

Infrastruktursystem Staat und Verwaltung

Ergebnisse aus dem Resilienz-Radar



Carolin Kahlisch
Christoph Kehl
Nona Bledow
Michaela Evers-Wölk
Pauline Rioussset

Juni 2026
Foresight-Report Nr. 9

Inhalt

1	Einleitung	3
2	Übersicht über aktuelle Trends	7
2.1	Digitale Transformation von Staat und Verwaltung	8
2.2	Struktureller Wandel des öffentlichen Sektors unter demografischem, personellem und fiskalischem Druck	12
2.3	Wachsende ökologische Herausforderungen an staatliche Steuerung und Finanzierung	17
2.4	Wandel im Verhältnis von Staat und Zivilgesellschaft	22
3	Systemische Risiken und ihre Auswirkungen auf das Infrastruktursystem Staat und Verwaltung	25
3.1	Status quo der Gefährdungslagen und Entwicklungsdynamiken	28
3.2	Gefährdungslagen im Zuge der Transformation	39
4	Fokusthemen	45
4.1	Fokusthema 1: Autonome KI-Agenten in der Verwaltung als operative Infrastruktur	45
4.2	Fokusthema 2: Verlässlichkeit staatlicher Information im Kontext synthetisch erzeugter Medien	46
5	Methodik und Vorgehen	47
6	Literatur	49
7	Anhang	59
7.1	Abbildungen	59
7.2	Kästen	59

1 Einleitung

Das Infrastruktursystem Staat und Verwaltung umfasst die institutionellen Strukturen, durch die Recht gesetzt und durchgesetzt, öffentliche Sicherheit gewährleistet sowie Sozial- und Verwaltungsleistungen erbracht werden. Damit bildet es die institutionelle Grundlage für das Funktionieren von Wirtschaft und Gesellschaft sowie für demokratische Teilhabe und rechtsstaatliche Ordnung. Das System schließt ein breites Spektrum parlamentarischer, exekutiver und judikativer Akteure auf Bundes-, Landes- und kommunaler Ebene ein, mit unterschiedlichen, teils verfassungsrechtlich verankerten Aufgaben und Zuständigkeiten.

Das System von Staat und Verwaltung in Deutschland ist historisch gewachsen und durch eine komplexe, mehrstufige und föderale Struktur geprägt (Abbildung 1.1). Es umfasst eine Vielzahl von Akteuren mit unterschiedlichen Aufgaben, Kompetenzen und Zuständigkeiten, die sich auf Bund-, Länder- und kommunaler Ebene verteilen. Die Steuerung erfolgt durch ein Zusammenspiel von parlamentarischen, exekutiven und judikativen Institutionen sowie durch hoheitliche und serviceorientierte Funktionen:

- *Parlamentarische Steuerung:* Die parlamentarische Steuerung umfasst Bundestag, Bundesrat und Landtage als legislative Kerninstitutionen. Sie beschließen Gesetze, kontrollieren die Regierung und gestalten die politische Willensbildung durch Wahlen, Debatten und öffentliche Konsultationen. Zentrale Akteure sind Abgeordnete, Fraktionen, Ausschüsse sowie Parteien und Verbände, die an der Meinungs- und Entscheidungsfindung mitwirken.
- *Regierungen und Verwaltungen:* Sie vollziehen Gesetze und erbringen öffentliche Aufgaben auf Bundes-, Landes- und kommunaler Ebene. Die Bundesregierung, Landesregierungen und kommunalen Verwaltungen agieren in einer hierarchischen Struktur, gestützt auf Behörden und öffentliche Unternehmen. Die Aufgaben reichen von der Gewährung von Sozialleistungen im Einzelfall bis zur großflächigen Infrastrukturplanung, wobei die Länder und Kommunen im Rahmen ihrer jeweiligen Zuständigkeiten über eigene Verwaltungskompetenzen verfügen.
- *Verwaltungsdienstleistungen:* Bürger/innen sowie Unternehmen und Selbstständige sind auf eine Vielzahl administrativer Leistungen angewiesen – von der Ausstellung von Dokumenten und Genehmigungen über die Bearbeitung diverser Anträge bis hin zu steuerlichen und gewerberechtlichen Verfahren. Diese Leistungen werden auf allen Verwaltungsebenen erbracht, zunehmend auch digital über E-Government-Portale. Zentrale Akteure sind Bundes-, Landes- und kommunale Behörden sowie nachgeordnete Einrichtungen.
- *Justiz:* Die Judikative sichert als unabhängige Gewalt die Rechtmäßigkeit durch ein mehrstufiges Gerichtssystem, vom Bundesverfassungsgericht bis zu den Amtsgerichten. Richter/innen, Staats- und Rechtsanwält/innen handeln nach den Prinzipien der Unparteilichkeit und Gesetzesbindung. Die Justizverwaltung liegt bei den Ländern; die Verfahrensgesetze sind bundeseinheitlich geregelt.
- *Innere Sicherheit und Verteidigung:* Hoheitliche Sicherheitsfunktionen umfassen Verteidigung, Polizei, Nachrichtendienste und Zoll, die für Gefahrenabwehr, Strafverfolgung und Grenzschutz zuständig sind. Die Zusammenarbeit zwischen Bund und Ländern wird durch Gremien

wie die Innenministerkonferenz koordiniert, basierend auf Polizeirecht und bundesweiten Sicherheitsgesetzen.

Abbildung 1.1 Systembild



Eigene Darstellung

Die Stärkung der Resilienz im Infrastruktursystem Staat und Verwaltung erfordert eine gezielte Modernisierung zentraler Strukturen, um die Handlungs- und Leistungsfähigkeit des Staates unter Bedingungen digitaler, gesellschaftlicher und ökologischer struktureller Veränderungen langfristig zu sichern. Drei zentrale Transformationsziele konnten für das Infrastruktursystem identifiziert werden:

- **Organisations- und Personalmodernisierung:** Eine zukunftsfähige öffentliche Verwaltung erfordert moderne Arbeitsweisen, Führungsstrukturen und Formen der Zusammenarbeit. Dazu gehören der Aufbau einer zeitgemäßen Führungskultur, die Förderung von Motivation und Leistungsorientierung sowie die Etablierung professioneller Change-Management-Strukturen. Moderne Arbeitsformen – agil, hybrid oder kollaborativ – können mehr Flexibilität und Innovationsfähigkeit schaffen. Gleichzeitig sind Qualifizierung und kontinuierliche Weiterbildung entscheidend, um den wachsenden Kompetenzanforderungen gerecht zu werden.
- **Digitalisierung und technologische Modernisierung:** Die Digitalisierung bildet eine zentrale Grundlage für höhere Effizienz, Transparenz und Krisenfestigkeit des Infrastruktursystems. Der Ausbau nutzungsfreundlicher E-Government-Angebote, die Automatisierung von Prozessen, der Einsatz KI-gestützter Verfahren sowie die Konsolidierung interoperabler IT- und Registerstrukturen stärken die Leistungsfähigkeit der Verwaltung. Digitale Sicherheit, Open Data und nachhaltige IT-Infrastrukturen tragen zudem zu Vertrauen, Teilhabe und Ressourcenschonung bei.

- *Ökologische Nachhaltigkeit und Klimaneutralität:* Angesichts des Klimawandels sind umfassende Maßnahmen erforderlich, um die Treibhausgasemissionen des Infrastruktursystems Staat und Verwaltung zu senken und damit einen Beitrag zur angestrebten Klimaneutralität Deutschlands bis 2045 zu leisten. Klimaneutrale Gebäude und Liegenschaften, nachhaltige Beschaffung, CO₂-arme Mobilität und energieeffiziente IT-Strukturen sollen die Bundesverwaltung bis 2030 klimaneutral ausrichten. Dies gilt auch für die meisten Bundesländer, die ebenfalls Initiativen zur treibhausgasneutralen Landesverwaltung verabschiedet haben. Staat und Verwaltung übernehmen dabei eine Vorbildfunktion und leisten zugleich einen strukturellen Beitrag zur langfristigen Stabilität und Resilienz des Systems.

Kernergebnisse

Prägende Entwicklungen

Vier Trendcluster prägen derzeit das Infrastruktursystem Staat und Verwaltung:

- *Digitale Transformation:* Digitalisierung, Automatisierung und KI führen zu grundlegenden Veränderungen in Arbeitsweisen, Steuerungslogiken und Bürger-Staat-Interaktionen.
- *Struktureller Wandel des öffentlichen Sektors:* Alternde Belegschaften, Fachkräftemangel und enger werdende Haushalts- und Investitionsspielräume (insbesondere kommunal) verknappen Kapazitäten und erzwingen Priorisierung.
- *Wachsende ökologische Herausforderungen:* Klimawandelfolgen, Extremwetterrisiken und Klimaziele erhöhen den Druck auf Planung, Finanzierung, Beschaffung und Monitoring.
- *Wandel im Verhältnis von Staat und Zivilgesellschaft:* Zunehmende Polarisierung und Vertrauenserosion treffen auf eine verschärfte hybride Bedrohungslage (Cyber/Desinformation) und verändern damit die Voraussetzungen politischer Steuerung und öffentlicher Kommunikation.

Status quo der Gefährdungslagen

Die aktuelle Gefährdung des Infrastruktursystems durch die meisten systemischen Risiken ist insgesamt als eher hoch einzustufen. Die Funktionsfähigkeit und Stabilität des Infrastruktursystems werden derzeit vor allem durch Versorgungsengpässe, etwa den Fachkräftemangel und finanzielle Engpässe, aber auch Cyberkriminalität, geopolitische Konflikte und gesellschaftliche Polarisierung gefährdet.

Zukünftige Entwicklung der Gefährdungslagen

In den kommenden Jahren ist von einer weiter steigenden Gefährdungslage auszugehen. Treiber dieser Entwicklung sind die fortschreitende Digitalisierung, anhaltende geopolitische Spannungen und Polarisierungstendenzen in der deutschen Gesellschaft. Zusätzlich verstärken

Cyberkriminalität, die wachsende Machtkonzentration privatwirtschaftlicher Akteure und die Verbreitung von Desinformation den Druck auf das Infrastruktursystem.

Gefährdungslagen im Zuge der Transformation

Die Umsetzung der zentralen Transformationsziele – insbesondere der Organisations- und Personalmodernisierung, der Digitalisierung und technologischen Modernisierung des Infrastruktursystems sowie der ökologischen Nachhaltigkeit und Klimaneutralität – wird durch ausgeprägte Pfadabhängigkeiten erheblich erschwert. Dazu zählen eine unzureichende politische Priorisierung, historisch verfestigte Organisationsstrukturen und Verwaltungskulturen, an bestehenden Systemen orientierte Arbeitsweisen sowie begrenzte digitale Kompetenzen. Hinzu kommen finanzielle und personelle Engpässe sowie langfristige Bindungen durch bestehende Infrastrukturinvestitionen.

Fokusthemen

Für eine Vertiefung im Resilienz-Check werden zwei Fokusthemen vorgeschlagen, die an die beschriebenen Trendcluster anschließen: Fokusthema 1: Autonome KI-Agenten in der Verwaltung als operative Infrastruktur sowie Fokusthema 2: Verlässlichkeit staatlicher Information im Kontext synthetisch erzeugter Medien.

2 Übersicht über aktuelle Trends

Staat und Verwaltung in Deutschland sind durch eine komplexe föderale Struktur geprägt. Zuständigkeiten, Ressourcen und Entscheidungsbefugnisse verteilen sich je nach Politikfeld in unterschiedlicher Weise auf Bund, Länder und Kommunen. Überlagert werden diese Strukturen durch EU-Richtlinien und -Verordnungen sowie internationale Abkommen, die den Handlungsspielraum staatlicher Akteure auf allen Ebenen einschränken. Diese Mehrebenengovernance führt dazu, dass das Infrastruktursystem Staat und Verwaltung von komplexen internen Steuerungslogiken, multilateralen Abstimmungsprozessen und langfristigen rechtlichen Pfadabhängigkeiten geprägt ist.

Die folgenden Abschnitte präsentieren die Ergebnisse der Trendanalyse anhand der STEEP-Kategorien (social, technological, economic, ecological, political) als heuristischem Raster. Für jede Kategorie wurden auf Basis systematischer Literatur- und Quellenanalyse empirisch nachweisbare Trends identifiziert, die das Infrastruktursystem seit mindestens 3 Jahren maßgeblich prägen. Thematisch verwandte Trends wurden zu Trendclustern zusammengefasst, die jeweils übergeordnete Entwicklungslinien abbilden. Die Cluster orientieren sich an den STEEP-Kategorien, ohne diese strikt abzubilden; Überschneidungen zwischen den Kategorien sind inhaltlich unvermeidbar.

Die Kategorie „political“ wird im Folgenden nicht als eigenständiges Cluster ausgewiesen: Politische Trends wirken im Infrastruktursystem Staat und Verwaltung in alle anderen STEEP-Kategorien hinein und sind daher in den beschriebenen Trendclustern jeweils enthalten. Insgesamt lassen sich so vier zentrale Trendcluster unterscheiden:

- *Wandel im Verhältnis von Staat und Zivilgesellschaft:* Vertrauensverlust, gesellschaftliche Polarisierung und Bürokratielasten stehen einer Ausweitung neuer Beteiligungsformate gegenüber.
- *Digitale Transformation und Verwaltungsmodernisierung:* Digitalisierungsdruck, technologische Erneuerung und der Ausbau digitaler Infrastrukturen verändern Arbeitsweisen, Steuerungslogiken und Bürger-Staat-Interaktionen im öffentlichen Sektor.
- *Struktureller Wandel des öffentlichen Sektors:* Alternde Belegschaften, struktureller Fachkräftemangel und enger werdende Haushaltsspielräume erzwingen einen tiefgreifenden Wandel im öffentlichen Sektor.
- *Ökologische Herausforderungen staatlicher Steuerung:* Steigende Klima- und Biodiversitätsrisiken, wachsende Schadenskosten und neue Anforderungen an Anpassungs- und Steuerungsinstrumente erhöhen den Handlungsdruck auf staatliche Akteure.

Zu jedem Trendcluster wurden zusätzlich Emerging Issues identifiziert. Darunter fallen soziotechnische Entwicklungen, die sich noch nicht als Trend konsolidiert haben, aber in der Analyse als potenziell systemrelevant eingestuft wurden. Aufgenommen wurden Zukunftsentwicklungen, die Relevanz für die Resilienz wichtiger Funktionsbereiche des Systems aufweisen könnten, auch wenn ihre Entwicklungsrichtung noch unsicher ist. Ihre Bewertung ist daher mit höherer Unsicherheit behaftet als die der beschriebenen Trends.

2.1 Digitale Transformation von Staat und Verwaltung

Parlamente, Ministerien und die öffentliche Verwaltung durchlaufen eine umfassende technologische Modernisierung, die durch erhebliche Investitionen in digitale Infrastruktur und Prozessoptimierung vorangetrieben wird. Diese Transformation findet auf Bund-, Länder- und Kommunalebene statt und zielt auf Effizienzgewinne, bessere Bürgerbeteiligung und schnellere Verwaltungsvorgänge. Gleichzeitig entstehen neue Risiken: wachsende Cyberbedrohungen, kritische technische Abhängigkeiten, Fragmentierung über föderale Ebenen hinweg sowie Diskriminierungs- und Fairnessrisiken durch KI-gestützte Entscheidungsprozesse. Der Trendcluster betrifft alle Bereiche des Systembilds.

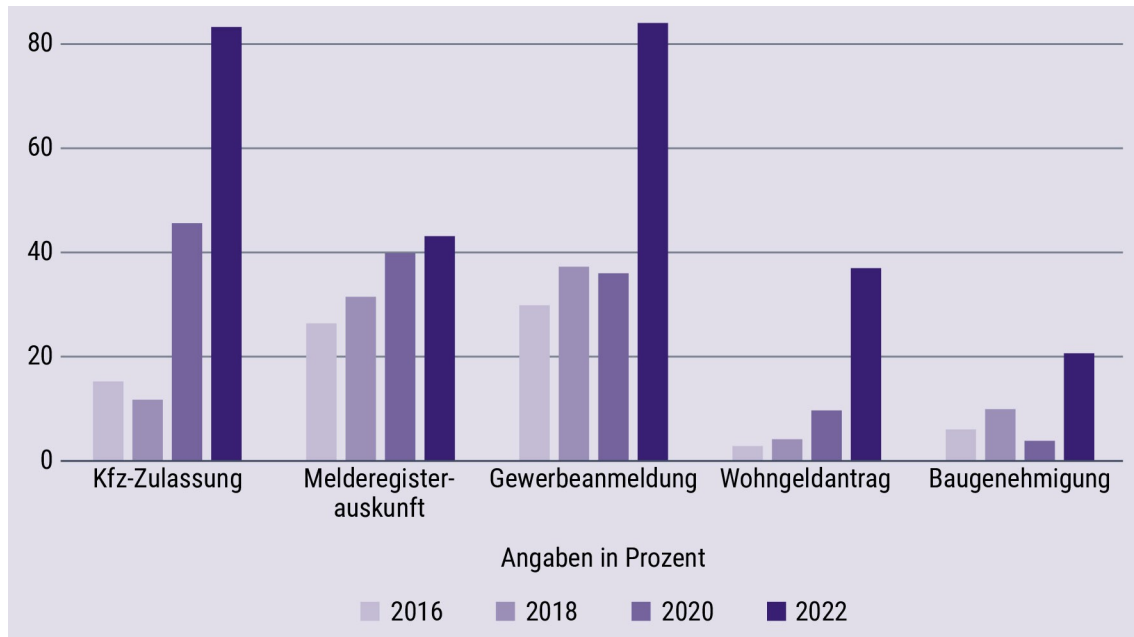
Die digitale Transformation von Staat und Verwaltung ist für Deutschland von hoher strategischer Relevanz, da sie direkt die Funktionsfähigkeit des Staates, die Wettbewerbsfähigkeit der Wirtschaft und die Lebensqualität der Bürger/innen beeinflusst. Sie wird in Deutschland seit über 25 Jahren systematisch vorangetrieben (Bitkom e. V. 2025b; Schuppan et al. 2025). Wichtige gesetzliche Meilensteine sind das E-Government-Gesetz (eGovG)¹ von 2013, das sich an die Bundesbehörden richtet und unter anderem die Einführung der elektronischen Akte regelt, sowie das Onlinezugangsgesetz (OZG)² von 2017. Das OZG verpflichtet Bund, Länder und Kommunen, bis spätestens Ende 2022 sämtliche Verwaltungsleistungen auch elektronisch über Verwaltungsportale anzubieten. Dieses Ziel wurde nicht erreicht – bis Anfang 2025 waren nur 196 der 575 Verwaltungsleistungen flächendeckend verfügbar (INSM o. J.). Dennoch hat sich laut Deutschland-Index 2025 die durchschnittliche Zahl online verfügbarer Verwaltungsleistungen pro Kommune zwischen 2021 und 2023 mehr als verdoppelt (Abbildung 2.1). Besonders stark fiel der Anstieg bei der Gewerbeanmeldung aus, die 2023 in 84 % der untersuchten Kommunen online abgewickelt werden konnte (Opiela et al. 2023, S. 37 f.). Auch die Nutzung von E-Government-Angeboten durch Bürger/innen und Unternehmen nimmt langsam, aber stetig zu (von 2013 bis 2023 um 11 Prozentpunkte auf 56 %) (Initiative D21/TU München 2023, 2024).³

1 E-Government-Gesetz vom 25. Juli 2013, zuletzt am 2. Dezember 2025 geändert

2 Onlinezugangsgesetz vom 14. August 2017, zuletzt am 19. Juli 2024 geändert

3 Parallel dazu hat die digitale Nutzungslücke – der Anteil der Bürger/innen, die ihren Bedarf an Behördenleistungen aktuell nicht online decken – von 2023 bis 2024 von 35 auf 31 % abgenommen. Sie ist damit aber nach wie vor höher als in Österreich (21 %) und der Schweiz (19 %) (Initiative D21 e. V./TU München 2023, 2024).

Abbildung 2.1 Anteil der Kommunen mit Onlineverfahren für ausgewählte Leistungen



Quelle: nach Opiela et al. (2023)

Die Verwaltungsdigitalisierung konzentriert sich aktuell auf fünf zentrale Hebel: die flächendeckende Einführung der E-Akte, den Ausbau cloudbasierter Infrastruktur, den Einsatz von KI zur Prozessunterstützung, die Automatisierung repetitiver Prozesse durch Robotic Process Automation (RPA) sowie die Umsetzung des Once-Only-Prinzips:

- Bei der *E-Akte* handelt es sich um die digitale Form der herkömmlichen Papierakte. Die E-Akte Bund wurde 2018 als zentraler Dienst für die Bundesverwaltung eingeführt. 2024 war der Rollout offiziell abgeschlossen und der Wirkbetrieb gestartet (ITZBund o. J.). Gemäß dem Gesetz zur Einführung der elektronischen Akte in der Justiz und zur weiteren Förderung des elektronischen Rechtsverkehrs von 2017 müssen Prozessakten ab dem 1. Januar 2026 elektronisch geführt werden. 15 Bundesländer gehen davon aus, dieses Ziel zu erreichen (Deutscher Richterbund 2025).
- Auf- und Ausbau von *Cloudlösungen* für staatliche und behördliche Stellen werden seit einigen Jahren politisch koordiniert vorangetrieben. Zwischen 2021 und 2024 erhöhte der Bund deutlich seine Ausgaben für die Cloudnutzung (Bundesregierung 2025). Mit dem Aufbau der Bundescloud für die Bundesverwaltung wurde bereits 2016 begonnen (ITZBund o. J.a). Parallel dazu wurde die Deutsche Verwaltungscloud⁴ als interoperable sowie föderale Cloudinfrastruktur etabliert und 2025 offiziell in den Wirkbetrieb überführt.
- *Künstliche Intelligenz* ist laut ThemenRadar 2025 in den Behörden angekommen: Zwei Drittel der befragten Verwaltungsmitarbeiter/innen von Bund, Ländern und Kommunen erproben oder verwenden generative KI-Tools in ihrer Arbeit (Kompetenzzentrum Öffentliche IT et al. 2025). In der Verwaltungspraxis kommen unter anderem KI-gestützte Chatbots für Bürgeran-

4 <https://deutsche-verwaltungscloud.de/> (18.6.2026)

fragen sowie automatisierte Bescheidsysteme (zum Beispiel für Standardanträge) ein, während Prognosemodelle (etwa zur Steuerprüfung oder Kriminalitätsprävention) erprobt werden; einen Überblick über die KI-Systeme der deutschen Verwaltung bietet der „Marktplatz der KI-Möglichkeiten“ des Beratungszentrums für Künstliche Intelligenz.⁵

- Bei RPA kommen Softwareroboter oder Bots zum Einsatz. Dabei handelt es sich um Computerprogramme, mit denen sich wiederholende, regelbasierte Tätigkeiten wie Datenübertragungen, Plausibilitätsprüfungen und die Verarbeitung von Anträgen automatisieren lassen. Die Einführung von RPA gewinnt in der deutschen Verwaltung zunehmend an Dynamik. Hamburg ist Vorreiter: Seit 2021 setzt die Stadt auf RPA und hatte Mitte 2024 50 Bots in der Verwaltung im Einsatz (Hensiek 2025). Auch für die Deutsche Rentenversicherung ist RPA ein wichtiger Bestandteil ihrer Digitalisierungsstrategie (Koç et al. 2021).
- Das *Once-Only-Prinzip* soll das Verwaltungshandeln beschleunigen und effizienter machen, indem Bürger/innen sowie Unternehmen die für digitale Verwaltungsleistungen benötigten Angaben und Nachweise nur noch ein einziges Mal an die Behörden übermitteln müssen (Bundesdruckerei o. J.). Der Datenaustausch zwischen den Behörden erfolgt im Rahmen der Registermodernisierung über das Nationale Once-Only-Technical-System (NOOTS) Weitere Voraussetzungen sind eine konsequente Ende-zu-Ende-Digitalisierung (entspricht OZG-Reifegrad 4) und Standardisierung der Verwaltungsleistungen.

Der Stand der Verwaltungsdigitalisierung in Deutschland ist stark durch föderale Strukturen geprägt. Zwischen den Bundesländern bestehen sowohl Unterschiede in der Umsetzungsgeschwindigkeit als auch in der inhaltlichen Ausgestaltung der Digitalisierungsstrategien. Eine im Juli 2024 veröffentlichte Studie, die auf Verwaltungsbefragungen und Experteninterviews basiert, untersuchte den Digitalisierungsstand in verschiedenen Verwaltungsbereichen und zeigte erhebliche Disparitäten in der Digitalisierungstiefe; dabei erweisen sich insbesondere die Steuerverwaltungen als Vorreiter (Gräfe et al. 2024). Auch der Smart-City-Index, ein von der Bitkom herausgegebenes Digitalranking deutscher Großstädte, stellt bei den betrachteten Indikatoren für Verwaltungsdigitalisierung (unter anderem interne Prozesse, Payment, OZG-Leistungen, Serviceportal) eine große Spannbreite zwischen den Kommunen fest (Bitkom e. V. 2025c).

Für kleinere Kommunen ist die Umsetzung von Digitalisierungsvorhaben besonders herausfordernd. Verantwortlich dafür sind die häufig knappe Personalsituation, fehlendes Know-how und die hohen Kosten für die Beschaffung, den Betrieb und die Wartung von Hard- und Software sowie für Informationssicherheit und Datenschutz (zum Beispiel Penetrationstests, Sicherheitsarchitekturen, Verschlüsselung, Zertifizierung). Wenngleich Bund und Länder ihre Investitionen in die Digitalisierung seit der COVID-19-Pandemie deutlich erhöht haben, wobei der größte Teil davon in die Verwaltungsdigitalisierung geflossen ist (ZEW 2025), liegt Deutschland im internationalen Vergleich bei der Verwaltungsdigitalisierung aktuell immer noch auf einem der hinteren Plätze (Bitkom e. V. 2025b). Generell stellt sich die Frage, wie leistungsfähige digitale Dienste auch dezentral und resilient betrieben werden können. Edge Computing ist ein möglicher Ansatz, der die Abhängigkeit von Cloudinfrastrukturen reduzieren könnte (Kasten 2.1).

5 <https://maki.beki.bund.de/a/bmi-makimo-app?kiosk> (18.6.2026)

Kasten 2.1 Emerging Issue: Edge Computing im öffentlichen Raum

Bei Edge Computing handelt es sich um eine dezentrale Form der Datenverarbeitung. Im Gegensatz zum Cloudcomputing, bei dem Daten zentralisiert in Rechenzentren gespeichert und verarbeitet werden, verlagert Edge Computing Rechenleistung und IT-Ressourcen in die Nähe der Datengenerierung. Datenverarbeitung und Speicherung erfolgen dezentral am Netzwerkrand (Edge), in direkter Nähe zu Datenquellen, wie IoT-Geräten, Sensoren und Endanwendungen (Zhai et al. 2024). Für die Verwaltungsdigitalisierung ist Edge Computing von strategischer Bedeutung, da es fundamentale Schwächen reiner Cloudansätze (Latenz, Bandbreite, Datenschutz) kompensiert und dadurch resiliente Smart-City- und E-Government-Anwendungen ermöglicht. Ein zentraler Vorteil ist unter anderem die Echtzeitfähigkeit: Da Daten direkt am Ort der Erhebung verarbeitet werden (zum Beispiel in der Ampelanlage oder im Wasserwerk), eignet sich die Technologie besonders für zeitkritische Prozesse, große Datenmengen und KI-Anwendungen. Dies eröffnet Potenziale für kritische Infrastrukturen – etwa in der Verkehrssteuerung oder im Hochwasserschutz. Edge Computing ermöglicht es zum Beispiel Kommunen, Verkehrsströme in Echtzeit zu optimieren, die öffentliche Sicherheit zu stärken und Umweltdaten präziser für die Stadtplanung zu nutzen. Besonders relevant für die Verwaltung ist zudem die Möglichkeit, sensible Daten (zum Beispiel an Bürgerterminals) bereits an der Quelle zu pseudonymisieren, bevor sie an Clouddienste weitergeleitet werden. Durch die verteilte Infrastruktur bleibt die Funktionsfähigkeit auch bei Ausfall einzelner Komponenten erhalten, während die Anfälligkeit für großflächige Cyberattacken sinkt (Jahnke/Niehoff 2024). Insgesamt kann Edge Computing die Resilienz von Staat und Verwaltung erhöhen, indem es Dezentralität, Reaktionsgeschwindigkeit, Datensouveränität und Systemmodularität stärkt. Voraussetzung ist jedoch, dass technologische Dezentralisierung mit institutioneller Koordination und einer robusten Sicherheitsarchitektur integriert umgesetzt wird.

Gleichzeitig ist die flächendeckende Umsetzung von Edge Computing mit erheblichen technischen und organisatorischen Hürden verbunden. Im Gegensatz zu hochstandardisierten Cloudrechenzentren basiert die Edgeinfrastruktur auf einer heterogenen Gerätelandschaft unterschiedlichster Hersteller und Leistungsklassen. Diese Fragmentierung erschwert nicht nur die Interoperabilität zwischen den Komponenten, sondern macht auch das zentrale Management und die Wartung des verteilten Netzwerks exponentiell komplexer als bei klassischen IT-Strukturen (Yang et al. 2022). Darüber hinaus schafft die Dezentralisierung neue Sicherheitsrisiken: Jedes Edgegerät – oft an öffentlich zugänglichen Orten wie Ampeln oder Bürgerterminals installiert – stellt einen potenziellen physischen und digitalen Angriffsvektor dar. Die Sicherstellung konsistenter Sicherheitsupdates über tausende verteilte Endpunkte hinweg ist eine massive operative Herausforderung, die ohne strikte Standards kaum zu bewältigen ist (Jahnke/Niehoff 2024). Letztlich soll Edge Computing kein Ersatz für Cloudinfrastrukturen sein, sondern eine sinnvolle Ergänzung dazu. Der Aufbau eines interoperablen europäischen Cloud-to-Edge-Kontinuums wird derzeit massiv durch das Großprojekt IPCEI-CIS (Important Project of Common European Interest – Next Generation Cloud Infrastructure and Services) vorangetrieben, an dem 12 EU-Mitgliedstaaten und über 150 Partner beteiligt sind (BMWE o.J.). Deutschland fördert das Vorhaben mit rund 750 Mio. Euro und koordiniert 29 Einzelprojekte, darunter das Projekt „Cloudbasierte Kommunikation im Krisenfall“. Hier testen die

Deutsche Rentenversicherung Bund und weitere Sozialversicherer, wie der Betrieb kritischer Infrastrukturen auch in Krisenszenarien resilient gesichert werden kann. Dabei wird erprobt, wie die Open-Source-Softwareplattform openDesk als Basis für eine souveräne Cloud- und Edgeinfrastruktur fungieren und die Handlungsfähigkeit in Extremsituationen stärken kann (ZenDiS 2026).

Mit der Modernisierungsagenda für Staat und Verwaltung (Bund) verpflichtete sich der Bund, bis Ende 2029 alle wesentlichen Verwaltungsleistungen gemäß § 6 EGovG vollständig digital durchzuführen (Bundesregierung 2025d). Parallel dazu bezieht die ebenfalls 2025 beschlossene Föderale Modernisierungsagenda auch die Länder mit ein. Zu den vereinbarten Maßnahmen gehören unter anderem der Aufbau einer souveränen nationalen Technologieplattform zur Digitalisierung der deutschen Verwaltung, die Registermodernisierung – also die Digitalisierung behördlicher Datensammlungen – sowie die Erleichterung des KI-Einsatzes. Zudem besteht das Ziel, sich aus der zunehmenden Abhängigkeit von amerikanischen Anbietern zu lösen, die sich unter anderem in rasant steigenden Bundesaussgaben für Microsoft-Lizenzen zeigt (Kipker/Kalain 2026) (Kapitel 3.1 – Machtkonzentrationen). Die digitale Souveränität der Verwaltungen soll gestärkt werden, indem vorrangig Open-Source-Ansätze und Angebote digital-souveräner Anbieter zur Anwendung kommen (Bundesregierung 2025b). Um die Verwaltung dabei zu unterstützen, wurde 2022 vom BMI das Zentrum für Digitale Souveränität der Öffentlichen Verwaltung (ZenDiS) gegründet. Nach Monitoringberichten von Bitkom gewinnt Open-Source-Software in Behörden bundesweit an Akzeptanz, auch wenn die zugrunde liegenden Erhebungen nicht repräsentativ sind (Wintergerst 2023).

2.2 Struktureller Wandel des öffentlichen Sektors unter demografischem, personellem und fiskalischem Druck

Der öffentliche Sektor steht vor einer dreifachen strukturellen Herausforderung: einer alternden Belegschaft, einem sich zuspitzenden Fachkräftemangel und strukturell unterfinanzierten Haushalten – besonders auf kommunaler Ebene. Während die Zahl der Beschäftigten steigt, sinkt die personelle Kapazität pro Aufgabe, da Stellen unbesetzt bleiben und die Belastung wächst. Gleichzeitig binden fixe Ausgaben – vor allem für soziale Sicherung und Zinsen – immer größere Anteile der Haushalte, während die Investitionslücken in Bildung, Infrastruktur und Pflege größer werden. Der mit den beschriebenen Trends verbundene Strukturwandel im öffentlichen Sektor betrifft grundlegend die Handlungsfähigkeiten des Staates. Der langfristig wirkende demografische Wandel wirkt auf mehreren Ebenen verschärfend und droht die Funktionsfähigkeit staatlicher Daseinsvorsorge und öffentlicher Dienstleistungen nachhaltig zu gefährden. Diese

Entwicklungen wirken quer über Institutionen sowie Bereiche des Systembilds und verändern Kapazitäten, Prozesse und Prioritätensetzung.

Die Beschäftigtenzahlen im öffentlichen Dienst steigen seit 2009 kontinuierlich an. 2024 waren 5,4 Mio. Menschen in der öffentlichen Verwaltung beschäftigt (Destatis 2025b). Das sind fast 100.000 mehr Beschäftigte als ein Jahr zuvor und über 1 Mio. mehr als 2012 (Abbildung 2.2). Aktuell arbeiten somit rund 11 % aller Erwerbstätigen in Deutschland im Staatsdienst (dbb 2025a). Der Zuwachs über die letzten Jahre entfällt größtenteils auf die Länder und Kommunen und ist vor allem auf steigende Bedarfe im Bildungswesen, in Kindertageseinrichtungen und im Bereich der öffentlichen Sicherheit zurückzuführen (Destatis 2025b; Hentze/Kauder 2024).

Abbildung 2.2 Öffentlicher Dienst: Beschäftigte nach Aufgabenbereich 2022



Quelle: nach Statistisches Bundesamt und eigenen Berechnungen des Demografieportals (o. J.b)

Trotz dieser steigenden Beschäftigungszahlen trifft der demografische Wandel den öffentlichen Dienst mit voller Wucht. Die Belegschaften altern rapide, mehr als ein Viertel der Beschäftigten ist bereits über 55 Jahre alt (dbb 2025a). Nach Einschätzung des dbb beamtenbund und tarifunion fehlen dem Staat angesichts wachsender Aufgaben schon heute über 600.000 Mitarbeitende, um seine Aufgaben effizient zu erledigen. Der größte Personalbedarf besteht aktuell an Schulen, in Kommunalverwaltungen sowie in der Kranken- und Altenpflege. In den kommenden 10 Jahren werden weitere 1,3 Mio. Beschäftigte aus dem öffentlichen Dienst ausscheiden (dbb 2025b). Seit mehreren Jahren wird daher auf einen wachsenden Mangel an qualifizierten Fachkräften in nahezu allen Bereichen des öffentlichen Sektors hingewiesen (Kapitel 3.1 – Versor-

gungssengpässe). Laut Prognosen des PwC (2022) könnte sich die Fachkräftelücke bis 2030 auf 1 Mio. erhöhen, wodurch die Konkurrenz mit dem Privatsektor um qualifizierte Arbeitskräfte (besonders im IT-Bereich) zunehmen dürfte (Prümer/Schnabel 2023).

Da die Altersstruktur und die Bedarfe zwischen Bund, Ländern und Kommunen sowie zwischen den Aufgabenbereichen stark variieren – so sind beispielsweise im Verkehrs- und Nachrichtenwesen 40 % der Erwerbstätigen über 55 Jahre alt, bei der Polizei 20 % und bei der Verteidigung 13 % (Demografieportal o. J.a) (Abbildung 2.3) – sind die Auswirkungen des demografischen Wandels nicht überall gleich gravierend.

Abbildung 2.3 Öffentlicher Dienst: über 55-jährige Beschäftigte in einigen Aufgabenbereichen 2022



Quelle: nach Daten des Statistischen Bundesamtes und eigenen Berechnungen des Demografieportals (o. J.a)

Als potenzieller Hebel zur Abmilderung des Personalengpasses rücken KI-Agenten in den Blick, die regelbasierte, aber zeitintensive Verwaltungsvorgänge – von der Vorprüfung baurechtlicher Anträge bis zur Konsistenzprüfung in Planfeststellungsverfahren – substanziell beschleunigen könnten (Kasten 2.2).

Kasten 2.2 Emerging Issue: KI-Agenten für Planungs- und Genehmigungsverfahren

KI-Agenten stellen eine Weiterentwicklung klassischer Automatisierungstechnologien wie Robotic Process Automation (RPA) dar und bieten angesichts der Ressourcenknappheit in der Verwaltung großes Potenzial. Gegenüber RPA, das starr regelbasiert agiert, definieren Peters und Martin (2026) KI-Agenten als „autonom agierende, kognitiv gesteuerte Softwaresysteme, die in der Lage sind, mehrstufige Ziele zu verfolgen, mit ihrer Umwelt zu interagieren und dabei funktionale Rollen innerhalb von Organisationen zu übernehmen“. KI-Agenten sind somit keine bloßen Werkzeuge zur Abarbeitung vordefinierter Skripte, sondern Artificial Bureaucrats, die auch wenig standardisierte Aufgaben eigenständig steuern und Entscheidungsspielräume nutzen. Mögliche Einsatzgebiete sind die autonome Vorprüfung von Baugenehmigungen, adaptives Bürgerservicemanagement oder komplexe Beschaffungsanalysen (McKinsey 2025). Durch die Vernetzung zu Multiagentensystemen lassen sich prinzipiell ganze Prozessketten ohne menschliche Mikrosteuerung automatisieren. Für eine agentische KI, die Planungs- und Genehmigungsverfahren für das Wasserstoffkernnetz beschleunigen soll, hat Deutschland kürzlich einen internationalen KI-Preis gewonnen (BMW 2026).

KI-Agenten können die Resilienz von Staat und Verwaltung in Planungs- und Genehmigungsverfahren damit vor allem durch Beschleunigung, Entlastung und höhere Verfahrensqualität stärken. Da sie komplexe Aufgaben, wie Aktenanalysen oder die inhaltliche Vorprüfung von Bürgeranliegen, autonom und rund um die Uhr übernehmen können, bieten sie ein erhebliches Potenzial zur Abmilderung des Fachkräftemangels. Laut McKinsey (2025) könnte ein flächendeckender Einsatz dieser Systeme die prognostizierte Personallücke um bis zu 50 % verringern. Dennoch hinkt die öffentliche Verwaltung bei der KI-Adoption dem Privatsektor deutlich hinterher. Eine Untersuchung der OECD (2025a) zeigt, dass KI in Behörden bislang überwiegend klassisch regelbasiert eingesetzt wird, während generative KI kaum Verbreitung findet. Ein wesentlicher Grund für diese Zurückhaltung liegt in den ungeklärten rechtlichen Risiken, insbesondere im Hinblick auf Datenschutz und Haftung, die sich bei autonomen Agenten noch verschärfen. Mit ihrer Einführung wandelt sich Software vom passiven Werkzeug zum eigenständigen Akteur. Dies wird problematisch, wenn Entscheidungswege undurchsichtig bleiben (Blackbox) oder fehlerhaft sind. Ein zentrales Risiko ist der Automation Bias: Die Gefahr besteht, dass menschliche Kontrolleure den Vorschlägen der KI blind vertrauen, was zu einer faktischen Autoritätsverschiebung vom Menschen auf die Maschine führt. Eine explizite KI-Governance, die nicht nur technische Compliance sichert, sondern auch die Mensch-Maschine-Interaktion transparent regelt, ist für den Einsatz von KI-Agenten daher unverzichtbar (Peters/Martin 2026). Zur besseren Nachvollziehbarkeit von KI-Entscheidungen in juristischen Kontexten können Methoden wie das Rule Mapping eingesetzt werden. Beim Rule Mapping werden Gesetze, Vorschriften und Verfahren von Anfang an in strukturierte, visuelle Entscheidungsmodelle und damit maschinenlesbare Formate überführt (Hartmann 2025).

Eine zentrale strukturelle Herausforderung für die staatliche Handlungsfähigkeit ist die wachsende Belastung der öffentlichen Haushalte durch feste Ausgaben. Ein großer Teil des Bundeshaushalts

ist bei der Haushaltsaufstellung bereits gebunden durch Verträge, gesetzliche soziale Leistungen und Personalausgaben (Bundesrechnungshof 2022). Die gebundenen Ausgaben betreffen insbesondere Sozialleistungen (inklusive Soziale Sicherung, Familie, Jugend und Arbeitsmarktpolitik) und stellen den größten Haushaltsposten dar. Ihr Anteil steigt seit Jahren, bedingt durch den demografischen Wandel: Zwischen 2011 und 2020 nahmen die Bundesausgaben für die soziale Sicherung um 45 % zu und machten 2024 45,8 % der Gesamtausgaben aus – ein struktureller, langjähriger Aufwärtstrend (BMF 2023; bpb 2023b).⁶ Weitere große Ausgabenbereiche bilden Verteidigung sowie Zinsausgaben, die sich 2024 auf 7,3 % der Bundesausgaben beliefen (BMF 2025). Durch den fortschreitenden demografischen Wandel, die zusätzlichen Tilgungsverpflichtungen aus den Corona-Notlagenkrediten sowie den Sondervermögen für die Bundeswehr (100 Mrd. Euro) und für Infrastruktur und Klimaneutralität (500 Mrd. Euro) werden die festen Belastungen in Zukunft weiter ansteigen und sich so die Gestaltungsmöglichkeiten der Exekutive verringern.

Dauerhaft steigende Sozialausgaben und Personalkosten (zum Beispiel durch Tarifabschlüsse) und allgemein wachsende Ausgaben bei stagnierenden oder rückläufigen Steuereinnahmen belasten die Kommunen ganz besonders. Deren Haushalte wiesen 2024 ein Rekorddefizit auf (KfW/difu 2025). Laut vorläufigen Daten stiegen die Schulden von Gemeinden und Gemeindeverbänden in Deutschland 2024 um 6,3 % auf ein Gesamtschuldenvolumen von 343,8 Mrd. Euro (Destatis 2025a). Diese Entwicklung macht sich in einem zunehmenden Investitionsstau bemerkbar. Der nach Einschätzung der kommunalen Finanzverwaltungen erforderliche Investitionsbedarf zur Herstellung eines adäquaten Zustands der Infrastruktur beläuft sich auf 215,7 Mrd. Euro – ein Anstieg um knapp 16 % gegenüber dem Vorjahr (KfW 2025). Diese Entwicklung bedroht die Funktionsfähigkeit zahlreicher kommunaler Aufgaben. Besonders betroffen sind die Bereiche Bildung (Schulgebäude: 67,8 Mrd. Euro Rückstand), Verkehrsinfrastruktur (53,4 Mrd. Euro), Brand- und Katastrophenschutz (19,93 Mrd. Euro) sowie Verwaltungsgebäude (19,5 Mrd. Euro) (KfW/difu 2025). 19 % der Kommunen geben an, den Unterhalt der Infrastruktur nur noch eingeschränkt oder gar nicht mehr leisten zu können. Dies wirkt sich direkt auf die Lebensqualität, die Resilienz und die Zukunftsfähigkeit der Gemeinden aus.

6 Bezogen auf die gesamten öffentlichen Haushalte Deutschlands beträgt der Anteil der sozialen Sicherung sogar 57 % (bpb 2023a).

2.3 Wachsende ökologische Herausforderungen an staatliche Steuerung und Finanzierung

Hohe und zunehmend erfasste ökonomische Belastungen durch globale Erwärmung, Extremwetterereignisse und Auswirkungen des Biodiversitätsverlustes erfordern systematische Lösungen zur Schadensbewältigung und Prävention. Parallel dazu gewinnt die Integration von Klimazielen in staatliche Haushaltsprozesse an Bedeutung, um öffentliche Ausgaben klimawirksam auszurichten und Transparenz über deren ökologische Folgen zu schaffen. Institutionell manifestiert sich dieser Wandel in der Verabschiedung verbindlicher Anpassungsstrategien und Gesetze, die Bund, Länder und Kommunen zur aktiven Auseinandersetzung mit Klima- und Biodiversitätsschutz verpflichten. Zudem wird die öffentliche Beschaffung zunehmend als Hebel für die Förderung von Nachhaltigkeit genutzt, indem Kreislaufwirtschafts- und Umweltkriterien in Vergabeverfahren verankert werden. Die im Trendcluster beschriebenen Entwicklungen betreffen in erster Linie die parlamentarische Steuerung (Haushaltsverhandlungen) sowie Regierungen und Verwaltungen.

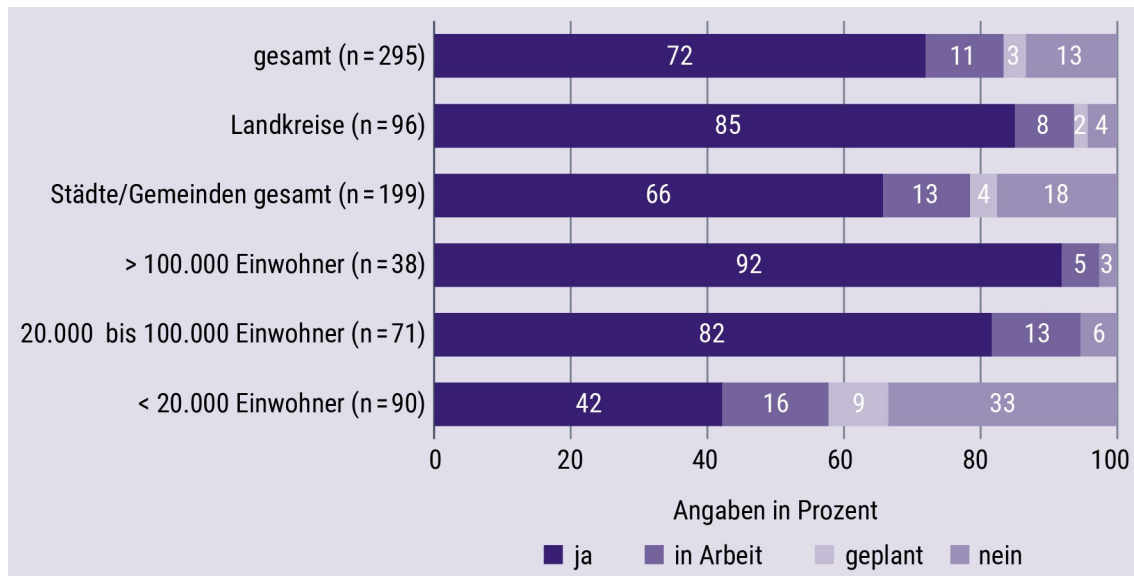
Schäden durch Extremwetterereignisse, wie Hitzeperioden, Überschwemmungen oder Starkregen, nehmen zu und stellen die öffentliche Hand vor wachsende finanzielle Herausforderungen. Prognos et al. (2022) schätzt die extremwetterbedingten Schäden für den Zeitraum von 2000 bis 2021 auf knapp 145 Mrd. Euro. Die Europäische Umweltagentur (EEA 2025) ermittelte für den Zeitraum 1980 bis 2024 kumulierte Schäden von knapp 187 Mrd. Euro in Deutschland, wovon schätzungsweise nur ein Drittel versichert war. Allein die Flutkatastrophe im Ahrtal 2021 verursachte Schäden von rund 40 Mrd. Euro; das aus öffentlichen Mitteln finanzierte Sondervermögen ‚Aufbauhilfe‘ umfasste 30 Mrd. Euro (Bär/Wilkens 2023). Zu den direkten Schäden kommen Kosten für präventive Maßnahmen hinzu – etwa für Hitzeschutz in Städten (zum Beispiel Begrünung, hitzeangepasste Infrastruktur) oder technisch-naturbasierten Hochwasserschutz (zum Beispiel Deichverstärkungen, Rückhaltebecken, Auenrenaturierung) – sowie indirekte Gesundheitskosten durch klimabedingte Belastungen. Diese Risiken werden durch den fortschreitenden Biodiversitätsverlust verschärft, da intakte Ökosysteme, wie Auen, Moore, Wälder oder urbane Grünflächen, als natürliche Puffer gegen Extremwetter wirken.

Klimaanpassung sowie Klima- und Biodiversitätsschutz werden zunehmend institutionell verankert, mit der Exekutive und Verwaltung auf Bundes-, Landes- und kommunaler Ebene als primären Adressaten. Die erste Deutsche Anpassungsstrategie an den Klimawandel (DAS, 2008) enthielt noch keine verbindlichen Ziele. 2023 wurde das Bundes-Klimaanpassungsgesetz (KAnG)⁷ verabschiedet, das Klimaanpassung als staatliche Aufgabe festschreibt und Kommunen zur Erstellung von Anpassungskonzepten verpflichtet. Die daraus resultierende Klimaanpassungsstrategie mit messbaren Zielen wurde von der Bundesregierung 2024 vorgelegt (UBA 2024). Auf kommunaler

⁷ Bundes-Klimaanpassungsgesetz vom 20. Dezember 2023

Ebene beschleunigt sich die Umsetzung: 2024 verfügten 72% der Kommunen über ein Klimaschutzkonzept und 87% über ein kommunales Klimaschutzmanagement (Koordination und Organisation von Klimaschutzaktivitäten), weitere 11 bzw. 9% arbeiteten daran – ein kontinuierlicher Zuwachs seit Erhebungsbeginn 2008 (Abbildung 2.4).

Abbildung 2.4 Klimaschutzkonzepte in Kommunen



Quelle: nach Overath/Rösler (2025)

Parallel dazu gibt es im Biodiversitätsschutz – wenn auch mit geringerer finanzieller und institutioneller Ausstattung – eine vergleichbare Entwicklung hin zu zielorientierteren und verbindlicheren Umsetzungsmechanismen: Die Nationale Strategie zur biologischen Vielfalt (2007) war noch programmatisch angelegt; die Fortschreibung aus 2020 (NBS 2030) enthält hingegen konkretere Ziele, Maßnahmen und Aktionspläne (NBS-Geschäftsstelle o. J.a). Eine wichtige, jedoch kaum erfüllte Voraussetzung für die Operationalisierung dieser Ziele ist die Verknüpfung ökologischer Daten, die bislang über verschiedene institutionelle Silos (Ökosystemdatenräume) fragmentiert sind (Kasten 2.3).

Kasten 2.3 Emerging Issue: bundesweite Ökosystemdatenräume

Der Schutz der Biodiversität steht seit den 1990er Jahren auf der politischen Agenda, die Umsetzung der vereinbarten Zielsetzungen zum Biodiversitätsschutz durch die damit betrauten Behörden und Verwaltungen hat sich jedoch als sehr herausfordernd erwiesen. Verantwortlich dafür ist auch die extreme Komplexität des Schutzgutes. Im Unterschied zum Klimaschutz, der oft

auf CO₂-Äquivalente als zentrale Steuerungsgröße reduziert werden kann, entzieht sich die Biodiversität einer eindimensionalen Messbarkeit. Im Handlungsfeld 6 der Nationalen Biodiversitätsstrategie findet sich zwar der Hinweis, dass sowohl für die Forschung als auch für das Verwaltungshandeln „grundsätzlich mehr aussagekräftige Daten über den Zustand und die Veränderungen der Biodiversität in Deutschland benötigt“ werden (NBS-Geschäftsstelle o. J.b). Die aktuelle Forschung zeigt jedoch: Das Kernproblem ist nicht nur der Mangel an Daten, sondern auch ihre massive Fragmentierung und mangelnde Interoperabilität (Islam et al. 2026). Vorliegende Daten sind über statistische (Statistisches Bundesamt), naturschutzfachliche (BfN) und wissenschaftliche (IOER) Silos verteilt und inhaltlich bzw. begrifflich oft nicht kompatibel.

Ökosystemdatenräume (Ecosystem Data Space) können dabei helfen, die vorliegenden Informationen für evidenzbasiertes Verwaltungshandeln zugänglich zu machen. Ein Ökosystemdatenraum ist kein physischer Speicherort, sondern eine dezentrale Infrastruktur, die heterogene Umweltdaten (zum Beispiel Satellitendaten, lokale Monitorings, Genbanken) durch gemeinsame Standards verbindet sowie Modelle und Rechenkapazitäten technisch und rechtlich verknüpft. Er ermöglicht den sicheren Austausch und die Verarbeitung von Daten über Organisationsgrenzen hinweg, ohne dass die Daten zentralisiert werden müssen. Für die Standardisierung eines Datenraums wird häufig auf die FAIR-Prinzipien (findable, accessible, interoperabel, reusable) zurückgegriffen (Islam et al. 2024):

- Auffindbar (findable): Globale IDs und Metadaten machen dezentrale Daten im gesamten Raum sichtbar.
- Zugänglich (accessible): Standardisierte Protokolle regeln den Zugriff (Authentifizierung).
- Interoperable (interoperabel): Semantische Standards ermöglichen die automatische Verknüpfung heterogener Quellen.
- Wiederverwendbar (reusable): Klare Lizenzen erlauben rechtssichere Nutzung für neue Fragestellungen (zum Beispiel KI-Training).

Auf Basis von Ökosystemdatenräumen lassen sich digitale Zwillinge von Ökosystemen erstellen. Dabei handelt es sich um ein dynamisches Echtzeit-Modell eines ökologischen Systems (zum Beispiel eines Waldes oder Ozeans), das dezentrale Datenquellen über den Ökosystemdatenraum nutzt und Simulationen (Was-wäre-wenn-Szenarien) ermöglicht (Islam et al. 2024). Das Projekt „Biodiversity Digital Twin“ (BioDT), das im Rahmen des Europäischen Rahmenprogramms für Forschung und Innovation Horizont Europa umgesetzt wurde, entwickelte zehn Prototypen digitaler Zwillinge, die verschiedene Herausforderungen der Biodiversität adressieren und Strategien zur Integration heterogener Daten, Modelle und Arbeitsabläufe innerhalb eines FAIR-Rahmens demonstrieren (Islam et al. 2026).

Ein operativer, vernetzter Ökosystemdatenraum eröffnet zahlreiche Potenziale für ein evidenzbasiertes Verwaltungshandeln. Er könnte dabei helfen, die Zuständigkeitsfragmentierung aufzubrechen, die Verwaltungen oft hemmt. Außerdem würde er Verwaltungen die Möglichkeit bieten, auch nicht amtliche Daten (zum Beispiel aus der Forschung, von Nichtregierungsorganisationen

oder Citizen Science) rechtssicher zu nutzen, weil Nutzungsrechte und -bedingungen im Datenraum einheitlich festgelegt sind und die Datenherkunft transparent dokumentiert wird (Lush et al. 2024). Und nicht zuletzt lassen sich durch automatisierte Analysen der gesammelten Daten Effizienzgewinne realisieren (Weiland et al. 2025). Damit können bundesweite Ökosystemdatenräume die Adaptivität (schnellere Reaktionsfähigkeit) und Transformationsfähigkeit (strategische Umweltsteuerung), aber auch die Robustheit (bessere Krisenvorsorge) von Staat und Verwaltung erhöhen. Voraussetzung sind hohe Datenqualität, Interoperabilität und verlässliche institutionelle Zuständigkeiten.

Den Parlamenten obliegt die Aushandlung des Mitteleinsatzes, die für Umwelt- und Klimaschutz zur Verfügung gestellt werden. Die entsprechenden öffentlichen Ausgaben (Investitionen und laufende Ausgaben) stiegen in Deutschland zwischen 2010 und 2022 von 8,5 auf 15,7 Mrd. Euro (UBA o. J.b). Seit 2011 bündelt der Bund einen Teil seiner Klimaschutzfinanzierung im Energie- und Klimafonds (seit 2022: Klima- und Transformationsfonds – KTF). Eine geplante Aufstockung des Fonds um 60 Mrd. Euro durch Umschichtung aus dem Corona-Sondervermögen wurde vom Bundesverfassungsgericht (BVerfG) im November 2023 für verfassungswidrig erklärt. 2024 betrugen die geplanten Programmausgaben des KTF 57,6 Mrd. Euro und sanken 2025 planmäßig auf 25,5 Mrd. Euro, wobei die tatsächlichen Ausgaben deutlich unter den Planwerten lagen (2022: 13,7 Mrd. Euro; 2023: 20,1 Mrd. Euro) (Deutscher Bundestag 2024; DIHK 2024). Während sich die deutsche Klimafinanzierung damit vor allem über zweckgebundene Fonds und Einzelprogramme entwickelt, integrieren international immer mehr Staaten Klimaziele systematisch in den Haushaltsprozess (Green Budgeting): Die Zahl der OECD-Länder mit Green-Budgeting-Systemen stieg von 14 (2020) auf 24 (2022) (OECD 2024b). Länder wie Frankreich oder Dänemark setzen bereits verbindliche Ansätze um, während Deutschland bislang über kein operationalisiertes, haushaltsweit verankertes Green-Budgeting-System verfügt. Zwar hat die Bundesregierung 2022 ein Konzept für ein Green-/SDG-Budgeting vorgelegt (Bär et al., 2022; Bär/Collmer, 2024), doch eine Umsetzung steht noch aus. Kommunen, die für die Umsetzung von Klimaschutz- und Anpassungsmaßnahmen von zentraler Bedeutung sind, sind weiterhin auf Förderprogramme von EU, Bund und Ländern angewiesen (KfW, 2023). Die Finanzierung ist damit weiterhin projektbasiert und kurzfristig (Kühl/Scheller 2025).

Neben dem Haushaltsprozess gewinnt auch die öffentliche Beschaffung als Instrument zur verbindlichen Verankerung von Nachhaltigkeitszielen zunehmend an Bedeutung. Sowohl international als auch in Deutschland werden Nachhaltigkeitsprinzipien in der öffentlichen Beschaffung zunehmend verbindlich verankert. Die OECD (2025b) stellt fest, dass immer mehr Mitgliedstaaten Strategien oder Politiken haben, die die explizite Integration von Umweltzielen in das Vergabewesen verlangen. In Deutschland verpflichten das KAnG, das Kreislaufwirtschaftsgesetz (KrWG)⁸ sowie die Allgemeine Verwaltungsvorschrift zur Beschaffung klimafreundlicher Leistungen (AVV Klima) öffentliche Auftraggeber des Bundes dazu, Klima- und Ressourcenschutzaspekte in Vergabeverfahren zu berücksichtigen. In der Nationalen Kreislaufwirtschaftsstrategie (2024)

8 Kreislaufwirtschaftsgesetz vom 24. Februar 2012, zuletzt am 2. März 2023 geändert

wird die öffentliche Beschaffung als zentrales Handlungsfeld eingestuft: Bund, Länder und Kommunen sollen ihre Marktmacht als Nachfrager nutzen, um ein Angebot an kreislauffähigen Produkten zu schaffen (Beschaffungsamt des BMI 2025). Trotz dieser politischen Weichenstellungen zeigen die verfügbaren Daten, die im Indikator 12.3 a–c der Nachhaltigkeitsstrategie zusammengefasst sind (basierend auf der Vergabestatistik des Statistischen Bundesamtes), dass die Vergaben mit Nachhaltigkeitskriterien in Deutschland zwar steigen (2021: 12,6 %; 2023: 14 %), aber noch weit von einem Regelfall entfernt sind (Destatis o. J.). Die Bertelsmann Stiftung (2024b) weist in einer Studie, die auf der Analyse von Ausschreibungsdaten beruht, sogar auf einen rückläufigen Einsatz von Nachhaltigkeitskriterien in der deutschen öffentlichen Beschaffung (insbesondere im kommunalen Bereich) hin. Die Umsetzung einer Haushaltsführung und Beschaffung, die mit den Klimazielen vereinbar ist, scheitert bislang häufig an der mangelnden Verfügbarkeit präziser Emissionsdaten. KI-gestützte Carbon-Assessment-Tools (Kasten 2.4) könnten diese Lücke schließen, indem sie CO₂-Bilanzen über Beschaffungs- und Haushaltszyklen hinweg automatisiert erfassen und bewerten.

Kasten 2.4 Emerging Issue: KI-gestützte Carbon-Assessment-Tools

KI-gestützte Carbon-Assessment-Tools gewinnen in der Nachhaltigkeitsbewertung zunehmend an Bedeutung, da sie die Erfassung und Analyse von CO₂-Emissionen entlang des gesamten Beschaffungs- und Haushaltszyklus weitgehend automatisieren. Moderne Systeme nutzen insbesondere Natural Language Processing (NLP), um unstrukturierte Dokumente – in Studien etwa Frachtbriefe und Finanzberichte (Oladeji/Mousavi 2023), perspektivisch aber auch Verwaltungsdaten, wie Rechnungen, Verträge oder Leistungsbeschreibungen – auszuwerten und daraus emissionsrelevante Informationen abzuleiten. Studien zeigen, dass diese KI-gestützten Verfahren nicht nur die Datenverfügbarkeit verbessern, sondern auch die Genauigkeit und Konsistenz von Carbon Assessments erhöhen können, da sie menschliche Fehler reduzieren und große Datenmengen systematisch auswerten (Andhov et al. 2025).

Während solche Tools im privatwirtschaftlichen Bereich – etwa in Supply-Chain-Management, ESG-Reporting oder nachhaltigkeitsorientierter Unternehmenssteuerung – bereits etabliert sind, besteht im öffentlichen Sektor eine deutliche Lücke (Andhov et al. 2025). Bestehende Vergabeleitlinien bleiben häufig unvollständig; insbesondere fehlen klare methodische Vorgaben und spezifische Kriterien (Bernardini et al. 2025). Ein KI-basiertes Carbon-Assessment-System, das in der deutschen Verwaltung im Einsatz wäre, ist bislang nicht bekannt. Allerdings gibt es in der Bauvergabe erste Erfahrungen und Pilotprojekte mit automatisierter Ökobilanzierung auf Basis von Building Information Modeling (BIM) (Hermann et al. 2024). Parallel dazu untersucht das AI Lab des Umweltbundesamtes (UBA o. J.a) systematisch die Potenziale von KI und Big Data für Umwelt- und Nachhaltigkeitsanwendungen.

Die Potenziale solcher Systeme liegen insbesondere in ihrer großen Hebelwirkung: Durch die automatisierte Bewertung von CO₂-Emissionen entlang der Beschaffungsprozesse könnten

Verwaltungen Klimawirkungen öffentlicher Ausgaben systematisch sichtbar machen. Dies eröffnet Möglichkeiten für eine evidenzbasierte Steuerung, für eine klimafreundlichere Vergabepraxis sowie für eine effizientere Allokation öffentlicher Mittel. KI-gestützte Carbon Assessment Tools können so die Resilienz öffentlicher Verwaltungen stärken, klimapolitische Steuerungsaufgaben auch unter wachsendem institutionellem Druck zu erfüllen. Gleichzeitig bestehen erhebliche Herausforderungen. Eine zentrale Hürde betrifft die technische Interoperabilität der KI-Tools mit den heterogenen, vielfach föderal zersplitterten Verwaltungs-IT-Systemen. Zudem ist die rechtliche Verankerung algorithmischer Bewertungen bislang unzureichend geklärt: Aspekte der Transparenz, der Nachvollziehbarkeit und der datenschutzrechtlichen Zulässigkeit der automatisierten Emissionsberechnung bedürfen einer systematischen Regulierung. Darüber hinaus fehlt es an standardisierten Emissionsfaktoren, die speziell auf öffentliche Güter, Bauleistungen, Infrastrukturinvestitionen oder Dienstleistungen zugeschnitten sind. Aktuelle Initiativen im Bereich Green Procurement betonen, dass ohne solche Standards algorithmische Bewertungen inkonsistent bleiben und Vergabeentscheidungen nicht rechtsfest unterstützt werden können (McKinney/Tarnay 2024).

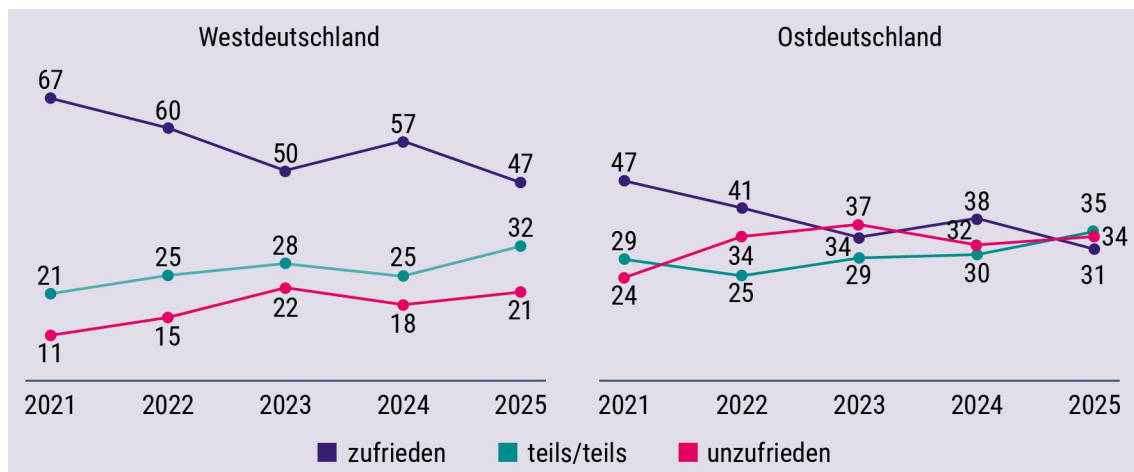
2.4 Wandel im Verhältnis von Staat und Zivilgesellschaft

Das Verhältnis zwischen Zivilgesellschaft und Staat in Deutschland ist in den letzten Jahren deutlich konfliktanfälliger geworden. Das Vertrauen in staatliche Institutionen und politische Prozesse schwindet, was sich in einer Zunahme demokratiekritischer Haltungen in Teilen der Bevölkerung sowie einer als steigend wahrgenommenen gesellschaftlichen Polarisierung zeigt. Diese Entwicklungen werden durch eine verschärfte sicherheitspolitische Bedrohungslage verstärkt, die hybride Risiken wie Cyberangriffe und Desinformation umfasst. Zugleich gewinnen Formate der Bürgerbeteiligung – von digitalen Plattformen bis zu institutionalisierten Bürgerräten – an Verbreitung und werden durch KI-gestützte Funktionen erweitert. Die beschriebenen Entwicklungen berühren zentrale Funktionen von Staat und Verwaltung. Vertrauen in staatliche Institutionen ist für die Legitimität politischer Entscheidungen und die Umsetzung langfristiger Reformen essenziell; gesellschaftliche Polarisierung und Vertrauensverlust gefährden diese Grundlagen. Besonders relevant sind die Auswirkungen auf parlamentarische Steuerung, innere Sicherheit und Verteidigung sowie Regierungen und Verwaltungen.

Während das Vertrauen in staatliche Institutionen und die Funktionsfähigkeit der Demokratie sinkt, nimmt die Zahl formeller Beteiligungsverfahren signifikant zu. Diese gegensätzliche

Entwicklung spiegelt einen tiefgreifenden Wandel im Verhältnis von Staat und Zivilgesellschaft wider. Die Mitte-Studie der Friedrich-Ebert-Studie sowie die Leipziger Autoritarismus-Studie werden seit 2006 bzw. 2002 alle 2 Jahre durchgeführt. Die Ergebnisse dieser sowie auch anderer Umfragen zeigen konsistent, bei grundsätzlich hoher Zustimmung zur Idee der Demokratie als solcher, einen deutlichen Rückgang der Demokratiezufriedenheit und ein erodierendes Vertrauen in die Funktionsfähigkeit der Demokratie seit 2019 bzw. 2022 (Brettschneider 2025; Decker et al. 2024; Körber-Stiftung 2025) (Abbildung 2.5).

Abbildung 2.5 Zufriedenheit mit der Demokratie in Deutschland



Quelle: nach Brettschneider (2025)

Dass die Demokratie in Deutschland gut funktioniert, wird jeweils von weniger als der Hälfte der Befragten bejaht, wobei das Vertrauen in die Demokratie in Westdeutschland höher ausfällt als in Ostdeutschland. Die Vertrauenserosion wird durch weitere Befragungen gestützt, die teilweise auch Rückschlüsse auf spezifische staatliche Institutionen erlauben (dbb 2025a; Edelman Trust Institute 2025; Gabel/Potthoff 2025; Körber-Stiftung 2025; OECD 2024a). Demzufolge ist das Vertrauen in die Parteien, die Exekutive (Bundes- und Landesregierungen) sowie den Bundestag besonders gering ausgeprägt, während Kommunalverwaltungen, Polizei und Gerichte tendenziell besser abschneiden (dbb 2025a; Körber-Stiftung 2025; OECD 2024a).

Die sicherheitspolitische Bedrohungslage in Deutschland hat sich in den letzten Jahren deutlich verschärft, unter anderem durch ein kontinuierlich wachsendes Extremisierungspotenzial im Inneren. Das BKA verzeichnet einen Höchststand politisch motivierter Straftaten (Verdopplung in 10 Jahren), wobei besonders Amts- und Mandatsträger angegriffen werden (BKA 2025). Die Zahlen weisen auf eine deutliche Zuspitzung politischer Konflikte und ein erhöhtes Radikalisierungspotenzial hin. Auch extremistische Straftaten und die Zahl der als extremistisch eingestuft Personen nehmen zu (BMI 2025). Verschärfend kommen zunehmende geopolitische Spannungen sowie die Ausweitung hybrider Bedrohungsformen hinzu. Dazu zählen staatlich gesteuerte Cyberangriffe auf kritische Infrastrukturen und gezielte Desinformationskampagnen (BMI 2025; Bunde et al. 2025). Gleichzeitig dokumentiert das Bundesamt für Sicherheit in der Informationstechnik (BSI) einen deutlichen Anstieg von Drohnenvorfällen im Umfeld von Energieanlagen, Flughäfen und militärischen Einrichtungen – allein von Januar bis Oktober 2025 wurden rund 850 verdächtige Vorfälle

registriert (BSI 2025; ntv 2025). Diese Entwicklungen führen zusammengefasst zu einem erheblich gestiegenen Bedarf an Überwachungs-, Schutz- und Präventionsmaßnahmen und bringen erweiterte operative Aufgaben für zivile Sicherheitsbehörden sowie die Bundeswehr mit sich.

Vor diesem Hintergrund wachsen die Bemühungen, die Legitimität politischer Entscheidungen durch neue Formate der Bürgerbeteiligung zu stärken. Studien der Friedrich-Ebert-Stiftung sehen in ihnen eine konstruktive Antwort auf Vertrauensverlust und Polarisierung. Die Zahl informeller, aber auch formaler Beteiligungsverfahren – wie Bürgerräten, Bürgerforen und andere deliberative Formate – ist seit spätestens 2020 in vielen Kommunen und verstärkt auch auf Landes- und Bundesebene signifikant gestiegen (Siepker et al. 2021). Die Datenbank des Fachverbands Mehr Demokratie und des Instituts für Demokratie- & Partizipationsforschung der Universität Wuppertal⁹ dokumentiert eine deutliche Zunahme losbasierter Bürgerräte in den 2020er Jahren: Während in den 2010er Jahren durchschnittlich sechs Losversammlungen jährlich stattfanden, waren es von 2020 bis 2023 fast 30 pro Jahr. Die überwiegende Mehrheit der losbasierten Bürgerbeteiligungsverfahren mit rund 80 % findet auf kommunaler Ebene statt (Mehr Demokratie e. V. 2024). Aachen etablierte 2022 als erste deutsche Stadt einen ständigen Bürgerrat mit regelmäßiger Beratung durch immer wieder neu ausgeloste Einwohner/innen zu wechselnden Themen. Auch partizipative Budgetierung hat sich als Format der Bürgerbeteiligung etabliert. Dabei entscheiden Bürger/innen direkt über die Verwendung eines Teils des kommunalen Haushalts. In Deutschland haben mittlerweile laut der Stiftung Mitarbeit über 100 Kommunen diese Beteiligungsform genutzt, wenn auch meist nicht kontinuierlich etabliert (Wegweiser Bürgergesellschaft o. J.). Über diese projektbezogenen Formate hinaus stellt sich die Frage, ob und wie digitale Technologien eine kontinuierlichere Rückkopplung zwischen Bevölkerung und staatlichen Entscheidungssträgern ermöglichen können (Kasten 2.5).

Kasten 2.5 Emerging Issue: Bürgerfeedbacksysteme in Echtzeit

Für eine funktionierende Demokratie ist es entscheidend, dass die Meinungen und Wünsche der Bevölkerung tatsächlich in politische Entscheidungen einfließen. Neue digitale Technologien für Beteiligung und Austausch setzen genau hier an. Sie sollen die Rückkopplung zwischen Bürger/innen sowie staatlichen Entscheidungen verbessern (Hubbard/Goux 2026). Digitale Partizipationssysteme ermöglichen theoretisch den Übergang von einzelnen Befragungen hin zu einem kontinuierlichen Dialog in Echtzeit (Shin et al. 2024). Wie das praktisch funktionieren kann, zeigen internationale Beispiele. Taiwan macht mithilfe KI-gestützter Tools wie Polis¹⁰ Meinungsbilder in Echtzeit sichtbar und stellt sie der Politik für Entscheidungen bereit. Die estnische Hauptstadt Tallinn wiederum zeigt mit der Plattform Rahvaalgatus.ee, wie Bürgeranliegen rechtssicher und nahtlos in parlamentarische Verfahren eingebunden werden können (Schachtner 2025).

⁹ <https://www.datenbank-buergerraete.info/> (18.6.2026)

¹⁰ <https://pol.is/> (18.6.2026)

In Deutschland sind echte Bürgerfeedbacksysteme in Echtzeit bislang die Ausnahme. Auf Bundesebene existiert mit EinfachMachen ein Portal zum Bürokratieabbau, das eine kontinuierliche Eingabe ermöglicht. Es dient jedoch eher als digitaler Beschwerdekanal denn als Steuerungsinstrument (Bundesregierung 2025c). Auf kommunaler Ebene dominieren Open-Source-Plattformen wie DIPAS (Hamburg), Consul Democracy und adhocracy+ (Liquid Democracy e.V.). Diese Tools sind auf projektbezogene, asynchrone Beteiligung ausgelegt (Shin et al. 2024): Sie strukturieren Feedback in festen Phasen, statt einen permanenten Echtzeitdialog zu ermöglichen. Eine systematische, rechtlich verbindliche Einbettung solcher Feedbackströme in formale Entscheidungen fehlt weitgehend.

Digitale Echtzeitsysteme bergen ein doppeltes Potenzial für die demokratische Resilienz. Einerseits kann die unmittelbare Responsivität das Vertrauen in staatliches Handeln stärken, da Entscheidungen transparenter und Rückmeldungen sichtbarer werden (Shin et al. 2024). Kontinuierliche Rückmeldungen zu Verwaltungsleistungen, Infrastruktur- oder Krisenmaßnahmen würden es ermöglichen, Fehlentwicklungen schneller zu erkennen und gezielt nachzusteuern. Andererseits helfen KI-gestützte Analysetools wie Polis dabei, in polarisierten Debatten gemeinsame Nenner herauszuarbeiten, die in klassischen Beteiligungsformaten oft unsichtbar bleiben. Gleichzeitig bestehen Risiken: Wenn Verwaltungen zwar Daten erheben, diese aber nicht verarbeiten oder in Entscheidungen einfließen lassen können, entsteht schnell der Eindruck von Pseudopartizipation – mit entsprechend negativem Effekt auf das Vertrauen (UNDEP 2025). Zudem verschärft ein ungleicher digitaler Zugang die Gefahr einseitiger Beteiligung. Ohne die Ergänzung durch analoge Formate besteht das Risiko, dass vor allem technikaffine Gruppen den Diskurs dominieren.

Die UNDP (2025) hat hierzu einen umfassenden Leitfaden veröffentlicht. Eine ihrer zentralen Schlussfolgerungen lautet, dass Technologie allein keine Demokratie stärkt. Erfolgreiche Plattformen benötigen demnach hybride Strategien, die digitale und analoge Beteiligungswege verbinden, sowie klare Verantwortlichkeiten, damit die Beiträge der Bürger/innen tatsächlich in politische Entscheidungen einfließen können.

Bürokratische Verfahren strukturieren die Interaktion zwischen Staat und Bürger/innen sowie Unternehmen. Sie sichern Rechtsgleichheit und nachvollziehbare Entscheidungen, werden von vielen Betroffenen zugleich aber als zunehmend aufwendig und komplex erlebt. Die zunehmende Zahl an Gesetzen, Vorschriften und Berichtspflichten geht auch für Behörden mit wachsenden Erfassungs-, Dokumentations- und Prüfaufgaben einher. Um das Vertrauen in den Staat zu stärken, hat sich die Bundesregierung deshalb im Koalitionsvertrag zum Ziel gesetzt, den Bürokratierückbau voranzutreiben. Obwohl die Politik schon seit vielen Jahren entsprechende Maßnahmen vorantreibt, unter anderem mit vier Bürokratieentlastungsgesetzen seit 2015, zeigen verschiedene Indikatoren, dass die Bürokratiebelastung in Deutschland immer weiter gestiegen ist. So nahm zwischen 2010 und 2024 das Bundesgesetzgebungsvolumen von rund 24.775 auf 39.536 Normseiten zu – ein Anstieg von etwa 60 % in 15 Jahren (Wagner 2025). Ein weiterer Indikator neben der Regulierungsdichte ist der Erfüllungsaufwand, der den Zeitaufwand und die

direkten Kosten abbildet, die Unternehmen sowie Bürger/innen durch die Befolgung gesetzlicher Vorgaben entstehen. Seit 2021 ist der Erfüllungsaufwand deutlich gestiegen. Die dadurch entstandenen direkten Bürokratiekosten (2015–2024) werden auf 86 Mrd. Euro geschätzt (ifo Institut 2024). Laut einer aktuellen Umfrage mussten Unternehmen in den letzten 3 Jahren 325.000 Arbeitskräfte zusätzlich einstellen, um die gewachsene Bürokratie zu bewältigen (Gerber 2025).

3 Systemische Risiken und ihre Auswirkungen auf das Infrastruktursystem Staat und Verwaltung

Ein leistungsfähiges Infrastruktursystem „Staat und Verwaltung“ bildet die zentrale Grundlage für öffentliche Ordnung, demokratische Stabilität sowie das Vertrauen in staatliche Handlungsfähigkeit und stellt zugleich eine wesentliche Voraussetzung für die Gewährleistung innerer Sicherheit dar (BBK 2026). Darüber hinaus schafft es die institutionellen und organisatorischen Rahmenbedingungen für zentrale gesellschaftliche Transformationsziele, insbesondere in den Bereichen Digitalisierung, Organisations- und Personalmodernisierung sowie ökologische Nachhaltigkeit.

Vor diesem Hintergrund stellen systemische Risiken eine besondere Herausforderung dar, da sie nicht isoliert auf einzelne Komponenten eines Infrastruktursystems wirken, sondern dessen Funktionsfähigkeit insgesamt gefährden können. Sie bezeichnen komplexe Gefahren oder Bedrohungen, die durch nicht lineare Wechselwirkungen gekennzeichnet sind, geografische, sektorale und soziale Grenzen überschreiten und ihre Wirkung häufig als Kaskaden- und Verstärkungseffekte entfalten. Zudem weisen sie stochastische Wirkungsketten auf und können beim Erreichen von Kipppunkten abrupte und tiefgreifende Veränderungen auslösen. Charakteristisch ist ferner eine häufig verzögerte gesellschaftliche Wahrnehmung und Regulierung (Renn et al. 2022).

Aufgrund dieser Eigenschaften wirken systemische Risiken selten isoliert, sondern betreffen häufig mehrere Infrastruktursysteme gleichzeitig. Das Infrastruktursystem „Staat und Verwaltung“ ist dabei sowohl unmittelbar betroffen als auch mittelbar in seiner Steuerungs- und Koordinationsfunktion gefordert, da es eine zentrale Rolle bei der Prävention, Bewältigung und Regulierung systemischer Risiken einnimmt.

Für die nachfolgende Analyse wird eine heuristische Systematisierung systemischer Risiken zugrunde gelegt, die die Bereiche Gesellschaft, Technologie, Umwelt, Wirtschaft und Politik umfasst. Auf dieser Grundlage werden diejenigen systemischen Risiken betrachtet, die in der wissenschaftlichen Literatur und im fachlichen Diskurs als besonders relevant für das Infrastruktursystem „Staat und Verwaltung“ herausgearbeitet wurden und daher als besonders gefährdend einzustufen sind. Im Kapitel 2.1 werden die Auswirkungen dieser Risiken entlang zweier miteinander verknüpfter Perspektiven analysiert: Zum einen wird der aktuelle Stand der Gefährdungslagen unter Berücksichtigung relevanter systemischer Risiken sowie deren absehbarer Entwicklungsdynamiken untersucht. Zum anderen wird analysiert, welche Risiken im Kontext laufender Transformationsprozesse mit Pfadabhängigkeiten verbunden sind und welche Implikationen sich daraus für die zukünftige Robustheit und Leistungsfähigkeit des Systems ergeben.

3.1 Status quo der Gefährdungslagen und Entwicklungsdynamiken

Das Infrastruktursystem Staat und Verwaltung ist durch eine Reihe systemischer Risiken gefährdet, die die einzelnen Systembereiche in unterschiedlichem Maße betreffen. Für jedes dieser Risiken wird im Folgenden die Gefährdungslage (gering, eher gering, mittel, eher hoch, hoch) auf Grundlage einer explorativen Einschätzung der Eintrittswahrscheinlichkeit, des potenziellen Schadensausmaßes sowie der Anzahl der betroffenen Infrastruktursystembereiche bewertet. Auf Basis der Einzelbewertungen und unter Einbezug der ausgewerteten Quellen sowie der geführten Fachgespräche ergibt sich für das Infrastruktursystem insgesamt aktuell eine Gefährdungslage, die als eher hoch einzustufen ist. Die Funktionsfähigkeit und Stabilität des Infrastruktursystems werden derzeit vor allem durch Versorgungsengpässe, etwa den Fachkräftemangel und finanzielle Engpässe, aber auch Cyberkriminalität, geopolitische Konflikte und gesellschaftliche Polarisierung gefährdet. Angesichts der in den Trendanalysen dargestellten fortschreitenden Digitalisierung, der anhaltenden geopolitischen Spannungen und von Polarisierungstendenzen in der deutschen Gesellschaft ist von einem weiteren Anstieg der Gefährdung des Infrastruktursystems auszugehen.

Versorgungsengpässe

Versorgungsengpässe stellen aktuell eine eher hohe Gefährdung für die Funktionalität und Stabilität des Infrastruktursystems dar. Zentrale Ursachen hierfür sind der Personal- und Fachkräftemangel sowie finanzielle Engpässe. Der Trendcluster „Struktureller Wandel des öffentlichen Sektors“ macht deutlich, dass sich der Personalengpass in den letzten Jahren verschärft hat und weiter ansteigt. Bis auf die parlamentarische Steuerung sind derzeit alle Bereiche des Infrastruktursystems von Personalmangel betroffen, besonders jedoch der öffentliche Dienst sowie die Verteidigung (Kapitel 2.2).

Die direkte Folge von unbesetzten Stellen im Verwaltungsbereich sind für Bürger/innen deutlich längere Bearbeitungs- und Wartezeiten, beispielsweise in Bauämtern, Standesämtern oder Fahrerlaubnisbehörden. Bei der Staatsangehörigkeitsbehörde in Jena betrugen die Wartezeiten für einen Termin 2024 beispielsweise 12 bis 14 Monate. Gleichzeitig führt der Personalmangel zu einer steigenden Arbeitsbelastung für die Beschäftigten im öffentlichen Dienst. Beschäftigte der Kriminalpolizei nennen den Personalmangel als den belastendsten Faktor am Arbeitsplatz (DHPol 2024). Personalengpässe im Bereich der inneren Sicherheit und Verteidigung führen zu einer eingeschränkten Arbeitsfähigkeit und Einsatzbereitschaft, was sich beispielsweise in längeren Ermittlungszeiten, sinkenden Aufklärungsquoten und geringerer Präsenz im ländlichen Raum äußert (GdP MV 2025). Die Einsatz- und Verteidigungsfähigkeit der Bundeswehr ist erheblich beeinträchtigt, da ein personelles Defizit von rund 20.000 Soldat/innen besteht und zahlreiche Dienstposten unbesetzt bleiben. Die in den vergangenen Jahren von der Bundeswehr unternommenen Maßnahmen zur Gewinnung neuen Personals haben bislang nur geringe Wirkung gezeigt. So konnte die Personalstärke von 2023 bis 2025 trotz gezielter Anwerbungsmaßnahmen nicht erhöht, sondern nur auf dem bisherigen Niveau gehalten werden (Wehrbeauftragte 2025).

Neben dem anhaltenden Personal- und Fachkräftemangel belasten auch Finanzierungsdefizite sowie ein erheblicher Investitionsstau das Infrastruktursystem, insbesondere die Bereiche Regierungen und Verwaltungen sowie die innere Sicherheit und Verteidigung. Für die Kommunen stellen enge Haushaltsspielräume infolge hoher Mittelbindungen, nur moderat steigender Steuereinnahmen und zunehmender Ausgaben für Sozialleistungen zentrale Herausforderungen in den vergangenen Jahren dar. 2024 befanden sich viele Kommunen in einer angespannten Finanzsituation und waren teilweise nicht in der Lage, zu investieren und ihre Infrastrukturen instand zu halten (Kapitel 2.2). In den Bundesländern Saarland, Nordrhein-Westfalen, Sachsen-Anhalt und Rheinland-Pfalz hat sich die Situation bei der öffentlichen Infrastruktur verschlechtert, was sowohl für die Lebensqualität der Bürger/innen als auch für die Standortqualität von Unternehmen negative Folgen hat (Freier et al. 2025). Im Systembereich der öffentlichen Verwaltung und bei sicherheitsnahen Organisationen führen ausbleibende Investitionen zu einem zunehmenden Sanierungsbedarf bei Liegenschaften, zu technischen Defiziten in der mobilen Ausstattung sowie zu Verzögerungen bei der flächendeckenden Modernisierung der IT-Infrastruktur (GdP 2025). In Mecklenburg-Vorpommern können digitale Beweismittel aufgrund einer mangelnden und veralteten technischen Grundausstattung sowie fehlender Software-Lizenzen bei der Kriminalpolizei nicht umfänglich gesichert und ausgewertet werden. Fehlende Investitionen in die technische Ausstattung führen dazu, dass der Ermittlungsauftrag nicht erfüllt werden kann (GdP MV 2025). Dies bedeutet für Bürger/innen und Unternehmen, dass Straftaten langsamer aufgeklärt werden oder teilweise ungeahndet bleiben, was das Vertrauen in staatliche Schutz- und Sicherheitsstrukturen schwächt.

Die Gefährdung des Infrastruktursystems Staat und Verwaltung durch das systemische Risiko Versorgungsengpässe wird sich nach aktuellen Einschätzungen in den kommenden Jahren weiter erhöhen. Zentrale Treiber dieser Entwicklung sind strukturelle Herausforderungen, wie der demografische Wandel, ein steigender Bedarf an qualifizierten Fachkräften (vor allem mit digitalen Kompetenzen) sowie wachsende Ausgaben für die Sicherstellung staatlicher Daseinsvorsorge und sozialer Leistungen. In der Folge steigt sowohl die Wahrscheinlichkeit von Störungen der Funktionsfähigkeit der öffentlichen Verwaltung als auch die der Gefährdung des Erhalts der öffentlichen Daseinsvorsorge, insbesondere in den Bereichen Verkehrsinfrastruktur und Bildung. Ebenso steigt das Risiko von Kaskadeneffekten, wie die wachsende Unzufriedenheit der Bürger/innen mit der allgemeinen Handlungsfähigkeit des Staates.

Cyberkriminalität

Die Gefährdungslage durch Cyberkriminalität wird für alle Bereiche des Infrastruktursystems aktuell als eher hoch eingeschätzt. In den vergangenen Jahren haben Cyberangriffe zugenommen (Kapitel 2.4). Behörden und öffentliche Verwaltungen sind besonders häufig von IT-Sicherheitsvorfällen, Phishing-Angriffen sowie Cyberspionage betroffen (BSI 2024; BSI 2025). 2024 erfasste das Bundesamt für Sicherheit in der Informationstechnik (BSI) 80 Cyberangriffe auf Bundesbehörden. 17 davon waren erfolgreich und betrafen die Installation von Schadsoftware, die unautorisierte Systemnutzung sowie den Datenabfluss (Bundesregierung 2025a). Die Zunahme der Vorfälle ist einerseits auf die fortschreitende Digitalisierung des Infrastruktursystems bei gleichzeitig geringer IT-Modernisierung und andererseits auf eine Professionalisierung der Angreifenden zurückzuführen, die verstärkt KI-gestützte Angriffsmethoden, wie Deepfakephishing sowie Zero-Day-Exploits (Angriff über eine noch unbekannte und ungepatchte Sicherheitslücke), einsetzen

und damit herkömmliche Abwehrmechanismen umgehen (Schulmann 2026). Neben der Bedrohung durch Kriminelle hat sich auch die Gefahr durch externe staatliche Akteure weiter verfestigt. Die Zunahme staatlich gesteuerter, gezielter und zugleich schwer nachweisbarer Angriffe steht im Zusammenhang mit geopolitischen Konflikten und wird häufig Gruppen zugeschrieben, die Verbindungen zu Russland, China und Nordkorea aufweisen. Ein Beispiel für staatlich gesteuerte Cyberattacken ist der Spionageangriff auf das dem Bundesministerium des Innern unterstellte Bundesamt für Kartographie und Geodäsie im Jahr 2021, der dem chinesischen Akteursumfeld zugeordnet wurde (dpa 2024b). Ein weiteres Beispiel ist der Hackerangriff auf die E-Mail-Postfächer des SPD-Parteivorstands im Jahr 2023, der dem russischen Militärgeheimdienst GRU zugeschrieben wurde (dpa 2024a). 2024 wurden außerdem Angriffe auf E-Mail-Postfächer verschiedener politischer Organisationen bekannt. Eine Angriffsfläche stellten insbesondere Webmail-Systeme dar, die frei über das Internet und ohne Multifaktor-Authentifizierung erreichbar waren (BSI 2024). Seit dem Angriff Russlands auf die Ukraine verzeichnet die Bundeswehr einen erheblichen Anstieg von Distributed-Denial-of-Service (DDoS)-Ereignissen auf ihre öffentlichen Portale (Stephan 2025). Aufgrund bestehender Schutzmaßnahmen werden die daraus resultierenden Auswirkungen derzeit jedoch noch als gering eingestuft.

Auch Kommunen geraten häufig in das Visier von Cyberangriffen. Neben der Erpressung von Geld verfolgen die Angreifer damit auch das Ziel, das Vertrauen in staatliche Stellen zu schwächen und damit Unsicherheit zu schaffen. Aufgrund von oft unzureichender Vorsorge, begrenzter und veralteter IT-Sicherheitsstrukturen, geringer Budgets sowie fehlendem Fachpersonal sind die Folgen eines erfolgreichen Cyberangriffs für die Funktionalität und Leistungserbringung des Systembereichs häufig erheblich (Karpenstein 2025; Schulmann 2026). Kommunen sind vor allem potenzielle Opfer von Ransomware- und DDoS-Angriffen. Diese können zu massiven Störungen bis hin zu Totalausfällen bei kommunalen Verfahren und Dienstleistungen führen. Im Oktober 2023 war ein kommunaler IT-Dienstleister betroffen, der für 72 Kommunen mit mindestens 1,7 Mio. Einwohner/innen in Nordrhein-Westfalen zuständig ist. Als Reaktion darauf fuhr der Dienstleister die Mehrheit seiner IT-Systeme herunter, was zum vollständigen Ausfall der IT-Infrastruktur führte und weitreichende Kaskadeneffekte auslöste (BSI 2024). Verwaltungen waren nicht mehr erreichbar (weder telefonisch noch per E-Mail), Sozialämter konnten keine Anträge bearbeiten oder Auszahlungen veranlassen, Zulassungsstellen, Standesämter und Meldebehörden blieben geschlossen (Heinrich Böll Stiftung o. J.). Ein weiteres Beispiel ist die großflächige E-Mail-Spamwelle 2024, die durch das Schadprogramm Emotet verursacht wurde. Das Schadprogramm infizierte auch zahlreiche IT-Systeme von Kommunalverwaltungen, indem es gezielt Schwachstellen in veralteter Software ausnutzte. Auf infizierten Computern las das Programm E-Mails aus und verschickte auch selbst welche, ohne dass dies bemerkt wurde. Darüber hinaus wurden Systeme verschlüsselt, um Geld zu erpressen. In der Folge mussten unter anderem Behördennetzwerke neu aufgebaut werden. Ein weiteres Beispiel ist der Ransomware-Angriff auf die Gemeindeverwaltung Untereisesheim in Baden-Württemberg, der die digitalen Verwaltungsdienstleistungen für mehrere Tage fast vollständig zum Erliegen brachte (Küng 2025). Insgesamt zeigen die Beispiele, dass Cyberangriffe auf Staat und Verwaltung zentrale Prozesse öffentlicher Dienste und damit die Funktionsfähigkeit und Stabilität des Infrastruktursystems erheblich beeinträchtigen können.

Vor dem Hintergrund aktueller wissenschaftlicher Bewertungen wird sich die Gefährdungslage für das Infrastruktursystem Staat und Verwaltung durch das systemische Risiko der Cyberkriminalität in den kommenden Jahren erheblich verschärfen. Zu den zentralen Treibern dieser Entwicklung zählen die fortschreitende Digitalisierung sowie der zunehmende Einsatz hochgradig

skalierbarer KI-gestützter Phishing- und Ransomware-Angriffe. Hinzu kommen eine weiter voranschreitende Vernetzung und Professionalisierung staatlicher und privater Tätergruppen, die vor dem Hintergrund anhaltender geopolitischer Spannungen ein stetig wachsendes Angriffspotenzial erzeugen. In der Folge steigen sowohl die Wahrscheinlichkeit weitreichender Störungen der Funktionsfähigkeit des Infrastruktursystems als auch die Risiken ausgeprägter Kaskadeneffekte. Dazu zählen beispielsweise steigende Schadenskosten oder lange Wiederherstellungszeiten von Systemen.

Machtkonzentration

Machtkonzentrationen privatwirtschaftlicher Akteure wirken sich auf alle Bereiche des Infrastruktursystems Staat und Verwaltung aus und führen derzeit zu einer eher hohen Gefährdungslage. Besonders hervorzuheben sind hier Technologiekonzerne: Die Digitalisierung des Infrastruktursystems führte in den vergangenen Jahren zu einer immer stärkeren Abhängigkeit von proprietären Softwarelösungen, Cloudinfrastrukturen und Hardware großer Technologiekonzerne. 96 % der Verwaltungsangestellten arbeiten täglich mit Microsoft-Produkten (ZenDiS 2025). Die Technologieanwendungen sind tief in Verwaltungsprozesse integriert, wodurch Verwaltungen und Behörden sowohl technisch als auch vertraglich stark an sie gebunden sind. Insbesondere US-amerikanische Softwareunternehmen wie Microsoft oder Oracle bauen ihre Marktmacht mit Blick auf die Verwaltungs-IT und im Bereich der KI stetig aus und stellen zentrale Clouddienste zur Verfügung. Auch große IT-Dienstleister gewinnen durch das Outsourcing kritischer Aufgaben an Einfluss auf das Infrastruktursystem.

Aufgrund dieser Abhängigkeiten ist die digitale Souveränität des Staates und damit auch die Handlungsfähigkeit der öffentlichen Verwaltung stark eingeschränkt (IT-Planungsrat 2020). Digitale Souveränität ist jedoch eine zentrale Voraussetzung zur Erfüllung hoheitlicher Aufgaben. Umgekehrt führen fehlende digitale Souveränität zu Einschränkungen der Wahlfreiheit öffentlicher Einrichtungen, zu einer Zunahme von Sicherheitsrisiken, zu einem Schwund der Transparenz über Kosten und Steuerungsmaßnahmen sowie zu einem Verlust der Budgethoheit der öffentlichen Hand über ihre IT-Ausgaben. So haben sich beispielsweise die Ausgaben für Softwarelizenzen des Bundes von 2023 bis 2024 verdreifacht (2024: 160 Mio. Euro) (Deutscher Bundestag 2025). Derzeit wird eine schrittweise Abkehr von der digitalen Unsouveränität durch die Politik gefordert, beispielsweise durch die Stärkung des Einsatzes von Open-Source-Software in der öffentlichen Verwaltung (BMDS 2024; Menhard 2025). Eine erfolgreiche Umstellung auf quelloffene Software gelang bisher nur Schleswig-Holstein. Der Wechsel zu europäischen Open-Source-Software-Anbietern ist herausfordernd, weil er zunächst mit zusätzlichen Kosten und erheblichem Zeitaufwand verknüpft ist.

Auch bei Hardwareprodukten für die Verwaltungsinfrastruktur gibt es hohe Machtkonzentrationen, denn die Produktion von Schlüsselkomponenten, wie Prozessoren, Netzwerktechnik, Chips oder Servern, wird von nur wenigen Herstellern, wie Intel, Cisco, TSMC oder Samsung, dominiert. Negative Auswirkungen der technologischen Abhängigkeiten zeigen sich auch durch Störungen globaler Lieferketten, die dazu führen, dass die IT nicht ausreichend mit Geräten ausgestattet wird. Ein Beispiel hierfür ist die Chipkrise, die zwischen 2021 und 2023 andauerte und durch die COVID-19-Pandemie sowie eine nachfolgend schwächere Konjunktur verursacht wurde. Verstärkt wird diese Problematik durch die hohe Marktkonzentration auf dem Halbleitermarkt, wo wenige

Anbieter dominieren. Der Systembereich der hoheitlichen Gefahrenabwehr ist darüber hinaus mit Blick auf Luftfahrzeuge und Satellitentechnik bereits heute von großen außereuropäischen Unternehmen abhängig. Beispielsweise sind F35-Kampffjets der Bundeswehr ohne Software-Updates aus den USA nicht einsatzfähig. Ein weiteres Beispiel für eine steigende Abhängigkeit von US-Konzernen in diesem Systembereich ist die Nutzung der Analysesoftware von Palantir, die sensible personenbezogene Daten verarbeitet, um die polizeiliche und militärische Arbeit zu unterstützen. In Deutschland wird die Software bereits von vier Bundesländern eingesetzt, obwohl der Einsatz der Software als umstritten gilt, da nicht auszuschließen ist, dass Daten an Drittstaaten bzw. in diesem Fall an amerikanische Geheimdienste abfließen (Schweizer Armee 2024).

Nach aktuellen fachlichen Einschätzungen wird sich die Gefährdungslage für das Infrastruktursystem Staat und Verwaltung durch das systemische Risiko Machtkonzentration durch weitere Digitalisierungsprogramme zukünftig noch erhöhen, sofern diese nicht durch gezielte Governance-, Souveränitäts- und Diversifizierungsstrategien flankiert werden. Die starke Abhängigkeit von Technologieunternehmen macht deutlich, wie tief proprietäre Software- und Cloudlösungen in Verwaltungsprozesse integriert sind. Demgegenüber stehen sowohl das Fehlen wettbewerbsfähiger europäischer Alternativen als auch die zögerliche Umstellung auf Open-Source-Lösungen in der öffentlichen Verwaltung. Dies erhöht – gerade vor dem Hintergrund geopolitischer Spannungen – die Risiken von Erpressbarkeit und politischer Einflussnahme (Kapitel 2.1). Zentral getrieben wird diese Entwicklung vor allem durch Deutschlands strukturelle wirtschaftliche Abhängigkeiten, den technologischen Innovationsvorsprung globaler Konzerne sowie die verschärfte geopolitische Wettbewerbslage. In der Folge wächst das Risiko einer fortschreitenden Erosion digitaler Souveränität deutlich. Steigende Kosten und ausgeprägte Lock-in-Effekte proprietärer IT- und Cloudsysteme schränken die strategischen und operativen Entscheidungsspielräume von Staat und Verwaltungen ein, während eingeschränkter Datenzugang und die Abhängigkeit von ausländischen Plattformanbietern die Kontrolle über kritische und sensible Verwaltungsdaten vermindern. Zugleich erhöhen wachsende Cyberrisiken sowie potenzielle politische Einflussnahmen die Gefährdung der Integrität staatlicher Prozesse und der Funktionsfähigkeit öffentlicher Verwaltung.

Technikversagen und eingeschränkte Technikbeherrschbarkeit

Die Gefährdungslage durch das systemische Risiko Technikversagen und eingeschränkte Technikbeherrschbarkeit wird derzeit für alle Bereiche des Infrastruktursystems als eher hoch eingestuft. Durch zunehmend digitale Verwaltungsabläufe und -dienstleistungen, wie die E-Akte Bund oder Identitäts- und Automatisierungslösungen, haben sich die Angriffsflächen sowie die Störanfälligkeit des gesamten Infrastruktursystems erhöht. Neben externen Faktoren wie Cyberkriminalität oder Softwarefehlern können auch interne Bedienfehler oder ein mangelndes Sicherheitsbewusstsein bzw. mangelnde Kompetenzen des Personals ursächlich für Technikversagen sein. Ausfälle von IT-Systemen, Plattformen oder Software können alle Infrastrukturbereiche betreffen und zu Prozessunterbrechungen führen. Ein Beispiel hierfür war der globale Ausfall von Amazon Web Services (AWS) im Oktober 2025, der durch einen Fehler im AWS-Datenbanksystem DynamoDB ausgelöst wurde. Davon betroffen waren unter anderem Dienste wie Signal oder Zoom. Auch der Microsoft-Konzern meldete einige Tage später einen mehrstündigen Ausfall des Clouddienstes Azure mit Auswirkungen auf zahlreiche Microsoft-Dienste wie Microsoft 365 oder

Outlook (BSI 2025b). Solche technischen Ausfälle können in der öffentlichen Verwaltung zu erheblichen Einschränkungen führen. Services für Bürger/innen, Unternehmen und andere Verwaltungseinheiten stehen dann nicht zur Verfügung und die Bearbeitungs- und Wartezeiten verlängern sich deutlich. Auch die Polizei war bereits durch IT-Probleme vom systemischen Risiko Technikversagen und eingeschränkter Technikbeherrschbarkeit betroffen. Anfang 2025 kam es beispielsweise an Flughäfen bundesweit zu Problemen, die durch technische Störungen im Bundeskriminalamt ausgelöst wurden. Betroffen waren vor allem die Grenzkontrollen der Bundespolizei – Passkontrollen mussten daraufhin manuell durchgeführt werden, was zu längeren Bearbeitungszeiten führte (Zoric 2025).

Eine eingeschränkte Technikbeherrschbarkeit ist im Bereich der öffentlichen Verwaltung derzeit vor allem eine Folge unzureichender Aus- und Weiterbildung des Personals hinsichtlich IT-Kompetenzen sowie mangelhafter Kenntnisse in den Bereichen Datenschutz und IT-Sicherheit. Aber auch bei digitaler Kollaboration, agilen Arbeitsformen, Datenanalysen sowie im sicheren Umgang mit KI-Modellen bestehen Fähigkeitslücken, die die effektive Nutzung technischer Systeme erheblich einschränken (McKinsey 2023, 2024). Die fortschreitende Digitalisierung der öffentlichen Verwaltung sowie die schnelle Entwicklung neuer Technologien, etwa in den Bereichen Automatisierung oder generative KI, erfordern zunehmend spezifische Fachkenntnisse des Personals, insbesondere zur Funktionsweise der oft komplexen technischen Systeme (Kapitel 3.2).

Die Gefährdungslage des Infrastruktursystems Staat und Verwaltung durch das systemische Risiko Technikversagen und eingeschränkte Technikbeherrschbarkeit wird sich nach derzeitiger fachlicher Bewertung in den kommenden Jahren weiter erhöhen. Zentrale Treiber dieser Entwicklung sind die fortschreitende Digitalisierung des Infrastruktursystems, die Integration zunehmend komplexer technischer Systeme und die wachsende Verflechtung von E-Government-Angeboten (Kapitel 2.1). Die Gefahr der eingeschränkten Technikbeherrschbarkeit wird durch datenschutz- und haftungsrechtliche Unsicherheiten sowie unklare Datenflüsse bei der Nutzung generativer KI-Modelle verstärkt. Künftig wird diese Gefahr durch den zunehmenden Einsatz autonomer KI-Agenten noch weiter zunehmen. Die unzureichende Kompetenzentwicklung im öffentlichen Dienst begünstigt diese Entwicklung zusätzlich. Auch diskriminierende oder nicht nachvollziehbare Ergebnisse KI-gestützter Entscheidungsprozesse können zu erheblichen Fehlsteuerungen führen. In der Folge steigen sowohl die Eintrittswahrscheinlichkeit weitreichender Störungen zentraler staatlicher Funktionen als auch das Risiko ausgeprägter Kaskadeneffekte, beispielsweise durch eine eingeschränkte Handlungsfähigkeit der Verwaltung, eine verzögerte Leistungserbringung, Datenverluste oder eine mangelnde Überprüfbarkeit der Datensicherheit.

Geopolitische Konflikte

Die Gefährdungslage, die von geopolitischen Konflikten ausgeht, wird für das gesamte Infrastruktursystems derzeit als eher hoch eingestuft, wobei der Systembereich der inneren Sicherheit und Verteidigung stärker als die anderen Bereiche betroffen ist. Zentrale geopolitische Entwicklungen vergangener Jahre, wie der russische Angriffskrieg auf die Ukraine, die Systemkonkurrenz zwischen den USA und China sowie die Handelskonflikte zwischen der EU und den USA, haben die Gefährdungslage für das Infrastruktursystem erhöht. Die Bundesregierung (2023) spricht in der Nationalen Sicherheitsstrategie von einer „komplexen Bedrohungslage“, von der zunehmend kritische Infrastrukturen bedroht sind. Neben militärischen und terroristischen Bedrohungen haben

hybride Angriffe in Deutschland deutlich an Relevanz gewonnen (Kapitel 2.4). In der Folge dieser Konflikte steht Deutschland unter erheblichem politischem, wirtschaftlichem und gesellschaftlichem Druck (Breuer 2025; Hüther 2025). Auch Fluchtbewegungen, die durch geopolitische Konflikte, beispielsweise in der Ukraine oder in Syrien, ausgelöst wurden, stellen das Infrastruktursystem vor erhebliche organisatorische, finanzielle und gesellschaftliche Herausforderungen.

Aufgrund des Krieges in der Ukraine und der zunehmenden sicherheitspolitischen Bedrohung durch Russland stieg der Druck auf die deutsche Verteidigungsfähigkeit in den vergangenen Jahren deutlich an. Zur Stärkung der NATO investiert Deutschland stark in die Verteidigungsfähigkeit des Landes. Mit Blick auf die Bundeswehr und Polizei zeigen sich derzeit allerdings Schwächen bei der technischen Ausstattung, beispielsweise bei der Drohnenabwehr. 2025 wurden vermehrt Drohnen über und in der Nähe von Bundeswehrstandorten sowie Flughäfen gesichtet, was zu Flugausfällen führte und die Unsicherheiten bei Sicherheitsbehörden im Umgang mit solchen Vorfällen aufzeigte. Angesichts der schnellen Entwicklung der Drohnentechnik und von Drohnenabwehrsystemen ist eine gute Ausstattung unerlässlich, um die Verteidigungsfähigkeit zu gewährleisten und Bundeswehrstandorte zu sichern (Wehrbeauftragte 2025).

Aktuell ist fachlich davon auszugehen, dass sich die Gefährdungslage für das Infrastruktursystem Staat und Verwaltung durch das systemische Risiko geopolitischer Konflikte in den kommenden Jahren erhöhen wird. Internationale Analysen prognostizieren eine zunehmende Häufigkeit von Konflikten, die insbesondere durch die geopolitische, ökonomische und ideologische Rivalität zwischen den USA und China, die sich zuspitzende Taiwan-Krise, die anhaltende Instabilität im Nahostkonflikt sowie den fortdauernden russischen Angriffskrieg gegen die Ukraine weiter verschärft werden (Kolodko 2025; Rudolf 2019; WEF 2023; Yang et al. 2022). In der Folge ist mit einem weiteren Anstieg hybrider Bedrohungen in Form staatlich gesteuerter Cyberangriffe, dem Einsatz von Drohnen und Desinformationskampagnen zu rechnen. Dabei steigt sowohl die Wahrscheinlichkeit weitreichender Auswirkungen auf zentrale Funktionen des Infrastruktursystems, wie die Sicherstellung der hoheitlichen Gefahrenabwehr, als auch das Risiko ausgeprägter Kaskadeneffekte – etwa durch die gezielte Schwächung des Vertrauens in staatliche Institutionen oder durch die steigenden finanziellen und organisatorischen Anforderungen zur Sicherung der inneren und äußeren Sicherheit.

Desinformation

Die Gefährdungslage durch Desinformation wird für alle Bereiche des Infrastruktursystem derzeit als eher hoch eingeschätzt. Besonders das Parlament und die politische Willensbildung sind bereits stark betroffen. Seit dem Aufkommen generativer KI ist die automatisierte Erstellung täuschend echter Texte, Bilder und Videos deutlich einfacher geworden. In Verbindung mit sozialen Medien, KI-Algorithmen und der zunehmenden Verlagerung von Meinungsbildungsprozessen auf digitale Plattformen haben interessierte Akteure die Möglichkeit, Desinformationen und Manipulationen schnell und großflächig zu verbreiten. Desinformation ist zudem ein zentraler Bestandteil hybrider Bedrohungen, die im Kontext geopolitischer Konflikte entstehen (Kapitel 2.4).

Desinformationen gefährden vor allem das Parlament und demokratische Prozesse. Sie zielen auf die politische Einflussnahme ab, um bestimmte Positionen zu stärken oder Verunsicherung in der Bevölkerung im Hinblick auf politische Entscheidungen oder Wahlergebnisse zu schaffen.

Ein Beispiel hierfür ist die Europawahl 2024: Ausländische Akteure verbreiteten bekannte Desinformationsnarrative und die prorussische Desinformationskampagne „Doppelgänger“ rief zur Wahl bestimmter Parteien auf (Bundesregierung 2024). Häufig werden bestehende Krisen und kontrovers geführte politische Debatten zu Migration, Energieversorgung, Klimawandel oder Sicherheitspolitik in den Kampagnen aufgegriffen und beispielsweise auch durch ausländische Akteure in falschen Zusammenhängen dargestellt. Der Umgang mit Desinformation setzt zunehmend digitale Medienkompetenzen bei Bürger/innen voraus, um Inhalte zu bewerten, zu hinterfragen und einzuordnen. Zwar wurden in der Vergangenheit Korrektive, wie beispielsweise Faktenchecks der Bundesministerien, aufgebaut – allerdings wirken sie bisher oft zu langsam oder erreichen nicht die intendierten Zielgruppen. Im Vergleich zu traditionellen Medien gelten für den digitalen Raum keine Regeln, die eine ausgewogene und sorgfältige Berichterstattung fördern.

Desinformationen können das Vertrauen in den Staat und staatliche Institutionen untergraben und das Verhalten von Bürger/innen direkt beeinflussen. Während der COVID-19-Pandemie behinderten Desinformationen in den sozialen Netzwerken die behördliche Kommunikation von Gesundheitsrisiken. Der Umgang mit diesen bewusst platzierten Falschinformationen war seitens der Bundes- und Landesbehörden eher defensiv, auf kommunaler Ebene wurden Richtigstellungen hingegen häufiger aktiv und personalisiert vorgenommen. Systematische Kommunikationsansätze gegen Desinformationen gab es größtenteils nicht (Schleicher et al. 2024).

Auch auf die Judikative hat Desinformation einen negativen Einfluss, insbesondere hinsichtlich der Prozesse der Beweisaufnahme und Urteilsfindung. Derzeit besteht das Risiko, dass insbesondere KI-generierte Inhalte fälschlicherweise als authentisch bewertet werden. Die Erkennung synthetisch generierter Inhalte spielt demnach eine Schlüsselrolle, um die Wahrheit von Manipulation bzw. Desinformation unterscheiden zu können (Kellermann/Labudde 2024). In Deutschland sind bereits zwei Fälle bekannt geworden, in denen Anwälte in Gerichtsverfahren nachweislich falsche, KI-generierte Schriftsätze einbrachten (Amos 2025). Auch die Polizei sieht sich einer immer größer werdenden Flut an Informationen gegenüber und muss einschätzen können, ob diese relevant und vertrauenswürdig sind. Im Katastrophenfall verbreiten sich Desinformationen besonders schnell, was die Arbeit der Sicherheitskräfte behindern kann. Auch die Bundeswehr ist von Desinformationen betroffen. Sie bewertet diese als hybride Beeinflussung, deren Ziel es ist, die Leistungsfähigkeit und Einsatzbereitschaft zu schwächen. Konkret geht es um Informationsmanipulation, die Entscheidungsprozesse stören oder die Einsatzmoral schwächen soll. Bisher sind die Auswirkung laut Bundeswehr jedoch gering, was auf Schulungen und Sensibilisierungsmaßnahmen der Truppen zurückgeführt wird (Wroblewski 2025).

Aktuellen fachlichen Einschätzungen zufolge wird sich die Gefährdungslage für das Infrastruktursystem Staat und Verwaltung durch das systemische Risiko Desinformation in den kommenden Jahren verschärfen. Zentrale Treiber sind geopolitischen Spannungen und das daraus resultierende steigende Interesse ausländischer Akteure an gezielter Einflussnahme sowie Fortschritte in der generativen KI. Letztere ermöglicht die automatisierte Erstellung von Inhalten und Medien und fördert deren schnelle, massenhafte Verbreitung. Dadurch steigt die Verwundbarkeit des Infrastruktursystems gegenüber manipulativen Informationen weiter, welche die öffentliche Meinungsbildung sowie demokratische Prozesse stark beeinflussen können. Dies kann zu wachsender gesellschaftlicher Verunsicherung und politischer Polarisierung sowie zu einem weiteren Rückgang des Vertrauens in politische und staatliche Institutionen führen (Kapitel 2.4).

Gesellschaftliche Polarisierung

Die Gefährdungslage durch gesellschaftliche Polarisierung ist derzeit für alle Bereiche des Infrastruktursystems als eher hoch einzustufen. Mehr als 80 % der Deutschen nehmen die Gesellschaft als gespalten wahr (Vorländer et al. 2025) und fast 50 % der Erwerbstätigen sorgen sich um den gesellschaftlichen Zusammenhalt (Kohlrausch 2023) (Kapitel 2.4). In den vergangenen Jahren hat die politische Polarisierung zugenommen, was sich auch in der politischen Kommunikation und der medialen Berichterstattung widerspiegelt. Diese Entwicklung wurde maßgeblich durch Social-Media-Plattformen vorangetrieben, denn sie basieren auf Algorithmen, die negativen Nachrichten und Provokationen mehr Sichtbarkeit verschaffen und populistischen sowie radikalen Kräften eine Plattform bieten (Fischer 2024; Weiser et al. 2025). Das größte Spaltungspotenzial wird derzeit den Themen Zuwanderung, Klimaschutz und Unterstützung der Ukraine zugeschrieben. Darüber hinaus zeigt sich eine steigende soziale Ungleichheit, die sich in sozioökonomischen Faktoren wie Einkommen und Bildungsniveau niederschlägt (Böhnke et al. 2023). Besonders in den unteren Einkommensklassen zeigen sich Tendenzen der Entfremdung von der Gesellschaft und vom politischen System, was sich auch in einem geringeren Vertrauen in staatliche Institutionen widerspiegelt (Spannagel/Brülle 2024) (Kapitel 2.4). In einer Bürgerbefragung des dbb beamtenbund und tarifunion geben 73 % der Befragten an, dass der Staat die Herausforderungen des Landes nicht bewältigen kann, wobei insbesondere Wähler/innen der Linkspartei (95 %) sowie der AfD und CDU (je rund zwei Drittel) dieser Ansicht sind (forsa 2025a). Gleichzeitig haben Übergriffe auf Kommunalpolitiker sowie Beschäftigte des öffentlichen Dienstes zugenommen, besonders betroffen sind Polizist/innen, Mitarbeiter/innen von Rettungsdiensten sowie Fahrer/innen von Bussen und Straßenbahnen (forsa 2025b; Hüster 2026).

Die gesellschaftliche Polarisierung zeigt sich 2024 auch in einem Höchststand politisch motivierter Straftaten. Das Bundeskriminalamt spricht von einer zunehmenden Herausforderung für die innere Sicherheit (Kapitel 2.4). In Deutschland werden darüber hinaus Aktionen zur Schwächung der Justiz beobachtet, bei denen beispielsweise zahlreiche Klagen eingereicht werden, um Gerichte zu blockieren und zu delegitimieren. Zudem versuchen Parteien, die über ein Drittel der Sitze in einem Parlament verfügen, den Mechanismus der Zweidrittelmehrheit auszunutzen, um beispielsweise Richterwahlen dauerhaft zu blockieren, was zu Verzögerungen in Parlamenten und Gerichten führen kann (Karpenstein/Kirschnick 2024; Zillesen et al. 2025).

Die Gefährdungslage für das Infrastruktursystem Staat und Verwaltung durch das systemische Risiko gesellschaftliche Polarisierung wird sich nach heutiger fachlicher Bewertung in den kommenden Jahren erhöhen. Zentrale Treiber sind die andauernden politischen Spannungen und die Zunahme sozialer Ungleichheit, die das Vertrauen in Institutionen weiter schwächen und die Stabilität des Infrastruktursystems gefährden. In der Folge nimmt die Wahrscheinlichkeit von Störungen der parlamentarischen Steuerung zu, etwa durch politische Blockaden oder gescheiterte Gesetzesvorhaben. Auch die Funktionsfähigkeit der inneren Sicherheit wird stärker herausgefordert, etwa durch eine Zunahme politisch motivierter Taten oder von Gewalt im öffentlichen Raum (Münch 2024). Ebenso steigt das Risiko von Kaskadeneffekten – etwa durch eine Reformunfähigkeit des Staates, die notwendige Modernisierungen des Infrastruktursystems verhindern kann, oder durch die Schwächung des Solidaritätsprinzips, wodurch die Finanzierung und die Akzeptanz der Sozialsysteme untergraben werden können.

Epidemien und Pandemien

Epidemien und Pandemien stellen ein systemisches Risiko mit aktuell eher hoher Gefährdungslage für das Infrastruktursystem dar. In der Vergangenheit war Deutschland nur selten von Pandemien betroffen. Die Folgen der COVID-19-Pandemie verdeutlichen jedoch, dass die Auswirkungen von Pandemien auf das Infrastruktursystem erheblich sind. So mussten viele Kommunen ihre Ämter schließen oder den Publikumsverkehr stark einschränken (dpa 2020). Im weiteren Verlauf der Pandemie kam es in Regionen mit hohem Infektionsgeschehen immer wieder zu starken Einschränkungen der Dienstleistungen von Ämtern und Behörden. Einschränkungen im Bürgerservice ergaben sich auch durch akuten Personalmangel aufgrund eines hohen Krankenstands – einzelne Bereiche waren zwischenzeitlich nicht funktionsfähig. Gleichzeitig erhöhte sich die Arbeitsbelastung des Personals deutlich; etwa ein Drittel der Beschäftigten der kommunalen Verwaltungen übernahm während der Pandemie zusätzliche Aufgaben (Kairies-Lamp/Steinkraus 2021). 2020 verfügten viele kommunale Verwaltungen noch nicht über eine ausreichend ausgebaute digitale Infrastruktur und boten ihren Beschäftigten daher seltener die Möglichkeit zur Arbeit im Homeoffice als die Landes- oder Bundesbehörden. Angesichts des Digitalisierungsschubs infolge der COVID-19-Pandemie und der damit einhergehenden Ausweitung von Homeoffice-Möglichkeiten ist davon auszugehen, dass zukünftige Pandemien effektiver bewältigt werden können.

In den kommenden Jahren bleibt die Gefährdungslage für das Infrastruktursystem durch das systemische Risiko Epidemien und Pandemien hoch und könnte sogar leicht zunehmen. Epidemien als regional begrenzte, aber zunehmend disruptive Krankheitsausbrüche ebenso wie das Potenzial neuer Pandemien werden durch vernetzte Lieferketten, Urbanisierung und klimabedingte Veränderungen begünstigt (TAB 2024). Für das Infrastruktursystem Staat und Verwaltung bedeutet dies einen steigenden Finanzbedarf – sowohl für präventive Maßnahmen als auch für die etwaige Bewältigung von Pandemien sowie für die Bereitstellung staatlicher Nothilfen zur Abfederung wirtschaftlicher und sozialer Folgen. Gleichzeitig steigt die gesellschaftliche Erwartung an die öffentliche Verwaltung, die digitale Transformation zügig umzusetzen, um die Funktionsfähigkeit von Behörden auch unter Pandemiebedingungen aufrechtzuerhalten und Verwaltungsdienstleistungen digital zugänglich zu machen.

Globale Erwärmung und Wetterextreme

Die Gefährdung des Infrastruktursystems durch globale Erwärmung und die Zunahme von Wetterextremen wird derzeit insgesamt als mittel eingestuft. Besonders die Bereiche Regierungen und Verwaltungen sowie innere Sicherheit und Verteidigung sind durch die Bewältigung der Folgen dieser systemischen Risiken sowie durch die erforderlichen Anpassungsmaßnahmen gefordert. In einer Umfrage von 2024 gaben 92 % von 271 befragten Kommunen an, in den vergangenen 10 Jahren bereits unter den Folgen von Starkniederschlägen, Hitzewellen und Hochwasser gelitten zu haben (Overath/Rösler 2025).

Behörden und Verwaltungen sehen sich dabei einer doppelten Herausforderung gegenüber: Zum einen sind sie direkt betroffen, etwa durch steigende Risiken für Infrastruktur und Betrieb (zum Beispiel Gebäudeschäden infolge von Extremwetterlagen) sowie einen erhöhten Aufwand für die Bewältigung von Katastrophen und die Schadensregulierung. Zum anderen obliegt ihnen die Rolle

als Gestalter und Treiber von Anpassungsmaßnahmen. Beispielsweise können sie Klimaschutzbelange in Entwicklungspläne auf Landes- und Regionalebene integrieren, um Menschenleben zu schützen und finanzielle Schäden sowie steigende öffentliche Belastungen zu begrenzen (BMUKN 2024) (Kapitel 2.3). Die Anpassung an den Klimawandel ist für Kommunen ein zentrales Thema, erfordert jedoch Personal und erhebliche Investitionen, die angesichts der Finanznot vieler Kommunen derzeit kaum realisierbar sind (Overath/Rösler 2025; Raffer 2023).

Nach aktuellen fachlichen Erkenntnissen wird sich die Gefährdungslage für das Infrastruktursystem Staat und Verwaltung durch die systemischen Risiken globale Erwärmung und Wetterextreme in den kommenden Jahren erhöhen. Der fortschreitende globale Klimawandel führt bereits heute zu einer messbaren Zunahme von Extremwetterereignissen, wie Hitzewellen, starken Frostepisoden, Winterstürmen, Gewittern und hochwasserrelevanten Starkregenereignissen (Kunz 2025), – ein Trend, der sich auch in Deutschland und Mitteleuropa weiter verstärken wird (Glaser 2025; Hildebrandt/Lemaitre 2025). Gleichzeitig steigt der Druck auf Kommunen, Klimaanpassungsmaßnahmen umzusetzen (Kapitel 2.3). Angesichts knapper finanzieller Ressourcen sind Kommunen jedoch kaum in der Lage, Planungsprozesse durchzuführen und Maßnahmen umzusetzen. Dadurch steigt das Risiko höherer finanzieller Aufwendungen für die Katastrophengewältigung und Schadensregulierung. Auch das Risiko ausgeprägter Kaskadeneffekte nimmt zu, etwa durch das sinkende Vertrauen in die staatliche Handlungsfähigkeit oder steigende Kosten für das Gesundheitssystem, zum Beispiel durch hitzebedingte Erkrankungen.

Blackouts

Die Gefährdungslage durch das systemische Risiko eines Blackouts wird für das Infrastruktursystem Staat und Verwaltung derzeit als eher gering eingeschätzt, da die Eintrittswahrscheinlichkeit eines flächendeckenden und langandauernden Blackouts in Deutschland nach aktueller Lage niedrig ist, was sich in der stabilen bzw. leicht abnehmenden durchschnittlichen Unterbrechungsdauer der Stromversorgung widerspiegelt (Bundesnetzagentur 2025; Bundesregierung o. J.). Im Falle eines solchen Ereignisses wären die Auswirkungen jedoch gravierend. Die Abhängigkeit des Infrastruktursystems Staat und Verwaltung von einer stabilen Stromversorgung ist in den letzten Jahren im Zuge der Digitalisierung stark gestiegen. Ein langandauernder Blackout würde sämtliche Bereiche des Infrastruktursystems massiv beeinträchtigen.

Die Gefährdungslage des Infrastruktursystems Staat und Verwaltung durch das systemische Risiko Blackout wird nach aktuellen Einschätzungen auf geringem Niveau bleiben. Die Energiewende und die zunehmende Digitalisierung des Energiesystems leisten zwar einen Beitrag zur Versorgungssicherheit, indem sie fossile Importabhängigkeiten reduzieren, Großanlagenrisiken verringern und digitale Steuerungssysteme für eine stabilere Netzführung nutzbar machen. Mit der wachsenden Abhängigkeit von IKT-Systemen entstehen jedoch auch neue Risikofaktoren für die Versorgungssicherheit, insbesondere durch Cyberangriffe (BSI 2025b). Bundesnetzagentur und BSI fordern deshalb Maßnahmen zur Früherkennung von Cyberangriffen und eine Stärkung von Schutzmaßnahmen für Anlagen und Stromnetze. Trotz dieser neuen Risikotreiber bleibt das Gesamtrisiko eines Blackouts sehr gering, da das deutsche Stromsystem redundant aufgebaut ist, hohe Sicherheitsstandards gelten und Notfallpläne vorliegen, um die Stromversorgung im Ernstfall schnell wiederherzustellen.

Biodiversitätsverlust

Die durch Biodiversitätsverlust verursachte Gefährdungslage für das Infrastruktursystem Staat und Verwaltung ist derzeit als **gering** einzuschätzen. Sie wirkt sich aktuell vor allem indirekt und kumulativ aus, indem Ökosystemleistungen (zum Beispiel sauberes Wasser, Ernährungssicherheit, Krankheitsregulation) unter Druck geraten.

Die Gefährdungslage des Infrastruktursystems Staat und Verwaltung durch das systemische Risiko Biodiversitätsverlust wird sich nach aktuellen Einschätzungen erhöhen. Treiber dieser Entwicklung sind vor allem der hohe Flächenverbrauch, Monokulturen sowie Klimastress bei gleichzeitig zu langsam vereinbarten und greifenden politischen Gegenmaßnahmen (Reinke 2025). Langfristig erhöht dies die Anforderungen an staatliche Planungs-, Vollzugs- und Vorsorgeprozesse, weil Kommunen, Länder und Bund häufiger auf unsicherere ökologische Grundlagen reagieren und ihre Entscheidungen in Bereichen wie Wasserbewirtschaftung, Boden- und Flächennutzung, Infrastrukturunterhalt, Katastrophenvorsorge und Gesundheitsvorsorge anpassen müssen. Dadurch entstehen wachsende Risiken für staatliche Steuerungs- und Verwaltungsprozesse im Sinne größerer Planungsunsicherheiten, komplexerer Abstimmungsbedarfe und eines steigenden Aufwands für Monitoring, Bewertung und Koordination. Im Ergebnis dürfte der finanzielle Aufwand des Staates deutlich steigen – sowohl für Schutz- und Ausgleichsmaßnahmen als auch für technische Ersatzlösungen, Infrastruktur-, Wasser- und Gesundheitsvorsorge sowie den wachsenden administrativen Anpassungsbedarf. Zudem können Konflikte um knapper werdende Ressourcen wie sauberes Wasser oder fruchtbare Böden soziale und politische Spannungen verstärken.

3.2 Gefährdungslagen im Zuge der Transformation

Das Infrastruktursystem „Staat und Verwaltung“ befindet sich in einem tiefgreifenden Wandel und steht aktuell vor der Herausforderung, drei wesentliche Transformationsziele umzusetzen. Erstens ist die Organisations- und Personalmodernisierung Voraussetzung für die Stärkung der Leistungs- und Zukunftsfähigkeit der öffentlichen Verwaltung. Zweitens bilden Digitalisierung und technologische Modernisierung die Grundlage für eine effizientere, wirkungsvollere und gegenüber zukünftigen Herausforderungen widerstandsfähigere Verwaltung. Drittens sind aufgrund des Klimawandels umfassende Maßnahmen erforderlich, um die Treibhausgasemissionen des Infrastruktursystems zu senken und damit einen Beitrag zur angestrebten Klimaneutralität Deutschlands bis 2045 zu leisten. Die Umsetzung dieser Transformationen ist herausfordernd und kann durch verfestigte Entwicklungspfade (Pfadabhängigkeiten) verzögert oder erschwert werden. Im Folgenden werden zentrale Pfadabhängigkeiten im Kontext der drei Transformationsziele entlang zeitlicher und akteursbezogener Dimensionen analysiert. Eine abschließende Risikoperspektive verdeutlicht jeweils die potenziellen Gefahren bei Nichterreichen der angestrebten Entwicklungsziele in den drei Transformationsfeldern.

Organisations- und Personalmodernisierung

Das Infrastruktursystem Staat und Verwaltung ist in Deutschland im Hinblick auf das Ziel der Organisations- und Personalmodernisierung durch langfristige zeitliche Pfadabhängigkeiten geprägt. Zeitliche Pfadabhängigkeiten sind in der öffentlichen Verwaltung auf historisch verfestigte Organisationsstrukturen und eine Verwaltungskultur zurückzuführen, die stark auf Stabilität, Regelbindung und Fehlervermeidung ausgerichtet ist. Diese kulturelle und institutionelle Ausrichtung führt dazu, dass Veränderungen überwiegend inkrementell und mit langen zeitlichen Verzögerungen erfolgen. Gleichzeitig wird im Zuge veränderter Entwicklungsbedingungen zunehmend deutlich, dass diese historisch gewachsene Statik den dynamisch wachsenden und sich wandelnden Verwaltungsaufgaben immer weniger gerecht wird (forsa 2025). Trotz dieses Anpassungsdrucks wurde die politische Modernisierung der Verwaltung bisher vernachlässigt. Reformpläne wurden kaum umgesetzt. Das Fehlen einer klaren politischen Vision wirkt als zusätzlicher Verzögerungsfaktor im Veränderungsprozess (Achleitner et al. 2024). Strukturell wird diese Trägheit durch die starke Verrechtlichung und Bürokratisierung administrativer Strukturen verstärkt, die Organisations- und Personalveränderungen an formelle Gesetzgebungs-, Tarif- und Haushaltsprozesse bindet und damit lange Reformzyklen erzeugt. Außerdem erschwert der föderale Aufbau eine effiziente Steuerung und Umsetzung von übergreifenden komplexen Verwaltungsvorhaben. Daraus resultiert eine insgesamt geringe Umsetzungsdynamik, die auf die Schwierigkeiten in der föderalen Zusammenarbeit zurückzuführen sind (Achleitner et al. 2024).

Zeitliche Pfadabhängigkeiten innerhalb des Infrastruktursystems ergeben sich ebenfalls durch die Art der Anstellungsverhältnisse. Im öffentlichen Dienst überwiegt das Lebenszeitprinzip (Verbeamtung auf Lebenszeit), das durch stabile Laufbahnen und langfristige Beschäftigungsverhältnisse geprägt ist. Frühere Einstellungs- und Laufbahnentscheidungen wirken über Jahrzehnte fort und begrenzen die Handlungsspielräume bei der Personalmodernisierung, die häufig erst im Zuge von Pensionierungen und Generationswechseln möglich ist.

Neben zeitlichen wirken akteursbezogene Abhängigkeiten ebenfalls als Hemmnisse für die Organisations- und Personalmodernisierung im Infrastruktursystem. Auf Behörden- und Verwaltungsebene wird das Thema Führung bisher gering priorisiert, und zentrale Steuerungselemente wie das Personalmanagement werden bisher zu wenig strategisch und selten im Sinne eines strategischen Human-Resource-Managements umgesetzt. Fragen der vorausschauenden Kompetenzentwicklung oder der Professionalisierung von Führungskräften bleiben oft nachgeordnet (Hammerschmid 2024). Besonders deutlich zeigen sich akteursbezogene Pfadabhängigkeiten in den Einstellungs- und Rekrutierungspraktiken. Langwierige, stark formalistische und bürokratische sowie wenig wertschätzende Auswahlverfahren führen dazu, dass potenzielle Bewerber/innen abspringen oder sich überhaupt nicht bewerben. Die öffentliche Verwaltung agiert damit aus der Perspektive externer Akteure wenig wettbewerbsfähig auf dem Arbeitsmarkt. Verstärkt wird dieser Effekt durch eine starke Fixierung auf formelle Bildungsabschlüsse und Laufbahnvoraussetzungen, während Fach- oder Führungskompetenzen sowie informell erworbene Erfahrungen nur begrenzt berücksichtigt werden. Zudem bestehen kaum tarifliche Spielräume für die Anerkennung von extern erworbenen Erfahrungen (Achleitner et al. 2024). Das deutsche Verwaltungssystem gilt als ein eher geschlossenes System, das Quereinsteigern aus anderen Sektoren den Einstieg erschwert, obwohl gerade diese Akteursgruppe aufgrund ihrer externen Erfahrungen und Perspektiven über ein hohes Modernisierungspotenzial verfügt. Gleichzeitig wird die langfristige Bindung von Quereinsteigern/innen erschwert, was insbesondere auf Defizite im

Personalmanagement (zum Beispiel fehlende Fortbildungen oder Aufstiegsmöglichkeiten) und auf die starke Formalisierung und Bürokratisierung des Verwaltungshandels zurückzuführen ist (Hammerschmid 2024).

Auch Führungs- und Entscheidungsstrukturen tragen zur Reproduktion von akteursbezogenen Pfadabhängigkeiten bei. Die in vielen Verwaltungen vorherrschende Top-down-Führung ist auf Stabilität und Regelkonformität ausgerichtet und erweist sich bei tiefgreifenden Modernisierungsprozessen oft als hinderlich (Zejewski 2023). Die Einbeziehung der Bottom-up-Perspektive gilt in Innovationsprozessen hingegen als förderlicher für organisationales Lernen und Mitarbeiterengagement. Diese werden jedoch durch etablierte Zuständigkeitsprinzipien, hierarchische Entscheidungswege und formale Zustimmungserfordernisse auf der Arbeitsebene bisher ausgebremst. Insgesamt stabilisieren diese akteursbezogenen Pfadabhängigkeiten ein Selbstverständnis von Verwaltung, das auf interne Reproduktionslogiken, formale Sicherheit und hierarchische Steuerung ausgerichtet ist. Sie verlangsamen dadurch nicht nur die Organisations- und Personalmodernisierung, sondern begrenzen auch die Fähigkeit zentraler Akteure, externe Impulse aufzunehmen, neue Rollen einzunehmen und Transformation zu befördern.

Gelingt die Organisations- und Personalmodernisierung im Infrastruktursystem nicht, kann die Funktionsfähigkeit des Infrastruktursystems signifikant beeinträchtigt werden. Dies kann dazu führen, dass die Aufgaben der Daseinsvorsorge nur eingeschränkt erfüllt werden können. Zudem kann das Vertrauen der Bürger/innen in das Infrastruktursystem dadurch weiter sinken, was wiederum gesellschaftliche Konflikte und Polarisierung verstärken kann. Darüber hinaus erhöht eine organisatorisch und personell nicht modernisierte Verwaltung die Anfälligkeit des Infrastruktursystems für systemische Risiken, etwa durch eine verminderte Resilienz gegenüber externen Schocks wie Cyberangriffen oder Krisensituationen, in denen schnelle, koordinierte und kompetenzbasierte Reaktionen erforderlich sind.

Digitalisierung und technologische Modernisierung

Das Infrastruktursystem Staat und Verwaltung ist im Hinblick auf das Ziel der Digitalisierung und technologischen Modernisierung durch langfristige zeitliche Pfadabhängigkeiten gekennzeichnet, die in den vergangenen Jahren zu einer langsamen und nur ungenügend flächendeckenden Umsetzung der digitalen Transformation geführt haben. Besonders deutlich wird dies an der unzureichenden Umsetzung des OZG: Bis 2025 waren lediglich 349 der 575 Leistungen digital verfügbar (Bitkom e. V. 2025a). Die digitale Transformation des Infrastruktursystems ist eng an Gesetzgebungs-, Vergabe- und Datenschutzprozesse gebunden, die lange Reformzyklen erzeugen und schnelle Anpassungen erschweren. Zudem behindert die geringe Zusammenarbeit zwischen Bund, Ländern und Kommunen eine effiziente Umsetzung von Digitalisierungsmaßnahmen (Röhl/Engels 2025), was zu unterschiedlichen Digitalisierungsständen und -geschwindigkeiten auf Bund-, Länder- und kommunaler Ebene führt. Zeitliche Pfadabhängigkeiten ergeben sich außerdem aus den langfristigen Beschäftigungsverhältnissen und den etablierten Qualifikationsprofilen der Beschäftigten. Dies verlangsamt den notwendigen Aufbau digitaler Kompetenzen und den kulturellen Wandel in den Organisationen. Auch die Arbeitsweisen der öffentlichen Verwaltung, die durch Altsysteme (Legacyssysteme) und papierbasierte Prozesse geprägt sind, begrenzen die Geschwindigkeit und die Tiefe der Digitalisierung.

Neben zeitlichen wirken auch akteursbezogene Pfadabhängigkeiten auf die Erreichung des Transformationsziels der Digitalisierung und technologischen Modernisierung ein. Politische Akteure haben das Thema bisher unzureichend priorisiert, was sich auch in einer ungenügenden Bereitstellung finanzieller Mittel äußert und den Transformationsprozess bremst. Unzureichende gesetzliche Konkretisierungen, beispielsweise mit Blick auf den Verzicht einer Ende-zu-Ende-Digitalisierung im OZG, begünstigen eine lediglich oberflächliche Digitalisierung administrativer Abläufe. Gleichzeitig wurde nicht frühzeitig erkannt, dass die Verpflichtungen des OZG bestehende Organisationsstrukturen und ihre Mitarbeiter/innen überfordern können (Röhl/Engels 2025). Auch komplexe rechtliche Rahmenbedingungen und Rechtsunsicherheiten bremsen Digitalisierungsvorhaben und erschweren klare Entscheidungsprozesse (Röhl/Engels 2025). Aufgrund des langsamen Fortschritts der Verwaltungsdigitalisierung rücken politische Akteure das Thema gegenwärtig wieder stärker in den Fokus und versuchen bestehende Pfade zu verlassen. Institutionell zeigt sich das in der Schaffung des Bundesministeriums für Digitales und Staatsmodernisierung (BMDS), das eine koordinierende Rolle einnimmt und über ein eigenes Budget verfügt. Zudem werden adressatenorientierte, praxis- und digitaltaugliche Rechtsetzungen angestrebt, die die Transformationsprozesse beschleunigen sollen (BMDS 2025).

Auf kommunaler Ebene zeigen sich akteursbezogene Pfadabhängigkeiten durch Probleme bei der finanziellen Bewältigung notwendiger Digitalisierungsmaßnahmen (Marienfeldt et al. 2024), Personalengpässen sowie fehlender strategischer Planung und fehlendem professionellem Projektmanagement. Hinzu kommen Beharrungs- und Stagnationstendenzen aufseiten der politisch Verantwortlichen, die notwendige Reformprozesse verlangsamen oder blockieren können. Die Folge dieser Pfadabhängigkeiten auf kommunaler Ebene ist eine heterogene und oft ungleichmäßige Umsetzung der Verwaltungsdigitalisierung.

Pfadabhängigkeiten ergeben sich auch durch die Personalstrukturen der öffentlichen Verwaltungen. Der Fachkräftemangel und die fehlende Ausrichtung des Personalmanagements auf die Sicherung von digitalen Kompetenzen und Ressourcen bremsen die Verwaltungsdigitalisierung erheblich (Hammerschmid 2024). Darüber hinaus führen unzureichende Digitalkompetenzen und mangelndes Erfahrungswissen der Beschäftigten im Umgang mit Technologien dazu, dass der notwendige institutionelle Wandel besonders auf kommunaler Ebene ausbleibt. Auch die Ausbildungsstrukturen tragen zu akteursbezogenen Pfadabhängigkeiten bei: Digitalkompetenzen werden bisher unzureichend in der Ausbildung des Verwaltungsfachpersonals vermittelt und müssen meist später über Fort- und Weiterbildung erworben werden. Eine Anpassung der Ausbildungsverordnungen und Studienpläne erfolgte bisher nicht (Achleitner et al. 2024).

Ein Blick auf die Wissenschaft als Impulsgeber für die Modernisierung des Infrastruktursystems zeigt, dass bisher zu wenig anwendungs- und problemlösungsorientierte Forschung umgesetzt wurde, um zum Beispiel das Redesign von Verwaltungsprozessen besser zu verstehen. Gleichzeitig fehlen wissenschaftliche Untersuchungen, die als Grundlage für die Entwicklung gezielter und wirksamer Qualifizierungsangebote dienen und den Digitalisierungsprozess im Infrastruktursystem beschleunigen können (Rovner/Handke 2025).

Die Verwaltungsleistungen des Infrastruktursystems bleiben bei Nichterreichen des Digitalisierungsziels langsam, ineffizient und wenig nutzerorientiert, was die Erfüllung der staatlichen Kernaufgaben erschwert. Verzögerte oder unzureichende digitale Prozesse können zentrale öffentliche Leistungen beeinträchtigen (zum Beispiel Meldewesen, soziale Leistungen, Genehmigungsverfahren), zu einem ungleichen Zugang zu öffentlichen Leistungen und zu einer langsamen

Reaktionszeit des Staates führen. In der Folge kann das Vertrauen der Bürger/innen in staatliches Handeln weiter sinken, was soziale und politische Konflikte verstärken kann. Ein unzureichend digitalisiertes Infrastruktursystem kann besonders in Krisenzeiten die Aufrechterhaltung wesentlicher Funktionen staatlicher Leistungen nicht garantieren. Fragmentierte IT-Infrastrukturen und mangelnde digitale Resilienz können außerdem die Anfälligkeit des Infrastruktursystems für Cybersicherheitsrisiken und Datenverluste erhöhen.

Ökologische Nachhaltigkeit und Klimaneutralität

Das Infrastruktursystem Staat und Verwaltung ist hinsichtlich des Ziels, ökologisch nachhaltiger und klimaneutral zu werden, durch langfristige zeitliche Pfadabhängigkeiten gekennzeichnet. Zeitliche Pfadabhängigkeiten sind zunächst auf die eher langsame Schaffung rechtlicher Grundlagen und Klimaschutzkonzepte sowie die Planung von Umsetzungsmaßnahmen zur Erreichung der Klimaziele zurückzuführen. Die von der Bundesverwaltung bis 2030 angestrebte Klimaneutralität gilt beispielsweise nach Berechnungen des Bundesrechnungshofs von 2022 mit den vorgesehenen Maßnahmen als nicht erreichbar (KPMG 2023; Schuster/Klein 2023). Die angestrebte Vorbildfunktion des Bundes für andere Sektoren kann damit nicht erfüllt werden. Auf Landesebene zeigten sich in der Vergangenheit geringe Ambitionen einzelner Länder bei der Umsetzung der Klimaziele. 2023 wiesen nur zehn Bundesländer gesetzlich geregelte CO₂-Reduktionspfade auf (KPMG 2023). Erst seit 2025 verfügen nahezu alle Bundesländer über eigene Klimaschutzgesetze und konkrete Klimaschutzkonzepte, einschließlich Maßnahmenplanungen zur Erreichung klimaneutraler Landesverwaltungen (Haufe 2025).

Langfristige zeitliche Pfadabhängigkeiten des Infrastruktursystems ergeben sich darüber hinaus durch lang andauernde Bindungen an bestehende Infrastrukturinvestitionen. Gebäude, Verkehrs- und Energieinfrastrukturen sind auf jahrzehntelange Nutzungszeiträume ausgelegt und binden Verwaltungen an emissionsintensive Standards, die kurzfristig gar nicht oder nur mit hohen Kosten veränderbar sind. Außerdem werden zeitliche Pfadabhängigkeiten durch Beschaffungs- und Vergabestandards des Infrastruktursystems geprägt, die sich historisch an Kostenminimierung und Rechtssicherheit orientieren. Nachhaltige Zuschlagskriterien wie Lebenszykluskosten oder Klimawirkungen sind in öffentlichen Ausschreibungen noch nicht ausreichend verankert (Kozuch et al. 2024) (Kapitel 2.3).

Neben den zeitlich geprägten Pfadabhängigkeiten wirken auch akteursbezogene Pfade hemmend auf die ökologische und klimafreundliche Transformation des Infrastruktursystems. Eine unzureichende politische Priorisierung und Umsetzung konkreter Maßnahmen für eine treibhausgasneutrale Verwaltung sind auf allen Ebenen der öffentlichen Verwaltung zu beobachten. So kritisierte der Bundesrechnungshof 2023 beispielsweise den anhaltenden Trend zur Vergrößerung der Büroflächen der Bundesverwaltungen und die damit verbundenen steigenden Kosten und Treibhausgasemissionen durch den Strom- und Wärmeverbrauch (Tittelbach 2023). Die Umsetzung des Bundes-Klimaschutzgesetzes (KSG)¹¹ zeigt ressortübergreifend Herausforderungen in der strategischen Planung und Abstimmung. In mehreren Bundesministerien bestehen Defizite hinsichtlich kohärenter, langfristig ausgerichteter Strategien sowie einer ausreichenden Koordination der Maßnahmen zur Erreichung der Klimaziele. Besonders im Verkehrsressort werden

¹¹ Bundes-Klimaschutzgesetz vom 12. Dezember 2019, zuletzt am 15. Juli 2024 geändert

entsprechende Schwierigkeiten sichtbar. Laut Berichten an den Deutschen Bundestag (2025a) hat das Ressort seit 2019 keine ausreichenden Schritte unternommen, um die Vorgaben des KSG einzuhalten. Auch auf kommunaler Ebene müssen die bisherigen Aktivitäten als noch nicht ausreichend bewertet werden, da vielerorts noch grundlegende Beschlüsse zugunsten einer treibhausgasneutralen Kommunalverwaltung fehlen. In einer Kommunalbefragung des Umweltbundesamtes gaben nur 430 der 1.563 befragten Kommunen an, ein Neutralitätsziel für die kommunale Verwaltung festgelegt zu haben (UBA o. J.c).

Die Entwicklung gezielter Reduktionsmaßnahmen setzt voraus, dass die Treibhausgasemissionen der Verwaltung systematisch erfasst und gesteuert werden. Dass ein solches Monitoring bisher sowohl auf Bundes- als auch auf Landes- und kommunaler Ebene kaum etabliert ist, verweist auf akteursbezogene Pfadabhängigkeiten, insbesondere auf fehlende Verantwortungszuschreibungen, begrenzte Anreizstrukturen und eine geringe Priorisierung klimabezogener Steuerungsinstrumente (Schuster/Klein 2023). Dies erhöht die Unsicherheit für alle Akteure und erschwert zielgerichtete Investitionen in Maßnahmen, die nachgewiesene positive Effekte aufweisen. Die Bundesverwaltung erstellt zum Beispiel erst seit 2022 eine jährliche, behördenübergreifende Klimabilanz, um ihre Fortschritte messbar zu machen und gezielte Maßnahmen zur Reduktion der Treibhausgasemissionen zu entwickeln (BMWK o. J.). In der ersten Klimabilanz der Bundesregierung für die Bundesverwaltung werden zwar Fortschritte deutlich, etwa die Umstellung auf Ökostrom, aber auch Herausforderungen bei der Umstellung des Fuhrparks auf Elektrofahrzeuge (nur 4,5% der Fahrzeuge waren Ende 2022 rein elektrisch betrieben) sowie fehlende Zielmarken auf dem Weg zur Klimaneutralität (Bundesrechnungshof 2024; Pötter 2025).

Die verantwortlichen Akteure in den öffentlichen Verwaltungen sehen sich zum einen aufgrund fehlender finanzieller Mittel mit Herausforderungen bei der Realisierung von Klimaschutzmaßnahmen konfrontiert, was zu Umsetzungsdefiziten führt. Zum anderen sind auch Personalengpässe sowie begrenzte klima- und transformationsbezogene Kompetenzen der verantwortlichen Beschäftigten problematisch für die Umsetzung von Klimaschutzmaßnahmen und begünstigen akteursbezogene Pfadabhängigkeiten. Nachhaltigkeit und Klimaschutz werden häufig als Zusatzaufgaben behandelt, ohne dass ausreichende fachliche, ökonomische und systemische Kompetenzen systematisch aufgebaut werden. Darüber hinaus führen externe Entwicklungen, wie etwa der Fachkräftemangel in der Baubranche oder die steigenden Kosten für Bauleistungen, dazu, dass zentrale Bereiche, wie die Gebäudesanierung, nur langsam vorankommen (Schuster/Klein 2023).

Ein unzureichender Beitrag zur ökologischen Nachhaltigkeit und zum Klimaschutz schwächt die Fähigkeit von Staat und Verwaltung, langfristige gesellschaftliche Entwicklungen aktiv zu gestalten. Das Verfehlen der Treibhausgasneutralität durch staatliche Institutionen kann die gesetzlich festgelegte Vorbildwirkung der öffentlichen Hand beeinträchtigen und ein entsprechendes Reputationsrisiko mit sich bringen (KPMG 2023). Proteste gegen die staatliche Klimapolitik sind eine mögliche Folge und können die politische Polarisierung verstärken. Ein verzögerter Klimaschutz führt langfristig zu deutlich höheren Ausgaben für Schadensbewältigung, Anpassungsmaßnahmen sowie soziale Kompensationen. Unter anderem erhöht ein fortschreitender/ungebremselter Klimawandel das Risiko von Schäden an Gebäuden und Liegenschaften des Infrastruktursystems, etwa an Verwaltungsgebäuden und Schulen. Zudem können bei Nichterreichung verbindlicher Klimaziele zusätzliche Kosten für Straf- bzw. Kompensationszahlungen und rechtliche Verfahren entstehen. Diese zusätzlichen Belastungen können die finanziellen Engpässe im Infrastruktursystem weiter verschärfen.

4 Fokusthemen

Für eine vertiefende Untersuchung im Resilienz-Check schlagen wir zwei alternative Fokusthemen für das Infrastruktursystem Staat und Verwaltung vor. Die Auswahl erfolgte auf Grundlage zentraler Bewertungskriterien, wobei die Eignung für szenariobasierte Analysen eine besondere Rolle spielte. Diese wurde danach beurteilt, inwieweit ein Thema plausible, divergierende Zukunftsentwicklungen eröffnet und dabei zentrale Einflussfaktoren sowie ihre Wechselwirkungen und Unsicherheiten analytisch zugänglich macht. Ergänzend wurden die Technikfolgenrelevanz, der Bezug zu relevanten Trendclustern und Emerging Issues sowie der Beitrag zur Stärkung zentraler Systemeigenschaften (Anpassungsfähigkeit, Robustheit, Agilität) berücksichtigt. Die vorgeschlagenen Fokusthemen sind so gewählt, dass sie grundsätzlich auch für eine vertiefende Bearbeitung im Rahmen weiterer Formate des TAB geeignet sind.

4.1 Fokusthema 1: Autonome KI-Agenten in der Verwaltung als operative Infrastruktur

Vor dem Hintergrund der Entwicklungen, die in den Trendclustern „Digitale Transformation von Staat und Verwaltung“ sowie „Struktureller Wandel des öffentlichen Sektors“ beschrieben werden, gewinnen autonome KI-Agenten an strategischer Bedeutung (Kapitel 2.1 und 2.2). Sie eröffnen neue Möglichkeiten für die Weiterentwicklung der staatlichen Leistungserbringung und der internen Verwaltungsprozesse sowie für die Stärkung des Infrastruktursystems bei zunehmend begrenzten personellen Ressourcen (Kapitel 3.1 – Versorgungsengpässe). Erste Anwendungen zeigen bereits das Potenzial, komplexe Aufgaben zu automatisieren und Prozesse effizienter zu gestalten, etwa in Planungs- und Genehmigungsverfahren. Ihr breiter Einsatz und ihre systematische Integration in staatliche Strukturen stehen jedoch noch am Anfang. Gleichzeitig stellen KI-Agenten das System vor neue Herausforderungen, etwa bei der IT-Sicherheit, beim Datenschutz und bei Haftungsfragen, aber auch durch mögliche neue Abhängigkeiten von Technologieunternehmen und externen Dienstleistern, Kontrollverlust und intransparente Entscheidungswege.

Im Rahmen des Resilienz-Checks soll szenariobasiert analysiert werden, mit welchen Auswirkungen der Einsatz autonomer KI-Agenten auf die Prozesse, Leistungsfähigkeit und Organisation staatlicher Systeme verbunden ist und welches Potenzial besteht, die Resilienz des Infrastruktursystems Staat und Verwaltung zu stärken. Im Fokus steht die Entwicklung von Szenarien für eine operative Infrastruktur mit autonomen KI-Agenten unter unterschiedlichen technologischen, gesellschaftlichen und politisch-regulatorischen Bedingungen. Für die Szenarioentwicklung zentrale Einflussgrößen sind etwa der technologische Fortschritt bei autonomen KI-Agenten, die regulatorischen Rahmenbedingungen für KI oder der Fachkräftemangel im IT-Bereich. Untersucht werden die operative Leistungsfähigkeit von autonomen KI-Agenten, die notwendigen Anpassungen in den Verwaltungsorganisationen sowie die erforderlichen Kompetenzen und Governancemaßnahmen für den Einsatz autonomer KI-Agenten in Verwaltungsprozessen. Ziel ist es, auf dieser Grundlage ein systematisches Verständnis für die zukünftigen Rollen autonomer KI-Agenten im Infrastruktursystem Staat und Verwaltung zu entwickeln. Dabei werden Risiken, Zielkonflikte und Gestaltungsspielräume systematisch analysiert und darauf aufbauend Handlungsoptionen

entwickelt, um den Einsatz autonomer KI-Agenten strategisch zu gestalten und ihre Integration in staatliche Strukturen langfristig zu unterstützen.

4.2 Fokusthema 2: Verlässlichkeit staatlicher Information im Kontext synthetisch erzeugter Medien

Im Trendcluster „Wandel im Verhältnis von Staat und Zivilgesellschaft“ sowie in der Analyse des systemischen Risikos „Desinformation“ zeigt sich, dass die digitale Transformation die Interaktion zwischen staatlichen Akteuren und Bürger/innen grundlegend verändert und zugleich neue Manipulations- und Angriffsflächen schafft (Kapitel 2.4 und 3.1 – Desinformation). Ein wesentlicher Treiber dieser Entwicklung bildet die zunehmende Verbreitung KI-basierter, synthetischer Medien (zum Beispiel virtuelle Avatare oder Deepfakes), die die Erstellung täuschend echter Inhalte erleichtern. Mit sinkenden technischen Hürden wird die Verbreitung von Desinformationen erleichtert und durch Plattformlogiken weiter verstärkt. Neben kognitiven Verzerrungen nutzen automatisierte Accounts (Bots) Social-Media-Algorithmen aus und fördern so die schnelle Verbreitung und wahrgenommene Glaubwürdigkeit von Desinformationen. Für Staat und Verwaltung entstehen daraus neue Verwundbarkeiten im Austausch mit Bürger/innen, Unternehmen und anderen staatlichen Einrichtungen. Gefälschte behördliche Inhalte können Vertrauen ausnutzen, etwa durch manipulierte Videos vermeintlicher Amtsträger zum Beispiel mit falschen Evakuierungsanordnungen oder durch irreführende Angaben zu Antragsfristen und Förderbedingungen. Gleichzeitig kann auch die Kommunikation selbst verzerrt werden, etwa durch koordinierte Kampagnen oder automatisierte Interaktionen, die ein falsches Meinungsbild erzeugen. Die Verbreitung synthetischer Medien kann dazu führen, dass auch authentische Informationen vermehrt angezweifelt werden. Staatliche Kommunikation bewegt sich damit zunehmend im Spannungsfeld zwischen erhöhter Reichweite und Geschwindigkeit einerseits sowie wachsender Anfälligkeit für Manipulation andererseits. Die Verlässlichkeit staatlicher Information wird damit zu einer zentralen Voraussetzung für wirksames staatliches Handeln, Vertrauen und die Resilienz von Staat und Verwaltung. Dies gilt insbesondere vor dem Hintergrund steigender Erwartungen an staatliche Responsivität bei gleichzeitig begrenzten personellen Ressourcen in Verwaltungen (Kapitel 3.1 – Versorgungsengpässe).

Im Rahmen des Resilienz-Checks soll szenariobasiert analysiert werden, wie sich synthetische Medien und KI-basierte Kommunikationsdynamiken auf die Funktionsfähigkeit und Legitimität von Staat und Verwaltung auswirken. Im Fokus steht die Entwicklung von Szenarien für digital geprägte Informations- und Kommunikationsräume unter unterschiedlichen technologischen, gesellschaftlichen und politisch-regulatorischen Bedingungen. Für die Szenarioentwicklung zentrale Einflussgrößen sind etwa technologische Fortschritte bei generativer KI, gesellschaftliche Vertrauensniveaus und Medienkompetenz sowie politische und rechtliche Leitplanken im Umgang mit Desinformation. Untersucht werden die Wechselwirkungen zwischen technologischen Infrastrukturen und Plattformarchitekturen, institutionellen Strukturen und der Governance staatlicher Kommunikation sowie gesellschaftlichen Vertrauensdynamiken und normativen Ordnungsrahmen. Ziel ist es, Risiken, Zielkonflikte und Gestaltungsspielräume systematisch zu analysieren und darauf aufbauend Handlungsoptionen zu entwickeln, um die Dialogfähigkeit und Informationsintegrität zu stärken und die Funktionsfähigkeit von Staat und Verwaltung langfristig zu sichern.

5 Methodik und Vorgehen

Das Resilienz-Radar ist ein Baustein unserer erweiterten Foresightaktivitäten. Es soll als kontinuierliche Beratungsleistung den Deutschen Bundestag dabei unterstützen, kritische Infrastruktursysteme zukunftsfähig und resilient zu machen.

Weitere Informationen zum Resilienz-Radar und Resilienz-Check sowie die Ergebnisse zu den bereits behandelten Infrastruktursystemen finden Sie auf unserer Microsite „Foresight für das Parlament“.

Dem Resilienz-Radar liegt eine explizit soziotechnische Definition von kritischen Infrastruktursystemen zugrunde. Wir verstehen darunter Einrichtungen, Anlagen, Strukturen und Systeme, die für das reibungslose Funktionieren der Gesellschaft von zentraler Bedeutung sind. Sie umfassen nicht nur physische und technologische Komponenten, sondern auch ökonomische, soziale, politische, organisatorische und kulturelle Elemente, die mit der Entwicklung, Nutzung und Wartung von Infrastruktur in Verbindung stehen. Dieses Verständnis ist auch von entscheidender Bedeutung für die Resilienzgestaltung. Um Resilienz zu erreichen, ist es erforderlich, die soziotechnischen Rahmenbedingungen, aber auch Pfadabhängigkeiten ganzheitlich zu betrachten.

Der Fokus des Resilienz-Radars liegt auf aktuellen Trends, die das jeweilige Infrastruktursystem prägen, sowie spezifischer Gefährdungslagen durch systemische Risiken. Systemische Risiken können Gesellschaften oder Wirtschaftssysteme als Ganzes gefährden und beinhalten damit grundsätzlich auch die Gefahr, dass Funktionsfähigkeit und Stabilität von Infrastruktursystemen erheblich beeinträchtigt werden, wenn sich diese Risiken verwirklichen. Die Umsetzung des Resilienz-Radars erfolgt in aufeinander aufbauenden Arbeitsphasen. In allen Phasen wird die Expertise von Fachleuten einbezogen.

In der ersten Phase werden vor allem Foresight- und TA-Studien im Umfeld der ausgewählten Infrastruktursysteme erfasst und analysiert. Hierbei werden insbesondere mittel- bis langfristige Trends identifiziert, die nachweisbare Auswirkungen auf die Infrastruktursysteme haben. Ergänzend werden relevante wissenschaftliche Quellen zur Analyse von systemischen Risiken ausgewertet. Die Identifikation aufkommender soziotechnischer Trends erfolgt zusätzlich durch den Einsatz von Software- und KI-Technologien. Zum einen wird der eigens für das Resilienz-Radar aufgebaute Quellenpool genutzt, der einschlägige Datenbanken (zum Beispiel EPTA, ORBIS, Knowledge4Policy, OpenTA), Publikationen (Foresightstudien, Trendberichte, Konferenzsammlbände und Preprints), wissenschaftliche Plattformen (zum Beispiel ScienceDaily) sowie journalistischen Hintergrundanalysen (Tagesspiegel Background, Heise online) umfasst. Zum anderen werden Internetquellen (Blogs, Beiträge auf sozialen Medien, Nachrichten) mithilfe einer Medienmonitoringsoftware und von Topic Modeling analysiert.

In der zweiten Phase werden Einzel- und Gruppeninterviews mit ausgewählten Expert/innen durchgeführt, um deren Fachwissen, Einschätzungen und Meinungen zu wesentlichen Trends und Herausforderungen sowie zu Wirkungszusammenhängen im Kontext systemischer Risiken für die Infrastruktursysteme zu erfassen. Die Antworten der Befragten sowie weitere Kommentare, Hinweise und detaillierte Ausführungen werden protokolliert und die Ergebnisse anschließend qualitativ ausgewertet. Nach Bedarf wird unter ausgewählten Expert/innen eine explorative Onlineerhebung durchgeführt, in der auf Grundlage der vorangegangenen Schritte Trends ausgewählt und hinsichtlich ihrer Auswirkungen auf die Verletzlichkeit und Resilienz des genannten Infrastruktursystems bewertet werden. Die Resultate aller Arbeitsphasen werden abschließend integrativ analysiert und in den Foresight-Reports zusammengefasst.

Beteiligte Expert/innen:

- Liz Wehmeier, Universität Potsdam, wissenschaftliche Mitarbeiterin an der Professur für Politikwissenschaft, Verwaltung und Organisation
- Dr. Esther Görnemann, Weizenbaum-Institut e.V., Wissenschaftliche Referentin Forschungssynthesen
- Philipp Hofer, Universität Stuttgart, Betriebswirtschaftliches Institut, akademischer Mitarbeiter
- Dr. Julia Pohle, WZB Berlin Social Science Center, Co-Leader und Senior Researcher – Politics of Digitalization
- Prof. Dr. Birgit Schenk, Hochschule für öffentliche Verwaltung und Finanzen Ludwigsburg, Leiterin Institut für Digitale Transformation im öffentlichen Sektor

6 Literatur

- Achleitner, A.-K. et al. (2024): Innovationssystem Deutschland. Effizienz und Agilität der öffentlichen Verwaltung erhöhen. acatech – Deutsche Akademie der Technikwissenschaften, Berlin, https://doi.org/10.48669/ACA_2024-10
- Amos, M. (2025): Anwalt blamiert sich vor Gericht. Heute im Recht, <https://rsw.beck.de/aktuell/daily/meldung/detail/ag-koeln-312f13025-ki-schriftsatz-anwalt-halluzinationen-berufsrecht> (21.4.2026)
- Andhov, M. et al. (2025): Leveraging AI for sustainable public procurement. Opportunities and challenges. In: *Frontiers in Sustainability* 6, <https://doi.org/10.3389/frsus.2025.1603214>
- Bär, H.; Wilkens, M. (2023): Was uns Extremwetter bereits heute kostet und wie wir Klimaschutz und öffentliche Finanzen zusammendenken. Bertelsmann Stiftung, <https://www.zukunftdernachhaltigkeit.de/2023/04/27/was-uns-extremwetter-bereits-heute-kostet/> (13.11.2025)
- BBK (2026): KRITIS-Sektor: Staat und Verwaltung. Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, https://www.bbk.bund.de/DE/Themen/Kritische-Infrastrukturen/Sektoren/Branchen/Staat-Verwaltung/staat-verwaltung_node.html (21.4.2026)
- Bernardini, C. et al. (2025): Climate proofing of public procurement: a gap to be filled. In: *npj Climate Action* 4(1), Art. 2, <https://doi.org/10.1038/s44168-024-00207-0>
- Beschaffungsamt des BMI (2025): Nationale Kreislaufwirtschaftsstrategie sucht Expertinnen und Experten. https://www.nachhaltige-beschaffung.info/SharedDocs/Kurzmeldungen/DE/2025/250407_Aufruf_NKWS.html (13.11.2025)
- Bitkom e. V. (2025a): Bitkom-Analyse. 60 Prozent der Verwaltungsleistungen sind online verfügbar. <https://www.bitkom.org/Presse/Presseinformation/Bitkom-Analyse-60-Prozent-der-Verwaltungsleistungen-sind-online-verfuegbar> (21.4.2026)
- Bitkom e. V. (2025b): Digitalisierung: Deutschland im EU-Vergleich auf Platz 14. <https://www.bitkom.org/Presse/Presseinformation/Digitalisierung-Deutschland-EU-Vergleich-Platz-14> (11.12.2025)
- Bitkom e. V. (2025c): Smart City Index 2025. Ausführliche Ergebnisse. Berlin
- BKA (2025): Politisch motivierte Kriminalität: Höchster Anstieg seit Beginn der Erfassung. Bundeskriminalamt, https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/PMK/PMKZahlen2024/PMKZahlen2024_node.html (5.1.2026)
- BMDS (2024): Digitale Souveränität in der öffentlichen Verwaltung. Selbstbestimmt und handlungsfähig in die Zukunft. Bundesministerium für Digitales und Staatsmodernisierung, <https://bmds.bund.de/themen/digitale-souveraenitaet/digitale-souveraenitaet-in-der-oeffentlichen-verwaltung> (4.3.2026)
- BMDS (2025): Modernisierungsagenda – für Staat und Verwaltung (Bund). Für ein schnelles, digitales und handlungsfähiges Deutschland. Bundesministerium für Digitales und Staatsmodernisierung, Berlin
- BMF (2023): Sollbericht 2023: Ausgaben und Einnahmen des Bundeshaushalts. Bundesministerium für Finanzen, Berlin
- BMF (2025): Vorläufiger Abschluss des Bundeshaushalts 2024. Bundesministerium der Finanzen, <https://www.bundesfinanzministerium.de/Monatsberichte/Ausgabe/2025/01/Inhalte/Kapitel-3-Analysen/3-1-vorlaeufiger-abschluss-bundeshaushalt-2024.html> (12.12.2025)

- BMUKN (Hg.) (2024): Deutsche Anpassungsstrategie an den Klimawandel 2024. Vorsorge gemeinsam gestalten. Bundesministerium für Umwelt, Klimaschutz, Naturschutz und nukleare Sicherheit, Berlin
- BMWE (2026): Deutschland gewinnt internationalen KI-Preis - Neue KI-Plattform beschleunigt Genehmigungsverfahren. Bundesministerium für Wirtschaft und Energie, <https://www.bundeswirtschaftsministerium.de/Redaktion/DE/Pressemitteilungen/2026/02/20260204-deutschland-gewinnt-internationalen-ki-preis.html> (10.2.2026)
- BMWE (o. J.): IPCEI Nächste Generation Cloud Infrastrukturen und Services. Europa gemeinsam auf dem Weg zur Cloudinfrastruktur der Zukunft. Bundesministerium für Wirtschaft und Energie, <https://www.bundeswirtschaftsministerium.de/Redaktion/EN/Artikel/Industry/ipcei-cis.html> (16.6.2026)
- BMWK (o. J.): Klimabilanz der Bundesverwaltung 2022. Bundesministerium für Wirtschaft und Klimaschutz, https://www.bundeswirtschaftsministerium.de/Redaktion/DE/Downloads/J-L/klimabilanz-der-bundesverwaltung-2022.pdf?__blob=publicationFile&v=1 (24.7.2026)
- Böhnke, P. et al. (2023): Folgen sozialer Ungleichheit. Bundeszentrale für politische Bildung, <https://www.bpb.de/shop/zeitschriften/izpb/soziale-ungleichheit-354/520847/folgen-sozialer-ungleichheit/> (24.3.2026)
- bpb (2023a): Öffentliche Ausgaben nach Aufgabenbereichen. Bundeszentrale für politische Bildung, <https://www.bpb.de/kurz-knapp/zahlen-und-fakten/soziale-situation-in-deutschland/61871/oeffentliche-ausgaben-nach-aufgabenbereichen/> (28.7.2025)
- bpb (2023b): Sozialbudget. Bundeszentrale für politische Bildung, <https://www.bpb.de/kurz-knapp/zahlen-und-fakten/soziale-situation-in-deutschland/61890/sozialbudget/> (12.12.2025)
- Brettschneider, F. (2025): Demokratie-Monitor 2025. Universität Hohenheim, Stuttgart
- Breuer, C. (2025): Kriegstüchtige Streitkräfte und eine wehrhafte Gesellschaft sind zwei Seiten einer Medaille. In: ifo Schnelldienst 78(2), S. 3–6
- BSI (2024): Die Lage der IT-Sicherheit in Deutschland 2024. Bundesamt für Sicherheit in der Informationstechnik, Bonn
- BSI (2025a): Die Lage der IT-Sicherheit in Deutschland 2025. Bundesamt für Sicherheit in der Informationstechnik, Bonn
- BSI (2025b): Positionspapier. Cybersicherheit im Energiesektor Deutschlands. Bundesamt für Sicherheit in der Informationstechnik, Bonn
- BSI (2025c): Technischer Fehler bei AWS und Azure sorgt weltweit für Internet-Störungen. Bundesamt für Sicherheit in der Informationstechnik, https://www.bsi.bund.de/DE/Service-Navi/Abonnements/Newsletter/Buerger-CERT-Abos/Newsletter-Einfach-Cybersicher/Einfach_Cybersicher_251105/_documents/News-Update_2_AWS-Stoerung.html (24.7.2026)
- Bundesdruckerei (o. J.): Das Once-Only-Prinzip. <https://www.bundesdruckerei-gmbh.de/de/innovation-hub/once-only-prinzip> (16.6.2026)
- Bundesnetzagentur (2025): Droht der Black-out? Über die Stromversorgung in Deutschland. https://www.bundesnetzagentur.de/DE/Allgemeines/DieBundesnetzagentur/Insight/Texte/Energiewende/Blog17_Energiewende_Blackout.html (24.7.2026)
- Bundesrechnungshof (2022): Bericht nach § 88 Absatz 2 BHO an den Haushaltsausschuss des Deutschen Bundestages über die Grundbedingungen zur Sicherung nachhaltiger Staatsfinanzen. o. O.
- Bundesrechnungshof (2024): Bericht nach § 88 Absatz 2 BHO an das Bundeskanzleramt: Energieeffizienz des Fuhrparks der Bundesverwaltung. o. O.

- Bundesregierung (2023): Integrierte Sicherheit für Deutschland. Nationale Sicherheitsstrategie. Berlin
- Bundesregierung (2024): Soziales Netzwerk TikTok. Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion der CDU/CSU – Drucksache 20/12548 –. Deutscher Bundestag, Drucksache 20/12872, Berlin
- Bundesregierung (2025a): Auswirkungen von Cyberangriffen auf die Sicherheit und die Wirtschaft von Deutschland. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Manuel Höferlin, Maximilian Funke-Kaiser, Konstantin Kuhle, weiterer Abgeordneter und der Fraktion der FDP – Drucksache 20/14372 –. Deutscher Bundestag, Drucksache 20/14532, Berlin
- Bundesregierung (2025b): Besprechung des Bundeskanzlers mit den Regierungschefinnen und Regierungschefs der Länder am 4. Dezember 2025. Berlin
- Bundesregierung (2025c): Bundesregierung startet digitales Bürokratiemeldeportal. <https://www.bundesregierung.de/breg-de/aktuelles/einfach-machen-portal-2399358> (25.2.2026)
- Bundesregierung (2025d): Modernisierungsagenda für Staat und Verwaltung (Bund). Für ein schnelles, digitales und handlungsfähiges Deutschland. Berlin
- Bundesregierung (o. J.): Stromausfall – Was ist ein Blackout? <https://www.bundesregierung.de/breg-de/aktuelles/stromausfall-blackout-2129818> (24.7.2026)
- dbb (2025a): Monitor öffentlicher Dienst 2025. dbb beamtenbund und tarifunion, Berlin
- dbb (2025b): Personalmangel im öffentlichen Dienst. dbb beamtenbund und tarifunion, Berlin
- Decker, O. et al. (Hg.) (2024): Vereint im Ressentiment: Autoritäre Dynamiken und rechtsextreme Einstellungen. Gießen
- Demografieportal (o. J.a): Altersstruktur im öffentlichen Dienst. <https://www.demografie-portal.de/DE/Fakten/oeffentlicher-dienst-altersstruktur.html> (24.7.2026)
- Demografieportal (o. J.b): Beschäftigte im öffentlichen Dienst. <https://www.demografie-portal.de/DE/Fakten/oeffentlicher-dienst.html> (16.6.2026)
- Destatis (2025a): Integrierte kommunale Schulden steigen im Jahr 2024 um 6,3%. Statistisches Bundesamt, https://www.destatis.de/DE/Presse/Pressemitteilungen/2025/12/PD25_430_713.html (12.12.2025)
- Destatis (2025b): Öffentlicher Dienst 2024: Mehr Beschäftigte für Bildung und Kinderbetreuung. Statistisches Bundesamt, https://www.destatis.de/DE/Presse/Pressemitteilungen/2025/06/PD25_212_741.html (14.11.2025)
- Destatis (o. J.): Indikator 12.3a, b, c Nachhaltige Beschaffung. Statistisches Bundesamt, <https://dns-indikatoren.de/12-3-abc/> (16.6.2026)
- Deutscher Bundestag (2024): Haushalt 2025. KTF-Ausgaben schrumpfen. <https://www.bundestag.de/presse/hib/kurzmeldungen-1015396> (16.12.2025)
- Deutscher Bundestag (2025): Schriftliche Fragen mit den in der Woche vom 16. Juni 2025 eingegangenen Antworten der Bundesregierung. Drucksache 21/512, Berlin
- Deutscher Richterbund (2025): E-Akte: 15 von 16 Ländern wollen bis Jahresende fertig sein. <https://www.drj.de/newsroom/presse-mediencenter/nachrichten-auf-einen-blick/nachricht/news/e-akte-15-von-16-laendern-wollen-bis-jahresende-fertig-sein> (11.12.2025)
- DHPol (2024): MEGAVO-Studie. Projektbericht 2021–2024. Deutsche Hochschule der Polizei, Münster
- DIHK (2024): Weiterhin langsamer Mittelabfluss beim Klima- und Transformationsfonds. Deutsche Industrie- und Handelskammer, <https://www.dihk.de/de/themen-und-positionen/weiterhin-langsamer-mittelabfluss-beim-klima-und-transformationsfonds-116330> (16.12.2025)

- dpa (2020): Coronavirus-Krise: Thüringer Kommunen laufen auf Sparflamme. Süddeutsche Zeitung, <https://www.sueddeutsche.de/politik/erfurt-coronavirus-krise-thueringer-kommunen-laufen-auf-sparflamme-dpa.urn-newsml-dpa-com-20090101-200327-99-490573> (25.3.2026)
- dpa (2024a): Auswärtiges Amt bestellt russischen Diplomaten ein. ntv, <https://www.n-tv.de/politik/Auswaertiges-Amt-bestellt-russischen-Diplomaten-ein-article24918491.html> (4.3.2026)
- dpa (2024b): Berlin bestellt chinesischen Botschafter ein. zdfheute, <https://www.zdfheute.de/politik/china-botschafter-cyberattacke-deutschland-auswaertiges-amt-100.html> (4.3.2026)
- Edelman Trust Institute (2025): 2025 Edelman Trust Barometer. https://www.edelman.com/sites/g/files/aatuss191/files/2025-01/2025%20Edelman%20Trust%20Barometer%20Global%20Report_01.23.25.pdf (29.7.2026)
- EEA (2025): Economic losses from weather- and climate-related extremes in Europe. European Environmental Agency, <https://www.eea.europa.eu/en/analysis/indicators/economic-losses-from-climate-related> (13.11.2025)
- Fischer, S. (2024): In der Echokammer. Freiheit in den sozialen Medien ist eine Illusion. Algorithmen geben vor, welche Inhalte die Nutzer und Nutzerinnen lesen. Max-Planck-Gesellschaft, <https://www.mpg.de/21730745/soziale-netzwerke-echokammern> (29.7.2026)
- forsa (2025a): dbb Bürgerbefragung Öffentlicher Dienst. Einschätzungen, Erfahrungen und Erwartungen der Bürger. forsa Gesellschaft für Sozialforschung und statistische Analysen mbH, Berlin
- forsa (2025b): Gewalt gegen öffentlich Beschäftigte. dbb Bürgerbefragung Öffentlicher Dienst. forsa Gesellschaft für Sozialforschung und statistische Analysen mbH, Berlin
- Freier, R. et al. (2025): Kommunalen Finanzreport 2025. Knappe Kassen, große Aufgaben. Bertelsmann Stiftung, Gütersloh
- Gabel, R.; Potthoff, J. (2025): Vertrauenskrise in Deutschland? Ein europäischer Vergleich und Wege zu neuer Stabilität. Institut der deutschen Wirtschaft, Policy Paper 9, Köln
- GdP (2025): Husgen: Wir Polizisten müssen oftmals aus Scheiße Bonbons machen. Gewerkschaft der Polizei, <https://www.gdp.de/bund/de/stories/2025/08/wir-polizisten-muessen-oftmals-aus-scheisse-bonbons-machen> (13.8.2025)
- GdP MV (2025): Stellungnahme der Gewerkschaft der Polizei Mecklenburg-Vorpommern an den Innenausschuss des Landtages Mecklenburg-Vorpommern zur personellen und materiellen Lage der Landespolizei und den haushaltspolitischen Planungen 2026/2027. Gewerkschaft der Polizei Mecklenburg-Vorpommern, https://www.gdp.de/Mecklenburg-Vorpommern/Stories/2025/Aktuelle%20Stories/Tarif/Stellungnahme%20der%20GdP%20zur%20personellen%20und%20materiellen%20Lage%20der%20Landespolizei%20und%20den%20haushaltspolitischen%20Planungen%202026_2027.pdf (20.1.2026)
- Gerber, M. (2025): Die Betriebe mussten in den letzten drei Jahren 325.000 Arbeitskräfte zusätzlich einstellen, um die gewachsene Bürokratie zu bewältigen. IAB-Forum, <https://iab-forum.de/die-betriebe-mussten-in-den-letzten-drei-jahren-325-000-arbeitskraefte-zusaetzlich-einstellen-um-die-gewachsene-buerokratie-zu-bewaeltigen/> (17.12.2025)
- Glaser, R. (2025): Klimadämmerung. Klimawandel und Gesellschaft in Mitteleuropa seit 1800 – Entwicklungen, Folgen und Perspektiven. Berlin, https://doi.org/10.1007/978-3-662-71402-7_1
- Gräfe, P. et al. (2024): Verwaltungsdigitalisierung in Deutschland. Effekte auf die Vollzugsebene und Lehren für die Praxis. Hans-Böckler-Stiftung, Working Paper 346, Düsseldorf
- Hammerschmid, G. (2024): Zukunftsfähiges Personalmanagement in Zeiten der Digitalisierung: Was jetzt wichtig ist. In: PublicGovernance Winter 2023/2024, S. 6–12

- Hartmann, B. (2025): Bürokratieabbau per KI: Wie Bilder den Staat beschleunigen. Berliner Morgenpost, <https://www.morgenpost.de/wirtschaft/article410161464/buerokratieabbau-per-ki-wie-bilder-den-staat-beschleunigen.html> (24.2.2026)
- Haufe (2025): Klimaschutzgesetze der Bundesländer im Überblick. https://www.haufe.de/immobilien/wirtschaft-politik/klimaschutzgesetze-der-bundeslaender_84342_569462.html (1.5.2026)
- Heinrich Böll Stiftung (o.J.): Cyberangriff auf die Südwestfalen-IT 2023. KommunalWiki, https://kommunalwiki.boell.de/index.php/Cyberangriff_auf_die_Südwestfalen-IT_2023 (4.3.2026)
- Hensiek, J. (2025): Stadtverwaltung Lübeck: Personallücke durch Bots schließen. Haufe, https://www.haufe.de/oeffentlicher-dienst/digitalisierung-transformation/personalluecke-durch-bots-schliessen_524786_645562.html (7.8.2025)
- Hentze, T.; Kauder, B. (2024): Öffentlicher Dienst. Mehr Personal, noch mehr Bedarf. Institut der deutschen Wirtschaft, Kurzbericht 2/2024, Köln
- Hermann, F. et al. (2024): Automatisierte, BIM-basierte Ökobilanzierung am Beispiel des Infrastrukturbaus. In: Bautechnik 101(2), S. 128–133, <https://doi.org/10.1002/bate.202300115>
- Hildebrandt, A.; Lemaitre, C. (2025): Klimawandel in Städten und Kommunen: Prognosen – Herausforderungen – Chancen und Maßnahmen. In: Hildebrandt, A. et al. (Hg.): Zukunft Stadt: Die globale und lokale Bedeutung von SDG 11. SDG – Forschung, Konzepte, Lösungsansätze zur Nachhaltigkeit, Berlin, S. 57–92, https://doi.org/10.1007/978-3-662-70008-2_3
- Hubbard, S.; Goux, D. (2026): The Ecosystem of Deliberative Technologies for Public Input. Ash Center, <https://ash.harvard.edu/resources/the-ecosystem-of-deliberative-technologies-for-public-input/> (25.2.2026)
- Hüster, J. (2026): Bedroht im Amt. Tagesschau, <https://www.tagesschau.de/inland/innenpolitik/angriffe-kommunalpolitiker-kommunalwahlen-100.html> (24.3.2026)
- Hüther, M. (2025): Im Wettstreit der großen Mächte. Geopolitik dominiert Geoökonomie. In: ifo Schnelldienst 78(2), S. 17–20
- ifo Institut (2024): Entgangene Wirtschaftsleistung durch hohen Bürokratieaufwand. München
- Initiative D21 e. V.; TU München (2023): eGovernment MONITOR 2023. Berlin
- Initiative D21 e. V.; TU München (2024): eGovernment MONITOR 2024. Berlin
- INSM (o.J.): Digitale Transformation: Deutschland scheitert beim E-Government. Stand 9.4.2025. Initiative Neue Soziale Marktwirtschaft, <https://insm.de/aktuelles/publikationen/digitale-transformation-deutschland-scheitert-beim-e-government> (23.7.2025)
- Islam, S. et al. (2024): Bridging Data Standards and FAIR Principles in Biodiversity Digital Twinning: Prototyping, Challenges, Lessons Learned, and Future Plans. In: Biodiversity Information Science and Standards 8, Art. e133089, <https://doi.org/10.3897/biss.8.133089>
- Islam, S. et al. (2026): FAIR digital twins for biodiversity: enabling data, model, and workflow integration. In: npj Biodiversity 5(1), Art. 5, <https://doi.org/10.1038/s44185-025-00116-3>
- ITZBund (o.J.): Die E-Akte Bund – für die moderne Verwaltung. Informationstechnikzentrum Bund, <http://www.itzbund.de/DE/itloesungen/egovernment/eakte/eakte.html?nn=178942> (23.7.2025)
- Jahnke, N.; Niehoff, N. (2024): Datenwirtschaft und Edge-Computing. Potenziale, Herausforderungen und Handlungsempfehlungen. Fraunhofer-Institut für Software- und Systemtechnik, Dortmund
- Kairies-Lamp, N.; Steinkraus, M.-S. (2021): Verwaltung in Krisenzeiten – Auswirkungen der Pandemie auf den öffentlichen Dienst. In: PublicGovernance Frühjahr 2021, S. 12–15

- Karpenstein, S. (2025): Cybersecurity in Kommunen. Zwischen Gefahrenlage und Realität. eGovernment, <https://www.egovernment.de/cybersecurity-in-kommunen-zwischen-gefahrenlage-und-realitaet-a-54122fba111a088b989af489e2a3d5e2/> (1.5.2026)
- Karpenstein, U.; Kirschnick, S. (2024): Offene Flanken der Brandenburger Justiz. Verfassungsblog, <https://doi.org/10.59704/b86c3c0534d507b3>
- Kellermann, S.; Labudde, D. (2024): Deepfakes als Beweismittel. Zur Notwendigkeit der Authentizitätsprüfung von Bild-, Audio- und Videodaten. Das digitale Rig als Authentifizierungsmethode zur Erkennung von synthetischen Bild- und Videodaten. In: Klein, M. et al.: Informatik 2024. Gesellschaft für Informatik e. V., S. 295–307, https://doi.org/10.18420/INF2024_20
- KfW (2025): Wahrgenommener Investitionsrückstand der Kommunen bis 2024. Statista, <https://de.statista.com/statistik/daten/studie/1172001/umfrage/kommunaler-investitionsrueckstand/> (28.7.2025)
- KfW; difu (2025): KfW-Kommunalpanel 2025. Kreditanstalt für Wiederaufbau; deutsches Institut für Urbanistik, o. O.
- Kipker, D.-K.; Kalain, M. (2026): Bund zahlt in einem Jahr 500 Millionen Euro für Microsoft-Lizenzen. heise online, <https://www.heise.de/hintergrund/Microsoft-Abhaengigkeit-Bund-zahlt-in-einem-Jahr-fast-500-Millionen-Euro-11170931.html> (17.3.2026)
- Koç, H. et al. (2021): Robotic Process Automation und Digitale Service-Transformation bei der DRV. In: HMD Praxis der Wirtschaftsinformatik 58(5), S. 1230–1243, <https://doi.org/10.1365/s40702-021-00760-w>
- Kohlrausch, B. (2023): Fast die Hälfte der Erwerbspersonen macht sich große Sorgen um sozialen Zusammenhalt der Gesellschaft. Wirtschafts- und Sozialwissenschaftliches Institut, Düsseldorf
- Kolodko, G. W. (2025): Geopolitische Neuordnung. In: Trumps zweite Amtszeit. Cham, S. 47–53, https://doi.org/10.1007/978-3-032-02943-0_6
- Kompetenzzentrum Öffentliche IT et al. (2025): ThemenRadar 2025. Digitalthemen in der öffentlichen Verwaltung 2025. Berlin
- Körper-Stiftung (2025): Demokratie in der Krise 2025. <https://koerber-stiftung.de/projekte/demokratie-in-der-krise/umfrage-2025/> (16.12.2025)
- Kozuch, A. et al. (2024a): Besondere Herausforderungen bei der Implementierung nachhaltiger Beschaffung im öffentlichen Sektor. In: Fröhlich, E.; Jamal, Y. (Hg.): CSR und Beschaffung. Management-Reihe Corporate Social Responsibility, Berlin, S. 221–242, https://doi.org/10.1007/978-3-662-67858-9_9
- Kozuch, A. et al. (2024b): Nachhaltigkeit in der öffentlichen Beschaffung. Bertelsmann Stiftung, Focus Paper 23, Gütersloh, <https://doi.org/10.11586/2024096>
- KPMG (2023): Klimaschutz im öffentlichen Sektor – warum Handlungsbedarf besteht. KPMG AG Wirtschaftsprüfungsgesellschaft, Berlin
- Kühl, C.; Scheller, H. (2025): Kommunale Klimaschutzfinanzierung auf neue Füße stellen: Einführung einer neuen Gemeinschaftsaufgabe. Deutsches Institut für Urbanistik, Policy Papers 4, Berlin, <https://doi.org/10.34744/DIFU-POLICY-PAPERS-2025-4>
- Kunz, M. (2025): Serielles Clustering von Extremwetterereignissen in Mitteleuropa. Institut für Meteorologie und Klimaforschung Troposphärenforschung, https://www.imk-tro.kit.edu/14_11203.php (11.12.2025)
- Lush, V. et al. (2024): Assessing FAIRness of citizen science data in the context of the Green Deal Data Space. In: International Journal of Digital Earth 17(1), Art. 2344587, <https://doi.org/10.1080/17538947.2024.2344587>

- Marienfeldt, J. et al. (2024): Digitalisierung in Kommunen. Wo bleibt der erhoffte Durchbruch? Deutsche Vereinigung für Politikwissenschaft, <https://www.dvpw.de/blog/digitalisierung-in-kommunen-wo-bleibt-der-erhoffte-durchbruch-ein-beitrag-von-justine-marienfeldt-jakob-kuehler-sabine-kuhlmann-und-isabella-proeller#:~:text=Einerseits%20müs-sen%20und%20können%20sie%20aufgrund%20ihrer,jedoch%20mit%20begrenzten%20Res-sourcen%20parallel%20zum%20Tagesgeschehen> (20.1.2026)
- McKinney, J.; Tarnay, V. (2024): Using AI for green procurement. Open Contracting Partnership, <https://www.open-contracting.org/2024/08/30/using-ai-for-green-procurement/> (24.2.2026)
- McKinsey (2023): Action, bitte! Wie der öffentliche Sektor den Mangel an digitalen Fachkräften meistern kann. McKinsey & Company, Berlin
- McKinsey (2024): Generative künstliche Intelligenz in der öffentlichen Verwaltung – sieben Erfolgsfaktoren für eine flächendeckende Nutzung. McKinsey & Company, Berlin
- McKinsey (2025): KI-Agenten im Einsatz. So wird die öffentliche Verwaltung zukunftssicher. McKinsey Deutschland, <https://www.mckinsey.de/publikationen/2025-05-15-ki-agenten-im-einsatz> (23.2.2026)
- Mehr Demokratie e. V. (2024): Bürgerräte in Deutschland. Entwicklung und Vielfalt losbasierter Beteiligung. Berlin
- Menhard, E. (2025): Verwaltung in der Cloud: Bund macht sich abhängig von Amazon und Co. netzpolitik.org, <https://netzpolitik.org/2025/verwaltung-in-der-cloud-bund-macht-sich-abhaengig-von-amazon-und-co/> (26.7.2025)
- Münch, H. (2024): Gastbeitrag im SPIEGEL: „Wir brauchen eine Zeitenwende der inneren Sicherheit.“ Bundeskriminalamt, https://www.bka.de/DE/Presse/Interviews/2024/241220_GastbeitragSPIEGEL.html (24.3.2026)
- NBS-Geschäftsstelle (o. J.a): Deutschlands zentrale Naturschutzstrategie. <https://www.biologischeschevielfalt.de/strategie> (16.6.2026)
- NBS-Geschäftsstelle (o. J.b): Handlungsfeld 6 Digitalisierung, Daten und Forschung. <https://www.biologischeschevielfalt.de/strategie/uebergreifende-biodiversitaetsziele-fuer-deutschland/digitalisierung-daten-und-forschung> (24.2.2026)
- OECD (2024a): OECD Survey on Drivers of Trust in Public Institutions 2024 Results - Country Notes: Deutschland. Organisation for Economic Co-operation and Development, https://www.oecd.org/de/publications/oecd-survey-on-drivers-of-trust-in-public-institutions-2024-results-country-notes_a8004759-en/deutschland_1db98e83-de.html (30.7.2025)
- OECD (2024b): Green Budgeting in OECD Countries 2024. Paris, <https://doi.org/10.1787/9aea61f0-en>
- OECD (2025a): Governing with Artificial Intelligence. The State of Play and Way Forward in Core Government Functions. Paris, <https://doi.org/10.1787/795de142-en>
- OECD (2025b): Government at a Glance 2025. Organisation for Economic Co-operation and Development, Paris, <https://doi.org/https://doi.org/10.1787/0efd0bcd-en>
- Opiela, N. et al. (2023): Deutschland-Index der Digitalisierung 2023. Bertelsmann Stiftung, Gütersloh
- Overath, M.; Rösler, C. (2025): Das Klima schützen, die Energiewende gestalten, dem Klimawandel begegnen. Maßnahmen, Erfolge, Herausforderungen und Entwicklungen – Ergebnisse der Difu-Umfrage 2024. Deutsches Institut für Urbanistik, Policy Papers 6, Berlin, <https://doi.org/10.34744/DIFU-POLICY-PAPERS-2025-6>

- Peters, I.; Martin, N. (2026): KI-Agenten in der öffentlichen Verwaltung. Systematische Abgrenzung und konzeptioneller Definitionsrahmen. Technische Hochschule Wildau, WPRP01, Wildau, <https://doi.org/10.15771/wprp01>
- Pötter, B. (2025): Neue Analyse: Nicht mal die Bundesregierung ist auf Klima-Kurs. FOCUS online, https://www.focus.de/earth/neue-analyse-nicht-mal-bundesregierung-ist-auf-klima-kurs_cb21b242-f38d-4cf9-9dad-d82506c445d5.html (20.1.2026)
- Prognos et al. (2022): Übersicht vergangener Extremwetterschäden in Deutschland. Prognos AG, Institut für ökologische Wirtschaftsforschung; Gesellschaft für wissenschaftliche Struktur-forschung, Berlin
- Prümer, S.; Schnabel, C. (2023): Ist der Staat der bessere Arbeitgeber? In: Wirtschaftsdienst 103(9), S. 613–618
- PwC (2022): Fachkräftemangel im öffentlichen Sektor. PricewaterhouseCoopers, Berlin
- Raffer, C. (2023): Kommunale Investitionen in Klimaschutz und -anpassung. Finanzielle Dimensionen und Rolle der Kämmerereien. Sondergutachten im Rahmen des KfW-Kommunalpanels. Deutsches Institut für Urbanistik, Impulse 4, Berlin, https://doi.org/10.34744/10.34744/DIFU-IMPULSE_2023-4
- Reinke, M. (2025): Klimawandel und Biodiversität – Einflüsse globaler Entwicklungen auf die regionale biologische Vielfalt. In: Kramer, M. (Hg.): Systemische Nachhaltigkeit. Sektorspezifische und interdisziplinäre Blickwinkel. Wiesbaden, S. 49–57, https://doi.org/10.1007/978-3-658-47206-1_4
- Renn, O. et al. (2022): Systemic Risks from Different Perspectives. In: Risk Analysis 42(9), S. 1902–1920, <https://doi.org/10.1111/risa.13657>
- Rovner, M.; Handke, S. (2025): Digitale Transformation aus Sicht der Verwaltung: Erkenntnisse aus Leipzig und Dresden. In: Anke, J. et al. (Hg.): Digitale Identitäten und Nachweise. Wiesbaden, S. 105–121, https://doi.org/10.1007/978-3-658-47708-0_7
- Rudolf, P. (2019): Der amerikanisch-chinesische Weltkonflikt. Stiftung Wissenschaft und Politik, <https://www.swp-berlin.org/publikation/der-amerikanisch-chinesische-weltkonflikt> (21.4.2026)
- Schachtner, C. (2025): Estonia—Citizen Participation in the Capital City. In: Schachtner, C. (Hg.): The European Smart City Movement: Case Studies from Around Europe. Cham, S. 71–76, https://doi.org/10.1007/978-3-031-96700-9_8
- Schleicher, K. et al. (2024): Krisenkommunikation staatlicher Institutionen. Studienergebnisse und zentrale Erkenntnisse aus der COVID-19-Pandemie. In: Meißner, J.; Schach, A. (Hg.): Professionelle Krisenkommunikation. Wiesbaden, S. 131–154, https://doi.org/10.1007/978-3-658-43639-1_9
- Schulmann, H. (2026): ATHENEN Cybernation Deutschland. Sicherheit der IT der Länder. Frankfurt a. M.
- Schuppan, T. et al. (2025): Lernen aus der Vergangenheit?! Entwicklungslinien der Verwaltungsdigitalisierung in Deutschland aus den letzten 25 Jahren. Stein-Hardenberg Institut & Agora Digitale Transformation, o. O., <https://doi.org/10.5281/ZENODO.14793086>
- Schuster, F.; Klein, S. (2023): Klimaneutralität: teure Pflicht für die öffentliche Hand. PublicGovernance Sommer 2023, Berlin
- Schweizer Armee (2024): Palantir Technologies Inc. Schweizerische Eidgenossenschaft, Bern
- Shin, B. et al. (2024): A systematic analysis of digital tools for citizen participation. In: Government Information Quarterly 41(3), Art. 101954, <https://doi.org/10.1016/j.giq.2024.101954>
- Siepkner, L. et al. (2021): Trendanalyse – Engagement und Beteiligung in Deutschland. Münster

- Spannagel, D.; Brülle, J. (2024): Ungleiche Teilhabe: marginalisierte Arme - verunsicherte Mitte. Wirtschafts- und Sozialwissenschaftliches Institut, WSI Report 98, Düsseldorf
- Stephan, T. (2025): Cyberraum ist zu einem entscheidenden Faktor in der modernen Kriegsführung geworden. Angriffe im Netz. Bundeswehr, <https://www.bundeswehr.de/de/meldungen/cyberattacken-sicherheit-bedrohung-5893934> (4.3.2026)
- TAB (2024): Krisenradar – Resilienz von Gesellschaft, Politik und Wirtschaft durch Krisenvorhersage stärken. (Autor/innen: Behrendt, S. et al.) Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag, TAB-Arbeitsbericht 209, Berlin, <https://doi.org/10.5445/IR/1000171996>
- Tittelbach, S. (2023): Rechnungshof kritisiert Klimapolitik. Prüfungsergebnisse vorgestellt. Tagesschau, <https://www.tagesschau.de/inland/bundesrechnungshof-bau-boom-101.html> (20.1.2026)
- UBA (o. J.a): Anwendungslabor für Künstliche Intelligenz und Big Data am UBA. Stand 7.1.2025. Umweltbundesamt, <https://www.uba.de/n93305de> (16.6.2026)
- UBA (o. J.b): Ausgaben für den Umweltschutz. Stand 7.4.2025. Umweltbundesamt, <https://www.uba.de/n21890de> (16.12.2025)
- UBA (o. J.c): UBA-Kommunalbefragung „Klimaschutz in Kommunen“. Stand 15.8.2024. Umweltbundesamt, <https://www.uba.de/n107136de> (20.1.2026)
- UNDEP (2025): Guide to Digital Participation Platforms. United Nations Development Program, New York
- Vorländer, H. et al. (2025): Politische Polarisierung in Deutschland 2025. Mercator Forum Migration und Demokratie, Dresden
- Wagner, S. (2025): Der Bürokratie-Index: Messung des deutschen Gesetzgebungsvolumens und empirische Befunde. In: ifo Schnelldienst 78(07), S. 54–60
- WEF (2023): The Global Risks Report 2023. World Economic Forum, Genf
- Wegweiser Bürgergesellschaft (o. J.): Bilanz der Bürgerhaushalte in Deutschland. <https://www.buergergesellschaft.de/mitentscheiden/handlungsfelder-themen/buergerhaushalt/bilanz-der-buergerhaushalte-in-deutschland> (14.11.2025)
- Wehrbeauftragte (2025): Jahresbericht 2024 (66. Bericht). Unterrichtung durch die Wehrbeauftragte. Deutscher Bundestag, Drucksache 20/15060, Berlin
- Weiland, C. et al. (2025): FAIRification and AI-Readiness for Biodiversity Digital Twins. In: Biodiversity Information Science and Standards 9, Art. e181439, <https://doi.org/10.3897/biss.9.181439>
- Weiser, M. et al. (2025): How to Sell Democracy Online (Fast). Bertelsmann Stiftung, Gütersloh, <https://doi.org/10.5281/ZENODO.17098386>
- Wintergerst, R. (2023): Open Source Monitor 2023. Bitkom e. V., Berlin
- Wroblewski, M. (2025): Hybride Einflussnahme. Bedrohung durch Desinformation. Das Schlachtfeld ist der Verstand. Bundeswehr, <https://www.bundeswehr.de/de/meldungen/bedrohung-desinformation-cyber-5893466> (23.3.2026)
- Yang, J. et al. (2022): A Design and Application of Municipal Service Platform Based on Cloud-Edge Collaboration for Smart Cities. In: Sensors 22(22), Art. 8784, <https://doi.org/10.3390/s22228784>
- Zejewski, F. (2023): Innere Strukturen der Verwaltung verändern. In: Innovative Verwaltung 45, S. 37–39, <https://doi.org/10.1007/s35114-022-1494-6>

- ZenDiS (2026): Sozialversicherungen rüsten sich mit openDesk für den Krisenfall. Zentrum für Digitale Souveränität der Öffentlichen Verwaltung, <https://www.zendis.de/newsroom/presse/sozialversichererertenopendesk> (23.2.2026)
- ZEW (2025): Erstmals Bundesausgaben für Digitalisierung offengelegt. Leibniz-Zentrum für Europäische Wirtschaftsforschung, <https://www.zew.de/presse/pressearchiv/erstmals-bundesausgaben-fuer-digitalisierung-offengelegt> (8.12.2025)
- Zhai, Y. et al. (2024): Edge Computing. In: Zhai, Y. et al. (Hg.): Edge Computing Resilience: Overcoming Resource Constraints in Unstable Computing Environments. Singapore, S.1–10, https://doi.org/10.1007/978-981-97-6998-8_1
- Zillessen, F. et al. (2025): Das Justiz-Projekt: Verwundbarkeit und Resilienz der dritten Gewalt. Berlin, <https://doi.org/10.17176/20251129-153444-0>
- Zoric, T. (2025): IT-Störung bei der Bundespolizei sorgt für Probleme an Flughäfen. SWR, <https://www.swr.de/swraktuell/baden-wuerttemberg/computerausfaelle-bundespolizei-bundesweite-ausfaelle-flughafen-100.html> (4.3.2026)

7 Anhang

7.1 Abbildungen

Abbildung 1.1	Systembild	4
Abbildung 2.1	Anteil der Kommunen mit Onlineverfahren für ausgewählte Leistungen	9
Abbildung 2.2	Öffentlicher Dienst: Beschäftigte nach Aufgabenbereich 2022	13
Abbildung 2.3	Öffentlicher Dienst: über 55-jährige Beschäftigte in einigen Aufgabenbereichen 2022	14
Abbildung 2.4	Klimaschutzkonzepte in Kommunen	18
Abbildung 2.5	Zufriedenheit mit der Demokratie in Deutschland	23

7.2 Kästen

Kasten 2.1	Emerging Issue: Edge Computing im öffentlichen Raum	11
Kasten 2.2	Emerging Issue: KI-Agenten für Planungs- und Genehmigungsverfahren	15
Kasten 2.3	Emerging Issue: bundesweite Ökosystemdatenräume	18
Kasten 2.4	Emerging Issue: KI-gestützte Carbon-Assessment-Tools	21
Kasten 2.5	Emerging Issue: Bürgerfeedbacksysteme in Echtzeit	24

Herausgeber

Büro für Technikfolgen-Abschätzung
beim Deutschen Bundestag
Neue Schönhauser Straße 10
10178 Berlin

Telefon: +49 30 28491-0

E-Mail: buero@tab-beim-bundestag.de

www.tab-beim-bundestag.de

2026

Bildnachweis

ImageFlow/AdobeStock (S. 1)

DOI: 10.5445/IR/1000196376



Die Foresight-Reports fassen die Ergebnisse des Resilienz-Radars zusammen und erscheinen seit 2024 jährlich auf der Microsite (<https://foresight.tab-beim-bundestag.de>).

Das Resilienz-Radar (<https://foresight.tab-beim-bundestag.de/resilienz-radar/>) dient der Identifikation und Bewertung von Entwicklungen, die mit systemischen Risiken für kritische Infrastrukturen verbunden sind. Neben der Analyse zentraler Trends liegt der Fokus auf der Einschätzung von systemischen Risiken mit potenziell weitreichenden Auswirkungen, um die Gefährdungslage einzelner Infrastruktursysteme fundiert zu bewerten. Zudem werden jeweils infrastrukturspezifische Fokusthemen vorgeschlagen, die von besonderer Relevanz für eine vertiefende Untersuchung sind. Die Ergebnisse werden jährlich in den Foresight-Reports zusammengefasst.