



THINK TANK CORPORATE RESILIENCE EXECUTIVE SUMMARY BOARD

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

Hybrid warfare is not a theoretical threat, but a reality:

- At least €289 billion in economic damage annually: (through cyberattacks, industrial espionage, and sabotage (Bitkom 2025))
- Objectives: Erosion of trust, destabilization of markets, disruption of critical value chains
- Methods: Orchestrated combination of military, non-military, and economic instruments

Fundamental realignment of business models and value creation

According to the German government and leading intelligence services, Germany is "no longer at peace, but not yet at war." The current phase of hybrid threats—consisting of cyberattacks, physical sabotage, disinformation, and economic influence—is forcing the German economy to fundamentally realign its business models and value chains.

Strategic imperative: The economy must act independently

The economy cannot wait for government directives. The Operations Plan Germany (OPLAN DEU) is not an instruction manual for companies, but a military-civilian framework concept for overall national defense.

Industry is called upon to reorganize itself in order to:

- Reduce dependencies
- Eliminate vulnerabilities
- Secure critical business processes
- Ensure value creation under crisis conditions

Four strategic areas of action for the economy

1. Strengthen cyber and supply chain resilience

- Diversifying energy, raw material, and logistics relationships
- Establishing redundant IT and communication systems
- Regular vulnerability analyses and stress tests
- Reducing geopolitical dependencies through nearshoring and dual sourcing

2. Anchoring hybrid threats in risk management

- Systematic integration of hybrid scenarios into business continuity management (BCM)
- Modeling indirect dependencies (cloud service providers, KRITIS operators)
- Expansion of classic risk analyses to include geopolitical and hybrid scenarios

3. Institutionalizing cooperation and civil-military cooperation (ZMZ)

- Establishing joint early warning systems with authorities and industry associations
- Active preparation for support requests in crisis situations
- Integration into regional and national crisis mechanisms

4. Adapting governance and compliance structures

- Alignment with EU and NATO frameworks (NIS2, Cyber Resilience Act, Strategic Compass)
- Establishment of a company-wide resilience governance framework
- Integration of resilience into ESG and sustainability reporting (CSRD)

Resilience is not a question of cost, but a core security policy task:

- Companies play an active role in the overall national security architecture
- They secure critical services, infrastructure, and expertise even in crisis conditions
- Resilience is becoming a **strategic competitive factor** and value driver

Concrete measures

- Initiate resilience and risk analysis for all areas of the company (energy, supply chain, human resources, IT, communications, finance)
- Anchor strategic responsibility through responsibilities at the executive board level (CEO, CFO, CSO, CISO) – ideally via a Resilience Steering Committee
- Prioritize investments in redundant systems, protection of critical infrastructure, diversification of supply chains, cyber defense
- Institutionalize cooperation with the government and the Bundeswehr by participating in ZMZ structures, KRITIS alliances, and official situation briefings
- Conduct crisis exercises at the executive board level with realistic scenarios (blackout, cyberattack, supply chain failure)

Understand escalation levels

The economy must prepare for four escalation levels:

- Consent case: Preparation for possible tensions
- Tension scenario: Activation of emergency laws for organizational and logistical defense preparations (Art. 80a GG)
- Defense case: Armed attack on federal territory/German troops or an immediate threat (Art. 115a-115l GG)
- Alliance case: NATO Article 5 – Germany as a logistical hub for up to 800,000 allied soldiers

Key message to political decision-makers

The business community is ready to take on responsibility – but needs:

- Clear communication and coordination structures between the state, the Bundeswehr, and industry
- Legal certainty in the event of mobilization, requisitioning, and compensation
- Transparency regarding priorities in energy, transport, and resources
- Institutionalized cooperation through a "National Resilience Industry Forum"
- Integration into national crisis exercises and information platforms

Conclusion: Resilience as a key strategic priority

The hybrid threat situation is forcing the German and European economies to strategically realign themselves. Only through targeted investments in resilience, cooperation, and prevention can the economy remain capable of acting under the conditions of hybrid conflicts.

Resilience is not a cost factor, but a key driver of value creation in an age of systemic uncertainty.

Recommended action

Resilience should be treated as a top priority in order to establish comprehensive resilience governance in the short term. Integration into strategic corporate planning, ESG reporting, and risk management is essential for the future viability of the German economy and of each individual company.

Full white paper at



Publisher

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

The **Corporate Resilience Think Tank** 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 was developed through close cooperation between industry and academia at the Technische Hochschule Ingolstadt in the field of "Value Creation through Corporate Security" and is closely linked to the MBA program **in 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 Group Security, Dr. Ing. h.c. F. Porsche AG)

Alexander Klotz (Head of Group Security, BMW AG)

Marco Mille (Head of Corporate Security, Siemens AG)

Johannes Strümpfel (Siemens AG; President of the 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 Technical University of Ingolstadt.

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](#)