protect and further develop critical technologies (Kleinhans, Jha 2025; Europäische Kommission 2025).

In summary: technology has become a central arena of geopolitical competition. For companies, this means that innovation can no longer be viewed solely in terms of efficiency and growth, but is an integral part of a comprehensive strategy that combines economic, security and geopolitical dimensions (Europäische Kommission 2023b; BSI 2025).

4 The Strategic Resilience Gap of Companies in Germany and Europe

Germany has a powerful industrial base, technological know-how and considerable economic resources. However, the requirements for economic competitiveness and corporate resilience have changed fundamentally. In a world that increasingly requires adaptability, digital and technological sovereignty, a resilient energy supply and geopolitical agility, structural vulnerabilities are becoming more apparent. These concern in particular strategic dependencies, technological capabilities and the ability to respond quickly and effectively to external disruptions.

4.1 Four Conflict Systems in an Economic Stress Test

Russia's war of aggression against Ukraine, the war of the United States and Israel against Iran, the tensions in the Taiwan Strait and the restrictive tariff and trade policy of the United States reflect different geopolitical conflict dynamics and put the economic resilience of German and European companies to the test. This is particularly evident in

the considerable restrictions on shipping through the Strait of Hormuz and their impact on energy supply, transport costs and international supply chains.

Conflict system	Risk for companies	Opportunity for companies
Russia - Ukraine	Energy and raw material shocks, disrupted Eastern European supply chains, rising security requirements and possible effects of higher defense spending on public budgets and investment priorities.	Accelerated development of a diversified and more resilient energy supply (LNG, renewables, hydrogen); growth of the defense industry; participation in the reconstruction of Ukraine (reconstruction needs approx. USD 588 billion over the next ten years, as of December 2025; World Bank et al. 2026).
Iran - USA	Higher oil prices and transport costs; considerable impairment of strategic maritime trade routes, in particular the Strait of Hormuz, and indirect effects on other international transport links; planning uncertainty for exporters.	Diversification of energy and trade relations; development of alternative transport routes and more resilient logistics networks; additional demand for energy efficiency, infrastructure and security technologies.
China - Taiwan	Potentially far-reaching disruptions to global semiconductor and technology supply chains with significant effects on export-oriented industries; in 2025, China was once again Germany's most important trading partner in terms of total goods trade (Destatis 2026).	Expansion of European semiconductor capacities (European Chips Act, Regulation (EU) 2023/1781); targeted de-risking; diversification of technological dependencies, strengthening of regional value chains and nearshoring

Conflict system	Risk for companies	Opportunity for companies
USA - EU (tariff and trade policy)	US tariff rules with an agreed general maximum tariff rate of 15% for most EU goods (political agreement in principle in August 2025; EU implementing rules in force since 1 July 2026), product-specific exemptions and higher special tariffs, particularly for steel and aluminum as well as repeated threats of additional tariffs (Die Bundesregierung 2026c); 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 (Eurostat 2026). Planning uncertainty for exports and investments.	Diversification into growth markets (e.g. India, ASEAN) and use of EU free trade agreements; local value creation in the United States to reduce trade policy risks, where economically and strategically sensible; strengthening of the EU single market.

Table 2: Conflict systems in an economic stress test: risks and opportunities for companies. Own presentation.

4.2 Case Study Ukraine: Economic Resilience under Wartime Conditions

With the start of the large-scale Russian invasion in February 2022, Ukraine faced massive attacks on critical infrastructure, considerable economic upheaval and far-reaching population movements. As early as autumn 2022, substantial parts of the energy infrastructure had been damaged; over 2022/23, around half of the power generation capacity was occupied, destroyed or damaged (IEA 2024). At the end of 2025, around 3.7 million people were displaced within Ukraine, while around 5.9 million refugees were abroad (IOM 2026; UNHCR 2026). These population movements considerably impaired the availability of labor and economic performance. The immediate consequence of the war was a decline in real gross domestic product of 28.8% in 2022 (Staatlicher Statistikdienst der Ukraine 2026)

Remarkable is the adaptability and resilience that parts of the Ukrainian economy developed despite ongoing hostilities: as early as 2023, the country recorded economic growth of around 5.5% (Staatlicher Statistikdienst der Ukraine 2026), albeit from a sharply reduced level of output. Contributing factors to economic stabilization included international financial aid, government support measures and the state-supported relocation of companies to safer parts of the country. Different adaptation mechanisms were evident in particular in the IT sector (remote work, relocation of services), agriculture (adjustment of sales and transport routes), the defense industry (expansion of domestic

production capacities), construction (repair and restoration of damaged infrastructure) and the energy sector (decentralized generation and restoration of critical supply capacities).

Indicator	Value
Decline in real GDP 2022	-28.8%
Power generation capacity 2022/23: occupied, destroyed or damaged	approx. 50%
Internally displaced persons / refugees abroad	3.7 million / 5.9 million
Economic growth 2023 (real GDP, compared with 2022)	≈ +5.5%

Table 3: Key figures of the Ukraine case study. Sources: see text.

Four strategic insights for companies:

1. Institutional and operational flexibility enables critical business processes to be adapted even under extreme disruption.

2. Digital capabilities and decentralized operating models can support the continuity of essential business functions.

3. Safeguarding critical value chains, key technologies and supply structures reduces systemic vulnerabilities.

4. Clear responsibilities, short decision-making paths and close cooperation between government and business strengthen responsiveness and adaptability.

4.3 International Comparison: Strategic Differences and Structural Gaps

Strategic dimension	Reference countries and findings
Decision-making speed	Denmark/Estonia: advanced digitalization of public administration and data-based administrative processes. USA: targeted industrial policy investment incentives through the CHIPS and Science Act. Germany faces the challenge of accelerating approval procedures and making administrative processes more efficient.
Strategic investment capacity	The United States and China deploy extensive state funding and industrial policy instruments in AI, semiconductors, energy and electromobility. Germany faces the challenge of consistently implementing existing industrial policy priorities, mobilizing investment and strengthening strategic key technologies in a targeted manner.
Innovation & digitalization	USA (Silicon Valley/venture capital), China (scaling of digital business models), Estonia (digital public administration), Israel (deep tech). Germany has a strong research and industrial landscape, but faces structural challenges, particularly in scaling young technology companies and in the availability of growth capital.
Skilled labor & labor market	Canada/Australia (points-based immigration), Singapore (targeted recruitment of international skilled workers). Germany faces the task of making the recruitment of skilled workers, recognition procedures and international mobility more efficient.
Resilience and efficiency	Switzerland/Norway/Finland (crisis preparedness), Japan/South Korea (strategic stockpiling and security of supply), USA (reshoring of critical capacities). Germany faces the challenge of systematically assessing and selectively reducing strategic dependencies in energy, critical raw materials, semiconductors and selected international supply chains.

Table 4: International comparison of strategic differences and selected structural challenges. Own presentation.

The strategic objective: an innovative, technologically powerful and resilient economy that uses digital technologies and AI productively, has reliable access to investment and growth capital and limits critical external dependencies in a targeted manner without giving up the advantages of the international division of labor.

Europe as a success factor: As an individual state, Germany is a significant economic and political actor whose strategic room for maneuver is considerably expanded by a strong and capable European Union. As the largest economy in the EU, Germany has a

special role to play in further developing the economic strength of the European single market, technological innovative capacity and joint strategic capability.

For companies, a high-performing European economic area opens up additional opportunities for scaling, diversification, technological cooperation and safeguarding against strategic dependencies. Joint European capability is thus becoming a key factor for competitiveness and corporate resilience.

4.4 The Systemic Resilience Gap: Ambition Meets Reality

Germany pursues the goal of systematically strengthening the resilience of government, business and society - among other things through the National Security Strategy (Nationale Sicherheitsstrategie), the National Security Council (Nationaler Sicherheitsrat) and the Operational Plan for Germany (Operationsplan Deutschland, OPLAN DEU) (Die Bundesregierung 2023; Die Bundesregierung 2025; Bundeswehr 2023). The ambition is clearly formulated: resilience is to be understood as a task for the state as a whole and for society as a whole, and implemented in close cooperation with business.

For the business community, however, there is so far no comprehensive, publicly accessible overall picture of the specific requirements and support services in a state of tension or defense (Spannungs- und Verteidigungsfall). As a military planning document, OPLAN DEU is classified; at the same time, information services, cooperation structures and contractual agreements with selected companies already exist. For the broad business community, the challenge therefore remains to identify their potential role and the resulting operational requirements early and with sufficient specificity (cf. Bundeswehr 2024).

Between this ambition and comprehensive operational implementation, structural challenges remain. Although important strategic and institutional foundations have been laid, their cross-departmental, federal and business-related operationalization remains a key task.

From the ThinkTank's perspective, nine potential structural gaps or fields of action can be distinguished in the current system (own analysis by the ThinkTank based on BBK 2024;

Bundeswehr 2024; BSI 2026b), which can be assigned to three overarching problem dimensions:

Problem dimension	Associated gaps
Steering and integration	Coordination gap · Platform gap · Total defense gap · Operationalization gap at the strategic level
Speed and implementation	Speed gap · Implementation gap
Sovereignty, capabilities and regulatory coherence	Digital sovereignty gap · Regulatory gap · Awareness gap

Table 5: Systematization of potential resilience gaps by three problem dimensions. Own analysis by the ThinkTank.

The systemic effect is decisive:

a lack of coordination can reduce the speed of response, delayed decisions can exacerbate implementation problems, dependencies make independent action more difficult, and fragmented regulation increases the complexity of preparedness and crisis management. The resilience gap should therefore not be understood merely as the sum of individual deficits. Its particular significance arises from interactions, mutual reinforcement and possible cascading effects between the various fields of action.

4.5 What This Means for Companies

- Limited predictability of government support in a crisis - decision-making paths, responsibilities and priorities are not always recognizable to companies early and consistently. The scope and timing of government support can therefore not be taken for granted.
- Structural time disadvantage compared with threat actors: the slower response speed of institutional systems shifts the room for maneuver in favor of faster, more adaptive actors.
- Implicit shift of responsibility for resilience to the companies themselves - in practice, this means building their own situational awareness and early warning systems, independently safeguarding critical processes, and establishing in-house resilience structures independent of government control.

Implication: Companies are becoming key actors in overall economic resilience. Their ability to maintain critical services even under exceptional stress contributes directly to the stability of their own value chains and of economic supply structures.

The core of every corporate resilience strategy is therefore a defined minimum value creation: companies should determine which minimum value-creating activities they must at least be able to perform even in a severe crisis in order to retain customers and secure liquidity, and which employees, intermediate products, systems and sites are indispensable for this. In standards terminology, the Minimum Business Continuity Objective (MBCO) according to ISO 22300 and ISO 22301 describes the minimum level of products and services acceptable during a disruption; the concept of minimum value creation used here builds on this but is not identical to it. A strategic resilience perspective complements this approach in particular by taking into account longer-term geopolitical crises, systemic dependencies and strategic corporate objectives (ISO 2019; ISO 2025; BSI 2023). Guidance on initial implementation can be found in Operational Guide 01, Module 3, Chapter 4.

The complete overview of the relevant security planning foundations and regulatory requirements (OPLAN DEU, NIS-2, DORA, Cyber Resilience Act and German Critical Infrastructure Protection Umbrella Act [KRITIS-Dachgesetz]) and a self-diagnosis checklist covering all nine gaps can be found in Operational Guide 01, Module 7, Chapter 8.

5 Economic Protection Initiative (Initiative Wirtschaftsschutz): The State as a Partner with Added Value?

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 2026). It positions the state as a partner and supporter, not as a substitute for corporate self-responsibility: companies remain responsible for their own security but receive targeted support through situational information, prevention, advice and better access to security authorities.

Business particularly welcomes the fact that there is now a cross-departmental political lead for economic protection. However, the central mismatch remains the fragmentation of government services: it often remains unclear to companies which authority is responsible in which situation and what response can realistically be expected. The number of centers, platforms and dialogue formats is growing faster than their connectivity with the business community.

For corporate management, this means that economic protection must be understood more strongly as a strategic success factor - not only as a protective function, but as a prerequisite for resilience, competitiveness and the ability to act. Objectives such as growth, innovation, international business and security of supply can be pursued more sustainably if risks from espionage, sabotage, cyberattacks, geopolitical tensions and hybrid threats are identified early and managed effectively. Closer cooperation with government agencies offers the opportunity to integrate situational awareness, prevention and crisis response more specifically into corporate strategy.

The National Economic Protection Strategy (Nationale Wirtschaftsschutzstrategie) also sets the objective of further developing the services offered by the security authorities and aligning them more closely with the needs of companies. For business, this results in the task of clearly defining, prioritizing and jointly presenting its own support needs.

Security associations play an important interface role here: they can consolidate requirements from corporate practice, articulate them to government agencies and thus help to make advisory, information and support services more tailored, practical and effective.

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 - from prevention and early detection to managing specific security situations.

The complete list of business requirements for the state (e.g. clear responsibilities, a central point of access, legally secure information exchange, practical security clearances) can be found in Operational Guide 01, Module 6, Chapter 7, supplemented by guidance on what companies should prepare internally.

6 Geopolitical Scenarios 2027-2030

Scenarios are not forecasts. They are thinking tools - structured descriptions of possible futures that help to make strategic decisions under uncertainty. The four scenarios below are not weighted by probability of occurrence; how each scenario develops depends on political decisions, technological developments and geopolitical shocks that cannot be foreseen today.

The strategic value lies not in predicting the future but in the question: Is our business model viable under all four scenarios? If not - what needs to change?

Scenario	Key message for companies
1. Large-scale conflict in Europe	Hybrid warfare, NATO fragmentation and a possible Baltic crisis affect critical infrastructure, supply chains, cybersecurity and employees - including companies that are not themselves a party to the conflict.
2. Escalation in the Taiwan Strait	A geo-economic system shock: Taiwan accounts for approx. 44% of global foundry capacity, approx. two thirds of the capacity for advanced processes (feature size of 16 nanometers (nm) and smaller; TrendForce 2024) and over 90% of the capacity for the most advanced chips below 10 nm (data as of 2019; SIA/BCG 2021). Even gray-zone measures affect financial markets, insurance premiums and shipping costs.
3. US-China technological decoupling	“Dual compliance” becomes a permanent condition. Export controls, investment screening and listing regimes are evolving into permanent instruments of strategic power projection - the logic of efficiency is complemented by the logic of security and sovereignty.
4. Fragmentation of the transatlantic partnership	Regulatory divergence instead of open confrontation: European companies increasingly need regionalized technology, data and governance structures.

Table 6: Overview of geopolitical scenarios 2027-2030. Own presentation.

The complete escalation levels, early indicators and impact analyses for all four scenarios - as a basis for stress-testing your own business model - can be found in Operational Guide 01, Module 5, Chapter 6.

The scenarios are described individually, but are not mutually exclusive: they can occur simultaneously or in combination and reinforce each other. Actors can also deliberately exploit a crisis in another region for their own purposes; according to NATO, China is a decisive enabler of Russia's war against Ukraine, in particular through its support for the Russian defense industry (NATO 2024).

The year 2026 demonstrates the economic relevance of parallel conflicts: The ongoing war in Ukraine and the war of the United States and Israel against Iran, together with the considerable restrictions on shipping through the Strait of Hormuz, are putting pressure on energy prices, logistics and economic predictability at the same time. A stress test should therefore also consider combined escalation paths from at least two scenarios (Operational Guide 01, Module 5, Chapter 6, Section 6.5).

7 Business-Relevant Implications and Opportunity Areas

Today's geopolitical upheavals are not temporary disruptions that can be bridged through operational adjustments. The changes are far more than short-term market and supply chain disruptions. They place new demands on strategic leadership - with direct implications for strategy, organizational structures, capital allocation and partnership models. Executive boards and management teams face the task of regularly reviewing business models, market positioning and investment priorities under changed geopolitical conditions: Which products and markets remain sustainable, taking into account technological shifts including AI-driven developments and technological dependencies, political conditions and the availability of resources in the long term?

7.1 Potentially Strategically Viable Markets

EU single market: a central anchor with a largely harmonized legal framework, industrial depth and an industrial policy increasingly geared toward strategic autonomy and technological competitiveness.

India: the world's most populous country since 2023 (UN DESA 2024), with a growing domestic market and positioning as a strategically autonomous actor between Western and emerging power centers. Tensions with Pakistan can increase regional security, investment and supply chain risks.

Southeast Asia (ASEAN): benefits from nearshoring effects, young populations and dynamic middle classes (FDI inflows in 2024 of approx. USD 226 billion, driven among other things by the restructuring of international supply chains; ASEAN-Sekretariat/UNCTAD 2025).

Gulf region: transformation from a resource-based to a knowledge-based economy with considerable capital deployment (IMF 2025); since 2026, however, with significantly increased security and supply risks due to the Iran war, attacks on energy infrastructure in the Gulf and the massive impairment of shipping through the Strait of Hormuz (Euronews 2026a).

Brazil and Mercosur: the interim trade agreement between the EU and Mercosur (Argentina, Brazil, Paraguay, Uruguay) has been provisionally applied since 1 May 2026 and is gradually reducing tariffs (Die Bundesregierung 2026d); the region combines raw material, agricultural and energy potential with significant industrial and sales markets. While the interim trade agreement is already being provisionally applied, the full conclusion of the more comprehensive partnership agreement is still pending (review by the Court of Justice of the EU, pending approval by the European Parliament).

7.2 Nine Critical Dependencies

Energy · Supply chains · Digitalization · Semiconductors & key components · Security (IT, political stability, compliance) · Cloud and data center infrastructure · Cyber technologies · Physical security · Satellite, navigation and timing services. An in-depth analysis of each field including guiding questions on your own dependency situation can be found in Operational Guide 01, Module 4, Chapter 5.

Example (illustrative): A medium-sized manufacturer controls its production via software that runs in the cloud of a non-European provider, sources printed circuit boards from only one region in East Asia and relies on GNSS positioning and time stamps for its logistics. It is therefore vulnerable in three fields at once (cloud, electronic components, satellite services); if one of them fails, in the worst case the entire value creation comes to a standstill. Dependency mapping makes such couplings visible before, in an emergency, they lead to operational disruptions.

The guiding principle for resilient business models is: sovereignty, capability to act, strategic robustness.

7.3 Four Opportunity Areas with Future Potential

Opportunity area	Core of the opportunity
Defense & dual-use	Growing demand for national and collective security is driving investment in software, sensors, robotics, cybersecurity and resilient energy supply - including for medium-sized technology companies.
Infrastructure & energy	Grids, storage, hydrogen and resilience engineering form an investment spectrum spanning decades for integrated solution providers.
Digital sovereignty	Political and regulatory pressure is creating a growth market for secure cloud/edge architectures, cybersecurity and trustworthy AI “made in Europe”; AI itself is becoming a growth area, for example for sovereign AI infrastructure and AI-supported security services.
Regional value creation	Customers increasingly pay not only for the product but for delivery capability, security standards, regulatory compliance and resistance to disruption.

Table 7: Four opportunity areas with future potential. Own presentation.

These opportunity areas are not speculative visions of the future but are already backed today by political investment programs, regulatory decisions and changing demand patterns: for example, the special fund for infrastructure and climate neutrality

(Sondervermögen Infrastruktur und Klimaneutralität) with up to EUR 500 billion for additional investments, which are to be approved in the period 2025-2036 and serve, among other things, the goal of climate neutrality by 2045 (SVIKG 2025), the NATO commitment of 5% of GDP by 2035, divided into at least 3.5% for core defense spending and up to 1.5% for other defense- and security-related investments, for example in critical infrastructure, network security, civil preparedness and innovation (NATO 2025), the EU instrument SAFE with loans of up to EUR 150 billion for joint defense procurement (Rat der Europäischen Union 2025) and the European Chips Act (Europäische Union 2023). Companies that act now secure structural advantages.

8 Conclusion: Key Messages for Corporate Management

From situational picture to decision - the guiding question is: Which decisions must companies make today, in the coming six months and in the long term to remain resilient, competitive and adaptable? The following seven key messages summarize what matters now from the strategic perspective of corporate management.

1. Geopolitics is no longer a peripheral issue but a central strategic leadership task - with a direct impact on markets, supply chains, capital, talent, innovation, raw materials and energy, and locations.

2. Germany's resilience gap is real and measurable - in decision-making speed, digitalization, energy independence and strategic focus.

3. The state is building support structures (National Economic Protection Strategy (Nationale Wirtschaftsschutzstrategie), OPLAN DEU), but their operational implementation is still incomplete - companies should not rely on consistently dependable government steering in a crisis.

4. Companies are becoming key actors in overall economic resilience - with the consequence that they need to build their own situational awareness, early warning systems and resilience structures.

5. Four geopolitical scenarios 2027-2030 (conflict in Europe, Taiwan escalation, US-China decoupling, transatlantic fragmentation) should serve as a stress test for the company's own business model.

6. Nine critical dependencies - energy, supply chains, digitalization, semiconductors, security, cloud and data centers, cyber, physical security, satellite services - determine the actual vulnerability and should be mapped systematically.

7. Geopolitical change opens up a wide range of opportunities: defense & dual-use, infrastructure & energy, digital sovereignty including AI applications for European industry, in particular mechanical engineering, and regional value creation are the strategic opportunity areas of the coming years.

The aim is not to predict future developments precisely but to provide a robust, company-specific frame of reference for strategic decisions in an increasingly volatile geopolitical environment.

9 Further Reading: Operational Guide 01

The accompanying “Operational Guide 01” translates the strategic findings and implications for action summarized in this document into concrete working tools for operational practice: function-specific catalogs of measures including the protection of employees and exposed executives and the risks posed by AI, possible risk multipliers, a maturity check for the resilience architecture with a three-level assessment scale, guidance on the use of AI and illustrative first steps for implementation, dependency mapping in nine fields, the scenario stress test 2027-2030 with worksheet and combination check, the checklist of requirements for the state and the regulatory roadmap (OPLAN DEU, NIS-2, DORA, Cyber Resilience Act, German Critical Infrastructure Protection Umbrella Act [KRITIS-Dachgesetz]), market entry criteria and opportunity areas in detail. The modules of the guide follow a working logic (understanding impacts, analyzing risks, building capabilities, mapping dependencies, testing scenarios, using interfaces with government and regulation, tapping individual opportunities) and therefore do not follow the chapter sequence of this white paper.

Contacts and Networks

Institution	Responsibility
VSW Bundesverband	Network of responsibility for economic protection; Vision 2029 as the leading authority for economic protection - point of contact, source of ideas and platform for knowledge transfer, further education and cooperation.
ThinkTank Corporate Resilience	Think tank for strategic trends, geopolitical analyses and future scenarios; contact via the feedback form (see foreword).
Advisory Board MBA Strategy, Global Risk & Security Management (THI)	Academic link to Technische Hochschule Ingolstadt; program advice and research cooperation.

References

This list contains the sources of the Strategic White Paper and of Operational Guide 01.

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 (2024): Verfassungsschutzbericht 2024. [Annual Report on the Protection of the Constitution 2024]. Published on 10 June 2025. Available at: https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/verfassungsschutzberichte/2025-06-10-verfassungsschutzbericht-2024.pdf?__blob=publicationFile&v=4 (accessed 17 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).

BfV - Bundesamt für Verfassungsschutz (2026): Cyberangriffe - Gefahren, Risiken und Schutz vor staatlich gesteuerten Attacken. [Cyberattacks - Dangers, Risks and Protection against State-Controlled Attacks]. February 2026. Available at: https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/cyberabwehr/2026-02-cyberangriffe.html (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).

BSI - Bundesamt für Sicherheit in der Informationstechnik (2026c): PHP: Kritische Schwachstellen bedrohen Webanwendungen weltweit. [PHP: Critical Vulnerabilities Threaten Web Applications Worldwide]. Cyber security warning BITS-H 2026-297981-1032, Version 1.0, 21 October 2026. Available at: https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Cybersicherheitswarnungen/DE/2026/2026-297981-1032.pdf?__blob=publicationFile&v=2 (accessed 23 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).

Destatis - Statistisches Bundesamt (2026): China im Jahr 2025 wieder wichtigster Handelspartner Deutschlands. [China Again Germany's Most Important Trading Partner in 2025]. Press release No. 056 vom 20 February 2026. Available at: https://www.destatis.de/DE/Presse/Pressemitteilungen/2026/02/PD26_056_51.html (accessed 29 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).

Eigner, Leo (2025): Chinas Vision für Wissenschaft und Technologie. [China's Vision for Science and Technology]. CSS Analysen zur Sicherheitspolitik, No. 364, July 2025. Zürich: Center for Security Studies, ETH Zürich. Available at: https://ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse364-DE.pdf (accessed 17 June 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 (2023a): Commission Recommendation on critical technology areas for the EU's economic security for further risk assessment with Member States. C(2023) 6689 final. Available at: https://defence-industry-space.ec.europa.eu/system/files/2023-10/C_2023_6689_1_EN_ACT_part1_v8.pdf (accessed 17 June 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 (2025): Cloud Sovereignty Framework. Version 1.2.1, October 2025. Available at: https://commission.europa.eu/document/download/09579818-64a6-4dd5-9577-446ab6219113_en?filename=Cloud-Sovereignty-Framework.pdf (accessed 17 June 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 Kommission; Hoher Vertreter der Union für Außen- und Sicherheitspolitik (2025): Joint White Paper for European Defence Readiness 2030. JOIN(2025) 120 final, 19 March 2025. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025JC0120 (accessed 5 November 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 (2023): Regulation (EU) 2023/1781 of the European Parliament and of the Council of 13 September 2023 establishing a framework of measures for strengthening Europe’s semiconductor ecosystem (Chips Act). Available at: https://eur-lex.europa.eu/eli/reg/2023/1781/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).

IEA - International Energy Agency (2024): Ukraine's Energy Security and the Coming Winter. Paris: IEA. Available at: https://www.iea.org/reports/ukraines-energy-security-and-the-coming-winter (accessed 30 September 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).

IOM - International Organization for Migration (2026): Ukraine Internal Displacement Report. General Population Survey, Round 22, January 2026 (data as of December 2025: 3,712,000 internally displaced persons). IOM Displacement Tracking Matrix. Available at: https://dtm.iom.int/reports/ukraine-internal-displacement-report-general-population-survey-round-22-january-2026 (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).

JRC - Joint Research Centre (2025): Open but Not Powerless: Towards a Common Understanding of EU Digital Sovereignty. Science for Policy Brief. Available at: https://publications.jrc.ec.europa.eu/repository/bitstream/JRC144908/JRC144908_01.pdf (accessed 17 June 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).

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

Merz, Friedrich (2026): Speech by Federal Chancellor Friedrich Merz at the Munich Security Conference on 13 February 2026. Available at: https://www.bundesregierung.de/breg-en/federal-government/speech-munich-security-conference-2407298 (accessed 23 October 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).

Münchner Sicherheitskonferenz (2026): Munich Security Report 2026: Under Destruction. Munich, February 2026. Available at: https://securityconference.org/en/publications/munich-security-report (accessed 23 October 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).

NATO (2025): The Hague Summit Declaration. Declaration of the Heads of State and Government, The Hague, 25 June 2025. Available at: https://www.nato.int/cps/en/natohq/official_texts_236705.htm (accessed 30 September 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).

ODNI/NCSC - Office of the Director of National Intelligence, National Counterintelligence and Security Center (2025): Safeguarding Western Tech Startups: Exploitation of International Pitch Competitions. 4 September 2025. Available at: https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/NCSC_SOF_2025-09-04_SafeguardingWesternTechStartups.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).

Rat der Europäischen Union (2022): A Strategic Compass for Security and Defence. Adopted on 21 March 2022, press release. Available at: https://www.consilium.europa.eu/en/press/press-releases/2022/03/21/a-strategic-compass-for-a-stronger-eu-security-and-defence-in-the-next-decade/ (accessed 26 October 2026).

Rat der Europäischen Union (2025): Security Action for Europe (SAFE) instrument. In force since 29 May 2025. Available at: https://www.consilium.europa.eu/de/policies/safe/ (accessed 30 September 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).

Staatlicher Statistikdienst der Ukraine (2026): Gross domestic product of Ukraine, annual figures 2022 and 2023 after regular revision (real GDP 2022: -28.8%; 2023: +5.5%). Kyiv: Derzhstat. Preliminary figure 2023 (+5.3%): press release „The preliminary estimate of the GDP for 2023 was made“, 28 March 2024, available at: https://stat.gov.ua/en/news/preliminary-estimate-gdp-2023-was-made; revision to +5.5% (2025) reported, among others, by Kyiv Post: https://www.kyivpost.com/post/50412 (accessed 4 November 2026).

SVIKG (2025): Gesetz zur Errichtung eines Sondervermögens Infrastruktur und Klimaneutralität of 30 September 2025 (BGBl. 2025 I No. 230) [Act establishing a Special Fund for Infrastructure and Climate Neutrality]. Available at: https://www.gesetze-im-internet.de/svikg/BJNR0E60A0025.html (accessed 30 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).

U.S. Department of State (2025): Report to Congress on U.S.-Origin Technology that the Chinese Communist Party (CCP) is Using in the Military-Civil Fusion (MCF) Strategy of the PRC. 27 August 2025. Available at: https://www.state.gov/wp-content/uploads/2025/08/Report-U.S.-Technology-in-the-Military-Civil-Fusion-Strategy-Revision-Accessible-8.27.2025.pdf (accessed 17 June 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).

UNHCR (2026): Ukraine Refugee Situation. Operational Data Portal (dynamic); data as of end of December 2025: approx. 5.9 million refugees from Ukraine recorded globally. Available at: https://data.unhcr.org/en/situations/ukraine (accessed 4 November 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).

World Bank; Government of Ukraine; European Union; United Nations (2026): Ukraine - Fifth Rapid Damage and Needs Assessment (RDNA5): February 2022 - December 2025. Report, 23 February 2026; data as of 31 December 2025 (recovery and reconstruction needs of USD 587.7 billion for 2026-2035). Available at: https://documents1.worldbank.org/curated/en/099022026094036395/pdf/P514499-22f93f3a-4278-42bc-b907-db9553d12069.pdf; accompanying press release: https://www.worldbank.org/en/news/press-release/2026/02/23/updated-ukraine-recovery-and-reconstruction-needs-assessment-released (accessed 4 November 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).

Wübbeke, Jost; Meissner, Mirjam; Zenglein, Max J.; Ives, Jaqueline; Conrad, Björn (2016): Made in China 2025: The making of a high-tech superpower and consequences for industrial countries. MERICS Papers on China No. 2, December 2016. Berlin: Mercator Institute for China Studies. Available at: https://merics.org/en/report/made-china-2025 (accessed 17 June 2026).

Zenglein, Max J.; Holzmann, Anna (2019): Evolving Made in China 2025: China's industrial policy in the quest for global tech leadership. MERICS Papers on China No. 8, July 2019. Berlin: Mercator Institute for China Studies. Available at: https://merics.org/sites/default/files/2020-04/MPOC_8_MadeinChina_2025_final_3.pdf (accessed 26 October 2026).

List of Abbreviations

ASEAN	Association of Southeast Asian Nations
BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (Federal Office of Civil Protection and Disaster Assistance)
BfV	Bundesamt für Verfassungsschutz (Federal Office for the Protection of the Constitution)
BMI	Bundesministerium des Innern (Federal Ministry of the Interior)
BRICS	Group of states Brazil, Russia, India, China, South Africa (expanded)
BSI	Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security)
DORA	Digital Operational Resilience Act (Regulation (EU) 2022/2554)
ESG	Environmental, Social, Governance
EU	European Union
FDI	Foreign Direct Investment
GNSS	Global Navigation Satellite System
IEA	International Energy Agency
IMF	International Monetary Fund
IOM	International Organization for Migration
IP	Intellectual Property
IT	Information technology
JRC	Joint Research Centre of the European Commission
AI	Artificial Intelligence
SMEs	Small and medium-sized enterprises
CCP	Chinese Communist Party
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)
ODNI	Office of the Director of National Intelligence
OECD	Organisation for Economic Co-operation and Development
OPLAN DEU	Operationsplan Deutschland (Operational Plan for Germany)
SAFE	Security Action for Europe (EU instrument for defense procurement)
SVIKG	Act establishing a Special Fund for Infrastructure and Climate Neutrality (Gesetz zur Errichtung eines Sondervermögens Infrastruktur und Klimaneutralität)
THI	Technische Hochschule Ingolstadt
UNHCR	United Nations High Commissioner for Refugees
VC	Venture Capital
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**

White Paper 02 - ThinkTank Corporate Resilience, November 2026