

Gruppe B – „Politische Fragen“ (Grün)

Das Wettrüsten Selbst vorsichtige Firmen geraten unter Druck, Sicherheitsmargen zu verkleinern, weil Konkurrenten – andere Firmen, andere Staaten – sonst schneller sein könnten. Ein klassisches Gefangenendilemma. <i>Quelle: Bloomberg, 10.09.2026; Coxon-Statement, TIME, 09.09.2026</i>	Kritische Infrastruktur ist bereits digital Stromnetze, Wasserwerke und Fabriken werden über Steuerungssoftware (SCADA-Systeme) betrieben. Wer diese Systeme kompromittiert, wirkt unmittelbar physisch – ganz ohne Roboter. <i>Quelle: eigene Darstellung (SCADA-Sicherheitsdebatte)</i>
Kapital wird Realität Zugriff auf Finanzmärkte oder Unternehmenskonten könnte genutzt werden, um schrittweise reale Vermögenswerte wie Fabriken oder Rechenzentren zu erwerben oder deren Bau zu beauftragen. <i>Quelle: eigene Darstellung</i>	Der Flaschenhals Robotik (Kritik) Fortschritte bei Robotern hinken der Sprach- und Planungsfähigkeit von KI-Systemen weit hinterher. Mechanische Zuverlässigkeit und Energieversorgung sind harte physische Grenzen. <i>Quelle: eigene Darstellung</i>
Autonome Waffensysteme Militärische Anwendungen wie Drohnenschwärme verbinden KI-Entscheidungen bereits heute direkt mit physischer Gewaltausübung, unabhängig von Zukunftsszenarien. <i>Quelle: eigene Darstellung</i>	Regulierung als Antwort Die EU hat mit dem AI Act ein umfassendes Regelwerk für KI-Risiken geschaffen. Kritiker bezweifeln, ob regionale Regeln gegen globalen Wettbewerbsdruck bestehen können. <i>Quelle: EU AI Act (2024/2026)</i>
Exportkontrollen als politisches Werkzeug Auch der Zugang zu den leistungsfähigsten KI-Modellen selbst wird inzwischen politisch reguliert, etwa durch befristete Zugangsbeschränkungen aus außenpolitischen Gründen. <i>Quelle: eigene Darstellung, vgl. aktuelle Exportkontroll-Debatten 2026</i>	KI als anerkanntes Wirtschaftsrisiko Im aktuellen Allianz Risk Barometer ist KI innerhalb eines Jahres von Platz 10 auf Platz 2 der größten globalen Geschäftsrisiken aufgestiegen. <i>Quelle: Allianz Risk Barometer 2026</i>
Air-Gapping als Gegenmaßnahme (Kritik) Viele kritische Systeme sind bewusst nicht mit dem Internet verbunden oder redundant abgesichert – die tatsächliche Angriffsfläche ist oft kleiner als befürchtet. <i>Quelle: eigene Darstellung, Gegenposition</i>	Screening als Kontrollpunkt (Kritik) Anbieter von DNA-Synthese-Dienstleistungen prüfen Bestellungen; das eigentliche Nadelöhr liegt oft nicht im Wissen, sondern in Laborausrüstung und regulierten Lieferketten. <i>Quelle: eigene Darstellung, Gegenposition</i>

Vertiefungskarten Gruppe B

Menschen als Werkzeug Ein System braucht keinen eigenen Roboterarm, wenn es Menschen durch Bezahlung, Überzeugung oder Täuschung dazu bringen kann, in seinem Sinne zu handeln. <i>Quelle: eigene Darstellung</i>	Biologie als Einfallstor KI-Unterstützung bei der Analyse biologischer Daten könnte die Hürde für die Entwicklung gefährlicher biologischer Substanzen senken – Information wird zu Materie, sobald Labortechnik hinzukommt. <i>Quelle: eigene Darstellung, vgl. Sicherheitsmaßnahmen führender KI-Anbieter</i>
Menschliche Freigabeschleifen (Kritik) Bei den meisten aktuellen autonomen Waffensystemen ist ein „Human-in-the-loop“ vorgesehen, auch wenn dessen tatsächliche Wirksamkeit in der Praxis umstritten bleibt. <i>Quelle: eigene Darstellung, Gegenposition</i>	

