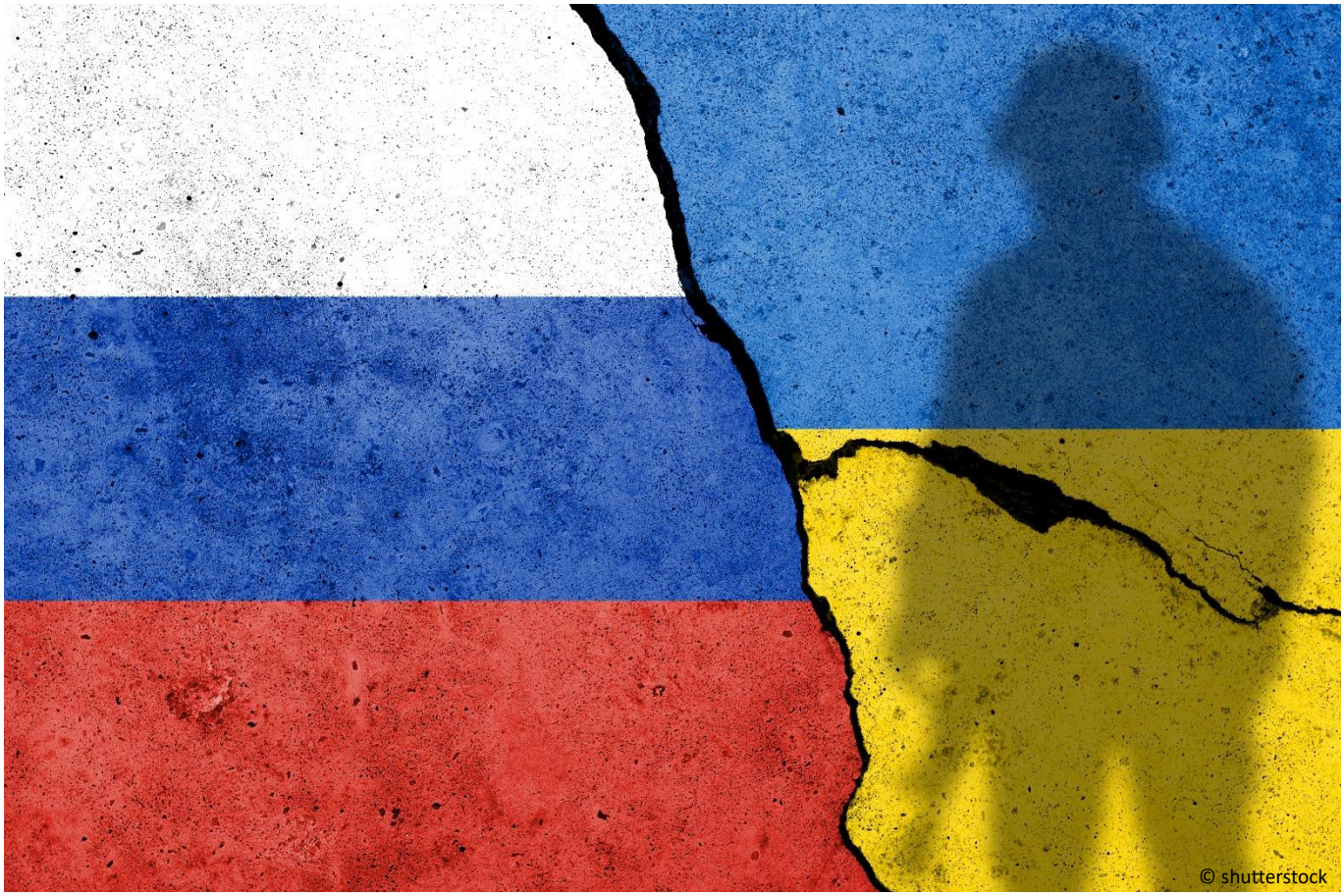
Centrum für Europäische Politik
FREIBURG | BERLIN

cepAdhoc

Nr. 4 | 2023 16. Mai 2023

Vorteil Ukraine: Wie KI die Kräfteverhältnisse im Krieg verändert

Anselm Küsters und Jörg Köpke



Eine Frage von Leben und Tod: Digitale Technologien wie künstliche Intelligenz (KI) prägen zunehmend das Geschehen auf dem Schlachtfeld. Mit dem Überfall Russlands auf die Ukraine hat sich die Kriegsführung revolutioniert. Die Front zwischen Krim und Donbass wird tragischerweise zum Versuchsfeld. Doch trotz aller Erfolge der Ukraine und einer Überlegenheit des Westens zeigen bisherige Erfahrungen und KI-Experimente, dass autonome Militärsysteme dauerhaft keine Wunderwaffen sind.

Inhaltsverzeichnis

1 Einleitung

Während westliche Parlamente und Regierungen noch über mögliche Rüstungsexporte diskutieren, nehmen digitale Technologien längst eine **entscheidende militärische und geopolitische Rolle** ein. Russlands Überfall auf die Ukraine ist der erste Krieg, in dem beide Seiten in großem Umfang digitale Kampfmittel wie etwa Drohnen einsetzen.[1] Hinzu kommen täglich rund 200 Cyberangriffe, die insbesondere Moskau als Teil seiner **hybriden Kriegsführung** nutzt.[2] Die Ukraine bietet der militärischen Weltmacht Russland durch kreativ eingesetzte, ursprünglich nicht-militärische Technologien erstaunlich erfolgreich Paroli.[3] Anschauliche Beispiele sind Elon Musks Starlink-Satelliten oder DJI-Flugdrohnen. Der ukrainische Minister für digitale Transformation, Mykhailo Fedorov, kündigte unlängst weitere Pläne für moderne autonome Systeme und militärische Start-ups an.[4]

Der Ukraine-Krieg wirft mit Blick auf den drohenden, von China forcierten Konflikt um Taiwan ein Schlaglicht auf die **künftige Rolle von KI im Militärbereich**. Peking und Washington treiben derzeit jeweils die Entwicklung von autonomen, miteinander kommunizierenden Drohnenschwärmen voran. China will noch in diesem Jahr zur weltweit führenden KI-Macht aufsteigen und hat eine aggressive, innovationsorientierte Militärstrategie verabschiedet.[5] Auch Großbritannien forscht an KI-gesteuerten Robotern, die es Bodentruppen ermöglichen sollen, strategisch bedeutsame Brücken zu zerstören – ebenfalls motiviert durch die Erfahrungen in der Ukraine.[6]

Wie sollte sich Westeuropa in diesem **digitalen Wettbewerb** positionieren? Kritische Stimmen fordern, militärische KI generell international zu ächten. Andere halten derartige Systeme für unverzichtbar, um die Sicherheit des Westens nicht einseitig aufs Spiel zu setzen. Analysen des Ukraine-Konfliktes, Erfahrungen mit autonomen Waffensystemen sowie Experimente zu KI-Anwendungen zeigen, wie notwendig es ist, die Interaktion zwischen Mensch und Maschine systematisch zu evaluieren, um negative Effekte, etwa durch „friendly fire“, zu verhindern. Künftige Verhandlungen zur Regulierung sogenannter verantwortungsbewusster KI im militärischen Bereich sollten entsprechende Standards verbindlich festlegen.

2 Militärische Macht im KI-Zeitalter

Die Automatisierung militär-technologischer Innovationen schritt in den vergangenen Jahren zunehmend voran. Im KI-Zeitalter sind laut Verteidigungsexperte Paul Scharre **vier Schlüsselelemente für militärische Macht** entscheidend: zu sammelnde und auszuwertende Daten, eine lückenlose Kontrolle über Chip-Lieferketten, Humankapital und industrielle Innovationskraft sowie die Verzahnung von KI mit Wirtschaft, Gesellschaft und Militär. Scharre nennt Beispiele, in denen sogenannte KI-Agenten bestimmte Kriegssituationen simulieren.[7]

Das KI-Zeitalter wird **militärische Macht neu verteilen**. Russland hat dabei zurzeit offenbar die schlechteren Karten. Seit Kriegsbeginn haben mehr als **100.000 IT-Spezialisten** und damit zehn Prozent aller

---

1 The Ukraine-Russia Drone War Is Crowdsourced and Made in China (foreignpolicy.com).
2 Digitale Schizophrenie - Tagesspiegel Background.
3 Ebenso relevant war in der Anfangszeit zudem die militärisch-taktische Drohne TB2 Bayraktar eines türkischen Anbieters. TB2 Bayraktar : Grande stratégie d'un petit drone | IFRI - Institut français des relations internationales.
4 Ukraine wants a robot army (wired.com).
5 The PLA's Strategic Support Force and AI Innovation (brookings.edu).
6 British army seeks AI-powered robots to allow troops to demolish bridges in combat (inews.co.uk).
7 Four Battlegrounds | Paul Scharre | W. W. Norton & Company (wwnorton.com).

zuvor im Technologiesektor Beschäftigten Russland den Rücken gekehrt.[8] Im gleichen Zeitraum hat sich die Zahl ukrainischer Militär-Start-ups verzehnfacht.[9] Zudem ist die ukrainische Tech-Szene international besser vernetzt. Sie nutzt Initiativen wie „Army of Drones“, um schneller an ausländische Drohnen-Hardware zu gelangen. Dem internationalen Hacker-Kollektiv Anonymous gelingt es regelmäßig, ebenso Kritik am Krieg in russischen Medien zu platzieren wie Terabytes an **gehackten Dateien** zu veröffentlichen.[10] Zuletzt konnten ukrainische Hacker der „Cyber Resistance“ E-Mails eines russischen Spions erbeuten, der die US-Präsidentenwahl 2016 hatte manipulieren wollen.[11]

Die Folgen dieses technologischen Ungleichgewichtes sind auf dem Schlachtfeld bereits deutlich sichtbar. Kiew setzt KI effektiver als Moskau ein. Dabei geht es insbesondere um **geografische Aufklärung und Zielerkennung**. So werden beispielsweise Open-Source-Daten wie geopolitisch sensible Fotos in sozialen Medien mit KI analysiert.[12] Ukrainische Entwickler haben KI-Systeme darauf trainiert, getarnte feindliche Panzer mit Live-Aufnahmen von Drohnen zu identifizieren und annähernd in Echtzeit zu zerstören.[13] Die Systeme sind so programmiert, dass sie permanent eigenständig dazulernen. Da diese Drohnen im Flug kein GPS verwenden, liefen russische Gegenmaßnahmen zunächst oft ins Leere. Als Reaktion auf russische Raketenangriffe von Kriegsschiffen im Schwarzen Meer hat die Ukraine Drohnenboote entwickelt, die Sprengstoff transportieren und KI zur Zielerkennung nutzen.[14] Das ukrainische Tech-Unternehmen Primer passte seinen KI-Dienst **für Sprachtranskription** und Übersetzung so an, dass dieser abgefangene russische Kommunikation schnell verarbeitet und automatisch Informationen über die Streitkräfte extrahiert.[15] Die Ukraine macht sich dabei zunutze, dass russische Soldaten oft unverschlüsselt miteinander kommunizieren. Ende Februar schrieb Fedorov, der Einsatz innovativer Militärtechnologien sei einer der Bereiche, in denen die Ukraine Russland stets einen Schritt voraus sei.[16]

Auch Russland versucht, moderne digitale Techniken einzusetzen. Doch diese **beschränken sich bislang vor allem auf hybride Angriffe im Cyber-Raum**.[17] Die unlängst veröffentlichten „Vulkan Files“ zeigen, wie der russische Geheimdienst mit Hilfe des in Moskau ansässigen Rüstungsunternehmens NTC Vulkan Cyberangriffe orchestriert, Desinformationen verbreitet und das Internet zensiert.[18] Auf dem Schlachtfeld tut sich der Kreml hingegen schwer und greift auf technisch relativ simple sogenannte Kamikaze-Drohnen aus Iran zurück. Viele Indizien sprechen dafür, dass sich das russische Militär bei der Invasion der Ukraine vornehmlich auf die traditionelle Kriegsführung mit Panzern, Artillerie und Luftwaffe konzentriert hat. Laut Alex Karp, Chef des Big-Data-Unternehmens Palantir, ist Russland aufgrund des Mangels an eingesetzten KI-Technologien „massiv im Nachteil“.[19] Selbst die technisch erfolgreichen Cyber-Operationen Moskaus führten zu keinen operativen Vorteilen. Der zu Kriegsbeginn erfolgte Angriff auf den Provider Viasat legte zwar die Satellitenkommunikation über der Ukraine lahm,

---

8 How Russia killed its tech industry | MIT Technology Review.
9 Ukraine wants a robot army (wired.com).
10 Hacker im Cyberkrieg: Die kuriosesten Angriffe von Anonymous auf den Kreml (watson.de).
11 Demokraten-Hack 2016: Ukrainische Hacker wollen russischen Spion gehackt haben - Golem.de.
12 Ukraine A Living Lab for AI Warfare (nationaldefensemagazine.org).
13 Artificial intelligence helps drones destroy camouflaged Russian vehicles (gagadget.com).
14 Ukraine wants a robot army (wired.com).
15 One year on: 10 technologies used in the war in Ukraine - TechInformed.
16 Tech innovation helps Ukraine even the odds against Russia’s military might - Atlantic Council
17 Schon seit Oktober 2021 greifen dem FSB nahestehenden Hacker gezielt Konten von ukrainischen Organisationen an, im Januar 2022 identifizierten Experten von Microsoft eine großangelegte Malware-Operation. ACTINIUM targets Ukrainian organizations - Microsoft Security Blog; Destructive malware targeting Ukrainian organizations - Microsoft Security Blog.
18 Russlands Strategie der Cyberkriegsführung offengelegt – EURACTIV.de.
19 Palantir CEO Alex Karp on Responsible AI in Warfare | REAIM 2023 - YouTube.

verfehlte aber deutlich das Ziel, ukrainische Kommando- und Aufklärungsoperationen zu behindern.[20] Stattdessen führte er zu unbeabsichtigten Spillover-Effekten, indem er die Satellitenmodems deutscher Windkraftanlagen deaktivierte.

Russlands KI-Nachteil erklärt sich vor allem aus einem wichtigen **Systemunterschied**. Die Technologiesektoren der beiden Länder hängen von ihrem **jeweiligen Ordnungssystem** ab. In Russland entwickeln Staatsunternehmen im Auftrag der Regierung Rüstungsgüter, während es in der Ukraine ein breites privates Spektrum an Firmen, Start-ups und Tüftlern gibt.[21] Das ukrainische Waffenarsenal ist vielfältiger und daher schwieriger zu bekämpfen. Laut Fedorov verfügt die Ukraine über das notwendige IT-Talent und die Flexibilität, um neue technische Konzepte innerhalb kurzer Zeit „vom Reißbrett auf das Schlachtfeld" zu übertragen.[22] Im starken Kontrast dazu basieren auch die jüngsten Spionageaktivitäten des russischen Nachrichtendienstes auf vielen alten Elementen, die bereits aus früheren Kampagnen bekannt sind.[23] In dem Maße, in dem die von Putin reglementierte und vergraulte Technologiebranche Russlands ins Hintertreffen gerät, sinkt die Fähigkeit des Kremls, moderne militärische KI einzusetzen.

3 Auf dem Weg zu verantwortungsbewusster KI?

Auch wenn digitale Technologien dem Westen militärpolitische Vorteile bieten, werfen sie die Frage nach ihrer Beherrschbarkeit auf. Konkret könnte der verstärkte Einsatz von autonomen Funktionen und KI-Systemen im Ukraine-Krieg die **Entwicklung völlig autonomer Waffen beschleunigen**, deren Einsatz nie vollständig kontrolliert werden kann. Im vergangenen Jahrzehnt wurden Initiativen wie die 2012 gegründete „Campaign to Stop Killer Robots" populär. Potenziell unkontrollierbare Technologien sollten frühzeitig verboten werden, da sie nach Ansicht der Aktivisten Menschenrechte verletzen und so zu einer Zunahme von Konflikten führen.

Durch Russlands Angriffskrieg hat diese Debatte jedoch eine neue Qualität erhalten. Im Rahmen des ersten globalen Gipfels zu **verantwortungsbewusster KI** im militärischen Bereich, der Mitte Februar 2023 in den Niederlanden stattfand, präsentierte das US-Außenministerium eine sogenannte politische Erklärung, unter welchen Voraussetzungen derartige Waffen entwickelt werden sollten.[24] Diese Erklärung sieht kein Verbot militärischer KI vor, sondern listet abstrakt „best practices" auf. So heißt es, dass KI-Waffen nur im Einklang mit internationalen Gesetzen entwickelt werden dürften, wobei die technischen Prinzipien transparent sein sollten. Einige Forscher überlegten zudem, wie man autonome militärische Systeme so konstruieren kann, dass sie sich ethisch zumindest besser verhalten als konventionelle Soldaten.[25]

---

[20] Cyber Operations in Russia's War against Ukraine - Stiftung Wissenschaft und Politik (swp-berlin.org).

[21] Ukrainian developers use artificial intelligence for more accurate drones bombardment • Mezha.Media. Gleichwohl steht außer Frage, dass die ukrainische Wirtschaftsordnung weiter reformiert werden muss. Auch wenn momentan das Kriegsrecht die gesamte Wirtschaft und ihre Verwaltung den militärischen und sicherheitspolitischen Erfordernissen unterordnet, gab es bereits vor dem Krieg Defizite vor allem in Form von Korruption, beispielsweise in den Bereichen Justiz und Staatsunternehmen. Für eine Analyse, siehe: Reforming the Ukrainian Economy and State: The Unfinished Business | Publications | CESifo.

[22] Ukraine's millennial minister leads digital fight against Russia | The Hill.

[23] Espionage campaign linked to Russian intelligence services - Baza wiedzy - Portal Gov.pl (www.gov.pl).

[24] Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy, Department of State. Für eine Analyse, siehe: The US Pushing for Responsible AI in Military Use (holisticai.com).

[25] Arkin, R. (2009). Governing Lethal Behavior in Autonomous Robots (1st ed.). Chapman and Hall/CRC.

Eine auf ethischen Prinzipien basierende Verbotsforderung ist jedoch in der gegenwärtigen geopolitischen Lage nicht mehr vermittelbar, sie wäre aus westlicher Sicht sogar **naiv**. Der Ukraine-Krieg zeigt als quasi **tragisches Test-Labor**, dass KI in künftigen Konflikten eingesetzt werden wird – allen ethischen Grundsätzen zum Trotz. Zu verlockend sind die Vorteile auf dem Schlachtfeld, große Datenmengen analysieren, Feindbewegungen vorhersagen und auf etwaige Bedrohungen schnell reagieren zu können. Doch autonome KI-Waffen können auch im eigenen Lager zu unkontrollierbaren Problemen wie „friendly fire" führen. Deswegen ist es nicht nur aus ethischer, sondern auch aus militär-strategischer Sicht wichtig, frühzeitig **Strategien für ihre Überwachung** zu entwickeln, die frühere Fehler autonomer Systeme berücksichtigen.[26]

4 Aus der Vergangenheit lernen

Bisherige Erfahrungen mit automatisierten Militärsystemen offenbaren gravierende Probleme, die sich im KI-Zeitalter exponentiell steigern werden. Während des Irak-Krieges kam es beispielsweise zum Abschuss eines britischen Tornados durch die US-Marine. Ein Computer-Programm der Amerikaner hatte den Kampfjet **fälschlicherweise als irakische Rakete klassifiziert**. Die im Patriot-Flugabwehrsystem einprogrammierten Kriterien hätten angesichts der damaligen Kapazitäten des Irak viel enger gefasst werden müssen, wie eine parlamentarische Untersuchung später ergab.[27]

Dieser Vorfall wird in der **AI Incident Database**, einer Onlineenzyklopädie mit bekannten KI-Vorfällen, unter der Rubrik „folgenschwere Fehler" aufgelistet.[28] Die Datenbank enthält zahlreiche weitere Fälle, in denen automatische Waffensysteme aufgrund fälschlicher Klassifikationen zu unbeabsichtigten Opfern führten.[29] Experten bezweifeln, dass eine autonome Waffe jemals in der Lage sein wird, angemessen zwischen zivilen und militärischen Zielen zu unterscheiden.[30] Solche Systeme verstoßen daher gegen das sogenannte **Diskriminierungsprinzip**, wonach bei der Anwendung von Gewalt zwischen Militär und Zivilisten unterschieden werden muss.[31]

Die beschriebenen Klassifizierungsprobleme könnten sich bei der nächsten Generation militärischer KI, wie automatisierten Drohnenschwärmen, potenzieren. So benötigen KI-basierte Waffensysteme vollständige, relevante und granulare Daten, um trainiert zu werden. Durch die **dynamische, komplexe und feindselige Natur von Konfliktumgebungen** ist ihre Anwendung außerhalb von Laboren aber extrem fehleranfällig, da neue oder unvorhersehbare Faktoren nicht in den Trainingsdaten enthalten sind.[32] Das ändert sich nun: Mit jedem Tag, den der Ukraine-Konflikt andauert, werden KI-Systeme mit realen Daten von einem realen Schlachtfeld trainiert.[33] Das macht es für Länder wie China, das eigene Ambitionen für militärische KI-Systeme hegt, **attraktiver, Waffen zu liefern**, um von den Daten zu profitieren.

---

[26] Understanding the errors introduced by military AI applications (brookings.edu).
[27] maaszg710.doc (publishing.service.gov.uk).
[28] Atherton, Daniel. (2003-03-22) Incident Number 444. in Lam, K. (ed.) Artificial Intelligence Incident Database. Responsible AI Collaborative. Retrieved on March 1, 2023 from incidentdatabase.ai/cite/444.
[29] Atherton, Daniel. (2003-04-02) Incident Number 445. in Lam, K. (ed.) Artificial Intelligence Incident Database. Responsible AI Collaborative. Retrieved on March 1, 2023 from incidentdatabase.ai/cite/445.
[30] Kallenborn, Z. (2021). Meet the Future Weapon of Mass Destruction, the Drone Swarm. Bulletin of the Atomic Scientists, https://thebulletin.org/2021/04/meet-the-future-weapon-of-mass-destruction-the-drone-swarm/.
[31] Dresp-Langley Birgitta (2023), The weaponization of artificial intelligence: What the public needs to be aware of, Frontiers in Artificial Intelligence 6, https://www.frontiersin.org/articles/10.3389/frai.2023.1154184.
[32] Holland Michel, Arthur. 2021. Known Unknowns: Data Issues and Military Autonomous Systems. Geneva: United Nations Institute for Disarmament Research. https://doi.org/10.37559/SecTec/21/AI1.
[33] Ukraine A Living Lab for AI Warfare (nationaldefensemagazine.org).

5 Risiko: unbekannt und nicht überwachbar

Angesichts dieser Probleme besteht derzeit überwiegend Konsens darin, dass militärische KI-Systeme eine Kombination aus automatisierten Abläufen und menschlichen Eingriffsmöglichkeiten bieten sollten. Auch wenn die Einsicht in ein solches „**human in the loop**"-Modell grundsätzlich zu begrüßen ist, muss angesichts der folgenreichen Entscheidungen von Waffensystemen über Leben und Tod vor dem Irrglauben gewarnt werden, dass eine derartige Kombination aus Mensch und Maschine für eine sichere, robuste Nutzung ausreicht. Denn Menschen akzeptieren oft die empfohlene Entscheidung eines KI-Systems, selbst wenn sie falsch sein sollte – ein Problem, das als **KI-Overreliance**, oder „blindes Vertrauen" in KI, bezeichnet wird.

Mithin ist das Zusammenspiel von Mensch und Maschine schwierig abzuschätzen, weil Menschen nicht immer rational auf die Empfehlungen eines Computers reagieren.[34] So folgten Teilnehmer in einem Experiment den absichtlich schlecht programmierten Ratschlägen des Algorithmus auch dann noch, wenn sie es eigentlich längst hätten besser wissen müssen.[35] Manche Forscher hoffen, blindes Vertrauen in KI-Systeme zu reduzieren, indem sie diese zwingen, ihre **Entscheidungen zu erklären**. Doch Tests zufolge erhöhen solche Erklärungen lediglich die Wahrscheinlichkeit, dass Menschen die Empfehlung der KI akzeptieren – unabhängig davon, ob sie korrekt ist.[36]

Eine Lösung, die zumindest experimentell funktioniert, besteht darin, nicht nur eine Erklärung bereitzustellen, sondern die Menschen auch zu ermutigen, sich mit dieser kognitiv auseinanderzusetzen.[37] Es ist allerdings fraglich, ob für einen derart ausgefeilten Prozess genügend Zeit bleibt, wenn es auf dem Schlachtfeld um Millisekunden geht. Militärische KI behandelt komplexe Aufgaben, was impliziert, dass die KI-Erklärungen oft genauso komplex zu verstehen sein werden wie die Aufgabe selbst. Ein Experte, der sich mit den angesprochenen „friendly fire"-Vorfällen im Irak auseinandergesetzt hat, warnt davor, dass die Details des Einsatzes ballistischer Raketen „**zu komplex und zeitlich zu begrenzt** für eine direkte menschliche Beteiligung" sind.[38]

6 Ein risikobasierter Ansatz mit strukturierten Tests

Während KI im Militärbereich zunehmend relevant und zugleich fehleranfällig wird, hinkt die Debatte über ihre Regulierung hinterher.[39] Es gibt **keine multilateralen Vereinbarungen**, **Zertifizierungsprozesse oder globalen Standards**, die robuste und vertrauenswürdige KI-Waffensysteme sicherstellen. Bezeichnenderweise ist die erwähnte US-Erklärung über verantwortungsvolle militärische KI nicht rechtsverbindlich. Die aktuellen UN-Verhandlungen zu letalen autonomen Waffensystemen in Genf treten auf der Stelle.[40] Doch solche Regeln sind dringend geboten, da ein ethisches Design von KI-Waffen laut einem führenden Informatiker zwar „theoretisch interessant" aber „nicht praktikabel" ist.[41]

---

[34] Algorithmic Risk Assessment in the Hands of Humans (iza.org).

[35] Biermann, Jan and Horton, John J. and Walter, Johannes, Algorithmic Advice as a Credence Good (2022). ZEW - Centre for European Economic Research Discussion Paper No. 22-071, http://dx.doi.org/10.2139/ssrn.4326911.

[36] [2006.14779] Does the Whole Exceed its Parts? The Effect of AI Explanations on Complementary Team Performance (arxiv.org).

[37] [2212.06823] Explanations Can Reduce Overreliance on AI Systems During Decision-Making (arxiv.org).

[38] Patriot Wars | Center for a New American Security (en-US) (cnas.org).

[39] Amazon.com: Death machines: The ethics of violent technologies: 9781526114846: Schwarz, Elke: Bücher.

[40] Verhandlungen von der CCW in die UNO? - Tagesspiegel Background.

[41] Michael Wooldridge, A Brief History of Artificial Intelligence, New York 2020, S. 195.

Inspiration könnte vom **KI-Gesetz** kommen, dass die EU-Gesetzgeber zurzeit ausverhandeln. Der Vorschlag folgt einem **risikobasierten Ansatz**, da er besonders schädliche KI-Praktiken verbietet. Auch wenn der aktuelle Gesetzesvorschlag der EU militärische KI-Systeme explizit ausschließt, können sein Rahmen und die horizontalen Anforderungen auch für KI-Anwendungen im militärischen Bereich zur Entwicklung relevanter Normen beitragen.[42] So wären analoge Kategorisierungen denkbar, nach denen tödliche autonome Waffen verboten würden, während alle anderen militärischen KI-Systeme Anforderungen bezüglich Risikomanagement, Dokumentation, Transparenz, Überprüfbarkeit, Robustheit und Cybersicherheit erfüllen müssten.

Da Menschen bei der Überwachung von KI-Empfehlungen oft versagen, muss die Wirksamkeit von militärischen „human-in-the-loop"-Modellen **strukturiert evaluiert** werden.[43] Eine solche transparente Dokumentation würde einen rationaleren politischen Diskurs über dieses Thema fördern, weil bisherige Forschungen zu autonomen Waffensystemen fast ausschließlich unter Verschluss im militärischen Bereich Anwendung finden.[44] Wenn sich bei diesen Tests herausstellt, dass Menschen sogenannte Killer-Drohnen oder andere KI-Systeme nicht effektiv kontrollieren können, sollten sie in die Kategorie verbotener militärischer KI eingetragen werden.

Russlands Angriff auf die Ukraine sowie die steigenden geopolitischen Spannungen mit China zwingen westliche Politiker, sich ernsthaft mit der Nutzung militärischer KI auseinanderzusetzen. Doch die potenziellen Folgen eines Einsatzes KI-getriebener Waffen sind nur vage abschätzbar. Deshalb muss die Öffentlichkeit für die **Gefahren sensibilisiert** werden. Aufgabe der Politik ist es, mit rechtlichen Kategorisierungen, Transparenzpflichten und strukturierten Tests der menschlichen Überwachbarkeit dieser Systeme **verbindliche Rahmenbedingungen** zu setzen.

[42] Challenges of Governing AI for Military Purposes and Spill-Over Effects of the AI Act | Futurium (europa.eu).
[43] Analog für andere KI-Bereiche: The AI Act should use humans to monitor AI only when effective – EURACTIV.
[44] Dresp-Langley Birgitta (2023), The weaponization of artificial intelligence: What the public needs to be aware of, Frontiers in Artificial Intelligence 6, https://www.frontiersin.org/articles/10.3389/frai.2023.1154184.

Centrum für Europäische Politik
FREIBURG | BERLIN

Autor:

Dr. Anselm Küsters, Fachbereichsleiter Digitalisierung & Neue Technologien
kuesters@cep.eu

Dr. Jörg Köpke, Leiter Kommunikation Centrum für Europäische Politik
koepke@cep.eu

Centrum für Europäische Politik FREIBURG | BERLIN
Kaiser-Joseph-Straße 266 | D-79098 Freiburg
Schiffbauerdamm 40 Räume 4205/06 | D-10117 Berlin
Tel. + 49 761 38693-0

Das **Centrum für Europäische Politik** FREIBURG | BERLIN, das **Centre de Politique Européenne** PARIS, und das **Centro Politiche Europee** ROMA bilden das **Centres for European Policy Network** FREIBURG | BERLIN | PARIS | ROMA.

Das gemeinnützige Centrum für Europäische Politik analysiert und bewertet die Politik der Europäischen Union unabhängig von Partikular- und parteipolitischen Interessen in grundsätzlich integrationsfreundlicher Ausrichtung und auf Basis der ordnungspolitischen Grundsätze einer freiheitlichen und marktwirtschaftlichen Ordnung.