

Cybernation Deutschland: Strategie für eine nationale KI-Infrastruktur*

Von Prof. Dr. Carsten Binnig^{1,2,3,4}, Prof. Dr. Jan Peters^{2,3,4}, Prof. Dr. Kristian Kersting^{1,2,3,4},
Prof. Dr. Antonio Krüger^{2,5}, Prof. Dr. Dr. Thomas Lippert⁶, Prof. Dr. Haya Schulmann^{1,6},
Prof. Dr. Michael Waidner^{1,4,7}

Version vom 30.09.2025

Kontakt: Prof. Dr. Haya Schulmann, schulmann@em.uni-frankfurt.de

Die künstliche Intelligenz (KI) hat sich innerhalb weniger Jahre – seit der Veröffentlichung von *GPT 3.5* durch *OpenAI* im Jahr 2022 – zur zentralen digitalen Schlüsseltechnologie entwickelt. Der Einfluss der KI geht heute weit über die Informationstechnologie hinaus – sie krempelt die gesamte Arbeitswelt um, ändert, wie und was wir lehren und lernen, was wir über die Welt zu wissen glauben, wie wir forschen und Neues erschaffen, wie und was wir untereinander kommunizieren. Dieser Einfluss verschafft Nationen, Unternehmen und Forschungseinrichtungen, die in der KI-Entwicklung führend sind, eine beispiellose Machtposition.

So ähnlich erging es uns schon einmal vor ungefähr 70 Jahren, als Computer begannen, unser Leben auf den Kopf zu stellen. Bis heute haben wir es in Deutschland und Europa nicht geschafft, zu einer führenden IT-Nation zu werden, und beklagen unsere mangelnde digitale Souveränität. Die KI bietet uns nun aber eine zweite Chance: auch sie gestaltet die Welt neu, steht aber in ihrer Entwicklung noch so weit am Anfang, dass es für uns noch eine realistische Chance gibt, in die Führungsgruppe aufzusteigen.

Notwendig dafür ist, in die weitere Entwicklung der sogenannten Basismodelle (Foundational Models) an vorderster Front einzusteigen. Diese sogenannten Frontier-Modelle enthalten das generelle Sprach-, Wissens- und Problemlösungsvermögen, auf dem die meisten modernen KI-Anwendungen aufbauen. Basismodelle werden von ihren Anbietern vortrainiert, d.h. sie werden mit möglichst vielen und hochwertigen Daten gefüttert, bei Sprachmodellen z.B. mit Artikeln, Büchern, Forschungsdatenbanken, Internetseiten und sozialen Medien. Analoges gilt für Basismodelle für andere Medien, z.B. Video und Audio, sowie für eingebettete KI in der Robotik, wo Wahrnehmung, Planung und Aktion in physischen Systemen integriert werden. Für spezielle Anwendungen müssen diese Basismodelle dann in einem »Finetuning« angepasst (z.B. durch fortlaufendes Training mit domänenspezifischen Daten) und in die IT-Umgebung des Kunden integriert und dort ständig überwacht und aktualisiert werden.

* Teile dieses Whitepapers basieren auf dem Artikel »Deutschland am KI-Wendepunkt« von Haya Schulmann und Michael Waidner, erschienen am 31. August 2025 in der Frankfurter Allgemeinen Zeitung

¹ ATHENE Nationales Forschungszentrum für angewandte Cybersicherheit

² DFKI Deutsches Forschungszentrum für künstliche Intelligenz

³ hessian.AI Hessisches Zentrum für künstliche Intelligenz

⁴ Technische Universität Darmstadt, Fachbereich Informatik

⁵ Universität des Saarlandes, Saarbrücken

⁶ Goethe-Universität Frankfurt am Main, Institut für Informatik

⁷ Fraunhofer-Institut für Sichere Informationstechnologie SIT, Darmstadt

Wer die großen Basismodelle, die Frontier-Modelle, und ihr Vortraining kontrolliert, bestimmt die Spielregeln der digitalen Welt. Führend sind derzeit US-amerikanische Unternehmen – bei Sprachmodellen sind es *OpenAI (GPT)*, *Google (Gemini)*, *Anthropic (Claude)* und *Meta (Llama)* –, mit etwas Abstand gefolgt von chinesischen Firmen – z.B. *Baidu (ERNIE)*, *Alibaba (Qwen)*, *Huawei (Pangu- Σ)* und *DeepSeek*. Das derzeit größte deutsche Sprachmodell ist *Luminous Supreme* von *Aleph Alpha*, das mit 70 Milliarden Parametern deutlich kleiner ist als die erwähnten Basismodelle aus den USA. *Llama-3* hat bis zu 405 Milliarden Parameter, GPT-4 wird teilweise sogar auf 1,76 Billionen geschätzt. Diese Größenunterschiede sind signifikant: Größere Basismodelle können in der Regel mehr Muster aus den Trainingsdaten erfassen, was zu besserem Kontextverständnis und weniger Fehlern führen kann.

Deutschland muss eine nationale KI-Infrastruktur mit eigenen, konkurrenzfähigen Basismodellen entwickeln und betreiben, um nicht dauerhaft von amerikanischen und chinesischen Anbietern abhängig zu bleiben. Neben exzellenter Forschung und Entwicklung sowie ausreichend Fachkräften braucht es dafür ein Netzwerk von KI-Rechenzentren: einige sehr große Rechenzentren, in EU-Sprechweise »KI-GigaFactories«, zum Training großer Basismodelle und mehrere regionale, kleinere KI-Rechenzentren zur Anpassung und zum Betrieb der Modelle (Inferenz). Die Kosten hierfür sind enorm: Jede KI-GigaFactory soll nach Vorstellung der EU mindestens 100.000 spezialisierte Recheneinheiten aufweisen, heute sind das sogenannte GPUs, und kostet daher voraussichtlich 3 bis 5 Milliarden Euro. Die Betriebskosten werden durch den Energieverbrauch dominiert – angesichts der sehr hohen Stromkosten in Deutschland keine gute Nachricht. Nach Schätzungen der International Energy Agency benötigen aktuelle große KI-Rechenzentren ungefähr so viel Energie wie 100.000 durchschnittliche Haushalte, Tendenz steigend. Das Training eines großen Basismodells kostet derzeit zwischen 30 und mehreren 100 Millionen Euro. Rechnet man alles zusammen, investieren die USA derzeit in der Größenordnung von mehreren hundert Milliarden Euro pro Jahr in Forschung, Entwicklung und Infrastruktur für KI, vorwiegend aus der Wirtschaft. China liegt etwas dahinter, andere Länder wie Japan, Südkorea, Saudi-Arabien und die Vereinigten Arabischen Emirate, aber auch Frankreich fahren ihre Investitionen derzeit deutlich hoch. Viel Geld ist also notwendig, aber mit der richtigen Strategie kann Deutschland bis 2030 zu den führenden KI-Nationen aufsteigen.

Folgen digitaler Abhängigkeit in der KI

Solange wir keine eigenen Frontier-Modelle, also Basismodelle der Spitzenklasse, auf einer von uns selbst kontrollierten KI-Infrastruktur entwickeln, hängen wir von den Angeboten aus den USA und China ab. Die Risiken solcher Abhängigkeiten sind konkret und vielfältig.

Ein im Ausland entwickeltes Sprachmodell kann, bewusst oder unbewusst, fremde Wertevorstellungen in deutsche Verwaltungsprozesse, Bildungssysteme oder die Justiz einbringen. Modelle, die auf einer anderen Rechtskultur beruhen, könnten Entscheidungen in der Sozialverwaltung verfälschen. Medizinische Systeme, trainiert auf Daten einer anderen Bevölkerungsgruppe, können in deutschen Kliniken zu Fehldiagnosen führen. Ebenso können narrative Verzerrungen in Trainingsdaten das Geschichtsbild in Medien, Schulen und Universitäten beeinflussen. Hinzu kommt die Gefahr politischer Einflussnahme: Wenn in der öffentlichen Verwaltung oder im Bildungsbereich fremdentwickelte Such- oder Sprachsysteme dominieren, können sie langfristig Narrative verstärken, die nicht unseren eigenen demokratischen Grundsätzen entsprechen. Auch wirtschaftlich ist die Abhängigkeit gefährlich: Anbieter können Preise diktieren, den Zugang einschränken oder Schnittstellen verändern. Deutschland ist in der industriellen Robotik derzeit noch weltweit führend, aber diese Position könnte durch aktuell fehlende KI-Kompetenz und digitale Abhängigkeit verloren gehen. Solche Mechanismen können gezielt als Instrument hybrider Kriegsführung eingesetzt werden, etwa um gesellschaftliche Spaltungen zu vertiefen, Vertrauen in Institutionen zu untergraben oder öffentliche Debatten subtil in eine gewünschte Richtung zu lenken.

Mit der Entwicklung und dem Training der Modelle allein ist das Problem jedoch noch nicht gelöst: wir müssen auch die verwendete Infrastruktur selbstbestimmt betreiben und verwalten. Wer die Infrastruktur betreibt und kontrolliert, kann sie jederzeit verteuern, einschränken oder uns ganz entziehen, kann unsere Entwicklungen beeinflussen und kann unsere Daten »absaugen«. Infrastruktur meint dabei den kompletten IT- und Betriebsstack, also Chips und Hardware, Software für die Entwicklung, zum Management und Betrieb, zur Sicherheit, Fehlertoleranz und Resilienz, alle Technologien für Daten- und Rechenzentren, vom Energie- bis zum Kühlmanagement.

Man könnte nun anführen, dass europäische Regulierungen wie die Datenschutz-Grundverordnung und das KI-Gesetz starke Leitplanken definieren, die uns absichern und europäischen Anbietern einen Vorteil im Markt geben. Allerdings hatten ähnliche Maßnahmen in anderen IT-Bereichen kaum eine Wirkung auf den Weltmarkt und auf den Erfolg der europäischen IT-Branche. Allein mit rechtlichen Mitteln lassen sich die genannten Risiken sicher nicht behandeln.

Deutschland braucht eine umfassende KI-Strategie

Mit welcher Strategie kann Deutschland bis 2030 zu einer der führenden KI-Nationen werden?

Erstens muss Deutschland — Staat und Wirtschaft gemeinsam — ausreichend finanzielle Mittel für einen stufenweisen, auf 3 bis maximal 5 Jahre verteilten Aufbau und Betrieb der eingangs skizzierten nationalen KI-Infrastruktur zur Verfügung stellen. Um die Kosten für den deutschen Staat möglichst gering zu halten, sollte diese Infrastruktur in einen größeren europäischen Verbund eingebettet und von der Wirtschaft mitfinanziert werden – ähnlich wie dies auch die EU zur Bedingung für die Förderung von KI-Gigafactories macht. Dafür ist zwar viel Geld erforderlich, aber realistischerweise müssten wir diese Mittel so oder so aufbringen, wenn nicht für die eigene Infrastruktur, dann für die Anbieter aus USA oder China.

Die Technologie für die Rechenzentren, insbesondere GPUs, kommt derzeit vorwiegend aus den USA. Langfristig wäre es daher wünschenswert, auch im KI-Hardwarebereich mehr Unabhängigkeit zu erreichen. Vorhaben zur Stärkung der Halbleiterindustrie in Europa, etwa der European Chips Act der EU und die Mikroelektronik-Strategie und High-Tech Agenda der Bundesregierung, sollten daher einen besonderen Schwerpunkt auf Entwurf und Produktion von KI-Hardware legen.

Dasselbe gilt für die oben erwähnten weiteren Technologien zur Entwicklung, Einrichtung und Betrieb von Rechenzentren, Datenräumen und anderen KI-Infrastrukturen. Auch diese kommen vorwiegend aus dem Ausland, und auch hier wäre eine deutlich geringere Abhängigkeit bzw. Kooperation auf Augenhöhe wünschenswert. Strategien und Initiativen zur Stärkung der europäischen und nationalen digitalen Souveränität sollten daher besonders diese KI-Infrastrukturen berücksichtigen.

Zweitens müssen wir die umfangreichen Datenschätze, über die wir in Deutschland und Europa verfügen, für das Training allgemeiner und spezieller Modelle zugänglich machen. Letztlich sind es diese Daten, die den Wert der Modelle ausmachen und die uns die Kontrolle zurückgeben. Das erfordert ein pragmatisches Vorgehen hinsichtlich z.B. Daten- und Urheberschutz, was wiederum entsprechende Mechanismen zur Kuratierung, gegen Cyberangriffe sichere und vertrauenswürdige Datenräume und faire Geschäftsmodelle für diese Datenräume voraussetzt.

Drittens, damit eine solche Infrastruktur strategisch wirksam wird, muss sie eng mit einer starken, exzellent vernetzten Forschungslandschaft zusammenarbeiten. Es müssen deutlich mehr KI-Fachkräfte ausgebildet und relevante KI-Aspekte in allen Studien- und Ausbildungsfächern berücksichtigt werden. Nur so entstehen aus Rechenleistung und Daten tatsächlich leistungsfähige und vertrauenswürdige KI-Systeme. Da die gene-

relative KI noch jung ist und ihre Entwicklung vom wissenschaftlichen Fortschritt abhängt, kommt der Forschungsexzellenz für die zukünftige Wettbewerbsfähigkeit besondere Bedeutung zu. Dank gezielter öffentlicher Förderung steht Deutschland in der KI-Forschung und -Ausbildung recht gut da, mit Forschungseinrichtungen wie den Mitgliedern der KI-Kompetenzzentren und anwendungsorientierten Einrichtungen wie dem *DFKI (Deutsches Forschungszentrum für Künstliche Intelligenz)*, dem *Jülich Supercomputing Centre (JSC)* und diversen von Bund und Ländern finanzierten Hochschulzentren, insbesondere *hessian.ai* in Hessen. Das *Nationale Forschungszentrum für angewandte Cybersicherheit ATHENE* fokussiert sich auf Cybersicherheit von und durch KI in enger Zusammenarbeit mit den oben genannten Zentren. Das *RIG (Robotik-Institut-Germany)* fokussiert sich auf die Verschmelzung von KI und Robotik für Industrie 4.0, autonome Systeme und Human-Robot-Interaction. Auch aus der Privatwirtschaft kommen umfangreiche Initiativen. In Heilbronn entsteht mit Mitteln der *Dieter Schwarz-Stiftung* der *IPAI (Innovation Park Artificial Intelligence)*, ein Campus, der führende KI-Akteure aus Wirtschaft und Wissenschaft an einer Stelle zusammenbringt.

Forschung braucht es nicht nur zum maschinellen Lernen und Robotik, sondern auch zur Entwicklung der zugrunde liegenden Informatiktechniken und Anwendungen, z.B. Hochleistungsrechnen, Green IT, Quantencomputing, Cybersicherheit.

Viertens müssen Cybersicherheit und Resilienz von Anfang an beim Aufbau und Betrieb der KI-Infrastruktur berücksichtigt werden. Die Bedrohungslage für eine nationale KI-Infrastruktur ist komplex und reicht von staatlicher Einflussnahme bis hin zu kriminellen Angriffen. Staatliche Akteure könnten versuchen, durch Spionage Zugriff auf wertvolle Modelle und Trainingsdaten zu erlangen, Trainingsprozesse gezielt zu sabotieren oder versteckte Backdoors in Modelle einzuschleusen, um langfristig Zugriffsmöglichkeiten zu schaffen. Denial-of-Service-Angriffe auf die kritische Infrastruktur können den Betrieb stören oder ganz lahmlegen. Kriminelle Gruppen setzen auf Ransomware, um Rechenzentren zu erpressen, stehlen Modelle für den lukrativen Weiterverkauf oder nutzen ungesicherte Ressourcen für Cryptojacking. Hinzu kommt die Gefahr der Wirtschaftsspionage: Ausländische Wettbewerber könnten gezielt auf deutsche Innovationen abzielen, unterstützt durch Insider in Unternehmen oder Forschungseinrichtungen, oder durch Supply-Chain-Angriffe über manipulierte Hardware-Komponenten. Eine wirksame nationale KI-Strategie muss diese Bedrohungen von Anfang an adressieren und Cybersicherheit nicht als nachträgliche Schutzmaßnahme, sondern als integralen Bestandteil der gesamten Architektur begreifen. Eine nationale KI-Infrastruktur sollte daher von Anfang an sicher konzipiert werden. Zero-Trust-Architekturen, zentrale Security-Operations, Hardware-Sicherheitsmodule, kontinuierliches Red-Teaming und physische Sicherung und Lagebilderstellung sind unverzichtbar. Angesichts der strategischen Bedeutung müssen die Systeme auch gegen künftige Bedrohungen wie Quantenangriffe gewappnet sein. Langfristig müssen Zertifizierungen etabliert werden, die Sicherheit und Vertrauenswürdigkeit der Infrastruktur regelmäßig prüfen.

Fünftens, es braucht eine möglichst frühzeitige Standardisierung innerhalb der nationalen KI-Infrastruktur. Föderale Zersplitterung riskiert Mehrfachbeschaffungen, inkompatible Systeme, ineffiziente Auslastung und Sicherheitslücken. In Kanada scheiterte die parallele Entwicklung föderaler und provinzieller KI-Plattformen an Inkompatibilitäten; erst eine nationale *Digital Research Alliance* brachte Abhilfe. In Deutschland zeigen die 16 verschiedenen Schulplattformen der Länder die Kosten und Ineffizienz solcher Fragmentierung. Für die Wissenschaft und Anwendung in Wirtschaft und Verwaltung bedeutet Standardisierung eine einheitliche und moderne technische Basis, gerechte Ressourcenvergabe, hohe Auslastung und einheitliche Sicherheitsstandards auf hohem Niveau. Sie macht die Infrastruktur zu einem klaren, verlässlichen Partner für internationale Kooperationen. Für Bund und Länder reduziert die Standardisierung die Kosten für neue Infrastrukturen und wahrt den Wert existierender Investitionen.

Sechstens, es braucht eine effektive Umsetzungsstruktur für diese Strategie. Alles bisher Skizzierte ist leistbar, wenn Politik, Wirtschaft, Gesellschaft und Wissenschaft dahinterstehen. Wir müssen uns einig sein,

dass wir den oben erwähnten KI-Wendepunkt nutzen wollen, um unsere Position in der globalen IT-Landschaft deutlich zu verbessern, und nicht wieder denselben Fehler wie zuvor in der IT machen und uns mit Nischentechnologien wie domänenspezifischem Finetuning von Modellen oder dem Status eines KI-Anwenders und Hüters von Datenschätzen begnügen.

Standortfragen für Rechenzentren und ihre Infrastruktur müssen sachlich und schnell geklärt werden, ohne sich in endlosen Planungs- und Einspruchsverfahren zu verlieren oder sachfremde Kriterien in den Vordergrund zu stellen. Besonders wichtig ist dabei die Energiefrage: KI ist energiehungrig, Trainieren benötigt zudem hohe Versorgungssicherheit. Wind- und Solarenergie allein genügen hierfür nicht, sie unterliegen starken wetterabhängigen Schwankungen. Die Schweiz und Norwegen planen daher große KI-Rechenzentren in der Nähe von Wasser-, die USA in der Nähe von konventionellen und Kernkraftwerken. Weltweit treibt die KI die Planungen für neue Kraftwerke an, einschließlich neuer Atomreaktoren. Energiekosten und Versorgungssicherheit sollten auch bei uns entscheidend sein für die Standortfindung. KI-Rechenzentren mit weniger Anforderungen an die Versorgungssicherheit, also solche für Inferenz oder kleinere Modelle, sollten dort entstehen, wo Strom günstig erzeugt wird, z.B. in der Nähe von Windkraft- und Solaranlagen im Norden und Osten, und wo es besonders einfach ist, mit den angestrebten Kunden breitbandig und latenzarm zu kommunizieren, z.B. im Großraum Frankfurt-Rhein-Main, der mit dem *DE CIX*, dem weltgrößten Internetknoten, besonders gut an das Internet angebunden ist. Rechenzentren mit hohen Anforderungen an die Versorgungssicherheit sollten in der Nähe entsprechender Kraftwerke (also Kohle/Gas oder Wasser) sein, da es an den ebenfalls notwendigen Energieübertragungskapazitäten insbesondere in Nord-Süd-Richtung mangelt. In Bezug auf Versorgungssicherheit bietet sich NRW als Standort in besonderem Maße an.

Die Bundesregierung strebt an, dass wenigstens eine KI-Gigafactory in Deutschland mit Förderung der EU gebaut werden soll. Das *Forschungszentrum Jülich* gilt aus fachlicher Sicht als besonders gut geeigneter Betreiber größter HPC- und KI-Infrastrukturen: Mit *JUPITER* gibt es dort bereits ein KI-optimiertes Hochleistungsrechensystem, viel Erfahrung in Aufbau und Betrieb solcher Systeme und Zugriff auf zuverlässige Energie und Kommunikation. Die Realität in Deutschland ist aber leider weit entfernt von solchen rationalen Überlegungen. Statt dass sich alle hinter Jülich stellen und die nächsten Schritte im Wettbewerb um die Förderung der EU für den Aufbau einer KI-Gigafactory in Deutschland planen, wird in Teilen der Politik und Wirtschaft die Standortwahl als Instrument der Regionalentwicklung missverstanden und so unser Erfolg in der KI ohne Not geopfert.

Entscheidungen wie diese müssen sachlich und wissenschaftsgeleitet gefällt werden, zentralisiert an einer Stelle mit klarer Verantwortung und klaren Befugnissen. Geschwindigkeit ist hier besonders kritisch – wichtige Grundsatzfragen wie die Standortwahl für KI-Rechenzentren müssen früh und schnell gefasst werden, Entwicklungszyklen bei Modellen und Software-Stacks liegen derzeit bei 12 bis 18 Monaten. Nichts bremst große Vorhaben effektiver aus als Verantwortungsdiffusion in Kombination mit aufwändigen Abstimmungsprozessen, egal ob in großen Industriekonsortien oder zwischen den Bürokratien verschiedener Bundesministerien und Landesregierungen. Die KI-Strategie und ihre Umsetzung müssen deshalb auch in Deutschland zur Chefsache gemacht, also im Bundeskanzleramt angesiedelt sein. Für die fachliche Steuerung und den Ausgleich von Interessen zwischen Wissenschaft, Wirtschaft und Politik sollte von Anfang an ein entsprechend besetzter, wissenschaftsgeleiteter KI-Rat eingerichtet werden. Vertreten sein sollten neben Bund und Ländern die wichtigsten Fachdisziplinen, insbesondere aus der Informatik (maschinelles Lernen, Hochleistungsrechnen, Software, Kommunikation, Cybersicherheit, Robotik und autonome Systeme), sowie die wichtigsten KI-Anwendungsgebiete und Industrien.

Weder die stark privatwirtschaftlich geprägte KI-Strategie der USA noch der staatszentrierte Ansatz Chinas passt zu den Rahmenbedingungen und Zielen Deutschlands. Ein rein gewinnorientierter Unternehmensansatz birgt die Gefahr, dass kurzfristige Renditeziele Grundlagenforschung vernachlässigen, Abhängigkeiten

von einzelnen Konzernen entstehen und strategische Technologien ohne demokratische Kontrolle entwickelt werden. Ein ausschließlich staatlich gesteuertes Modell wiederum leidet oft unter bürokratischer Trägheit, langen Entscheidungswegen und mangelnder Marktnähe. Für Deutschland bietet sich daher ein hybrider Ansatz an, bei dem die Forschung die strategische Ausrichtung und wissenschaftliche Qualität sichern, während Industriepartner praxisnahe Umsetzung und Skalierung übernehmen, eingebettet in klare politische Leitplanken.

Die Umsetzung der Strategie sollte deshalb einer eigenständigen, unabhängigen Deutschen KI-Agentur mit dem KI-Rat als Aufsichtsrat übergeben werden. Diese KI-Agentur sollte über sehr große Freiheitsgrade z.B. hinsichtlich Planungsverfahren, Beschaffungswesen und Gehaltsstrukturen und über ein für mehrere Jahre gesichertes Budget verfügen. Um alle Beteiligten – Wissenschaft, Wirtschaft, Gesellschaft, Bund und Länder – mitzunehmen, sollte die KI-Agentur einen detaillierten Umsetzungsplan entwickeln, der für alle die notwendigen Anreize zur Kooperation und gemeinsamen Finanzierung schafft.

Roadmap der nationalen KI-Strategie

KI-Agentur und nationale KI-Strategie

- Bis Mitte 2026: Bund, Länder und die deutsche Wirtschaft gründen und finanzieren eine Public-Private-Partnership zur gemeinsamen Errichtung und zum gemeinsamen Betrieb von KI-Gigafactories in Deutschland.
- Bis Ende 2026: Auf der Ebene des Bundeskanzleramts und der Staatskanzleien wird ein wissenschaftsgeleiteter, aber auch Wirtschaft, Gesellschaft und Verwaltung berücksichtigender Nationaler KI-Rat geschaffen.
- Bis Ende 2026: Bund, Länder und der KI-Rat legen eine umfassende, auf Technologieführerschaft bis 2030 ausgerichtete Nationale KI-Strategie des Bundes und der Länder sowie einen dazugehörigen Umsetzungsplan vor. Die Umsetzung soll durch die zu gründende KI-Agentur gesteuert und jährlich durch den KI-Rat geprüft und angepasst werden.
- Bis Ende 2027 und danach fortlaufend: Evaluierung der Strategie durch den KI-Rat hinsichtlich ihrer Auswirkung auf die nationale und europäische Innovationsfähigkeit in KI und Digitalisierung, sowie auf den Auf- und Ausbau von KI-Reallaboren und Empfehlungen für entsprechende Anpassung bestehender Regelungen durch die Gesetzgeber.
- Bis Ende 2027: Änderungen der rechtlichen Rahmenbedingungen mit dem Ziel einer ersten deutlichen Absenkung der Energiekosten für KI-Rechenzentren in Richtung des Niveaus der USA.
- Bis Ende 2027: Bund und Länder gründen die Deutsche KI-Agentur, die die Verantwortung für die Umsetzung der nationalen KI-Strategie übernimmt. Die KI-Agentur kann die Fortsetzung der o.g. PPP sein. Soweit notwendig, soll die KI-Agentur auch für die Errichtung und den Betrieb von Teilen der KI-Infrastruktur (Rechenzentren, Datenräume) verantwortlich sein oder als Ankermkunde für andere Betreiber dienen. Die KI-Agentur soll einen für mehrere Jahre gesicherten Haushalt erhalten und zur Umsetzung der Strategie in hohem Maße selbständig handeln können (z.B. hinsichtlich Vergaberecht, Arbeits- und Tarifrecht).
- Bis Ende 2027: Änderungen der rechtlichen Rahmenbedingungen durch Bund und Länder, so dass Planung, Bau und Betrieb von KI-Rechenzentren und anderen wichtigen KI-Infrastrukturen beschleunigt und der Betrieb und Zugriff auf die notwendigen Infrastrukturen (Energie, Kommunikation) erleichtert werden.

- Bis Ende 2027: Die KI-Agentur definiert einheitliche Standards für die nationale KI-Infrastruktur. Diese sollen soweit möglich verbindlich sein; für andere Bereiche sollen z.B. durch geförderte Pilotprojekte und Zusagen für privilegierten Zugang Anreize zur Übernahme dieser Standards geschaffen werden.

KI-Infrastruktur

- Bis Mitte 2026: Gründung einer KI-Datenallianz zwischen Wirtschaft, Verwaltung und Wissenschaft, auf nationaler oder europäischer Ebene, auf nationaler Ebene mit Unterstützung und ggf. späteren Trägerschaft durch die KI-Agentur.
- Bis Ende 2027: KI-Datenallianz veröffentlicht Standards und Policies zur gesichert rechtskonformen und im umfassenden Sinne fairen Bereitstellung von Daten für KI-Anwendungen.
- Bis Ende 2027: Darauf aufbauend Bereitstellung eines europäischen oder nationalen KI-Datenräumen, der allen Teilnehmenden die rechtssichere Nutzung von Daten zusichert.
- Bis Ende 2030: Die nationale KI-Infrastruktur soll schrittweise auf wenigstens zwei KI-Gigafactories (die erste bis Ende 2028) sowie wenigstens 10 weitere regionale KI-Rechenzentren ausgebaut werden (die ersten bis Ende 2027).

Ambitionierte KI-Forschungsstrategie

- Anfang 2026: Die Bundesregierung legt – der *High-Tech Agenda* folgend – eine ressort- und länderübergreifende, auf Technologieführerschaft ausgerichtete KI-Forschungs-, Entwicklungs- und Bildungsstrategie als Teil der o.g. Nationalen KI-Strategie vor in enger Abstimmung mit den bestehenden KI-Strukturen, insbesondere den KI-Kompetenzzentren und weiteren wichtigen KI-Akteuren in Deutschland. Die Strategie sichert den Zugang der Forschung zur nationalen KI-Infrastruktur; stabilisiert die existierenden erfolgreichen Forschungszentren und fördert die übergreifende Zusammenarbeit in Forschung (UF und AUF), Wirtschaft und Verwaltung. Sie unterstützt die akademische, berufliche und schulische Bildung im Bereich KI. Sie schafft Anreize zur Stärkung des Innovationssystems der deutschen Wissenschaft und Wirtschaft, d.h. Forschung und Innovationen müssen sich für alle Beteiligten lohnen und dürfen nicht durch Überregulation und schlechte Arbeitsbedingungen behindert werden. Diese Strategie soll auf die Unterstützung des gesamtstrategischen Ziels – Technologieführerschaft bis 2030 – ausgerichtet, also deutlich anwendungsorientiert sein.
- Ende 2027: Die nationalen Aktivitäten – Zugriff der Forschung auf nationale KI-Infrastruktur, Verbund von Forschungszentren – sollen auf EU-Ebene in ein “CERN für KI” einfließen, wie z.B. von der *Group of Chief Scientific Advisors* der EU und *CLAIRNE (Confederation of Laboratories for Artificial Intelligence Research in Europe)* gefordert, also in einen EU-weiten Forschungsverbund mit Zugriff auf große KI-Infrastrukturen, wissenschaftsgeleitet, aber unter Beteiligung der Wirtschaft.
- Bis Ende 2027: Aufbau nationaler Testfelder für KI-basierte Robotik in Kooperation zwischen Robotik-Institut-Germany (RIG), Industrie und regionalen KI-Zentren

Cybersicherheit und -resilienz von KI-Infrastruktur und -Anwendungen

- Bis Ende 2027: Die KI-Agentur legt konkrete Empfehlungen und Vorgaben zur Cybersicherheit und -resilienz von KI-Infrastrukturen und KI-Anwendungen vor. Dies soll die allgemeinen Zielsetzungen z.B. im AI Act und Vorgaben z.B. im NIS2-Umsetzungsgesetz umsetzen und so eine einheitliche Sicherheitsarchitektur realisieren.