Wissenschaftlicher Beirat des Erhard-Eppler-Kreises

Künstliche Intelligenz und Friedenssicherung

Diskussionspapier

Karl Hans Bläsius, Peter Brandt, Ute Finckh-Krämer, Jasmin S. A. Link, Heinz Stapf-Finé, Christian Weiß

Juli 2026

Dieses Diskussionspapier gibt ausschließlich die Auffassung der Autorinnen und Autoren wieder. Es handelt sich nicht notwendigerweise um eine offizielle Stellungnahme des Erhard-Eppler-Kreises.

Künstliche Intelligenz (KI) ist derzeit eines der in Wissenschaft und Öffentlichkeit am meisten diskutierten Themengebiete. Angesichts der multiplen weltweiten Krisen rückt dabei auch zunehmend die Frage in den Fokus, inwieweit Künstliche Intelligenz für militärische Zwecke eingesetzt werden sollte (Krause 2021). Vor allem ethische Fragestellungen werden in diesem Zusammenhang breit diskutiert (Hawking 2018). Gleichzeitig wird auch immer wieder ein erheblicher Aufholbedarf für Deutschland im internationalen Vergleich, beispielsweise gegenüber China und den USA, diagnostiziert und die Forderung nach einem verstärkten Einsatz dieser Techniken im militärischen Bereich auch in Deutschland erhoben (Zowislo-Grunewald et al. 2026). Das Gefühl eines Aufholbedarfs entsteht dabei durch eine Tendenz zum Folgeverhalten, die als Nebeneffekt von pfadabhängigen Prozessen, wie zum Beispiel der Digitalisierung, hervorgerufen wird (Link 2021). Beim Blick auf die technologische Entwicklung anderer Staaten und ihre Begründungen für die Entwicklung von KI zur Unterstützung der Verteidigungsfähigkeit (Borchert et al. 2024) kann die Wahrnehmung einer Notwendigkeit entstehen, sich dem auch anschließen zu müssen. Gleichzeitig beflügeln Aufrüstungsspiralen eher Konflikte, als dass sie der Friedenssicherung dienen. So ist aus der Aggressionstheorie bekannt, dass die Verfügbarkeit von Waffen die Einsatzwahrscheinlichkeit und damit das Auftreten von bewaffneten Konflikten erhöht (Berkowitz 1993).

Neben der Betrachtung von historischen, militärischen, ethischen, soziologischen und friedenspolitischen Aspekten lohnt bei der Bewertung der Frage, inwieweit der Einsatz von Künstlicher Intelligenz zu militärischen Zwecken ge- oder verboten ist, ein Blick auf die Konsequenzen einer zunehmenden Automatisierung von militärischer Technik. Letztlich handelt es sich nämlich auch beim Einsatz Künstlicher Intelligenz um nichts anderes als eine besonders moderne und ausgefeilte Softwareumsetzung, welche als Innovation die Fähigkeit, aus Erfahrungen zu lernen, sowie eine gewisse selbstständige Anpassung an äußere Umstände umfasst.

Revolution der Kriegsführung durch KI

Im militärischen Bereich gibt es ein großes Spektrum an Automatisierungspotenzial, wobei auch KI-Techniken zum Einsatz kommen, um Zeitverläufe zu verkleinern und Wirkungen zu vergrößern. KI kann nicht nur in Waffensystemen mit immer mehr Autonomie, sondern auch für die Aufklärung, die Erstellung von detaillierten Lagebildern des Gegners, die Auswahl von Zielen und die Planung von Aktionen genutzt werden (Grand-Clément 2023). Der Grad der (Teil-)Autonomie ist dabei unterschiedlich (Unterscheidung nach Beck 2026):

- KI wird eingesetzt zur Aufklärung und Informationsverarbeitung. Hierbei werden Satellitenbilder ausgewertet oder Muster in Kommunikationsdaten aufgedeckt.
- Entscheidungsunterstützungssysteme beeinflussen, welche Ziele für militärische Angriffe in den Blick geraten. Das Entscheidungsfenster für menschliche

Entscheider ist hierbei stark vorstrukturiert, oft unter enormem Entscheidungsdruck.

- Schließlich existieren (teil-)autonome Waffensysteme, die eigenständig bestimmte kriegerische Handlungen ausführen können.

Eine Gemeinsamkeit ist bei allen Einsatzfeldern, dass sich die Kontrolle über die Informationen auf die KI-Systeme beziehungsweise auf deren technologische Bereitsteller verschiebt, und der Mensch angesichts der Masse von Informationen kognitiv überfordert ist. Daneben gibt es Merkmale, die bisher wenig beachtet und diskutiert werden, die in der Debatte um die Nutzung von KI für militärische Aufgaben jedoch Berücksichtigung finden sollten:

1. KI kann auf der Grundlage von automatischen Entscheidungen oder noch zu bestätigenden Vorentscheidungen militärische Abläufe erheblich beschleunigen. Diese Entscheidungen können allerdings auch falsch sein und sind nicht zwangsläufig besser als Entscheidungen von Menschen.
2. Die Fähigkeiten eines Gegners bezüglich KI-Anwendungen sind weitgehend unbekannt. Kräftevergleiche sind nur schwer möglich, was leicht zu Fehlkalkulationen und unkontrollierbarem Wettrüsten führen kann.
3. Die klassischen Methoden der Rüstungskontrolle greifen bei KI-basierten Technologien nicht.
4. Die Integration von KI-basierten Entscheidungen in die Befehlskette kann zusätzliche Schnittstellen für eine Manipulation schaffen und zu Blockaden der grundsätzlichen Handlungs- und Einsatzfähigkeit führen.
5. Technologische Abhängigkeiten können die Fähigkeiten zur eigenständigen Entscheidungsfindung schwächen und zum Beispiel über Standortsignale Strategien verraten.
6. Eine Integration von KI-Systemen im militärischen Bereich kann daher im Extremfall nicht zu einer Stärkung, sondern zur Schwächung der eigenen Fähigkeiten führen.

Schnellere Entscheidungen, aber nicht notwendig bessere

In der öffentlichen Diskussion wird oft der Eindruck vermittelt, dass KI deutlich besser geeignet sei, um riesige Datenmengen und eine höhere Komplexität zu bewältigen und deswegen zur Entscheidungsfindung grundsätzlich zu bevorzugen sei. Dies ist aber trügerisch, denn Abläufe können zwar erheblich beschleunigt werden, aber Entscheidungen sind nicht notwendig besser, bloß weil sie schneller und auf der Basis von mehr Daten getroffen werden. Das Problem der Unsicherheit der Informationsgrundlage lässt sich nicht mit KI lösen, unabhängig von deren technischem Reifegrad. Aus unsicheren Informationen können prinzipiell keine sicheren Schlüsse gezogen werden (Evans et al. 2015).

Richtig ist hingegen, dass mithilfe von KI riesige Datenmengen in kurzer Zeit verarbeitet und für Entscheidungen genutzt werden können. Solche Entscheidungen basieren auf einer großen Vielfalt von unterschiedlichen Erkennungsaufgaben. Dazu gehören zum Beispiel die Erkennung angreifender Flugobjekte, sowie zugehöriger Merkmale wie Objekttyp, Position, Richtung und Geschwindigkeit, aber auch Truppenbewegungen, Erkenntnisse aus Geheimdienstinformationen, Unterscheidung von Freund und Feind, Unterscheidung von Kombattanten und zivilen Personen und so weiter. Das Problem hierbei ist, dass die Kriterien, die für solche Erkennungsaufgaben nutzbar sind, oft vage, unsicher und unvollständig sind.

Vage Kriterien können beispielsweise die Größe von Objekten und die Helligkeit von Signalen betreffen, wobei auch uneindeutige Zwischenwerte auftreten können. Mit anderen Worten können vage Merkmale nicht einfach nur durch die beiden Möglichkeiten „wahr“ oder „falsch“ beschrieben werden, sondern es kann auch etwas dazwischen auftreten. Bei unsicheren Kriterien kann nur eine Wahrscheinlichkeit dafür bestimmt werden, ob sie „wahr“ oder „falsch“ sind. Deshalb können Erkennungsaufgaben meistens nicht vollständig zuverlässig gelöst werden und es sind keine sicheren Entscheidungen möglich (Bläsius 2026).

Ein Beispiel hierfür ist die Unterscheidung von Kombattanten und zivilen Personen. Als ein Erkennungsmerkmal kann in diesem Fall etwa gelten, dass Kombattanten häufiger einen Helm tragen als zivile Personen. Die Unsicherheit tritt in diesem Fall doppelt auf. Die Erkennung, ob eine Person einen Helm trägt, ist bereits als solche mit Unsicherheit behaftet. Ein Bild kann Merkmale enthalten, die auf einen Helm deuten, aber die Interpretation kann auch falsch sein, denn es ist zum Beispiel eine Verwechslung mit einer Mütze denkbar. Aus dem bloßen Tragen eines Helmes wiederum den Schluss zu ziehen, dass es sich um einen Kombattanten handelt, ist ebenfalls unsicher, denn zum Beispiel werden Helme auch häufig beim Bauhandwerk verwendet. Im Ergebnis wird von KI-Systemen also nur eine Wahrscheinlichkeit berechnet, dass es sich bei der untersuchten Person um einen Kombattanten handelt. Dadurch kann es folglich zu tragischen Fehlschlüssen kommen, die aufgrund der verwendeten Technik unvermeidbar sind.

Als weitere Schwierigkeit kommt hinzu, dass militärische Gegner üblicherweise viel dafür tun, eine Erkennung zu erschweren. Tarnen und Täuschen gehörte schon immer zu den Grundprinzipien des Militärs. Ein Gegner kann darüber hinaus sogar selbst KI einsetzen, um eine Erkennung zu erschweren. Insgesamt wird das Niveau der Unsicherheit dadurch weiter erhöht.

Erkennungssysteme basieren zudem häufig auf Deep Learning mit riesigen Lerndatenmengen. Deswegen hängt die Qualität der Systeme entscheidend von der Qualität dieser Daten ab. Verzerrungen, veraltete Daten oder bewusste Manipulationen mit gefälschten Daten können die Erkennung erschweren oder zu falschen Ergebnissen führen (Szegedy et al. 2013). Wenn es keine adäquaten Daten gibt, mit denen KI-Systeme trainiert werden könnten, was beispielsweise in Bezug auf Atomwaffen der Fall ist (Richard/El Moubayed 2026), vergrößert sich das Risiko, dass die KI falsche Ergebnisse liefert – im Fall von Atomwaffen mit unabsehbaren Folgen für die gesamte Menschheit.

In manchen Fällen könnten automatische Entscheidungen besser als diejenigen sein, die

ein Mensch treffen würde. Wie dargelegt, wird es in anderen Fällen jedoch umgekehrt sein. Da militärische Abläufe mit Hilfe von KI aber erheblich beschleunigt werden, wird zunehmend für Menschen die Zeit fehlen, KI-Entscheidungen zu prüfen und gegebenenfalls korrigierend und mäßigend einzugreifen, zum Beispiel um Eskalationsspiralen zu verhindern.

Mangelnde Transparenz über Fähigkeiten

In der Vergangenheit hat ein Kräftevergleich zwischen den Militärmächten für Transparenz und ein gewisses Maß an Sicherheit gesorgt. Soldaten, Panzer, Flugzeuge und Schiffe konnten gezählt und verglichen werden und solche Zahlen konnten auch Grundlage für Vereinbarungen sein. 1992 wurde zwischen NATO-Staaten und Staaten der ehemaligen UdSSR der Open-Skies-Vertrag geschlossen, der gegenseitige Kontrollen militärischer Objekte erlaubte und so dem Anliegen diente, die Transparenz von Fähigkeiten zu verbessern und damit Vertrauen aufzubauen. Aus diesem Vertrag sind die USA 2020 ausgestiegen. Russland schloss sich diesem Schritt 2021 an.

Bei softwarebasierten Waffen wie KI- und Cyberwaffen fehlt eine solche Transparenz (Boulanin et al. 2017). Die Fähigkeiten eines Gegners im Bereich KI und im Cyberraum sind unbekannt. Selbst bei einem Einsatz, wie zum Beispiel bei den Kriegen in Gaza und dem Iran, werden meist nur Teilfunktionen verwendet. Die Systeme können viele weitere Fähigkeiten enthalten, die nicht sichtbar werden. Auch die eigenen Fähigkeiten können nicht vollständig bekannt sein. Darüber hinaus können Cyberwaffen meist nicht in realen Umgebungen getestet werden, weil das Risiko von Kollateralschäden zu groß wäre. Zum Beispiel hat der 2010 entdeckte Angriff von Seiten der USA und Israels mit dem Schadprogramm Stuxnet auf eine Urananreicherungsanlage im Iran erhebliche Kollateralschäden verursacht. Versehentlich sind dabei mehr als 50.000 Computer in Indien, Indonesien, Pakistan und weiteren Staaten infiziert worden (Schneier 2015). Wenn die gegnerischen Fähigkeiten unbekannt sind und dies – in abgeschwächter Form – auch für die eigene Fähigkeiten gilt, kann es leicht zu Fehleinschätzungen kommen, die in Krisenzeiten zu Handlungen mit gravierenden Folgen führen könnten. Eine zu groß gewachsene Infrastruktur mit vernetzten KI-Komponenten und mobilem Serverzugriff kann zu strukturellen Schwachstellen hinsichtlich manipulierbarer Kommunikationsketten und Datenströme oder teilweisem oder vollständigem Ausfall der Struktur führen.

Rüstungskontrolle

In den Bereichen Cyberraum und KI ist eine Rüstungskontrolle im klassischen Sinne somit kaum möglich, weil die entsprechenden Systeme im Wesentlichen auf Software und Daten beruhen. Trotzdem gibt es dazu auf der Ebene der Vereinten Nationen diverse Aktivitäten, die sowohl den zunehmenden Einsatz von KI in militärischen Systemen und in bewaffneten Konflikten als auch die Konsequenzen der zivilen Nutzung von KI für Frieden und Sicherheit adressieren (Bruun et al. 2026). Es zeichnet sich ab, dass Verhaltensregeln und vertrauensbildende Maßnahmen als Ansatzpunkt genommen werden, um Rüstungswettläufe und unbeabsichtigte Eskalationen zu verhindern. In

Bezug auf tödliche autonome Waffensysteme (Lethal Autonomous Weapon Systems, LAWS) wurde seit 2017 mehrfach im Rahmen einer Gruppe von Regierungsexpertinnen und -experten über Definitionen und mögliche Regeln für den Einsatz derartiger Waffensysteme diskutiert, auch unter dem Aspekt der Vereinbarkeit mit dem humanitären Kriegsvölkerrecht (Bruun et al. 2026, S. 438 ff).

Zunehmender Kontrollverlust

Im militärischen Gefecht kann eine höhere Handlungsgeschwindigkeit eine höhere Überlebenswahrscheinlichkeit bedeuten. Von einer Nutzung von KI in kriegerischen Situationen erhofft man sich daher militärische Vorteile, insbesondere wenn Entscheidungs- und Handlungsprozesse dadurch immer schneller ablaufen. Diese Vorteile bestehen jedoch nur, solange sichergestellt werden kann, dass die Stoßrichtung der Aktionen dem operationalen Ziel entspricht. In der internationalen Diskussion wird derzeit noch überwiegend gefordert, dass bei Waffeneinsätzen mit Tötungsfolgen ein Mensch in der Entscheidungsschleife sein muss (Bruun et al. 2026, S. 440ff). Jedoch stellt sich die Frage, ob die einem Menschen vorliegenden Informationen und die verfügbare Zeit reichen, um angemessen in einen automatisierten Ablauf eingreifen zu können.

Zusätzlich zum technisch bedingten Kontrollverlust, der mit zunehmender Automatisierung entsprechend wächst, gibt es noch einen hierarchiebedingten Kontrollverlust, der mit der Einführung von KI einhergeht. Bei der Integration von KI in die Befehlskette stellt sich die Frage: Wem vertraut man mehr, Mensch oder Maschine? In dem Moment, in dem sich in einem Einsatz diese Frage stellt, bedeutet ein Nachdenken einen Zeitverlust und möglicherweise eine geringere Überlebenswahrscheinlichkeit. Also muss auch die Beantwortung dieser Frage vortrainiert sein. Bei KI-Komponenten, insbesondere solchen, die auf generativer KI aufbauen, lässt sich allerdings nicht sicher nachvollziehen, welche Datengrundlage die KI genau in welcher Form verwendet hat, um eine konkrete Entscheidung zu treffen (Akyurek et al. 2017). Wenn den Ergebnissen von KI-Anwendungen blind vertraut wird, entscheidet de facto die KI und nicht mehr ein Mensch, auch wenn offiziell Menschen die Verantwortung für die Einsätze tragen müssen.

Je mehr KI-Elemente in die Befehlskette integriert sind, umso schwieriger ist es für die Beteiligten, auf eine funktionierende rein menschliche Befehlskette zurück zu schwenken (Pfadabhängigkeit, Link 2018). Wenn der Zugriff auf die KI-Antworten über ein digitales Endgerät erfolgt, eröffnet diese digitale Schnittstelle in der Befehlskette zudem Möglichkeiten für Manipulationen von außen und im schlimmsten Fall sogar feindliche Übernahmen.

Solche Gefahren werden auch beim Militär gesehen, und werden zum Beispiel bei der Konferenz des Joint Air Power Competence Centre (JAPCC) diskutiert. In der Ankündigung heißt es übersetzt: „Wie können wir Soldaten befähigen, Vertrauen in maschinelle Ergebnisse aufzubauen, Voreingenommenheit und Manipulation zu erkennen und sinnvolle Kontrolle zu behalten, während sich das Tempo der Operationen der Geschwindigkeit von Maschinen annähert?“ (JAPCC 2026, eigene Übersetzung)

Technologische Abhängigkeiten gefährden die Sicherheit

Ein technologisches Gerät zu verwenden, das die eigenen Fähigkeiten ergänzt oder erweitert, birgt die Gefahr von diesem abhängig zu werden. In Bezug auf KI-Systeme betrifft das insbesondere die eigenständige Bilderkennung, die eigenständige (schnelle) verantwortungsvolle Entscheidungsfindung, das Vertrauen auf das eigene Team und die Teamkompetenz. Die gesunkenen individuellen Fähigkeiten können die Funktionsweise ganzer Befehlsketten und Gruppenoperationen schwächen. Dieser Effekt ist für hoch technologisierte Kontrahenten oder Technologiekonzerne möglicherweise schneller messbar oder prognostizierbar als es für die realen Teampartner erkennbar ist. Folglich müsste es begleitend zur technologischen Einführung ein internes Monitoring der generierten Abhängigkeiten und eine Prognose über deren Auswirkungen geben.

Politische Folgerungen

Aufrüstung wird derzeit in vielen Staaten enorm vorangetrieben und die Ausgaben für neue Waffensysteme steigen massiv an. In künftigen Kriegen werden Fähigkeiten im Zusammenhang mit KI und im Cyberraum eine zentrale Rolle spielen. Die Unsicherheit darüber, in welchem Umfang andere Staaten bereits im Bereich KI aufgerüstet haben, dabei sind, oder befähigt sind, dies zu tun, führt dazu, dass die Kapazitäten und Fähigkeiten der anderen eher über- als unterschätzt werden. Dies hat wiederum zur Folge, die eigene Einstiegsnotwendigkeit tendenziell zu überschätzen, sowohl in der Einschätzung der Handlungsgeschwindigkeit als auch im Umfang der Investitionen. Es ist derzeit jedoch noch gar nicht absehbar, wie man sich gegen angenommene oder tatsächliche KI-Fähigkeiten anderer schützen kann, weil die tatsächlichen Fähigkeiten eines Gegners in diesem Bereich weitgehend unbekannt bleiben werden. Die derzeitige massive Aufrüstung liefert daher keine Lösungen, sondern erhöht die Sicherheitsrisiken zusätzlich. Kriege sind heutzutage zudem selten auf die beteiligten Staaten begrenzt, sondern können weltweite Folgen haben. Dies gilt insbesondere für wirtschaftliche Aspekte sowie den Cyberraum und schlimmstenfalls auch bei einem eventuellen Einsatz von Atomwaffen. Aufgrund der zunehmenden globalen Auswirkungen von bewaffneten Konflikten sowie einer Technikentwicklung, die absehbar zu menschlichem Kontrollverlust führen wird, muss die Institution Krieg überwunden werden.

Auf dem Weg dahin wäre ein internationales Übereinkommen notwendig, das autonome Waffensysteme verbietet, wie beispielsweise vom Internationalen Komitee des Roten Kreuz gefordert (ICRC 2021). Dass die meisten Staaten in den letzten Jahren entsprechende Resolutionen in der Generalversammlung der Vereinten Nationen mitgetragen haben und Generalsekretär Guterres im Juni 2025 einen Bericht über militärische Anwendungen von KI und ihre Auswirkungen auf Frieden und Sicherheit veröffentlicht hat, ist ein gutes Zeichen (Bruun et al. 2026, S. 443 ff). Um Risiken zu reduzieren sind wirksame weltweite Vereinbarungen erforderlich. Dafür muss die Diplomatie, auch und gerade auf der Ebene der Vereinten Nationen, gestärkt werden.

Referenzen

Akyurek, Ekin; Bolukbasi, Tolga; Liu, Frederick; Xiong, Binbin; Tenney, Ian; Andreas, Jacob; Guu, Kelivn. Towards Tracing Knowledge in Language Models Back to the Training Data. Findings of the Association for Computational Linguistics: EMNLP 2022. 2022.

Beck, Susanne. Illusion der Beherrschbarkeit. Rechtliche Verantwortung bei der Nutzung (teil)autonomer Waffensysteme im Krieg. In: APuZ 29-30/2026, S. 22-27, https://www.bpb.de/shop/zeitschriften/apuz/militaer-2026/579529/illusion-der-herrschbarkeit/.

Berkowitz, Leonard. Aggression: Its causes, consequences, and control. McGraw-Hill Book Company, 1993.

Bläsius, Karl Hans. Künstliche Intelligenz und Krieg, Springer Verlag, 2026, Kapitel 2.

Borchert, Heiko; Torben Schutz; Joseph Verbovszky. The very long game: 25 case studies on the global state of defense AI. Springer Nature, 2024.

Boulanin, Vincent; Verbruggen, Maaike. Mapping the Development of Autonomy in Weapon Systems, 2017. SIPRI. https://www.sipri.org/publications/2017/other-publications/mapping-development-autonomy-weapon-systems.

Bruun, Laura; Palayer, Jules; Boulanin, Vincent. Artificial intelligence and international peace and security. In: SIPRI Yearbook 2026: Armaments, Disarmament and International Security, S. 437-459. https://www.sipri.org/sites/default/files/YB26%2014%20AI%20Governance.pdf.

Evans, Jonhathan; Thompson, Valeria; Over, David. Uncertain deduction and conditional reasoning. Frontiers in Psychology, 6, 398, 2015.

Grand-Clément, Sarah. Artificial Intelligence Beyond Weapons: Application and Impact of AI in the Military Domain. United Nations Institute for Disarmament Research (UNIDIR), Genf, 2023. https://unidir.org/publication/artificial-intelligence-beyond-weapons-application-and-impact-of-ai-in-the-military-domain/.

Hawking, Stephen. Kurze Antworten auf große Fragen. Klett-Cotta, 2018.

International Committee of the Red Cross (ICRC). ICRC position on autonomous weapon systems. Online 2021. https://www.icrc.org/en/document/icrc-position-autonomous-weapon-systems.

Link, Jasmin S.A. Induced Social Behavior: Can Path Dependence or Climate Change induce Conflict? Dissertation, 2018.

Link, Jasmin S.A. Pfadabhängigkeit und Lock-in. In: Schmiedchen, Frank et al. Wie wir leben wollen. Kompendium zu Technikfolgen von Digitalisierung, Vernetzung und Künstlicher Intelligenz 2021, S. 61-81.

JAPCC, Joint Air and Space Power Conference 2026, Panel 4, https://www.japcc.org/conference/#conference-panels

Krause, Ulf. Künstliche Intelligenz im Militär. Springer Gabler. Book, 2021.

Schneier, Bruce. Data und Goliath - Die Schlacht um die Kontrolle unsere Welt, Redline Verlag, 2015.

Szegedy, Christian; Zaremba, Wojciech; Sutskever, Ilya; Bruna, Joan; Erhan, Dumitru; Goodfellow, Ian; Fergus, Rob. Intriguing properties of neural networks, arXiv preprint arXiv:1312.6199, 2013.

Richard, Ulysse; El Moubayed, Yorgo. AI nuclear decision making has a data problem. Bulletin of the Atomic Scientists, https://thebulletin.org/2026/04/ai-nuclear-decision-making-has-a-data-problem/.

Zowislo-Grunewald, Natascha; Beitzinger, Frank; Gehringer, Ferdinand Alexander; Spreen, Dierck. Mehr KI für Verteidigung und Resilienz. Konrad-Adenauer-Stiftung, 2026. https://www.kas.de/de/analysen-und-argumente/detail/-/content/mehr-ki-fuer-verteidigung-und-resilienz.