

KI in der Verteidigung: zwischen Ambition und Realität

Eine multiperspektivische Meta-Analyse



**Wir
gestalten
Zukunft**

VDI Research

Bild: © Getty Images/gorodenkoff

KI in der Verteidigung: zwischen Ambition und Realität

Eine multiperspektivische Meta-Analyse

Executive Summary

KI verändert den Verteidigungssektor grundlegend – doch die Kluft zwischen politischer Rhetorik und operativer Wirklichkeit ist erheblich.

Dieses Research Paper des VDI Technologiezentrums wertet sechs Leitquellen und 25 nationale Fallstudien aus und destilliert fünf Kernbefunde:

1. Evolution, nicht Revolution. Streitkräfte scheitern nicht an fehlender Technologie, sondern an Bürokratie, Datenmangel und Kulturwandel.
2. Kontrolle: gefordert, nicht gesichert. „Meaningful human control“ ist Konsens – die technischen Voraussetzungen fehlen.
3. Recht hinkt hinterher. Völkerrecht und Exportkontrollen greifen bei dual-use-fähiger, softwarebasierter KI kaum.
4. Low-Tech schlägt Hightech. Kommerzielle Drohnenschwärme mit Open-Source-KI sind operative Realität – Gegenmaßnahmen fehlen.
5. Doppelte Agenda für Deutschland: Souveränität im Spitzensegment und Robustheit gegen asymmetrische KI-Bedrohungen.

Der ganz zentrale Befund: Die KI-Transformation der Verteidigung ist kein Technologieproblem – sie ist ein Organisationsproblem ...

Das VDI Technologiezentrum versteht sich in dieser Gemengelage als Brückenbauer – zwischen ziviler Innovation und verteidigungspolitischem Bedarf, zwischen technologischer Analyse und politischer Einordnung, zwischen Normung und operativer Realität. Als Innovationsagentur und Clustermanager Defence NRW bringt es die Fähigkeit mit, die technologischen, organisatorischen und normativen Dimensionen dieser Transformation nicht nur einzeln zu bewerten, sondern integriert zu denken und handlungsfähig zu machen.

Einführung

Die Integration Künstlicher Intelligenz (KI) in den Verteidigungssektor wird weltweit als eine der folgenreichsten technologischen Transformationen des 21. Jahrhunderts bewertet. Doch zwischen politischer Rhetorik und operativer Wirklichkeit klafft eine erhebliche Lücke.

Für Entscheiderinnen und Entscheider und jene, die sich im schnellen Wandel der Felder der KI und der Sicherheit und Verteidigung orientieren wollen, sind Informationen oftmals nur auf einer oberflächlichen, tagesaktuellen und notwendigerweise unbeständigen Ebene zugänglich. Hier ist Vermittlung gefragt, die Praxiswissen mit Empirie und Theorie verbinden kann.

Die vorliegende Meta-Analyse nimmt die Diskrepanz zwischen zunehmender Anwendung KI-basierter Systeme und der mangelnden Auseinandersetzung mit dieser Technologie zum Ausgangspunkt und untersucht auf Grundlage von sechs aktuellen Leitquellen, wie sich der globale Diskurs zu Verteidigungs-KI tatsächlich darstellt – jenseits von Schlagzeilen und Zukunftsversprechen. Sie verfolgt dabei ein doppeltes Ziel: Sie bietet erstens eine evidenzbasierte Bestandsaufnahme des globalen Diskurses zu Verteidigungs-KI und leitet daraus zweitens konkrete Implikationen für Forschung, Entwicklung und Innovation ab.

Den konzeptionellen Rahmen liefert dabei die Studie **The Very Long Game** von Borchert, Schütz und Verbovszky (2024), die 25 nationale Fallstudien zum gegenwärtigen Stand von KI im Verteidigungsbereich systematisch vergleicht. Ihr zentraler Befund lautet: **KI ist nicht als singuläre Technologie zu verstehen, sondern als ein Werkzeugkasten heterogener Methoden** – von maschinellem Lernen über Computer Vision bis hin zu Natural Language Processing. Der operative Fokus der meisten Nationen liegt derzeit auf der sogenannten „zweiten Welle“ der KI, also auf korrelativem Lernen aus großen

Perspektive	Quelle	Funktion in der Meta-Analyse
Politisch-normativ	UN-Resolution 79/239 (2024) UN-Generalsekretärsbericht A/80/78 (2025)	Globaler Konsens und Dissens zur Normsetzung; multilateraler Ordnungsrahmen
Strategisch-vergleichend	Borchert/Schütz/Verbovszky: The Very Long Game (2024)	Empirischer Realitätscheck durch 25 nationale Fallstudien; DOTLMPFI-Systematik
Technisch-ethisch	SIPRI: AWS und AI-DSS (2025) CNTR Monitor (2025)	Differenzierte Technologieanalyse; Rüstungskontrollperspektive; geopolitische Einordnung
Implementierungsorientiert	EC AI Factsheet (2025)	Umsetzung strategischer Prinzipien in konkrete EDF-geförderte Projekte

Datenmengen, während die „dritte Welle“ – kontextbezogenes Denken und autonomes Selbstlernen – sich noch in einem frühen Forschungsstadium befindet.

Anstatt über zukünftige Möglichkeiten zu spekulieren, konzentriert sich **The Very Long Game** auf die gegenwärtige Praxis und strukturiert die Analyse entlang der DOTLMPFI-Handlungsfelder (Doctrine, Organization, Training, Leadership, Material, Personnel, Facilities, Interoperability). Diese Systematik verdeutlicht, dass die Einführung von KI in den Streitkräften weit mehr erfordert als technologische Forschung: Sie verlangt eine tiefgreifende konzeptionelle, organisatorische und kulturelle Transformation. Der Übergang von rein menschlicher Operationsführung zu einer komplexen Mensch-Maschine-Interaktion ist, so die Autoren, ein langwieriger evolutionärer Prozess – „a very long game“ – der ein umfassendes Überdenken militärischer Macht in all ihren Dimensionen erfordert.

Dieser Befund motiviert die vorliegende Meta-Analyse: Wenn die Einführung von Verteidigungs-KI tatsächlich ein derart vielschichtiger Transformationsprozess ist, dann muss auch die analytische Bewertung multiperspektivisch angelegt sein.

Als Innovationsagentur versteht das VDI Technologiezentrum die strukturierte Bewertung

technologischer Transformationsprozesse – vom strategischen Rahmen über die organisatorische Implementierung bis zur operativen Einführung – als wichtige Kernkompetenz und Beitrag zur informierten Politikberatung im Bereich Verteidigung und Sicherheit.

Quellenauswahl und strukturelle Verbindungen

Die Auswahl der sechs analysierten Quellen begründet sich durch ihre systematische Multiperspektivität. Sie decken das gesamte Spektrum der Debatte ab – von der globalen Normsetzung über institutionelle Strategien bis hin zu detaillierten nationalen Fallstudien (siehe Tabelle oben).

Die Quellen bilden in ihrer Gesamtheit eine komplementäre Informationsgrundlage zur Debatte über KI in der Verteidigung. Ausgehend von ihren strukturellen Verbindungen werden durch eine multiperspektivische Meta-Analyse wiederkehrenden Thesen, Widersprüche sowie Lücken in der Debatte identifiziert und im Überblick dargestellt.¹ Daraus werden abschließend zentrale Stoßrichtungen für Forschung, Entwicklung und Innovation abgeleitet.

Strukturelle Verbindungen

Die UN-Resolution 79/239 (2024) bildet den politischen Auslöser für den Generalsekretärsbericht A/80/78 (2025), der als Sammlung

¹ Die UN-Resolution 79/239 bildet den politischen Auslöser für den Generalsekretärsbericht A/80/78. SIPRI vertieft die konzeptionelle Unterscheidung zwischen AWS und AI-DSS, die in den UN-Dokumenten gefordert, aber nicht ausgeführt wird. Das EC AI Factsheet stellt konkrete im EDF geförderte Projekte vor und verdeutlicht damit die Übersetzung abstrakter Prinzipien in die Implementierungspraxis. Der CNTR Monitor ergänzt die geostrategische Dimension (Halbleiter-Lieferketten, Innovationswettbewerb). The Very Long Game liefert den empirischen Realitätscheck durch 25 nationale Fallstudien.

nationalen Positionen und Stakeholder-Beiträge die in der Resolution geforderte Bestandsaufnahme liefert. SIPRI (2025) vertieft analytisch die Unterscheidung zwischen autonomen Waffensystemen (AWS) und KI-gestützten Entscheidungsunterstützungssystemen (AI-DSS), die in den UN-Dokumenten gefordert, aber nicht im Detail ausgeführt wird – und schließt damit eine konzeptionelle Lücke der politisch-normativen Debatte.

Das EC AI Factsheet (2025) zeigt exemplarisch, wie eine Staatengruppe – die Europäische Union (EU) – strategische Prinzipien in konkrete, im Rahmen des Europäischen Verteidigungsfonds (EDF) geförderte Projekte übersetzt und damit den Brückenschlag von der Norm zur Implementierung vollzieht. Der CNTR Monitor (2025) ergänzt die geostrategische und geoökonomische Dimension, die in den eher politisch-rechtlich fokussierten Dokumenten fehlt – insbesondere die Analyse globaler Halbleiter-Lieferketten, das Konzept des „geopolitischen Innovationswettlaufs“ und die rüstungskontrollpolitische Einordnung neuer Dual-Use-Technologien.

The Very Long Game (2024) dient schließlich als umfassender Realitätscheck für die oft abstrakten politischen Ambitionen der anderen Dokumente. Die 25 nationalen Fallstudien zeigen, dass die in den UN-Berichten und bei SIPRI diskutierten Herausforderungen – Bürokratie, kulturelle Widerstände, Datenmangel, fragmentierte Beschaffungsprozesse – in der Praxis die Hauptbremsklötze der KI-Transformation darstellen.

Wiederkehrende Thesen, Widersprüche und Evidenz

Die systematische Gegenüberstellung der sechs Quellen offenbart sowohl bemerkenswerte Konvergenzen als auch signifikante Spannungsfelder. Im Folgenden werden diese entlang von fünf Leitdimensionen analysiert – menschliche Kontrolle, völkerrechtliche Rahmung, technologischer Reifegrad, Dual-Use-Regulierung und strategische Stabilität – und mit Erkenntnissen aus der operativen Realität aktueller Konflikte konfrontiert.

Konsentzierte Kernthesen

These 1: Der Mensch-im-Zentrum-Ansatz als universelles Paradigma

Alle sechs Dokumente betonen die Notwendigkeit eines „**human-centric approach**“: Demnach bilden menschliche Kontrolle, Verantwortung und Rechenschaftspflicht das normative Fundament der gesamten globalen Debatte. Die UN-Resolution (2024) fordert explizit die Wahrung menschlicher Urteilsfähigkeit über Gewaltanwendung; SIPRI differenziert zwischen der direkten Autonomie von AWS und der indirekten Beeinflussung durch AI-DSS; **The Very Long Game** dokumentiert, dass selbst technologisch ambitionierte Nationen wie Israel oder Südkorea den Mensch-Maschine-Schnittstellen zentrale Bedeutung beimessen. Die Notwendigkeit menschlicher Kontrolle wird durch die Erkenntnis verschärft, dass KI durch die Beschleunigung von Entscheidungsprozessen das Risiko von Fehlkalkulationen erhöht. Der CNTR Monitor diagnostiziert eine „**Kriegsführung im Prozessortakt**“; SIPRI identifiziert den **automation bias** als zentralen indirekten Risikopfad.

Für Forschung und Entwicklung (FuE) bedeutet dies: Human-Machine Teaming, Explainable AI (XAI) und kognitionswissenschaftlich fundierte Schnittstellenentwicklung sind keine optionalen Zusätze, sondern konstitutive Anforderungen an jedes verteidigungsrelevante KI-System.

These 2: Anwendbarkeit des bestehenden Völkerrechts

Es herrscht breiter Konsens, dass das humanitäre Völkerrecht (IHL) auf den gesamten Lebenszyklus militärischer KI anwendbar ist (UN24, UN25, SIPRI). Der SIPRI-Bericht betont dabei, dass die Verantwortung stets beim Menschen verbleibt – auch wenn das „**many hands problem**“, also die Verteilung von Verantwortung über Entwickler, Kommandeure und Bediener, die Zurechenbarkeit im Einzelfall erheblich erschwert.

These 3: KI als Befähigerin jenseits autonomer Waffen

Die Diskussion hat sich merklich von der engen Fokussierung auf letale autonome Waffensysteme (LAWS) zu einem breiteren Verständnis von KI als „**Force Multiplier**“ und „**Enabler**“ verschoben. Das EC AI Factsheet listet An-

wendungen von Echtzeit-Lagebildern über Logistikoptimierung bis zu Cybersicherheit auf; der UN-Bericht (2025) identifiziert Aufklärung, Kommandoführung, unbemannte Systeme und Wartung als zentrale Einsatzfelder. **The Very Long Game** bestätigt empirisch, dass die meisten Nationen KI primär in unterstützenden Funktionen einsetzen – Deutschland etwa betrachtet KI gemäß dem Kapitel „Herr und Diener“ primär als unterstützendes Werkzeug, nicht als eigenständige Akteurin. Das EC AI Factsheet bestätigt diesen breiten Anwendungsfokus auf Implementierungsebene: Der Europäische Verteidigungsfonds (EDF 2025–2027) investiert gezielt in Echtzeit-Lagebilder (AI4DEF), automatisierte Bedrohungserkennung (PANDORA, AIDEDex), Cybersicherheit (EU-GUARDIAN) und Mensch-Maschine-Interaktion (LODESTAR) – und übersetzt damit den in allen Quellen konstatierten „Enabler“-Ansatz in konkrete EDF-Projekte.

These 4: Dual-Use als strukturelles Regulierungsproblem

Der Dual-Use-Charakter von KI durchzieht alle Quellen als Leitmotiv. Der CNTR Monitor warnt, dass Foundation Models die Hürden für fortgeschrittene militärische Funktionen senken und traditionelle Rüstungskontrollansätze – konzipiert für materielle, zählbare Waffensysteme – schlecht zu softwarebasierten, schnell veränderbaren KI-Systemen passen. **The Very Long Game** zeigt, dass die zivile Führungsrolle bei der KI-Entwicklung fast alle untersuchten Nationen vor das gleiche Dilemma stellt: Wie kann militärische Innovation von zivilen Durchbrüchen profitieren, ohne die Kontrolle über sicherheitskritische Anwendungen zu verlieren?

Eine besondere Facette des Dual-Use-Problems zeigt sich in der **internationalen Proliferation KI-unterstützter Drohnentechnologie**. Der CNTR Monitor dokumentiert die rasante Verbreitung unbemannter Systeme in aktuellen Konflikten und warnt vor der Weiterverbreitung an staatliche wie nicht staatliche Akteure. **The Very Long Game** bestätigt in der Iran-Fallstudie (**Viel Donner, kein Regen**), dass auch ressourcenbeschränkte und sanktionierte Staaten in der Lage sind, militärisch wirksame unbemannte Systeme zu entwickeln und zu exportieren – ein Befund, der die Grenzen bestehender Exportkontrollregime unterstreicht. Die UN-Resolution 79/239 (2024) adressiert dieses Risiko explizit durch den Verweis auf Proliferationsrisiken an nicht staatliche Akteure als eine der zentralen Herausforderungen militärischer KI (UN24, UN25).

Zentrale Widersprüche und divergierende Evidenz

Widerspruch 1: „KI-Wettrüsten“ versus „Geopolitischer Innovationswettbewerb“

Die erste zentrale Kontroverse betrifft die Frage, wie die globale KI-Dynamik im Verteidigungsbereich zu charakterisieren ist. Auf der einen Seite steht die insbesondere in den UN-Dokumenten prominent vertretene Warnung vor einem „KI-Wettrüsten“ – also einer unkontrollierten Spirale gegenseitiger technologischer Aufrüstung, die Kooperation unterminiert und Eskalationsrisiken erhöht. Auf der anderen Seite steht die vom CNTR Monitor vorgeschlagene Diagnose eines „geopolitischen Innovationswettkampfs“, der Elemente des Wettbewerbs und der Kooperation kombiniert und damit differenziertere politische Handlungsoptionen eröffnet. Die folgende Tabelle stellt beide Perspektiven dem empirischen Befund gegenüber:

	UN-Perspektive	CNTR-Perspektive	Empirischer Befund
Framing	Warnung vor einem neuen „arms race“	Plädoyer für „geopolitischen Innovationswettbewerb“ – Kombination aus Wettbewerb und Kooperation	Die meisten Nationen kämpfen mit grundlegenden Implementierungsproblemen
Evidenzgrad	Plausible, aber eher normativ-politische Zukunftsannahme	Differenziertere Kategorisierung	Hoch: 25 Fallstudien zeigen langsamen, mühsamen Fortschritt

The Very Long Game stützt die CNTR-These indirekt, aber nachdrücklich: Die Fallstudien – von Kanadas „maroder Dateninfrastruktur“ über Spaniens „langsames Erwachen“ bis zu Indiens „passiven Ambitionen“ – dokumentieren, dass die meisten Nationen von einem tatsächlichen Wettrüsten weit entfernt sind. Der CNTR Monitor differenziert zudem die Strategien der USA, von China und der EU nach Netzwerkgliederung, Zielen und Technologieverständnis und diagnostiziert die Wettrüsten-Rhetorik als kontraproduktiv, da sie kooperative Rahmenwerke untergräbt.

Widerspruch 2: Disruptive Transformation versus evolutionäre Realität

Die politische Debatte – insbesondere in den UN-Dokumenten – impliziert häufig eine unmittelbar bevorstehende disruptive Transformation, die dringendes Handeln erfordert. Dem steht ein robuster empirischer Befund gegenüber: **The Very Long Game** charakterisiert die militärische KI-Adoption als „Evolution, nicht Revolution“ (exemplarisch: Australien). Die meisten Staaten befinden sich in der Phase der „Second-Wave-AI“ und ringen mit Basisherausforderungen wie Dateninfrastruktur, Beschaffungsbürokratie und kulturellem Wandel. Selbst die USA – mit den größten Investitionen – kämpfen mit dem „Tal des Todes“ zwischen Forschung und skalierbarer militärischer Anwendung.

Allerdings gilt die These der „langsamen Evolution“ primär für Friedensstreitkräfte mit ihren bürokratischen Beschaffungsprozessen und kulturellen Beharrungskräften. Die Ukraine zeigt, dass unter existenziellem Druck eine fundamentale Beschleunigung möglich ist – jedoch um den Preis fehlender Standardisierung, unklarer Qualitätskontrolle und einer Ad-hoc-Governance, die langfristig nicht tragfähig sein dürfte. Für die FuE-Planung ergibt sich daraus die Notwendigkeit, sowohl für evolutionäre Friedensadoption als auch für krisenbedingte „Rapid Adoption“ vorbereitet zu sein.

Widerspruch 3: „Daten als neues Öl“ versus „Defense Data Reality“

Offizielle Strategien vieler Nationen bezeichnen Daten als strategisches Asset von höchstem Wert. **The Very Long Game** widerspricht mit dem Konzept der „**defense data reality**“: Im

Gegensatz zum kommerziellen Sektor herrschen im Militär Datenknappheit, fragmentierte Systeme und mangelnde Interoperabilität. SIPRI stützt diese Aussage, indem es auf die schlechte Datenqualität auf dem Schlachtfeld als fundamentales Zuverlässigkeitsproblem hinweist.

Auch hier liefert die Ukraine einen differenzierenden Befund: Unter Kampfbedingungen generiert das Land beispiellose Mengen an operativen Echtzeiten – Sensor-, Drohnen-, Aufklärungs- und Gefechtsdaten in einem Volumen und einer Granularität, die in Friedenszeiten nicht verfügbar wären. Die „**defense data reality**“ der Datenknappheit ist demnach primär ein Strukturproblem von Friedensstreitkräften; im Krieg entsteht ein Datenüberfluss, der seinerseits neue Herausforderungen schafft: Qualitätssicherung unter Zeitdruck, Auswertungs-kapazität, Echtzeit-Verarbeitung und die Frage, wie Algorithmen, die mit Friedensdaten trainiert wurden, unter den radikal anderen Bedingungen eines Hochintensitätskonflikts performen.

Für FuE bedeutet dies: Forschung zu **Few-Shot Learning, Transfer Learning**, synthetischer Datengenerierung und robusten KI-Methoden, die mit limitierten, verrauschten und unsicheren Daten operieren können, ist nicht inkrementell, sondern strategisch prioritär. Gleichzeitig müssen Methoden des **Domain Shift** – der Übertragung von Modellen zwischen Trainings- und Einsatzumgebungen – gezielt beforscht werden.

Widerspruch 4: Notwendigkeit neuer Verträge

Die UN-Berichte dokumentieren eine Spaltung der Staatengemeinschaft: Einige Staaten fordern dringend ein neues, rechtsverbindliches Instrument (insbesondere für AWS), während andere das bestehende Völkerrecht für ausreichend halten. SIPRI legt nahe, dass für AI-DSS möglicherweise ein eigenständiger neuer Prozess erforderlich ist, da diese Systeme in den bestehenden AWS-Debatten unzureichend adressiert werden. Der CNTR Monitor verweist auf die fragmentierte internationale Regulierungslandschaft (EU AI Act, US Executive Order, chinesische Strategie) als zusätzliche Komplexitätsebene.

Widerspruch 5: Absolute Halbleiter-Abhängigkeit versus asymmetrische Realität

Der CNTR Monitor zeichnet ein Bild globaler KI-Fähigkeiten, das maßgeblich durch den Zugang zu spezialisierten Halbleitern bestimmt wird: USA (Chipdesign), Niederlande (EUV-Maschinen), Taiwan (Produktion). Exportkontrollen und die Stargate-Initiative (500 Mrd. \$) unterstreichen die geopolitische Dimension dieser Abhängigkeit. Die implizite Annahme: ohne Zugang zu fortschrittlichen Chips keine relevante militärische KI; der Iran widerlegt diese These jedoch: Trotz umfassender Sanktionen und eingeschränktem Zugang zu globalen Technologiemärkten hat der Iran eine militärisch wirksame KI-unterstützte Drohnenfähigkeit aufgebaut.² Für die FuE-Strategie bedeutet dies eine doppelte Herausforderung: Einerseits muss Europa eigene Halbleiterkapazitäten für Spitzen-KI ausbauen (CNTR-Empfehlung); andererseits müssen Gegenmaßnahmen gegen Low-Tech-KI-Bedrohungen – Schwarmabwehr, Systeme zur Drohnerkennung und -neutralisierung – mindestens gleichrangig beforscht werden.

Identifizierte Lücken der Debatte

Die folgenden Lücken wurden durch einen systematischen Abgleich der sechs Quellen mit dem STEEP-Analyserahmen (Social, Technological, Economic, Environmental, Political) sowie den DOTLMPFI-Handlungsfeldern identifiziert. Der Vergleichsmaßstab ist somit nicht die Gesamtheit verfügbarer Literatur, sondern die Frage, welche für eine umfassende Bewertung essenziellen Dimensionen in keiner der analysierten Leitquellen hinreichend behandelt werden. Die Meta-Analyse identifiziert mehrere solche Themenfelder, die für eine umfassende Bewertung essenziell wären:

Nicht staatliche Akteure und asymmetrische

KI-Nutzung: Während das Proliferationsrisiko in allen Quellen erwähnt wird, fehlt eine systematische Analyse der KI-Fähigkeiten und -Strategien nicht staatlicher Akteure – von privaten Militärunternehmen bis zu terroristischen Netzwerken. Die Ukraine-Fallstudie in **The Very Long Game** (Crowdsourcing, Freiwilligeninitia-

tiven) deutet an, wie schnell sich unkonventionelle Innovationsmodelle entwickeln können. Die iranische Proliferation von KI-unterstützter Drohnentechnologie an Proxies wie Hisbollah und Huthi zeigt, dass diese Lücke nicht nur theoretischer Natur ist, sondern bereits operative Realität.

Test, Verifikation und Validierung (TVV)

militärischer KI: Obwohl alle Quellen auf Zuverlässigkeitsprobleme und das „Black Box“-Problem hinweisen, fehlen detaillierte Auseinandersetzungen mit konkreten TVV-Methoden, Standards und Zertifizierungsansätzen für sicherheitskritische militärische KI-Systeme.

Psychologische und kognitive Dimensionen:

Der **automation bias** – die menschliche Neigung, algorithmischen Empfehlungen unkritisch zu folgen – wird von SIPRI thematisiert, doch die breitere kognitionswissenschaftliche Forschung zu Mensch-KI-Interaktion unter Stress, Zeitdruck und Informationsüberflutung bleibt in allen Quellen unterbelichtet.

Umwelt- und Ressourcendimensionen: Der enorme Energie- und Ressourcenbedarf von KI-Infrastrukturen (Rechenzentren, Kühlsysteme, seltene Erden) wird in keiner Quelle systematisch mit den verteidigungspolitischen Anforderungen an Resilienz und Autarkie verknüpft. Das EC AI Factsheet erwähnt „energieeffiziente KI-Hardware“ als Priorität, ohne dies zu vertiefen.

Langfristige gesellschaftliche Implikationen:

Die STEEP-Dimension **Social** – etwa die Frage, wie die KI-Transformation der Streitkräfte das Verhältnis zwischen Militär und Gesellschaft verändert, oder die Auswirkungen auf Veteranen und das Berufsbild des Soldaten – bleiben weitgehend unbearbeitet.

Zentrale Stoßrichtungen für Forschung, Entwicklung und Innovation

Die vorliegende Meta-Analyse verdeutlicht: Die KI-Integration in der Verteidigung ist ein multidimensionaler Transformationsprozess, der sich durch eine charakteristische Spannung zwischen

² Analysen geborgener Shahed-Drohnen dokumentieren, dass diese zu einem erheblichen Anteil aus kommerziell verfügbaren Komponenten westlicher Hersteller bestehen. Siehe hierzu z. B. die Datenbank „Foreign components in weapons“ des ukrainischen Verteidigungsministeriums: <https://war-sanctions.gur.gov.ua/en/components>.

politischer Dringlichkeit und operativer Komplexität auszeichnet. Der empirisch belegte evolutionäre Charakter dieser Transformation – das „**very long game**“ – ist kein Argument für Abwarten, sondern für strategisch fokussierte und zugleich realistische FuE-Investitionen. Die aktuellen Konflikte in der Ukraine und im Nahen Osten zeigen gleichzeitig, dass unter existenziellem Druck eine radikale Beschleunigung möglich ist – und dass asymmetrische Akteure – verstanden als staatliche oder nicht staatliche Akteure, die durch unkonventionelle Strategien und kosteneffiziente Technologienutzungen Wirkungen erzielen, die in keinem proportionalen Verhältnis zu ihren Mitteln stehen – mit begrenzten Ressourcen militärisch relevante KI-Fähigkeiten entwickeln können, die technologisch überlegene Gegner vor erhebliche Herausforderungen stellen.

Aus der Synthese der Quellen und der Konfrontation mit der operativen Realität aktueller Konflikte ergeben sich sechs zentrale Innovationsrichtungen, die in ihrer Gesamtheit die FuE-Agenda für Verteidigungs-KI in den kommenden Jahren prägen werden:

1. KI-Methoden für die Defense Data Reality. Die sogenannte **defense data reality** – also die im Militär strukturell vorherrschende Datenknappheit, fragmentierte Systeme und mangelnde Interoperabilität – erfordert zunächst einen Paradigmenwechsel hin zu KI-Methoden, die mit limitierten, verrauschten und adversarial beeinflussten Daten zuverlässig operieren können. Technologien wie **Few-Shot Learning, Transfer Learning** und synthetische Datengenerierung rücken damit ins Zentrum der Forschungsagenda. Die ukrainische Erfahrung verdeutlicht zudem, dass der **Domain Shift** – die Übertragung friedenszeitlich trainierter Modelle auf die radikal anderen Bedingungen eines Hochintensitätskonflikts – als eigenständiges Forschungsproblem verstanden werden muss.
2. Vertrauenswürdige und erklärbare KI. Eng damit verknüpft ist die Forderung nach vertrauenswürdiger und erklärbarer KI: Die quellenübergreifend konsentrierte Notwendigkeit menschlicher Kontrolle ist nur einlösbar, wenn KI-Systeme ihre Entscheidungs-
- logik transparent machen. Explainable AI (XAI) ist damit keine akademische Disziplin, sondern eine operative Voraussetzung – für die völkerrechtliche Überprüfbarkeit, das Vertrauen der Operateure und die gesellschaftliche Akzeptanz in Demokratien. Dies wiederum setzt robuste Test-, Verifikations- und Validierungsmethoden (TVV) voraus, die als eigenständiges Forschungsfeld mit neuen Standards, Testumgebungen und Zertifizierungsverfahren systematisch aufgebaut werden müssen. Da viele verteidigungsrelevante KI-Systeme auf zivilen Technologien basieren, ist die Entwicklung gemeinsamer zivil-militärischer Standards besonders dringlich – militärische und zivile Normungsorganisationen müssen hier zusammenwirken, um kohärente Dual-Use-Zertifizierungsverfahren zu schaffen.
3. Agile Innovationsökosysteme und Beschaffungsreform. Auf der organisatorischen Ebene zeigen die Fallstudien, dass traditionelle, lineare Beschaffungsprozesse der Innovationsdynamik von KI strukturell nicht gewachsen sind. Das „Tal des Todes“ zwischen Forschung und Skalierung, Frankreichs starre Budgettrennung und Spaniens verspätete KMU-Integration illustrieren das Problem ebenso wie das ukrainische Gegenmodell, das unter existenziellem Druck durch Crowdsourcing und Integration ziviler IT-Talente eine radikal beschleunigte Innovation ermöglicht hat. Die Entwicklung agiler Innovationsökosysteme – mit **Regulatory Sandboxes, DevSecOps**-Ansätzen und der systematischen Vernetzung von Streitkräften, etablierter Industrie und Start-ups – ist daher eine Voraussetzung für die erfolgreiche Operationalisierung von Verteidigungs-KI.
4. Technologische Souveränität und asymmetrische Gegenmaßnahmen. Auf der geökonomischen Ebene verlangt die Abhängigkeit von spezialisierten Halbleitern den Ausbau europäischer technologischer Souveränität in Chip-Architekturen, Edge Computing und energieeffizienter KI-Hardware. Zugleich mahnt das iranische Beispiel, die Fokussierung auf Spitzentechnologie nicht zum blinden Fleck werden zu lassen: Kosteneffizient skalierte Drohenschwärme auf Basis älterer Chipgenerationen und Open-Source-Modelle

stellen eine asymmetrische Bedrohung dar, die eigene Gegenmaßnahmen erfordert.

5. Adversariale Robustheit und Counter-AI. Schließlich zeigen die aktuellen Konflikte, dass adversariale Robustheit und Counter-AI von einem akademischen Randthema zu einer operativen Kernforderung geworden sind. Wenn beide Konfliktparteien KI-gestützte Systeme einsetzen, wird die Fähigkeit, gegnerischer Manipulation zu widerstehen – von Spoofing über **adversarial attacks** bis zur elektronischen Kriegsführung – zur Überlebensfrage. Die ukrainische Antwort auf russisches GPS-Jamming durch Glasfasersteuerung illustriert die Dynamik dieses technologischen Wettlaufs zwischen Maßnahme und Gegenmaßnahme, der als eigenständiges Forschungsfeld mit entsprechender Förderung etabliert werden muss.
6. Gesellschaftliche Dimension der KI-Transformation. Schließlich verlangt die gesellschaftliche Dimension der KI-Transformation eine systematische Beforschung der Auswirkungen auf das Verhältnis zwischen Streitkräften und Gesellschaft. Die STEEP-Dimension „Social“ – vom veränderten Berufsbild des Soldaten über die demokratische Kontrolle algorithmischer Entscheidungsprozesse bis hin zu Fragen der gesellschaftlichen Akzeptanz – bleibt in allen analysierten Quellen weitgehend unbearbeitet und stellt ein eigenständiges Forschungsfeld dar.

Bibliografie

Borchert, H., Schütz, T. & Verbovszky, J. (2024). The Very Long Game – 25 Case Studies on the Global State of Defense AI. Springer. <https://doi.org/10.1007/978-3-031-58649-1>

EC (2025). AI Factsheet: AI in Defence. European Commission, Defence Industry and Space. <https://defence-industry-space.ec.europa.eu/system/files/2025-12/Factsheet%20AI%20in%20Defence.pdf>

Göttsche, M., Reis, K. & Daase, C. (Hrsg.) (2025). Neue Realitäten in der globalen Sicherheit durch KI. CNTR Monitor – Technologie und Rüstungskontrolle 2025. PRIF. https://www.cntrarmscontrol.org/fileadmin/Medien/Monitor/CNTR_Monitor_2025_DE.pdf

SIPRI (2025). Autonomous Weapon Systems and AI-enabled Decision Support Systems in Military Targeting: A Comparison and Recommended Policy Responses. <https://doi.org/10.55163/YQBY3151>

UN General Assembly (2024). Resolution 79/239. <https://docs.un.org/en/A/RES/79/239>

UN General Assembly (2025). Artificial intelligence in the military domain and its implications for international peace and security. Report of the Secretary-General, A/80/78. <https://docs.un.org/en/A/80/78>

Annex: Annotierte Bibliografie

CNTR Monitor (2025)

Göttsche, M., Reis, K. & Daase, C. (Hrsg.) (2025).

Neue Realitäten in der globalen Sicherheit durch KI. CNTR Monitor – Technologie und Rüstungskontrolle 2025. Frankfurt am Main: PRIF – Leibniz-Institut für Friedens- und Konfliktforschung.

https://www.cntrarmscontrol.org/fileadmin/Medien/Monitor/CNTR_Monitor_2025_DE.pdf

Der CNTR Monitor 2025 ist ein umfassender wissenschaftlicher Bericht des Leibniz-Instituts für Friedens- und Konfliktforschung, der die drastischen Veränderungen der globalen Sicherheit durch KI und neue Spitzentechnologien analysiert. Das Dokument beleuchtet kritische Schnittstellen zwischen KI und militärischen Anwendungen, wie etwa autonome Drohenschwärme, die automatisierte Entwicklung biologischer Kampfstoffe sowie die geopolitischen Spannungen im Rahmen globaler Chipkriege. Ein zentrales Anliegen der Autoren und Autorinnen ist die Modernisierung der Rüstungskontrolle, da herkömmliche Verträge kaum auf die schnelle, immaterielle Natur von Software-Anwendungen und Dual-Use-Technologien vorbereitet sind. Neben der Warnung vor Risiken wie der schwindenden menschlichen Kontrolle zeigt der Bericht jedoch auch auf, wie KI als Werkzeug für eine präzisere internationale Verifikation und Transparenz genutzt werden kann. Letztlich dient das Werk als strategischer Leitfaden für politische Entscheidungsträger, um durch verantwortungsvolle Governance und internationale Kooperation die Stabilität in einer technologisch hochgerüsteten Welt zu bewahren.

Kernaussage: KI transformiert bereits heute die globale Sicherheit; traditionelle Rüstungskontrolle muss sich anpassen, internationale Kooperation ist trotz geopolitischer Spannungen für verantwortliche KI-Governance notwendig.

Einführung: Wie die Materialisierung von KI globale Sicherheitsrisiken und Governance verändert

- KI entwickelt sich von akademischen Experimenten zu operativen Realitäten in Militär und kritischen Infrastrukturen.
- Herausforderungen: Dual-Use-Charakter erschwert Regulierung; Foundation Models

senken Hürden für fortgeschrittene Funktionen.

- Rüstungskontrolle: Traditionelle Ansätze passen schlecht zu softwarebasierten, schnell veränderbaren KI-Systemen.
- Institutionelle Lücken: Fragmentierte internationale Regulierungsansätze (EU AI Act, US-Richtlinien, China-Strategie).

KI, Halbleiter und Chipkriege

- Geopolitische Abhängigkeiten: KI-Fortschritte hängen von spezialisierten Halbleitern ab.
- Globale Lieferkette: USA (Chipdesign), Niederlande (EUV-Maschinen), Taiwan (Produktion), China (28nm+ Chips).
- Strategische Rivalitäten: USA-China-Wettbewerb durch Exportkontrollen und massive Investitionen (Stargate Initiative 500 Mrd. \$).
- Empfehlungen: Europa sollte heimische Halbleiterproduktion ausbauen, kritische Assets schützen, KI als kritische Infrastruktur anerkennen.

KI im geopolitischen Innovationswettbewerb

- Kritik des „Wettrüsten“-Framings: Plädoyer für „geopolitischen Innovationswettbewerb“ – Kombination aus Wettbewerb und Kooperation
- Analyse von USA, China, EU: Unterschiedliche Ansätze bei Netzwerkorganisation, Zielen und Technologieverständnis
- Empfehlungen: Vermeidung der Wettrüsten-Rhetorik, Stärkung kooperativer Rahmenwerke, differenzierte Kommunikation

Kriegsführung im Prozessortakt: Der zunehmende Einsatz von KI beim Militär

- Breiter Einsatz: KI in gesamter „Wirkungskette“ – von Aufklärung bis Wirkungskontrolle
- Beispiele: Projekt Maven (Zielerfassung), Gospel/Lavender (Israel), autonome Verteidigungssysteme
- Sicherheitsbedenken: Beschleunigung der Kriegsführung, Erosion menschlicher Kontrolle
- REAIM-Initiative: 60 Staaten einigten sich auf unverbindliche Prinzipien für „verantwortliche“ militärische KI-Nutzung

KI im Labor: Die Zukunft des Biodesigns

- Fortschritte: KI-gestützte Proteindesign-Tools (AlphaFold, AlphaProteo) revolutionieren Biodesign
- Risiken: Automatisierte Entwicklung schädlicher Organismen, Cyber-Bio-Angriffe, Umgehung von Biosicherheitsvorkehrungen
- Sicherheitslücken: Im Gegensatz zu Large Language Models fehlen bei Biodesign-Tools oft klare Sicherheitsvorkehrungen
- Empfehlungen: Risikobewertung in allen Phasen, gestufte Zugangsmodelle, integrierte Bio- und Cybersicherheit

KI-Entwicklungen in der Chemie

- Anwendungen: ChemCrow und ähnliche Tools für Reaktionsplanung, Eigenschaftsvorhersage, Literaturanalyse
- Dual-Use-Charakter: Chancen für Chemiewaffenerkennung vs. Risiken bei Missbrauch für Toxinentwicklung
- Empfehlungen: Ethikschulungen, KI-Regulierung, Sicherheitsmechanismen, eingeschränkter Zugang zu fortgeschrittenen Tools

KI in der Verifikation

- Potenzial: KI kann große Datenmengen aus Sensoren, Satelliten und öffentlichen Quellen analysieren
- Herausforderungen: „Explainability“ – KI-Entscheidungen müssen nachvollziehbar sein; Vertrauen in internationale Abkommen
- Zukunft: KI wird unverzichtbar für Verifikationsregime, aber menschliche Inspektoren und Inspektorinnen müssen finale Entscheidungen treffen

Trends

Drohnen: Aktuelle Entwicklungen

- Massenproduktion: Ukraine produzierte 2024 2,2 Mio. Drohnen, plant 4,5 Mio. für 2025
- Neue Taktiken: Schwarmangriffe (150 Drohnen bei „Spinnennetz“-Operation), Fiber-Optic-Steuerung gegen elektronische Störungen
- KI-Integration: Autonome Zielerkennung, KI-Piloten für Kampffjets (Deutschland: Helsing/Saab „Centaur“)

Nuklearphysik: Neue Reaktorgenerationen

- SMRs/NARs: Modulare Kleinreaktoren und alternative Reaktorkonzepte als CO₂-arme Energiequellen
- HALEU-Problematik: Höher angereicherter Brennstoff (bis 20 % ²³⁵U) erhöht Proliferationsrisiken
- Überwachungsherausforderungen: Mehr Standorte, dezentrale Verteilung erschwert Sicherungsmaßnahmen

Chemie: Autonome Laboratorien

- Funktionsweise: KI-gesteuerte Robotelabore für automatisierte Synthese und Optimierung
- Dual-Use: Chancen für Gegenmittel-Synthese vs. Risiken bei Kampfstoff-Produktion
- Einschränkungen: Hohe technische Komplexität macht Missbrauch derzeit weniger wahrscheinlich

Biotechnologie: Spiegelleben und Chiralität

- Konzept: Synthetische Organismen aus spiegelbildlichen Biomolekülen, biochemisch unvereinbar mit natürlichem Leben
- Risiken: Könnten Immunsysteme umgehen, sich unkontrolliert ausbreiten
- Expertenempfehlung: Moratorium oder strenge globale Standards vor technischer Realisierbarkeit

Biotechnologie: DNA-Synthese-Screening

- Herausforderung: Wachsende Verfügbarkeit von DNA-Synthese erhöht Missbrauchsrisiken
- Aktuelle Lücken: Nur ~80 % des Weltmarkts unterliegt freiwilligem Screening
- KI-Risiken: KI-gestützte Proteindesign-Tools können bestehende Screening-Systeme umgehen

Emerging Disruptive Technologies

- Analyse militärischer Technologiestrategien von fünf Demokratien (Australien, Deutschland, UK, Japan, USA)
- Top-Prioritäten: Kommunikationstechnologie, konventionelle Fähigkeiten, KI, Raketentechnologie
- Raketenproblem: Destabilisierende Wirkung konventioneller Raketen bisher international kaum diskutiert

- Deutschland: Bedarf an intensiverer öffentlicher Debatte über Technologieentscheidungen

Anhang: Rüstungskontrollverträge

- Kernwaffen: Vertrag über die Nichtverbreitung von Kernwaffen, Comprehensive Nuclear-Test-Ban Treaty, bilaterale US-Russland-Abkommen, regionale kernwaffenfreie Zonen
- Chemische/Biologische Waffen: Übereinkommen über das Verbot biologischer Waffen, Übereinkommen über das Verbot chemischer Waffen, UN-Mechanismen, Exportkontrollen
- KI-Governance: REAIM-Prinzipien, Bletchley Declaration, nationale Regulierungsansätze (EU AI Act, US Executive Order)

SIPRI (2025)

SIPRI (2025). **Autonomous Weapon Systems and AI-enabled Decision Support Systems in Military Targeting: A Comparison and Recommended Policy Responses**. Stockholm: Stockholm International Peace Research Institute. <https://doi.org/10.55163/YQBY3151>

Dieser Bericht des Stockholm International Peace Research Institute (SIPRI) aus dem Jahr 2025 untersucht die technologischen und regulatorischen Unterschiede zwischen autonomen Waffensystemen (AWS) und KI-gestützten Entscheidungsunterstützungssystemen (AI-DSS) im militärischen Kontext. Während AWS eigenständig Ziele angreifen, dienen AI-DSS dazu, menschliche Soldaten durch Datenanalyse bei der Zielauswahl und Angriffsplanung zu beraten. Die Autoren und Autorinnen betonen, dass beide Technologien das Risiko unbeabsichtigter Schäden bergen, wobei bei AI-DSS insbesondere die Gefahr einer menschlichen Überreaktion oder blinden Vertrauens in algorithmische Empfehlungen im Vordergrund steht. Das Dokument dient als strategischer Leitfaden für politische Entscheidungsträger, um die Einhaltung des Völkerrechts zu gewährleisten und neue Rahmenbedingungen für die menschliche Kontrolle über KI auf dem Schlachtfeld zu definieren.

Kernaussage: AWS und AI-DSS unterscheiden sich fundamental in ihrer Funktionsweise, teilen aber technische Risiken; beide erfordern klare Governance-Strukturen zur Wahrung menschlicher Kontrolle und Völkerrechtskonformität.

Einführung und Charakterisierung

- AWS (autonome Waffensysteme): Können Ziele identifizieren, auswählen und angreifen ohne menschliche Intervention
- AI-DSS (KI-gestützte Entscheidungsunterstützungssysteme): Computergestützte Tools, die Informationen zur Unterstützung militärischer Entscheidungen bereitstellen

Auswirkungen auf Entscheidungen zum Gewalteinsatz

- Beide Systeme verändern die menschliche Rolle beim Gewalteinsatz
- AWS: Führen Entscheidungen autonom aus
- AI-DSS: Beeinflussen und formen menschliche Entscheidungen

Umfang im Zielbindungszyklus

- AWS: Begrenzt auf die Missionsausführungsphase (Phase 3)
- AI-DSS: Breitere Anwendung über mehrere Phasen des Zielbindungszyklus hinweg
- Risiken unbeabsichtigter Schäden
- Zuverlässigkeitsprobleme: Beide Systeme teilen technische Limitierungen der KI
- Unvorhersehbare Ausfälle und schwer erkennbare Fehlfunktionen
- „Black Box“-Problem bei komplexen KI-Systemen
- AWS: Direkter Risikopfad – falsche Zielerkennung führt zu sofortiger Gewaltanwendung
- AI-DSS: Indirekter Risikopfad – Schäden entstehen nur, wenn Menschen auf falsche Informationen reagieren

Rechtliche Aspekte

- IHL-Anforderungen: Beide Systeme unterliegen den Regeln des humanitären Völkerrechts
- Fragen zur erlaubten Abhängigkeit von automatisierten Systemen
- Verantwortung verbleibt bei Menschen, nicht bei Maschinen
- „Many hands problem“ – Verteilung der Verantwortung über mehrere Akteure

- Artikel-36-Überprüfungen: AWS sind klar überprüfungspflichtig als Waffensysteme; Unklarheit bei AI-DSS

Politische Antworten

- Ansatz 1: AI-DSS in bestehende AWS-Bemühungen einbeziehen (Nutzung vorhandener Expertise vs. Risiko der Vernachlässigung KI-spezifischer Probleme)
- Ansatz 2: Neuen Prozess für AI-DSS etablieren (spezifischer Fokus vs. zusätzlicher Ressourcenbedarf)
- Ansatz 3: Keinen spezifischen Ansatz für AI-DSS (Flexibilität vs. Mangel an gezielten Maßnahmen)

Empfehlungen

1. Multilateralen Prozess für AI-DSS erwägen – Abwägung der drei verfügbaren Ansätze
2. AWS-Expertise für AI-DSS nutzen – Erkenntnisse aus AWS-Politik übertragen
3. Forschung zu AI-DSS intensivieren – Wissenslücken schließen, besonders zu Datenschutz und Menschenrechten

Europäische Kommission (2025)

Europäische Kommission (2025). **AI Factsheet: Artificial Intelligence in Defence**. Brüssel: Generaldirektion Verteidigungsindustrie und Raumfahrt.
<https://defence-industry-space.ec.europa.eu/system/files/2025-12/Factsheet%20AI%20in%20Defence.pdf>

Dieses Factsheet der Europäischen Kommission beleuchtet die zentrale Rolle von KI bei der Modernisierung der europäischen Verteidigungssysteme. Es verdeutlicht, dass die zukünftige Kriegsführung maßgeblich durch Algorithmen und Rechenleistung geprägt wird, wobei der Europäische Verteidigungsfonds (EDF) gezielt Projekte zur automatisierten Bedrohungserkennung und Cybersicherheit finanziert. Trotz des technologischen Fortschritts wird die Notwendigkeit von hoher Zuverlässigkeit und menschlicher Aufsicht betont, um den besonderen Risiken und ethischen Herausforderungen in militärischen Konflikten gerecht zu werden.

Kernaussage: Die EU investiert systematisch in vertrauenswürdige KI-Technologien für die

Verteidigung unter besonderer Berücksichtigung ethischer Standards, Cybersicherheit und menschlicher Kontrolle.

Rolle von KI in der Verteidigung

- KI ist zentral für die moderne Kriegsführung: Staaten investieren massiv, weil zukünftige Schlachtfelder genauso von Algorithmen und Rechenleistung wie von Waffen abhängen

Besonderheiten militärischer KI

- Militärische KI muss in feindlichen Hochrisikoszenarien extrem zuverlässig, widerstandsfähig und sicher sein
- Fehler gefährden direkt Menschenleben, daher stehen Tests und Cybersicherheit im EDF im Fokus

EU-Prioritäten (EDF 2025–2027)

- Vertrauenswürdige KI
- Bessere Verarbeitung komplexer Daten
- Verbesserte Mensch-Maschine-Interaktion
- Autonomes Lernen mit wenig menschlichem Eingriff
- Energieeffiziente KI-Hardware

Hauptvorteile

- Echtzeit-Lagebild und schnellere Bedrohungserkennung
- Bessere Koordination autonomer Systeme
- Effizientere Logistik und präzisere Zielidentifikation
- Geringere Gefährdung von Soldaten und Soldatinnen
- Bessere Schadensbewertung

Risiken

- Ethische und rechtliche Probleme
- Anfälligkeit für Cyberangriffe und gegnerische KI
- Überabhängigkeit und unvorhersehbare Entscheidungen
- Verzerrte Daten und Interoperabilitätsprobleme

Beispiele für EDF-Projekte

- Cyber-Verteidigung und Sprengsatz-Erkennung: PANDORA, AIDEDex
- KI-Cloud und Verschlüsselung: AI4DEF, PRIVILEGE
- Lernfähige KI-Frameworks: FaRADAI, EU-GUARDIAN, KOIOS, Alnception

- AR-gestützte Soldatensysteme und Sprachtechnologien: LODESTAR, ARCHER, NEMO, SALT4D

UN-Generalversammlung (2024)

UN General Assembly (2024). **Resolution 79/239: Artificial intelligence in the military domain.** New York: United Nations. Angenommen am 24. Dezember 2024.

<https://docs.un.org/en/A/RES/79/239>

In dieser Resolution der Generalversammlung der Vereinten Nationen vom Dezember 2024 wird bekräftigt, dass das Völkerrecht und die Menschenrechte uneingeschränkt für den gesamten Lebenszyklus von KI im militärischen Sektor gelten. Der Text unterstreicht die Notwendigkeit einer verantwortungsvollen Anwendung, um Gefahren wie ein unkontrolliertes Wettrüsten, algorithmische Voreingenommenheit oder eine sinkende Hemmschwelle für Konflikte zu minimieren. Ein zentrales Ziel ist die Förderung eines inklusiven multilateralen Dialogs, der insbesondere die digitale Kluft zwischen Industrie- und Entwicklungsländern überbrücken soll. Zu diesem Zweck wird der Generalsekretär beauftragt, einen umfassenden Bericht über die globalen Herausforderungen und Chancen dieser Technologie zu erstellen, wobei ein besonderes Augenmerk auf Aspekte jenseits autonomer Waffensysteme gelegt wird.

Kernaussage: Diese Resolution stellt den ersten umfassenden multilateralen Rahmen für KI im militärischen Bereich dar und betont die Notwendigkeit einer verantwortungsvollen Entwicklung unter Wahrung des Völkerrechts.

Präambel und Grundprinzipien

- Rechtlicher Rahmen: Internationale Gesetze (UN-Charta, humanitäres Völkerrecht, Menschenrechte) gelten für den gesamten Lebenszyklus von KI im militärischen Bereich
- Verantwortungsvolle Anwendung: Betonung menschenzentrierter, verantwortlicher, sicherer und vertrauenswürdiger KI
- Anwendungsbereich: Von Vorplanung über Entwicklung bis zur Außerbetriebnahme; ausschließlich militärische Anwendungen

Chancen und Risiken

- Potenzielle Vorteile: Verbesserung der Einhaltung des humanitären Völkerrechts, besserer Schutz von Zivilisten
- Herausforderungen: Rüstungswettlauf, Fehlkalkulationen, niedrigere Konfliktschwelle, Proliferationsrisiken, algorithmische Voreingenommenheit, Kontrollverlust

Operative Maßnahmen

- Rechtliche Bestätigung (§ 1): Internationale Gesetze gelten für alle Phasen des KI-Lebenszyklus
- Nationale und internationale Anstrengungen (§ 2-3): Förderung von Initiativen und multilateralem Dialog
- UN-Unterstützung (§ 4-6): Wissensvermittlung, Kapazitätsaufbau, internationale Zusammenarbeit
- Berichterstattung (§ 7-8): Mitgliedstaaten-Befragung und substantieller Bericht für die 80. Generalversammlung
- Zukünftige Behandlung (§ 9): Eigenständiger Tagesordnungspunkt

Besondere Erwähnungen

- Autonome Waffensysteme: Abgrenzung – Resolution fokussiert auf Bereiche außerhalb letaler autonomer Waffensysteme
- Internationale Kooperation: Überbrückung der digitalen Kluft, Multi-Stakeholder-Ansatz

UN-Generalversammlung (2025)

UN General Assembly (2025). **Artificial intelligence in the military domain and its implications for international peace and security: Report of the Secretary-General. Dokument A/80/78.** New York: United Nations.

<https://docs.un.org/en/A/80/78>

Dieser UN-Bericht dokumentiert einen umfassenden internationalen Dialog über die Integration von KI im militärischen Sektor und deren Auswirkungen auf den globalen Frieden. Er strukturiert sich als eine Sammlung nationaler Positionen und Expertenbeiträge, die das Spannungsfeld zwischen operativen Vorteilen – wie erhöhter Präzision und dem Schutz eigener Truppen – und erheblichen Sicherheitsrisiken beleuchten. Ein zentrales Motiv des Textes ist die Forderung nach menschlicher Kontrolle und

Verantwortlichkeit, insbesondere, um eine unbeabsichtigte Eskalation von Konflikten oder die Schwächung des Völkerrechts zu verhindern. Der Bericht dient als Grundlage für künftige Governance-Strukturen und betont die Notwendigkeit multilateraler Zusammenarbeit, um ein unkontrolliertes Wettrüsten zu vermeiden.

Kernaussage: Der Bericht schafft eine gemeinsame Wissensbasis über KI im militärischen Bereich und liefert Empfehlungen für verantwortungsvolle Governance unter Betonung menschlicher Kontrolle und Völkerrechtskonformität.

Einführung

- Auftrag: Bericht gemäß UN-Resolution 79/239 zu Chancen und Herausforderungen von KI im militärischen Bereich
- Fokus: Bereiche außerhalb letaler autonomer Waffensysteme
- Methodik: Befragung von Mitgliedstaaten, internationalen Organisationen, Zivilgesellschaft, Wissenschaft und Industrie

Hintergrund

- Rasante technologische Entwicklung mit weitreichenden gesellschaftlichen Auswirkungen
- KI verändert alle Aspekte militärischer Angelegenheiten fundamental
- Staaten nutzen bereits KI in Verteidigungsoperationen
- Anwendungen gehen weit über autonome Waffensysteme hinaus

Chancen und Herausforderungen

Chancen:

- Geschwindigkeit und Effizienz: Verbesserte Informationsanalyse und Entscheidungsfindung
- Anwendungsbereiche: Aufklärung, Überwachung, Reconnaissance, Entscheidungsunterstützung, Kommando/Kontrolle, unbemannte Systeme, Cybersicherheit, Logistik, Wartung
- Friedenssicherung: Beitrag zu internationalem Frieden durch bessere Situationsanalyse
- Völkerrecht: Potenzielle Verbesserung der Einhaltung des humanitären Völkerrechts

Herausforderungen:

- Technische Risiken: Algorithmus-Bias, Datenverzerrung, technische Ausfälle, Cyberverwundbarkeiten, mangelnde Transparenz („Black Box“-Problem)
- Sicherheitsrisiken: Beschleunigte Eskalation, Proliferation an nicht staatliche Akteure, potenzielle Destabilisierung
- Rechtliche/ethische Bedenken: Verantwortung und Rechenschaftspflicht, Schutz von Zivilisten, menschliche Kontrolle über Gewaltanwendung

Bestehende und entstehende normative Vorschläge

- Grundprinzipien: Völkerrechtskonformität, verantwortungsvoller Ansatz (flexibel, ausgewogen, realistisch), menschenzentriert (bedeutsame menschliche Kontrolle)
- Technologische Prinzipien: Sicherheit und Zuverlässigkeit, Transparenz und Nachvollziehbarkeit, angemessene Governance

Initiativen im Bereich militärischer KI

- Internationale Foren: UN-Pakt für die Zukunft, Global Digital Compact, Abrüstungskommission, United Nations Institute for Disarmament Research
- Von Staaten geführte Initiativen: Political Declaration on Responsible Military Use of AI, REAIM-Gipfel, Paris Declaration, AI Safety Summit, G7
- Regionale Initiativen: ASEAN, Mendoza-Erklärung (Amerika), NATO-KI-Strategie

Nächste Schritte

- Dialog-Bedarf: Weitere Studien, Risikominderung, Entwicklung normativer Frameworks
- Governance-Ansätze: Diskussion über Rechtsverbindlichkeit, Vermeidung von Fragmentierung, Multi-Stakeholder-Ansatz
- Prioritäten: Völkerrechts-Compliance, gemeinsame Definitionen, Vertrauensbildung, Kapazitätsaufbau

Beobachtungen und Schlussfolgerungen des Generalsekretärs

- Zentrale Erkenntnisse: Transformatives Potenzial mit Doppelcharakter (Chancen und Risiken), Kernherausforderung der menschlichen Kontrolle

- Kritische Bereiche: Besondere Aufmerksamkeit bei Gewaltanwendung, dringende Empfehlung für menschliche Kontrolle über Nuklearentscheidungen, KI darf Proliferation von Massenvernichtungswaffen nicht erleichtern
- Empfehlungen: Etablierung eines UN-Prozesses, Kapazitätsaufbau, Multi-Stakeholder-Integration

Annexe

- Mitgliedstaaten-Antworten: 31 Länder plus EU mit detaillierten Positionen
- Stakeholder-Beiträge: Internationale Organisationen (Internationales Komitee des Roten Kreuzes, Afrikanische Kommission), Zivilgesellschaft (12 Organisationen), Wissenschaft (4 Institute), Industrie (Microsoft)

The Very Long Game (2024)

Borchert, H., Schütz, T. & Verbovszky, J. (Hrsg.) (2024). **The Very Long Game: 25 Case Studies on the Global State of Defense AI**. Cham: Springer Nature.

<https://link.springer.com/book/10.1007/978-3-031-58649-1>

Dieses Werk bietet eine umfassende vergleichende Analyse, wie 25 Nationen KI im Verteidigungsbereich implementieren. Die Herausgeber betonen, dass KI das Potenzial hat, der bedeutendste Force Multiplier in der Militärgeschichte zu werden, dass ihre Einführung jedoch eine tiefgreifende konzeptionelle, organisatorische und kulturelle Transformation erfordert. Anstatt über zukünftige Möglichkeiten zu spekulieren, konzentriert sich das Buch auf die gegenwärtige Praxis und analysiert jede Nation anhand der DOTLMPFI-Handlungsfelder: Denken über Verteidigungs-KI, Entwickeln, Organisieren, Finanzieren, Einführen und Betreiben sowie Ausbilden.

Kernaussage: Der Übergang von rein menschlicher Kriegsführung zu einer Mensch-Maschine-Interaktion ist ein langwieriger Prozess („a very long game“), der ein umfassendes Überdenken militärischer Macht erfordert; der globale Ansatz variiert erheblich zwischen Nationen.

Methodischer Rahmen

- Analytisches Framework: DOTLMPFI-Handlungsfelder
- Fokus auf gegenwärtige Praxis statt Zukunftsspekulation
- KI als Werkzeugkasten verschiedener Methoden (maschinelles Lernen, Computer Vision)
- Schwerpunkt auf „zweiter Welle“ der KI (korrelatives Lernen), „dritte Welle“ (kontextbezogenes Denken) noch in Entwicklung

Regionale Schwerpunkte und zentrale Erkenntnisse

Nordamerika:

- USA: Riskanter Inkrementalismus – trotz massiver Forschung Schwierigkeiten bei Überführung in skalierbare militärische Fähigkeiten; organisatorische Anstrengungen (CDAO) vs. bürokratische Trägheit
- Kanada: „Zähne fressen Schwanz“ – Kultur des Operationsprimats behindert Dateninfrastruktur; Gefahr des Anschlussverlusts ohne kulturelle Wende

Europa – Westeuropa:

- UK: Glänzende Aussichten, große Herausforderungen – exzellente Forschungsbasis (Deep Mind), klare Strategie, aber Brexit-Folgen und Ressourcenknappheit
- Schweden: Fruchtbarer Boden – hochdigitalisierte Gesellschaft, „Totale Verteidigung“, Priorisierungsrisiko bei konventionellem Wiederaufbau
- Finnland: Vorsichtige datengesteuerte Evolution – pragmatischer Ansatz, F-35-Integration als Katalysator
- Dänemark: Server vor Panzern? – Bedarf an „digitalem Rückgrat“, Mangel an KI-Kompetenz als Hauptrisiko
- Deutschland: Herr und Diener – struktureller Pazifismus prägt KI-Ansatz, KI als unterstützendes Werkzeug; Bedarf an präziseren Zielen und Industriepolitik
- Niederlande: Nutzung der Datenwissenschaft – „Information Manoeuvre“ und Multi-Domain-Operations--Konzept, REAIM-Ausrichtung unterstreicht Ethik-Fokus
- Frankreich: Steiniger Weg zur Skalierung – souveränes KI-Ökosystem (ARTEMIS.IA), Trennung von Forschungs- und Beschaffungsbudgets behindert agile Entwicklung

Europa – Südeuropa:

- Spanien: Langsames Erwachen – KI seit 2020 im Fokus, dominiert von Großunternehmen; Bedarf an KMU-Integration
- Italien: Erkundung eines neuen Force Enablers – Späteinsteiger, internationale Kooperationen (GCAP), „Forza NEC“-Programm
- Griechenland: Potenzial nutzen – türkische Rivalität als Treiber, High-Tech-Beschaffung (F-35, Rafale); Risiko von „Black Boxes“

Europa – Nordost und Baltikum:

- Estland: Gefangen zwischen Heute und Morgen – E-Government-Vorreiter, aber konservatives Militär; kein „First Adopter“, Nischen-Teamplayer

Naher Osten:

- Türkei: Wegweisende Technologie – autonome Systeme als Zukunft, Drohnen-Erfolg (Bayraktar TB2); Herausforderung Mensch-Maschine-Interaktion
- Israel: Organisiertes Chaos – informelle Kultur ermöglicht schnellen Wissensaustausch; Bedarf an formellerer nationaler Strategie
- Iran: Viel Donner, kein Regen – KI als Mittel gegen Isolation, asymmetrische Fähigkeiten; technologische Unterlegenheit und Propagandafokus

Asien – Süd:

- Indien: Passive Ambitionen, aktive Beschränkungen – riesiger Talentpool, aber Innovations- und Strategiedefizit; „Silo-Ansatz“ vs. notwendiger „Hydra-Ansatz“

Asien – Ost:

- China: „Überholen in der Kurve“ – Anspruch auf KI-Weltführung bis 2030, militärisch-zivile Fusion, „intelligentisierte“ Kriegsführung; Abhängigkeit von Halbleiter-Lösung
- Japan: Langen Schatten überwinden – Überwindung militärischer Forschungszurückhaltung, verschlechtertes Sicherheitsumfeld als Treiber

- Südkorea: Der Eine Ring – KI als Lösung für demografische Probleme; Erfolg abhängig von Beschaffungsreformen und Talentgewinnung
- Taiwan: Intelligente Verteidigung – asymmetrische Vorteile angestrebt, Trennung Regierung-Militär; Bedarf an FuE-Entbürokratisierung
- Singapur: Verteidigungsinnovation neu denken – „Ops-Tech“-Ansatz, Digital and Intelligence Service (DIS) als KI-Enabler

Ozeanien:

- Australien: Evolution, nicht Revolution – bemannte-unbemannte Teams (Ghost Bat), ASCA-Initiative; evolutionärer vs. disruptiver Ansatz

Eurasien:

- Russland: Hohe Hoffnungen, harte Realitäten – KI als Fähigkeitslücken-Schließer, Sanktionen und Stagnation; Priorisierung auf elektronische Kampfführung und unbemannte Systeme
- Ukraine: Überleben des Klügsten – KI als Überlebenswerkzeug, Crowdsourcing und Freiwillige, „lebendes Labor“ für KI-Kriegsführung

Übergreifende Erkenntnisse

- Kulturelle Transformation als Kernherausforderung neben technologischer Entwicklung
- Unterschiedliche Geschwindigkeiten und Prioritäten zwischen Nationen
- Spannung zwischen kurzfristigen operativen Bedürfnissen und langfristiger KI-Vision
- Bedeutung von Talent, Dateninfrastruktur und Mensch-Maschine-Interaktion
- Governance und ethische Frameworks als zunehmend kritische Faktoren

Empfohlene Zitierweise

Braun, A.; Cammann M., Holtmannspötter, D.; Prokopf C.; Schneider-Bertenburg, L. (2026). „KI in der Verteidigung: zwischen Ambition und Realität. Eine multiperspektivische Meta-Analyse“. VDI Research-Paper 31, VDI Technologiezentrum GmbH Düsseldorf. www.vditz.de/service/ki-in-der-verteidigung

Über VDI Research


VDI Research ist Teil des VDI Technologiezentrums (VDI TZ) und analysiert aus der Perspektive längerfristiger Vorausschau technologische und gesellschaftliche Zukunftsfragen. Zu den Publikationen gehören u. a. Studien, Analysen und VDI Research-Paper.

Weitere Publikationen von VDI Research und des VDI Technologiezentrums unter: vditz.de/service/publikationen

Ihre Ansprechpersonen

Dr. Anette Braun
Technologieberaterin VDI Research
E-Mail: braun_a@vdi.de

Dr. Lino Schneider-Bertenburg
Technologieberater Verteidigung
E-Mail: lino.schneider-bertenburg@vdi.de

VDI Technologiezentrum GmbH
VDI-Platz 1, 40468 Düsseldorf
www.vditz.de
 @technikzukunft.bsky.social · 