Bundesakademie
für Sicherheitspolitik

Arbeitspapier Sicherheitspolitik, Nr. 3/2026 17. Februar 2026

Unternehmen in der gesamtstaatlichen Sicherheitsvorsorge:
Warum wirtschaftliche Resilienz sicherheitspolitisch entscheidend ist

von Tina Behnke und Leonie Limbach

Die sicherheitspolitische Lage Europas fordert von Deutschland, Sicherheit ganzheitlich neu zu denken und zu gestalten. Die Wirtschaft ist dabei kein Randakteur, sondern zentraler Pfeiler gesamtstaatlicher Handlungsfähigkeit. Gesamtstaatliche Sicherheitsvorsorge entsteht im Zusammenspiel staatlicher, wirtschaftlicher und gesellschaftlicher Akteure – sie schützt Bevölkerung, Lebensgrundlagen und wirtschaftliche Wertschöpfung gleichermaßen. Wirtschaftliche Resilienz ist Voraussetzung dafür, dass Versorgung, gesellschaftliche Stabilität und staatliche Steuerungsfähigkeit erhalten bleiben. Dies gilt im zunehmend von hybriden Angriffen, geopolitischem Druck und wirtschaftlicher Verwundbarkeit geprägten Normalbetrieb ebenso wie in Krisen- und Notlagen. Dieses Arbeitspapier bündelt Erkenntnisse aktueller Studien und internationaler Vergleichsbeispiele, um Handlungsempfehlungen zu formulieren, wie wirtschaftliche Resilienz als dauerhafte Führungsaufgabe verstanden und systematisch in die gesamtstaatliche Sicherheitsvorsorge eingebettet werden kann.

Ausgangslage: Sicherheitspolitik jenseits des Militärischen

Europa sieht sich mit einer neuen Phase hybrider Angriffe konfrontiert: Cyberangriffe, Sabotageakte, Desinformation sowie wirtschaftlicher Druck werden gezielt eingesetzt, um die Funktionsfähigkeit von Staat, Wirtschaft und Gesellschaft zu beeinträchtigen und damit das Gesamtsystem zu schwächen. Dies wiederum untergräbt das Vertrauen in die Demokratie. Diese Angriffe zielen zunehmend auf die Grundlagen des Alltags – Energie, Kommunikation, Transport und Versorgung. Die regelbasierte, internationale Ordnung befindet sich in einer tiefen Krise und ist von zunehmender Instabilität geprägt. Insbesondere Russlands hybrider Krieg gegen den Westen, Cyberangriffe und gezielte Desinformation verschärfen die Bedrohungslage für Deutschland kontinuierlich. Zugleich ist die Verlässlichkeit der transatlantischen Partnerschaft, lange Fundament europäischer Sicherheit, nicht mehr selbstverständlich. Europäische Staaten müssen verstärkt eigene Vorsorge, Schutz und Durchhaltefähigkeit schaffen – nicht allein militärisch, sondern auch zivil, wirtschaftlich und gesellschaftlich.

Dazu bedarf es einer Gesamtstaatlichen Sicherheitsvorsorge (GSV). Dieses Arbeitspapier verwendet diesen Begriff bewusst, um klarzustellen, dass Sicherheit nicht erst im Spannungs- oder Verteidigungsfall relevant wird, sondern das gesamte Kontinuum staatlichen Handelns umfasst – vom Frieden über Krisen und hybride Angriffe bis hin zu Ausnahmelagen. GSV schließt ausdrücklich Vorsorge-, Resilienz- und Schutzmaßnahmen im Normalbetrieb ein. Ihr Ziel ist, staatliche, wirtschaftliche und gesellschaftliche Funktionsfähigkeit frühzeitig zu sichern, um Eskalationen vorzubeugen und Handlungsfähigkeit unterhalb der Schwelle des Verteidigungsfalls zu erhalten. Dieses Arbeitspapier bündelt dazu zentrale Erkenntnisse aktueller Studien.[1]

[1] Siehe Strategy& (2026): *Business into Breach – A Vision for Economic Resilience and Civil Preparedness* [online]; Zentrum Nachhaltige Transformation an der Quadriga Hochschule Berlin/BwConsulting GmbH/MHP Management- und IT-Beratung GmbH (2025): *Privatwirtschaftlich-militärische Zusammenarbeit für ein verteidigungsfähiges und resilientes Deutschland* [online]; Handelskammer Hamburg/Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2025): *Vorsorgeplan „Krisen, Katastrophen, Konflikte: Wie Sie Ihr Unternehmen in unsicheren Zeiten schützen“* [online].

 | ISSN 2366-0805

Die Funktionsfähigkeit Deutschlands beruht in weiten Teilen auf privatwirtschaftlichen Leistungen. Überwiegend Unternehmen tragen Energie, Logistik, digitale Dienste, Ernährung und Gesundheitswirtschaft. Als zentraler Wirtschafts- und Infrastruktur-Knotenpunkt Europas ist Deutschland stark von sicheren Lieferketten, Verkehrswegen, Energieflüssen und Kommunikationsnetzen abhängig. Heute prägen Fragilität, Abhängigkeiten und hybride Angriffe bereits den Normalzustand. Über das gesamte Kontinuum zwischen Normalbetrieb und Krise entscheidet die Stabilität der Wirtschaft darüber, ob staatliche und gesellschaftliche Funktionen aufrechterhalten werden können. Wirtschaftliche Resilienzvorsorge ist damit keine rein unternehmerische Aufgabe, sondern ein zentraler Bestandteil von Handlungsfähigkeit und GSV.

Resilienz bezeichnet in diesem Arbeitspapier die Fähigkeit von Unternehmen, ihre Funktions- und Handlungsfähigkeit auch unter außergewöhnlichen Krisen- und Gefahrenlagen durch Vorsorge, Anpassungsfähigkeit und wirksames Krisenmanagement zu sichern. Dazu gehört, Störungen auszuhalten, sich an veränderte Bedingungen anzupassen und nach einer Beeinträchtigung die Funktionsfähigkeit wiederherzustellen – also in einen gewünschten, stabilen Zustand zurückzufinden.

Zentrale Herausforderungen aus Sicht der Wirtschaft

Der private Sektor ist sicherheitspolitisch unverzichtbar, wird jedoch noch zu selten systematisch als Teil der GSV verstanden. Ausgelöst durch Pandemie, Energiekrise oder Lieferkettenstörungen wurden Resilienzmaßnahmen in den vergangenen Jahren vielfach nur reaktiv umgesetzt. Häufig gelten sie weiterhin als technisches oder compliance-getriebenes Thema und nicht als integraler Bestandteil strategischer Unternehmensführung. Gleichzeitig entwickelt sich Resilienz zunehmend zu einem Wettbewerbs- und Standortfaktor. Belastbare Lieferketten, Anpassungsfähigkeit und Durchhaltefähigkeit beeinflussen Marktchancen, Reputation, Finanzierungsmöglichkeiten und den Zugang zu Aufträgen. Wirtschaftliche Resilienz ist damit nicht nur Ausdruck gesellschaftlicher Verantwortung, sondern Voraussetzung langfristiger Wertschöpfung. Erforderlich ist eine dauerhafte Verankerung auf Management- und Vorstandsebene. Dazu gehören regelmäßige sicherheits- und geopolitische Lagebewertungen, Szenarioanalysen und Investitionsentscheidungen, die systematisch auf ihre Auswirkungen auf Durchhaltefähigkeit geprüft werden. Resilienz umfasst dabei unter anderem redundante Lieferketten, kritische Lagerhaltung, robuste IT- und Cybersicherheitsarchitekturen sowie belastbare Krisen- und Kommunikationsstrukturen. Wirtschaftliche Resilienz ist zudem eine Führungsaufgabe.

Mit dem am 29. Januar 2026 vom Bundestag beschlossenen KRITIS-Dachgesetz liegt erstmals ein bundesweit einheitlicher Rechtsrahmen für den physischen Schutz Kritischer Infrastruktur vor. Das Gesetz verpflichtet Betreiber zentraler Versorgungsleistungen – insbesondere in den Bereichen Energie, Wasser, Gesundheit und Transport – zu erweiterten Sicherheitskonzepten, regelmäßigen Risikoanalysen sowie zu Resilienz- und Notfallplänen. Positiv hervorzuheben ist, dass damit eine lange bestehende Regelungslücke geschlossen und die Bedeutung wirtschaftlicher Resilienz als Bestandteil von GSV ausdrücklich anerkannt wird. Zugleich zeigt die parlamentarische Debatte, dass das Gesetz vor allem größere Unternehmen adressiert und viele mittelständische Akteure sowie kommunale Infrastruktur bislang nur begrenzt einbezieht. Für alle Unternehmen aber bedeutet das KRITIS-Dachgesetz einerseits mehr Klarheit über staatliche Erwartungen, andererseits zusätzlichen Umsetzungsaufwand. Um die angestrebte Schutzwirkung tatsächlich zu erreichen, sind in jedem Fall flankierende Unterstützungsmaßnahmen erforderlich – insbesondere praxisnahe Leitlinien, Beratung und Förderangebote sowie eine stärkere Einbindung von Ländern, Kommunen sowie Industrie- und Handelskammern.

Zugleich bestehen häufig noch Lücken zwischen Bedrohungslage und Unternehmensplanung. Geschäftsfortführungs- und Krisenpläne orientieren sich oft an kurzfristigen Einzelereignissen. Mehrwöchige, multifaktorielle Belastungen – etwa gleichzeitige Energieknappheit, Cyberangriffe und Personalausfälle – werden selten integriert betrachtet. Besonders kleine und mittlere Unternehmen bleiben dadurch strukturell verwundbar, obwohl sie zentrale Funktionen regionaler Versorgung und Wertschöpfung übernehmen. Hinzu kommen Defizite an den Schnittstellen zwischen Staat und Wirtschaft. Austauschformate sind häufig technisch fokussiert, fragmentiert oder für kleinere Unternehmen kaum zugänglich. Wirksame GSV erfordert jedoch gemeinsame Lagebilder, klare Rollen, feste Ansprechpartner und regelmäßig erprobte Verfahren.

Internationale Orientierung: Lehren aus Skandinavien und Estland

Internationale Beispiele zeigen, dass nationale Resilienz dort besonders ausgeprägt ist, wo Unternehmen systematisch und dauerhaft in staatliche Vorsorgekonzepte eingebunden sind – nicht erst in Krise und Krieg, sondern als integraler Bestandteil ziviler Sicherheit und gesamtstaatlicher Durchhaltefähigkeit. Länder wie Schweden, Finnland, die Schweiz und Estland begreifen Eigenvorsorge der Wirtschaft nicht als freiwilligen Zusatz, sondern als klar formulierte staatliche Erwartung und festen Bestandteil nationaler Sicherheitskultur.

Schweden hat Anfang 2026 mit der Broschüre „Preparedness for businesses: In case of crisis and war" erstmals ein landesweit gültiges Dokument zur Vorbereitung aller Unternehmen auf Krisen- und Kriegslagen vorgelegt. Darin formuliert der Staat klare Erwartungen an die Eigenvorsorge: Kontinuitäts- und Notfallplanung, personelle Vorsorge, Priorisierung kritischer Leistungen, Notfallkommunikation sowie die Mitwirkung an regelmäßigen Übungen. Der Übergang vom Alltag in Krisen wird dabei systematisch mitgedacht. Finnland und die Schweiz verfolgen vergleichbare Ansätze. Beide Staaten setzen seit Jahren auf eine ausgeprägte Vorsorge- und Sicherheitskultur, in der wirtschaftliche Akteure als unverzichtbarer Bestandteil nationaler Resilienz gelten. Verbindliche Rahmenbedingungen für Eigenvorsorge sowie regelmäßige, realitätsnahe Übungen unter Annahmen von Knappheit, Ausfällen und langanhaltenden Belastungen prägen in beiden Ländern die Praxis. Estland ergänzt diesen Ansatz durch eine konsequent digital gedachte Resilienzstrategie. Staatliche und privatwirtschaftliche IT-Infrastrukturen sind über standardisierte Schnittstellen, kompatible Systeme und klar geregelte Kooperationsmechanismen miteinander verbunden. Strukturierter Informationsaustausch, abgestufte Zugriffs- und Meldewege sowie gemeinsam genutzte digitale Lagebilder sind institutionell verankert und rechtlich abgesichert. Estland versteht Krisenvorsorge, Cyber-Resilienz und Reaktionsfähigkeit als geteilte Verantwortung von Staat, Wirtschaft und Gesellschaft und stellt sie regelmäßig in gemeinsamen Übungen auf die Probe.

Der internationale Vergleich verdeutlicht: Resilienz ist dort wirksam, wo sie als dauerhafte Grundbedingung wirtschaftlichen Handelns verstanden wird und Teil einer gelebten gesamtstaatlichen Sicherheitsvorsorge ist. Dieser Befund soll nicht die strukturellen Unterschiede zwischen kleineren nordischen und baltischen Staaten einerseits und Deutschland andererseits ausblenden – weder hinsichtlich der Bevölkerungsgröße, der föderalen Komplexität noch der historisch bedingten Vorsorgekultur dieser Länder. Dennoch lassen sich aus diesen Beispielen übertragbare Erkenntnisse ableiten, weil sich ihre Wirksamkeit empirisch belegen lässt – nicht hypothetisch für den Verteidigungsfall, sondern messbar im Grundbetrieb und in realen Krisensituationen der vergangenen Jahre. Während der Energiekrise 2022/23 konnte Finnland durch vorbereitete Koordinationsmechanismen zwischen Staat und Wirtschaft binnen weniger Monate ein LNG-Terminal zum Import von Flüssiggas in Betrieb nehmen und damit schneller als vergleichbare Infrastrukturprojekte in anderen europäischen Staaten auf die Versorgungskrise reagieren. Estlands digitale Verwaltungsstrukturen erwiesen sich während der COVID-19-Pandemie als hochverfügbar, während in Deutschland Gesundheitsämter und Schulplattformen vor erheblichen technischen Herausforderungen standen. Die regelmäßigen *Total-Defence*-Übungen Schwedens (Aurora-Reihe 2017, 2020, 2023) integrieren systematisch KRITIS-Unternehmen in realistische Belastungsszenarien und institutionalisieren damit eine Übungspraxis, die in Deutschland erst im Aufbau begriffen ist.

Deutschland verfügt zwar über strategische Konzepte der zivilen Sicherheit, doch bleibt deren praktische Umsetzung bislang fragmentiert. Das zeigt sich beispielhaft an den Rahmenrichtlinien für die Gesamtverteidigung, der Konzeption Zivile Verteidigung und der Nationalen Strategie zum Schutz Kritischer Infrastrukturen. Klare, adressatengerechte Erwartungshaltungen an Unternehmen und eine systematische, flächendeckende Einbindung der Wirtschaft in Vorsorge-, Übungs- und Durchhalteplanungen sind nur punktuell vorhanden. Gerade eine praxisnahe, verbindliche und langfristig angelegte Einbindung der Wirtschaft in staatliche Planungs- und Entscheidungsprozesse ist jedoch entscheidend, um staatliche Handlungsfähigkeit, Versorgungssicherheit und gesellschaftliche Stabilität unter multiplen Druck- oder Krisenbedingungen aufrechtzuerhalten.

Handlungsansätze für Deutschland

Für Deutschland ergibt sich die Notwendigkeit eines Paradigmenwechsels von punktueller Krisenreaktion hin zu kontinuierlicher Vorsorge. Fünf Felder sind dabei von besonderer Bedeutung. **Erstens** gehört Resilienz auf die Managementebene. Strategische Lageanalysen, Stresstests und die Bewertung sicherheitspolitischer Abhängigkeiten sollten regelmäßig erfolgen. Politik und Verwaltung sollten branchenübergreifende Orientierungshilfen auf Basis realistischer Belastungsszenarien bereitstellen – etwa zur Notstromversorgung bei mehrtägigen Stromausfällen, zur Datensicherung bei Cyberangriffen oder zu Personal-engpässen bei Pandemien. Praxisnahe Referenzwerte unterstützen Unternehmen bei der eigenen Risikoabwägung, ohne in ihre Entscheidungsfreiheit einzugreifen. Gleichzeitig sollten Behörden ihre Vorbildfunktion wahrnehmen und Resilienz systematisch stärken – etwa durch klare Zuständigkeiten im Katastrophenschutz und die konsequente Umsetzung der europäischen NIS2-Richtlinie zur Cybersicherheit.

Ein konkretes Beispiel für eine solche unterstützende Maßnahme ist der gemeinsam vom Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) und der Handelskammer Hamburg entwickelte Vorsorgeplan „Krisen, Katastrophen, Konflikte: Wie Sie Ihr Unternehmen in unsicheren Zeiten schützen“ vom Dezember 2025. Er richtet sich insbesondere an kleine und mittlere Unternehmen und übersetzt sicherheitspolitische Anforderungen in praxisnahe Handlungsschritte – von Szenarioanalysen über Notfallorganisation bis hin zu Personal-, Infrastruktur- und Lieferkettenvorsorge. Der Vorsorgeplan verdeutlicht, dass Resilienz nicht erst im Ernstfall entsteht, sondern das Ergebnis systematischer Vorbereitung im Normalbetrieb ist. Solche niedrigschwelligen, anwendungsorientierten Formate sind ein wesentlicher Baustein, um Unternehmen flächendeckend in die gesamtstaatliche Sicherheitsvorsorge einzubinden.

Zweitens sollten Bund, Länder und Kommunen gemeinsam mit Unternehmen regelmäßige Übungen durchführen. Die Szenarien sollten multikausal angelegt sein – etwa die Kombination aus Stromausfall, IT-Störung und Lieferkettenunterbrechung – und gezielt auch kleine und mittlere Unternehmen einbeziehen. Solche Übungen schaffen Handlungssicherheit, Vertrauen und eingespielte Abläufe.

Drittens sollten Maßnahmen zur Stärkung von Krisen- und Kontinuitätsmanagement gezielt den Mittelstand ansprechen. Hier sind die betroffenen Bundesressorts gemeinsam mit ihren Geschäftsbereichsbehörden gefordert, zu unterstützen und praxistaugliche Leitlinien bereitzustellen. Die Bundesländer operationalisieren diese über ihre Innen- und Wirtschaftsressorts. Auf regionaler Ebene übersetzen die Industrie- und Handelskammern, Branchen- und Unternehmensnetzwerke die Maßnahmen in niedrigschwellige Formate. Staatliche Unterstützung sollte primär über Beratung, Weiterbildungsangebote, standardisierte Praxisübungen und – insbesondere für kleine und mittlere Unternehmen – mobile Beratungsteams erfolgen, nicht über zusätzliche Regulierung.

Viertens sollte die Politik die gesellschaftliche Querschnittsfunktion von Unternehmen stärker hervorheben. Maßnahmen wie interne Krisenkommunikation, Cyber-Awareness-Schulungen oder die Unterstützung freiwillig Engagierter stärken nicht nur die betriebliche Stabilität, sondern wirken über den Betrieb hinaus. Beschäftigte tragen im Arbeitsumfeld erworbene Kompetenzen – etwa in IT-Sicherheit oder Krisenorganisation - in ihr privates Umfeld und ehrenamtliches Engagement. Diese Aktivitäten lassen sich an Konzepte der Corporate Social Responsibility anknüpfen und entfalten gesamtgesellschaftliche Wirkung.

Fünftens kann wirtschaftliche Resilienz nur dann wirksam sein, wenn sie institutionell verankert wird. Deutschland sollte – aufbauend auf Erfahrungen anderer Staaten – regionale Koordinierungsplattformen etablieren, die an bestehende Strukturen des Bevölkerungsschutzes anknüpfen. Konkret können dies auf Landesebene regelmäßige Runde Tische zwischen Ministerien, Kammern, Verbänden und Schlüsselunternehmen sein; auf Kreis- und Kommunalebene wären das lokale Sicherheitspartnerschaften mit der Wirtschaft, in denen Verwaltung, ansässige Unternehmen und Einsatzorganisationen quartalsweise Vorsorge- und Wiederanlaufplanung abstimmen. Dort werden gemeinsam Krisenkontakte gepflegt, Kapazitäten erfasst (etwa Notstromaggregate, Kommunikationstechnik), Prioritäten für die Wiederversorgung festgelegt und regelmäßige Übungen durchgeführt.

Dabei bleibt die Abgrenzung zu militärischen Zuständigkeiten bewusst gewahrt. Ziel sollte die kontinuierliche Sicherheitsvorsorge im Alltag sein – die Sicherstellung staatlicher und wirtschaftlicher Funktionsfähigkeit im Frieden und in Krisen, ausdrücklich unterhalb der Schwelle des Spannungsfalls. Entsprechend sollten privatwirtschaftliche Kapazitäten in Bereichen wie Energie, IT, Kommunikation, Logistik und Gesundheitsversorgung frühzeitig und zivil eingebunden werden. Diese zivil-staatliche Kopplung stärkt die Resilienz des Gesamtsystems und bildet einen zentralen Baustein gesamtstaatlicher Sicherheit.

Schlussfolgerungen

Gesamtstaatliche Sicherheitsvorsorge ist ohne die Wirtschaft nicht denkbar. Unternehmen sichern nicht nur Wertschöpfung und Beschäftigung, sondern in Krisen- und Notlagen auch die Grundfunktionen des Gemeinwesens – von Versorgung über Kommunikation bis zur Gesundheitsversorgung. Viele Unternehmen leisten bereits heute aus eigenem Antrieb wichtige Beiträge zur Resilienz: zum Beispiel durch vorausschauendes Risikomanagement, Notfallplanung, Schulung ihrer Mitarbeitenden oder die Unterstützung des Bevölkerungsschutzes. Diese Eigeninitiative ist wertvoll und sollte anerkannt werden.

Es geht nun darum, diese Einzelinitiativen systematisch zu vernetzen, durch klare staatliche Orientierungshilfen zu unterstützen und in eine GSV einzubetten. Deutschland verfügt über strategische Grundlagendokumente, muss die praktische Einbindung der Wirtschaft jedoch konsequenter, verbindlicher und langfristiger gestalten – national wie europäisch. Europäische Initiativen wie die Preparedness Union Strategy und Regulierungen wie NIS2 bieten hierfür einen gemeinsamen Rahmen, den Deutschland aktiv mitgestalten und national umsetzen sollte. Eine an internationalen Beispielen orientierte, auf deutsche Strukturen zugeschnittene GSV stärkt die Resilienz von Staat, Wirtschaft und Gesellschaft gleichermaßen.

Sicherheit in der Wirtschaft und Wirtschaft in der Sicherheit sind die beiden Seiten wirtschaftlicher Resilienz. Nur wenn staatliche und privatwirtschaftliche Akteure frühzeitig koordiniert zusammenarbeiten, bleiben Versorgung, Arbeit und Kommunikation auch in Krisen- und Notlagen ausreichend stabil. Wirtschaftliche Handlungsfähigkeit wird so selbst zum Schutzfaktor für Bevölkerung und Gemeinwesen.

Oberstleutnant i.G. Tina Behnke *ist die Persönliche Referentin des Präsidenten der Bundesakademie für Sicherheitspolitik (BAKS).* ***Leonie Limbach*** *ist aus dem Bundesministerium des Innern als Studien-referentin an die BAKS entsendet. Die Autorinnen geben ihre persönliche Meinung wieder.*

Alle Ausgaben der Arbeitspapiere Sicherheitspolitik sind verfügbar auf:
www.baks.bund.de/de/service/arbeitspapiere-sicherheitspolitik