FOREUS

KLASSIFIZIERUNG
OFFEN

MONATLICHER LAGE- UND RISIKOBERICHT

EUROPEAN RISK REPORT

AUSGABE JUNI 2026

HERAUSGEBER
Foreus

AUSGABE
Juni 2026

BEOBACHTUNGSZEITRAUM
1. Mai – 31. Mai 2026

00 EXECUTIVE SUMMARY

GEOPOLITISCHE ENTWICKLUNGEN

Der FOREUS European Risk Report, Juni 2026 analysiert die aktuelle europäische Risikolandschaft im Spannungsfeld geopolitischer Unsicherheit, zunehmender Cyber-Bedrohungen, wirtschaftlicher Instabilität sowie gesellschaftlicher und infrastruktureller Verwundbarkeiten. Europa befindet sich weiterhin in einem Umfeld wachsender Fragmentierung, in dem geopolitische Konflikte, hybride Einflussoperationen und wirtschaftliche Spannungen zunehmend direkte Auswirkungen auf Unternehmen, Institutionen und kritische Infrastrukturen haben.

Besonders der Krieg in der Ukraine, globale Machtverschiebungen zwischen westlichen Staaten, Russland und China sowie steigende geopolitische Spannungen beeinflussen Sicherheits- und Wirtschaftsstrukturen innerhalb Europas nachhaltig. Parallel dazu nehmen hybride Bedrohungen wie Desinformationskampagnen, Cyberoperationen und digitale Einflussnahme auf gesellschaftliche und politische Prozesse weiter zu.

Cyber-Bedrohungen entwickeln sich weiterhin zu einem der zentralen Risikofaktoren für Europa. Staatlich unterstützte Hackergruppen, Ransomware-Kampagnen und Angriffe auf kritische Infrastrukturen erhöhen den Druck auf Unternehmen und öffentliche Einrichtungen erheblich. Gleichzeitig führen wirtschaftliche Unsicherheiten, Sanktionen, regulatorische Anforderungen und instabile Lieferketten zu steigenden Risiken für Unternehmen und Investoren.

Darüber hinaus verschärfen gesellschaftliche Polarisierung, politische Radikalisierung und wirtschaftlicher Druck die Herausforderungen für die innere Stabilität europäischer Staaten. Gleichzeitig gewinnen Klima-, Energie- und Infrastrukturthemen zunehmend strategische Bedeutung, da Versorgungssicherheit und Resilienz kritischer Systeme stärker in den Fokus rücken.

Ziel

Der FOREUS European Risk Report verfolgt das Ziel, Entscheidungsträgern ein integriertes Lagebild Europas bereitzustellen, strategische Entwicklungen frühzeitig sichtbar zu machen und die Bedeutung von Resilienz, Frühwarnung und strukturierter Entscheidungsfähigkeit hervorzuheben.

Was die Analyse zeigt

Die Analyse zeigt deutlich, dass Risiken heute nicht mehr isoliert betrachtet werden können. Geopolitische, technologische, wirtschaftliche und gesellschaftliche Entwicklungen greifen zunehmend ineinander und erzeugen komplexe hybride Risikolagen für Staaten, Unternehmen und Institutionen.

01 LAGEÜBERSICHT EUROPA

ÜBERBLICK

Aktuelle Risikolage in Europa

Die sicherheitspolitische Lage in Europa bleibt durch eine Vielzahl komplexer und miteinander vernetzter Risiken geprägt. Geopolitische Spannungen, hybride Bedrohungen und zunehmende Extremwetterereignisse stellen staatliche Institutionen, kritische Infrastrukturen und die Gesellschaft weiterhin vor erhebliche Herausforderungen.

RISIKOÜBERSICHT

Gesamtrisikoindex für Europa

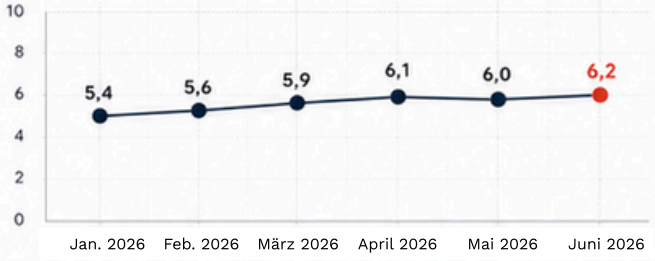
Geopolitische Spannungen	7,5
Terrorismus & Extremismus	6,1
Cyber-Bedrohungen	7,0
Wirtschaftliche Risiken	5,8
Gesellschaftliche Stabilität	5,5
Umwelt- & Klimarisiken	6,3

Skala: 0 (sehr niedrig) – 10 (sehr hoch)

Vergleich zum Vormonat: ↗

RISIKOENTWICKLUNG IM VERLAUF

Gesamtrisikoindex (letzte 6 Monate)



TOP RISIKOTREIBER

Höchste Auswirkungen im Berichtszeitraum

1. **Eskalation des Ukraine-Konflikts**
   Zunehmende militärische Aktivitäten und hybride Angriffe mit potenzieller Ausweitung auf NATO-Territorium.
2. **Zunahme cyber-gestützter Spionage**
   Staatlich unterstützte Akteure intensivieren Angriffe auf kritische Infrastrukturen und Regierungsnetzwerke.
3. **Desinformationskampagnen**
   Gezielte Beeinflussung von Wahlen und öffentlicher Meinung in mehreren EU-Mitgliedstaaten.
4. **Energieversorgung & Abhängigkeiten**
   Anhaltende Instabilität auf Energiemärkten und Abhängigkeiten von nicht-europäischen Lieferanten.
5. **Klimabedingte Naturereignisse**
   Zunehmende Extremwetterlagen gefährden Infrastruktur und Versorgungssicherheit.

ZUR EINORDNUNG

Dieser Bericht basiert auf offenen und vertraulichen Quellen, eigenen Analysen sowie der Zusammenarbeit mit nationalen und internationalen Partnerbehörden. Die Bewertung erfolgt gemäß der FOREUS Risikomethodik.

DETAILANALYSEN

Entwicklungen in ausgewählten Risikodomänen

GEOPOLITISCHE SPANNUNGEN — HOCH ↑

Der Krieg in der Ukraine dauert an, mit intensiven Kämpfen im Osten und verstärkten Raketenangriffen auf kritische Infrastruktur. Spannungen im Westbalkan und im östlichen Mittelmeerraum bleiben erhöht.

TERRORISMUS & EXTREMISMUS — MITTEL-HOCH ↑

Erhöhte Aktivität extremistischer Gruppierungen im Online-Raum. Rückkehrbewegungen aus Konfliktgebieten bleiben ein Risiko. Anschlagsgefahr in urbanen Zentren bleibt bestehen.

CYBER-BEDROHUNGEN — HOCH ↑

Staatlich geförderte Cyberangriffe nehmen zu. Besonders betroffen: Energie, Transport, Gesundheitswesen und Behörden. Ransomware-Angriffe auf kommunale Einrichtungen steigen.

WIRTSCHAFTLICHE RISIKEN — MITTEL →

Wirtschaftliches Wachstum bleibt verhalten. Inflation geht leicht zurück, bleibt jedoch über Zielniveau. Handelskonflikte und Lieferkettenprobleme wirken belastend.

GESELLSCHAFTLICHE STABILITÄT — MITTEL →

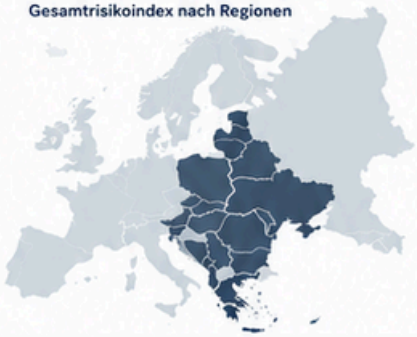
Proteste und gesellschaftliche Spannungen nehmen in einigen Ländern zu, insbesondere im Zusammenhang mit Migration, Inflation und politischen Entwicklungen.

UMWELT- & KLIMARISIKEN — MITTEL-HOCH ↑

Frühsommerliche Hitzewellen und Dürren erhöhen das Risiko für Waldbrände und Ernteausfälle. Überschwemmungen in Nord- und Osteuropa.

REGIONALE RISIKOBEWERTUNG

Gesamtrisikoindex nach Regionen



Osteuropa	7,1
Südosteuropa	6,3
Westeuropa	5,8
Nordeuropa	5,2
Südeuropa	6,0

AUSBLICK

Erwartungen für den kommenden Monat

- Fortgesetzte geopolitische Spannungen mit potenziellen Eskalationen.
- Cyber-Bedrohungen bleiben auf hohem Niveau, gezielte Angriffe zu erwarten.
- Saisonale Klimarisiken können sich regional verschärfen.

02 GEOPOLITIK

GEOPOLITISCHE SPANNUNGEN & HYBRDRIDE EINFLUSSOPERATIONEN IN EUROPA

Europa befindet sich im Jahr 2026 weiterhin in einer Phase zunehmender geopolitischer Unsicherheit und strategischer Fragmentierung. Der anhaltende Krieg in der Ukraine, Spannungen im Nahen Osten sowie die wachsende globale Rivalität zwischen westlichen Demokratien und autoritären Machtzentren wie Russland und China beeinflussen die sicherheitspolitische und wirtschaftliche Stabilität Europas nachhaltig. Parallel dazu verschiebt sich die moderne Konfliktführung zunehmend in hybride Räume, in denen klassische militärische Mittel mit digitalen, wirtschaftlichen und gesellschaftlichen Einflussoperationen kombiniert werden.

Besonders auffällig ist die steigende Anzahl koordinierter Desinformationskampagnen, welche gezielt darauf abzielen, gesellschaftliche Polarisierung zu verstärken, Vertrauen in demokratische Institutionen zu schwächen und politische Entscheidungsprozesse zu beeinflussen. Soziale Medien, alternative Nachrichtenplattformen und KI-generierte Inhalte werden verstärkt genutzt, um Narrative zu verbreiten, öffentliche Debatten zu manipulieren und Unsicherheit innerhalb europäischer Gesellschaften zu erzeugen. Gleichzeitig nehmen Einflussoperationen gegen kritische Infrastruktur, politische Institutionen und strategische Unternehmen zu.

Darüber hinaus zeigt sich, dass geopolitische Konflikte zunehmend direkte Auswirkungen auf europäische Unternehmen haben. Sanktionen, Handelsrestriktionen, instabile Lieferketten sowie politische Spannungen zwischen internationalen Akteuren führen zu erhöhten wirtschaftlichen Risiken und strategischer Unsicherheit.

Besonders betroffen sind energieabhängige Industrien, Technologieunternehmen, Logistiknetzwerke sowie Betreiber kritischer Infrastruktur.

Auch Cyberoperationen entwickeln sich zunehmend zu einem geopolitischen Instrument staatlicher und staatsnaher Akteure. Angriffe auf Energieversorger, öffentliche Einrichtungen, Kommunikationssysteme und industrielle Netzwerke werden verstärkt als Mittel strategischer Destabilisierung eingesetzt. Parallel dazu steigt die Gefahr verdeckter Einflussnahme auf demokratische Prozesse, Wahlen und gesellschaftliche Meinungsbildung innerhalb Europas.

Die geopolitische Lage verdeutlicht zunehmend, dass sich Europa nicht mehr ausschließlich mit klassischen Sicherheitsbedrohungen auseinandersetzen muss, sondern mit einer hybriden Form globaler Einflussnahme, bei der Information, Technologie, Wirtschaft und gesellschaftliche Stabilität unmittelbar miteinander verbunden sind. Resilienz, strategische Frühwarnung und die Fähigkeit, komplexe Entwicklungen frühzeitig zu erkennen und einzuordnen, gewinnen dadurch für Staaten, Unternehmen und Institutionen erheblich an Bedeutung.

> **ANALYTISCHE EINSCHÄTZUNG**
> Aus analytischer Sicht zeigt sich eine deutliche Professionalisierung der globalen Cyberbedrohungslage. Angreifer agieren zunehmend arbeitsteilig, international vernetzt und wirtschaftlich organisiert. Besonders kritisch ist dabei die Entwicklung hin zu hochkomplexen Multi-Stage-Angriffen, bei denen klassische Cyberoperationen mit wirtschaftlicher Einflussnahme, Informationsoperationen und hybriden Destabilisierungsmaßnahmen kombiniert werden.

WIRTSCHAFTLICHE RISIKOFAKTOREN

Ein wesentlicher wirtschaftlicher Risikofaktor ergibt sich aus der steigenden Verwundbarkeit europäischer Wertschöpfungsketten. Supply-Chain-Angriffe führen dazu, dass einzelne kompromittierte Dienstleister oder Softwareanbieter erhebliche Auswirkungen auf zahlreiche Unternehmen gleichzeitig auslösen können. Dadurch entstehen systemische Risiken, die weit über den eigentlichen Angriff hinausreichen und ganze Branchen oder kritische Versorgungsstrukturen betreffen können. Die potenziellen wirtschaftlichen Schäden umfassen dabei nicht nur unmittelbare Betriebsunterbrechungen, sondern auch Produktionsausfälle, Reputationsschäden, regulatorische Sanktionen, Rechtsstreitigkeiten sowie langfristige Vertrauensverluste gegenüber Kunden, Investoren und Partnern.

03 CYBER-BEDROHUNGEN

CYBER-BEDROHUNGEN GEGEN UNTERNEHMEN & KRITISCHE INFRASTRUKTUR

Cyberangriffe zählen weiterhin zu den bedeutendsten Bedrohungen für Staaten, Unternehmen und kritische Infrastrukturen innerhalb Europas. Die digitale Vernetzung wirtschaftlicher und gesellschaftlicher Prozesse schafft zwar erhebliche Effizienzgewinne, erhöht jedoch gleichzeitig die Verwundbarkeit gegenüber staatlich unterstützten Hackergruppen, organisierten Cyberkriminellen und hybriden Angriffsoperationen. Besonders betroffen sind Energieversorger, Gesundheitswesen, Transport- und Logistikunternehmen, Finanzinstitute sowie öffentliche Verwaltungseinrichtungen.

Im Verlauf der vergangenen Monate konnte europaweit eine deutliche Zunahme komplexer Cyberoperationen beobachtet werden. Neben klassischen Ransomware-Angriffen gewinnen insbesondere Supply-Chain-Angriffe an Bedeutung. Dabei werden nicht primär die eigentlichen Zielunternehmen attackiert, sondern externe Dienstleister, Softwareanbieter oder Partnerunternehmen kompromittiert, um indirekten Zugriff auf kritische Systeme und sensible Daten zu erhalten. Diese Form der Angriffsmethodik erschwert die frühzeitige Erkennung erheblich und erhöht die potenziellen Auswirkungen entlang gesamter Wertschöpfungsketten.

Parallel dazu nehmen staatlich unterstützte Cyberoperationen weiter zu. Insbesondere geopolitische Spannungen führen dazu, dass Cyberangriffe verstärkt als strategisches Instrument genutzt werden, um wirtschaftlichen Schaden zu verursachen, Informationen zu beschaffen oder kritische Infrastrukturen gezielt zu destabilisieren. Europäische Behörden und Unternehmen sehen sich dabei zunehmend professionellen Angreifern gegenüber, die langfristig operieren, moderne Verschleierungstechniken einsetzen und hybride Ansätze verfolgen, welche Cyberoperationen mit Desinformation und wirtschaftlichem Druck kombinieren. Besonders kritisch bleibt die Bedrohungslage im Bereich kritischer Infrastruktur. Energieversorgung, Wasserwerke, Kommunikationsnetze und öffentliche Verwaltungsstrukturen stellen attraktive Ziele dar, da erfolgreiche Angriffe direkte Auswirkungen auf Versorgungssicherheit, öffentliche Ordnung und gesellschaftliche Stabilität haben können. Gleichzeitig zeigt sich, dass viele Betreiber kritischer Systeme weiterhin mit veralteter Infrastruktur, fehlender Segmentierung sowie unzureichender Cyber-Resilienz konfrontiert sind.

Auch mittelständische Unternehmen geraten zunehmend in den Fokus von Angreifern. Oft fehlen ausreichende Sicherheitsmaßnahmen, spezialisierte Fachkräfte oder strukturierte Krisen- und Incident-Response-Prozesse. Dadurch entstehen erhebliche Risiken für Datenverlust, Betriebsunterbrechungen, Reputationsschäden und wirtschaftliche Folgekosten. Besonders problematisch ist dabei die steigende Professionalisierung krimineller Gruppierungen, die Ransomware-as-a-Service-Modelle, KI-gestützte Angriffsmethoden sowie automatisierte Social-Engineering-Kampagnen einsetzen.

Darüber hinaus entwickeln sich Cyberangriffe zunehmend zu einem geopolitischen Machtinstrument. Staaten nutzen digitale Operationen verstärkt zur strategischen Informationsbeschaffung, wirtschaftlichen Einflussnahme und Destabilisierung geopolitischer Gegner. Unternehmen und Institutionen befinden sich dadurch zunehmend an der Schnittstelle zwischen wirtschaftlicher Tätigkeit und geopolitischer Konfliktdynamik.

ANALYTISCHE EINSCHÄTZUNG

Aus analytischer Sicht zeigt sich eine deutliche Professionalisierung der globalen Cyberbedrohungslage. Angreifer agieren zunehmend arbeitsteilig, international vernetzt und wirtschaftlich organisiert. Besonders kritisch ist dabei die Entwicklung hin zu hochkomplexen Multi-Stage-Angriffen, bei denen klassische Cyberoperationen mit wirtschaftlicher Einflussnahme, Informationsoperationen und hybriden Destabilisierungsmaßnahmen kombiniert werden.

WIRTSCHAFTLICHE RISIKOFAKTOREN

Ein wesentlicher wirtschaftlicher Risikofaktor ergibt sich aus der steigenden Verwundbarkeit europäischer Wertschöpfungsketten. Supply-Chain-Angriffe führen dazu, dass einzelne kompromittierte Dienstleister oder Softwareanbieter erhebliche Auswirkungen auf zahlreiche Unternehmen gleichzeitig auslösen können. Dadurch entstehen systemische Risiken, die weit über den eigentlichen Angriff hinausreichen und ganze Branchen oder kritische Versorgungsstrukturen betreffen können. Die potenziellen wirtschaftlichen Schäden umfassen dabei nicht nur unmittelbare Betriebsunterbrechungen, sondern auch Produktionsausfälle, Reputationsschäden, regulatorische Sanktionen, Rechtsstreitigkeiten sowie langfristige Vertrauensverluste gegenüber Kunden, Investoren und Partnern.

04 WIRTSCHAFTLICHE UNSICHERHEIT

WIRTSCHAFTLICHE UNSICHERHEIT, SANKTIONEN & Lieferkettenrisiken

Die europäische Wirtschaft befindet sich weiterhin in einem Umfeld erhöhter Unsicherheit und struktureller Belastung. Inflation, geopolitische Spannungen, internationale Handelskonflikte sowie zunehmende regulatorische Anforderungen beeinflussen die Stabilität zahlreicher Branchen und verändern strategische Entscheidungsprozesse innerhalb Europas nachhaltig. Unternehmen sehen sich dabei nicht nur mit wirtschaftlichem Druck konfrontiert, sondern zunehmend auch mit geopolitischen und sicherheitsrelevanten Risiken entlang globaler Wertschöpfungs- und Lieferketten.

Besonders deutlich zeigt sich diese Entwicklung im Zusammenhang mit internationalen Sanktionen und Exportkontrollen. Geopolitische Konflikte zwischen westlichen Staaten, Russland, China sowie weiteren regionalen Akteuren führen zu einer zunehmenden Fragmentierung internationaler Handelsstrukturen. Sanktionen entwickeln sich dabei immer stärker zu einem strategischen Instrument wirtschaftlicher Einflussnahme und betreffen mittlerweile nicht mehr ausschließlich einzelne Staaten, sondern zunehmend Unternehmen, Technologien, Finanzstrukturen und kritische Rohstoffketten.

Vor allem europäische Unternehmen geraten dadurch unter erheblichen Anpassungsdruck. Regulatorische Anforderungen im Bereich Sanktionen, Dual-Use-Güter, Lieferkettensorgfaltspflichten sowie internationale Compliance-Vorgaben nehmen kontinuierlich zu. Gleichzeitig steigt die Komplexität globaler Lieferketten. Viele Unternehmen verfügen nur eingeschränkt über Transparenz hinsichtlich wirtschaftlicher Eigentümerstrukturen, Zwischenhändler oder geopolitischer Risiken innerhalb ihrer Liefernetzwerke.

Besonders kritisch bleibt Europas Abhängigkeit von strategischen Rohstoffen, Technologien und internationalen Produktionsstandorten. Lieferengpässe, geopolitische Spannungen und wirtschaftliche Unsicherheiten können innerhalb kurzer Zeit erhebliche Auswirkungen auf Versorgungssicherheit, Produktionsfähigkeit und Preisentwicklung haben. Besonders betroffen sind Branchen wie Energie, Industrie, Pharma, Verteidigung und Halbleitertechnologie.

Zusätzlich erhöhen Inflation, volatile Energiepreise und regulatorische Anforderungen den Druck auf europäische Unternehmen. Investitionsentscheidungen werden zunehmend von geopolitischen Entwicklungen, internationalen Abhängigkeiten sowie Compliance- und Reputationsrisiken beeinflusst.
Gleichzeitig nehmen wirtschaftliche Einflussoperationen, Lieferkettenangriffe und regulatorische Risiken im Bereich Dual-Use-Technologien weiter zu. Unternehmen müssen ihre Resilienz daher deutlich breiter denken als noch vor wenigen Jahren.

ANALYTISCHE EINSCHÄTZUNG

Aus analytischer Sicht befindet sich Europa in einer Phase zunehmender geoökonomischer Fragmentierung. Internationale Handelsbeziehungen werden verstärkt von strategischen Interessen, Sicherheitsüberlegungen und geopolitischen Machtverschiebungen beeinflusst.

WIRTSCHAFTLICHE RISIKOFAKTOREN

Ein wesentlicher wirtschaftlicher Risikofaktor ergibt sich aus der zunehmenden Instabilität globaler Lieferketten. Produktionsverlagerungen, Handelsrestriktionen, Exportkontrollen, Sanktionen sowie politische Spannungen zwischen internationalen Machtblöcken führen zu steigenden Beschaffungskosten, längeren Lieferzeiten und wachsender Unsicherheit bei Investitions- und Produktionsentscheidungen.

Besonders betroffen sind energieintensive Industrien, Technologieunternehmen, pharmazeutische Versorgungsketten, Verteidigungsindustrien sowie Betreiber kritischer Infrastruktur. Die Folge sind sinkende Planbarkeit, erhöhte Kapitalbindung sowie steigender wirtschaftlicher Druck auf europäische Unternehmen.

05 GESELLSCHAFTLICHE POLARISIERUNG

GESELLSCHAFTLICHE POLARISIERUNG & INNERE STABILITÄT EUROPAS

Europa sieht sich weiterhin mit zunehmender gesellschaftlicher Polarisierung und wachsenden Spannungen innerhalb demokratischer Systeme konfrontiert. Migration, wirtschaftlicher Druck, steigende Lebenshaltungskosten sowie politische Unsicherheit führen in mehreren europäischen Staaten zu einer spürbaren Verschärfung gesellschaftlicher Konflikte. Parallel dazu nehmen Protestbewegungen, politische Radikalisierung und digitale Einflusskampagnen weiter zu.

Besonders soziale Medien und digitale Plattformen verstärken gesellschaftliche Spannungen zunehmend. Emotionale Debatten, Desinformation und algorithmisch verstärkte Polarisierung beeinflussen öffentliche Diskurse und erschweren sachliche politische Auseinandersetzungen. Gleichzeitig wächst in Teilen der Bevölkerung das Misstrauen gegenüber staatlichen Institutionen, politischen Entscheidungsträgern und etablierten Medien.

Auch wirtschaftliche Unsicherheit trägt zur gesellschaftlichen Belastung bei. Inflation, Wohnraumprobleme, Energiepreise sowie Zukunftsängste erhöhen den sozialen Druck innerhalb vieler europäischer Gesellschaften. In mehreren Staaten führen diese Entwicklungen zu verstärkten Protesten, politischer Fragmentierung und einer zunehmenden Polarisierung zwischen unterschiedlichen gesellschaftlichen Gruppen.

Darüber hinaus beobachten europäische Sicherheitsbehörden eine steigende Aktivität extremistischer und radikalisierter Akteure. Sowohl politisch motivierter Extremismus als auch digitale Radikalisierungsprozesse entwickeln sich zunehmend zu einer Herausforderung für öffentliche Sicherheit und gesellschaftliche Stabilität.

Besonders hybride Einflussoperationen aus dem Ausland nutzen bestehende Spannungen gezielt aus, um demokratische Systeme weiter zu destabilisieren und gesellschaftliche Unsicherheit zu verstärken.

Die innere Stabilität Europas entwickelt sich dadurch zunehmend zu einem strategischen Sicherheitsfaktor. Gesellschaftliche Resilienz, Vertrauen in Institutionen sowie die Fähigkeit, mit Krisen und Unsicherheiten umzugehen, gewinnen erheblich an Bedeutung. Staaten und Unternehmen müssen sich zunehmend auf ein Umfeld einstellen, in dem gesellschaftliche Entwicklungen direkte Auswirkungen auf wirtschaftliche Stabilität, politische Entscheidungsprozesse und öffentliche Sicherheit haben können.

> **ANALYTISCHE EINSCHÄTZUNG**
> Aus analytischer Sicht lässt sich beobachten, dass hybride Einflussoperationen zunehmend professioneller, technologisch komplexer und strategisch koordinierter durchgeführt werden. Staatliche und staatsnahe Akteure nutzen digitale Plattformen, soziale Medien, KI-generierte Inhalte, alternative Informationsnetzwerke sowie gezielte Desinformationskampagnen, um gesellschaftliche Polarisierung zu verstärken, Unsicherheit zu erzeugen und öffentliche Debatten gezielt zu beeinflussen.

WIRTSCHAFTLICHE RISIKOFAKTOREN

Ein wesentlicher wirtschaftlicher Risikofaktor ergibt sich aus der steigenden Volatilität gesellschaftlicher und politischer Rahmenbedingungen. Unternehmen sehen sich zunehmend mit Reputationsrisiken, regulatorischer Unsicherheit, gesellschaftlichem Druck sowie potenziellen Protest- und Destabilisierungsdynamiken konfrontiert.

Besonders betroffen sind Unternehmen mit hoher öffentlicher Sichtbarkeit, kritischer Infrastruktur, internationaler Vernetzung oder gesellschaftspolitischer Relevanz. Bereits einzelne Desinformationskampagnen oder digitale Einflussoperationen können erhebliche Auswirkungen auf Marktwert, Kundenvertrauen oder operative Stabilität entfalten.

06 KLIMA & ENERGIE

KLIMA-, ENERGIE- & INFRASTRUKTURRESILIENZ

Europa steht zunehmend vor langfristigen Herausforderungen im Zusammenhang mit Klimaentwicklung, Energieversorgung und der Stabilität kritischer Infrastrukturen. Extreme Wetterereignisse, geopolitische Spannungen sowie die hohe Abhängigkeit von komplexen Versorgungs- und Energiesystemen erhöhen den Druck auf Staaten, Unternehmen und Betreiber kritischer Infrastruktur erheblich. Gleichzeitig wächst die Gefahr, dass klimatische, technische und geopolitische Risiken immer stärker miteinander verbunden werden.

Besonders Hitzewellen, Überschwemmungen, Dürren und extreme Wetterlagen führen bereits heute in mehreren europäischen Regionen zu Belastungen für Energieversorgung, Transportnetzwerke und öffentliche Infrastruktur. Schäden an Straßen, Bahnverbindungen, Kommunikationssystemen sowie Strom- und Wasserversorgung können innerhalb kurzer Zeit erhebliche wirtschaftliche und gesellschaftliche Auswirkungen verursachen. Gleichzeitig steigen die Kosten für Schutzmaßnahmen, Instandhaltung und infrastrukturelle Anpassungen kontinuierlich an.

Auch die europäische Energieversorgung bleibt ein zentraler Risikofaktor. Geopolitische Spannungen, internationale Abhängigkeiten und volatile Energiemärkte beeinflussen Versorgungssicherheit und Preisstabilität nachhaltig. Besonders kritische Infrastrukturen wie Energieversorger, Stromnetze, Wasserwerke und Kommunikationssysteme geraten zunehmend in den Fokus geopolitischer Spannungen sowie potenzieller Cyber- und Sabotageoperationen. Parallel dazu wächst die Sorge vor infrastrukturellen Verwundbarkeiten innerhalb Europas. Blackout-Risiken, technische Ausfälle, Cyberangriffe sowie physische Angriffe auf kritische Versorgungssysteme stellen erhebliche Herausforderungen für öffentliche Sicherheit und wirtschaftliche Stabilität dar.

Parallel dazu wächst die Sorge vor infrastrukturellen Verwundbarkeiten innerhalb Europas. Blackout-Risiken, technische Ausfälle, Cyberangriffe sowie physische Angriffe auf kritische Versorgungssysteme stellen erhebliche Herausforderungen für öffentliche Sicherheit und wirtschaftliche Stabilität dar. Viele europäische Staaten und Unternehmen stehen vor der Aufgabe, ihre Resilienz gegenüber komplexen Krisenszenarien deutlich zu erhöhen.

Darüber hinaus zeigt sich zunehmend, dass Klima-, Energie- und Infrastrukturthemen nicht mehr isoliert betrachtet werden können. Versorgungssicherheit, gesellschaftliche Stabilität, wirtschaftliche Leistungsfähigkeit und geopolitische Entwicklungen sind eng miteinander verbunden. Die Fähigkeit, kritische Systeme resilient zu gestalten und auch in Krisensituationen funktionsfähig zu halten, entwickelt sich damit zu einem strategischen Sicherheitsfaktor für Europa.

ANALYTISCHE EINSCHÄTZUNG

Aus analytischer Sicht entsteht dadurch eine neue Form systemischer Verwundbarkeit. Kritische Infrastrukturen sind heute hochgradig miteinander vernetzt und voneinander abhängig. Ausfälle einzelner Systeme können dadurch erhebliche Kettenreaktionen auslösen und weitreichende Auswirkungen auf Versorgungssicherheit, öffentliche Ordnung, industrielle Produktion sowie gesellschaftliche Stabilität entfalten.

WIRTSCHAFTLICHE RISIKOFAKTOREN

Ein wesentlicher wirtschaftlicher Risikofaktor ergibt sich aus der zunehmenden Wahrscheinlichkeit infrastruktureller Unterbrechungen und deren potenziellen Auswirkungen auf Produktion, Logistik und Versorgungsketten. Bereits kurzfristige Ausfälle von Energie- oder Kommunikationssystemen können erhebliche wirtschaftliche Schäden verursachen, Produktionsprozesse unterbrechen, Lieferketten destabilisieren und kritische Dienstleistungen beeinträchtigen. Besonders exponiert sind energieintensive Industrien, Gesundheitswesen, Telekommunikation, Finanzsysteme, Transport- und Logistiknetzwerke sowie Betreiber kritischer Infrastruktur.

07 STRATEGIE ABLEITUNGEN

STRATEGISCHE ABLEITUNGEN & HANDLUNGSEMPFEHLUNGEN FÜR UNTERNEHMEN

1. Cyber- & Krisenresilienz professionalisieren
Unternehmen müssen ihre Cyber-Resilienz, Krisenkommunikation und Incident-Response-Strukturen kontinuierlich weiterentwickeln. Moderne Bedrohungen erfordern schnelle Entscheidungsfähigkeit sowie klar definierte Krisen- und Eskalationsprozesse.

2. Lieferketten & geopolitische Risiken laufend überwachen
Internationale Lieferketten, Geschäftspartner und geopolitische Entwicklungen sollten regelmäßig auf potenzielle Risiken, Abhängigkeiten und regulatorische Veränderungen überprüft werden.

3. Strategische Frühwarn- und Intelligence-Fähigkeiten aufbauen
Die Fähigkeit, Risiken frühzeitig zu erkennen und Entwicklungen strategisch einzuordnen, wird zunehmend zu einem entscheidenden Wettbewerbsfaktor für Unternehmen und Institutionen.

4. Reputations- & Informationsschutz stärken
Digitale Reputation, Informationssicherheit und der Schutz sensibler Unternehmensdaten gewinnen zunehmend an Bedeutung. Unternehmen sollten Monitoring- und Schutzmechanismen im Bereich Informations- und Reputationsrisiken professionalisieren.

5. Resilienz als strategischen Wettbewerbsfaktor verstehen
Die Fähigkeit, auch unter Unsicherheit stabil, handlungsfähig und anpassungsfähig zu bleiben, entwickelt sich zunehmend zu einem entscheidenden Erfolgs- und Sicherheitsfaktor innerhalb Europas.

6. Kritische Infrastruktur & operative Kernprozesse absichern
Geschäftskritische Systeme, Kommunikationswege und operative Prozesse sollten regelmäßig auf technische, organisatorische und physische Verwundbarkeiten überprüft werden.

7. Gesellschaftliche & regulatorische Entwicklungen stärker berücksichtigen
Politische Polarisierung, neue Regulierungen und gesellschaftliche Veränderungen können direkte Auswirkungen auf Unternehmen, Märkte und Investitionsentscheidungen haben.

8. Energie- & Versorgungssicherheit strategisch bewerten
Unternehmen sollten ihre Abhängigkeiten im Bereich Energie, Rohstoffe und internationale Versorgungsketten analysieren und alternative Szenarien vorbereiten.

9. Entscheidungsgeschwindigkeit in Krisensituationen erhöhen
In komplexen Krisenlagen wird die Fähigkeit, schnell und strukturiert Entscheidungen treffen zu können, zu einem zentralen Erfolgsfaktor für Unternehmen und Institutionen.

10. Technologie, Sicherheit & Strategie stärker verbinden
Unternehmen müssen technologische Entwicklungen, Sicherheitsaspekte und strategische Unternehmensführung zunehmend integriert betrachten, um langfristig resilient und wettbewerbsfähig zu bleiben.

HYBRID INTELLIGENCE SERVICE

EUROPEAN RISK REPORT

Ausgabe Juni 2026

KONTAKT & PRESSEANFRAGEN

PRESSEANFRAGEN
public@foreusgroup.com

WEB
www.foreusgroup.com

HERAUSGEBER
Foreus Group Europe GmbH