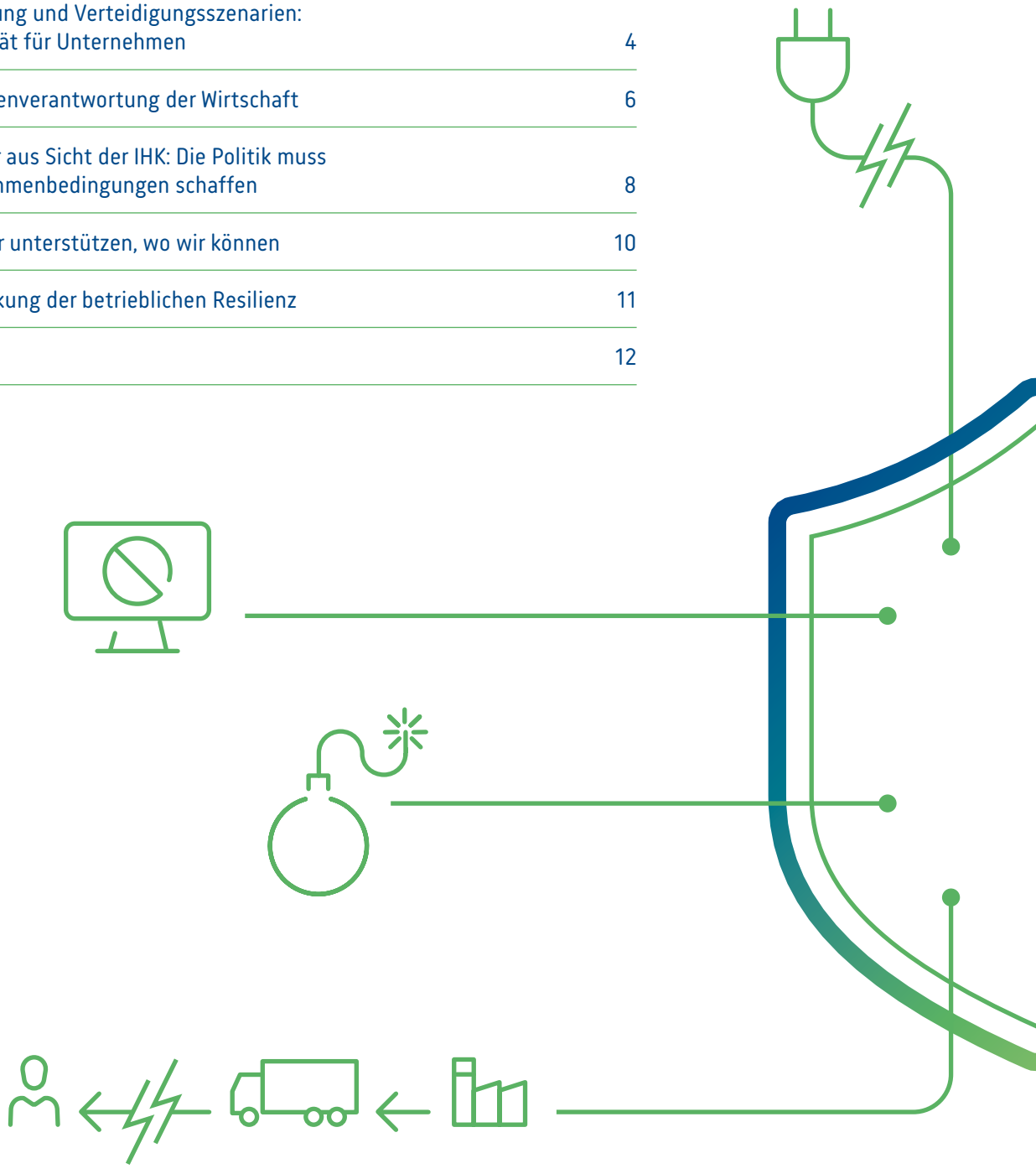
IHK Industrie- und Handelskammer Hannover

#IHK_STANDPUNKTE

Sicherheit und Resilienz

#IHK_STANDPUNKTE

INHALT

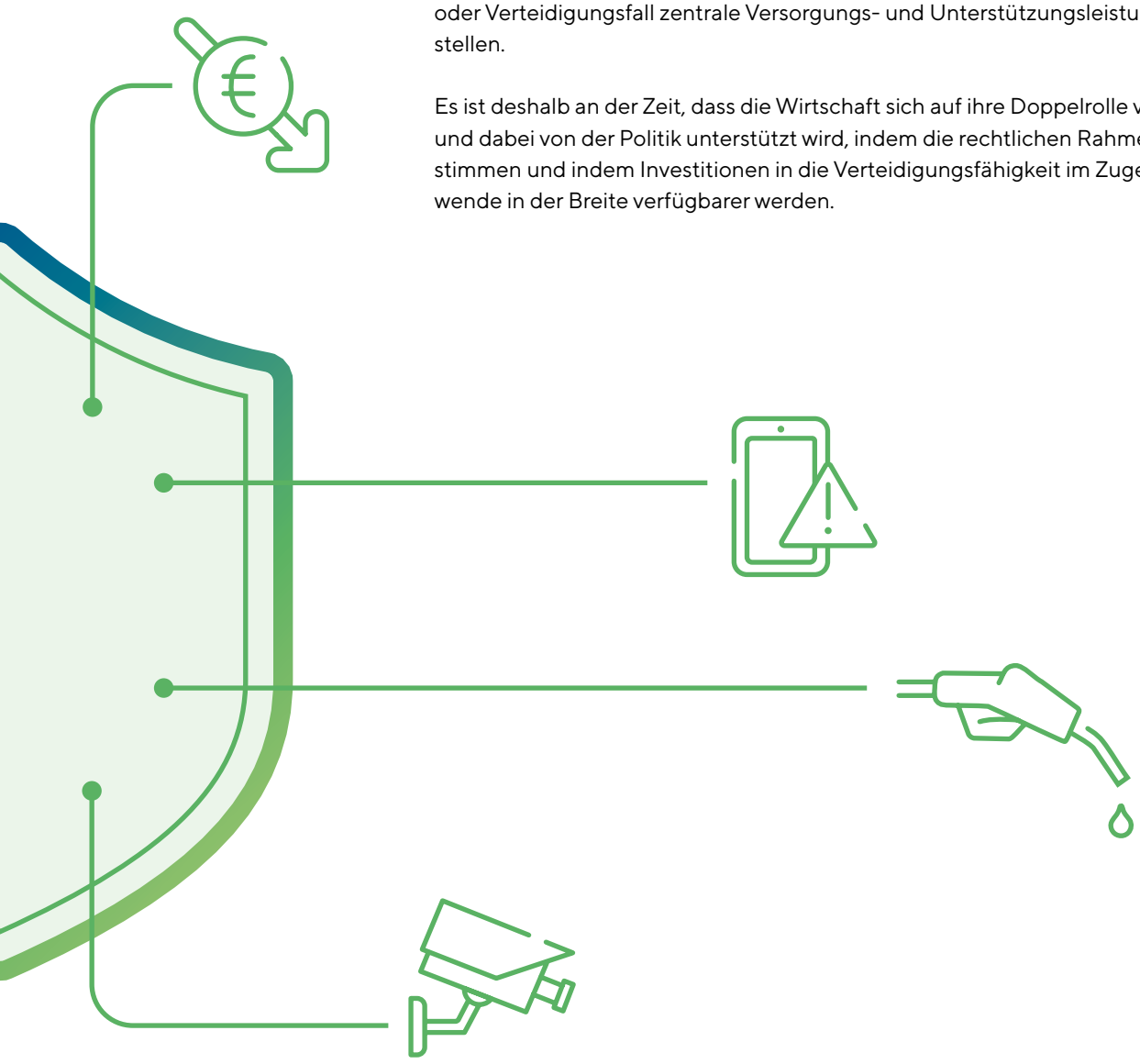


1.
Darum geht es

Die von der Bundesregierung beschlossenen Maßnahmen zur Steigerung des Verteidigungsetats sind wichtige Schritte, um die Verteidigungsfähigkeit Deutschlands zu stärken. Um den Standortfaktor Frieden und die Stabilität in Deutschland in der komplexen sicherheitspolitischen Lage zu sichern, braucht es neben militärischen Fähigkeiten auch eine starke, innovative und resiliente Wirtschaft, die in der Lage ist, unter außergewöhnlichen Bedingungen handlungsfähig zu bleiben.

Denn die Lage „zwischen Frieden und Krieg“ bringt neue Anforderungen an die Wirtschaft mit sich. Unternehmen sehen sich zunehmend mit der Aufgabe konfrontiert, sicherheitsrelevante Risiken zu erkennen, zu bewerten und in ihre strategische Planung einzubeziehen. Sie geraten verstärkt ins Visier feindlich gesinnter Akteure – etwa durch Cyberangriffe, Sabotage oder Spionage. Zudem wird von ihnen erwartet, im Spannungs- oder Verteidigungsfall zentrale Versorgungs- und Unterstützungsleistungen bereitzustellen.

Es ist deshalb an der Zeit, dass die Wirtschaft sich auf ihre Doppelrolle vorbereitet – und dabei von der Politik unterstützt wird, indem die rechtlichen Rahmenbedingungen stimmen und indem Investitionen in die Verteidigungsfähigkeit im Zuge der Zeitenwende in der Breite verfügbarer werden.



2.
Hybride Bedrohung und Verteidigungsszenarien: Eine neue Realität für Unternehmen

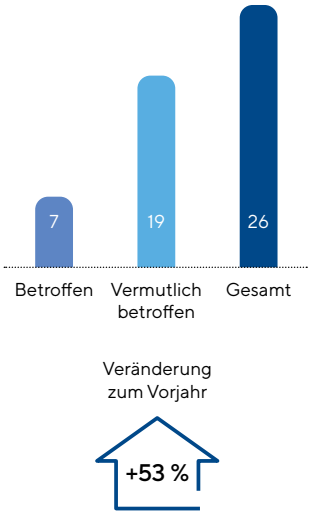
Spätestens seit dem russischen Überfall auf die Ukraine sieht sich Europa, obwohl völkerrechtlich im Frieden, zunehmend mit sogenannten hybriden Angriffen konfrontiert. Diese zeichnen sich durch ihre Vielschichtigkeit aus: Akteure greifen in Form von Cyberattacken auf IT-Systeme, Sabotageakten an Verkehrs- oder Energieinfrastruktur, dem Ausspähen sensibler wirtschaftlicher Informationen oder der gezielten Verbreitung manipulativer Inhalte in sozialen Netzwerken an, um politische, gesellschaftliche und wirtschaftliche Systeme gezielt zu destabilisieren.

Solche Angriffe können regional begrenzt oder flächendeckend erfolgen, kritische Infrastruktur oder militärische Anlagen zum Ziel haben – ihre Auswirkungen auf unternehmerische Abläufe sind jedoch unmittelbar spürbar: Kommunikationswege fallen aus, Produktions- oder Lieferketten werden unterbrochen, sensible Daten gehen verloren, es kommt zu Energieengpässen. All das sind reale Gefahren, die sich mutmaßlich bereits heute ereignen und die Unternehmen in Zukunft noch stärker betreffen können.

Hybride Bedrohungen können isoliert auftreten, jedoch auch der Vorbereitung militärischer Konflikte dienen. Kommt es zu einer militärischen Eskalation, etwa an der Ostflanke der NATO, wird Deutschland zur logistischen Drehscheibe für die Bündnispartner. Bis zu 400.000 Soldatinnen und Soldaten müssten auf Basis des sogenannten Operationsplans Deutschland in kurzer Zeit mitsamt Fahrzeugen und Ausrüstung verlegt werden.

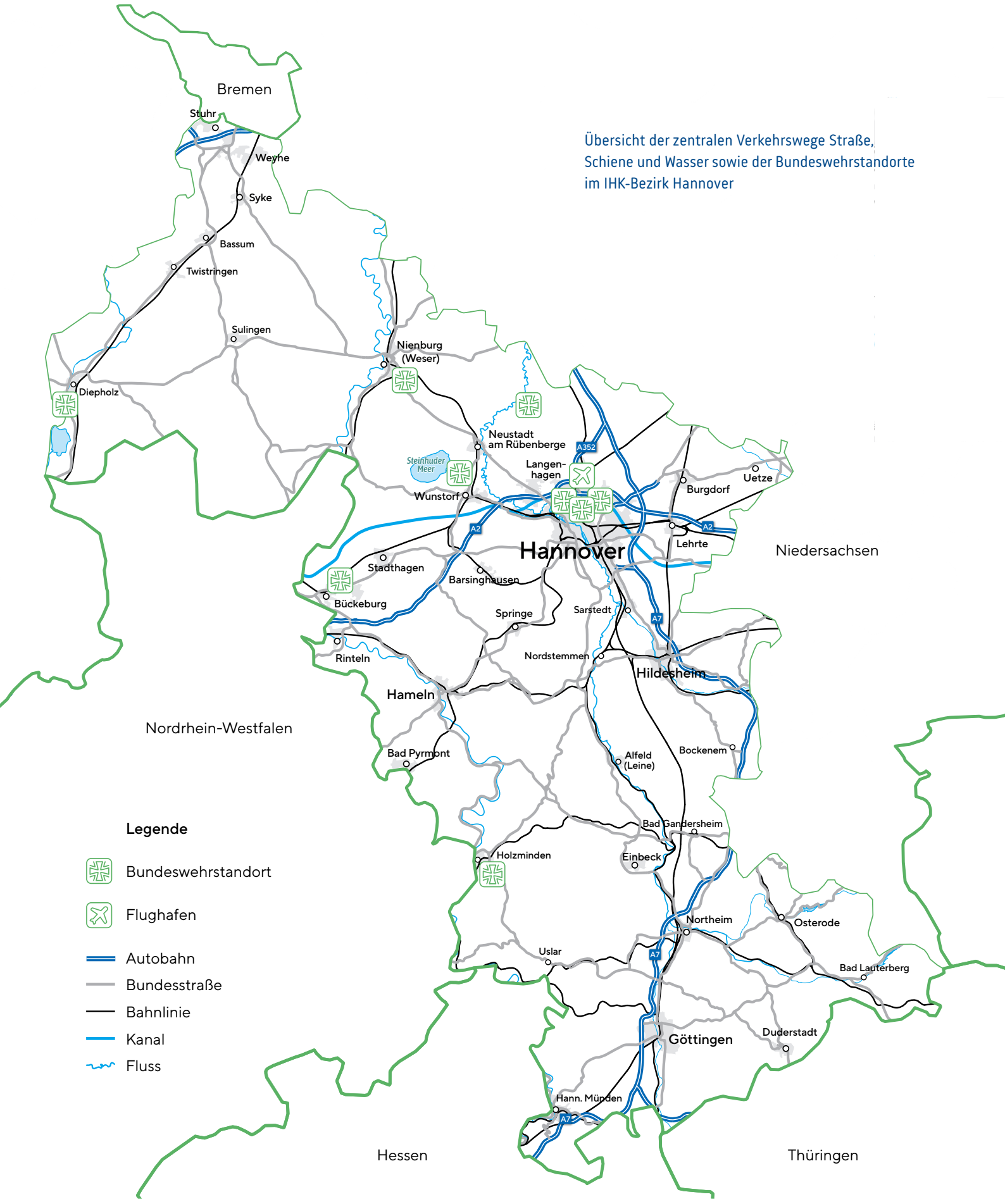
Die IHK-Region Hannover nimmt dabei eine strategische Schlüsselposition ein: Zum einen, aufgrund ihrer geografisch zentralen Lage und der Funktion als bedeutender Verkehrsknotenpunkt für Straße und Schiene im norddeutschen Raum – mit direkter Anbindung an die Seehäfen und das Hinterland. Zum anderen, weil sich hier bedeutende Bundeswehrstandorte wie der Militärflughafen Wunstorf befinden.

Sabotage nimmt zu
(Angaben in %)
26 % aller Unternehmen sind entweder von Sabotage betroffen, oder vermuten dies, ohne es zweifelsfrei nachweisen zu können. Tendenz steigend (+9 Prozentpunkte im Vergleich zu letztem Jahr)



Quelle: Bitkom Research 2024

Der wirtschaftliche Normalbetrieb auf Basis marktwirtschaftlicher Mechanismen bleibt – auch in Krisenzeiten – größtenteils bestehen. Erst wenn der Spannungs- (Art. 80a GG) oder Verteidigungsfall (Art. 115a GG) durch den Bundestag mit einer Zwei-Drittel-Mehrheit festgestellt wird, also ein militärischer Konflikt unmittelbar absehbar ist, können auf Basis der Sicherstellungs- und Vorsorgegesetze darüber hinaus auch Requirierungen und Enteignungen erfolgen. Einzelne Notstandsgesetze können alternativ bereits mit einer einfachen Mehrheit auf Basis des Zustimmungsfalls (Art. 80a Abs. 1 Satz 1) aktiviert werden.


Übersicht der zentralen Verkehrswege Straße, Schiene und Wasser sowie der Bundeswehrstandorte im IHK-Bezirk Hannover
Bremen
Stuhr
Weyhe
Syke
Bassum
Twistringen
Sulingen
Diepholz
Nienburg (Weser)
Neustadt am Rübenberge
Steinhuder Meer
Langen-hagen
A352
Wunstorf
Burgdorf
Uetze
A2
Hannover
Lehrte
Niedersachsen
Stadthagen
Barsinghausen
Bückeburg
Springe
Sarstedt
A7
Rinteln
Nordstemmen
Hildesheim
Hameln
Nordrhein-Westfalen
Bad Pyrmont
Alfeld (Leine)
Bockenem
Bad Gandersheim
Holzminden
Einbeck
Northeim
Osterode
Uslar
Bad Lauterberg
Göttingen
Duderstadt
Hann. Münden
Hessen
Thüringen
Legende
Bundeswehrstandort
Flughafen
Autobahn
Bundesstraße
Bahnlinie
Kanal
Fluss

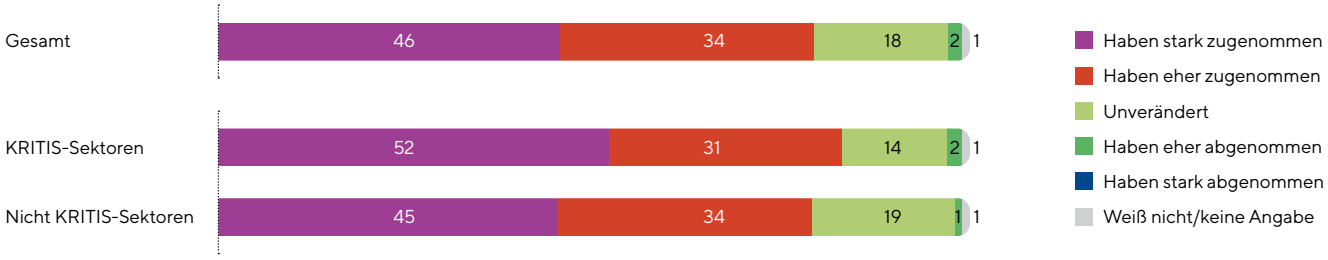
3.
Resilienz als Eigenverantwortung der Wirtschaft

In dieser neuen, komplexen Gefahrenlage zwischen Frieden und Krieg gewinnt die Fähigkeit von Unternehmen, auch unter erschwerten Bedingungen funktionsfähig zu bleiben, an Bedeutung. Resilienz wird zu einem weiteren wichtigen Standortfaktor, der frühzeitige Vorbereitungsmaßnahmen erforderlich macht – als Teil der unternehmerischen Risikovorsorge. Das bedeutet dabei die präventive Vorbereitung, das angemessene Reagieren im Ereignisfall und die Fähigkeit, aus einer Krise zu lernen und gestärkt hervorzugehen.

Hierbei muss klar sein: Es gibt keine staatliche Vollkaskoversicherung. Die Verantwortung für Vorsorge und Schutz liegt primär bei den Unternehmen selbst. Dabei gibt es keine universelle Lösung. Jedes Unternehmen ist anders strukturiert, verfolgt individuelle Geschäftsmodelle und weist einen unterschiedlichen Grad an „Systemrelevanz" auf. Der Weg zur Krisenfestigkeit beginnt entsprechend mit einer ehrlichen Bestandsaufnahme: Ist mein Unternehmen in der Lage, auch unter erhöhten Bedrohungslagen arbeitsfähig zu bleiben? Kann die Handlungsfähigkeit trotz äußerer Störungen gewahrt werden? Denkbare Szenarien reichen von gezielten Angriffen bis hin zu systemischen Ausfällen und beinhalten unter anderem:

- Cyberangriffe,
- Spionage und Sabotage,
- Stromausfälle bis hin zu flächendeckenden Blackouts,
- Ausfall von Kommunikationsmitteln oder der Internetverbindung,
- personelle Engpässe, etwa durch den Wegfall von Reservisten oder ehrenamtlichen Kräften in Feuerwehr, THW und Rettungsdiensten,
- Kraftstoff- und Betriebsstoffmangel,
- Engpässe bei Sicherheitsdiensten oder Werkschutz,
- nationale wie internationale Lieferkettenstörungen,
- branchenspezifische Liquiditätsprobleme infolge externer Krisen.

Cyberangriffe nehmen zu (Angaben in %)
Unternehmen sowohl aus KRITIS-Sektoren (Betreiber kritischer Anlagen wie Energie, Wasser, Verkehr, Gesundheit) als auch sonstige Unternehmen berichten von stark zugenommenen Cyberattacken in den letzten 12 Monaten. Schaden: 178,6 Milliarden Euro.

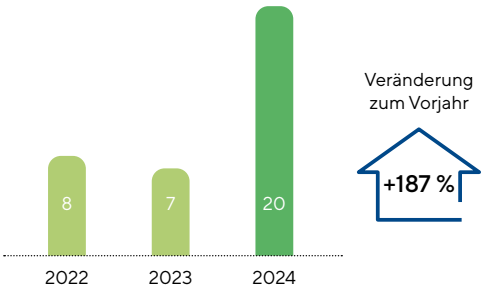


Basis: Alle Unternehmen (n = 1.003) | Abweichungen von 100 Prozent sind rundungsbedingt | Quelle: Bitkom Research 2024

Im Anhang befindet sich vor diesem Hintergrund eine Checkliste zur Orientierung für Unternehmen, um die eigene Resilienz sowohl im Hinblick auf organisatorische Strukturen als auch auf technische und personelle Schutzmaßnahmen zu analysieren und gezielt zu stärken. Die Checkliste ersetzt keine umfassende Risikoanalyse, kann aber als pragmatisches Werkzeug dienen, um erste Sicherheitslücken zu identifizieren und die betrieblichen Vorsorgemaßnahmen weiterzuentwickeln.

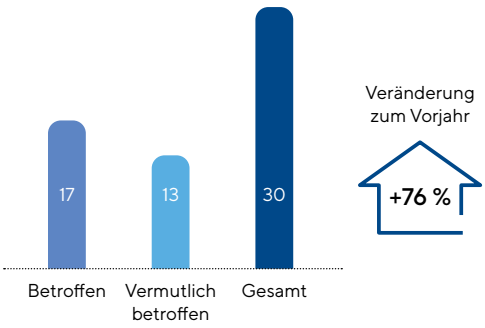
Im Krisen- oder Verteidigungsfall würde entscheidend sein, dass kritische wirtschaftliche Versorgungsleistungen weiterhin funktionieren. Dazu zählen insbesondere die Bereitstellung von Lebensmitteln, Medikamenten, Treibstoffen, Ersatzteilen sowie logistischen Dienstleistungen wie Transport, Lagerung und Verteilung. Fällt auch nur einer dieser Bereiche aus, drohen weitreichende Folgen für Gesellschaft, Verwaltung und Streitkräfte. Deshalb muss der Schutz dieser wirtschaftlichen Kernfunktionen oberste Priorität haben – und zwar als gemeinsame Aufgabe von Unternehmen, Politik und öffentlicher Hand.

Immer häufiger werden hinter Angriffen ausländische Geheimdienste vermutet (Angaben in %)
2024 vermuteten Unternehmen bei 20 % der Cyberangriffe, Sabotageakte oder Spionagefälle ausländische Geheimdienste als Täter. 2022/2023 lag der Anteil noch bei 8 % bzw. 7 %.



Quelle: Bitkom Research 2024

Ausspähungen nehmen zu (Angaben in %)
Bei 30 % aller Unternehmen wurden Anrufe abgehört, oder vermutlich abgehört, ohne es zweifelsfrei nachweisen zu können. Tendenz steigend.



Quelle: Bitkom Research 2024

4.

Handlungsfelder aus Sicht der IHK Hannover: Die Politik muss die richtigen Rahmenbedingungen schaffen

Damit Unternehmen ihre Resilienz systematisch und wirksam stärken können, braucht es ein unterstützendes politisches Umfeld. Gerade in wirtschaftlich herausfordernden Zeiten ist es notwendig, dass Betriebe in der Lage sind, in ihre Krisenfestigkeit zu investieren, ohne dabei ihre Wettbewerbsfähigkeit aufs Spiel zu setzen.

Erste organisatorische Maßnahmen lassen sich mit überschaubarem Aufwand umsetzen. Andere hingegen erfordern je nach Risikolage auch substanzielle Investitionen, beispielsweise in robuste IT-Systeme, Zugangskontrollen, physische Sicherungen, redundante Energie- und Wasserversorgung, alternative Kommunikationswege oder gezielte Vorratshaltung.

Die sicherheitspolitische Zeitenwende ist nicht nur mit neuen Risiken verbunden, sondern kann auch erhebliche wirtschaftliche Perspektiven eröffnen. Die umfassenden öffentlichen Investitionen in Verteidigung, innere Sicherheit und Infrastrukturen haben das Potenzial, neue Märkte und Nachfrage in Bereichen zu schaffen, die bislang im Hintergrund standen. Dadurch entstehen auch Chancen für Unternehmen, die sich frühzeitig strategisch ausrichten. Niedersachsen und insbesondere die IHK-Region Hannover haben hierbei beste Voraussetzungen, eine führende Rolle einzunehmen – sofern die Politik die richtigen Vorzeichen setzt.

RESILIENZANPASSUNGEN FÖRDERN

Resilienz darf kein Privileg jener Unternehmen sein, die allein aufgrund hoher gesetzlicher Schwellenwerte als kritisch oder verteidigungswichtig gelten und deshalb im Fokus besonderer staatlicher Aufmerksamkeit stehen. Auch relevante kleine und mittlere Betriebe müssen in die Lage versetzt werden, ihre Widerstandsfähigkeit gegenüber hybriden Bedrohungen zu stärken. Dafür braucht es gezielte Unterstützung, die Investitionen in Sicherheit als Standortvorsorge anerkennt und die Unternehmen insbesondere bei der praktischen Umsetzung begleitet.

- Sicherheit ESG-kompatibel einordnen: Investitionen in die Versorgungssicherheit oder Notstromversorgung müssen im Rahmen der EU-Taxonomie und nationaler ESG-Kriterien als nachhaltige Maßnahmen gelten, und nicht als Risikopositionen bei der Finanzierung.
- Steuerliche Anreize und gezielte Förderinstrumente setzen: Es benötigt verständliche, digital zugängliche und ohne übermäßige Bürokratie geführte Finanzierungs- und Fördermöglichkeiten, beispielsweise über den Europäischen Fonds für regionale Entwicklung (EFRE) oder die regionale Wirtschaftsförderung.
- Niedrigschwellige Beratung und Umsetzungsunterstützung schaffen: Es braucht gerade für KMU passgenaue Informationsangebote, Schulungen und vernetzte Anlaufstellen.
- Rechtssichere Möglichkeit der Datenabfrage schaffen: Es bedarf einer rechtssicheren und datenschutzkonformen Regelung, die es Organisationen ermöglicht, den Reservistenstatus sowie ehrenamtliche Tätigkeiten ihrer Mitarbeitenden abzufragen.
- Die Polizei mit mehr Befugnissen ausstatten: Hybride Bedrohungen, zum Beispiel Spionagedrohnen, müssen rasch und effektiv bekämpft werden können.
- Sicherheitsüberprüfungen für sensible Stellen beschleunigen.

SCHNELLER WERDEN, INNOVATIONEN UNTERSTÜTZEN, STATT ZU HEMMEN

Innovationsfähigkeit und Geschwindigkeit sind entscheidend, wenn es darum geht, die Sicherheits- und Verteidigungsfähigkeit Deutschlands zu stärken. Der aktuelle Investitionsschub darf nicht an veralteten Vergabeverfahren, langen Genehmigungszeiten oder überbordender Regulierung scheitern. Gerade in sicherheitsrelevanten Sektoren braucht es ein neues Denken: agiler, mutiger, strategischer. Insbesondere Start-ups und Mittelständler müssen mit klaren Perspektiven und fairen Bedingungen eingebunden werden.

- Bürokratie abbauen, Vergabeprozesse erleichtern: Die Vergabe von öffentlichen Aufträgen auf europäischer und nationaler Ebene muss vereinfacht werden, damit Unternehmen mit vertretbarem Aufwand Zugang erhalten. Die Geschwindigkeit muss mit technologischen Entwicklungen und Innovationszyklen Schritt halten. Die sogenannten EU-Omnibus-Verordnungen sind ein erster Schritt in die richtige Richtung.
- „Bauturbo" auf den Weg bringen: Genehmigungen, Flächenausweisungen und industrielle Skalierung müssen beschleunigt werden. Gleichzeitig ist sicherzustellen, dass moderne Produktionsstandards und Umweltauflagen handhabbar bleiben.
- Lieferketten absichern: Kritische Vorprodukte und Komponenten müssen dauerhaft verfügbar sein. Hierfür braucht es resiliente, strategische, internationale Partnerschaften und ggf. diversifizierte Beschaffungswege.

KRITISCHE INFRASTRUKTUR MODERNISIEREN UND SCHÜTZEN

Im Rahmen der umfassenden Investitionen in die Verteidigungsfähigkeit ist eine wehrtaugliche Modernisierung der Verkehrsinfrastruktur, vor allem von Bahnhöfen, Brücken, Schienenverkehrswegen, Autobahnen und weiteren relevanten Verkehrsanlagen, in Höhe von 1,5 Prozent des Bruttoinlandsprodukts bis 2035 vorgesehen..

- Doppelnutzung ermöglichen: Nicht nur militärische Fahrzeuge, sondern auch zivile Lkw und Schwerlasttransporte sollen von verbesserter Infrastruktur profitieren. So wird „toter Stahl" vermieden und ein langfristiger Nutzen für den Wirtschaftsstandort geschaffen.
- Verkehrswege mit der Wirtschaft priorisieren: Gemeinsam mit Unternehmen sollte entschieden werden, welche Verkehrswege zuerst modernisiert werden – orientiert an Bedarfen der Verteidigungsfähigkeit und wirtschaftlicher Relevanz.

CHANCEN FÜR DIE RÜSTUNGSINDUSTRIE

Die sicherheitspolitische Zeitenwende erfordert eine leistungsfähige Rüstungsindustrie. Damit neben den Konzernen insbesondere kleine und mittlere Betriebe zum Aufbau sicherheitsrelevanter Kapazitäten beitragen können, brauchen sie verlässliche Rahmenbedingungen. Ziel muss sein, technologisches Know-how zu nutzen, Marktzugänge zu öffnen und Investitionen langfristig planbar zu machen.

- Verlässliche Verteidigungshaushalte: Langfristige finanzielle Planung über Legislaturperioden hinweg ist nötig, um Unternehmen Investitionssicherheit zu geben und Kapazitäten nachhaltig auszubauen.
- Praxistaugliche Verträge für den Mittelstand: KMU brauchen verlässliche Konditionen, zum Beispiel durch Festpreisverträge. Aufwendige Prüfungen und übermäßige Bürokratie erschweren den Markteintritt.
- Verteidigungsinvestitionen nachhaltig einstufen: Investitionen in verteidigungsrelevante Technologien, etwa Dual-Use-Produkte, sollten im Rahmen der EU-Taxonomie als nachhaltig anerkannt werden.
- Bürokratie abbauen: Vergabe- und Zertifizierungsverfahren müssen schneller und einfacher werden. Die geplanten Neufassungen des Bundeswehrbeschaffungsgesetzes und des Vergabetransformationspakets sind die richtigen Signale.
- Sicherheitsüberprüfungen beschleunigen: Schnellere Überprüfungen für Arbeitnehmer und Arbeitnehmerinnen.
- Kooperationen erleichtern: Europäische und internationale Zusammenarbeit braucht praktikable Rahmenbedingungen – etwa durch interoperable Standards, gemeinsame Plattformen und beschleunigte Verfahren.

DIALOG ZWISCHEN WIRTSCHAFT UND POLITIK STÄRKEN

Die Sicherheitslage erfordert ein abgestimmtes Handeln aller föderalen Ebenen: Sicherheitsbehörden, Zivilschutzorganisationen, Kammern, Verbände, Industrie, Unternehmen und Kommunen benötigen Klarheit darüber, welche Rolle sie im Kontext von Gesamtverteidigung einnehmen, welche Pflichten sie im Krisenfall treffen könnten und wer in welchem Szenario zuständig ist. Wir begrüßen daher die Einrichtung des sogenannten Sicherheitspolitischen Dialogs Niedersachsen, der die wichtigsten Stakeholder der zivilen und militärischen Verteidigung zusammenbringt.

Diese Fragen lassen sich nicht erst im Ereignisfall klären. Sie gehören auf die Tagesordnung eines strukturierten und kontinuierlichen Dialogs zwischen Wirtschaft, Verwaltung und Politik auf Landesebene ebenso wie regional. Dabei ist wichtig:

- Gemeinsames Verständnis für die sicherheitspolitische Bedrohungslage und die Notwendigkeit, resilienzfördernde Maßnahmen zu ergreifen
- Klare Kommunikation zur Rolle der Wirtschaft in der Gesamtverteidigung: Zuständigkeiten, Pflichten und Unterstützungsbedarfe müssen frühzeitig und verständlich benannt werden.
- Strukturierter Austausch mit Landesregierung und kommunalen Akteuren: Ziel ist eine Klärung der Rollenverteilungen und der Kommunikationskanäle in unterschiedlichen Szenarien – von der hybriden Bedrohungsphase bis zum Verteidigungsfall.

5.
Rolle der IHK Hannover:
Wir unterstützen, wo wir können!

Die IHK versteht sich als Mittlerin zwischen Wirtschaft, Staat und Gesellschaft, und unterstützt ihre Mitgliedsunternehmen dabei, ihre Rolle in der Gesamtverteidigung konstruktiv und handhabbar zu gestalten.

Der geplante Ausbau der Bundeswehr auf bis zu 500.000 Einsatzkräfte sowie eine mögliche Rückkehr zur Wehrpflicht werden spürbare Folgen für den zivilen Arbeitsmarkt haben. Reservisten und Ehrenamtliche im Bevölkerungsschutz werden häufiger für Übungen oder Einsätze abgerufen. Gerade kleine und mittlere Unternehmen müssen sich auf personelle Ausfälle einstellen – oft, ohne zu wissen, wer im Betrieb betroffen wäre. Datenschutzrechtliche Hürden verhindern bislang eine rechtssichere Erfassung.

Parallel steigt der Bedarf an Fachkräften in sicherheitsrelevanten zivilen Bereichen, etwa bei IT-Dienstleistern, im Objektschutz oder in der Energieversorgung. Diese zusätzliche Nachfrage trifft auf bereits angespannte Arbeitsmärkte.

Die IHK sensibilisiert Unternehmen für sicherheitspolitische Risiken und informiert über die wirtschaftliche Rolle in hybriden Bedrohungslagen sowie im Spannungs- und Verteidigungsfall. Über Veranstaltungen, Leitfäden und Informationsformate vermittelt sie praxisnahes Wissen zu Notfallplanung, Resilienzmaßnahmen und gesetzlichen Vorgaben. Sie schafft Austauschformate mit Verwaltung, Bundeswehr und Hilfsorganisationen und bringt wirtschaftliche Interessen in politische Prozesse ein, etwa bei Fragen der Wehrpflicht, Reservistenfreistellung oder Ausgestaltung von Förderprogrammen. Auch das Potenzial verteidigungsrelevanter Technologien und Dual-Use-Anwendungen wird gezielt adressiert, mit dem Ziel, Unternehmen beim Einstieg in die Verteidigungsindustrie und bei der Entwicklung innovativer Lösungen zu unterstützen. Im Krisen- und Verteidigungsfall übernimmt die IHK gesetzlich vorgesehene Mitwirkungsaufgaben, etwa bei der Unabkömmlichstellung von Beschäftigten oder der Umsetzung von Sicherstellungsmaßnahmen.

Weitere Informationen
„Wirtschaft und Gesamtverteidigung“:
www.hannover.ihk.de/sicherheitspolitik

Veranstaltungen
zum Thema Sicherheit und Resilienz:
www.hannover.ihk.de/va-sicherheit

Checkliste zur Stärkung der betrieblichen Resilienz

OPERATIVES KRISENMANAGEMENT ETABLIEREN

Bereits mit einfachen organisatorischen Maßnahmen lassen sich wesentliche Grundlagen für die Resilienz im Betrieb schaffen. Viele dieser ersten Schritte erfordern keine großen Investitionen, helfen im Ernstfall aber bei der Aufrechterhaltung zentraler Abläufe.

1. **Eigenes Lagebild erstellen**

- ☑ Ist mein Unternehmen oder Teile meiner Lieferkette ein besonderes Angriffsziel – etwa aufgrund sicherheitsrelevanter Tätigkeiten oder Zulieferfunktionen für kritische Infrastrukturen?
- ☑ Wie könnten sich verschiedene Krisen- und Angriffsszenarien auf das Unternehmen auswirken?

2. **Zuständigkeiten und Prozesse im Unternehmen festlegen**

- ☑ Ist ein/e Krisenverantwortliche/r oder ein Krisenstab benannt, bei der/dem im Ernstfall alle Informationen zusammenlaufen?
- ☑ Gibt es eine erprobte Alarmierungs- und Entscheidungsstruktur?
- ☑ Wie funktioniert die interne und externe Kommunikation im Notfall?
- ☑ Welche Prozesse sind für den Betrieb unerlässlich bzw. kritisch?
- ☑ Existieren Notfallpläne für den Ausfall von Schlüsselpersonal oder wichtigen Anlagen?
- ☑ Gibt es Notrufnummern, um Kolleginnen und Kollegen und wichtigste Kunden im Notfall zu erreichen? Wer ruft wen wann an?
- ☑ Ist dokumentiert, welche Mitarbeitenden über besondere Fähigkeiten für den Notfall verfügen (z. B. Ersthelfer, Fahrer, Sprachkenntnisse)?
- ☑ Liegen Informationen vor, ob Mitarbeitende als Reservisten oder ehrenamtlich in Hilfsdiensten tätig sind und im Krisenfall kurzfristig ausfallen könnten?
- ☑ Welche Unterlagen sollten in Papierform als Backup bereitliegen?

3. **Mit Sicherheitsakteuren vernetzen**

- ☑ Besteht ein funktionierender Kontakt zu lokalen Behörden, etwa zum LKA, Feuerwehr, THW, Wirtschaftsschutz oder IHK?
- ☑ Weiß mein Unternehmen, an wen es sich im Notfall konkret wenden kann?
- ☑ Sind die Ansprechpersonen für Krisenfälle in umliegenden Organisationen und Unternehmen bekannt? Könnte ein Austausch im Quartiersverbund nützlich sein, um Ressourcen zu teilen?

WEITERBILDEN UND REDUNDANZEN AUFBAUEN

Ob, wie und in welchem Umfang zusätzlich in Resilienz investiert wird, muss jedes Unternehmen auf Basis einer individuellen Risikoanalyse selbst entscheiden. Technische, bauliche oder personelle Lösungen können sinnvoll sein, sind aber in der Regel mit Kosten verbunden und erfordern eine strategische Abwägung.

1. **Resiliente Mitarbeitende**

- ☑ Sind die Mitarbeitenden geschult, um Bedrohungen frühzeitig zu erkennen (z. B. Phishing-Mails, verdächtige Personen auf dem Firmengelände)?
- ☑ Sind Hintergrundüberprüfungen für bestimmte Bereiche sinnvoll?

2. **Cybersecurity und IT-Systeme**

- ☑ Besteht Handlungsbedarf bei der IT-Sicherheit?
- ☑ Sind bei der Datensicherung oder der Kommunikation redundante Lösungen von mehreren Anbietern erforderlich?
- ☑ Ist ein Recovery-Plan bei Cyber-Angriffen vorhanden?

3. **Objektschutz**

- ☑ Ist die physische Sicherheit des Unternehmensgeländes von hoher Relevanz?
- ☑ Sind Zugangskontrollen erforderlich?
- ☑ Sind Investitionen in Zäune, Schlösser, Sicherheitspersonal und/oder Videoüberwachung sinnvoll?

4. **Energie**

- ☑ Gibt es alternative Standorte oder eine Versorgung durch mehrere Energieanbieter?
- ☑ Existieren eigene Stromerzeugungskapazitäten (z. B. PV-Anlage, Biogas)?
- ☑ Ist Brennstoff (z. B. Öl, Holz, Gas) in ausreichender Menge vorrätig?
- ☑ Liegt ein Notfallplan für Stromausfälle vor?

DIESE CHECKLISTE MIT HILFREICHEN LINKS FINDEN SIE HIER:

Resilienz ist bei jedem Unternehmen individuell zu definieren. Die Liste dient zur Orientierung und hat keinen Anspruch auf Vollständigkeit.

Industrie- und Handelskammer
Hannover

IMPRESSUM

Herausgeberin
Industrie- und Handelskammer Hannover
Bischofsholer Damm 91 · 30173 Hannover
Tel. 0511 3107-0
www.hannover.ihk.de

Redaktion
Hannes Oswald
Sicherheitspolitik
Tel. 0511 3107-404
hannes.oswald@hannover.ihk.de

Alexander Krause
Klaus Pohlmann
Georg Thomas

Layout und Gesamtherstellung
Frank Loeser grafik+design
Kampstraße 59 · 30629 Hannover
Tel. 0511 668661
info@frank-loeser.com

Bildnachweise
Olga Demina, Adobe Stock (Titel); Bundeswehr/Marco Dorow (S. 7)

Stand: September 2025

Die Broschüre finden Sie online unter **www.hannover.ihk.de/ihk_standpunkte**