THINK TANK CORPORATE RESILIENCE

WHITE PAPER

Economic consequences of hybrid threats for companies and their value chains – How should the economy prepare now?

- Hybrid warfare as a strategic challenge for the German economy -

VSW Bundesverband

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

December 2025

Foreword

Security as an economic framework condition

Hybrid threats are increasingly shaping everyday business life. Cyberattacks, sabotage, disinformation, and geopolitical trade barriers have a direct impact on business models, value chains, and strategic decisions. Security is therefore no longer a marginal factor, but a key economic prerequisite.

Vulnerability of networked economies

As export-oriented, highly networked economic areas, Germany and Europe are particularly vulnerable to disruptions. Geopolitical escalations, systemic competition, and a fragmented global economy have permanently changed the predictability of markets. Attacks on critical infrastructure and economically relevant espionage are on the rise.

From wake-up call to strategy

The "Operation Plan Germany" has raised awareness among many companies. However, isolated reactions are not enough. The decisive factor is the strategic classification of security-related risks: What is critical to business – and how can the company remain capable of acting in the long term?

Security as a competitive factor

Hybrid threats cause hundreds of billions of Euros in damage every year and influence investment, innovation, and competitiveness. Nevertheless, security is often still treated as a cost or compliance issue – not as a factor in value creation and corporate value.

Resilience as a management task

This white paper consistently considers security from the perspective of corporate management. Resilience is understood as a strategic task that affects governance, value creation, and decision-making structures in equal measure.

Collaboration creates resilience

Resilience does not arise in isolation. It requires structured exchange between business, government, and security authorities, as well as the dismantling of silos and the building of trust.

The aim of this white paper

The white paper supports decision-makers in systematically anchoring resilience as a competitive and value-adding factor and in strategically managing security.

The ThinkTank Corporate Resilience and the VSW as a platform for responsibility

At this interface, the **ThinkTank Corporate Resilience** positions itself **as a strategic think tank** and **the VSW Bundesverband** as **a network of responsibility**. The aim is to shape security as a joint value-adding task, provide guidance, and strengthen dialogue between companies, politicians, and authorities. In doing so, the **ThinkTank Corporate Resilience** supports the **VSW's Vision 2029** of establishing itself as **the leading authority for economic protection** – a point of contact, source of inspiration, and platform for knowledge transfer, further training, and cooperation.

For the publisher ThinkTank Corporate Resilience

Prof. Dr. Marc Knoppe Johannes Strümpfel

Publisher:

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

The **ThinkTank Corporate Resilience** creates a platform that brings together strategic trends, geopolitical analyses, and future scenarios from the resilience perspective of chief security officers with the business perspective of CEOs, executive boards, supervisory boards, and shareholders. It arose from close cooperation between business and science at the Technische Hochschule Ingolstadt in the field of "Value Creation through Corporate Security" and is closely linked to the MBA program **Strategy, Global Risk & Security Management**.

The think tank was initiated by Sven Dawson, Florian Haacke, Alexander Klotz, Marco Mille, Johannes Strümpfel, and Prof. Dr. Marc Knoppe to offer C-Suite, Chief Security Officers, and authorities a forum for future-oriented thinking and strategic exchange on systemic risks **from an economic 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 Corporate Security, Dr. Ing. h.c. F. Porsche AG)

Alexander Klotz (Head of Corporate Security, BMW AG)

Marco Mille (Head of Corporate Security, Siemens AG)

Johannes Strümpfel (Siemens AG; President of VSW Bundesverband)

Strategic Foresight Lab

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

in cooperation with the

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

Your opinion is important to us!

FAQ & Feedback on the White Paper

The challenges of hybrid warfare affect us all:
the economy, science, and society. In order to develop viable solutions together, we would like to include your perspective.

Do you have any questions or suggestions?

Please use our feedback questionnaire or contact our think tank 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 common questions and learn more about the topic.

👉**Contact & Feedback**

Table of Contents

Executive Summary

This white paper analyzes the **economic dimension of hybrid threats** and their impact on the stability of companies, global value chains, and critical infrastructures. It highlights the business, organizational, and corporate strategy challenges resulting from this hybrid warfare. The Operation Plan Germany (OPLAN DEU) is part of the Framework Guidelines for Total Defense (RRGV) (BMI 2024) and defines the regulatory requirements in the context of civil and military defense. OPLAN DEU focuses on three of the seven pillars of total defense[1] and represents the link between civil and military defense (BMI 2024).

Hybrid threats (Bundestag 2025a, 2025b, 2024a, 2024b, NATO 2025b, Sperling 2025) – an orchestrated combination of military, non-military, and economic instruments – have become a **key risk factor for the resilience and value creation** of European companies. They include in particular:

- Cyberattacks (e.g. ransomware, industrial espionage, attacks on ERP and production systems)
- Physical disruptions (e.g. sabotage of energy and logistics networks, drone activities, arson and power attacks),
- Espionage (e.g. spying attempts, insider threats, drone overflights),
- Disinformation and economic influence to destabilize markets, employees, and society.

These hybrid operations aim to erode trust, stability, and security of supply. The **economic damage** caused by cyberattacks, economic and industrial espionage, and sabotage is estimated at **over €289 billion annually** in Germany alone (Bitkom 2025).

This presents companies with a new responsibility: they must identify, assess, and secure their dependencies, vulnerabilities, and critical interfaces with government infrastructure. OPLAN DEU defines concrete expectations for the economy for the first time—from securing critical processes and providing logistical and support to ensuring cyber and communications security in times of tension and defense.

Key areas of action for the economy

- **Strengthening cyber and supply chain resilience**
  Diversify energy, raw material, and logistics relationships to reduce geopolitical

[1] 3 pillars of OPLAN DEU: Civil defense: 1. Support for the armed forces; Military defense: 2. Homeland security/national territorial defense, 3. Operational base/hub Germany

dependencies; establish redundant IT and communications systems; conduct regular vulnerability analyses and stress tests.

- **Anchoring hybrid threats in risk management**
  Systematically integrate hybrid scenarios into risk and business continuity management (BCM); model indirect dependencies (e.g. cloud service providers, KRITIS operators).

- **Cooperation and civil-military cooperation (ZMZ)**
  Institutionalization of joint early warning systems, situation reports, and crisis mechanisms between industry, the armed forces, authorities, and industry associations; active preparation for support requests in accordance with OPLAN DEU.

- **Adapt governance and compliance structures**
  Alignment with EU and NATO frameworks (NIS2, Cyber Resilience Act, Strategic Compass, Military Mobility); establishment of a company-wide resilience governance framework.

Economic responsibility in overall defense

Today, the resilience of the economy is not only a core business management task, but also a core security policy task. Companies play an active role in the overall national security architecture by maintaining critical services, infrastructure, and expertise even in crisis conditions.

This white paper provides suggestions on how company management can prepare their organizations for the escalation stages of "hybrid warfare, consent, tension, defense, and alliance," how they can ensure operational continuity and legal compliance, and how **resilience** can be established **as a strategic competitive advantage**.

Only through targeted investments in resilience, cooperation, and prevention can the German and European economies remain capable of acting even under the conditions of hybrid threats. **Resilience is therefore not a cost factor, but a key driver of value creation in an age of systemic uncertainty.**

1 Operation Plan Germany in the context of the economy

1.1 OPLAN DEU: The Bundeswehr operational plan for national and alliance defense.

OPLAN DEU, which is not publicly available and is classified as confidential, is a central military element for national and alliance defense. It defines the operational integration between the military forces of the Bundeswehr and the civilian support structures of the state and the economy (BMI 2024).

Germany plays a pivotal role within Europe in this regard: in the event of defense or alliance, up to 800,000 allied soldiers and around 200,000 vehicles must be deployed, supplied, and protected on German territory within six months. This requires close cooperation between state institutions, the Bundeswehr, industry, and civil society—especially in the areas of transport, energy, logistics, maintenance, communications, medical care, and law.

OPLAN DEU thus marks a new phase in national defense planning, in which civilian resilience is understood as part of national security.

1.2 Civil-military cooperation (ZMZ): Structures for cooperation between industry, authorities, and the armed forces.

Civil-military cooperation (ZMZ) – known internationally as *Civil-Military Cooperation (CIMIC)* – describes the systematic cooperation between the Bundeswehr, authorities, industry, and civil society (BBK 2025c, BMVg 2023, Green Paper 2025). In peacetime, CIMIC focuses on disaster relief and support for civil infrastructure (e.g. flood relief, technical support). In times of tension, defense, or alliance, however, it serves to support the armed forces in fulfilling their military mission, for example by providing resources, logistics, or personnel.

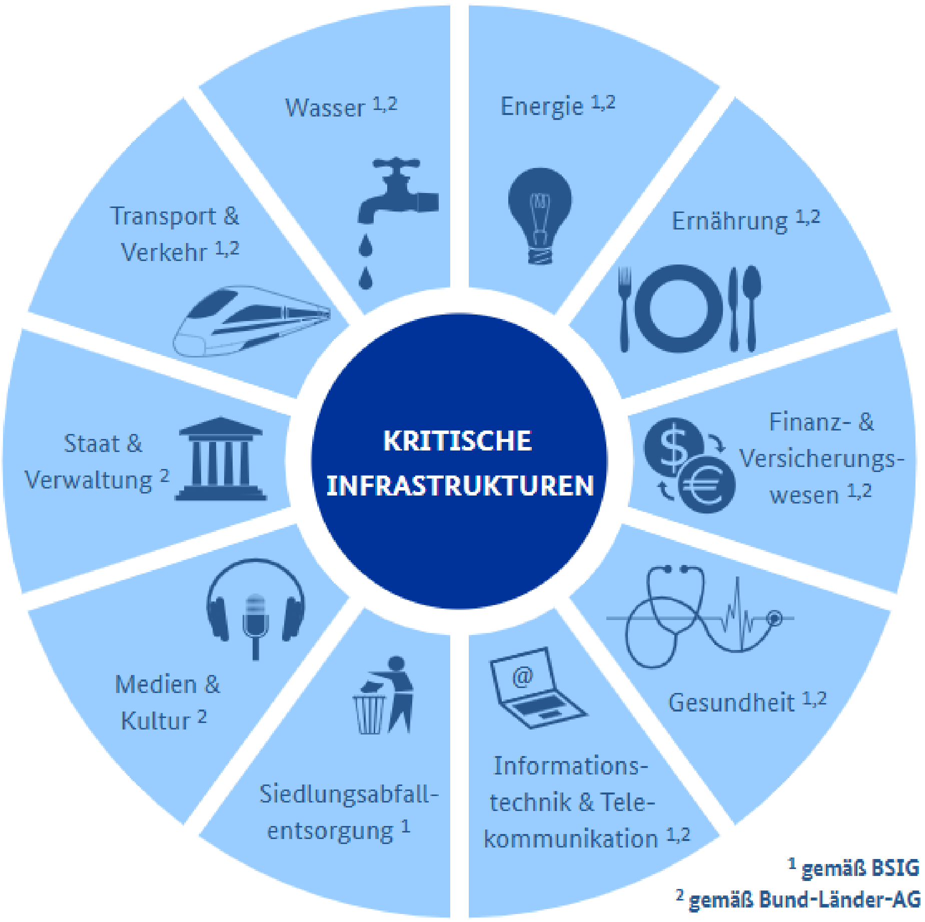
For companies, **this means** that in the event of a crisis, they become partners in the state security architecture – with clearly defined tasks, reporting channels, and priorities.

1.3 KRITIS: Critical service providers and infrastructures of particular importance for supplying the population.

Critical infrastructures (KRITIS) are facilities and companies whose failure or impairment would lead to significant supply bottlenecks, disruptions to public safety, or economic damage (BBK 2025a, 2025b, 2021).
These include, in particular, sectors such as energy, water, food, transport, information technology, health, finance, administration, and media.

KRITIS operators[2] are the focus of hybrid threats and military planning. They are considered the first targets of possible acts of sabotage or cyberattacks, as their paralysis would have an immediate impact on society's and the military's ability to act. Accordingly, their resilience is required by law, including the IT Security Act 2.0, the NIS2 Directive, and the EU Cyber Resilience Act (BMI 2023b, BSI 2024; EU Commission 2025, 2022a, 2022b).

KRITIS is divided into 10 sectors and forms the basis for the state and economy to protect critical infrastructures:



Sectors and industries KRITIS (BBK 2025b)

[2] A company or organization that operates critical infrastructure (KRITIS) and is therefore responsible for supplying the population with essential goods and services (BBK 2025a).

1.4 European dimension

OPLAN DEU is firmly embedded in the European security architecture and complements the strategic initiatives of NATO and the European Union. The key reference frameworks are the EU Strategic Compass, the NIS2 Directive, the Cyber Resilience Act, and the Military Mobility Program (EU Commission 2025, 2022a, 2022b; NATO 2025a, 2024). These instruments make it clear that

- Resilience is becoming the European standard. Security and reporting requirements are being harmonized across the EU.

- Energy and raw material flows will be coordinated supranationally in the event of a crisis.

- Transport corridors can be prioritized for military use or temporarily repurposed.

- Industry is becoming a player in security policy – particularly through dual-use technologies and arms cooperation.

This makes it clear that

In the future, the European economy will be an integral part of an overall defense policy that strategically links security, competitiveness, and sustainability (Bafa 2021, BMI 2024, EU Commission 2025).

1.5 Consent case, tension case, defense case, and alliance case

The following table provides a brief overview of the classification and explanation of consent, tension, defense, and alliance cases.

	Case of consent (Art. 80a GG)	**State of tension (Art. 80a GG)**	**Defense case (Art. 115a GG)**	**Alliance case (NATO Art. 5 / Art. 87a GG)**
Trigger	Simple majority in the Bundestag; activation of individual security powers.	Threat to the Federal Republic of Germany; determination by a majority of the Chancellor.	Military attack on the FRG or German troops abroad; serious terrorist or cyber attack.	Attack on NATO member triggers obligation to provide assistance.
Majority requirement	Simple majority	Chancellor majority	Two-thirds majority Bundestag + approval of the Bundesrat	NATO decision (confirmed nationally)
Legal consequences	Activation of individual security powers.	Full activation of security laws; possible conscription.	Universal conscription; extended executive powers.	Military or civilian support for the attacked state.
Typical occasions	Political crises, international developments.	Impending military conflicts or state/terrorist threats.	Attack on the Federal Republic of Germany or German forces; terrorist or cyber attacks.	Attack on NATO partners by a state or terrorist organization.

1.6 Corporate roles in the context of defense

In times of tension and defense, companies take on an active role within the overall national security architecture.
Their tasks go far beyond crisis management and range from securing supplies to supporting military and civilian structures.
Key roles include:

- **Maintaining** critical processes and services (e.g. energy, production, supply).
- **Provision of** logistical, technical, and personnel capacities for military and civilian purposes.

- **Participation in** cyber defense and communications security, in particular to protect corporate and customer networks**.**

- **Supporting civil society,** for example through supplies, accommodation, or technical assistance.

Conclusion

Companies are becoming **systemically important partners in the national resilience network**—at the interface between business, government, and society. This requires forward-looking planning, clear responsibilities, and regular coordination with authorities, chambers of commerce, and the armed forces. The business community must prepare for this, because the **current situation of hybrid threats** is not only intensifying global competition, but **also jeopardizing German and European competitiveness** – particularly in terms of value chains, supply capabilities, and innovative strength.

For this to succeed, **investment incentives**, government support programs, and clear regulatory frameworks **are needed** that view resilience not as an additional burden, but as **a strategic task for the future and an opportunity for innovation**. At the same time, **in many places**, **politics** is **still too far removed from reality and the constraints on companies**, which delays or hinders necessary decisions. Economic and security policy must therefore be considered together: **resilient corporate structures are now as much a security policy goal as an industrial policy goal**.

It is important to secure the technological leadership and economic strength of Germany and Europe not only from a business perspective, but also in the interests of European security, stability, and independence.

2 Scenarios – Impact on business models

2.1 Hybrid threat situation

The European security architecture is facing a lasting test and is in a transitional phase of security policy characterized by hybrid threats, geopolitical tensions, and an increasing intertwining of civil and military tasks. Due to its economic importance and central location, Germany is considered **a key target for hybrid influence** (EU Commission 2023, Sperling 2025).

Hybrid activities—including disposable agents, espionage attempts, cyberattacks on government and industrial targets, targeted disinformation campaigns, drone flights over critical infrastructure, industrial espionage, and espionage by covert agent networks—are now part of Russia's ongoing strategy to influence Germany and its European partners (Edwards & Seidenstein 2025, NATO 2025b, Sperling 2025).

The goal: to destabilize Western societies and economic structures (BfV 2025a, 2025b), erode social cohesion, weaken political decision-making capacity, and undermine economic stability without crossing the threshold into open conflict.

The Bundeswehr and its partner institutions assume a four-stage system: peace – hybrid warfare – crisis – war (BMVg 2023).
According to the assessment of the federal government and leading intelligence services, Germany is "no longer at peace, but not yet at war," but rather in a state of hybrid threat (Bundeskanzleramt 2023; BfV 2025a, 2025b) – the phase of military-hybrid intensification described above (Bundeskanzleramt 2023; BMVg 2023, Hartmann 2025, Grünbuch ZMZ 4.0 2025).

European nations and NATO are responding to this threat with increased deterrence measures, higher defense spending, military modernization, and expanded joint exercises. Germany is making a significant contribution to this by strengthening its cyber defense, expanding its capabilities to counter hybrid threats, and increasing its defense budget (Sperling 2025). Meanwhile, Russian intelligence services are intensifying their espionage activities to identify critical infrastructure and defense-related facilities and prepare them for potential acts of sabotage (BfV 2025b). This continuous spiral of escalation in the gray zone of hybrid warfare requires European nations, and European companies in particular, to develop new defensive measures (EEAS 2024).

The inherent danger of this "military-hybrid intensification" lies in its risk of initiating a creeping transition to another scenario 2: military escalation, a Russian attack on NATO territory. Persistent strain from hybrid operations can lead to a degradation of collective resilience and a perceived fragmentation of European security alliances (Kather 2024). It could lead to internal disruption within NATO due to the withdrawal of member states such as Slovakia and Hungary, which would create a dangerous security gap in Central Europe. In such a context, current hybrid operations would no longer serve primarily to disrupt, but rather to maximize destruction and **deliberately paralyze critical**

infrastructure in Germany and other NATO countries (Metis 2024, Edwards & Seidenstein 2025).

A transition to scenario 2 would mean an escalation from hybrid warfare to a conventional military confrontation, for example through a coordinated military operation in the Baltic states aimed at capturing the strategically important Suwalki Corridor between Lithuania and Poland. This would pose a direct threat to NATO territory and trigger the "alliance case" (Pöhlmann 2025).

For companies, **this results in** a structural threat to their entire value chains, as hybrid attacks not only cause operational bottlenecks and quality losses, but can also have a lasting impact on strategic assets such as innovation capabilities, market positions, and intellectual property.

2.2 Escalation dynamics and risk progression

The strategy of "military-hybrid intensification" deliberately exploits the "gray zone" between peace and war to overload Western systems.
Observable patterns include:

- Cyber and information operations that specifically target corporate networks and supply chains (BSI 2024).
- Physical acts of sabotage against energy, transport, or communications infrastructure.
- Manipulation of markets and disinformation to influence public opinion and investment decisions.
- Targeted attacks on resilience structures, e.g. security agencies or research centers.

The danger lies in the creeping transition from this hybrid phase to open military escalation, for example through incidents on NATO's eastern flank (SWP 2025, 2024). An attack on NATO territory would trigger Article 5 of the North Atlantic Treaty and immediately involve Germany in overall operational defense (Metis 2024, NATO 2025a, 2024).

2.3 Germany's strategic role

As Europe's largest economy and NATO's logistical hub, Germany bears **central operational responsibility** in the event of an emergency **(**BMI 2024).
This role **has a direct impact on industry** – especially on companies with critical infrastructure, defense-related production, or transnational supply chains.

The following economic effects are to be expected:

- Increased demand for security-related goods (e.g. energy, logistics, communications, IT security).
- Bottlenecks and disruptions in global supply chains due to military prioritization or sanctions.
- Stronger regulation and legal obligations to support government defense tasks.
- Growing threats in cyberspace, including attacks on industrial control systems and cloud infrastructures.
- Reputation and market changes due to social polarization or misinformation.

These **factors directly influence business models**, market strategies, and investment decisions. Companies must actively integrate the interface between business and security policy into their strategic planning.

This comprehensive mobilization and the associated logistical and security policy requirements would have far-reaching consequences for German companies. They would be directly affected by increased demand for certain goods and services, but would also face stricter security requirements, potential supply chain disruptions, and an increase in cyber threats, which is already a daily occurrence (Bundeswehr 2025).

Continued and precise analysis of these transition phases is therefore critical for risk assessment and the development of adequate prevention and response strategies. It is crucial to understand the mechanisms and indicators of this potential escalation.

2.4 Implications for action for companies

The **continued escalation of hybrid threats** requires the **business community to reassess risk and resilience management** in the context of individual value creation.

The following strategic implications are key:

- **Integration of security and resilience strategies** into corporate governance and ESG structures.
- **Establishment of resilient supply chains** with regional redundancies ("dual sourcing," nearshoring).
- **Increasing cyber resilience** through segmentation, emergency drills, and coordination with the BSI, CERT-Bund, and authorities.
- **Establishment of early warning and situation assessment systems** to identify geopolitical and economic risks.
- **Stronger networking with government structures** (ZMZ, IHK, KRITIS cluster) for crisis response.

Companies that implement appropriate governance and security mechanisms at an early stage gain a decisive competitive advantage: **resilience becomes an economic success factor**.

3 Strategic fields of action for companies – critical success factors

3.1 Energy & raw material supply

Relevance

Energy is the central prerequisite for production, logistics, and communication – and thus the backbone of all industrial value creation. In times of tension or defense, government intervention, rationing, prioritization, or acts of sabotage can have a significant impact on a company's ability to operate. Germany remains highly dependent on imported energy sources and critical raw materials; at the same time, energy and raw material flows are considered strategic targets for hybrid influence (BMWK 2024a, 2024b; BNetzA 2025, 2024).

Key risks

- Supply disruptions: Blackouts, cyberattacks, physical sabotage, or failure of substations and pipelines.
- Rationing & government prioritization: Energy sources and fuels are prioritized for armed forces, critical infrastructure sectors, and government agencies.
- Dependence on imports: Vulnerability due to geopolitical or logistical bottlenecks (gas, oil, rare earths, metals).
- Cost and price risks: Volatile markets, increases in transport costs.
- Lack of resilience in self-sufficiency: Insufficient redundancies, lack of emergency power or storage capacities.

Strategic objectives

- Maintaining operational and production capabilities through resilient energy and raw material supplies in crisis and defense situations.
- Reduction of dependencies by establishing alternative, regional, and decentralized energy sources.
- Ensuring the energy supply of critical systems (IT, communication, security, production).
- Early involvement in national supply priorities and allocation mechanisms (BMWE, BNetzA, ZMZ).
- Protecting our own energy infrastructure from physical and cyber attacks.
- Integration of energy resilience into business continuity and crisis management.

Critical measures & governance

- Emergency and resilience planning:
  Development of emergency plans for power outages, including redundancies, priorities, and decision-making processes; regular simulations ("blackout drills").
- Decentralized self-sufficiency:
  Investment in photovoltaic, battery, and biogas capacities; establishment of local storage and diesel reserves to bridge supply bottlenecks.
- Interfaces with authorities:
  Active coordination with grid operators, BNetzA, BMWE, and ZMZ agencies on reporting and prioritization procedures in the event of a crisis.
- Cyber and physical security:
  Hardening of control technology and OT systems; physical security of transformer stations, tank farms, energy centers; 24/7 monitoring.
- Diversification of supply sources:
  Establishment of redundant supply and transport structures for energy and raw materials, including strategic partnerships with European suppliers.
- Energy efficiency and reserves:
  Reduction of energy requirements through efficiency measures; creation of operational "crisis reserves" for prioritized processes.
- Regular stress tests:
  Conducting energy stress tests and crisis exercises with internal and external partners to validate redundancies and decision-making processes.

3.2 Supply chains & logistics

Relevance

Global supply chains form the backbone of industrial production and value creation. However, their complexity and international interdependence make them highly vulnerable—especially in times of tension or defense.

Military prioritization of transport routes, export restrictions, or fuel and personnel shortages can lead to massive disruptions. As Europe's logistics hub, Germany is particularly exposed (BMI 2024, Hartmann 2025).

Key risks

- Disruption of international supply chains due to military prioritization, sanctions, or infrastructure losses.
- Shortages in transport and personnel: loss of truck drivers, rail and port logistics; limited air freight capacities.
- Single-source dependencies: Concentration of critical components on a few suppliers or regions.

- Cyber and sabotage risks along the transport chain (tracking systems, port control systems, OT networks).
- Resource shortages and price shocks due to energy or raw material crises.

Strategic goals

- Maintaining delivery and transport capabilities even in the event of military prioritization or infrastructure failures.
- Reducing dependencies by diversifying suppliers, transport routes, and regions.
- Strengthening transparency and control along the entire supply chain (Tier 1 to Tier n).
- Integration of supply chain risks into company-wide business continuity management (BCM) and crisis management.
- Stockpiling critical materials and products to bridge disruptions.
- Establishment of coordinated processes with authorities, ZMZ structures, and network operators.

Critical measures & governance

- Risk transparency & prioritization:
  Systematic analysis of dependencies (Tier 1 to Tier n); identification of single points of failure; development of a dynamic risk heat map.
- Diversification & regionalization:
  Development of dual sourcing strategies, nearshoring of European supply chains, use of regional hub structures ("hub-and-spoke models").
- Crisis-proof logistics:
  Conclusion of framework agreements with alternative carriers and freight forwarders; planning of redundant transport corridors; definition of military and civilian priorities with authorities.
- Coordination with government & military:
  Early coordination with ZMZ agencies, Bundeswehr LogCom, and BMVg on the use of military-relevant infrastructure and the avoidance of conflicting objectives.
- Security and cyber hardening:
  Securing logistical IT systems (e.g. ERP, tracking, port management); physical protection of critical transshipment points.
- Resilience tests and exercises:
  Conducting regular supply chain stress tests, scenario analyses, and joint exercises with partners and authorities.

3.3 Internal infrastructure

Relevance

Our own sites and facilities are the physical foundation of value creation. They secure production, logistics, research, and communication. In times of tension or defense, industrial sites become both strategic and symbolic targets of hybrid attacks—such as sabotage, drone flights, espionage, or cyber attacks on building control systems. In addition, regional operational plans (OPLAN DEU, national defense concepts) can limit the availability of space, energy, and personnel (BMVg 2023; BMI 2024, 2023b).

Key risks

- Physical sabotage and espionage: drone reconnaissance, manipulation of supply lines or access systems.
- Internal dependencies: Global corporate networks and internal supply structures as a risk in the event of site failure.
- Regional restrictions: Military use or prioritization of transport routes, energy and communications infrastructure.
- Social risks: Influence on employees, social tensions, disinformation in location regions.
- Inadequate protection concepts: Lack of redundancy, security zones, or surveillance systems.

Strategic objectives

- Ensuring the operational capability of critical sites in the event of a crisis or defense situation.
- Building physical and organizational resilience for key sites and employees.
- Reducing internal dependencies through regional redundancies and alternative capacities.
- Early detection and defense against hybrid threats at and around company locations.
- Integrating site resilience into overall governance (security, BCM, facility, HR, IT).

Critical measures & governance

- Site classification:
  Identification and prioritization of critical production, logistics, and management locations according to national, economic, and defense policy relevance (KRITIS definition, DIN SPEC 14027).
- Physical protection measures:
  Reinforcement of access, video, perimeter, and drone protection systems; integration of security monitoring into central control centers.

- Redundancy & contingency planning:
  Establishment of alternative locations or "hot sites" for production, data processing, and crisis management.
- Security and situation drills:
  Regular site drills covering sabotage, failure, evacuation, and emergency operations; involvement of regional authorities and ZMZ structures.
- Monitoring & early warning:
  Use of sensors, drone detection, and OSINT monitoring to detect potential threats in the vicinity of facilities.
- Security governance:
  Definition of responsibilities in the interaction between corporate security, facility management, IT, and business continuity.

3.4 Country and location perspective

Relevance

Multinational companies operate in a complex environment of different national security, legal, and crisis regulations. In the event of tension or defense, national laws (e.g. security, energy security, and occupational safety laws) apply in parallel with European and NATO regulations. A lack of harmonization, different escalation levels, and divergent communication and decision-making channels can significantly impair a company's ability to act.

For internationally active companies, a uniform, cross-border crisis and security management system is therefore essential (EU Commission 2025, 2022a; NATO 2024).

Key risks

- Divergent national security and crisis requirements (e.g. activation of mobilization or reporting obligations).
- Lack of harmonization with EU, NATO, and partner country regulations.
- Unclear responsibilities between national subsidiaries, authorities, and headquarters.
- Inconsistent communication across country and legal system boundaries.
- Reputational and liability risks in the event of non-compliance with national security or compliance obligations.

Strategic goals

- Establishment of a uniform, internationally coordinated crisis and emergency management system.
- Ensuring legal and regulatory compliance at all national and international locations.
- Harmonization of security-related standards and processes in line with EU, NATO, and national requirements.
- Consistent communication and decision-making processes between headquarters, subsidiaries, and authorities.
- Integration of location and country risks into the central risk management and business continuity framework.

Critical measures & governance

- Harmonization & standardization:
  Development of uniform crisis, security, and communication guidelines for all country organizations (including escalation and approval processes).
- Governance framework:
  Establishment of a central, internationally coordinated security governance system with clear roles (HQ, national subsidiaries, authorities).
- Legal and compliance monitoring:
  Regular review of national security and crisis laws; integration into the compliance management system.
- Cross-border crisis exercises:
  Conducting joint crisis exercises with international locations, authorities, and ZMZ structures.
- Communication architecture:
  Ensuring redundant, internationally synchronized communication channels; defining clear reporting and decision-making channels.
- Consideration of geopolitical risks:
  Assessment of the security situation in relevant countries (e.g.,NATO's eastern flank, Indo-Pacific) in the context of strategic location decisions.

3.5 Products and services

Relevance

In times of tension or defense, products and services are prioritized not only according to economic criteria, but also according to security and supply policy criteria. **Companies with systemically important or dual-use products may be subject to government control, reporting requirements, or production restrictions**.
An early assessment of systemic relevance and dual-use potential is therefore crucial in order to maintain security of action, supply, and planning (Bafa 2021, BMWK 2024a, 2024b; EU Commission 2022).

Key risks

- Production interruptions due to resource shortages, power outages, or government intervention.
- Government control and prioritization (e.g. manufacturing for the armed forces or critical infrastructure).
- Loss of flexibility due to the reallocation of production capacities or export restrictions.
- Legal risks due to lack of classification of dual-use goods.
- Dependence on intermediate products and sensitive suppliers with security-relevant interfaces.

Strategic goals

- Ensuring the continuous provision of system-critical products and services.
- Early identification and evaluation of security-related and dual-use products.
- Maintaining production capacity despite government intervention or resource constraints.
- Making the business model more flexible to adapt to regulatory prioritization requirements.
- Integrating product and service resilience into business continuity, supply chain, and risk management.

Critical measures & governance

- System relevance analysis:
  Evaluation of the portfolio according to criticality (KRITIS reference, security policy significance, civil and military use).
- Dual-use compliance:
  Review of existing export and trade restrictions; establishment of clear classification and reporting processes (in accordance with EU Dual-Use Regulation 2021/821).
- Production and resource planning:
  Development of emergency production plans with prioritization and reserves for critical goods.
- Coordination with authorities:
  Establishment of fixed communication channels with BMWE, BMVg, and ZMZ offices to coordinate production capacities in the event of a crisis.
- Governance & reporting:
  Integration of product-related resilience indicators into corporate management (e.g. production capacity, material availability, government control capabilities).
- Research & innovation:
  Promotion of security-related innovations with European added value (e.g.,via EDF, IPCEI, Horizon Europe).

3.6 Markets & customer behavior

Relevance

Crises, tensions, or defense situations profoundly change demand, purchasing power, and market structures. Supply chain disruptions, energy shortages, inflation, export bans, or **military priorities lead to disruptions in supply and demand** that directly affect sales markets and customer relationships. Companies must be able to anticipate market dynamics and adapt their strategies flexibly (IFW 2024; IMF 2024, OECD 2025).

Key risks

- Demand slumps or demand shocks due to loss of purchasing power or government intervention.
- Shift in market priorities in favor of goods relevant to security or supply.
- Loss of international sales markets as a result of sanctions, conflicts, or logistical restrictions.
- Reputational risks in business relationships in geopolitically sensitive regions.
- Consumer behavior under crisis stress: increasing sensitivity to price, origin, and security of supply.

Strategic goals

- Maintaining economic capacity to act through flexible market and product strategies.
- Early detection of market and demand shifts for proactive adjustment of production and sales.
- Securing key sales markets through geographic diversification and strategic partnerships.
- Strengthening customer loyalty through trust, security of supply, and clear crisis communication.
- Integrating market risks into strategic planning, crisis management, and business continuity.

Critical measures & governance

- Market scenarios & early warning systems:
  Establishment of continuous market and environment analyses to identify geopolitical, regulatory, and social trend changes.
- Diversification of the sales structure:
  Development of alternative markets within the EU or friendly partner countries ("friend-shoring").
- Customer management & communication:
  Transparent information about delivery capabilities, supply situations, and priorities in the event of a crisis.

- Contract and risk protection:
  Inclusion of force majeure, delivery guarantee, and prioritization clauses in key customer contracts.
- Innovation and product strategy:
  Focus on products with high crisis resistance (e.g. energy efficiency, security, supply, digitalization).
- Resilience monitoring:
  Integration of market-related key figures into risk management (e.g. sales resilience, customer stability, demand volatility).

3.7 Cyber, communication, and operating systems

Relevance

IT, communication, and operating systems are the critical points of modern corporate resilience. In hybrid conflicts, cyberattacks, disinformation, espionage, and sabotage are the preferred means of destabilizing critical infrastructure and value chains. With the entry into force of the NIS2 Directive and the EU Cyber Resilience Act (CRA), companies are also legally obliged to design digital systems to be resilient, reportable, and secure. A failure of central IT, OT, or communication systems directly jeopardizes management, control, and production capabilities—and thus national and economic security.

Key risks

- Cyberattacks on ERP, production, and control systems (IT/OT), often via supply chains or compromised third-party providers.
- Data loss or manipulation through ransomware, espionage, or sabotage.
- Dependence on cloud service providers outside the EU (lack of data sovereignty).
- Communication failures in the event of interruptions to public networks, the internet, or mobile communications.
- Disruptions to critical providers (e.g. AWS, Microsoft, Google) with cascading effects on entire industries.
- Lack of integration of cyber situation, crisis communication, and business continuity.

Strategic goals

- Ensuring the functionality of critical IT, communication, and operating systems in the event of a crisis or defense situation.
- Strengthening cyber resilience through multi-layered protection, detection, and recovery measures.
- Establishing self-sufficient communication and decision-making capabilities in the event of public network or cloud infrastructure failure.
- Ensuring data sovereignty and system access in geopolitical crises or in the event of government intervention.

- Establishing clear governance for cyber and information security (involvement of CSO, CISO, CIO, and BCM).
- Integration into national and international situation assessments (BSI, CERT-Bund, NATO Cyber Command, EU CSIRT Network).

Critical measures & governance

- Technical resilience measures:
  Establishment of redundant and segmented network structures (zero trust architecture).
  Introduction of self-sufficient communication systems (satellite, out-of-band, shortwave).
  Offline-capable backups of business-critical data and systems.
- Reporting and cooperation obligations:
  Implementation of NIS2 and CRA requirements, including 24-hour reporting obligation for security incidents.
  Establishment of direct communication channels to BSI, CERT-Bund, and European CSIRT networks.
- Cyber situation assessment & crisis integration:
  Anchoring cyber and IT situation assessments in crisis teams and business continuity management (BCM).
  Use of government and commercial threat intelligence platforms (BSI, NATO MISP, EU-SOCTA).
- Training and resilience testing:
  Conducting regular cyber and recovery exercises, including physical attack scenarios.
  Integration of red team tests, tabletop exercises, and blackout scenarios into the BCM cycle.
- Legal & contract management:
  Review of cloud and IT contracts for crisis and access clauses; securing emergency access and data sovereignty.

3.8 Personnel & Workability

Relevance

Employees are the critical resource for any business and social resilience. In the event of tension, defense, or alliance, legal obligations (e.g.,Art. 12 GG, Work Security Act (ASG), Civil Protection and Alternative Service Acts)[3] apply, which allow the state to dispose of workers. At the same time, security situations, evacuations, mobilization, or psychological stress lead to significant absences and losses in efficiency. Companies must therefore be both legally predictable and organizationally resilient in order to remain operational despite staff withdrawals, mobilization, or crisis pressure.

Key risks

- Staff shortages due to the call-up of reservists or compulsory civilian protection services (e.g. THW, fire department, civil defense).
- Work absences due to evacuations, protective measures, or family obligations.
- Overwork and mental exhaustion due to ongoing crises and high security requirements.
- Security risks due to disinformation, ideological influence, or disloyal behavior.
- Lack of role and representation structures for key personnel.
- Lack of transparency regarding defense or civil protection duties among the workforce.

Strategic objectives

- Ensuring minimum staffing levels/operational capability in all critical processes.
- Establishing knowledge and functional redundancy to safeguard value creation.
- Transparency regarding reservist status, honorary positions, and deployment duties while maintaining data protection.
- Ensuring employee protection, including evacuation, welfare, and psychological support measures.
- Legal predictability through coordination with authorities (e.g. BMAS, BMVg, ZMZ structures).
- Promotion of a resilient corporate culture that strengthens loyalty, care, and personal responsibility.

Critical measures & governance

- Role and minimum staffing planning:
  Definition of critical functions and personnel requirements per location and process.

[3] Excerpts from the legal framework or regulations can be found in Appendix 1.

- Reserve and volunteer management:
  Establishment of a confidential self-disclosure system in compliance with the GDPR; cooperation with initiatives such as *"Employers and Reserves"* (BMVg).
- Leave and return agreements:
  Regulations on the obligation to return to work and job security after reserve duty or civil defense involvement.
- Cross-training & knowledge management:
  Development of redundant skills and deputy models in key processes.
- Psychological & social resilience:
  Introduction of care and employee assistance programs, psychological crisis support, training for managers in dealing with stressful situations.
- Legal & organizational precautions:
  Review of corporate obligations under ASG (§ 3), Civil Service Act (§ 79 ZDG), and Occupational Safety and Health Act.
  Coordination with disaster control authorities and ZMZ coordinators to ensure operational capability in defense cases.
- Crisis exercises & scenarios:
  Conducting regular tabletop exercises with authorities (e.g. ZMZ, BSI, disaster control), integration of personnel and communication structures.

3.9 Law & governance – government control & regulation

Relevance

In the event of tension or defense, a variety of security and control mechanisms come into force that deeply affect corporate processes.
The state's goal is to maintain national and alliance defense – this includes the control of production, supply chains, energy, personnel, and communication. For companies, this means that legal certainty, governance, and compliance become decisive resilience factors.

Key risks

- Obligation to provide goods and services to the armed forces or civil defense.
- Production requirements and interventions in supply chains, e.g. prioritization of military orders.
- Insurance gaps (war, terrorism, cyberattacks) and the resulting cost risks.
- Legal uncertainties in the event of government requisition or mobilization.
- Liability risks for management in the event of non-fulfillment of government obligations.

- New compliance requirements due to national and European security legislation (NIS2, KRITIS-Dachgesetz, Verteidigungswirtschaftsverordnung)[4] .

Strategic goals

- Legal certainty in cases of tension, defense, and alliance.
- Establishment of clear governance structures with defined roles, responsibilities, and decision-making processes.
- Anchoring security and defense obligations in corporate policies.
- Ensuring compliance with national and international legal frameworks.
- Transparent cost and compensation mechanisms in the event of government intervention.
- Integration of legal and regulatory resilience into enterprise risk management (ERM).

Critical measures & governance

- Board ownership:
  Anchoring security, crisis law, and resilience in the responsibility of the highest management level (C-level, supervisory board, and owners).
- Governance structure:
  Establishment of a **Resilience & Compliance Steering Committee at board level** with interfaces to corporate security, IT, legal, finance, HR, and supply chain.
- Regulations & guidelines:
  Creation of a **resilience and crisis policy** with defined escalation paths, approval processes, and documentation requirements.
- Legal review:
  External expert opinions on obligations under security, labor, and economic laws (e.g., ASG, LV/BV laws)[5] .
- Contract management:
  Review of contracts for force majeure, delivery prioritization, and cost reimbursement clauses.
- Insurance coverage:
  Extension of existing policies to cover war, terrorism, cyber, business interruption, and political risks.
- Compliance & training:
  Training of managers on legal obligations and liability risks in times of tension.

[4] Excerpts from the legal framework or regulations can be found in Appendix 2.

[5] Excerpts from the legal framework or regulations can be found in Appendix 1.

- Documentation & evidence management:
  Preparation of standard forms, reporting channels, and verification protocols (e.g. to meet government requirements).

3.10 Finance & liquidity

Relevance

In security crises, financial markets, capital flows, and credit mechanisms come under considerable pressure. Payment systems can be restricted, insurance policies can become partially ineffective, and capital flows can be blocked by sanctions or government intervention. Companies must therefore **proactively secure their financial resilience** in order **to remain liquid** and ensure operational continuity even in the event of market standstill, energy crises, or cyber incidents. Financial management thus becomes a **strategic component of corporate security**.

Key risks

- Liquidity bottlenecks as a result of production losses, credit cuts, or delivery stoppages.
- Payment defaults by customers and suppliers due to economic instability.
- Collapse of the capital market or payment systems (TARGET2, SWIFT, SEPA).
- Insurance gaps (war, terrorism, cyber) and limited claims settlement.
- Inflation, interest rate shocks, and currency volatility due to geopolitical tensions.
- Lack of predictability of compensation or cost coverage in the event of government intervention.

Strategic objectives

- Ensuring liquidity for at least 3-6 months of crisis operations.
- Maintaining payment transactions even in the event of central system failure.
- Reducing financial dependencies on individual banks, insurers, or countries.
- Integration of financial risks into crisis and business continuity management.
- Creating transparency regarding support and protection mechanisms at EU, federal, and state level.
- Hedging corporate assets against geopolitical, operational, and macroeconomic shocks.

Critical measures & governance

- Liquidity management & stress tests:
  Building up liquidity and cash reserves for multiple scenarios; daily monitoring of key financial indicators.
- Financial redundancy:
  Use of multiple banks and alternative payment service providers; preparation for offline payments (e.g. manual bookings, emergency accounts).
- Credit lines & emergency financing:
  Early coordination with banks regarding crisis lines, guarantees, and sureties; establishment of internal liquidity pools.
- Insurance coverage:
  Review and extension of existing policies to cover war, terrorism, cyber, supply chain, and business interruption risks.
- Support and security instruments:
  Use of EU programs (*InvestEU Crisis Response*, *Resilience and Recovery Facility*) and national mechanisms (KfW crisis loans, guarantees).
- Financial compliance & documentation:
  Establishment of emergency approval processes and verification structures for cost tracking and government compensation[6] .
- Board reporting:
  Integration of financial and liquidity risks into enterprise risk management (ERM) and monthly reporting to CEO/CFO.

Recommended governance anchoring

- Responsibility lies with the CFO/CRO, integrated into the crisis management team and BCM.
- Development of a financial resilience playbook (credit lines, contact persons, approval processes).
- Regular liquidity and insurance reviews (quarterly basis).
- Integration into OPLAN-relevant planning processes for energy, supply chain, and security functions.

[6] Information on financing and support programs for the economy can be found in Appendix 3.

3.11 Technology & Innovation

Relevance

Technological independence is a central pillar of national and corporate resilience. **Dependencies on key technologies from outside Europe** – particularly in the areas of semiconductors, AI, cloud infrastructure, communications, and space technologies – **jeopardize both operational security and strategic capacity to act in the event of a crisis**. The EU Chips Act, the Cyber Resilience Act (CRA), and the Key Digital Technologies (KDT JU) program form the regulatory basis for European technological sovereignty, which companies must actively integrate into their security architecture.

Key risks

- Supply stoppages and export restrictions for critical technologies (e.g., semiconductors, sensor technology, software).
- Dependence on non-European suppliers (e.g., US clouds, Asian semiconductors, AI platforms).
- Cyber risks due to manipulation of hardware or software components.
- Technology gaps in European value chains (e.g. in defense, aerospace, or energy systems).
- Sanction or licensing risks when using dual-use technologies in third countries.
- Delayed innovation cycles due to regulatory uncertainty and lack of European scalability.

Strategic goals

- Ensuring technological sovereignty by strengthening key European technologies.
- Diversifying and localizing critical innovation and production partners.
- Integration of dual-use technologies in research, development, and industrial implementation.
- Protecting intellectual property (IP) and critical development data through proprietary security architecture.
- Cooperation with European innovation clusters (EDA, ESA, EU Defense Innovation Scheme).
- Early integration of technological risks into corporate and security risk management.

Critical measures & governance

- Technology mapping:
  Identification of key technologies, their supply chains, and dependencies (e.g. semiconductors, AI models, cloud, quantum computing, space travel).
- Sovereignty strategy:
  Development of an internal roadmap to reduce non-European dependencies and promote local innovation partnerships.

- Cooperation & Promotion:
  Participation in EU programs (*Horizon Europe, EDF, Key Digital Technologies Joint Undertaking*).
  Use of national funding mechanisms (e.g. BMBF "Sovereign IT").
- Protection & security:
  Integration of ITAR/EAR compliance, cybersecurity by design, and know-how protection into development processes.
- Dual-use governance:
  Evaluation of research projects with regard to security-related applications, export control, and ethical compliance.
- Technology resilience tests:
  Verification of critical system recovery times in the event of supplier or software platform failure.
- IP security & innovation protection:
  Establishment of secure development environments, especially for defense-related or security-critical applications.

Political-strategic classification

Technological resilience is not purely an economic issue, but part of the European security architecture. The EU specifically promotes the development of its own value chains in security-relevant areas (semiconductors, aerospace, quantum and energy technologies). Companies are called upon to design innovations not only in a market-driven manner, but also with security in mind – as part of a *"corporate sovereignty strategy"* in the interests of national and European resilience.

3.12 Ecology & sustainability

Relevance

Sustainability remains a mandatory strategic goal even in times of tension and defense. However, companies are increasingly facing conflicts of interest between security of supply, energy efficiency, and CO_2 reduction. The EU taxonomy, the Green Deal Industrial Plan, the Corporate Sustainability Reporting Directive (CSRD), and national climate laws continue to impose sustainability obligations even in times of crisis. This makes sustainability a core component of the security architecture – ecologically, economically, and socially.

Key risks

- Conflicting goals between security of supply and climate targets (e.g. reactivation of fossil fuels).
- Resource scarcity (water, rare earths, recycled materials).
- Dependence on unsustainable supply chains outside the EU.
- Regulatory risks in the event of non-compliance with ESG obligations (fines, damage to reputation).
- Loss of reputation due to perceived abandonment of sustainability goals in times of crisis.
- Physical climate risks (e.g. heat waves, extreme weather) with a direct impact on production and logistics.

Strategic goals

- Maintaining ESG compliance even in crisis and defense scenarios.
- Integration of sustainability into the resilience strategy – "Sustainable Security" (Knoppe 2025).
- Ensuring the supply of critical resources in accordance with ecological and social criteria.
- Promoting energy-efficient and low-emission production processes despite crisis requirements.
- Establishing closed material and energy cycles (circular economy).
- Anchoring ecological aspects in crisis and emergency planning (e.g. replacement procurement, location strategy).

Critical measures & governance

- Sustainability resilience program:
  Integration of ESG parameters into risk management, business continuity, and security strategy.
- Circular economy & resource management:
  Establishment of recycling structures and reuse systems to reduce material dependencies.
- Climate risk management:
  Integration of physical climate risks (heat, drought, storms) into location and production decisions.
- ESG compliance & reporting requirements:
  Ensuring reporting capability in accordance with CSRD/ESRS, even in the event of disrupted data collection or crisis operations.
- Green procurement strategy:
  Prioritizing sustainable suppliers and contract clauses on minimum environmental and social performance.

- Energy management & self-sufficiency:
  Expansion of photovoltaics, battery storage, biogas, and hydrogen to combine security of supply and CO_2 reduction.
- Stakeholder communication:
  Transparent presentation of conflicting goals (e.g. temporary energy consumption from fossil sources) in ESG reporting.

Political-strategic classification

Sustainability is not just climate protection, but also a strategic resilience policy. The EU Green Deal emphasizes the interconnection between decarbonization, raw material sovereignty, and crisis resilience. Companies that understand sustainability as part of their security strategy ensure regulatory acceptance, social trust, and long-term competitiveness. ESG is therefore not a "soft" issue (Knoppe 2025), but a prerequisite for national and corporate defense capabilities.

3.13 International interdependencies & geopolitics

Relevance

Global value creation and geopolitical stability are increasingly intertwined. Tensions between major powers, sanctions, raw material nationalism, and the increasing use of economic means as a geopolitical instrument are turning companies into strategic players in a new security economy. International cooperation, partner networks, and production relocations are thus becoming part of the resilience architecture of modern industrial companies.

Key risks

- Sanctions and export restrictions (e.g. Russia, China, Iran) that disrupt supply chains and sales markets.
- Politically motivated trade barriers (tariffs, technology restrictions, licensing requirements).
- Dependence on geopolitically unstable regions for energy, raw materials, or intermediate products.
- Shift in strategic alliances (e.g., BRICS+, Indo-Pacific alliances).
- Competition from state-subsidized markets (e.g. US: Inflation Reduction Act; China: State Industrial Strategy).
- Increase in hybrid influence activities via international subsidiaries, suppliers, or logistics routes.
- Fragmentation of multilateral systems (WTO, UN) and loss of reliable arbitration mechanisms.

Strategic goals

- Strengthening economic and political freedom of action through diversification of global value chains.
- Minimizing geopolitical dependencies on critical markets, partners, and technologies.
- Establishment of a geopolitical early warning system to assess and manage international risks.
- Integration of geopolitical scenarios into business, risk, and investment decisions.
- Cooperation within security-reliable areas (EU, NATO, G7, like-minded nations).
- Protecting international subsidiaries, data flows, and assets from government access or expropriation.

Critical measures & governance

- Geopolitical risk management:
  Establishment of a "GeoRisk Board" involving corporate security, strategy, and risk management.
- Friendshoring strategy:
  Reorganization of supply chains in politically stable regions ("resilient supply zones") within the EU, EEA, and NATO partner countries.
- Diversification & regionalization:
  Expansion of European manufacturing and procurement locations (nearshoring, dual sourcing).
- Sanctions and export control compliance:
  Systematic review in accordance with EU, US, and national law (ITAR, EAR, BAFA).
- Protection of foreign assets:
  Contract clauses and insurance coverage against political risks, expropriation, and government intervention (e.g., PRI insurance, MIGA coverage).
- Global situation analysis:
  Use of government and intelligence service situation reports (AA, BMVg, NATO StratCom, EEAS, EU INTCEN).
- Coordination of international crisis responses:
  Close coordination between company locations, foreign representations, and national crisis teams (AA Crisis Center, ZMZ).
- Security architecture in third countries:
  Assessment of political stability, legal certainty, and security situation prior to investments or expansions.

Political-strategic classification

OPLAN DEU is embedded in European and transatlantic security structures. At the same time**,** EU countries are developing their own national OPLAN concepts (e.g., France: *Plan ORSEC Défense*, Poland: *Plan Obronny RP*, Sweden: *Totalförsvarsplanen*). These programs illustrate the fusion of economic performance and national defense capabilities.

Companies with an international presence are therefore becoming part of national resilience planning – they must design their global supply, energy, and information networks in such a way that they remain stable even in times of geopolitical stress. The focus is shifting from "just-in-time" to **"just-in-case,"** from efficiency to strategic autonomy.

3.14 Cooperation & Networks

Relevance

Resilience comes from networking – **no company can survive a crisis in isolation**. The ability to act quickly, in a coordinated and trusting manner with authorities, partners, and industry players in crises and defense situations is crucial for stability and the ability to act. The establishment of such networks is increasingly seen as part of the national security architecture.

Cooperation between industry, the state, the armed forces, and associations forms the backbone of a functioning overall defense. Programs such as civil-military cooperation (ZMZ) or the federal government's KRITIS alliances already promote this interdependence today – but they must be actively operationalized at the corporate level.

Key risks

- Lack of coordination between companies, authorities, and military agencies.
- Information deficits and parallel situation assessments ("information silos").
- Lack of involvement in crisis communication and government reporting chains.
- Lack of networking with regional CMC agencies and disaster control authorities.
- Reliance on informal contacts instead of structured cooperation.
- Lack of integration of industry interests into government crisis planning (e.g. energy, transport, personnel).

Strategic goals

- Institutionalized cooperation with authorities, the armed forces, chambers of commerce and industry, and industry associations.
- Establishment of robust resilience networks along the entire value chain.
- Coordination of crisis and emergency plans with government agencies and regional ZMZ commands.

- Development of joint situation and information structures (e.g. CERTs, crisis platforms, BSI reporting channels).
- Promotion of a culture of security and resilience across industry boundaries.
- Coordinated communication in the event of a crisis (one-voice policy between companies, authorities, and the media).

Critical measures & governance

- Participation in resilience networks:
  Membership in KRITIS alliances, industry associations (BDI, Bitkom, VCI, VSW), IHK networks, and government resilience programs.
- Civil-military cooperation (ZMZ):
  Establishment of contact structures with regional civil-military cooperation staff of the German Armed Forces, joint exercises, and exchange in the event of a crisis.
- Interface management:
  Establishment of clear reporting and communication channels to the BMI, BSI, BMWE, BBK, THW, disaster control, CERT-Bund, and state authorities.
- Cooperation agreements:
  Development of bilateral or cross-sector agreements on mutual support (e.g. supply, transport, IT support).
- Crisis exercises & scenarios:
  Regular participation in cross-state and cross-industry exercises (e.g. LÜKEX, EU CIP exercises).
- Information security & trust:
  Use of secure communication platforms for confidential exchanges (e.g. VS-NfD-compliant channels).
- Knowledge exchange & lessons learned:
  Participation in resilience forums, industry exchanges, and scientific collaborations with research institutions.

Political-strategic classification

Cooperation is a security factor. With the National Security Strategy (Bundeskanzleramt 2023), the KRITIS Regulation (BMI 2023b), OPLAN DEU, and the Act to Strengthen Resilience in Civil Protection (BMI 2023a), the German federal government has laid the foundation for systematically integrating companies into the national resilience network. Industry, government, and society should thus act in an integrated rather than sequential manner—preventively, in a coordinated and binding manner.

Companies that see their ability to cooperate as part of their security strategy not only increase their own crisis resilience, but also contribute directly to the country's defense and competitiveness.

3.15 Crisis communication - Communication matrix (internal/external) - Stakeholder communication

Relevance

In a hybrid threat situation, communication determines trust, legitimacy, and stability. **In times of tension**, **companies are more in the public eye** – they are part of the public security architecture and bearers of social responsibility. Transparent, consistent, and credible communication thus becomes a strategic resilience factor.

At the same time, the risks are increasing: disinformation campaigns, manipulative narratives, and targeted discrediting on social media can massively damage a company's reputation within hours. Crisis communication must therefore be not only reactive, but also preventive, coordinated, and integrated with security.

Key risks

- Loss of trust due to missing or contradictory communication.
- Reputational damage as a result of lack of transparency, misreporting, or misinformation.
- Disinformation and information warfare against companies (deepfakes, social media manipulation, troll networks).
- Uncoordinated spokesperson roles and lack of coordination between company divisions.
- Lack of integration into government communication structures (BMI, BBK, MoWaS).
- Overloading of communication channels in the event of a crisis.

Strategic goals

- Securing trust among employees, customers, authorities, and the public.
- Uniform, coordinated communication based on the one-voice principle.
- Maintaining information sovereignty through active and credible crisis communication.
- Integration into national communication and warning systems (e.g., MoWaS, BSI reporting systems).
- Early detection and combating of disinformation.
- Transparent presentation of the company's social role and responsibility.

Critical measures & governance

- Crisis communication manual:
  Definition of roles, spokesperson rights, escalation paths, approval processes, and communication channels.
- Communication matrix:
  Clear responsibilities for internal and external stakeholders (executive board, HR, customers, media, authorities, suppliers, external service providers).
- Countering disinformation:
  Monitoring social media, identifying manipulative content, close cooperation with authorities and platform operators.
- Stakeholder dialogues:
  Regular exchange with authorities, associations, media, and employees to build trust.
- One-voice policy:
  Consistent messaging - coordinated between communications, corporate security, HR, legal, and the executive board.
- Training & media simulation:
  Regular training and camera/interview training for press spokespeople and executives.
- Psychosocial communication:
  Support for employees in crises through empathetic, credible, and solution-oriented communication.
- Secure communication channels:
  Use of redundant systems (e.g, satellite, shortwave, secure intranet solutions).

Political-strategic classification

Crisis communication is not a PR issue, but rather a matter of security communication.
It must be embedded in the overall national communication architecture – in particular in the information channels of the BBK, BMI, BSI, and Bundeswehr (ZMZ).
The Modular Warning System (MoWaS) serves as a central interface for trustworthy information and crisis warnings. Companies should integrate themselves into these communication flows at an early stage to ensure consistent situation reports and coordinated messages.

In hybrid conflicts**, the** following applies: **"Whoever controls communication controls perception."** A credible, responsible communication style not only strengthens reputation, but also social resilience – a contribution to overall defense.

3.16 Monitoring & early warning system

Relevance

Early information determines the scope for action. In a time of geopolitical instability, increasing cyber threats, and hybrid influence operations, a robust early warning system is the central building block of strategic resilience. It enables companies to proactively identify and assess risks and take corrective action before critical thresholds are reached.

Corporate security is ideally qualified to play a key role here: as an interface between the state, business, intelligence services, and internal departments, it coordinates the overall assessment of the situation, integrates external and internal sources of information, and derives decisions for management and crisis teams.

Key risks

- Lack of integration of situation information from government, private, and internal sources.
- Delayed detection of security-related trends (e.g. cyberattacks, sabotage, geopolitical escalations).
- Information silos and a lack of assessment expertise within the company.
- Lack of coordination with authorities (BSI, ZMZ, CERT-Bund).
- Insufficient indicators for early detection of supply, personnel, or infrastructure risks.
- Lack of connection between strategic risk reporting and operational situation assessment.

Strategic goals

- Establishment of an integrated situation assessment system that brings together security-related information from all sources.
- Proactive early detection and assessment of risks in the political, technological, physical, and digital environment.
- Ensuring the decision-making ability of the executive board and crisis management team through up-to-date, reliable, and consolidated information.
- Seamless connection to national and European warning and information structures (BSI, CERT, BBK, NATO, EU).
- Anchoring a permanent early warning process in corporate security governance.

Critical measures & governance

- Establishment of a central situation center (Security Intelligence Hub):
  Consolidation and evaluation of all security-related information (cyber, geo, industry, personnel, security, supply chain).
- Government information interfaces:
  Direct connection to
  - BSI (cyber warnings, CERT-Bund),
  - BMI / BBK (crisis and civil protection),
  - BMVg / ZMZ (civil-military cooperation),
  - AA Crisis Center / EU INTCEN (geopolitical situation reports).
- Private intelligence services:
  Use of commercial providers for cyber threat intelligence, OSINT, satellite data, and geopolitical analysis.
- Internal situation assessment:
  Integration of data from IT security monitoring, plant security, supply chain monitoring, personnel availability, and facility management.
- Critical partner assessment:
  Identification and categorization of business partners, service providers, and suppliers according to criticality ("single points of failure").
- Early warning indicators (KPIs & thresholds):
  Definition of measurable early warning signals (e.g. delivery delays, anomalies in cyber logs, regional escalation reports).
- Reporting & decision support:
  Daily, weekly, or event-driven status reports for CSOs, CROs, CEOs, and crisis teams.
- Automation & AI use:
  Use of AI-supported trend analysis and pattern recognition for risk developments (cyber, geo, energy, supply chain).
- Cooperation with authorities:
  Participation in cross-industry security and situation briefings (BSI Alliance for Cyber Security, BDI Security Networks, ZMZ exercises).

Political-strategic classification

A functioning early warning system is not only operational but also strategically systemically relevant. It closes the information gap between the state and the economy – a central goal of the national security strategy ((Bundeskanzleramt 2023) and OPLAN DEU. Companies that have their own situation assessment and analysis capabilities actively contribute to national resilience.

In cooperation with the authorities, a public-private intelligence structure is created that

- identifies risks more quickly,
- shortens operational response times, and
- supports government decision-making processes.

This enables corporate security to develop into **an early warning system for corporate management** – a decisive factor for security, competitiveness, and overall social stability.

4 Recommendations for action

Corporate resilience cannot be achieved through day-to-day operations alone – it requires strategic leadership and active responsibility at the highest management level. The signs are unmistakable: geopolitical uncertainty, hybrid threats, and tighter regulation. Resilience is no longer a voluntary option, but a mandatory task for supervisory boards, executive boards, and management – in large corporations as well as in small and medium-sized enterprises. OPLAN DEU highlights the paradigm shift: the economy is an integral part of the national security architecture. The consequence is clear: **resilience is a matter for top management.**

Resilience is the new competitive edge—a tangible competitive advantage and key success factor. The ability to remain capable of acting and delivering even under pressure is becoming the central benchmark of business excellence. Those who remain capable of delivering in crises win their orders, while their competitors lose out. Those who communicate transparently retain customers and investors in the long term. Strategic foresight, operational preparation, and credible communication **pay off directly on the bottom line** – in terms of revenue, profit, brand, reputation, financial stability, and enterprise value – and make companies reliable partners in their role as systemically important players in national security.

Investments in strategic and operational resilience measures are investments in business continuity, robust business models, and long-term profitability. Resilient companies secure their position among the global leaders in technology and innovation. **It is time to act – now, not tomorrow.**

4.1 Corporate Resilience Framework (CRF)

The Corporate Resilience Framework (CRF) defines the strategic responsibilities, governance structures, and operational measures necessary to ensure a company's ability to act in times of crisis, tension, and defense. **It supports small and large companies** alike in arming themselves against hybrid threats and geopolitical challenges and **in establishing a resilience system tailored to their individual needs**. To this end, the Corporate Resilience Framework (CFR) is divided into four levels:

- Strategic leadership by CEO & C-suite
- Governance, compliance, and operating model
- Corporate security organization (CSO office)
- Resilience measures program (strategic & operational)

4.2 Role of CEO & C-Suite

Corporate management bears overall responsibility for the resilience, security, and functionality of the company. It defines the strategic framework and manages priorities, resources, and decisions.

- Initiate resilience and risk analysis:
  Holistic assessment of all areas of the company (energy, supply chain, human resources, IT, communications, finance).

- Embedding in corporate strategy:
  Resilience and security as integral components of ESG, sustainability, and governance reporting requirements (CSRD).

- Establishment of a "Resilience Steering Committee" for cross-functional management at the executive board level (CEO, CSO, CFO, CISO, HR).

- Anchor strategic responsibility:
  Define responsibilities at the executive board level (CEO, CFO, COO, CSO, CISO).

- Prioritize strategic investments in resilience:
  Establish redundant systems, protect critical infrastructure, diversify supply chains, strengthen cyber defenses.

- Review the value chain under defense conditions:
  Strengthen the resilience of value chains and core operational processes, develop a *business model for times of crisis* – not to be confused with normal BCM operations.

- Institutionalize cooperation with the state and the Bundeswehr::
  Participate in ZMZ structures, KRITIS alliances, and official situation briefings.

- Crisis exercises at the executive board level:
  Regular tabletop exercises with realistic scenarios (e.g. blackout, cyberattack, delivery failure).

4.3 Governance, compliance, and operating model

This section defines structures, processes, and tools used to manage, measure, and develop resilience. Governance creates clarity about responsibilities, reporting lines, and decision-making logic.

4.3.1 GOVERNANCE STRUCTURE

- Establishment of a governance and compliance framework contingency planning – definition of roles, escalation paths, reporting obligations, and liability limits.
- Establishment of clear decision-making, escalation, and reporting lines between the operational level and the executive board.
- Close integration with IT security, HR, supply chain, facility management, and communications.
- Ensuring legal compliance with relevant regulations (Work Safety Act, KRITIS Regulation, BSI Act, NIS2).
- Documentation of decision-making processes and risk assessments for verification purposes vis-à-vis supervisory authorities and insurers.

4.3.2 REPORTING & RESILIENCE DASHBOARD

Transparent, data-based reporting creates control and decision-making capabilities. It links operational resilience measures with strategic corporate management and documents the effectiveness of the precautions taken.

- Reporting framework:
  Development of standardized resilience reporting (crisis status, risks, measures, trends),
  Monthly reporting to the executive board, supervisory board, and relevant authorities.
  Integration into existing governance and audit processes (risk management, compliance, ESG, CSRD).
- Resilience dashboard:
  Establishment of a KPI-based dashboard for ongoing assessment. Reporting to the Executive Board and Supervisory Board on the threat situation, status of measures, and resilience impact.
- Key performance indicators (KPIs):
  Degree of energy self-sufficiency, recovery time objective for critical systems, cyber incident response time, personnel availability in key processes, delivery capability in terms of infrastructure capacity

- Reporting in the annual report:
  Integration of a *resilience index* as a control variable – analogous to ESG criteria (economic, environmental, social, security policy).

- Review & lessons learned:

  - After each exercise and each incident, evaluation of effectiveness, adjustment of strategies and processes,

  - Follow-up on all crises, exercises, and security incidents ("after-action review").

  - Documentation of findings and integration into guidelines, training, and processes.

  - Systematic adaptation of the resilience framework to new threat situations and regulatory requirements.
    Regular review of the effectiveness of the corporate resilience framework

- External transparency & ESG integration

  - Consideration of security and resilience-related aspects in ESG and sustainability reports (CSRD).

  - Use of the Resilience Index as a supplementary control variable alongside economic indicators.

  - Disclosure of relevant security and risk measures to stakeholders (authorities, investors, the public).

4.4 Role of corporate security

Corporate security is an **essential strategic pillar of corporate resilience** (Knoppe 2025, 2024). It ensures the protection of people, assets, and information and establishes the link between government security architecture[7] and operational resilience management. Corporate security is the central unit for assessing strategic resilience factors and provides potential scenarios (e.g. geopolitical risk and success factors in value chains) that can have a lasting impact on companies' bottom lines. Corporate security is therefore suitable as a central resilience platform for developing and managing company-wide resilience processes and enabling companies to continue operating and creating value even in the face of crises and hybrid threats.

4.4.1 STRATEGIC TASKS OF CORPORATE SECURITY[8]

- Establishment of the Resilience Steering Committee and anchoring of the CSO function.
- Developing strategic scenarios related to geopolitical, technological, and economic changes (basis for decision-making by senior management).
- Development and implementation of an integrated resilience and security strategy for crisis and defense situations.
- Establishment and operation of an integrated resilience and information system for situation awareness, threat analysis, and early warning.
- Defense against espionage, sabotage, and hybrid attacks, including cyber, disinformation, and insider threats.
- Design-to-resilience: Integration of resilience and security aspects into all business processes.
- Protection and maintenance of the functionality of critical locations, systems, and processes (physical, digital, personnel).
- Establishment of clear communication channels in crises: internal and external escalation matrix (management, authorities, partners).
- Management and prioritization of security-related resources in coordination with the Executive Board and authorities.

[7] e.g. BMI, BMWE, BMVg, intelligence services, KRITIS networks, etc.

[8] Checklist see Appendix 4

4.4.2 OPERATIONAL TASKS OF CORPORATE SECURITY[9]

- Situation awareness and support for crisis communication and ensuring consistent information in line with the one-voice principle.
- Interface management with authorities, the Bundeswehr, NATO partners, intelligence services, and security networks.
- Site security: protection of critical sites, facilities, and employees.
- Employee safety (e.g. evacuation).
- Promotion of a culture of security, awareness, and training throughout the company.
- Training and sensitization of all employees in the areas of security awareness, crisis behavior, and resilience.
- Regular audits and exercises to check effectiveness and responsiveness.

4.5 Resilience measures program

This section brings together all operational and technical measures that contribute to stabilization, security, and recoverability. Strategic resilience programs ensure the company's ability to act in crises, situations of tension, or defense scenarios. They bridge operational failures, stabilize critical processes, and ensure that energy, IT, supply chains, and communications remain functional even under government control or infrastructure bottlenecks.
Time horizon: 30 to 180 days after the onset of a crisis.

4.5.1 IMMEDIATE PROGRAM (0-30 DAYS)

- **Establishment of a company-wide crisis management team:**
  Clear roles, clear communication matrix (internal/external) and decision-making processes; connection to government structures (BSI, ZMZ, BBK).
- **Securing critical processes:**
  energy supply, IT operations, communication, transport logistics.
- **Reserve and emergency personnel management:**
  Recording of key personnel, exemption rules, and minimum staffing plans. Ensuring minimum staffing and the ability to act at all levels.

[9] Checklist see Appendix 5

- **Communication & information flow:**
  Establishing the one-voice principle; defining communication manuals and approval processes.

- **Contacting authorities:**
  Registration in regional ZMZ structures, exchange with disaster control, IHK, BBK. KRITIS networks

4.5.2 STABILIZATION PROGRAM (30–180 DAYS)

- **Redundant energy and IT systems:**
  Establish alternative energy sources, emergency power, backup data centers, offline operability.

- **Diversify supply chains and markets:**
  Dual sourcing, nearshoring, stockpiling critical materials, securing transport routes.

- **Increase cyber resilience:**
  Zero-trust architecture, network segmentation, emergency communications, cyber exercises.

- **Scenario planning:**
  Develop crisis and defense scenarios, including market, personnel, and communication dimensions.

- **Establishing a governance framework:**
  Clear responsibilities, escalation paths, compliance and liability assessment (e.g. Work Safety Act, KRITIS Regulation).

- **Storage & supply:**
  Stockpiling of critical products and materials for 30–90 days.

- **Industry cooperation:**
  Networking with partners for mutual protection in crisis situations.

4.5.3 TECHNICAL RESILIENCE

- Establishment of redundant energy and IT systems to maintain operations in island mode (emergency power, offline IT, independent data networks).

- Implementation of self-sufficient communications infrastructures (satellite, shortwave, out-of-band systems) for command and reporting capabilities.

- Establishment of backup data centers and segmented networks to ensure operational capability despite external cyber or infrastructure failures.

- Integration of energy and IT contingency plans into business continuity and crisis management.

4.5.4 OPERATIONAL RESILIENCE (SUPPLY CHAINS, MARKETS, RESOURCES)

- Diversification and regionalization of supply chains and sales markets; establishment of regional backup structures to reduce dependencies.
- Establishment of inventories and stockpiling strategies for critical materials, spare parts, and operating resources (horizon: 30–90 days).
- Adaptation of market and product strategies to geopolitical and security-related changes.
- Conducting regular stress tests for delivery capability under realistic crisis scenarios.

4.5.5 COOPERATION & NETWORKS

- Institutionalization of partnerships with government agencies (BSI, ZMZ, BBK, Bundeswehr, IHK).
- Participation in cross-industry security and resilience networks ("all instead of one").
- Promotion of mutual support between companies, especially in logistics, energy supply, and IT infrastructure.
- Regular crisis and communication exercises with authorities and partners.

5 Industry examples in the context of OPLAN DEU

The industry examples are based on the current situation of military-hybrid intensification and its significance for industrial value creation. This is accompanied by further international trade restrictions, supply bottlenecks, and international tariffs, which are exacerbating the economic value creation of German and European companies. The first effects are already being felt in the economy. Only a few of the most important industries are presented here as examples, as a detailed list of all sectors would go beyond the scope of this white paper.

5.1 Food industry & logistics

The hybrid threat posed by Russia presents a multifaceted challenge for the food industry and the general food supply. An escalation could have far-reaching economic consequences.

Challenges

Logistical bottlenecks were already a major issue during the COVID-19 pandemic. Hybrid threats or an escalation of the conflict could exacerbate these bottlenecks due to military prioritization or sabotage. This would lead to significant delays throughout the value chain, which would primarily affect the supply of goods to the population due to severely limited availability. This is exacerbated by a shortage of personnel caused by refugee movements or the call-up of reservists, especially in the areas of agriculture, logistics, and distribution. This has a direct impact on the operation of stores, logistics centers, and transport fleets.

In addition to the direct impact on food retailers, the availability of raw materials will have a particularly immediate effect on supply. Disrupted international trade, sanctions, or export bans could mean that raw materials for food production are only available to a very limited extent, if at all. The extreme uncertainty and the threat of shortages will lead to increased panic buying among the population, which will further exacerbate the already tense situation regarding the availability of goods and may lead to unequal distribution within the population.

Conclusion

All these factors would contribute significantly to a drastic increase in food prices. Shortages, increased production costs, and transport risks would be passed on directly to consumers, massively increasing the cost of living and reducing household purchasing power.

5.2 Automotive industry

The automotive industry is one of the highest-revenue and most employment-intensive sectors in Germany. Hundreds of thousands of employees work for manufacturers, suppliers, and service providers along a complex value chain. Due to its high economic and social significance, the automotive industry is an attractive target for hybrid forms of influence and attack. Targeted disruptions to production or the spread of disinformation can cause considerable economic damage and at the same time create uncertainty among the population. Companies along the entire supply chain must therefore prepare themselves at an early stage for a wide range of potential security incidents – from cyberattacks, espionage, and spying to sabotage, disinformation campaigns, and physical attacks.

The reliability of the supply chain is an essential part of maintaining production. In the past, failures in this area have led to disruptions and even production downtime.

Challenges

The German automotive industry sources many parts from Eastern Europe, including Poland. An escalation of the scenario between NATO and Russia to Poland would have far-reaching consequences for the entire German automotive industry and its suppliers, including disruption to local markets and supply chains.

Many parts, such as electronic control units (ECUs), high-voltage (HV) battery parts, sensors, and body parts, are produced there and delivered to Germany. A conflict would affect production and, in the worst case, completely block transport routes and logistics processes. Just-in-time and just-in-sequence processes in Germany would be at risk without redundancies and functioning BCM processes.

Poland is a sales market, including for electric vehicles (EVs) and plug-in hybrids (PHEVs). A military conflict would affect purchasing power for automobiles. In addition, there could be export bans in conflict regions, including for sensitive technologies used in vehicle parts.

Even in the run-up to a conflict, energy and thus production prices could rise dramatically, and the prices for supplying local suppliers with raw materials such as lithium, cobalt, and nickel would also increase.

Ultimately, investment in research into future technologies such as autonomous driving and vehicle digitalization would stagnate or cease altogether, which would have a lasting impact on global competition.

Conclusion

The automotive industry should already be expanding its location and cybersecurity measures in a targeted manner and comprehensively developing its crisis management capabilities. This includes regularly updating emergency and response plans, practical training and exercises, and establishing alternative supply and logistics structures. Many of these measures require advance preparation, such as the qualification and integration of new suppliers in the event of a failure due to hybrid or military impacts. Only through early preparation can the industry strengthen its resilience to complex threat situations.

5.3 Energy sector

The energy sector is classified as critical infrastructure (KRITIS) and plays a central role in national defense planning within the framework of OPLAN DEU. Energy producers and grid operators contribute significantly to security of supply and are potential targets for hybrid attacks.

If the security situation continues to deteriorate without open hostilities, the threat of cyberattacks, acts of sabotage, and targeted disinformation campaigns will increase. Energy companies are therefore required to strengthen their resilience in several areas. This includes prioritized supply, i.e. ensuring the energy supply for military facilities, hospitals, and other critical infrastructure, for example. In addition, increased security measures must be taken, such as additional physical and digital safeguards like access controls, network segmentation, and continuous 24/7 monitoring.

Challenges

Crisis management also plays a crucial role: companies may have to participate in situation meetings, implement official directives quickly, and therefore need internal crisis teams to coordinate these measures. Emergency operations require the provision of backup power capacities and a high level of blackout resilience. Business continuity management must take particular account of personnel and resource shortages. Key personnel may be called up for military or emergency services duties, and truck drivers, equipment, or space may also be requisitioned by the military. Companies are therefore required to determine availability and plan for backup capacity and flexible logistics solutions.

Conclusion

OPLAN DEU makes it clear that energy supply is not only an economic task, but also a security policy task. Companies must regularly update their emergency and crisis plans, train their staff accordingly, and invest in technical, digital, and organizational resilience in order to remain operational even in the event of staff shortages and resource bottlenecks.

A particularly challenging aspect of the electricity supply is the interaction between the various players: generators, transmission system operators, distribution system operators, and the Federal Network Agency. This must be practiced in order to be able to respond adequately in case of need and to limit power outages or restore supply quickly.

In addition, all producers and network operators are economically independent companies that can only implement measures within the framework of legal requirements and taking economic factors into account.

5.4 Culture & Media

The culture and media sector is part of critical infrastructure (KRITIS) and plays a central role in social resilience, opinion-forming, and identity creation, especially in times of tension and defense. Cultural institutions, media companies, and journalists are not only bearers of democratic values, but can also be targets of hybrid threats.

In the event of a significant deterioration in the security situation without open hostilities, the threat to cultural and media institutions increases considerably. Attacks take place primarily in the digital space, through disinformation and targeted destabilization of public opinion.

Challenges

- Disinformation campaigns: dissemination of pro-Russian narratives via social media, deepfakes, and manipulated content to divide society
- Physical or cyber attacks on broadcasting and media companies
- Targeted attacks on cultural assets: sabotage or digital deletion of cultural heritage (e.g. digital archives, media libraries)
- Restriction of journalistic work: obstruction or targeted discrediting of media professionals

Role of the Modular Warning System (MoWaS)[10]

- Dissemination of reliable information to warn the population:
MoWaS is used to disseminate warnings, recommendations for action, and clarifications via radio, television, apps (e.g. NINA), and cell broadcast.

- Coordination with broadcasters and media companies: Public broadcasters are obliged and private broadcasters are encouraged to adopt MoWaS messages and classify them editorially in order to warn the population.

- Risk: Manipulation or overload of MoWaS interfaces through cyberattacks could jeopardize the credibility of government communications.

Conclusion

In the event of defense, the culture and media sector becomes part of the overall national defense architecture. Requirements increase significantly, particularly in the areas of information sovereignty, cultural heritage preservation, and social resilience.

- Maintaining reporting: Media companies must be able to broadcast despite possible evacuations, power outages, or staff shortages. Trained personnel for reporting from crisis and war zones.

- Combating disinformation: Government agencies and the media must cooperate closely to quickly identify and refute false information.

- Strengthening cultural resilience: Cultural offerings (e.g. music, theater, literature) can help stabilize the population.

- Protecting cultural institutions: Museums, theaters, archives, and monuments, as well as broadcasting and media companies, must be secured against physical attacks or looting.

- Central warning and information platform: MoWaS may become the primary interface for government communication with the population.

- Integration with cultural and media actors: Communication partners such as telecommunications providers or media companies receive up-to-date situation information and recommendations for action via MoWaS.

[10] The **Modular Warning System (MoWaS)** is the central technical system used to disseminate official warnings about dangerous situations in Germany. It is operated by the Federal Office for Civil Protection and Disaster Assistance (BBK) (see https://www.bbk.bund.de/DE/Warnung-Vorsorge/Warnung-in-Deutschland/MoWaS/mowas_node.html).

- Expansion of reach: Use of shortwave radio, loudspeaker vehicles, cell broadcast, warning apps, and digital display boards to ensure the dissemination of information in the event of a failure of traditional media.

The culture and media sector is not only a carrier of information and identity, but also a strategic target for hybrid threats. Securing cultural institutions, ensuring independent reporting, and defending against disinformation are security policy tasks. MoWaS plays a key role in this as a trusted communication channel between the government, the media, and the population.

5.5 Aerospace industry

The aerospace industry is one of Europe's most economically important high-tech sectors. It combines high value added, long-term innovation cycles, and global export markets with critical infrastructure for communication, navigation, and logistics. As a dual sector (civil/military), it is also central to technological sovereignty and industrial resilience in Germany and Europe. Its core industrial areas include:

- Transport and reconnaissance fleets and their operation and maintenance (air mobility, ISR)
- Satellite and communication systems,
- civilian and military airports as logistical hubs,
- Manufacturing and maintenance companies (OEMs, MROs, suppliers),
- European space programs (Galileo, Copernicus, IRIS²), and
- key industrial players (e.g. Airbus, OHB, MT Aerospace, Safran, Thales Alenia).

Challenges

The industry is globally integrated, research-intensive, and dependent on highly specialized suppliers. This makes it particularly vulnerable to geopolitical, technological, and logistical disruptions. Key stress factors include:

- Cyber and sabotage attacks on production, control, and satellite systems
- Failure of critical suppliers and logistics chains (titanium, electronics, software)
- Energy and communication bottlenecks in the operation of factories, airports, and ground stations
- Attacks on airports or airspace infrastructure (e.g. GPS interference, drones)
- Espionage against high technology and secret development programs

- Political dependencies in global supply chains (e.g. titanium from Russia, components from Asia)
- Export restrictions and sanctions on military-related technologies
- Failures of satellite infrastructure due to cyberattacks or collisions in orbit
- Loss of skilled personnel due to mobilization, evacuation, or overload
- Drone and GPS interference operations in the vicinity of critical airports or test sites.
- Disinformation against defense and aviation companies ("war profiteers," "military industry").
- Attempts to sabotage energy and communications hubs, especially at sites with military or dual functions.
- Disruption of data connections to satellites and ground control centers.

For companies, this means an increasing need for diversification, strategic redundancy, and resilient partnerships within Europe.

In the event of a crisis or defense situation, the industry becomes an immediate part of the national security and supply chains. The following are economically crucial:

- Provision of military transport capacities (troops, material, wounded).
- Maintaining flight and maintenance operations under increased security conditions.
- Participation in satellite, communications, and reconnaissance systems for NATO and the EU.
- Prioritization of energy and spare parts supplies for military fleets and space infrastructure.
- Integration of civil aviation operations into military air transport logistics (host nation support).
- Obligations under the Work Security Act (ASG) for technical and flight operations personnel.
- Ensuring flight and operational safety while allowing military use of civilian infrastructure.
- Protection of space infrastructure (satellites, ground stations, data lines).
- Continuity of supply chains for highly specialized suppliers.

- Ensuring cyber, secrecy, and espionage protection in international cooperation
- Resilient energy and communications supply for production and control sites
- Coordination with authorities, BMVg, BMWE, BSI, DLR, and NATO agencies
- Public acceptance and trust in military-civilian use

Conclusion

For management and owners, this has a direct impact on business continuity, contract fulfillment, delivery capability, and corporate reputation. The resilience of the aerospace industry directly influences Europe's economic competitiveness and technological sustainability. An economically resilient aerospace sector not only increases Europe's security, but also protects the added value, innovative strength, and long-term market positioning of its companies. Only through forward-looking investments, robust supply chains, and coordinated cooperation between industry, government, and European partners can the aerospace industry secure its role as the economic backbone and innovation driver of Europe in the long term.

5.6 Security service providers & private security – impact on companies

Security service providers are an essential part of site and event security for many companies during normal operations. In times of tension and defense, however, their availability can be significantly limited. This is due to the provisions of the laws on payment in kind, security, and precautionary measures, as well as possible government service obligations. **Security service providers may** be **partially or completely withdrawn** and deployed by the state for higher-priority protection tasks, especially in the area of critical and defense-related infrastructure. Although the police and homeland security forces are generally responsible for guarding such objects, their personnel resources are limited. Therefore, it is likely that the state will make use of private security forces. Companies must therefore take into account even in peacetime that external security services will only be available to a limited extent or not at all in the event of a crisis.

Challenges

Private sector sites – even those with high security requirements – could only be protected to a limited extent in the event of a defense situation. Companies must therefore create structures at an early stage to secure personnel, critical processes, and real estate independently.

Area	**Possible restriction**	**Legal basis / Reason**
Staff availability	Security personnel may be called up or conscripted → Staff shortages.	Wehrpflichtrecht / § 13 ZSKG
Prioritization of protected objects	The state prioritizes critical infrastructure → Guarding private-sector properties becomes secondary.	Federal security and defense planning
Contractual situation	Private security contracts may be restricted or temporarily suspended.	Overriding public interest
State access	The police/Bundeswehr may take over or order security tasks.	GG Art. 87a, Wehr- und Polizeirecht
Material and logistics bottlenecks	Protective equipment and vehicles may be in short supply or prioritized by the state.	Securing laws

Conclusion

Since external security service providers are only available to a limited extent in the event of a crisis, it makes sense to set up an internal reserve team. The aim is to provide the minimum necessary security for system-critical locations. This team can consist of the following groups:

- Corporate security personnel (from less critical areas)
- Employees with previous military or government service (provided they are not subject to compulsory service)
- Technically trained personnel (facility management, engineering)

To reduce the risk of a complete loss of external service providers, companies can consider:

- Contractual provisions on the obligation to work in the event of a crisis, as far as legally possible
- Use of foreign security service providers whose personnel may be more difficult to conscript
- However, security risks, higher costs, and potential influence of the country of origin must be weighed up
- Agreements between companies and the state, especially for defense-related infrastructure, to avoid deductions or get support from territorial forces

Assessment: Foreign personnel can increase potential availability, but also increase economic and espionage risks. Operational prioritization ensures that scarce security resources can be used in a targeted manner.

Category	Significance	Examples	Security priority
A **system critical**	Essential for production or safety-related services	Data center, production core, R&D with protection requirements	Very high (internal + external + authorities)
B **Necessary for operations**	Relevant for operation, but reducible	Administration building, replacement warehouse	Medium (limited surveillance)
C **Subordinate**	Can be temporarily shut down	Guest houses, training centers	Low (technical security sufficient)

In addition, technical systems should be strengthened to partially compensate for the loss of personnel:

- Resilient access control systems
- Enhanced video surveillance and sensor technology
- semi-autonomous surveillance systems (drones, robotics)
- Redundant power supply (generators, emergency power systems) for critical systems

Security service providers are reliable partners in peacetime, but their availability is limited in times of tension or defense. This poses a **strategic risk** for companies **in terms of site security, operational capability, and know-how protection.**

Internal reserve capacities, prioritization, technical redundancies, and early coordination with the government and external service providers can significantly reduce this risk and strengthen operational resilience in the long term.

6 Key questions for industry in the context of OP-Plan DEUTSCHLAND

The German economy is facing increasing uncertainty about its role, responsibilities, and rights within OPLAN DEU in the context of overall defense. Many companies, especially operators of critical infrastructure (KRITIS) and export-oriented industries, recognize significant information deficits regarding legal, organizational, and operational processes in the event of tension, defense, or alliance.

The following questions, which have emerged from various industry associations, security networks, and corporate dialogues, illustrate the **structural need for orientation** between the state, the economy, and the Bundeswehr. They can be divided into ten thematic areas.

6.1 Structural deficits

Five overarching problem areas currently shape the industry perspective:

- Unclear priorities and responsibilities – particularly in the areas of energy, transport, personnel, and cyber defense.
- Lack of transparency in legal mechanisms – for example, in mobilization, authority to issue instructions, and reporting obligations.
- Inadequate communication structures – between companies, authorities, the armed forces, and federal states.
- Incomplete coordination regarding cyber, KRITIS, and supply chain risks.
- Lack of regulations for compensation and liability in the event of government intervention.

It is therefore recommended that an **"OPLAN DEU Industry Forum"** be established as a permanent coordination and dialogue body between the federal government, the armed forces, industry associations, and key companies.

6.2 Energy supply & prioritization

- How is the energy and fuel supply prioritized in the event of a conflict or defense situation?
- Which sectors are considered priority sectors, and what criteria are used for classification?
- Are there allocation quotas or quotas for industry, KRITIS, and defense companies?

- Who coordinates the distribution of energy and raw materials between the civilian economy and the armed forces?

- How are companies informed and involved once prioritization measures take effect?

- What exceptions or emergency mechanisms apply in the event of an impending production stoppage?

6.3 Mobilization & Legal Framework

- How are the mobilization regulations for companies and employees structured?

- What legal obligations arise from the escalation levels (consent, tension, defense, alliance)?

- How are reservists and key personnel in security-relevant companies treated?

- Which laws apply if NATO responds militarily without Germany declaring a state of defense?

- Which authorities have the power to issue instructions to companies, and how are decisions communicated?

6.4 Supply chains, markets & transport

- Are there delivery or transport priorities in favor of the Bundeswehr or NATO that affect civilian companies?

- Which transport corridors are reserved for military use, and how is coordination and compensation handled?

- What government mechanisms are in place for reimbursement of costs when civilian capacities are used?

- How can planning security for supply chains and sales markets be ensured?

6.5 Cyber security & information situation

- How are cyber attacks reported and supported – via BSI, CERT-Bund, ZMZ offices, or federal states?

- How can companies be integrated into government situation assessments (cyber and hybrid threats)?

- What reporting obligations and information channels apply in the event of tension or defense?

- How is classified information securely passed on to industry partners?

- What government mechanisms exist to combat disinformation that specifically targets companies?

6.6 Government use, liability & compensation

- What criteria are used to select locations or resources for military purposes?

- How is reimbursement or compensation regulated in the event of government use?

- What standard procedures or application channels exist (BBK, BMVg, federal states)?

- How are liability issues and insurance coverage handled when companies act on instructions?

6.7 Communication, Authorities & Governance

- Is there a central point of contact for companies to clarify questions about OPLAN DEU?

- Is there a coordination office for business and Bundeswehr or a national resilience secretariat?

- What role do ZMZ offices play in direct economic communication?

- What is the chain of command and escalation between the federal government, the states, and the business community?

- Is there a central information portal or situation dashboard through which instructions, priorities, and situations are communicated?

6.8 KRITIS, prioritization & protection

- How are companies classified as KRITIS, defense-critical, or defense-relevant?

- Which authority provides information about this categorization and the resulting obligations?

- What protection and support mechanisms exist for these companies (e.g. security support, support programs)?

- How are government resilience programs (KRITIS-Dachgesetz, NIS2, Cyber Resilience Act) coordinated and communicated?

6.9 Regional & Operational Implementation

- Where are the Convoy Support Centers (CSCs) located, and what role do they play for industry and logistics?

- What are the operational implications for companies in their vicinity (security requirements, access, use)?

- How are companies integrated into regional OPLAN implementation structures?

6.10 Additional fundamental questions

- How is data and secrecy protection ensured in the context of growing civil-military cooperation?

- How are European mechanisms (NATO, EU, Strategic Compass, Military Mobility) integrated at the national level?

- How are SMEs without their own security organization supported?

- What role do trade associations (BDI, VCI, Bitkom, BDLI, etc.) play in coordination?

- How can we ensure that resilience measures remain economically viable?

- How can joint exercises and simulation games between industry, government agencies, and the Bundeswehr be institutionalized?

Conclusion:

Industry issues clearly show that there are significant gaps in coordination, communication, and legislation between the state, industry, and the armed forces. A binding, transparent structure – **such as an OPLAN DEU industry forum or an Industry & Resilience Task Force** – is necessary to establish planning security, decision-making authority, and trust. Only through institutionalized cooperation can the functioning of the German economy be ensured in times of tension and defense.

7 Contacts and networks

Institution	**Responsibility**
BMI	Internal security, overall coordination of civil defense
BMVg / Bundeswehr (ZMZ)	Military support, host nation support
BBK	Civil protection, KRITIS coordination
BSI (Bundesamt für Sicherheit in der Informationstechnik) / CERT-Bund	Cyber situation, attack detection, reporting system
BMWE	Economic control, industry coordination
IHK / BDI / Industry associations	Information sharing, exchange with companies
THW / Federal States / Disaster control authorities	Operational support in the event of a crisis
VSW	
ZMZ structures of the Bundeswehr / Regional contact persons	

Appendix: Excerpts from the legal framework & checklists

Appendix 1: Personnel and operational capability

Law / Framework	Content / Meaning
Art. 12 GG	Obligation to perform military or civilian service in the event of defense.
Arbeitssicherstellungsgesetz (ASG, § 3)	State guarantee of labor for defense purposes.
Zivildienstgesetz (§ 79 ZDG)	Possibility of calling up persons who have been deferred in the event of tension or defense.
Katastrophenschutzgesetz & ZMZ-Doktrin	Cooperation between industry, authorities, and the Bundeswehr in civil protection.

Appendix 2: Governance

Law / Framework	Content / Significance
Grundgesetz (Art. 80a, 115a)	Definition of states of tension and defense, activation of security laws.
Arbeitssicherstellungsgesetz (ASG)	State security of labor for defense purposes (§§ 1–3).
Verteidigungswirtschaftsverordnung (VWiV)	Regulation of state intervention in production and delivery processes.
Security and supply laws	Control of critical resources (energy, food, transport).
NIS2 / KRITIS-Dachgesetz	EU-wide framework for ensuring digital and physical resilience.
BGB / HGB	Liability issues in the event of government claims and force majeure situations.

Appendix 3: Finance & liquidity

Level	Mechanism / Institution	Relevance
EU	*InvestEU / RRF / Solidarity Mechanism*	Supports companies in reconstruction and crisis financing.
Bund	*KfW crisis programs, guarantees BMWE / BMF*	Supports liquidity in government-recognized crisis situations.
EZB / BaFin	*Liquidity Coverage Ratio (LCR), Counter-Cyclical Buffer (CCyB)*	Flexibilisation of capital buffers in crisis mode.
Insurance	*War and terrorism exclusions*	Review of coverage gaps and renegotiation required.

Appendix 4: Checklist Strategic tasks of corporate security

Resilience governance

0 Establishment of a Resilience Steering Committee at board level

0 Anchoring the CSO function

0 Defining the company-wide resilience strategy for crises, stress, and defense scenarios

Strategic early warning & scenarios (corporate foresight security)

0 Development of a multidimensional scenario model (geopolitics, technology, cyber, supply chain, regulation)

0 Derivation of strategic options for action for management, portfolio management, and location prioritization

0 Assessment of the resilience of all business areas, value creation stages, and critical assets

Design-to-resilience

0 Integration of resilience principles into product development, site security, supply chain design, IT architecture, and HR processes

0 Ensuring that key products, programs, and supply chains function stably under stress, crisis, or hostile influence

Integrated security and situation awareness system

0 Establishment of a company-wide situation picture covering cyber, physical, geo, personnel, business continuity, intelligence, and supply chain

0 Introduction of an early warning and analysis program that translates strategic trends and threats into fact-based management impulses

Protection against complex threats

0 Development of a defense model to ward off hybrid attacks: cyber operations, disinformation, insiders, espionage, sabotage, supply chain access

0 Establishment of an intelligence-based security program (including strategic cooperation with authorities, partners, NATO structures)

Strategic communications architecture (crisis and influence management)

0 Ensuring a consistent, confident, and credible line of communication with authorities, investors, employees, and the public

0 Establishment of an OPLAN-DEU-compatible escalation and approval process

Resource prioritization and decision support

0 Management of resources, budgets, and critical capabilities based on strategic risks and corporate priorities

0 Decision support for management, the executive board, and the supervisory board on security-related and geopolitical issues

Appendix 5: Checklist of operational tasks of corporate security

Situation management & crisis operations

0 Operation of an integrated operations center for situation awareness, monitoring, and response.

0 Ensuring the one-voice principle in communication and decision-making.

0 Supporting the crisis management team with fact-based analysis and expert assessment.

Authority and network management

0 Continuous coordination with authorities, the armed forces, intelligence services, NATO partners, KRITIS networks, and industry associations.

0 Support for all interfaces in accordance with the requirements of OPLAN DEU, including mobilization, transport, energy, and protection of critical assets.

Protection of locations, systems, and personnel

0 Physical security, access control, perimeter protection, visitor management.

0 Global employee security, including travel, evacuation, and expat protection programs.

0 Protection of sensitive sites and supply chains.

Cyber, information, and secrecy protection

0 Operational countermeasures against espionage, data leakage, sabotage, social engineering.

0 Implementation of confidentiality protection in accordance with national guidelines (GHB, security checks).

0 Close integration of physical security, OT security, and cyber defense.

Exercises, audits, and security culture

0 Regular exercises (stress/red team exercises, government agency exercises, mobilization tests).

0 Training for all employees to strengthen the culture of safety and resilience.

Literature

1. **Bafa (2021).** Die neue EU-Dual-Use-Verordnung (Verordnung (EU) 2021/821). https://www.bafa.de/SharedDocs/Downloads/DE/Aussenwirtschaft/afk_merkblatt_eu-dual-use-vo.pdf?__blob=publicationFile&v=2 zuletzt aufgerufen am 11.12.2025
2. **BBK (2025a).** Kritische Infrastrukturen https://www.bbk.bund.de/DE/Themen/Kritische-Infrastrukturen/kritische-infrastrukturen_node.html?utm_source=chatgpt.com zuletzt aufgerufen am 11.12.2025
3. **BBK (2025b).** Sektoren und Branchen. https://www.bbk.bund.de/DE/Themen/Kritische-Infrastrukturen/Sektoren-Branchen/sektoren-branchen_node.html zuletzt aufgerufen am 11.12.2025
4. **BBK (2025c).** Zivil-Militätische Zusammenarbeit (ZMZ). https://www.bbk.bund.de/SharedDocs/Downloads/DE/Krisenmanagement/zmz-flyer.pdf?__blob=publicationFile&v=5 zuletzt aufgerufen am 11.12.2025
5. **BBK (2021).** Bundesamt für Bevölkerungsschutz und Katastrophenhilfe. Definitionen von Schutzzielen für Kritische Infrastrukturen. Forschung im Bevölkerungsschutz, Band 28. https://www.bbk.bund.de/SharedDocs/Downloads/DE/KRITIS/definition_von_schutzzielen_fuer_kritis.pdf?__blob=publicationFile&v=4 zuletzt aufgerufen am 11.12.2025
6. **BfV (2025a).** Bundesamt für Verfassungsschutz. Verfassungsschutzbericht 2024 https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/verfassungsschutzberichte/2025-06-10-verfassungsschutzbericht-2024.pdf?__blob=publicationFile&v=4&utm_source=chatgpt.com zuletzt aufgerufen am 11.12.2025
7. **BfV (2025b).** Bundesamt für Verfassungsschutz. Gefährdung durch russische Spionage, Sabotage und Desinformation. https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/spionage-und-proliferationsabwehr/2025-05-gefaehrdungen-durch-russische-spionage-sabotage-und-desinformation.pdf?__blob=publicationFile&v=5 zuletzt aufgerufen am 11.12.2025
8. **Bitkom (2025).** Studie Wirtschaftsschutz 2025 (DE) https://www.bitkom.org/Bitkom/Publikationen/Studie-Wirtschaftsschutz?utm_source=chatgpt.com zuletzt aufgerufen am 11.12.2025
9. **BMI (2024).** Rahmenrichtlinien für die Gesamtverteidigung – Gesamtverteidigungsrichtlinien – (RRGV). https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/sicherheit/RRGV.pdf?__blob=publicationFile&v=4 zuletzt aufgerufen am 11.12.2025
10. **BMI (2023a).** Deutsche Strategie zur Stärkung der Resilienz gegenüber Katastrophen. https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/BMI22017-resilienz-katastrophen.pdf?__blob=publicationFile&v=3 zuletzt aufgerufen am 11.12.2025
11. **BMI (2023b).** Bundesministerium des Innern. Positionspapier „KRITIS-Dachgesetz“ https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/stellungnahmen/kritis-dg/stn-up-kritis.pdf?__blob=publicationFile&v=3 zuletzt aufgerufen am 11.12.2025
12. **BMVg (2023).** Verteidigungspolitische Richtlinien 2023 Bundesministerium der Verteidigung zuletzt aufgerufen am 11.12.2025
13. **BMWK (2024a).** Bundesministerium für Wirtschaft und Klimaschutz. Bundesbericht Energieforschung 2024 Energie- und Rohstoffsicherheitsanalysen. https://www.bundeswirtschaftsministerium.de/Redaktion/DE/Publikationen/Energie/240716-bundesbericht-energieforschung-2024.html zuletzt aufgerufen am 11.12.2025
14. **BMWK (2024b).** Bundesministerium für Wirtschaft und Klimaschutz. Systementwicklungsstrategie 2024 https://www.bundeswirtschaftsministerium.de/Redaktion/DE/Publikationen/Klimaschutz/2024-systementwicklungsstrategie.pdf?__blob=publicationFile&v=10 zuletzt aufgerufen am 11.12.2025
15. **BNetzA (2025).** Bundesnetzagentur Monitoringbericht 2025. https://data.bundesnetzagentur.de/Bundesnetzagentur/SharedDocs/Mediathek/Monitoringberichte/MonitoringberichtEnergie2025.pdf zuletzt aufgerufen am 11.12.2025

16. **BNetzA (2024).** Bundesnetzagentur Monitoringbericht 2024. https://data.bundesnetzagentur.de/Bundesnetzagentur/SharedDocs/Mediathek/Monitoringberichte/MonitoringberichtEnergie2024.pdf zuletzt aufgerufen am 11.12.2025
17. **BSI (2024).** Bundesamt für Sicherheit in der Informationstechnik. Die Lage der IT-Sicherheit in Deutschland 2024. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2024.pdf?__blob=publicationFile&v=5 zuletzt aufgerufen am 11.12.2025
18. **Bundeskanzleramt (2023).** Integrierte Sicherheit für Deutschland. Nationale Sicherheitsstrategie. https://www.nationalesicherheitsstrategie.de/Sicherheitsstrategie-DE.pdf zuletzt aufgerufen am 11.12.2025
19. **Bundestag (2025a).** Fragen zur Notwendigkeit eines umfassenden Lagebilds zu Sabotage, Spionage und Desinformation. Drucksache 21/995 https://dserver.bundestag.de/btd/21/009/2100995.pdf zuletzt aufgerufen am 11.12.2025
20. **Bundestag (2025b).** Hybride Angriffe und Desinformation im Vorfeld der Bundestagswahl. Drucksache 20/14595 https://dserver.bundestag.de/btd/20/145/2014595.pdf zuletzt aufgerufen am 11.12.2025
21. **Bundestag (2024a).** Umsetzung Nationale Sicherheitsstrategie. Drucksache 20/13542 https://dserver.bundestag.de/btd/20/135/2013542.pdf zuletzt aufgerufen am 11.12.2025
22. **Bundestag (2024b).** Bericht zur Risikoanalyse für den Zivilschutz 2023. https://dserver.bundestag.de/btd/20/104/2010476.pdf zuletzt aufgerufen am 11.12.2025
23. **Bundeswehr (2025).** Operationsplan Deutschland https://www.bundeswehr.de/resource/blob/5920008/5eb62255741addec3f38d49a443d0282/booklet-operationsplan-deutschland-data.pdf zuletzt aufgerufen am 11.12.2025
24. **DIN SPEC 14027 (2024).** Geschäftsplan: Corporate Security - Anforderungen zur Stärkung physischer Resilienz von Organisationen https://www.din.de/de/forschung-und-innovation/din-spec/alle-geschaeftsplaene/wdc-beuth:din21:382621796/pdf-3562598 zuletzt aufgerufen am 11.12.2025
25. **Edwards, C.; Seidenstein, N. (2025).** The Scale of Russian Sabotage Operations Against Europe’s Critical Infrastructure. IISS. The International Institute for Strategic Studies. https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2025/08/pub25-095-the-scale-of-russian-sabotage-operations.pdf zuletzt aufgerufen am 11.12.2025
26. **EEAS (2024).** Strategic Compass: ANNUAL PROGRESS REPORTon the Implementation of the Strategic Compass for Security and Defence. https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en zuletzt aufgerufen am 11.12.2025
27. **EU-Commission 2025.** Commission Staff Working Docuemnt on Military Mobility. COM (2025) 847 final. https://transport.ec.europa.eu/document/download/c925bad5-7d13-4551-bfaa-03152dd468dd_en?filename=SWD_2025_847.pdf zuletzt aufgerufen am 11.12.2025
28. **EU-Commission (2023).** European Commission, Joint Research Centre (JRC) (2023). Hybrid Threats : A Comprehensive Resilience Ecosystem https://www.hybridcoe.fi/wp-content/uploads/2023/04/CORE_comprehensive_resilience_ecosystem.pdf zuletzt aufgerufen am 11.12.2025
29. **EU-Commission (2022a)** Cyber Resilience Act (2022). EU-Commission. Regulation (EU) 2024/2847. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R2847 zuletzt aufgerufen am 11.12.2025
30. **EU-Commission (2022b).** NIS2 Directive: securing network and information systems. Directive 2022/2555. https://digital-strategy.ec.europa.eu/en/policies/nis2-directive?utm_source=chatgpt.com zuletzt aufgerufen am 11.12.2025

31. **Grünbuch ZMZ 4.0 (2025).** Bubendorfer-Licht, S.; Eckert, L.; Hahn, A.; Krings, G.; Schäfer, I. Zivil-Militärische Zusammenarbeit 4.0 im militärischen Krisenfall. Eine Situationsbeschreibung, Analyse und Handlungsempfehlungen. https://zoes-bund.de/wp-content/uploads/2025/03/250306_Gruenbuch_ZMZ_digital.pdf zuletzt aufgerufen am 11.12.2025

32. **Hartmann, J. (2025).** DGAP Policy Brief Nr. 15 Juni 2025. Hybride Kriegsführung. Lehren zur Stärkung der europäischen Handlungsfähigkeit https://dgap.org/system/files/article_pdfs/15_DGAP%20Policy%20Brief%20Hybride%20Kriegsführung%203.pdf zuletzt aufgerufen am 11.12.2025

33. **IFW (2024).** Kiel Institute For The World Economy. Economic Outlook. No. 119(2024/Q4) https://www.kielinstitut.de/fileadmin/Dateiverwaltung/IfW-Publications/fis-import/78097681-d900-4bfe-9428-838e8b4ff77e-KKB_119_2024-Q4_Welt_EN.pdf?utm_source=chatgpt.com zuletzt aufgerufen am 11.12.2025

34. **IMF (2024).** World Economic Outlook. Policy Pivot, Rising Threats. https://www.imf.org/-/media/files/publications/weo/2024/october/english/text.pdf zuletzt aufgerufen am 11.12.2025

35. **Kather, T. (2024).** Nachgefragt. Wenn Russland die Nato angreifen würde, werden wir einen anderen Krieg sehen. https://www.bundeswehr.de/de/meldungen/nachgefragt-nato-verteidigungsbuendnis-5809526 zuletzt aufgerufen am 11.12.2025

36. **Knoppe, M. (2025).** Corporate Security als nachhaltiger Wertschöpfungsfaktor. In: Knoppe, M. (eds) Nachhaltige Wirtschaftskonzepte. SDG - Forschung, Konzepte, Lösungsansätze zur Nachhaltigkeit. Springer Gabler, Wiesbaden. https://doi.org/10.1007/978-3-658-47879-7_1

37. **Knoppe (2024).** Disruption und Wertschöpfung der Unternehmenssicherheit. In: Knoppe, M. (eds) Unternehmerische Wertschöpfung neu aufstellen. Springer Gabler, Wiesbaden. https://doi.org/10.1007/978-3-658-42270-7_1

38. **Metis (2024).** Universität der Bundeswehr Metis Studie Nr. 42 (Tsetsos, K., 2024). Szenarien russischer Einflussnahme bis 2030. Hybride Einwirkung Russlands auf die EU/NATO-Ostflanke https://metis.unibw.de/assets/pdf/metis-studie42-2024_12-rus_ostflanke.pdf zuletzt aufgerufen am 11.12.2025

39. **NATO (2025a).** Collective defence and Article 5. https://www.nato.int/en/what-we-do/introduction-to-nato/collective-defence-and-article-5 zuletzt aufgerufen am 11.12.2025

40. **NATO (2025b).** Virtual Manipulation Brief https://stratcomcoe.org/pdfjs/?file=/publications/download/VMB-Final-5aa5d.pdf?zoom=page-fit zuletzt aufgerufen am 11.12.2025

41. **NATO (2024).** Resilience, civil prepardeness and Article 3. https://www.nato.int/en/what-we-do/deterrence-and-defence/resilience-civil-preparedness-and-article-3?utm_source=chatgpt.com zuletzt aufgerufen am 11.12.2025

42. **OECD (2025).** OECD Economic Outlook. Resilient Growth but with Increasing Fragilities Volume 2025/2, N.118. https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/12/oecd-economic-outlook-volume-2025-issue-2_413f7d0a/9f653ca1-en.pdf zuletzt aufgerufen am 11.12.2025

43. **Pöhlmann, M. (2025).** Der Suwałki-Korridor. ZMSBw (Publikation / Opus). https://opus4.kobv.de/opus4-zmsbw/files/861/AK38_Suwalki_Poehlmann_2025.pdf zuletzt aufgerufen am 11.12.2025

44. **Sperling, N. (2025).** Hybride Bedrohungen. Die Bedrohung durch Russland im Cyber- und Informationsraum. https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum/aktuelles/bedrohung-russland-cyber-informationsraum-5981306?utm_source=chatgpt.com zuletzt aufgerufen am 11.12.2025

45. **SWP (2025).** Polens Sicherheitspolitik: amerikanische Ungewissheit und europäisches Moment. Die Zweifel an den USA wachsen.

https://www.swp-berlin.org/publications/products/aktuell/2025A24_PolensSicherheitspolitik.pdf zuletzt aufgerufen am 11.12.2025

46. **SWP (2024).** Die Neuvermessung der amerikanisch-europäischen Sicherheitsbeziehungen. Von Zeitwende zu Zeitwende. SWP-Studie 2024/S 15. https://www.swp-berlin.org/publications/products/studien/2024S15_sicherheitsbeziehungen_usa_europa.pdf zuletzt aufgerufen am 11.12.2025

List of abbreviations

Abbreviation		Meaning
AA	Auswärtiges Amt	Federal Foreign Office
ASG	Arbeitssicherstellungsgesetz	Employment Security Act
BDI	Bundesverband der Deutschen Industrie	Federation of German Industries
BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe	Federal Office for Civil Protection and Disaster Assistance
BMF	Bundesministerium der Finanzen	Federal Ministry of Finance
BMI	Bundesministerium des Innern und für Heimat	Federal Ministry of the Interior and Homeland
BMVg	Bundesministerium der Verteidigung	Federal Ministry of Defense
BMWE	Bundesministerium für Wirtschaft und Energie	Federal Ministry for Economic Affairs and Energy
BCM	Business Continuity Management	Business Continuity Management
BNetzA	Bundesnetzagentur	Federal Network Agency
BSI	Bundesamt für Sicherheit in der Informationstechnik	Federal Office for Information Security
CERT-Bund	Computer Emergency Response Team des Bundes	Federal Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team	Computer Security Incident Response Team
CRF	Corporate Resilience Framework	Corporate Resilience Framework
CSRD	Corporate Sustainability Reporting Directive	Corporate Sustainability Reporting Directive
EDA	European Defence Agency	European Defense Agency
EDF	European Defence Fund	European Defense Fund
ESG	Environmental, Social, Governance	Environmental, Social, Governance
EU INTCEN	EU Intelligence and Situation Centre	EU Intelligence and Situation Centre
ISR	Intelligence, Surveillance, Reconnaissance	Intelligence, Surveillance, Reconnaissance
ITAR/EAR	US Exportkontrollrecht	US export control law
KRITIS	Kritische Infrastrukturen	Critical infrastructures
LCR	Liquidity Coverage Ratio	Liquidity coverage ratio
MoWaS	Modulares Warnsystem des Bundes	Federal modular warning system
MRO	Maintenance, Repair & Overhaul	Maintenance, Repair & Overhaul
NIS2	EU-Richtlinie zur Netz- und Informationssicherheit	EU Directive on Network and Information Security
OT	Operational Technology	Operational Technology
OPLAN DEU	Operationsplan Deutschland	Operations Plan Germany
PHEV	Plug-In Hybrid Electric Vehicle	Plug-in hybrid electric vehicle
RRF	Recovery and Resilience Facility (EU)	Recovery and Resilience Facility (EU)
VWiV	Verteidigungswirtschaftsverordnung	Defense Industry Regulation
ZMZ	Zivil-Militärische Zusammenarbeit	Civil-Military Cooperation
ZSKG	Zivilschutz- und Katastrophenhilfegesetz	Civil Protection and Disaster Relief Act

Do you have any questions or suggestions?

Please use our feedback questionnaire or contact our think tank 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 common questions and learn more about the topic.

👉**Contact & Feedback**

White paper 01 ThinkTank Corporate Resilience, December 12, 2025