THINKTANK
CORPORATE RESILIENCE
EXECUTIVE SUMMARY BOARD

Wirtschaftliche Folgen hybrider Bedrohungen für Unternehmen und ihre Wertschöpfungsketten – Wie muss sich die Wirtschaft jetzt vorbereiten?

VSW
Bundesverband

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

Dezember 2025

Hybride Kriegsführung als strategische Herausforderung für die deutsche Wirtschaft

Hybride Kriegsführung ist keine theoretische Bedrohung, sondern Realität:

- Mindestens 289 Milliarden Euro volkswirtschaftlicher Schaden jährlich: (durch Cyberangriffe, Industriespionage und Sabotage (Bitkom 2025)
- Ziele: Erosion von Vertrauen, Destabilisierung von Märkten, Unterbrechung kritischer Wertschöpfungsketten
- Methoden: Orchestrierte Kombination aus militärischen, nicht-militärischen und wirtschaftlichen Instrumenten

Fundamentale Neuausrichtung von Geschäftsmodellen und Wertschöpfung

Deutschland befindet sich nach Einschätzung der Bundesregierung und führender Nachrichtendienste „nicht mehr im Frieden, aber noch nicht im Krieg". Die aktuelle Phase hybrider Bedrohungen – bestehend aus Cyberangriffen, physischer Sabotage, Desinformation und wirtschaftlicher Einflussnahme – zwingt die deutsche Wirtschaft zur fundamentalen strategischen Neuausrichtung ihrer Geschäftsmodelle und Wertschöpfungsketten.

Strategischer Imperativ: Wirtschaft muss eigenständig handeln

Die Wirtschaft kann nicht auf staatliche Vorgaben warten. Der Operationsplan Deutschland (OPLAN DEU) ist keine Bedienungsanleitung für Unternehmen**,** sondern ein militärisch-ziviles Rahmenkonzept für die staatliche Gesamtverteidigung.

Die Industrie ist gefordert, sich selbst neu zu formieren, um:

- Abhängigkeiten zu reduzieren
- Verwundbarkeiten zu beseitigen
- Kritische Geschäftsprozesse abzusichern
- Wertschöpfung unter Krisenbedingungen zu sichern

Vier strategische Handlungsfelder der Wirtschaft

1. **Cyber- und Lieferkettenresilienz stärken**

- Diversifizierung von Energie-, Rohstoff- und Logistikbeziehungen
- Aufbau redundanter IT- und Kommunikationssysteme
- Regelmäßige Schwachstellenanalysen und Stresstests
- Reduktion geopolitischer Abhängigkeiten durch Nearshoring und Dual Sourcing

2. Hybride Bedrohungen im Risikomanagement verankern

- Systematische Integration hybrider Szenarien in Business Continuity Management (BCM)
- Modellierung indirekter Abhängigkeiten (Cloud-Dienstleister, KRITIS-Betreiber)
- Erweiterung klassischer Risikoanalysen um geopolitische und hybride Szenarien

3. Kooperation und Zivil-Militärische Zusammenarbeit (ZMZ) institutionalisieren

- Aufbau gemeinsamer Frühwarnsysteme mit Behörden und Branchenverbänden
- Aktive Vorbereitung auf Unterstützungsanforderungen in Krisenfällen
- Integration in regionale und nationale Krisenmechanismen

4. Governance- und Compliance-Strukturen anpassen

- Ausrichtung auf EU- und NATO-Rahmenwerke (NIS2, Cyber Resilience Act, Strategic Compass)
- Aufbau eines unternehmensweiten Resilienz-Governance-Frameworks
- Integration von Resilienz in ESG- und Nachhaltigkeitsberichterstattung (CSRD)

Resilienz ist keine Kostenfrage, sondern eine sicherheitspolitische Kernaufgabe:

- Unternehmen übernehmen eine aktive Rolle in der gesamtstaatlichen Sicherheitsarchitektur
- Sie sichern kritische Dienstleistungen, Infrastruktur und Know-how auch unter Krisenbedingungen
- Resilienz wird zum **strategischen Wettbewerbsfaktor** und Wertschöpfungstreiber

Konkrete Maßnahmen

- Resilienz- und Risikoanalyse initiieren für alle Unternehmensbereiche (Energie, Lieferkette, Personal, IT, Kommunikation, Finanzen)
- Strategische Verantwortung verankern durch Zuständigkeiten auf Vorstandsebene (CEO, CFO, CSO, CISO) – idealerweise via Resilience Steering Committee
- Investitionen priorisieren in redundante Systeme, Schutz kritischer Infrastruktur, Diversifizierung von Lieferketten, Cyberabwehr
- Kooperation mit Staat und Bundeswehr institutionalisieren durch Teilnahme an ZMZ-Strukturen, KRITIS-Allianzen und behördlichen Lagebriefings
- Krisenübungen auf Vorstandsebene durchführen mit realistischen Szenarien (Blackout, Cyberangriff, Lieferkettenausfall)

Eskalationsstufen verstehen

Die Wirtschaft muss sich auf vier Eskalationsstufen vorbereiten:

- Zustimmungsfall**:** Vorbereitung auf mögliche Spannungen
- Spannungsfall: Aktivierung von Notstandsgesetzen für organisatorische und logistische Verteidigungsvorbereitungen (Art. 80a GG)
- Verteidigungsfall: Bewaffneter Angriff auf das Bundesgebiet / deutsche Truppen oder eine unmittelbare Drohung (Art. 115a-115l GG)
- Bündnisfall**:** NATO-Artikel 5 – Deutschland als logistische Drehscheibe für bis zu 800.000 alliierte Soldaten

Zentrale Botschaft an politische Entscheidungsträger

Die Wirtschaft ist bereit, Verantwortung zu übernehmen – benötigt jedoch:

- Klare Kommunikations- und Koordinationsstrukturen zwischen Staat, Bundeswehr und Industrie
- Rechtssicherheit bei Mobilmachung, Inanspruchnahme und Entschädigung
- Transparenz über Priorisierungen bei Energie, Transport und Ressourcen
- Institutionalisierte Kooperation durch ein „Industrieforum nationale Resilienz"
- Integration in nationale Krisenübungen und Informationsplattformen

Fazit: Resilienz als zentrale strategische Priorität

Die hybride Bedrohungslage zwingt die deutsche und europäische Wirtschaft zur strategischen Neuausrichtung. Nur durch gezielte Investitionen in Resilienz, Kooperation und Prävention bleibt die Wirtschaft unter den Bedingungen hybrider Konflikte handlungsfähig.

Resilienz ist kein Kostenfaktor, sondern ein zentraler Wertschöpfungstreiber im Zeitalter systemischer Unsicherheit.

Handlungsempfehlung

Resilienz sollte als Chefsache behandelt werden, um kurzfristig eine umfassende Resilienz-Governance zu etablieren. Die Integration in die strategische Unternehmensplanung, ESG-Berichterstattung und das Risikomanagement ist unverzichtbar für die Zukunftsfähigkeit der deutschen Wirtschaft und eines jeden einzelnen Unternehmens.

Vollständiges Whitepaper unter

Herausgeber

ThinkTank Corporate Resilience: *Wo Wirtschaft und Wissenschaft vorausdenken*

Der **ThinkTank Corporate Resilience** schafft eine Plattform, auf der strategische Trends, geopolitische Analysen und Zukunftsszenarien aus der Resilienzperspektive von Chief Security Officers mit der Business-Sicht von CEOs, Vorständen, Aufsichtsräten und Anteilseignern zusammengeführt werden. Er ist aus der engen Zusammenarbeit zwischen Wirtschaft und Wissenschaft an der Technischen Hochschule Ingolstadt im Bereich „Wertschöpfung durch Corporate Security“ entstanden und eng mit dem MBA-Programm **Strategy, Global Risk & Security Management** verbunden.

Initiiert wurde der ThinkTank von Sven Dawson, Florian Haacke, Alexander Klotz, Marco Mille, Johannes Strümpfel und Prof. Dr. Marc Knoppe, um C-Suite-Vertreter, Chief Security Officers und Behörden ein Forum für zukunftsorientiertes Denken sowie den strategischen Austausch über systemische Risiken **aus wirtschaftlicher Sicht** zu bieten.

in Kooperation mit dem

VSW-Bundesverband und dem

Beirat MBA Strategy, Global Risk & Security Management der Technische Hochschule Ingolstadt.

FAQ & Feedback zum Whitepaper

Die Herausforderungen hybrider Kriegsführung betreffen uns alle:
Wirtschaft, Wissenschaft und Gesellschaft. Um gemeinsam tragfähige Lösungen zu entwickeln, möchten wir Ihre Perspektive einbeziehen.

Haben Sie Fragen oder Anregungen?

Nutzen Sie unseren Feedback-Fragebogen oder kontaktieren Sie direkt unseren Thinktank. Ihre Impulse sind wertvoll und können entscheidend dazu beitragen, zukünftige Veröffentlichungen noch praxisnäher und relevanter zu gestalten.

Besuchen Sie unsere FAQs, um Antworten auf häufige Fragen zu erhalten und sich tiefer in das Thema einzuarbeiten.

👉 **Kontakt & Feedback**