In der öffentlichen Debatte erscheint KI vor allem als ein Effizienzversprechen: weniger Kosten, mehr Automatisierung, „Standortvorteil“. Schaut man aber genauer hin, kippt das Bild: Unternehmen warnen in ihren Pflichtberichten vor KI als Risiko, Sicherheitsforscher sehen kritische Infrastruktur verwundbarer denn je. Wenn nur noch eine kleine Schicht von Experten und Beratern versteht, was auf den Servern läuft, dann entsteht eine neue Abhängigkeit: Wer die Modelle baut und betreibt, bestimmt de facto die Regeln. Von **Günther Burbach**.

Es gibt diesen typischen politischen Moment: Ein Band wird durchschnitten, Kameras klicken, ein „KI-Innovationszentrum“ wird eingeweiht. Im Hintergrund hängen Plakate: „Wettbewerbsfähigkeit“, „Standort sichern“, „Europa an die Spitze“.

Parallel dazu passiert etwas anderes, worüber kaum jemand öffentlich spricht: Unternehmen warnen in ihren Pflichtberichten vor KI als Risiko, Sicherheitsforscher sehen kritische Infrastruktur verwundbarer denn je, Militärs hängen an der Satellitenverbindung eines US-Milliardärs und Parlamente verteilen Milliarden, ohne dass auch nur eine Handvoll Abgeordneter erklären könnte, wie diese Systeme konkret funktionieren.

Die Frage ist nicht mehr: „Kommt KI?“. Sie ist da. Die Frage ist: Wem vertrauen wir und was passiert, wenn dieses Vertrauen enttäuscht wird?

Firmen im KI-Rausch: Produktivität oben, Risiko im Kleingedruckten

In der öffentlichen Debatte wirkt es, als sei KI vor allem ein Effizienzversprechen: weniger Kosten, mehr Automatisierung, „Standortvorteil“. Schaut man aber dahin, wo Unternehmen zur Ehrlichkeit gezwungen sind, in die Pflichtangaben gegenüber Aufsichtsbehörden, kippt das Bild.

In aktuellen US-Börsenberichten verweisen inzwischen Hunderte Konzerne auf KI als Geschäftsrisiko: von fehlerhaften automatisierten Entscheidungen über diskriminierende Modelle bis zu Datenpannen und Haftungsfragen. Das sind keine Kritiker von außen, sondern die Unternehmen selbst, die notgedrungen aufschreiben müssen, was schiefgehen kann, wenn sie ihre Prozesse KI-Systemen überlassen.

Parallel dazu zeigen internationale Umfragen: Ja, KI ist in den meisten großen Firmen angekommen , aber der geschäftliche Nutzen bleibt begrenzt, weil die Systeme kaum sauber in die Arbeitsabläufe eingebettet sind. Frontarbeiter fühlen sich häufiger bedroht als entlastet, und nur eine Minderheit versteht überhaupt, wie die eingesetzten Modelle funktionieren.

Der Kernwiderspruch: Der Investitionsdruck ist enorm, der Verständnishorizont gering. Viele Vorstandsetagen haben Angst, „abgehängt“ zu werden, also kaufen sie lieber, bevor sie verstehen.

Komplexität als Herrschaftsmittel

Genau hier beginnt das politische Problem. Wenn nur noch eine kleine Schicht von Experten, Beratern und Technologiekonzernen versteht, was auf den Servern läuft, dann entsteht eine neue Abhängigkeit: Wer die Modelle baut und betreibt, bestimmt de facto die Regeln.

Die meisten Bürger stehen dieser Entwicklung mit einer Mischung aus Faszination und Unbehagen gegenüber. Sie sehen Deepfakes, Chatbots und automatisierte Entscheidungen, aber niemand erklärt ihnen nachvollziehbar, wer am Ende die Verantwortung trägt. Gleichzeitig wachsen Umfragen zufolge Zweifel an der Verlässlichkeit von KI-Systemen und der Wunsch, bei wichtigen Entscheidungen Menschen statt Maschinen das letzte Wort zu überlassen.

Das Ergebnis ist eine doppelte Entmündigung:

- Die einen werden mit bunten KI-Versprechen ruhiggestellt („Es wird alles smarter“).
- Die anderen erleben KI im Alltag vor allem als Blackbox, die über Kredite, Versicherungen, Wohnungssuche oder Sozialleistungen mitentscheidet – ohne echte Einspruchsmöglichkeit.

Kritische Infrastruktur: Wenn „smarter“ auch verwundbarer heißt

Besonders brisant wird es dort, wo KI in sicherheitskritische Systeme wandert: Energie, Verkehr, Industrieanlagen, Krankenhäuser.

Fachgremien warnen inzwischen offen, dass unkontrollierte Automatisierung mit KI neue Verwundbarkeiten schafft: Jede Entscheidung, die vorher ein erfahrener Mensch traf, wird zur Angriffsfläche, wenn sie von einem lernenden System getroffen wird, das über Netzwerke erreichbar ist.

Gleichzeitig warnen Risikoforscher: KI senkt die Schwelle für Cyberangriffe, macht sie zielgenauer, schwerer nachverfolgbar und damit attraktiver, bis hin zur Bedrohung von Stromnetzen oder Wasserversorgung.

Was heute als „smarte“ Steuerung verkauft wird, kann morgen zum Einfallstor werden, nicht weil KI per se „böse“ wäre, sondern weil man sie in Infrastrukturen presst, die ohnehin schon verwundbar sind.

Die entscheidende Frage lautet also nicht: *„Kann KI unser Netz stabiler machen?“* Sondern: „Wer kontrolliert die Systeme, wer haftet im Ernstfall und welche Redundanzen gibt es, wenn die KI ausfällt oder angegriffen wird?“

Der Starlink-Moment: Wenn ein Privatmann über Kriege mitentscheidet

Wie gefährlich Abhängigkeit wird, sieht man im Krieg. Die Ukraine ist längst darauf angewiesen, dass die Satellitendienste eines Privatunternehmens funktionieren: Starlink liefert Kommunikations- und Dateninfrastruktur für Militär und Zivilbevölkerung. Als es im Sommer zu einem globalen Ausfall des Dienstes kam, waren militärische Verbindungen und Drohnenoperationen der Ukraine für Stunden gestört.

Man kann das aus zwei Perspektiven lesen:

- Ohne Starlink wäre die Ukraine noch verletzlicher, die Technik hat Leben gerettet.
- Ein Softwarefehler in einem US-Konzern reicht aus, um einen Teil der militärischen Kommunikation eines europäischen Landes lahmzulegen, und niemand im Parlament hat darüber wirklich Kontrolle.

Zugleich verhandeln Regierungen über den Ankauf solcher Dienste wie klassische Rüstungsgüter. Damit verschieben sich Machtachsen: Von demokratischer Kontrolle hin zu Vertragsverhältnissen mit privaten Tech-Monopolisten.

Palantir & Co.: Wenn KI zum Grenzregime und Sicherheitsapparat gehört

Auch im Inneren werden KI-Systeme längst nicht nur als „Produktivitätswerkzeuge“ eingesetzt, sondern als Machtinstrumente:

- In der Migrationspolitik kommen immer mehr Systeme zum Einsatz, die Daten von Migrantinnen und Migranten auswerten, Bewegungen prognostizieren oder „Risikoprofile“ erstellen.
- Recherchen zeigen, dass Unternehmen wie Palantir bei europäischen Überwachungs- und Grenzprojekten eine zentrale Rolle spielen, bis hin zur Unterstützung illegaler

Pushbacks und hochvernetzter Überwachung an den EU-Außengrenzen.

Offiziell geht es um „Effizienz“, „verdachtsunabhängige Analyse“ oder „bessere Informationslage“. Real bedeutet es oft: ein weitgehend unsichtbares Kontrollsystem, das mit Daten arbeitet, die Betroffene weder überblicken noch korrigieren können.

Die politische Kommunikation dazu ist, freundlich formuliert, zurückhaltend. Man redet lieber von Start-ups, Innovation und „KI-Standort Europa“, als offen auszusprechen, welche Überwachungsinfrastruktur bereits im Aufbau ist.

Smart Home, Smart City, Smart Control

Die gleichen Muster finden sich im Alltag:

Unter dem Label „Energiesparen“, „Sicherheit“ oder „Komfort“ werden uns Systeme verkauft, die Wohnungen, Städte und Verkehrswege permanent vermessen. Jede smarte Kamera, jedes vernetzte Türschloss, jeder „intelligente“ Zähler erzeugt Daten und damit die Möglichkeit, Verhalten zu analysieren, vorherzusagen, zu sanktionieren.

Die Argumentation ist stets ähnlich:

- Wir wollen den Planeten retten → also brauchen wir detaillierte Verbrauchsdaten.
- Wir wollen Sicherheit → also brauchen wir Gesichtserkennung, Musteranalyse, Verhaltensprofile.

Was selten dazugesagt wird: Wer sitzt eigentlich auf der anderen Seite dieser Datensammlung?

- Öffentliche Stellen, die chronisch unterbesetzt sind?
- Konzerne, deren Geschäftsmodell auf Datenverwertung beruht?
- Sicherheitsbehörden, die schon heute mit Grundrechten auf Kriegsfuß stehen?

Technisch ist die flächendeckende Überwachung keine dystopische Science-Fiction mehr, sondern eine Frage der politischen Entscheidung. Die Bausteine sind da, KI macht sie nur

effizienter und billiger.

Politik zwischen Hype, Hilflosigkeit und Milliardenprojekten

In dieser Lage wäre es Aufgabe der Politik, **Tempo herauszunehmen**, Risiken nüchtern abzuwägen und dort „Nein“ zu sagen, wo der Preis für Demokratie und Grundrechte zu hoch ist. Stattdessen dominiert ein merkwürdiger Mix aus Panik („Wir dürfen nicht abgehängt werden!“) und technischer Ahnungslosigkeit.

Die EU versucht mit dem AI Act zumindest grobe Leitplanken einzuziehen. Gleichzeitig sprechen große Tech-Konzerne in Deutschland und Europa offen davon, Teile der Regulierung seien „toxisch“ für Innovation und werden prompt mit Subventionen für Rechenzentren, Chipfabriken und Datenprojekte bedacht.

Die eigentliche Debatte – Welche KI wollen wir überhaupt, in wessen Besitz und unter wessen Kontrolle – wird nach hinten geschoben. Stattdessen wird der Streit auf juristische Detailfragen verengt: Hochrisiko-System ja/nein, Haftungsfragen, Compliance-Auflagen. Alles wichtig, aber zu kurz gegriffen.

Vertrauen ist keine Strategie

Man kann KI weder dämonisieren noch wegwünschen. Sie wird bleiben, und sie kann in vielen Bereichen sinnvoll sein: in der Medizin, in der Forschung, in der Unterstützung von Routinetätigkeiten, die Menschen ermüden.

Aber all das beantwortet nicht die eigentliche Frage:
Wem vertrauen wir, wenn immer mehr lebenswichtige Entscheidungen über Systeme laufen, die nur wenige beherrschen?

- Vertrauen wir privaten Tech-Konzernen mit globalen Interessen?
- Vertrauen wir Sicherheitsapparaten, die schon heute kaum demokratisch kontrolliert sind?
- Vertrauen wir politischen Entscheidungsträgern, die Hardware einweihen, aber Software nur aus PowerPoint-Folien kennen?

Solange es keine eigenständige, öffentlich kontrollierte digitale Infrastruktur gibt, von Kommunikationsnetzen über Cloud-Ressourcen bis zu offenen KI-Modellen, bleibt jede

Aufrüstung mit KI ein Risiko: für Demokratie, für Souveränität und am Ende auch für die Menschen, die im Namen der Effizienz „optimiert“ werden.

Die eigentliche „Zeitenwende“ wäre nicht, noch mehr Milliarden in KI-Projekte zu pumpen, die niemand durchschaut, sondern zu sagen:

- Es gibt Bereiche, in denen KI nichts verloren hat.
- Es gibt Infrastrukturen, die redundant, analog und menschlich kontrollierbar bleiben müssen.
- Und es gibt eine Grenze, ab der nicht mehr die Frage zählt, wie wir „mitspielen“, sondern ob wir als Gesellschaft überhaupt noch entscheiden, nach welchen Regeln gespielt wird.

Quellen:

- Microsoft „Digital Defense Report 2025“ – PDF des vollständigen Reports.
- Ernst & Young (EY) „Cyber and AI Oversight Disclosures: What Companies Shared in 2025“ – Analyse zur Offenlegung von KI- und Cyberrisiken in großen Firmen.
- “Cyber and AI Oversight Disclosures: What Companies Shared in 2025” – Harvard Law School Forum on Corporate Governance
- “Cybersecurity Snapshot: Top Guidance for Improving AI Risk Management, Governance and Readiness” – Tenable Blog, Oktober 2025
- “Reputation, security, compliance: Why AI risk disclosures are surging” – Journal of Accountancy, Oktober 2025
- “Global Cybersecurity Outlook 2025” – World Economic Forum (WEF) Report

Titelbild: Shutterstock AI Generator – Inhalt wurde von einem Algorithmus mit künstlicher Intelligenz (KI) erstellt / shutterstock.com