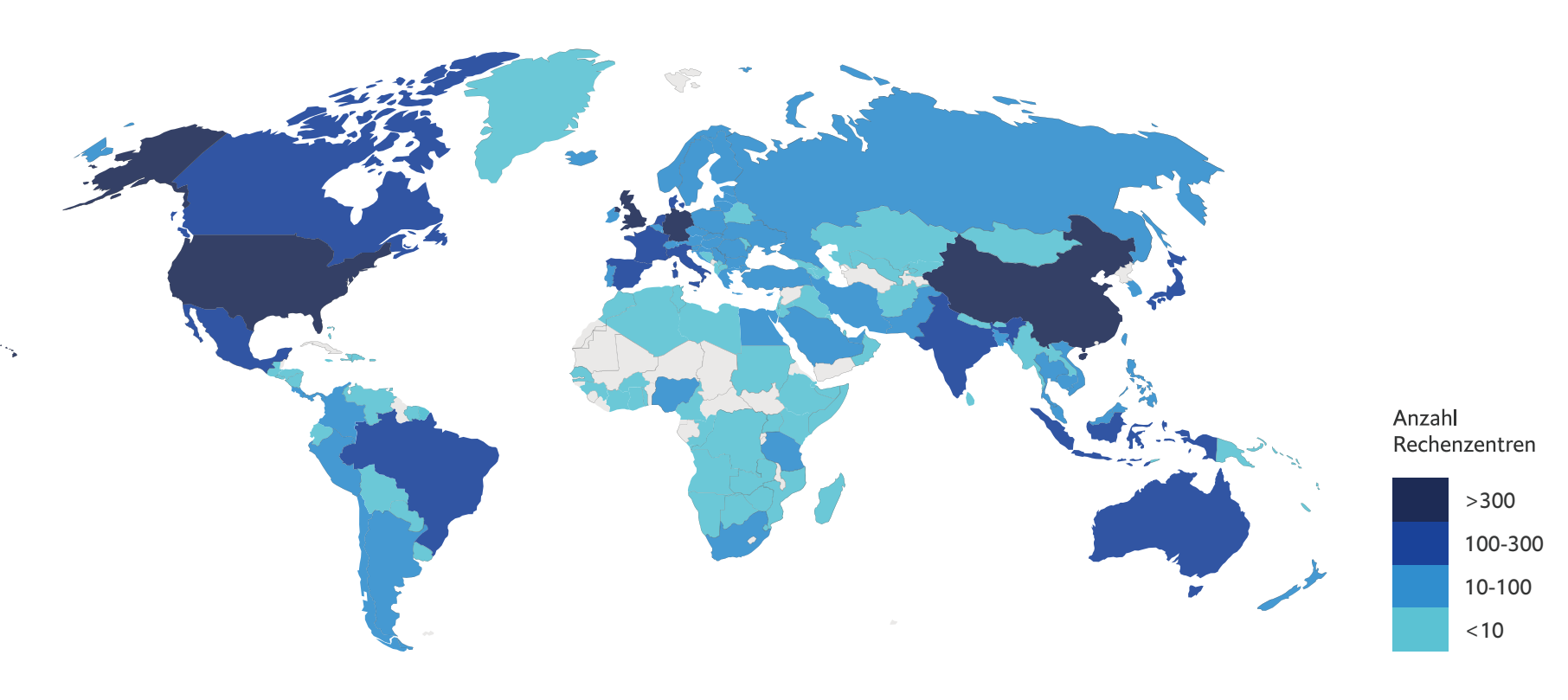
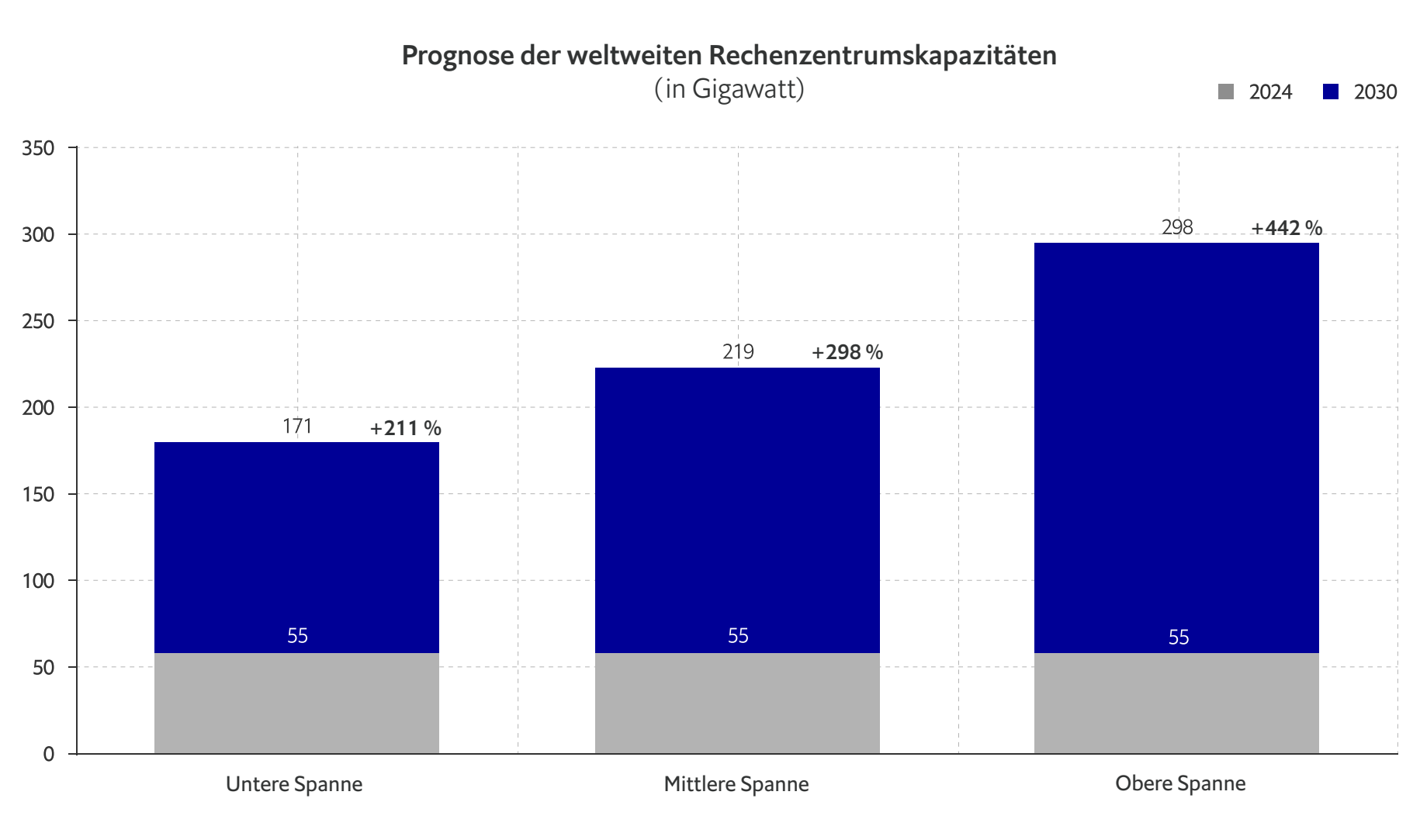
Fundamente in Gefahr: Beurteilung der Resilienz von Rechenzentren und digitalen Infrastrukturen

Unscheinbar, aber unverzichtbar: Rechenzentren sind die stillen Motoren moderner Unternehmen – und halten die Weltwirtschaft am Laufen.

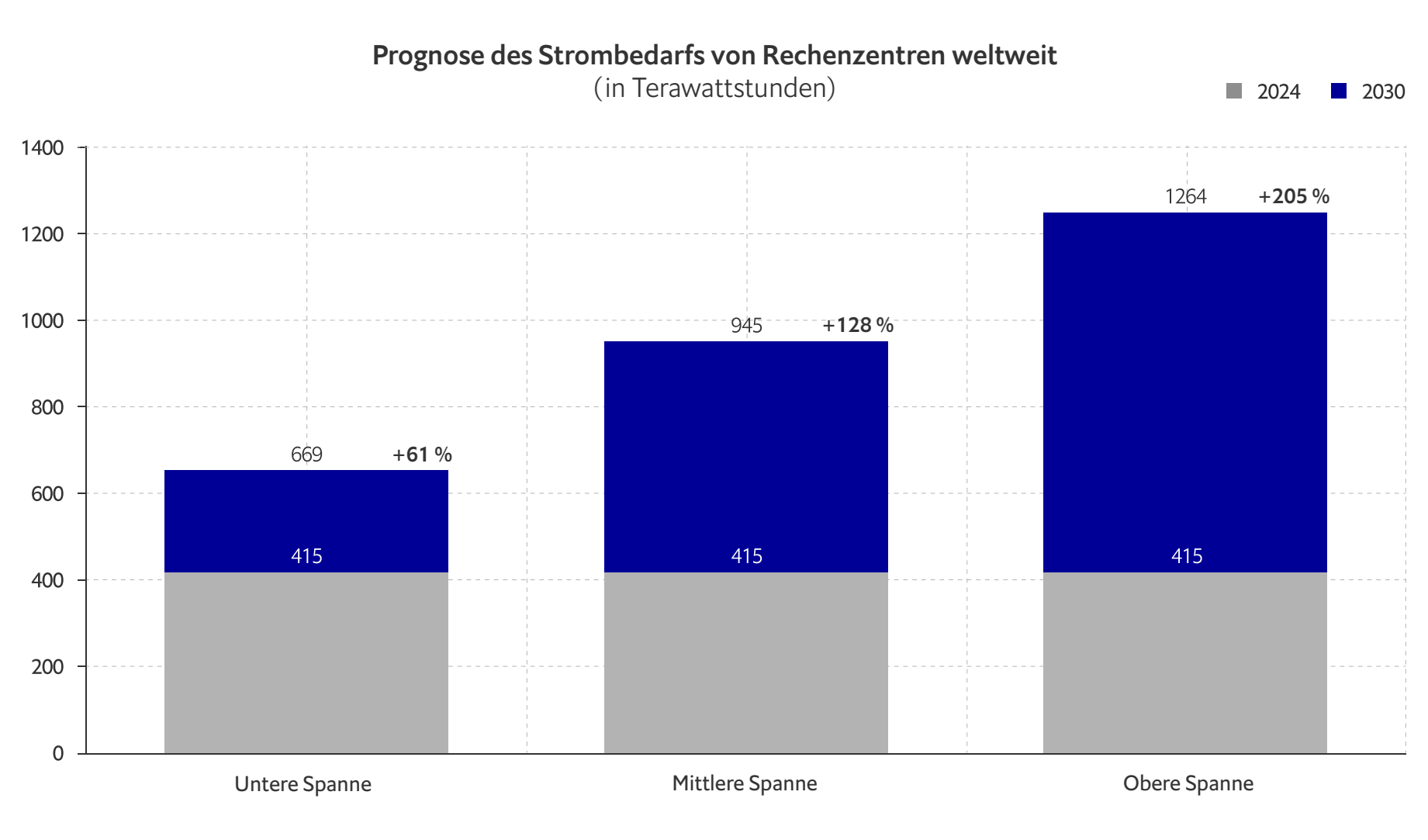
Weltweit gibt es über 11.800 Rechenzentren, fast die Hälfte davon befindet sich in den USA.



Seit dem Einzug von KI werden Rechenzentrumskapazitäten rasant ausgebaut. Schätzungen zufolge sollen sich die aktuellen Kapazitäten bis zum Jahr 2030 verdreifachen.



Der Kapazitätsausbau wird in den kommenden sechs Jahren den Energiebedarf deutlich erhöhen.



Mit der immer schnelleren Verbreitung von KI steigt auch der globale Bedarf an Rechenleistung und Speicherplatz. Dem gegenüber stehen die Komplexität globaler Lieferketten, der hohe Druck hinsichtlich Nachhaltigkeit und die rasante technologische Weiterentwicklung. Die Konsequenz: ein komplexes Geflecht an neuen Risiken. **Viele dieser Bedrohungen unterscheiden sich von den bislang bekannten Gefährdungen – Betroffene sind mit diesen Herausforderungen oftmals überfordert.**

Rechenzentren können ganz unterschiedlichen Risiken ausgesetzt sein. Manche Ereignisse treten isoliert auf und betreffen nur bestimmte Standorte, z. B. technische Ausfälle oder lokale Störungen. Systemische Schwachstellen hingegen bergen die Gefahr einer Kettenreaktion und haben weitreichendere Folgen für Wirtschaft und Infrastruktur. Economist Impact hat die vier größten systemischen Risiken ermittelt, die die Resilienz von Rechenzentren und digitalen Infrastrukturen bedrohen:

Systemische Risiken für Rechenzentren

1 Handelskonflikte und nationale Sicherheit

2 Politische Instabilität und hybrider Konflikt

3 Auswirkungen des Klimawandels

4 Bedrohung durch Quantencomputer

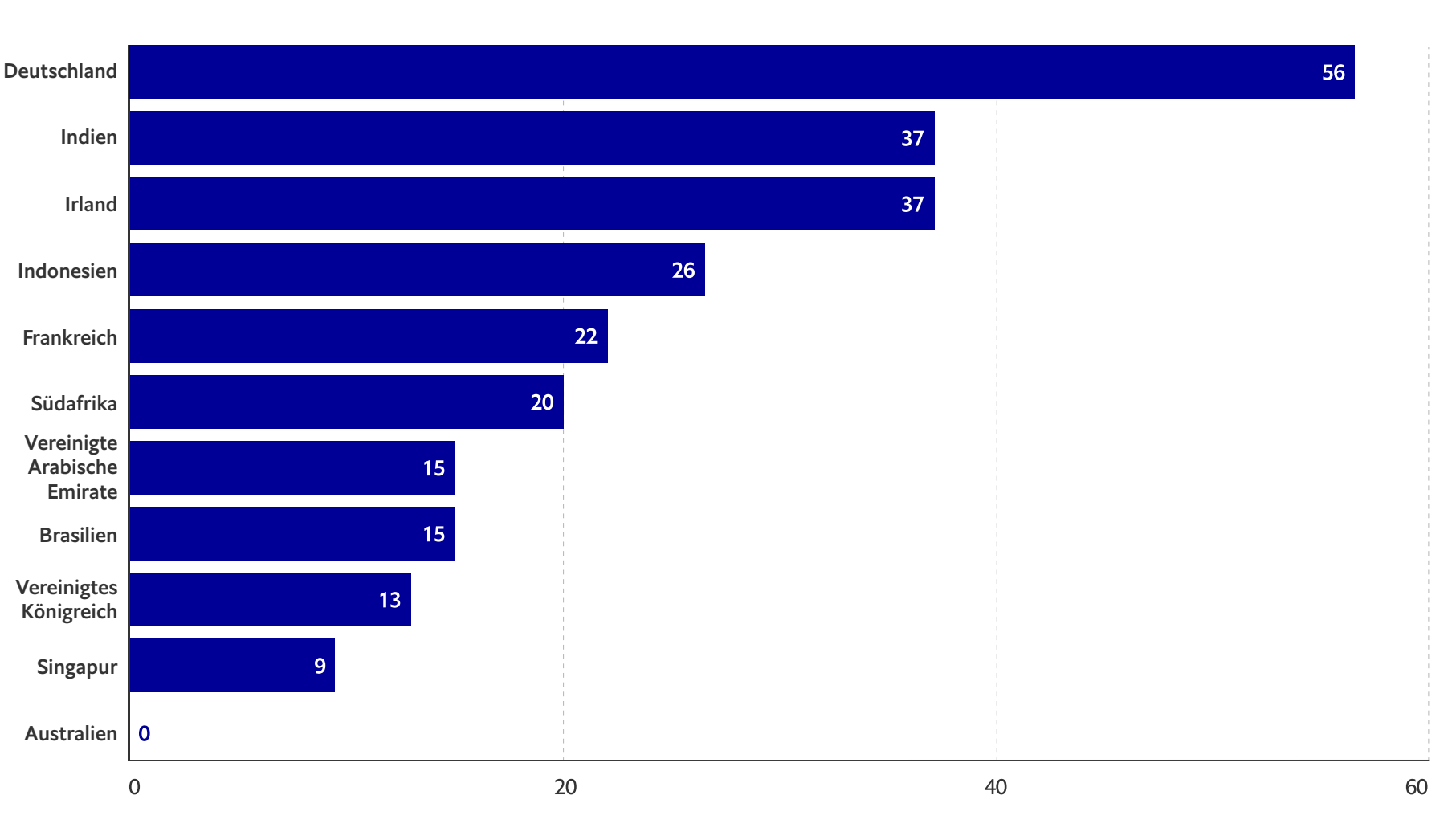
1 Handelskonflikte und nationale Sicherheit

Marktkonzentration führt zu struktureller Verwundbarkeit. Die Abhängigkeit von einzelnen Lieferunternehmen und Standorten macht die gesamte Infrastruktur anfällig: So kann ein einziger Vorfall wie ein Handelskonflikt zwischen den USA und China den Betrieb von Rechenzentren weltweit stören, Expansionen verzögern und die Kosten in die Höhe treiben.

Aufgrund seiner industrie- und exportorientierten Wirtschaft wäre Deutschland von einem Handelskonflikt mit den USA am stärksten betroffen. Im Gegensatz dazu ist der Handelsverkehr zwischen Australien und den USA deutlich moderater. Folglich ist davon auszugehen, dass sich US-Zölle deutlich weniger auf Australien als auf andere Länder auswirken werden.

Wie anfällig ist das Land für die Auswirkungen eines Handelskriegs mit den USA unter der Trump-Regierung?

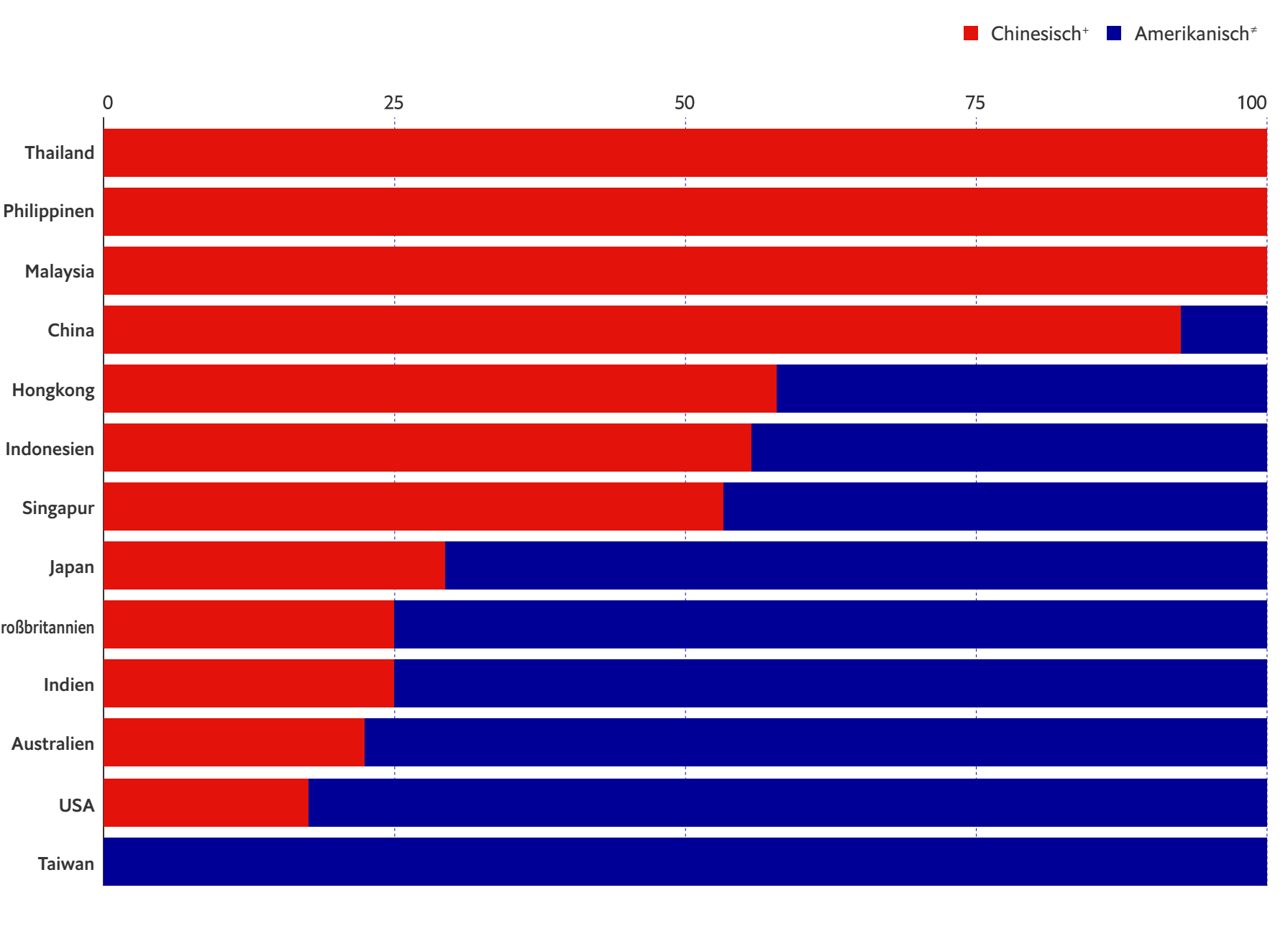
(0=geringes Risiko,100=hohes Risiko)



Quelle: Economist Intelligence Unit (2025)

Marktkonzentration von Cloud-Anbietenden

Anteil der Verfügbarkeitszonen für Cloud-Computing[*] unter der Kontrolle der größten chinesischen oder amerikanischen Cloud-Anbietenden, Oktober 2023 (in %)



[*] Unabhängige Cluster von einem oder mehreren Rechenzentren
[+] Huawei, Alibaba und Tencent [≠] Google, Microsoft und Amazon

Quelle: „Cloud empires' physical footprint", von V. Lehdonvirta et al., Oxford Internet Institute working paper, Dezember 2023

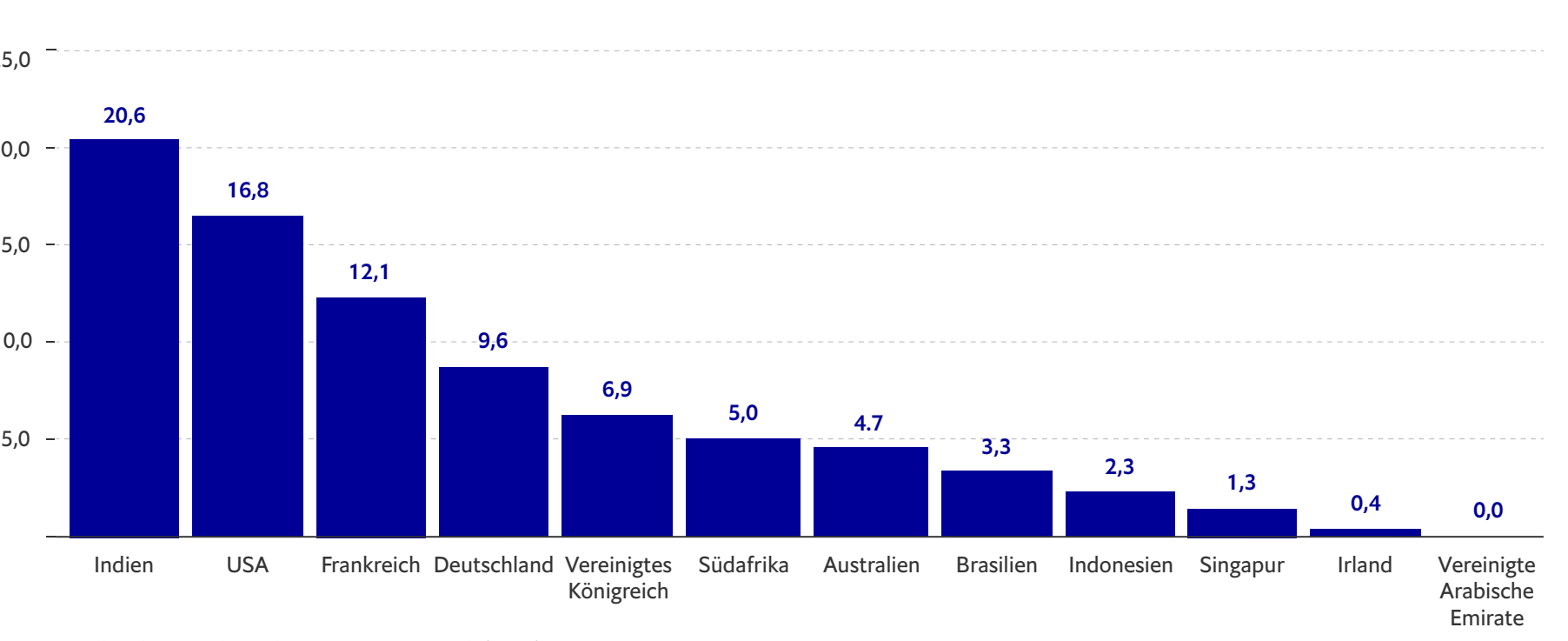
Quelle: V. Lehdonvirta et al, Oxford Internet Institute (2023)

2 Klimawandel

Der Klimawandel stellt Rechenzentren vor Herausforderungen. Der wachsende Energiebedarf, häufiger auftretende Wetterextreme und Elementargefahren belasten die Stromnetze, erschweren die zuverlässige Kühlung von Rechenzentren und führen zu strengeren Umweltvorschriften. Für den zukünftigen Betrieb von Rechenzentren gilt es also, die Standortwahl und den Zugang zu Ressourcen zu überdenken. Der Umstieg auf erneuerbare Energien ist unumgänglich, um Rechenzentren am Laufen zu halten und gleichzeitig deren CO^2-Fußabdruck zu reduzieren.

Wie anfällig ist das Land für Klimarisiken wie z. B. Stürme, Überschwemmungen, Hitzewellen?

(Durchschnitt 1993-2022, hoher Wert = höheres Risiko von Klimawandel)



Quelle: Klima-Risiko-Index von Germanwatch (2025)

Rechenzentren erfordern rund **4 %** des weltweiten Energiebedarfs...

...könnten **6.482.400** durchschnittliche US-amerikanische Haushalte mit Strom versorgen...

...und bedingen damit **1 %** der weltweiten Treibhausgasemissionen.

Quelle: Klima-Risiko-Index – Germanwatch (2025)

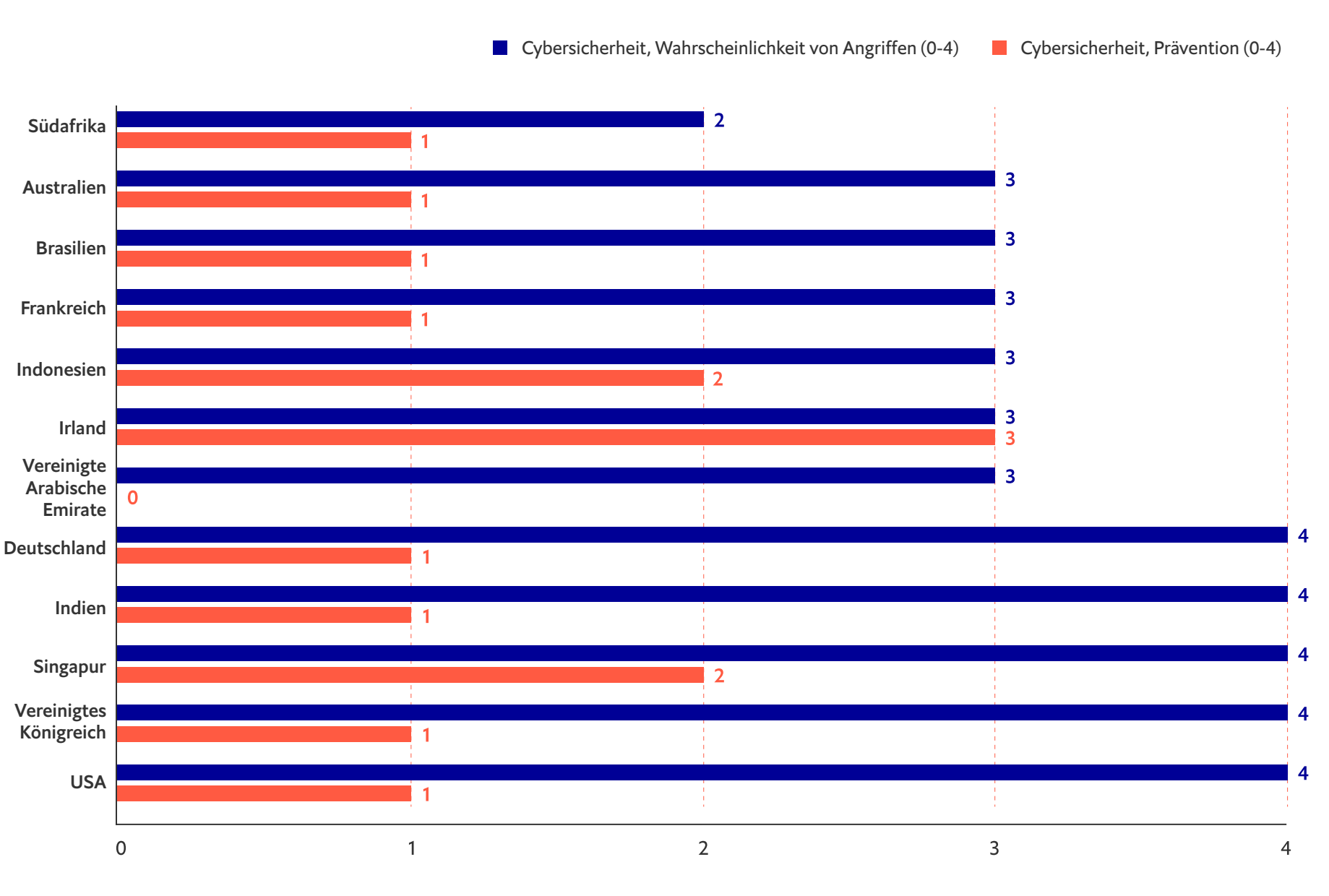
3 Politische Instabilität und hybrider Konflikt

Rechenzentren sind bei geopolitischen Spannungen immer häufiger die Zielscheibe. Im Zeitalter hybrider Konflikte werden Rechenzentren anfälliger, ob für Cyberangriffe, Service-Ausfälle oder physische Sabotage. Politische Instabilität stellt daher ein ernstzunehmendes Risiko für diese strategisch wichtigen Anlagen dar. Gleichzeitig wird deutlich, dass der gesamte Sektor nur unzureichend auf solche Risiken vorbereitet ist.

Anfälligkeit für Cyberattacken vs. Prävention

Wahrscheinlichkeit von Angriffen (0=geringes Risiko, 4=hohes Risiko)

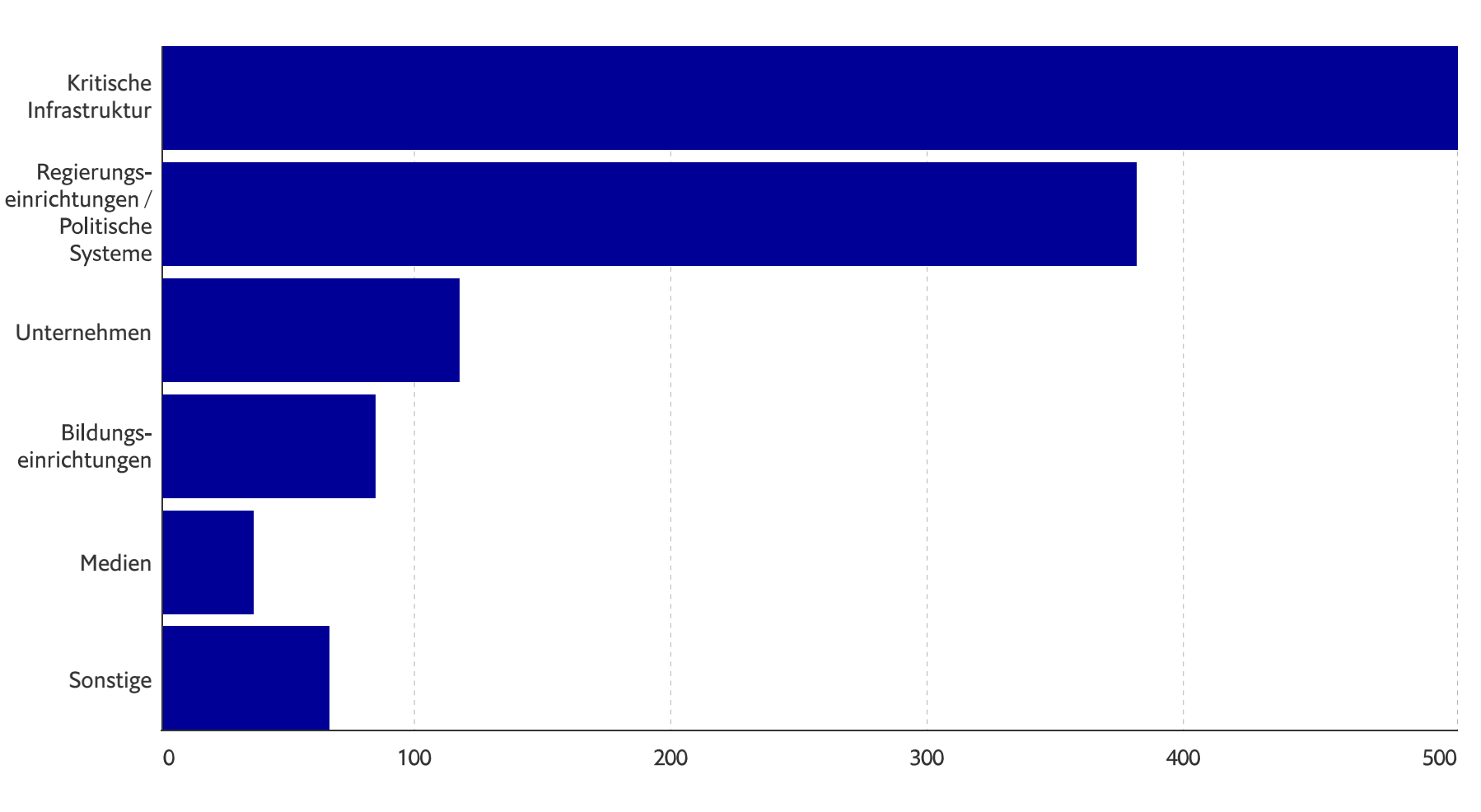
Prävention (0=hohes Schutzniveau gegen Cyberangriffe, 4=niedriges Schutzniveau gegen Cyberangriffe)



Quelle: Economist Intelligence Unit (2025)

Kritische Infrastrukturen wie Rechenzentren sind das häufigste Angriffsziel:

Anzahl der politischen Cyberattacken weltweit in verschiedenen Sektoren



Quelle: European Repository of Cyber Incidents, 2023

4 Technologische Fortschritte und Gefahren in Verbindung mit Quantencomputing

Der technologische Umbruch, angetrieben durch KI und Quantencomputing, hat zur Folge, dass bestehende Infrastrukturen schneller obsolet werden. Altsysteme sind im Hinblick auf Sicherheits- und Hardwareanforderungen nicht für Quantencomputing gerüstet. Zudem bringt das schnell wachsende Arbeitsvolumen, das die KI einnimmt, bestehende Kühl- und Energiesysteme an ihre Grenzen. Viele Länder treffen bereits entsprechende Vorkehrungen.

Bereiten sich Länder auf eine Disruption durch Quantencomputer vor?

	Ist eine nationale Strategie zur Vorbereitung auf Quantentechnologie vorhanden?	Ist ein Zeitplan für Post-Quanten-Kryptografie festgelegt?
USA	Ja	Ja
Vereinigtes Königreich	Ja	Ja
Deutschland	Ja	Nein
Singapur	Ja	Ja
Indien	Ja	Ja
Irland	Ja	Nein
Vereinigte Arabische Emirate	Ja	Nein
Südafrika	Ja	Nein
Brasilien	Ja	Nein
Indonesien	Ja	Ja
Australien	Ja	Ja
Frankreich	Ja	Nein

Quelle: Economist Impact (2025), offizielle nationale Quellen (2025)

Warum spielen diese systemischen Risiken eine Rolle?

Systemische Risiken wirken wie ein Katalysator auf die Schwachstellen im Ökosystem eines Rechenzentrums. Ihre Folge- und Wechselwirkungen erstrecken sich über technologische, ökologische und wirtschaftliche Aspekte hinweg, verstärken die operative Komplexität und machen das ganze System anfälliger.

Instabile Lieferketten und Marktkonzentration	Auflagen zu Umwelt und natürlichen Ressourcen	Veraltete Technologie	Compliance mit Gesetzen und Vorschriften
Geografische Konzentration und Abhängigkeit von Lieferunternehmen	Nachfrage nach erneuerbaren Energien	Cyberbedrohungen	Datenlokalisierung
Engpässe hinsichtlich Ressourcen und Personal	Wasserbedarf	Innovative Kühllösungen	Einschränkungen bezüglich Flächennutzung

Eine facettenreiche Risikolandschaft erfordert koordiniertes Vorgehen.

Das Zusammenspiel aus geopolitischen, ökologischen, technologischen und wirtschaftlichen Herausforderungen stellt die Resilienz digitaler Infrastrukturen auf die Probe. Trotz der Komplexität systemischer Risiken lassen sich Schwachstellen im Rahmen von gemeinsam umgesetzten, gezielten Strategien minimieren. Die folgenden Empfehlungen richten sich an Rechenzentren, Unternehmen und politische Agierende mit dem Ziel, eine stabilere, nachhaltige Infrastruktur für die Zukunft zu entwickeln.

Wie können Rechenzentren, Unternehmen und Regierungseinrichtungen zur Resilienzerhöhung beitragen?

Die geografische Verteilung ist für digitale Resilienz von zentraler Bedeutung.
Um gegenseitige Abhängigkeiten zu vermeiden und die Betriebssicherheit zu erhöhen, empfiehlt sich eine breitere Aufstellung der Infrastruktur – über Grenzen, Rechtssysteme und Klimazonen hinweg. Die Politik kann diesen Wandel unterstützen, indem sie Investitionen in bisher weniger genutzten Regionen mit stabilen Stromnetzen und günstigen Umweltbedingungen fördert, wie es in den skandinavischen Ländern der Fall ist. Solche Schritte sind jedoch mit zusätzlichen Risiken in Bezug auf Datensicherheit verbunden.

Die Diversifizierung der Lieferketten für digitale Infrastrukturen reduziert systemische Risiken. Unternehmen sollten bei der Beschaffung auf Dual Sourcing bzw. Multiple Sourcing in risikoarmen Regionen setzen und mit alternativen Lieferunternehmen kritischer Komponenten zusammenarbeiten. Durch Investitionen in die inländische Produktion von Halbleitern und Kühltechnologien können Regierungseinrichtungen die Abhängigkeit von Importen reduzieren bzw. die strategische Unabhängigkeit fördern.

Regulatorische Voraussicht und Szenarienplanung sind die Grundlage für eine zukunftsfähige Infrastruktur. Betreibende von Rechenzentren sollten der Früherkennung von Änderungen hinsichtlich Flächennutzungsplänen, Umweltauflagen und Nachhaltigkeitsvorgaben einen hohen Stellenwert zuschreiben, um Fehlinvestitionen zu vermeiden und rechtliche Compliance sicherzustellen. Angesichts der immer strengeren Vorschriften in Bezug auf Abwärmenutzung, Lärm und Wassereinsparung empfiehlt sich der Einsatz von Prognose-Tools, um zukünftige Risiken einzuschätzen und je nach Situation die richtigen Entscheidungen in Bezug auf Infrastrukturen und Investitionen treffen zu können.

Der Ausbau eigener Kapazitäten stärkt die Souveränität und Sicherheit.
Die inländische Entwicklung von Cloud-Diensten und Kernkomponenten wie Halbleitern und fortschrittlichen Kühlsystemen ist für die nationale Resilienz unerlässlich. Maßnahmen der Regierung – ob Industriepolitik, Investitionen in F&E oder die strategische Einstufung von Rechenzentren als kritische Infrastruktur – tragen zur digitalen Souveränität eines Landes bei und reduzieren die Abhängigkeit vom Ausland. Beispiele hierfür sind Brasilien und Großbritannien.

Eine Kombination aus erneuerbaren und zuverlässigen Energiequellen ist unumgänglich.
Rechenzentren stehen unter dem Druck, der rasant steigenden Nachfrage gerecht zu werden, jedoch auch wetter- und netzbedingte Stromausfälle zu vermeiden und ihren CO^2-Fußabdruck zu reduzieren. Die Lösung: Investitionen sowohl in Solar- und Windenergie als auch in Kernenergie und Speichertechnologien – netzgebunden und netzunabhängig. Mit Vorstößen wie die von Amazon und Google getätigten Investitionen in kleine modulare Kernreaktoren (SMR) bewegt sich der Sektor in Richtung einer zuverlässigeren, umweltschonenderen Stromversorgung. Regierungen sollten zudem höhere Standards für redundante Stromversorgung durchsetzen und die Planung netzunabhängiger Energieversorgung unterstützen.

Der Schlüssel für eine sichere digitale Zukunft: Technologien gegen die Bedrohung durch Quantencomputer. Mit Quantencomputing am Horizont ist Post-Quantum-Kryptografie von zentraler Bedeutung. Rechenzentren sollten ihre kryptografischen Fähigkeiten ausbauen und erste Pilotprojekte mit quantenresistenten Algorithmen in die Wege leiten. Auch Regierungen können die digitale Infrastruktur in der neuen Ära des Quantencomputing schützen, etwa durch nationale Strategien, die Förderung von F&E und die Einführung neuer Sicherheitsstandards, wie dies in den USA und zum Teil auch in Brasilien der Fall ist.

Das Konzept der Kreislaufwirtschaft muss in den nachhaltigen Ausbau der Rechenzentrumsbranche einbezogen werden. Durch Abwärmenutzung, Wasserrückgewinnung und höhere Energieeffizienz können Rechenzentren Umweltbelastungen und betriebliche Ineffizienzen deutlich senken. Mit Gesetzen und Anreizen sollte die Kreislaufwirtschaft auch auf Regierungsebene gefördert werden. Modelle aus Deutschland, Dänemark und Singapur zeigen, wie Innovation und Nachhaltigkeit durch gesetzliche Vorgaben verbessert werden, während der digitale Markt und die Nachfrage nach KI weltweit boomt.

Durch die Umsetzung von Kernstrategien wie Diversifizierung, vorausschauende Planung, Risikomanagement, Ausbau nationaler Kapazitäten und Kreislaufwirtschaft lassen sich die Resilienz und Nachhaltigkeit digitaler Infrastrukturen stärken.

Schnelles, koordiniertes und entschlossenes Handeln hilft, aufkommende Bedrohungen zu bewältigen und langfristige Performance sowie Wertschöpfung in einem zunehmend dynamischen globalen Umfeld zu sichern.

Im Auftrag von FM

Ansichten und Meinungen, die in diesem Artikel zum Ausdruck gebracht werden, stammen von der verfassenden Person und spiegeln nicht zwingendermaßen die offizielle Politik oder Haltung von FM wider.