

Videoreihe

Gesamttext zum Nachlesen

Einleitung

Das Team stellt sich zu Beginn der Reihe vor. Zusammen mit dem Team der Organisation Safe AI Germany arbeiten sie im Bereich der KI Sicherheit. Sie sind überzeugt, dass die Menschen, die in Deutschland politische Entscheidungen treffen, das Werkzeug verdienen, um dieses Thema wirklich zu verstehen. Die fünf Videos sind für dieses Publikum gemacht. Vorwissen ist dabei nicht nötig, gefragt ist nur die Bereitschaft hinzuschauen.

Die fünf Videos führen der Reihe nach durch folgende Fragen. Warum die eigene Wählerschaft das Thema bereits spürt. Was KI Sicherheit eigentlich ist. Was das für Deutschland bedeutet. Warum gerade jetzt der richtige Moment ist. Und was jede und jeder Einzelne tun kann.

Video 1, Warum Ihre Wählerschaft das bereits spürt

Die Sprecherin erzählt von jemandem, den viele wahrscheinlich kennen. Ein Mann, Mitte vierzig, zwei Kinder, Vollzeitjob. Er nutzt sein Smartphone den ganzen Tag, liest Nachrichten, schaut Videos, bekommt Empfehlungen. Seit einiger Zeit trägt er ein Gefühl mit sich, das er nicht ganz benennen kann. Er hat den Eindruck, den Dingen, die er sieht, nicht mehr so vertrauen zu können wie früher. Manchmal hält er inne und fragt sich, ob das, was er gerade sieht, überhaupt echt ist.

Dieser Mann ist keine Ausnahme. Im April 2026 hat Infratest dimap für die ARD über 1.300 Wahlberechtigte in Deutschland befragt. 45 Prozent erwarten, dass KI ihr Leben in den nächsten fünf Jahren verschlechtern wird. Über 90 Prozent halten KI generierte Deepfakes für ein hohes oder sehr hohes Risiko. Über 90 Prozent machen sich Sorgen, echte Nachrichten nicht mehr von gefälschten unterscheiden zu können.

Das Gefühl dieses Mannes ist also repräsentativ, das zeigen die Daten. Gleichzeitig hat der BSI in seinem Cybersicherheitsmonitor 2026 festgestellt, dass die meisten Menschen viel zu wenige Schutzmaßnahmen kennen. Nur 14 Prozent der Befragten informieren sich regelmäßig über Cybersicherheit, vier von zehn beschäftigen sich erst dann damit, wenn bereits etwas passiert ist. Auch beim Thema KI generierte Inhalte zeigt sich diese Lücke, nur etwa ein Drittel schaut bei möglicherweise KI generierten Inhalten überhaupt genauer hin.

Diese Menschen wählen, sie sind in jedem Wahlkreis vertreten. Sie schreiben ihren Abgeordneten vielleicht keine Briefe über KI, tragen die Unsicherheit aber trotzdem mit sich.

Was dieser Mann aus dem Interview spürt, ist das sichtbare Ende einer viel tieferen Frage, nämlich wer die Systeme eigentlich baut, die ihm Informationen liefern, wer sie trainiert hat und wessen Interessen darin eingeschrieben sind. Diese Systeme entscheiden zunehmend auch

über ihn, über die Wohnung, die er sucht, über den Kredit, den er beantragt, über Bewerbungen, die er verschickt. Diese Fragen reichen weit über Deepfakes hinaus, sie fangen dort aber an.

Genau in diesem Moment wird Politik relevant, immer dann, wenn etwas im Leben von Menschen passiert, das sie nicht alleine navigieren können, und jemand den Rahmen dafür setzen muss.

KI Sicherheit ist genau dieser Rahmen. Was das konkret bedeutet, zeigt Video zwei.

Video 2, Warum KI Sicherheit uns alle angeht

Die Welt zu verändern bringt immer Risiken mit sich. In der Vergangenheit haben wir das oft erst verstanden, als der Schaden bereits angerichtet war. Bei Künstlicher Intelligenz können wir uns dieses Vorgehen nicht leisten, denn die Zeit drängt.

KI ist keine technologische Revolution wie jede andere. In einer globalisierten, vernetzten Welt verbreitet sich diese Technologie in beispiellosem Tempo. Vor gerade einmal fünf Jahren konnte man sich noch über KI Systeme amüsieren, die nicht erkannten, welche von zwei Zahlen die größere ist. Heute genügt eine einzige Zeile Code, um eine interaktive Webseite erzeugen zu lassen. Im allgemeinen Hype gehen dabei Risiken unter, die teils katastrophale Ausmaße annehmen können, Risiken, vor denen die KI Sicherheitsforschung und selbst die Entwicklerfirmen warnen.

Diese Gefahren lassen sich grob in drei Kategorien einteilen. Erstens könnten einzelne Akteure KI gezielt einsetzen, um großflächigen Schaden anzurichten, etwa durch Cyberangriffe oder die Entwicklung von Biowaffen. Zweitens besteht die Möglichkeit, dass sich KI Systeme unkontrolliert verhalten, ein Risiko, das wächst, je mehr Verantwortung diese Systeme übernehmen und je länger die Aufgaben werden, die sie eigenständig erledigen. Drittens gibt es ein gesellschaftliches Risiko, zum einen die enorme Macht, die sich derzeit bei wenigen großen Unternehmen in noch weniger Ländern konzentriert, zum anderen die Abhängigkeit, die wir selbst gerade von dieser Technologie entwickeln.

Verschärft wird all das durch den Wettlauf verschiedener Akteure um das führende KI System. Neue Systeme entstehen deutlich schneller, als die Sicherheitsforschung oder die gesetzlichen Grundlagen Schritt halten können.

Neben diesen katastrophalen Risiken dürfen die greifbaren, nahen Gefahren nicht vergessen werden, die wirtschaftliche Abhängigkeit, die Einflussnahme auf Entwicklung, Verbreitung und Regulierung von KI Systemen, der Wandel des Arbeitsmarktes, und die Frage, wie sich in sozialen Medien noch Echtes von Gefälschtem unterscheiden lässt.

Jede Regierung muss sich fragen, wie sie mit diesen Themen umgeht. Um sie jedoch tatsächlich anzugehen und die Zukunft der KI mitzugestalten, müssen Europa und Deutschland handlungsfähig bleiben. Ohne Einfluss gibt es kein Mitspracherecht, keinen Hebel, keine Gestaltungsmöglichkeit und keinen Schutz für die eigenen Einwohnerinnen und Einwohner.

Handlungsfähig zu bleiben, auch das ist KI Sicherheit. Von den drei genannten Risiken ist das gesellschaftliche dasjenige, bei dem die deutsche Politik den direktesten Hebel hat. Genau dort setzen die nächsten Videos an. Wo Deutschland heute wirklich steht, zeigt Video drei.

Video 3, Wo steht Deutschland wirklich

Wer diese Systeme baut und trainiert, entscheidet auch darüber, wer sie kontrolliert und wer am Ende Zugriff auf sie hat. Deutschland ist eine der stärksten Industrienationen der Welt, trotzdem läuft ein Großteil der digitalen Infrastruktur auf Systemen, die wir nicht kontrollieren und deren Zugang langfristig nicht automatisch garantiert ist. Dieses Problem ist alt, es wird durch KI aber deutlich beschleunigt und bekommt dadurch ein neues Gewicht, für Deutschland und für Europa gemeinsam.

Schauen wir uns das konkreter an. 96 Prozent der deutschen Unternehmen kommen ohne den Import digitaler Technologien aus dem Ausland nicht aus, das zeigt die Studie Digitale Souveränität 2025 von Bitkom aus dem November 2025. 57 Prozent dieser Unternehmen würden ohne diese Importe maximal ein Jahr überleben. Diese Zahl ist über tausend kleine Beschaffungsentscheidungen entstanden, bei denen niemand das Gesamtbild im Blick hatte. Die genauen Zahlen verändern sich mit der Zeit, die jeweils aktuellen Werte werden deshalb fortlaufend auf der Website aufbereitet.

Drei Schichten dieser Abhängigkeit haben konkrete politische Konsequenzen.

Der erste Punkt betrifft den Rechtszugriff. Wenn eine deutsche Behörde, ein Krankenhaus oder ein Rüstungsunternehmen KI einsetzt, läuft das in der Mehrheit der Fälle auf amerikanischer Cloud Infrastruktur. Der CLOUD Act von 2018, die Clarifying Lawful Overseas Use of Data Act des US Department of Justice, erlaubt US Behörden unter bestimmten Bedingungen Zugriff auf diese Daten, unabhängig davon, wo die Server physisch stehen. Das ist geltendes Recht, das bereits angewendet wird, und es betrifft jedes europäische Land, das auf dieselbe Infrastruktur setzt.

Der zweite Punkt betrifft Investitionen und Talent. Private KI Investitionen in den USA lagen 2025 bei 285,9 Milliarden Dollar, in Deutschland bei 3,89 Milliarden Dollar. Wer in Deutschland KI erforscht, verdient im Schnitt ein Drittel dessen, was dieselbe Arbeit in den USA einbringt. Solange das so bleibt, wandert das Talent ab, das hierzulande selbst ausgebildet wird, und das gilt für die meisten europäischen Länder gleichermaßen.

Der dritte Punkt betrifft das industrielle Wissen. Volkswagen, Siemens und BASF bauen ihre Produktionssysteme zunehmend auf KI gestützte Prozesse um. Fertigungsdaten, Optimierungsalgorithmen und jahrzehntelang gesammeltes Know how laufen dabei auf Infrastruktur, die Konzerne mit Sitz in Seattle oder San Francisco betreiben.

Europa hat mit dem AI Act den ersten umfassenden rechtlichen Rahmen für KI weltweit geschaffen. Laut Stanford AI Index 2026 vertrauen weltweit mehr Menschen der EU als Regulierer als den USA oder China. Regeln brauchen jedoch Infrastruktur, um wirksam zu sein. Die Anzahl staatlich geförderter KI Supercomputer Cluster in Europa stieg von 3 im Jahr 2018 auf 44 im Jahr 2025, angetrieben durch EuroHPC.

Trotzdem bezeichnen sich 9 von 10 deutschen Unternehmen als digital abhängig, und 63 Prozent erwarten, dass diese Abhängigkeit in den nächsten fünf Jahren weiter zunimmt.

Bei einer Technologie wie künstlicher Intelligenz darf das so nicht bleiben. Die Einigkeit darüber existiert bereits, in Deutschland wie in Europa. Was fehlt, sind die Entscheidungen.

Genau diese Entscheidungen wirken sich direkt auf die Menschen aus, die Abgeordnete vertreten, auf die Patientin, deren Daten in einer amerikanischen Cloud liegen, auf die jungen Forscherinnen und Forscher, die ins Ausland abwandern, und auf die Arbeitsplätze, die an industriellem Wissen hängen, das gerade seinen Standort wechselt.

Welche Entscheidungen jetzt noch möglich sind und welche bereits wegfallen, darum geht es in Video vier.

Video 4, Warum jetzt

Man kann sich ein Fenster vorstellen, das sich ganz langsam schließt, nicht mit einem lauten Knall, sondern leise und Zentimeter für Zentimeter, kaum bemerkbar. Genau das passiert gerade mit dem politischen Gestaltungsspielraum bei Künstlicher Intelligenz.

Auch Nicht Handeln ist eine Entscheidung, denn sie gestaltet die Zukunft mit. Jeder Tag des Abwartens bedeutet, dass andere festlegen, welche Technologien genutzt werden, welche Regeln gelten und welche Werte die Systeme von morgen prägen. Je später die Politik handelt, desto stärker werden künftige Entscheidungen bereits durch heutige technische und institutionelle Weichenstellungen vorgegeben. Aktuell schließen sich gleich drei solcher Zeitfenster.

Das erste Fenster betrifft die digitale Souveränität. Mit dem Marktplatz der KI Möglichkeiten, kurz MaKI, hat Deutschland einen wichtigen Schritt gemacht. Behörden können KI Anwendungen teilen, voneinander lernen und bestehende Lösungen nutzen. Doch mit jeder neuen Beschaffung wird zugleich festgelegt, auf welchen Technologien der Staat künftig arbeitet. Das Fundament der digitalen Verwaltung von morgen entsteht also bereits heute, und ist es einmal gelegt, lässt es sich später nur schwer verändern.

Das zweite Fenster betrifft die europäische Recheninfrastruktur. Wo Europa mit EuroHPC aktuell steht, wurde bereits in Video drei gezeigt. Entscheidend ist nun, warum das Zeitfenster gerade jetzt zählt. KI wartet nicht, bis die europäische Infrastruktur fertig aufgebaut ist. Wer heute Modelle entwickelt, braucht heute Rechenleistung. Fehlen europäische Kapazitäten, entstehen Abhängigkeiten von außereuropäischen Anbietern für Rechenleistung, Hardware und Cloud Infrastruktur. Selbst Mistral AI nutzt dafür Teile seiner Rechenleistung über Microsofts Cloud. Aus Zwischenlösungen werden Strukturen, aus Strukturen werden Abhängigkeiten, und sind sie einmal entstanden, lassen sie sich später kaum noch auflösen.

Das dritte Fenster betrifft die Regeln von morgen. Der AI Act, ebenfalls aus Video drei bekannt, braucht technische Standards, damit seine Regeln in der Praxis greifen. Wissenschaft, Zivilgesellschaft und Unternehmen sollen daran mitwirken, verfügen dabei aber nicht alle über die gleichen Ressourcen, um sich einzubringen. Wer heute die Standards mitgestaltet, prägt

damit die Systeme von morgen, und auch hier gilt, einmal gesetzte Standards lassen sich später nur schwer wieder ändern.

Was können Abgeordnete konkret tun? Erstens können sie dazu beitragen, dass Deutschland KI in der öffentlichen Verwaltung nicht nur in einzelnen Projekten, sondern strategisch einsetzt, mit Transparenz, Wissensaustausch und gemeinsamen Standards als Grundlage. Zweitens können sie mit dazu beitragen, dass Europa seine eigene Recheninfrastruktur schneller aufbaut und langfristige Abhängigkeiten begrenzt. Drittens können sie sich dafür einsetzen, dass die Regeln von morgen gemeinsam von Wissenschaft, Zivilgesellschaft, Wirtschaft und öffentlichen Institutionen gestaltet werden, statt allein von denjenigen mit den meisten Ressourcen bestimmt zu werden.

So bleibt das Fenster für politische Gestaltung auch morgen noch offen. Welche Zukunft entsteht, entscheidet sich nicht irgendwann, sondern jetzt. Welche Szenarien daraus erwachsen können, zeigt das nächste Video.

Video 5, Was Sie tun können

In einem der Interviews hat eine Bundestagsabgeordnete eine einfache Frage gestellt. Was macht die KI eigentlich auf meinem Computer? Was technisch klingt, ist politisch, denn dahinter stehen vier zentrale Fragen. Wer entscheidet? Wer setzt die Ziele? Wer behält Handlungsmacht? Und wem dient die Technologie?

Ein Forschungsteam des MIT beschreibt hier eine responsibility gap, eine Verantwortungslücke. Diejenigen, die am meisten von KI Risiken betroffen sein könnten, tragen am wenigsten Verantwortung dafür, diese Risiken anzugehen. Anders gesagt, diejenigen, die entscheiden, sind oft am wenigsten betroffen, während diejenigen, die die Folgen tragen, kaum mitentscheiden.

Diese Lücke ist kein rein technisches Problem, sie betrifft demokratische Steuerung und Vertrauen in staatliches Handeln. Es geht also darum, was daraus gemacht wird.

Man kann sich vorstellen, dass ein System Menschen auf Basis einer Vorhersage bewertet, statt auf Basis dessen, was sie tatsächlich getan haben. Man erhält dann eine Entscheidung, aber keine Erklärung. Vorhersagen sind eben keine Fakten. Transparenz, Erklärbarkeit und Verantwortung sind deshalb entscheidend.

KI bietet große Chancen. Entscheidend ist, unter welchen Regeln und in wessen Interesse sie genutzt wird. Ein Blick auf zwei mögliche Zukünfte macht das greifbar.

In der ersten Zukunft, der Fremdbestimmung, setzen nur wenige die Regeln. Die Ziele entstehen dort, wo Technologie entwickelt wird, und nicht dort, wo Menschen von ihr betroffen sind. Menschen erhalten Entscheidungen, aber keine Erklärungen, und die Technologie dient vor allem einzelnen Interessen. Der Alltag könnte so aussehen, dass jemand seinen Briefkasten öffnet und auf die Entscheidung über seinen Bauantrag wartet. Die Entscheidung ist da, doch niemand kann erklären, wie sie zustande gekommen ist. Mit der Zeit entsteht ein Gefühl der Ohnmacht, Entscheidungen wirken wie Naturgesetze, und Vertrauen geht verloren, weil Verantwortung unklar bleibt.

In der zweiten Zukunft, der Mitgestaltung, können Menschen mitentscheiden. Die Ziele werden gesellschaftlich und demokratisch ausgehandelt, Entscheidungen sind nachvollziehbar und anfechtbar, und die Technologie dient dem Gemeinwohl. Der Alltag könnte in diesem Fall so aussehen, dass dieselbe Person denselben Briefkasten öffnet und dieselbe Entscheidung über ihren Bauantrag erhält, diesmal aber nachvollziehen kann, wie sie zustande kam, Fragen stellen und widersprechen kann. Vertrauen entsteht, weil Menschen die Verantwortung behalten.

Keine dieser Zukünfte ist vorgegeben. Sie entsteht durch die Entscheidungen, die heute getroffen werden.

Was können Abgeordnete konkret tun? Erstens können sie Verantwortung einfordern und fragen, wer entscheidet, wer die Verantwortung trägt und wer diese Entscheidungen kontrolliert. Zweitens können sie dafür sorgen, dass über die Ziele von KI demokratisch entschieden wird, sodass Menschen, die die Folgen tragen, daran mitwirken können. Drittens können sie dafür sorgen, dass Menschen Entscheidungen verstehen und ihnen widersprechen können, ein Recht, das bereits existiert, unter anderem in Artikel 22 der Datenschutzgrundverordnung. Viertens können sie politische Rahmenbedingungen schaffen, die festlegen, welchen Zielen KI dienen soll und wo ihre Grenzen liegen.

Man kann dabei an den Mann aus dem ersten Video denken, Mitte vierzig, zwei Kinder, Vollzeitjob. Er wird wahrscheinlich keinen KI Bericht lesen. Aber er wird merken, wenn Entscheidungen nicht nachvollziehbar sind, wenn er keine Wohnung bekommt, keinen Kredit, wenn seine Bewerbung aussortiert wird und niemand ihm sagen kann, warum. Er erhält ein Ergebnis, aber keine Erklärung.

Eine demokratische Zukunft ist eine Zukunft der Mitgestaltung, eine Zukunft, in der die Menschen, die die Folgen tragen, auch mitgestalten können. Dieser Mann trägt die Folgen. Deshalb sollte seine Stimme zählen.

Die jeweiligen Quellen können direkt neben den einzelnen Videos eingesehen werden.