

FEL-Auslandsstipendium Rafail Kasapis

© shutterstock_ktdesign

Energiewende und Cybersicherheits-Regulatorik

Vereinigte Staaten von Amerika

Autoren Allgemein USA: **Rafail Kasapis / Chiara Bassini**
Autor Energiewende und Cybersicherheit: **Rafail Kasapis**

Datum/Stand: **November 2025**

Allgemein

Stand Energiewende

Die USA haben unter der Biden-Harris-Regierung (2021–2024) im Rahmen der *Long-Term Strategy for Net-Zero Emissions* und des Inflation Reduction Act (IRA, 2022) das Ziel festgelegt, bis 2035 eine klimaneutrale Stromversorgung und bis 2050 Klimaneutralität der Gesamtwirtschaft zu erreichen. Diese ambitionierte Agenda wird durch den IRA, das bislang größte US-Klimaprogramm mit über 370 Mrd. USD, finanziell unterstützt.¹

Er fördert Investitionen in erneuerbare Energien, grünen Wasserstoff, Energiespeicher, Elektromobilität sowie die Modernisierung der Netzinfrastruktur. Im Jahr 2023 wurde in den USA eine Rekordkapazität von 42 GW an neuen erneuerbaren Energien ans Netz gebracht (Solar rund 32,4 GW² und Wind mit rund 8,5 GW³). Der Anteil erneuerbarer Energien am US-Strommix erreichte 2024 etwa 24 %, während Kernenergie rund 20 % und fossile Energieträger 56 % beitrugen. Führende Bundesstaaten beim Ausbau sind Texas, Kalifornien und Florida.⁴

Seit dem Amtsantritt von Präsident Donald Trump im Januar 2025 hat sich die energie- und klimapolitische Ausrichtung verschoben: Die neue Regierung setzt stärker auf Energiesouveränität und Wirtschaftswachstum, hat den Austritt aus dem Pariser Klimaabkommen eingeleitet (noch nicht vollzogen) und die Förderung für Offshore-Wind und Elektromobilität reduziert. Zugleich wurden Genehmigungsverfahren für Öl-, Gas- und LNG-Projekte beschleunigt.

Dennoch bleibt der Inflation Reduction Act als Bundesgesetz in Kraft. Zahlreiche Bundesstaaten mit eigener Klimagesetzgebung, wie Kalifornien, New York, Massachusetts und Washington, führen ihre Programme weiter und nutzen weiterhin IRA-Fördermittel. Der Übergang zu einer klimaneutralen Energieversorgung verlangsamt sich somit, wird aber nicht gestoppt.

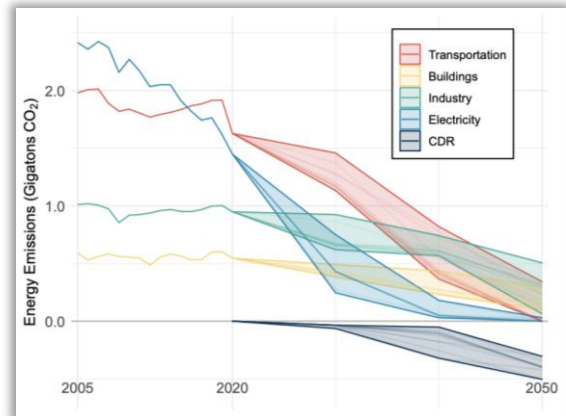


Abbildung 1: U.S. Energie-CO2-Emissionen bis 2050 nach Wirtschaftssektoren.¹

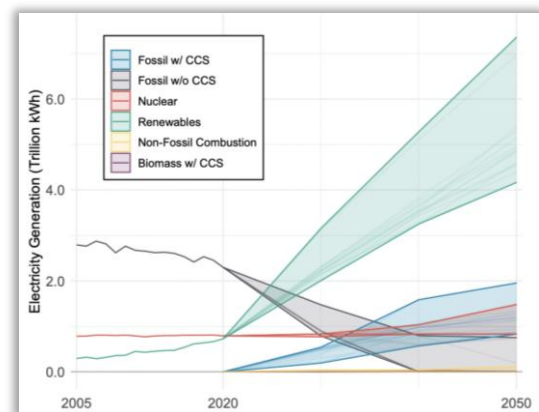


Abbildung 2: U.S. Stromerzeugung 2005-2050. Erzeugung nach Quellen in Milliarden Kilowattstunden.¹



Status Quo: Voraussetzungen für die Digitalisierung der Energiewende

Technische Voraussetzungen

- Das US-Stromnetz ist föderal fragmentiert und vielerorts überlastet.
- Über 1 000 GW Solar- und 250 GW Windprojekte warten derzeit auf Netzanschluss.
- Laut DOE muss sich die Netzkapazität bis 2050 mindestens verdoppeln, um die Klimaziele zu erreichen.
- Der Digitalisierungsgrad ist weit fortgeschritten. Bereits Ende 2023 waren über 80 % der Gebäude mit intelligenten Zählern ausgestattet und Smart Grids werden zunehmend integriert.⁵
- Gleichzeitig nehmen Cyberrisiken deutlich zu, was Investitionen in Netzsicherheit notwendig macht.

Politische Voraussetzungen

- Unter der Biden-Harris-Regierung wurden durch den Inflation Reduction Act (IRA) wichtige Rahmenbedingungen für Investitionen in Netze und Digitalisierung geschaffen.⁶
- Seit Präsident Trumps Amtsantritt (2025) liegt der Fokus stärker auf Energiesouveränität und Deregulierung; einige Förderprogramme wurden reduziert.
- Dennoch bleiben zentrale Infrastrukturprojekte bestehen, und Bundesstaaten wie Kalifornien, New York und Massachusetts führen ihre Digital-Energy-Initiativen weiter.

Welche Faktoren sind für die Energiewende bzw. Digitalisierung des Energiesektors förderlich und welche nicht?

Förderlich

- Der Inflation Reduction Act (IRA) bleibt der wichtigste Investitionsmotor und sichert Förderung für die Energiewende.
- Die USA verfügen über eine hohe Innovationskraft und führende Position in KI, Automatisierung und digitalen Energielösungen, was die Netzsteuerung und Energieeffizienz verbessert.⁷
- Die weit verbreitete Smart-Meter-Infrastruktur ermöglicht datenbasierte Netzoptimierung und flexible Verbrauchersteuerung.
- Bundesstaatliche Programme in Kalifornien, New York oder Massachusetts treiben den Ausbau erneuerbarer Energien unabhängig von der Bundespolitik weiter voran.

Nicht förderlich

- Netzengpässe und ein massiver Anschluss-Backlog bei Solar- und Windprojekten bremsen den Ausbau.⁷
- Die uneinheitliche Regulierung zwischen Bund, Staaten und Netzbetreibern erschwert Investitionen und Planungssicherheit.
- Der politische Kurswechsel seit 2025 führt zu Unsicherheit über künftige Förderbedingungen.
- Cyberrisiken und der steigende Strombedarf durch Rechenzentren und KI belasten die Netzstabilität.

Allgemeine Digitalisierungstrends in den Vereinigten Staaten

- Die USA bleiben Weltmarktführer in Künstlicher Intelligenz (KI). 2023–2025 wurden über 100 neue KI-Basismodelle entwickelt.⁸ KI wird zunehmend für Energieprognosen, Netzsteuerung und Effizienzanalysen eingesetzt.⁹
- Der Energiebedarf digitaler Infrastrukturen wächst rasant: Rechenzentren verbrauchen rund 4 % des US-Stroms und könnten bis 2027 auf 7 % steigen.¹⁰
- Große Technologieunternehmen wie Amazon, Microsoft und OpenAI investieren in Kernenergie und erneuerbare Projekte, um ihre Rechenzentren klimaneutral zu betreiben.¹¹
- Internet of Things (IoT), Smart Grids und Blockchain-Technologien werden breit in Stadt- und Netzsystemen eingesetzt, um Energieflüsse effizienter und transparenter zu gestalten.¹²
- Quanteninformatik entwickelt sich zu einem strategischen Schwerpunkt der US-Forschung und soll künftig bei der Optimierung komplexer Energiesysteme eingesetzt werden.¹³



Fokusthema Cybersecurity Regulatorik

Neue Trends im Bereich der Cybersecurity Regulatorik

• Erhöhung der Standards und Transparenz von Vorfällen (Incident Reporting)	• Die US-Regierung hat mit der Executive Order 14028 (2021), dem National Security Memorandum (2021) und der National Cyber Strategy (2023) einen umfassenden strategischen Rahmen geschaffen, der von konkreten Verbesserungen der Cybersicherheit der Bundesbehörden bis hin zum Schutz kritischer Infrastrukturen reicht.¹⁴ • Die Cybersecurity and Infrastructure Security Agency (CISA) hat Richtlinien für staatliche, lokale Behörden und den privaten Sektor erstellt, um Cybervorfälle zu melden. Diese sollen schnelle Reaktionen und den Informationsaustausch fördern, um Vorfälle einzudämmen. Das National Institute of Standards and Technology (NIST) bietet einen Rahmen, der einen strukturierten Ansatz zur Vorfallsmeldung und der Bewältigung unterstützt.¹⁵
• Organisationsübergreifende Zusammenarbeit zu Standards und Trainings	• Die organisationsübergreifende Zusammenarbeit von Ministerien in den USA bei der Umsetzung von Cybersecurity-Standards wie zur Zero Trust Architecture im Rahmen von NIST¹⁶ oder der Cybersecurity Baseline in NAURAC ist entscheidend, um eine ganzheitliche Abwehr gegen digitale Bedrohungen zu gewährleisten. Durch die enge Koordination von Ressorts wird eine kohärente nationale Strategie zur Sicherung kritischer Infrastrukturen entwickelt und implementiert.¹⁷
• Integration von Technologien und Compliance	• Die Integration von KI in die Praktiken der Cybersicherheit wird zunehmend entscheidend für die Erkennung und Reaktion auf Bedrohungen. Unternehmen werden ermutigt, KI-gesteuerte Lösungen zu nutzen, um ihre Sicherheitslage angesichts der sich entwickelnden Bedrohungen zu verbessern.^{8,18} • Die Verlagerung hin zu Zero-Trust-Sicherheitsmodellen gewinnt an Zugkraft, wobei betont wird, dass keine Entität standardmäßig vertrauenswürdig sein sollte, wodurch potenzielle Angriffsflächen reduziert werden.

Welche Faktoren sind für die Regulatorik der Cybersicherheit förderlich und welche nicht?

Förderlich • Die US-Regierung hat Strategien wie die National Cybersecurity Strategy initiiert, die den Bedarf an modernen, maßgeschneiderten Regulierungsrahmen betonen, die sich an sektorspezifischen Risikoprofilen orientieren. Dieser Ansatz zielt darauf ab, die Vorschriften zu harmonisieren, was ein effektiveres Regulierungsumfeld fördern könnte. • Durch Incidents Reporting und Standardisierung im Reporting wird die Cybersicherheit in den USA erhöht, indem Bedrohungen besser sichtbar werden, der rasche Informationsaustausch erleichtert, die nationale Sicherheit gestärkt und eine bessere Reaktion auf Vorfälle in allen Bereichen der kritischen Infrastruktur gefördert wird.	Nicht förderlich • Durch den föderalen Staat obliegen einige Kompetenzen nicht der Bundesregierung, sondern ausschließlich dem jeweiligen Bundesstaat. Regulierung und Cybersicherheitsanforderungen in verschiedenen Staaten können zu Teilen miteinander in Konflikt stehen.¹⁹ • Die sich rasch entwickelnden Cyberbedrohungen stellen herkömmliche statische und rückwärtsgewandte Regulierungsmodelle vor Herausforderungen. Die Vorschriften müssen anpassungsfähig sein, um mit dem technologischen Fortschritt und neuen Bedrohungen Schritt zu halten.
--	--



Wichtige Akteure

Anlaufstellen für Energie und Digitalisierung in den Vereinigten Staaten

Federal Energy Regulatory Commission (FERC) – Zuständig für die Regulierung des zwischenstaatlichen Energiehandels und die Aufsicht über Großhandelspreise für Strom, Erdgas und Öl. → www.ferc.gov

Department of Energy (DOE) – Hauptverantwortliche Bundesbehörde für Energiepolitik, Forschung und Innovation. Das DOE fördert erneuerbare Energien, Netzsicherheit und Digitalisierung, unter anderem durch das *Office of Cybersecurity, Energy Security and Emergency Response (CESER)*. → www.energy.gov

Energy Information Administration (EIA) – Liefert unabhängige Daten und Analysen zur Energieversorgung der USA. → www.eia.gov

Environmental Protection Agency (EPA) – Zuständig für Umwelt- und Klimaschutzprogramme im Energiesektor. → www.epa.gov

Weitere relevante Organisationen:

United States Energy Association (USEA) – www.usea.org

National Association of Regulatory Utility Commissioners (NARUC) – www.naruc.org

Smart Electric Power Alliance (SEPA) – www.sepapower.org

National Association of State Energy Officials (NASEO) – www.naseo.org

Referenzen

¹ <https://www.whitehouse.gov/wp-content/uploads/2021/10/us-long-term-strategy.pdf>

² <https://de.statista.com/statistik/daten/studie/29265/umfrage/neu-installierte-nennleistung-der-solarenergie-in-den-usa-seit-2004/>,

³ <https://www.energy.gov/sites/default/files/2023-08/land-based-wind-market-report-2023-edition.pdf>

⁴ <https://www.statista.com/statistics/183396/proportion-of-renewables-in-us-electricity-generation-since-2000/>

⁵ <https://www.power-grid.com/smart-grid/metering/smart-meter-penetration-surpasses-80-in-north-america/>

⁶ <https://home.treasury.gov/policy-issues/inflation-reduction-act>

⁷ <https://www.boeckler.de/de/boeckler-impuls-aufbruchstimmung-in-den-usa-62062.htm>

⁸ https://hai-production.s3.amazonaws.com/files/hai-ai-index-2025-policy-highlights.pdf?utm_source=chatgpt.com

⁹ <https://www.gtai.de/de/trade/usa/branchen/ki-investitionen-in-den-usa-steigen-sprunghaft-an-1775554>

¹⁰ https://www.mckinsey.com/industries/private-capital/our-insights/how-data-centers-and-the-energy-sector-can-sate-ais-hunger-for-power?utm_source=chatgpt.com

¹¹ <https://www.nasdaq.com/articles/billionaires-bill-gates-jeff-bezos-and-sam-altman-are-investing-nuclear-energy-hand-over>

¹² <https://technologymagazine.com/top10/top-10-technology-trends-for-2024>

¹³ <https://www.quantum.gov/>

¹⁴ <https://www.dhs.gov/publication/harmonization-cyber-incident-reporting-federal-government>

¹⁵ <https://www.nist.gov/cybersecurity>

¹⁶ <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf>

¹⁷ <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>

¹⁸ <https://security.googleblog.com/2024/11/leveling-up-fuzzing-finding-more.html>

¹⁹ <https://www.naruc.org/core-sectors/critical-infrastructure-and-cybersecurity/cybersecurity-for-utility-regulators/cybersecurity-baselines/>



KONTAKT

Jana Hammerer
Expertin Digitale Technologien

Tel.: +49 30 66 777-825
E-Mail: jana.hammerer@dena.de

Deutsche Energie-Agentur GmbH (dena)

Chausseestraße 128 a
10115 Berlin

www.dena.de | www.future-energy-lab.de

Stand 11/2025

Alle Rechte sind vorbehalten. Die Nutzung steht unter dem Zustimmungsvorbehalt der dena.