THINK TANK CORPORATE RESILIENCE

EXECUTIVE SUMMARY CSO

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

VSW
Bundesverband

December 2025

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

Executive Summary Chief Security Officers

Hybrid warfare: Strategic realignment of corporate security

Germany is currently experiencing a phase of military hybrid intensification. Corporate security is thus evolving from a protective service provider to a strategic enabler of corporate resilience and an operational interface between business, government, and the Bundeswehr. Proactive action in the CSO role is becoming increasingly important: it is the **driving force behind resilience management and situation awareness**, which go beyond traditional reactive risk management.

Hybrid threats are not future scenarios, but everyday operational situations:

- At least €289 billion in annual damage from cyberattacks, industrial espionage, and sabotage (Bitkom 2025)
- Coordinated attacks on: production systems, supply chains, energy supply, personnel, communication
- Goals: destabilization, extortion, erosion of trust and operational capability
- Actors: State-controlled APT groups, hybrid operations, organized crime

Corporate security is the operational pillar of corporate resilience in the context of OPLAN DEU:

1. **From property protection to overall defense architecture**
    - Integration into national security structures (ZMZ, BSI, CERT-Bund, BBK)
    - Operational interface with the Bundeswehr, intelligence services, and authorities
    - Participation in official situation assessments and crisis exercises
2. **From reactive to anticipatory**
    - Establishment of an integrated early warning system (Security Intelligence Hub)
    - 24/7 situation awareness across all threat dimensions
    - Proactive threat analysis instead of incident response
3. **From silo to integration**
    - Integration with IT security, HR, supply chain, facilities, legal, communications
    - Member of the Resilience Steering Committee at board level
    - Direct reporting line to CEO/CRO

Strategic areas of action

1. Energy & raw materials supply

- Securing critical energy infrastructure (transformer stations, emergency power systems, tank farms)
- Cyber and physical hardening of OT systems and energy control centers
- Coordination with BNetzA and energy suppliers on prioritization
- Establishment of decentralized self-supply (PV, batteries, diesel reserves)

2. Supply chains & logistics

- Risk transparency across the entire supply chain (Tier 1 to Tier n)
- Securing logistical IT systems (ERP, tracking, port management)
- Physical protection of critical transshipment points and transport routes
- Development of dynamic risk heat maps and dual sourcing strategies

3. Internal infrastructure & locations

- Site classification according to KRITIS definition (DIN SPEC 14027)
- Reinforcement of access, perimeter, and drone protection systems
- Establishment of alternative locations ("hot sites")
- Use of sensor technology, drone detection, and OSINT monitoring

4. Cyber, communication, and operating systems

- Securing critical IT, OT, and communication systems
- Establishment of redundant and segmented network structures (zero trust)
- Introduction of self-sufficient communication systems (satellite, out-of-band)
- 24-hour reporting obligation under NIS2 for security incidents
- Direct communication channels to BSI, CERT-Bund, NATO Cyber

5. Personnel & operational capability

- Transparency regarding reservist status and civil defense duties (GDPR-compliant)
- Ensuring minimum staffing levels in critical processes
- Protecting the workforce from physical and psychological threats
- Cross-training, deputy models, and employee assistance programs

6. Products and services

- Evaluating the portfolio according to system relevance and dual-use potential
- Protection of security-relevant production data and developments
- Dual-use compliance in accordance with EU Regulation 2021/821
- Securing defense-related production lines

7. Legal & Governance

- Ensuring compliance with security laws
- Embedding resilience in corporate policies
- Clarifying liability issues in the event of government claims
- Extension of insurance policies (war, terrorism, cyber)

8. Technology & Innovation

- Protecting intellectual property and critical development data
- Protecting research facilities against espionage
- Evaluation of dual-use technologies
- Integration of ITAR/EAR compliance and IP security

9. International Interdependencies & Geopolitics

- Geopolitical risk management for all international locations
- Protecting foreign assets from government access
- Sanctions and export control compliance
- Use of government and intelligence situation reports

10. Markets & Customer Behavior

- Monitoring of geopolitical, regulatory, and social trends
- Early detection of reputation risks through hybrid influence operations

- Protection against disinformation campaigns
- Social media monitoring and OSINT integration

11. Country and location perspective

- Harmonization of security-related standards across all international locations
- Establishment of centralized, internationally coordinated security governance
- Legal and compliance monitoring of national security laws
- Cross-border crisis exercises

12. Finance & liquidity

- Ensuring solvency in the event of system failure
- Protection of financial IT and transaction data
- Use of multiple banks and alternative payment service providers
- Integration of financial risks into BCM

Monitoring & early warning system: core task of the CSO

Establishment of a security intelligence hub with four components:

1. **Government information interfaces**
   - BSI (cyber warnings, CERT-Bund)
   - BMI/BBK (crisis and civil protection)
   - BMVg/ZMZ (civil-military cooperation)
   - AA Crisis Center/EU INTCEN (geopolitical situation reports)
2. **Private intelligence services**
   - Cyber threat intelligence, OSINT, satellite data, geopolitical analyses
3. **Internal situation assessment**
   - IT security, plant security, supply chains, personnel, facility management
4. **Early warning indicators (KPIs)**
   - Delivery delays, cyber anomalies, regional escalations, energy availability

Crisis communication: Security as an information hub

- Securing information sovereignty
- Ensuring a single voice policy
- Countering disinformation
- Social media monitoring against manipulative content
- Integration into MoWaS (modular warning system)

The role of the CSO

- Strategic and operational leader in the national resilience network
- Coordinator between companies, authorities, and the Bundeswehr
- Responsible for the situation assessment for all security-related dimensions
- Decision preparer for time-critical measures
- Interface to government crisis teams and ZMZ structures

Responsibilities: Protection of critical locations, maintenance of communication capabilities, coordination with security forces, implementation of government directives in accordance with ASG

In a hybrid threat situation, the quality of security work determines business continuity, employee safety, reputation protection, financial stability, legal compliance, and national capacity to act.

Conclusion:

Corporate security is the operational and strategic pillar of corporate resilience and the interface to the overall government security architecture.

Full white paper at

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 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 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 Technische Hochschule 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**

VSW
Bundesverband

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