zukunftsInstitut

# KI-Souveränität

## Strategische Handlungsoptionen für Unternehmen in DACH und Europa

**WHITEPAPER**

**GEOPOLITIK | KRITISCHE INFRASTRUKTUR | KI**

ZUKUNFTSINSTITUT GMBH, JUNI 2026

# Alles, was wir mit KI nutzen, ist zugleich angreifbar – und erzeugt damit eine symmetrische Verwundbarkeit.

**Zukunftsinstitut Megatrendstudie Sicherheit**

Zur Megatrend-studie Sicherheit

**3x**

AWS-Angriffe Bahrain & VAE

**€200 Mrd.**

EU-KI-Invest Horizon & Digital Europe

**100 %**

MCF-Pflicht aller chinesischen Unternehmen

**< 1 Min**

KI-Targeting (von 12 Stunden auf 45 Sekunden)

# Executive Summary

Künstliche Intelligenz ist zu einer tragenden Größe geopolitischer Macht, wirtschaftlicher Wettbewerbsfähigkeit und nationaler Sicherheit geworden. Die USA und China setzen ihre KI-Strategien mit hoher Geschwindigkeit um. Europa verfolgt einen eigenen Weg – mit erkennbaren Stärken und ebenso erkennbaren Lücken.

Dieses Whitepaper verbindet drei Perspektiven: die Erkenntnisse der ZI-Megatrendstudie Sicherheit 2026, aktuelle geopolitische KI-Strategien der großen Akteure und konkrete Handlungsoptionen für Unternehmen im DACH-Raum – ergänzt durch den KI-Souveränitätskompass als praktisches Selbsteinordnungs-Instrument.

## Kernbotschaften

- KI-Souveränität ist ein mehrdimensionales Gestaltungsfeld – von Chips über Datenzugang bis zur Regulierungshoheit.
- Jede KI-Nutzung vergrößert zugleich die eigene Angriffsoberfläche. KI wirkt beschleunigend – für Angreifende wie für Verteidigende.
- Nicht der Standort eines Servers entscheidet über Souveränität, sondern wer Zugriff steuern und im Zweifel entziehen kann.
- Sicherheit lässt sich nicht isoliert auf IT-Systeme verengen, sondern muss technische, physische und informationelle Ebenen gemeinsam betrachten (ZI-Megatrendstudie Sicherheit 2026).

# 01 Ausgangslage: KI-Souveränität verstehen

# 1.1 Die geopolitische Ausgangslage

KI-Infrastruktur ist zu einem festen Bestandteil geopolitischer Auseinandersetzung geworden. Rechenzentren, Modelle und Chip-Lieferketten sind Knotenpunkte politischer und wirtschaftlicher Machtverhältnisse. Wer sie kontrolliert, beeinflusst künftige Entscheidungsprozesse – in Unternehmen wie in Staaten.

Einige Kennzahlen verdeutlichen die Schieflage: China hält nach Angaben des AI Index Report 2025 rund 70 % aller weltweit erteilten KI-Patente, während der europäische Anteil bei etwa 2,8 % liegt. Drei US-Hyperscaler kontrollieren zugleich etwa 68 % des globalen Cloud-Marktes. Diese Zahlen sind keine Prognose, sondern Beschreibung des gegenwärtigen Zustands.

Vier Abhängigkeitsfelder sind für Unternehmen besonders relevant:

| Abhängigkeit | Wirkung |
| --- | --- |
| **Daten** | Wer KI-Dienste externer Anbieter nutzt, speist deren Modelle häufig mit eigenen Geschäftsdaten – und vergrößert damit indirekt den Wissensvorsprung des Anbieters. |
| **Entscheidungslogik** | Modellarchitekturen und voreingestellte Prozesslogiken prägen mit, wie Entscheidungen strukturiert werden, und wirken damit langfristig auf die Denkweise im Unternehmen. |
| **Energie** | KI-Infrastruktur ist stromintensiv. Rechenzentren sind an lokale Energienetze gebunden – ein in der Souveränitätsdebatte häufig unterschätzter Faktor. |
| **Chips** | GPUs und spezialisierte Chips stammen von wenigen Herstellern. Taiwan ist in dieser Lieferkette der zentrale geopolitische Risikopunkt. |

# 1.2 Was KI-Souveränität bedeutet

KI-Souveränität bezeichnet die Fähigkeit eines Unternehmens oder Staates, Entscheidungen über Einsatz, Entwicklung und Schutz von KI-Systemen autonom, regelbasiert und resilient zu treffen – auf Basis bewusster Steuerung von Infrastruktur, Daten, Technologien und operativen Abhängigkeiten.

| Dimension | Inhalt |
| --- | --- |
| **Technologische Souveränität** | Kontrolle über Chips, Compute, Modelle und KI-Infrastruktur. |
| **Datensouveränität** | Zugang, Governance und Schutz geschäftskritischer Daten. |
| **Regulierungssouveränität** | Fähigkeit, an der Gestaltung von Standards, Normen und Regeln mitzuwirken. |
| **Operationelle Souveränität** | Kontrolle über Betrieb, Resilienz und strategische Handlungsfähigkeit im Ernstfall. |

**Souveränität bedeutet heute kontrollierte Abhängigkeit. Vollständige Unabhängigkeit ist weder erreichbar noch das sinnvolle Ziel. Entscheidend ist, die eigenen Abhängigkeiten zu kennen und bewusst zu wählen, wo man sie eingeht.**

Diese Definition lässt sich in vier Dimensionen auffächern, die im weiteren Verlauf des Papiers – insbesondere in den Handlungsfeldern in Kapitel fünf – wieder aufgegriffen werden.

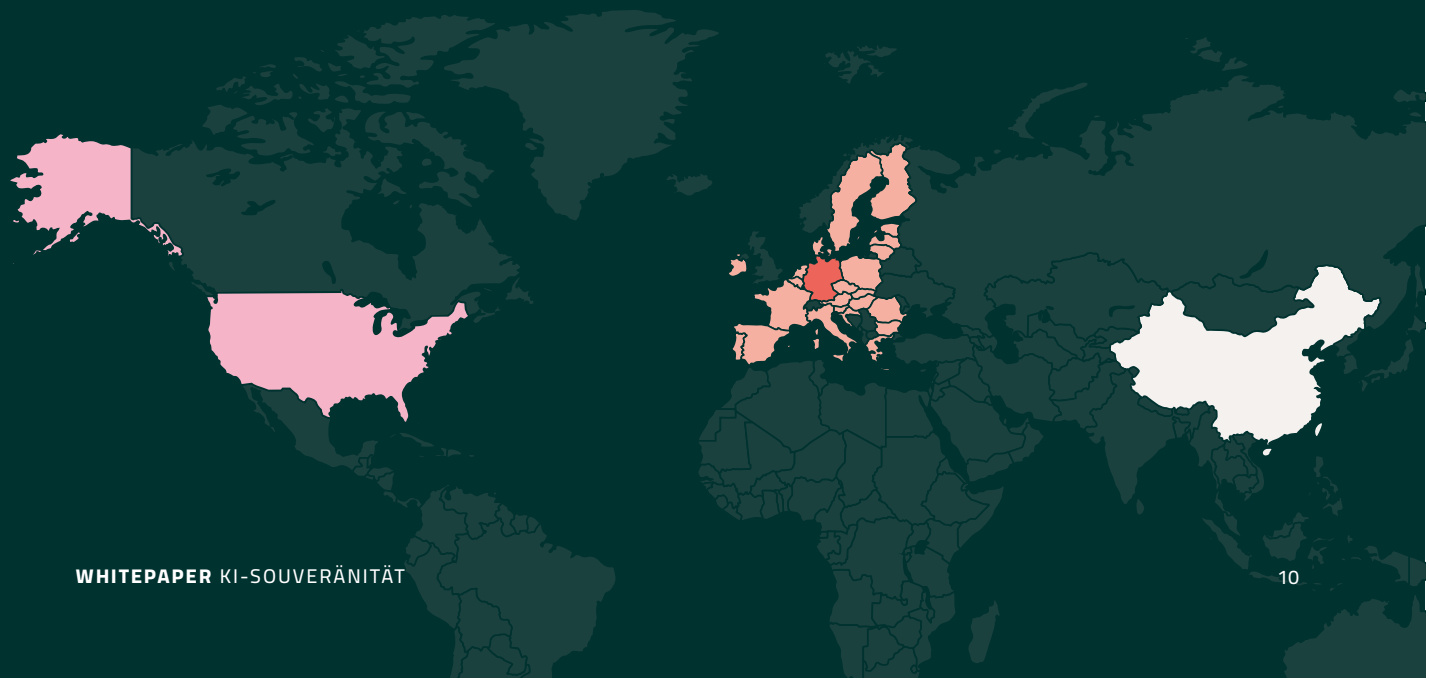
02

# Geopolitische KI-Strategien: Vier Akteure im Vergleich

# 2.1 Strategiematrix

Die folgende Übersicht ordnet ein, wie die vier wichtigsten Akteure ihre KI-Agenden ausrichten. Grundlage sind nationale Strategiepapiere und eigene Recherche des Zukunftsinstituts, Stand Mai 2026.

| | Deutschland | EU | USA | China |
|---|---|---|---|---|
| **Leitbild** | Technologische Souveränität; Lab-to-Market | AI Continent Action Plan; Apply AI; € 200 Mrd. | KI-Dominanz: Innovation, Infrastruktur, Sicherheit | AI Plus; nationaler Datenmarkt; systemische Beschleunigung |
| **Investition** | Hoch, national finanziert | € 200 Mrd. gesamt (Horizon & Digital Europe) | Sehr hoch, inklusive Militärhaushalt | 300 Mrd. USD bis 2030 |
| **Compute / Chips** | Mittel | AI Factories im Aufbau | Sehr hoch – Energie, Chips, Grid | Huawei Ascend 910C; SMIC 7nm |
| **Sicherheit** | BSI, KRITIS, NIS2 | AI Act High-Risk; NIS2 | Explizit militärisch eingebunden | MCF: 100 % Dual-Use per Gesetz |
| **Regulierung** | AI Act, DSGVO | AI Act als globaler Referenzrahmen | Deregulierung kombiniert mit Exportkontrollen | KI-Ethik-Export über BRI und UN-Gremien |



# 2.2 China: Systemisch organisierte Beschleunigung

China verfolgt die umfassendste staatlich integrierte KI-Industriepolitik weltweit. Vier Entwicklungen sind für Entscheider im DACH-Raum direkt relevant:

→ **15. Fünfjahresplan (2026–2030)**
300 Mrd. USD KI-Investition; AI-Plus-Pflicht für Unternehmen ab 500 Mio. RMB Umsatz; nationaler Datenmarkt als strategisches Steuerungsinstrument.

→ **DeepSeek-R1**
Erreicht nach Herstellerangaben GPT-4-Niveau bei einem Bruchteil der Trainingskosten. Open-Source-Verbreitung wird gezielt als Machtinstrument genutzt, um globale Adoption zu maximieren.

→ **Huawei Ascend 910C**
Erreicht laut Herstellerangaben 60–80 % der NVIDIA-H100-Leistung; in Kombination mit SMIC-7-nm-Fertigung entsteht eine weitgehend eigenständige Lieferkette.

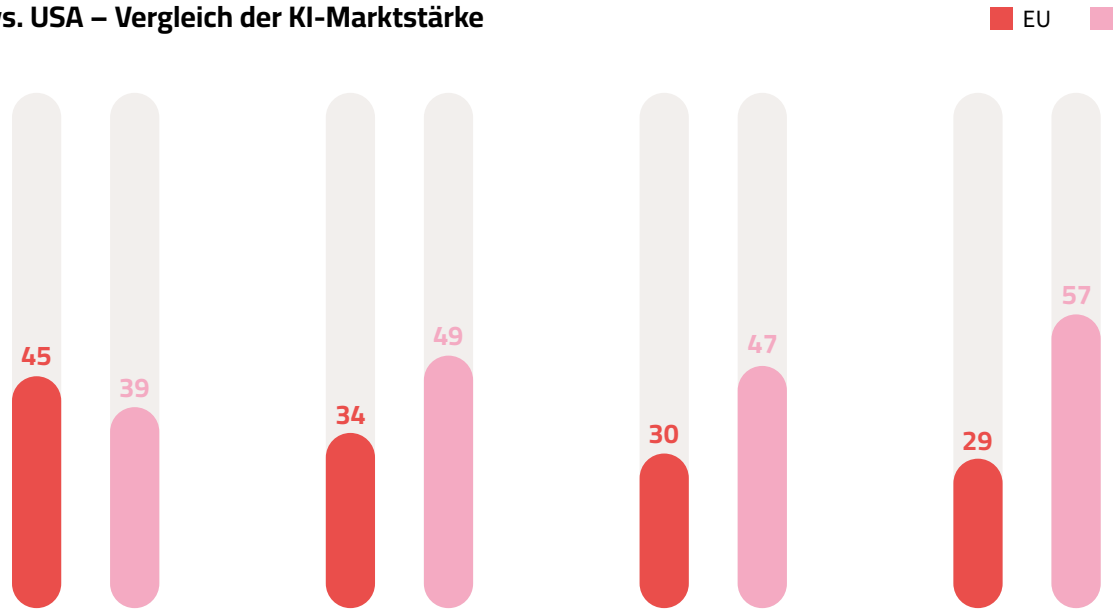
→ **Militär-Zivil-Fusion (MCF)**
Per Gesetz sind alle chinesischen Unternehmen – einschließlich Auslandstöchter – zur Technologieweitergabe an den Militärsektor verpflichtet.

# 2.3 Europa: vorhandene Stärken gezielt ausbauen

Europas Stärke liegt nicht im Wettbewerb um das größte Sprachmodell, sondern in der Fähigkeit, KI in bestehende industrielle Stärken zu integrieren. Die für Unternehmen relevantere Frage lautet deshalb weniger „Wer hat das beste Modell?“ als „Wer baut das leistungsfähigste KI-Ökosystem?“

Die Tabelle vergleicht einen Index für KI-Marktstärke zwischen EU und USA in vier Branchen. Im Manufacturing- und Supply-Chain-Segment liegt die EU vorn – einzige der vier Kategorien mit europäischer Führung. In den übrigen drei Bereichen liegen die USA deutlich voraus.

**EU vs. USA – Vergleich der KI-Marktstärke**




| Manufacturing & Supply Chain | Healthcare & Life Sciences | Finance & Insurance | R&D Tools |
|---|---|---|---|
| Einziger Bereich mit EU-Führung; München als stärkstes Signal | Strategische Priorität mit Wachstumspotenzial | UK wichtiger Akteur; Paris, Mailand spezialisiert | Deutschland und Schweden mit Spezialisierungstrend |

# Deutschland

## Industrielle Nische statt Generalanspruch

Deutschland ist das einzige EU-Land mit einem ausgeprägten Spezialisierungssignal: KI-Start-ups im Bereich Manufacturing & Supply Chain liegen rund 57 % über dem EU-Durchschnitt, München gilt als wichtigster substanzieller EU-Hub in diesem Segment. Gleichzeitig bleibt das Land in Healthcare und R&D Tools schwach aufgestellt – die Adoption ist breit, aber an vielen Stellen nicht tief.

# Polen

## Souveränität durch Steuerung statt durch eigene Modelle

Polen hat als einzige EU-Nation eine komplett neue, zentrale KI-Aufsichtsbehörde (KRiBSI) geschaffen und folgt damit dem Prinzip, Kompetenz zu bündeln statt zu verteilen. Die Stärke liegt nicht in eigenen Modellen, sondern in der Fähigkeit, KI gesellschaftlich und regulatorisch selbst zu steuern.

# Frankreich

## Starke Spitze, ungenutzte Breite

Frankreich verfügt über Weltklasse-Assets wie Mistral AI und Hugging Face, eine Investitionsankündigung von 109 Mrd. € und mit Präsident Macron einen sichtbaren politischen Treiber. Zugleich belegt das Land unter zehn untersuchten Nationen den letzten Platz bei der KI-Adoption im öffentlichen Dienst; 47 % der IT-Budgets fließen in Compliance, und 41 % der befragten KI-Startups erwägen einen Wegzug. Spitzenkompetenz und breite Anwendung fallen damit deutlich auseinander.

# 2.4 Drei Szenarien für Europa bis 2040

**Auf Basis der bisherigen Entwicklung lassen sich drei Pfade skizzieren, wie sich die Position Europas in der globalen KI-Landschaft bis 2040 verändern könnte. Sie sind als Orientierungsrahmen gedacht, nicht als Prognose.**

## EU als Abnehmer globaler KI-Netzwerke

Wenige Technologiekonzerne kontrollieren hochentwickelte KI-Systeme. Europa positioniert sich primär als Anwender. Eine naheliegende strategische Reaktion in diesem Szenario wäre der Aufbau hybrider Infrastruktur in Kombination mit starker Governance.

## Europa entwickelt einen eigenständigen Pfad

Die EU entwickelt eigene KI-Paradigmen jenseits der dominanten LLM-Architekturen. Investitionen in Bildung und vertikale, branchenspezifische KI-Lösungen tragen zu einem eigenständigen, wettbewerbsfähigen europäischen Weg bei.

## Globale Verlangsamung („KI-Winter")

Die KI-Entwicklung setzt sich fort, verlangsamt sich jedoch deutlich. Europa gewinnt dadurch Zeit für institutionelle Konsolidierung und den Aufbau von Governance-Strukturen.

Aktueller Fall (Juni 2026)

# 2.5 US-Exportkontrollen gegenüber Anthropic

Während der Fertigstellung dieses Whitepapers ereignete sich ein Vorfall, der mehrere der zuvor beschriebenen Mechanismen konkret sichtbar macht. Am Freitag, den 12. Juni 2026, erließen US-Behörden eine Exportkontrollanordnung gegenüber Anthropic, nach der die beiden neuesten Modelle des Unternehmens – Fable 5 und Mythos 5 – nur noch von US-Bürgern genutzt werden dürfen. Anthropic erklärte, eine technische Umsetzung dieser Vorgabe ohne weltweite Auswirkungen sei kaum möglich gewesen, unter anderem weil zahlreiche Nicht-US-Bürger für das Unternehmen arbeiten, und sperrte den Zugang in der Folge global.

Anthropic selbst bezeichnete die Anordnung öffentlich als nicht transparent, nicht fair und nicht auf technischen Fakten basierend.

**Drei Beobachtungen aus diesem Fall lassen sich mit den vorangegangenen Kapiteln verbinden:**

1

Die Anordnung bestätigt die in Kapitel 1.1 beschriebene These, dass nicht der Serverstandort über Kontrolle entscheidet, sondern die Hoheit über Technologie und Zugriffsrechte. Eine US-Behörde konnte regulatorischen Druck ausüben, der weltweit wirkte – unabhängig vom Willen des betroffenen Unternehmens.

2

Der Fall verdeutlicht die in Kapitel 2.3 beschriebene strukturelle Abhängigkeit Europas. Die Investorin Judith Dada (Visionaries Club), deren Essay „Europe 2031“ kurz vor dem Vorfall erschien, beschreibt den Mechanismus so: Es zeige, wie aus nationalen Interessen heraus über eine sehr mächtige Technologie Druck ausgeübt werden könne, und mache deutlich, dass Europa aktuell nicht gut genug aufgestellt sei, um sich in diesem Machtgefüge zu behaupten.

Aktueller Fall (Juni 2026)

# 2.5 US-Export-kontrollen gegen-über Anthropic

Thomas Jarzombek, Parlamentarischer Staatssekretär beim Bundesminister für Digitales, bezeichnete die Sperre als Weckruf für Europa und plädierte für einen hybriden Ansatz: Für Standardprozesse und interne Anwendungen sollten Unternehmen gezielt auf europäische Anbieter setzen, etwa das Cohere-Aleph-Alpha-Schwarz-Konsortium oder Mistral; nur wo diese nicht ausreichen, sollten weiterhin US-Frontier-Modelle zum Einsatz kommen. Seine Frage an die Industrie: ob Aufträge schlicht in die USA abfließen oder genutzt werden, um auch im Bereich KI eine eigene Lieferkette aufzubauen.

## Einordnung

Für die Praxis bedeutet dieser Fall vor allem, dass die im Kompass (Kapitel 6) abgefragten Abhängigkeiten von US-Hyperscalern (Frage 8) und die Prüfung von US Cloud Act und chinesischem MCF-Recht (Frage 9) keine theoretischen Compliance-Übungen sind, sondern unmittelbare Risikoindikatoren für die operative Handlungsfähigkeit eines Unternehmens. Er liefert zugleich ein konkretes, aktuelles Beispiel für Szenario A aus Kapitel 2.4: die Situation, in der wenige Technologiekonzerne über den Zugang zu KI-Systemen entscheiden.

# 05 Kritische Infrastruktur: KI als Angriffs-oberfläche

# 3.1 Neun Sicherheits-trends und ihre KI-Relevanz

Zur Megatrend-studie Sicherheit

**Die ZI-Megatrendstudie Sicherheit 2026 (ISBN 978-3-911642-05-7) identifiziert neun Trends, die den Sicherheitsrahmen der kommenden Jahre prägen. Sie werden hier mit Blick auf ihre KI-Relevanz zusammengefasst.**

## Power Blocks

Technologiekonzerne agieren zunehmend als geopolitische Akteure. KI-Infrastruktur ist Teil dieser Blocklogik: Wer Lieferketten kontrolliert, übt geopolitischen Einfluss aus.

## Game of Nations

Halbleiter sind zu einem geopolitischen Sicherheitsfaktor geworden. Ein Taiwan-Konflikt würde die globale GPU-Versorgung gefährden.

## Cyber Security

KI erweitert die Angriffsmöglichkeiten auf beiden Seiten. Angreifende setzen neue Technologien ohne regulatorische Beschränkungen ein, was die Dynamik beschleunigt.

## Risk Latency

Das Prinzip „Harvest now, decrypt later“ im Zusammenhang mit Quantencomputing macht Echtzeit-Reaktionsfähigkeit zur Notwendigkeit.

## Guardification

Ein dauerhafter Schutz- und Kontrollmodus wird zur neuen Normalität, mit zunehmender zivil-militärischer Sicherheitskonvergenz.

## Crumbling Modernity

Kritische Infrastrukturen bleiben verwundbar; Single Points of Failure bestehen weiterhin in Energie, IT und Logistik.

## Resilience

Ein Paradigmenwechsel von Effizienz zu Robustheit zeichnet sich ab. Business Continuity muss auch ohne durchgängige digitale Systeme funktionieren.

## Planetary Risk

Energiesicherheit wird zur KI-Souveränitätsfrage; Kernfusion gilt als langfristiger strategischer Faktor.

## Cold War 2.0

Hybride Angriffe auf kritische Infrastruktur – Wasser, Energie, Verkehr, Finanzwesen, Gesundheit – kombinieren häufig Ransomware mit Desinformation.

# 3.2 Drei Handlungs-szenarien für Unternehmen

**Aus den Sicherheitstrends lassen sich drei wiederkehrende Risikoszenarien ableiten, für die Unternehmen jeweils eine andere Form der Vorbereitung benötigen.**

## KI-gestützte Cyberangriffe

Automatisierte Schadprogramme können Software-Stacks in Echtzeit analysieren. Eine durchdachte Sicherheitsarchitektur – nicht ein einzelnes Produkt – ist die wirksamere Antwort; ein Assume-Breach-Ansatz sollte Teil der Planung sein.

## Ausfall kritischer KI-Dienste

Analoge Fallback-Prozesse für KI-gestützte Kernabläufe, papierbasierte Notfallpläne und deren regelmäßige Erprobung sichern die Handlungsfähigkeit im Ausfallfall.

## Hybride Bedrohungen

Physische Sabotage kombiniert mit KI-gestützter Desinformation erfordert eine integrierte Lageführung über technische, physische und informationelle Ebenen hinweg.

# 3.3 KI-Anwendungen und ihre Angriffsoberfläche

**Die folgende Übersicht ordnet typische KI-Anwendungen in zwei Gruppen: zunächst industrielle und technische Systeme, danach Anwendungen mit Bezug zu Finanzwesen, Kommunikation und Versorgung.**

## Industrielle und technische Systeme

| Anwendung | Abhängigkeit & Angriffsoberfläche |
|---|---|
| **Predictive Maintenance** | Beruht auf sensorbasierter Echtzeit-Überwachung. Manipulierte Eingabedaten (Adversarial Inputs) können Wartungssignale verfälschen. |
| **Energiemanagement / Smart Grid** | KI-gesteuerte Lastverteilung; eine Kompromittierung kann Stromausfälle auslösen. |
| **KI-Cybersicherheit (SIEM/SOAR)** | Das Sicherheitssystem selbst wird zur Angriffsoberfläche, wenn es kompromittiert wird. |
| **Medizinische KI** | Als High-Risk-Anwendung im Sinne des EU AI Act eingestuft; eine Kompromittierung kann Patientinnen und Patienten direkt gefährden. |

# 3.3 KI-Anwendungen und ihre Angriffsoberfläche

## Finanzwesen, Kommunikation und Versorgung

| Anwendung | Abhängigkeit & Angriffsoberfläche |
|---|---|
| **Finanzinfrastruktur** | Koordinierte Angriffe auf KI-gestützte Handelsmodelle können systemische Marktinstabilität erzeugen. |
| **Supply-Chain-Intelligence** | Vergiftete Datenquellen (Data Poisoning) können die gesamte Entscheidungsbasis korrumpieren. |
| **Kritische Kommunikation** | Die Sabotage von Datenkabeln in der Ostsee (2024/25) zeigte, dass KI-gestütztes Routing ein bevorzugtes Angriffsziel sein kann. |
| **Wasserversorgung** | Der dokumentierte Vorfall in Oldsmar, Florida (2021) zeigt das Zusammenspiel von technischer Manipulation und begleitender Desinformation. |

# 04

# Unternehmens-perspektive: Was SAP zeigt

SAP-CEO Christian Klein benennt einen Widerspruch, der für viele europäische Unternehmen typisch ist: Deutschland hat mit erheblichem Aufwand eine der souveränsten Cloud-Infrastrukturen der Welt aufgebaut – und SAP selbst zählt zugleich zu den größten Kunden der US-Hyperscaler.

> Nicht der Standort des Servers entscheidet, sondern ob niemand den Stecker ziehen kann und ob Geschäftsdaten vor fremdem Zugriff geschützt sind.
>
> **Christian Klein, SAP-CEO**

Aus dieser Beobachtung lassen sich fünf Handlungsprinzipien ableiten, die über den Einzelfall SAP hinaus für Unternehmen im DACH-Raum relevant sind:

| Handlungsprinzip | Bedeutung für Unternehmen |
|---|---|
| **Pragmatismus vor Ideologie** | Die zentrale Ausgangsfrage lautet: Welche Daten, Prozesse und Entscheidungen müssen tatsächlich besonders geschützt werden? Dort sollte der Schutzaufwand konzentriert werden. |
| **Abhängigkeiten kartieren** | Welche Hyperscaler werden genutzt? Wo liegen die Daten? Welche Verträge enthalten Zugriffsrechte für Drittstaaten – etwa über US Cloud Act oder chinesisches MCF-Recht? |
| **Risikotransparenz** | Eine ehrliche, vollständige Abhängigkeitskarte ist die Voraussetzung für souveräne Entscheidungen – nicht deren Ergebnis. |
| **Innovation priorisieren** | Die europäische Stärke liegt weniger im Wettlauf um große Basismodelle als in Anwendungsdomänen, Branchen-KI und regulatorischer Verlässlichkeit. |
| **Hybride Resilienz** | Europäische Kerndaten lassen sich mit global verfügbaren Compute-Kapazitäten kombinieren, statt sich auf eine einzige Lösung festzulegen. |

# 05 Vier Handlungsfelder für Unternehmen im EU-/DACH-Raum

1

## Abhängigkeiten kartieren und Schutzgrade priorisieren

- Eine KI-Angriffsflächen-Matrix für alle KRITIS-relevanten KI-Anwendungen erstellen.
- US-Cloud-Act- und China-MCF-Exposition in allen KI-Verträgen systematisch prüfen.
- Schutzklassen definieren: Kerndaten, sensitive Prozesse, sicherheitsrelevante Entscheidungen.

2

## Infrastruktur- und Compute-Resilienz aufbauen

- AI Factories, Gigafactories und IPCEI-Förderprogramme als Hebel zur Reduktion von Compute-Abhängigkeiten nutzen.
- Eine hybride Architektur verfolgen: Kerndaten auf EU-Infrastruktur, skalierbare Workloads über Hyperscaler.
- Analoge Fallbacks und papierbasierte Notfallpläne einrichten und regelmäßig testen.

3

## Regulierung als Gestaltungsfeld nutzen

- EU-AI-Act-High-Risk-Compliance frühzeitig als Investment behandeln, nicht als reine Pflichtübung.
- Das Vereinfachungspaket Digital Omnibus (2025) nutzen, um freiwerdende Ressourcen gezielt einzusetzen.
- Aktiv an ISO/IEC-, ITU- und UN-Gremien mitwirken, statt nur abzuwarten.

4

## Innovation und Thought Leadership sichern

- HaDEA-Projekte als Orientierung nutzen: Europäische KI-Stärke zeigt sich besonders in Healthcare, Industrie, Finanzwesen und Verwaltung.
- Eine 360-Grad-Sicherheitskultur etablieren: alle Mitarbeitenden schulen, Sicherheit als Führungsaufgabe verstehen.
- KI-Souveränität als eigenständiges Differenzierungsmerkmal gegenüber Kunden und Investoren positionieren.

06

# KI-Souveränitäts-kompass

## SELBSTEINORDNUNG

Der folgende Kompass mit 12 Fragen (rund 4 Minuten Bearbeitungszeit) hilft dabei, den eigenen Stand entlang vier Dimensionen einzuordnen: KI-Nutzung, Sicherheit & Resilienz, Souveränität & Abhängigkeiten sowie Strategie & Zukunftsfähigkeit.
Jede Frage wird mit A, B, C oder D beantwortet; die Auswertung folgt im Anschluss.

1 / 4

# KI-Souveränitäts-kompass: Fragebogen

## Dimension 1

### KI-Nutzung

**1. Wie intensiv nutzt Ihr Unternehmen KI in operativen Kernprozessen?**

- ☐ A Kaum vorhanden, wir beobachten erst
- ☐ B Erste Pilotprojekte laufen
- ☐ C KI ist in mehreren Prozessen integriert
- ☐ D KI ist durchgängig in Kernprozessen verankert

**2. In welchem Stadium befindet sich Ihre KI-Strategie?**

- ☐ A Wir verfolgen Entwicklungen, haben aber noch keine Strategie
- ☐ B Erste Pilotprojekte laufen, die Strategie entsteht
- ☐ C Die KI-Strategie ist formuliert und wird skaliert
- ☐ D KI ist etabliert, wir optimieren Wirkung und ROI

**3. Wie stark hat KI Ihre Entscheidungsprozesse verändert?**

- ☐ A Kaum Veränderung bisher
- ☐ B Einzelne Entscheidungen werden KI-gestützt
- ☐ C KI beschleunigt und verbessert viele Entscheidungen
- ☐ D KI hat unsere Entscheidungslogik grundlegend verändert

2 / 4

# KI-Souveränitäts-kompass: Fragebogen

**Dimension 2** — Sicherheit & Resilienz

**4. Wie gut ist Ihr Unternehmen auf KI-spezifische Cyberbedrohungen vorbereitet?**

- ☐ A Das Thema ist noch nicht systematisch adressiert
- ☐ B Einzelne Sicherheitsmaßnahmen sind vorhanden
- ☐ C KI-Sicherheit ist Teil unserer Gesamtarchitektur
- ☐ D Wir betreiben aktives KI-Angriffsflächen-Monitoring

**5. Existiert ein Notfallplan für den Ausfall zentraler KI-Dienste?**

- ☐ A Noch nicht vorhanden
- ☐ B Wird aktuell entwickelt
- ☐ C Plan existiert, wurde aber noch nicht getestet
- ☐ D Plan wird regelmäßig geprobt und aktualisiert

**6. Wie hoch ist das Risiko, dass ein Ausfall zentraler KI-Dienste Ihren Betrieb beeinträchtigt?**

- ☐ A Gering, KI ist noch nicht betriebskritisch
- ☐ B Moderat, Teile des Betriebs wären betroffen
- ☐ C Hoch, wesentliche Prozesse würden stillstehen
- ☐ D Sehr hoch, wir sind stark abhängig

3/4

# KI-Souveränitäts-kompass: Fragebogen

**Dimension 3** — Souveränität & Abhängigkeiten

**7. Wie gut kennen Sie Herkunft und Zugriffsrechte Ihrer KI-Infrastruktur?**

- ☐ A Weitgehend unklar
- ☐ B Teilweise kartiert, einzelne Systeme bekannt
- ☐ C Überwiegend kartiert, wesentliche Systeme bekannt
- ☐ D Vollständig kartiert mit dokumentierten Zugriffsrechten

**8. Welche Abhängigkeit von US-Hyperscalern (AWS, Azure, GCP) besteht?**

- ☐ A Sehr hoch, nahezu vollständige Abhängigkeit
- ☐ B Hoch, mehrheitlich US-Hyperscaler, teils Alternativen
- ☐ C Moderat, hybride Architektur mit europäischen Anteilen
- ☐ D Gering, überwiegend europäische oder eigene Infrastruktur

**9. Haben Sie US Cloud Act und China MCF als Zugriffsrisiko in Ihren Verträgen bewertet?**

- ☐ A Noch nicht systematisch geprüft
- ☐ B Erste Prüfungen laufen
- ☐ C Überwiegend bewertet, Maßnahmen in Arbeit
- ☐ D Vollständig bewertet und vertraglich adressiert

4 / 4

# KI-Souveränitäts-kompass: Fragebogen

**Dimension 4** — Strategie & Zukunftsfähigkeit

**10. Wie gut verfolgen Sie aktuelle geopolitische KI-Entwicklungen?**

- ☐ A Kaum, das ist bisher kein Thema bei uns
- ☐ B Gelegentlich, wir lesen, aber ohne Systematik
- ☐ C Regelmäßig, wir beobachten relevante Entwicklungen
- ☐ D Systematisch, wir analysieren und leiten Konsequenzen ab

**11. Welche Zeithorizonte adressiert Ihre KI-Strategie primär?**

- ☐ A Operativ, kurzfristige Effizienz im Fokus
- ☐ B 12 Monate, mittelfristige Planung dominiert
- ☐ C 3 Jahre, strategische Investitionen mit mehrjährigem Horizont
- ☐ D 5+ Jahre, langfristige Souveränitätsstrategie

**12. Wie behandelt Ihr Unternehmen den EU AI Act?**

- ☐ A Wir warten auf finale Klarheit
- ☐ B Wir verfolgen die Entwicklung
- ☐ C Die Compliance-Analyse läuft aktiv
- ☐ D Frühe Compliance wird als strategischer Vorteil genutzt

# KI-Souveränitäts-kompass: Auswertung

**Zählen Sie die Anzahl der Antworten für A bis D zusammen.** Daraus ergibt sich ein Profil entlang vier Entwicklungsstufen. Keine Stufe ist falsch – jede zeigt einen sinnvollen nächsten Schritt. Wer weiß, wo er steht, kann gezielter investieren.

## A Orientierung

**Sie bauen gerade Ihr Lagebild auf – ein naheliegender Ausgangspunkt.**

- → geopolitische KI-Strategien (USA, China, EU) verstehen und intern kommunizieren
- → eine Abhängigkeitskarte für die wichtigsten KI-Systeme erstellen
- → die ZI-Megatrendstudie Sicherheit als Grundlage für das nächste Strategiemeeting nutzen

## B Exploration

**Sie experimentieren aktiv – jetzt lohnt es sich, Risiken und Abhängigkeiten sichtbar zu machen.**

- → MCF- und Cloud-Act-Exposition in bestehenden KI-Verträgen prüfen
- → erste Pilotprojekte für europäische Infrastruktur starten
- → Resilienz-Szenarien für den Ausfall kritischer KI-Dienste durchspielen

## C Skalierung

**KI ist in Ihrer Organisation verankert – jetzt rücken Governance und Schutz in den Vordergrund.**

- → eine hybride Cloud-Strategie mit klar definierten Schutzklassen ausrollen
- → EU-AI-Act-High-Risk-Compliance als strategisches Investment umsetzen
- → ein KRITIS-KI-Konzept mit analogen Fallbacks verankern

## D Führung

**KI ist operationalisiert – jetzt lassen sich die Wettbewerbsvorteile der eigenen Souveränität gezielt nutzen.**

- → KI-Resilienz-KPIs messen und im Board kommunizieren
- → Angriffsflächen-Monitoring für kritische KI-Infrastruktur institutionalisieren
- → KI-Souveränität als Differenzierungsmerkmal gegenüber Kunden und Investoren positionieren.

Souveränität bedeutet heute kontrollierte Abhängigkeit. Entscheidend ist, wer Zugriff, Kontrolle und Abschaltmacht über Infrastruktur, Daten und operative Prozesse besitzt.

# Quellenverzeichnis

**Zukunftsinstitut**

Zukunftsinstitut GmbH (2026): Megatrendstudie Sicherheit – Die Sicherheitsarchitektur der Zukunft. ISBN 978-3-911642-05-7.

Gerstenberg, Uwe (2026): KI als Brandbeschleuniger. In: Megatrendstudie Sicherheit, S. 36–37 und S. 52–53.

**USA**

White House (2025): America's AI Action Plan. ai.gov/action-plan

NSCAI (2025): Superintelligence Strategy / Final Report. nationalsecurity.ai

Bureau of Industry and Security (2025/2026): Export Administration Regulations, AI Compute Export Controls.

**China**

Volksrepublik China (2026): 15. Fünfjahresplan (2026–2030) – KI und technologische Souveränität.

Volksrepublik China: Military-Civil Fusion (MCF) – Gesetz über nationale Verteidigung.

**Europäische Union**

European Commission (2024/2025): EU AI Act; AI Continent Action Plan; Apply AI Strategy; Digital Omnibus.

HaDEA (2026): Spotlight on: AI – Projects Enhancing EU Tech Sovereignty. 8. April 2026.

**Deutschland / SAP**

Bundesregierung Deutschland (2025): High-Tech-Agenda Deutschland.

Klein, Christian (SAP CEO) (2025/2026): Öffentliche Äußerungen zur europäischen KI-Souveränität.

**Sicherheit & Infrastruktur**

Stadler, Max (2024): Data Centers – Edges of a Wired Nation. MIT Press.

Statista / Stanford University (2025): Anteil der weltweit erteilten KI-Patente nach Regionen. AI Index Report 2025.

EuroStack / Gaia-X / OpenStack – europäische Infrastruktur- und Souveränitätsmodelle.

Öffentliche Stellungnahmen von Judith Dada und Thomas Jarzombek (Juni 2026)

Öffentliche Meldungen zu AWS-Angriffen Bahrain & VAE (März 2026)

## Impressum

Zukunftsinstitut GmbH
Kaiserstr. 53
60329 Frankfurt am Main
info@zukunftsinstitut.de

**Geschäftsführung**
Harry Gatterer

**Research**
Prof. Dr. Florina Speth
Prof. Dr. Dirk Stein

**Grafik**
Julia Pöllmann

**Hinweis zur Nutzung von KI**
Das Bildmaterial wurde mithilfe von künstlicher Intelligenz generiert und anschließend manuell nachbearbeitet.

zukunftsInstitut