Im vorliegenden Beitrag wird die These vertreten, dass die Bundesrepublik Deutschland sich der KI (Künstlichen Intelligenz) aus sicherheitspolitischer Sicht widmen muss, um ihre Verteidigungsfähigkeit angesichts der Zeitenwende auch in Zukunft gewährleisten zu können. Damit dies erfolgreich gelingen kann, gilt es, die nationalen industriepolitischen Forderungen mit einzubeziehen und den notwendigen Kontext in die meist generische KI-Debatte zu bringen. Wie dies erfolgreich funktionieren kann, zeigt sich anhand der komparativen Analyse ausgewählter Nachbarländer (Frankreich und UK), die gemeinsam mit ihrer nationalen Industrie und Wissenschaft an technologischen Lösungen für den militärischen KI-Einsatz arbeiten. Weiterhin gilt es im Rahmen des globalen Wettstreites um die KI-Vorherrschaft, aus europäischer Sicht die Vorhand zu gewinnen, um in dem sich veränderten globalen Verteidigungs- und Sicherheitsumfeld adäquat verteidigungs- und abschreckungsfähig zu sein. Dabei wird die Frage diskutiert, ob die von der EU in Gestalt des sogenannten AI-Act geplante Herangehensweise zur Erreichung dieses Ziels geeignet ist oder die Industrie allzu sehr in ihren technologischen Entwicklungsmöglichkeiten beschränken könnte.

Zu den industriepolitischen Folgerungen des Einsatzes Künstlicher Intelligenz im militärischen Bereich

Dr. Hans Christoph Atzpodien, Nawal Solh

Einleitung

In abstrakter Form war bereits vor dem russischen Angriff auf die Ukraine klar, dass Krieg als Mittel zur Durchsetzung politischer Ziele keineswegs undenkbar geworden ist. Ebenso bewusst war uns, dass ein heutiger Krieg mit ganz anderen Mitteln geführt würde als im 20. Jahrhundert. Zu nennen ist etwa die Erweiterung des „Gefechtsfeldes" um die Dimension Cyber und damit auch die weitere Abkehr vom „Krieg rein zwischen Kombattanten". Angriffe auf digitalisierte (kritische) Infrastrukturen und die IT allgemein, die beispielsweise Ausfälle in der Kommunikation oder Stromversorgung zur Folge haben oder in massiver Form Fehlinformationen in Bevölkerungsgruppen einsteuern, können erheblichen Schaden in einem auf Nachhaltigkeit ausgerichteten Gesellschaftssystem anrichten. In den Blick genommen werden muss zudem die unaufhaltsam fortschreitende Automatisierung und Autonomisierung von Waffensystemen, die eine völlig neue Form der Bedrohung darstellen. Eine Folge mag sein, dass zwar die Auseinandersetzungen zwischen solchen Systemen weniger einschneidend sein werden, dass sich aber die Bedrohungen umso mehr auf andere Felder verlagern, etwa auf die Zerstörung unserer zivilgesellschaftlichen Lebensadern. Denkbar erscheint auch, dass es bei feindseligen Auseinandersetzungen in Zukunft vor allem darum geht, wer im Rahmen eines *Information Warfare* in welcher Form über wen eine datengestützte Meinungsherrschaft ausüben kann.

In diesen Szenarien wird der Einsatz der Künstlichen Intelligenz (KI) eine entscheidende Rolle spielen. Hierbei ist zu betonen, dass der KI-Begriff zu generisch und kontextlos verwendet wird. Dies lässt sich auf das Fehlen einer allgemeingültigen Definition, insbesondere der Abstufung von KI, zurückführen. Das führt dazu, dass der KI-Begriff je nach Belieben oder Zweck (zum Teil auch synonym für Autonomie) verwendet wird. Mit entsprechend negativen Folgen für den Diskurs sowie für die gesellschaftliche Akzeptanz des Einsatzes von KI für Sicherheits- und Verteidigungszwecke. Um dem entgegenzusteuern und das Potenzial von KI-geführten Technologien zu beleuchten, sollte Deutschland in Erwägung ziehen, militärische KI als wichtigen Bereich in die nationale KI-Strategie zu integrieren und zukünftig eine eigene militärische KI-Strategie zu konzipieren.[1] Argumente für diese Maßnahmen sind zahlreich und werden von dem sich grundlegend veränderten Sicherheitsumfeld bekräftigt.

Die Bundesrepublik Deutschland muss sich der KI aus sicherheitspolitischer Sicht widmen, um ihre Verteidigungsfähigkeit auch in Zukunft gewährleisten zu können. Sie muss technologisch in der Lage sein, Angriffe mit KI-unterstützten Waffensystemen abzuwehren. Das Ziel, die eigene Verteidigungsfähigkeit zu stärken, hat höchste Priorität. Weiterhin wird von Deutschland erwartet, seine Führungsrolle zu erfüllen, sei es im Rahmen der NATO, der Europäischen Union oder der deutsch-französischen Zusammenarbeit. Grundvoraussetzung dafür ist die Abkehr von der in Deutschland dominierenden „Killerroboter"-Debatte.[2] Anstelle einer Angst-Risiko-Betrachtung brauchen wir eine ausgewogene Potenzial-Risiko-Betrachtung. Das im Hinblick auf den Personalmangel bei der Bundeswehr, den Schutz der Soldatinnen und Soldaten und vor allem auf die Notwendigkeit von KI für unsere Landesverteidigung.[3, 4] Dabei darf die Sicherheits- und Verteidigungsindustrie nicht daran gehindert werden, die für Abwehr-, Abschreckungs- und Verteidigungszwecke notwendigen Technologien zu entwickeln, und zwar im Interesse der inneren und äußeren Sicherheit Deutschlands, der EU sowie der NATO. Auch aus industrieller Sicht muss das Ziel sein, alles Erforderliche tun zu können, damit unser Land innerhalb seiner Bündnisstrukturen auch in Zukunft adäquat verteidigungsfähig ist.

Die Industrie und deren kommerzielle Anreiz-Mechanismen sollten immer als Hauptantriebskräfte der Innovation betrachtet werden.

Herausforderungen für die Positionierung Deutschlands

Ab 2014 entstand durch die Annexion der Krim eine neue Wahrnehmung in der Weise, dass auch wir in Europa einer durchaus neuen Bedrohungslage gegenüberstehen. Russlands völkerrechtswidriger Angriff auf die Ukraine und die in diesem Zusammenhang von Bundeskanzler Olaf Scholz ausgerufene Zeitenwende in der Sicherheits- und Verteidigungspolitik sollten zugleich Anlass für die Bundesregierung sein, sich intensiv mit dem Thema KI für die Landesverteidigung zu beschäftigen. Denn eins ist klar: Viele Staaten sind uns bereits einen großen Schritt voraus und arbeiten gemeinsam mit ihrer nationalen Industrie und Wissenschaft an technologischen Lösungen für den militärischen KI-Einsatz. Hier ein kurzer Blick auf unsere Nachbarn sowie auf die NATO.[5]

Frankreich

Im Gegensatz zu Deutschland nimmt sich die Politik in Frankreich aktiv des Themas an und hat als erster europäischer Staat 2019 eine Strategie für militärische KI veröffentlicht.[6] Dabei betrachtet das Land den militärischen Bereich als ein wichtiges Element seiner KI-Entwicklungsbemühungen. Bereits in dem 2018 veröffentlichten Villani-Report wurde die Notwendigkeit von KI in der Zukunft betont, um sowohl Sicherheitsmissionen zu gewährleisten als auch die Macht über potenzielle Gegner zu erhalten und die Position Frankreichs gegenüber seinen Verbündeten zu wahren.[7] Der Aspekt der Souveränität wird weiterhin in der nationalen Sicherheitsstrategie aufgegriffen. Darin wird betont, dass in einem Kontext, der von ausländischen privaten oder staatlichen Akteuren beherrscht wird, Frankreich sich nicht damit abfinden kann, von Technologien abhängig zu sein, über die es keine Kontrolle hat.[8] Im speziellen Fall der militärischen KI und um die Vertraulichkeit und Kontrolle der nationalen Informationen zu gewährleisten, ist es unerlässlich, dass die technologische Souveränität bewahrt wird. Dies lässt sich auch als Aufgabe für die nationale Industrie übersetzen, die gemeinsam mit dem Staat an technologischen Lösungen arbeiten soll und für die hohe Investitionen vorgesehen sind.[9] Frankreichs Attitüde zu KI kann als Chance für die Bundesregierung gesehen werden, um in Zukunft mit Frankreich in der KI-Forschung zusammenzuarbeiten. Diese deutsch-französische Zusammenarbeit stellt für die französische Seite ein weiteres nationales strategisches Ziel dar.

Dem Beispiel Frankreichs und des Vereinigten Königreichs folgend sollte Deutschland eine eigene militärische KI-Strategie konzipieren.

Vereinigtes Königreich

Ein weiteres Beispiel für eine entemotionalisierte und sachliche Auseinandersetzung mit der Thematik lässt sich in der im Juni 2022 veröffentlichten *UK Defence Artificial Intelligence Strategy* wiederfinden. Verteidigungsminister Ben Wallace betont, dass KI ein enormes Potenzial zur Verbesserung der Fähigkeiten hat, jedoch allzu oft als potenzielle Bedrohung dargestellt wird: „KI-gestützte Systeme stellen in der Tat eine Bedrohung für unsere Sicherheit dar, wenn sie in den Händen unserer Gegner sind, und wir müssen unbedingt verhindern, dass wir ihnen einen entscheidenden Vorteil verschaffen.“[10] Die UK-Strategie zielt darauf ab, das KI-Ökosystem des Vereinigten Königreichs im Bereich Verteidigung und Sicherheit zu stärken und dabei die grundlegende Notwendigkeit der Zusammenarbeit mit Partnern aus Regierung, Industrie und Wissenschaft anzuerkennen.

Im Vergleich zwischen Deutschland, Frankreich und dem Vereinigten Königreich wird sehr schnell deutlich, dass fehlende Kooperation sowie unterschiedlicher Umgang mit militärischer KI künftig die europäische Verteidigungszusammenarbeit gefährden kann und die Verteidigungsindustrien aller drei Länder KI-bezogene Fähigkeiten nicht unabhängig von den Positionen ihrer Regierungen entwickeln können.[11]

NATO

Dies hat auch die NATO in den letzten Jahren verstanden, angetrieben durch den globalen Wettstreit um die KI-Vorherrschaft, aber auch durch Chinas und Russlands zunehmende Investitionen in militärische KI sowie angesichts des veränderten globalen Verteidigungs- und Sicherheitsumfeldes.[12] Am 21. Oktober 2021 einigten sich die NATO-Verteidigungsminister auf die erste NATO-Strategie für Künstliche Intelligenz. Generalsekretär Jens Stoltenberg sagte, die Bemühungen seien eine Reaktion auf „autoritäre Regime, die um die Entwicklung neuer Technologien ringen“[13]. Die Strategie stützt sich auf eine umfassende Zusammenarbeit zwischen der NATO, der Privatwirtschaft und der Wissenschaft, auf einen fähigen Mitarbeiterstab aus technischen und politischen KI-Talenten der NATO, auf eine robuste, relevante und sichere Dateninfrastruktur sowie auf angemessene Cyber-Abwehrmaßnahmen.[14]

Die NATO-Verbündeten und Partnerstaaten haben einen starken Anreiz, eng zusammenzuarbeiten, um technologisch einen Vorsprung vor ihren Gegnern bewahren zu können.[15] Damit dies gelingen kann, werden Standardisierungen und Regulierungen benötigt. Im Zuge dieser Bemühungen wurde in einem zweiten Schritt beim NATO-Gipfel 2022 in Spanien ein neues strategisches Konzept verabschiedet, in welchem das Thema KI-Technologie enorm an Bedeutung gewonnen hat. In diesem aktuell wichtigsten Dokument des Bündnisses nimmt KI nun einen großen Raum in der kollektiven Verteidigungsorientierung ein, wobei dieses Commitment mit dem geplanten *Innovation Fund* noch einmal an Glaubwürdigkeit gewinnt. Der eine Milliarde US-Dollar schwere neue NATO-Innovationsfonds soll mit dem „Defense Innovation Accelerator for the North Atlantic" (DIANA) zusammenwirken, der ebenfalls im neuen strategischen Konzept der NATO erwähnt wird.[16] Ziel ist es, Regierungen, den Privatsektor und die Wissenschaft zusammenzubringen, um den technologischen Vorsprung gewährleisten zu können und damit die kollektive Verteidigungsfähigkeit zu garantieren. Dabei beabsichtigt Frankreich, den Zugang zu französischen Einrichtungen – wie Testzentren und Beschleunigerstandorten – zu erleichtern, die aus dem sehr umfangreichen und vielfältigen französischen Innovationssektor stammen. In Deutschland ist lediglich ein Testcenter vorgesehen, was die Positionierung Deutschlands zu KI im Rahmen des Bündnisses ein Stück weit relativiert. Generalsekretär Stoltenberg betont im Zuge dessen: „Mit einem Zeitrahmen von 15 Jahren wird der NATO-Innovationsfonds dazu beitragen, jene im Entstehen begriffenen Technologien zum Leben zu erwecken, die unsere Sicherheit in den kommenden Jahrzehnten verändern können, das Innovationsökosystem des Bündnisses stärken und die Sicherheit unserer eine Milliarde Bürgerinnen und Bürger stärken."[17] In der Theorie bedeuten diese Strategie sowie die vorgeschlagenen Maßnahmen ohne Zweifel einen Schritt in die richtige Richtung. Jedoch stellt die Tatsache, dass sich die NATO-Mitglieder in sehr unterschiedlichen Stadien befinden, wenn es darum geht, über KI im militärischen Kontext nachzudenken, in der Praxis ein Problem dar.

Militärische KI in Deutschland

Ein Beispiel dafür ist Deutschland, das bisweilen dafür kritisiert wird, sich nur langsam mit dem Thema militärische KI auseinandergesetzt

zu haben, obwohl viele deutsche Unternehmen exzellente Arbeit in diesem Bereich leisten. Vielfach wurden in Deutschland ethische, moralische und rechtliche Beschränkungen gegen militärische KI-Anwendungen geltend gemacht, jeweils auch mit Konsequenzen für die künftige Wettbewerbsfähigkeit der deutschen Sicherheits- und Verteidigungsindustrie vor dem Hintergrund eines großen internationalen Konkurrenzdrucks.[18] Dabei darf die deutsche Sicherheits- und Verteidigungsindustrie nicht den Anschluss an die technische Entwicklung anderer Länder verlieren, in denen militärische KI seit Langem eine Schlüsselrolle spielt (wie in den USA und Israel). Dies ist auch im nationalen Interesse, da KI als Motor des zukünftigen Wirtschaftswachstums dienen wird, sei es im zivilen oder im militärischen Bereich. Dies lässt sich aus einer McKinsey-Studie aus dem Jahr 2017 entnehmen. Die Studie prognostiziert, dass bis 2030 das Bruttoinlandsprodukt (BIP) Deutschlands durch den frühen und konsequenten Einsatz von intelligenten Robotern und selbstlernenden Computern um bis zu vier Prozent oder umgerechnet 160 Milliarden Euro höher liegen könnte als ohne den Einsatz von KI.[19]

KI für die Landesverteidigung

Angesichts der Zeitenwende und der Gefahrenlage werden die politisch Verantwortlichen auch hierzulande die Einführung von militärischen KI-Lösungen als notwendig ansehen müssen, nicht zuletzt auch bei der Bewaffnung des Cyberspace. Dies wird deutlich in dem von Bossong, Rieks und Koch veröffentlichten *FAZ*-Artikel „Künstliche Intelligenz für die Landesverteidigung“. Die Autorinnen und Autoren argumentieren, dass Deutschland auch die militärischen Möglichkeiten dieser Schlüsseltechnologie verstehen und einbeziehen muss, um drohende Gefahren abwehren zu können und um einen Einfluss auf die weitere Entwicklung zu behalten. Dies geht nach Auffassung der Autorinnen und Autoren Hand in Hand mit einem verantwortlichen Umgang mit KI, wie am Beispiel des deutsch-französischen Kampfflugzeugprojektes „Future Combat Air System“ (FCAS) zu erkennen ist.[20]

Künstliche Intelligenz war in Deutschland lange genug in erster Linie eine wirtschaftliche Frage und eine gesellschaftliche Herausforderung, wie es an den bereits erwähnten „Killerroboter“-Debatten zu erkennen war. Hierzu erklärt Ulrike Franke, „dass Deutschland eine gewisse

Abneigung gegen KI zeigt, die dazu führt, dass die öffentliche und die politische Debatte sich eher für mögliche Verbote in Bezug auf diese Systeme interessiert und eher weniger, wie man Elemente davon auch selbst einsetzen will“[21]. Der Grund dafür sei historischer Natur.

Die geopolitischen und militärischen Aspekte der KI-Nutzung sind erst in den letzten Monaten zu einem Reflexionsgegenstand geworden, an dem unbedingt weitergearbeitet werden sollte. Dafür bedarf es eines nationalen politischen Willens, eine neue KI-Strategie auszuarbeiten, in der die Bundesregierung militärische KI als wichtigen Bereich integriert oder sogar, wie Frankreich und Großbritannien, eine eigene militärische KI-Strategie konzipiert. In dieser gilt es zu klären, wie Entwicklung und Anwendung militärischer KI für unsere Streitkräfte und deren Ausrüster verantwortungsvoll gestaltet werden können.

Herausforderungen für die Positionierung der deutschen Sicherheits- und Verteidigungsindustrie

Dem „Strategiepapier der Bundesregierung zur Stärkung der Sicherheits- und Verteidigungsindustrie“ vom 12. Februar 2020 folgend, ist es im nationalen Interesse, das industrielle KI-Know-how im Bereich Sicherheit und Verteidigung zu schützen sowie dafür einen Rechtsrahmen und Standards zu etablieren, die Unternehmen Rechtssicherheit bieten.[22] Diese wiederum sind notwendig, um zum einen die Entwicklungsfreiräume im Rahmen der etablierten Regularien zu erhalten und zum anderen Bundeswehr und NATO als industrielle Partner dienen zu können. Während über die letzten Jahrzehnte hinweg ein erheblicher Teil der Forschung in staatlich finanzierten Laboren und Universitäten durchgeführt wurde, findet heute der größte Teil der KI-Spitzenforschung in privaten Unternehmen statt.[23] Darüber hinaus sollte vor allem der Austausch zwischen ziviler und militärischer KI-Forschung in Deutschland keinen Restriktionen unterliegen, um zu vermeiden, dass mögliche positive Effekte aus einem solchen Austausch verhindert werden. Sicher ist, dass man nicht von strategischer Autonomie in Europa sprechen könnte, wenn Deutschland oder Europa insgesamt nicht bereit wären, diesen Anspruch auch materiell, mit „State-of-the-Art-Waffentechnologien“ zu unterfüttern.

Die Mensch-Maschine-Interaktion

Dabei muss geklärt werden, wie Entwicklung und Anwendung militärischer KI für unsere Streitkräfte und deren Ausrüster verantwortungsvoll gestaltet werden können. Es bedarf einer gesellschaftspolitischen Akzeptanz, die es den Streitkräften und der Industrie erlaubt, mit diesen Technologien umzugehen, sie weiterzuentwickeln und sie im Verteidigungs- und Bündnisfall entsprechend einzusetzen. Hierbei erweist sich die Debatte über die Rolle des Menschen, insbesondere mit Blick auf die sogenannte *Meaningful Human Control* (MHC), vielfach als Hürde. Gleichermaßen finden Themen wie Drohnen oder auch autonome Waffensysteme oftmals nicht in einer auf Fakten basierten Debatte, sondern in einer emotionalen Diskussion statt. Es wird über die Forderung nach einem *Human in the Loop* diskutiert, aber zu wenig darüber, was wir eigentlich machen, wenn andere Staaten über Systeme verfügen und diese zum Einsatz bringen, die ihrerseits auf derartige ethisch-bedingte Restriktionen keine Rücksicht nehmen beziehungsweise allein aufgrund der Geschwindigkeit des Angriffs und der hohen Reaktionszeit des Menschen keinen Raum für den *Human in the Loop* mehr lassen.

Um sachgerechte Antworten zu geben, ist es wichtig, sich einen Überblick über die heutigen Herausforderungen zu verschaffen, die den Bedarf an Automatisierung (einschließlich des Einsatzes von KI) im Verteidigungsbereich vorantreiben. Zu den Herausforderungen gehören die Kriegführung „in Maschinengeschwindigkeit", die Komplexität des Schlachtfeldes, die Datenflut und die Tatsache, dass mögliche Gegner im Zweifel alle verfügbaren autonomen Waffensysteme auch einsetzen werden. Letztendlich geht es im Bereich rein defensiver Mittel bei der Entwicklung von militärischen Fähigkeiten stets darum, einem potenziellen Gegner überlegen zu sein. In diesem Sinne sollte militärische KI als *Enabler* gesehen werden, primär um Abschreckung gewährleisten, aber auch im Falle eines Angriffs durch Dritte in der Abwehr technologisch überlegen agieren zu können.

Um mehr Realismus in die Debatte zu bringen, hat die AeroSpace and Defence Industries Association of Europe (ASD) eine Systematik der ethischen Angemessenheitsprüfung von *Meaningful Human Control* beim Einsatz von KI in Waffensystemen entwickelt.[24] Hiernach wird ein teilweiser Verzicht auf unmittelbare *Human Control* eines KI-gestützten Defensivsystems umso eher gerechtfertigt, je höher

der *Impact* einer Bedrohung oder eines Angriffs ist. Lässt also die Art der Bedrohung zu ihrer wirksamen Bekämpfung keine menschliche Intervention mehr zu, wie im Beispiel von *Fight at Machine Speed*, so ist sie nach diesem ethischen Maßstab auch nicht zu fordern.[25] Darüber hinaus betont die ASD, dass KI in diesem Verständnis als ein Instrument gesehen werden muss und somit keine Waffe an sich ist.

EU AI Act

Wenn es um die Frage geht, ob und in welchen Formen wir KI nutzen sollen oder nicht, stehen wir vor keiner Wahl, es nicht zu tun. Alles andere wäre aus verteidigungspolitischer Sicht eine Art Selbstaufgabe. Es geht also nicht um die Frage des „Ob", sondern nur um das „Wie". Natürlich bedarf es in der EU bestimmter Regularien für die Unternehmen, die an militärischen KI-Lösungen arbeiten. Jedoch ist der Versuch, Technologien zu regulieren, die noch nicht entwickelt wurden, schwieriger, als die Regelung jener Technologien, deren Fähigkeiten, Auswirkungen und Merkmale bereits bekannt sind. Konkret zeigt sich diese Schwierigkeit an der im April 2021 von der Europäischen Kommission vorgeschlagenen Verordnung über Künstliche Intelligenz, auch bekannt als *Artificial Intelligence Act* (EU AI Act).[26] Diese Verordnung soll für Entwickler, Hersteller und Anwender verbindliche Anforderungen für die Entwicklung und Anwendung von KI-Systemen festlegen, bevor diese auf den Markt gebracht oder in Gebrauch genommen werden.

Dies stellt an sich schon ein Hindernis dar, das gegebenenfalls als Innovationshemmnis gesehen werden kann. Kritik kommt von Katerna Yordanova, die sich auf die Bereiche Menschenrechte im digitalen Umfeld und der Wirtschaft spezialisiert hat. Sie erklärt, dass es in der Tat besorgniserregend sei, KI-Praktiken EU-weit auf der Grundlage von Kriterien zu verbieten, die alles andere als eindeutig sind.[27] Dabei erweist sich vor allem Artikel 5 des Verordnungsentwurfs als fragwürdig, in dem KI-Anwendungen mit „unannehmbarem Risiko" verboten werden. Dies erzeugt nämlich den Eindruck, dass die Kommission sich mehr für den deklaratorischen Wert der Verbote als für ihre praktische Wirkung interessiert.[28] So könnte man annehmen, dass die Bedeutung der dort gelisteten Verbotstatbestände für die nationale oder gar europäische Sicherheit bei der Konzeption der Verordnung weitgehend ausgeblendet wurde. Zwar wird im Fall

Militär eine Ausnahme dahingehend gemacht, dass ausschließlich für militärische Zwecke entwickelte oder verwendete KI-Systeme von dem Verbot ausgeschlossen werden. Jedoch ist bekannt, dass in der Industrie auch solche KI-Technologien entwickelt werden, die zunächst nicht rein militärischen Zwecken dienen, im weiteren Entwicklungsgang aber militärische Ausprägungen erfahren, die erst dann rein militärischen Zwecken dienen. Nur in seltenen Fällen werden KI-Lösungen von vornherein ausschließlich für militärische Zwecke entwickelt. Dies begründet die Gefahr, dass die EU-ansässige KI-anwendende Industrie aus KI-bezogenen Entwicklungen bereits lange vor dem Zeitpunkt ausscheiden muss, an dem sich die Entwicklung als eindeutig für militärische Zwecke bestimmt kategorisieren und damit von dem genannten Verbotstatbestand ausnehmen lässt. Dies wäre fatal für die Entwicklungsperspektiven der EU-basierten KI-Industrie und würde im Zweifel dazu führen, dass sich die in der EU beheimateten Streitkräfte stattdessen mit einschlägigen KI-Produkten etwa aus den USA oder Israel versorgten. Plakativ gesprochen kann man dies als eine drohende Selbstamputation militärischer KI-Entwicklungen und -Anwendungen in EU-Europa bezeichnen.

Artikel 6 des geplanten AI Act, der sich mit Hochrisiko-KI-Systemen befasst, findet ebenfalls zahlreiche Kritikerinnen und Kritiker. Der Hauptgeschäftsführer der Vereinigung der Bayerischen Wirtschaft e. V. (vbw), Bertram Bosse, erklärte dazu, dass es für die Zukunftsfähigkeit unseres Wirtschaftsstandortes entscheidend sei, die Chancen Künstlicher Intelligenz aktiv zu nutzen. Indem er den von der Europäischen Kommission gewählten risikobasierten Ansatz generell unterstützt, kritisiert er jedoch die Definition des Hochrisikobereichs, der zu weit gefasst sei. Seiner Meinung nach, die sicherlich auch von vielen Akteuren aus der Sicherheits- und Verteidigungsindustrie geteilt wird, darf nicht jede Sicherheitskomponente von Maschinen unter diese Regelung fallen, da sonst die Industrie 4.0 ausgebremst wird.[29]

Ähnliche Stimmen kommen vonseiten der Politik. „Während wir risikoreiche KI-Systeme regulieren sollten, würden unverhältnismäßige Anforderungen an KI-Produkte und -Dienstleistungen Forschung und Innovation sowie unser europäisches Wachstumspotenzial und unsere internationale Wettbewerbsfähigkeit schwächen“, sagt Axel Voss, Mitglied des Europäischen Parlamentes. „Statt Verbote für ganze Aspekte der KI, wie zum Beispiel

die Gesichtserkennung, obwohl solche Technologien auch Vorteile für unsere Sicherheit bieten, sollten wir uns an das Prinzip ‚so viel wie nötig, so wenig wie möglich' halten."[30] Denn nur so verhindern wir, dass die Regularien zu Innovationsbremsen werden und unsere Unternehmen vor einer Art „Flaschenhalsproblematik" stehen, in denen sie aus Angst vor hohen Strafen bestimmte Innovationen von vornherein meiden. Bei aller grundsätzlichen Berechtigung von Restriktionen im Umgang mit ethisch kritischen KI-Anwendungen erfordert die Innovations- und Wettbewerbsfähigkeit, dass die geplante EU-Gesetzgebung für militärische und sicherheitsrelevante Anwendungen angemessene Ausnahmetatbestände schafft, die auch der entwickelnden Industrie zugutekommen und diese nicht vom weltweiten Wettbewerb abschneiden. Die beabsichtigte Überregulierung wird die Forschungsstandorte in Deutschland und Europa gefährden sowie das von der Europäischen Kommission erklärte Ziel, „europäische technologische Souveränität" zu erreichen, in weite Ferne rücken.[31] Stattdessen wird es möglicherweise dazu kommen, dass militärische KI-Systeme aus Drittstaaten beschafft werden.

Weitere Sorgen bezüglich des geplanten EU AI Act kommen vor allem von kleinen und mittelständischen Unternehmen, dem Rückgrat der deutschen und europäischen Sicherheits- und Verteidigungswirtschaft.[32] Die Unternehmen müssen geeignete Maßnahmen ergreifen, um sicherzustellen, dass sie das Gesetz einhalten, was auf Unternehmensebene zusätzliche Kosten verursachen wird. Dies wird deutlich bei den spezifischen Bestimmungen des AI Act für „hochriskante" KI. Darunter fallen der Aufbau eines Qualitätsmanagementsystems, Erstellung und Pflege der technischen Dokumentation, die Durchführung einer Konformitätsbewertung (und Wiederholung von Bewertungen, wenn das KI-System wesentliche Änderungen erfährt), die Gewährleistung der menschlichen Aufsicht über das System und die Überwachung mit Blick auf potenzielle Risiken sowie die Sicherstellung, dass das KI-System mit anderen einschlägigen Rechtsvorschriften (wie der Datenschutz-Grundverordnung) in Einklang steht. Benjamin Mueller, leitender politischer Analyst am Center for Data Innovation mit Schwerpunkt auf KI und Technologie-Governance, geht davon aus, dass die rechtliche Komplexität des geplanten Gesetzes und die damit verbundenen Compliancekosten eine abschreckende Wirkung auf Investitionen in KI haben werden.[33] Ähnliches berichtet die Europäische Investitionsbank, die in ihrem Investment Report 2020/2021 die

Tatsache betont, dass die Europäische Union nicht viele Innovationsführer hervorzubringen scheint, insbesondere im digitalen Bereich, was ihre langfristige Wettbewerbsfähigkeit gefährden könnte.[34]

Fazit

Die Industrie und deren kommerzielle Anreizmechanismen sollten immer als Hauptantriebskräfte der Innovation betrachtet werden. Im Rahmen der sicherheitspolitischen Aspekte der KI-Technologien ist der Wissenstransfer zwischen staatlichen und privaten Akteuren, unter anderem deutschen Unternehmen, für eine effiziente Nutzung von Forschungsergebnissen entscheidend. Diese leisten mit ihren Ergebnissen einen wichtigen Beitrag für die zukünftig benötigte Landesverteidigung. Dabei kann die deutsch-französische Zusammenarbeit als ein guter Anfang zur Verbesserung der verteidigungsrelevanten KI-Forschung in Europa gesehen werden. Gleichwohl sollte die Bundesrepublik Deutschland ebenfalls eigenständig agieren und sich der KI aus sicherheitspolitischer Sicht widmen und militärische KI als wichtigen Bereich in ihre nationale KI-Strategie integrieren. Dem Beispiel Frankreichs und des Vereinigten Königreichs folgend, sollte Deutschland eine eigene militärische KI-Strategie konzipieren. Für die deutsche Sicherheits- und Verteidigungsindustrie müssen dabei Entwicklungsfreiräume erhalten bleiben, um den Streitkräften von EU und NATO, insbesondere aber der Bundeswehr, als industrielle Partnerin gerade auch im Bereich militärischer KI dienen zu können. Dies gilt ebenfalls für die EU, die ähnlich wie das Vereinigte Königreich vorgehen sollte, nämlich mit der Absicht, die Einführung und Nutzung von KI-gestützten Lösungen und Fähigkeiten in den Bereichen Sicherheit und Verteidigung zu ermöglichen anstatt sie zu behindern, wie das Beispiel des geplanten EU AI-Act verdeutlicht. Wie bereits von Ulrike Franke betont, sollten die Europäerinnen und Europäer in Anbetracht der Veränderungen, die durch KI im militärischen Bereich zu erwarten sind, sowie in Anbetracht der intensiven Beschäftigung mit militärischer KI in anderen Ländern – vor allem in den USA, China und Russland – der Entwicklung eigener militärischer KI mehr Aufmerksamkeit schenken.[35] Denn nur so kommt man dem Ziel der strategischen Souveränität Europas näher.

1 Vgl. Zhao, Zhijiang (2020). Germany Needs to Consider Military AI. In: AICGS.org, 23.9.2020. https://www.aicgs.org/2020/09/germany-needs-to-consider-military-ai/ (letzter Zugriff: 29.9.2022).

2 Vgl. Voß, Oliver (2017). Wie Gefährlich Ist Künstliche Intelligenz? In: Tagesspiegel.de. https://www.tagesspiegel.de/politik/killerroboter-und-co-wie-gefaehrlich-ist-kuenstliche-intelligenz/20602292.html (letzter Zugriff: 29.9.2022).

3 Dirk Reiners, et al. (2021). The Combination of Artificial Intelligence and Extended Reality: A Systematic Review In: Frontiers in Virtual Reality, vol. 2. https://doi.org/10.3389/frvir.2021.721933.

4 Bossong, Nora et al. (2022). Deutschlands Sicherheit: Künstliche Intelligenz für die Landesverteidigung. In: *Faz.net*. https://www.faz.net/aktuell/wirtschaft/in-welchem-rahmen-ist-ki-sinnvoll-fuer-die-verteidigung-17765528.html (letzter Zugriff: 29.9.2022).

5 An dieser Stelle sei zusätzlich verwiesen auf das Kapitel „Internationale Perspektiven" in diesem Sammelband.

6 Ministère des Armées (2019). Rapport De La Task Force IA Septembre 2019. https://www.defense.gouv.fr/sites/default/files/aid/20200108-NP-Rapport%20de%20la%20Task%20Force%20IA%20Septembre.pdf (letzter Zugriff: 29.9.2022).

7 Villani, Cédric/Bonnet, Yann/Rondepierre, Bertrand (2018). For a Meaningful Artificial Intelligence: Towards a French and European Strategy. Paris: Conseil National du Numérique (French Digital Council).

8 Actualisation stratégique et revue stratégique 2017. In: Defense.Gouv.fr, 2021, https://www.defense.gouv.fr/dgris/politique-defense/actualisation-strategique-revue-strategique-2017 (letzter Zugriff: 29.9.2022).

9 AI Task Force (2019). Artificial Intelligence in Support of Defence. Report of the AI Task Force 2019. In: Defense.Gouv.fr, 2019. https://www.defense.gouv.fr/sites/default/files/aid/Report%20of%20the%20AI%20Task%20Force%20September%202019.pdf (letzter Zugriff: 29.9.2022).

10 Secretary of State for Defence (2022). Defence Artificial Intelligence Strategy. Policy Paper. In: *Gov.uk*, 15.6.2022. https://www.gov.uk/government/publications/defence-artificial-intelligence-strategy/defence-artificial-intelligence-strategy (letzter Zugriff: 29.9.2022).

11 Franke, Ulrike Esther (2019). Not smart enough: The poverty of European military thinking on artificial intelligence. European Council on Foreign Relations. In: Ecfr.eu, 18.12.2019. https://ecfr.eu/publication/not_smart_enough_poverty_european_military_thinking_artificial_intelligence/ (letzter Zugriff: 29.9.2022).

12 Nelson, Nicholas/Luzum, Nico (2022). Helping NATO to embrace Artificial Intelligence. In: *CEPA.org*, 3.5.2022. https://cepa.org/helping-nato-to-embrace-artificial-intelligence/ (letzter Zugriff: 29.9.2022).

13 NATO (2022). Press Conference by NATO Secretary General Jens Stoltenberg ahead of the meetings of NATO Defence Ministers on 21 and 22 October at NATO Headquarters. In: *NATO.int*, 20.10.2021. https://www.nato.int/cps/en/natohq/opinions_187622.htm?selectedLocale=en (letzter Zugriff: 29.9.2022).

14 NATO (2021). Summary of the NATO Artificial Intelligence Strategy. In: *NATO.int*, 22.10.2021. https://www.nato.int/cps/en/natohq/official_texts_187617.htm (letzter Zugriff: 29.9.2022).

15 Hunter Christie, Edward (2022). Defence Cooperation in Artificial Intelligence: Bridging the

Transatlantic Gap for a Stronger Europe In: European View, vol. 21, no. 1, SAGE Publications, pp. 13–21. doi:10.1177/17816858221089372.

16 NATO (2022). NATO sharpens technological edge with innovation initiatives. In: *NATO.int*, 7.4.2022. https://www.nato.int/cps/en/natohq/news_194587.htm (letzter Zugriff: 29.9.2022).

17 NATO (2022). NATO Launches Innovation Fund. In: *NATO.int*, 30.6.2022. https://www.nato.int/cps/en/natohq/news_197494.htm?selectedLocale=en (letzter Zugriff: 29.9.2022).

18 Mölling, Christian (2020): Vom Flickenteppich Deutscher Sicherheitspolitik. In: *Internationale Politik*, 75 (5), S. 79–83.

19 McKinsey (2017). Smartening up with Artificial Intelligence (AI) – What's in it for Germany and its Industrial Sector? In: *McKinsey.com*, 4.2017. https://www.mckinsey.com/de/~/media/mckinsey/locations/europe%20and%20middle%20east/deutschland/news/presse/2017/2017-04-24/170419_mckinsey_ki_final_m.pdf (letzter Zugriff: 29.9.2022).

20 Bossong, Nora et al. (2022). Deutschlands Sicherheit: Künstliche Intelligenz für die Landesverteidigung. In: *Faz.net*. https://www.faz.net/aktuell/wirtschaft/in-welchem-rahmen-ist-ki-sinnvoll-fuer-die-verteidigung-17765528.html (letzter Zugriff: 29.9.2022).

21 Reintjes, Thomas (2022). Kalter Intelligenter Krieg – Wie Algorithmen die geostrategische Lage Verändern. In: *Deutschlandfunk*. https://www.deutschlandfunk.de/ki-kuenstliche-intelligenz-waffensysteme-100.html (letzter Zugriff: 29.9.2022).

22 Die Bundesregierung (2020). Strategiepapier der Bundesregierung zur Stärkung der Sicherheits- und Verteidigungsindustrie vom 12.2.2020. https://www.bmwk.de/Redaktion/DE/Downloads/S-T/strategiepapier-staerkung-sicherits-und-verteidigungsindustrie.pdf?__blob=publicationFile&v=4 (letzter Zugriff: 29.9.2022).

23 Franke, Ulrike (2021). Artificial Intelligence Diplomacy. In: *Europarl.Europa.eu.* https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662926/IPOL_STU(2021)662926_EN.pdf (letzter Zugriff: 29.9.2022).

24 Vgl. United States (2012). Department of Defence DIRECTIVE 3000.09, 2012. https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/300009p.pdf (letzter Zugriff: 29.9.2022).

25 ASD Concept Paper Meaningful Human Control. https://www.asd-europe.org/ (letzter Zugriff: 29.9.2022).

26 Europäische Komission (2021). Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union. In: *Europa.eu*. https://op.europa.eu/de/publication-detail/-/publication/e0649735-a372-11eb-9585-01aa75ed71a1 (letzter Zugriff: 29.9.2022).

27 Yordanova, Katerina (2022). The EU AI Act – Balancing Human Rights and Innovation Through Regulatory Sandboxes and Standardization. Competition Policy International. In: *Competitionpolicyinternational.com*, 3.2022. https://www.competitionpolicyinternational.com/wp-content/uploads/2022/03/8-The-EU-AI-Act-Balancing-Human-Rights-and-Innovation-Through-Regulatory-Sandboxes-and-Standardization-Katerina-Yordanova.pdf (letzter Zugriff: 29.9.2022).

28 Michael Veale, and Frederik Zuiderveen Borgesius (2022). Demystifying the Draft EU Artificial Intelligence Act. Cornell University Library, arXiv.org. doi:10.9785/cri-2021-220402.

29 Zühlke, Karin (2022). Vbw Zum Geplanten EU AI Act: KI Braucht Innovationsfreundlichen Rechtsrahmen – Strategien & Trends. In: *Elektroniknet.de*. https://www.elektroniknet.de/elektronikfertigung/strategien-trends/ki-braucht-innovationsfreundlichen-rechtsrahmen.197467.html (letzter Zugriff: 29.9.2022).

30 Clarck, Laurie (2021). Meps Are Preparing To Debate Europe's AI Act. These Are The Most Contentious Issues. In: Tech Monitor. https://techmonitor.ai/policy/meps-are-preparing-to-debate-europes-ai-act-these-are-the-most-contentious-issues (letzter Zugriff: 29.9.2022)

31 European Commission (2020). Europe: The Keys To Sovereignty – European Commission. In: Europa.eu, 11.9.2020. https://ec.europa.eu/commission/commissioners/2019-2024/breton/announcements/europe-keys-sovereignty_en (letzter Zugriff: 29.9.2022).

32 European Defence Agency (2016). Handbook For Defence Related SMEs. In: *Europa.eu*, 3.3,2016. https://eda.europa.eu/publications-and-data/brochures/handbook-for-defence-related-smes (letzter Zugriff: 29.9.2022).

33 Mueller, Benjamin (2021). How Much Will the Artificial Intelligence Act Cost Europe? In: *Report – Information Technology and Innovation Foundation*, 26. 7.2021. https://itif.org/publications/2021/07/26/how-much-will-artificial-intelligence-act-cost-europe/ (letzter Zugriff: 29.9.2022).

34 European Investment Bank (2021). EIB Investment Report 2020/2021: Building a smart and green Europe in the COVID-19 Era. In: *Eib.org*. https://www.eib.org/en/publications/investment-report-2020 (letzter Zugriff: 29.9.2022).

35 Franke, Ulrike (2020). Europe Needs A Plan For AI In The Military Realm. In: *The Security Times*. https://www.the-security-times.com/europe-needs-plan-ai-military-realm/.

Bibliografie

AI Task Force (2019). Artificial Intelligence in Support of Defence. Report of the AI Task Force 2019. In: *Defense.Gouv.fr*, 2019. https://www.defense.gouv.fr/sites/default/files/aid/Report%20of%20the%20AI%20Task%20Force%20September%202019.pdf (letzter Zugriff: 29.9.2022).

Secretary of State for Defence (2022). Defence Artificial Intelligence Strategy. Policy Paper. In: *Gov.uk*, 15.6.2022. https://www.gov.uk/government/publications/defence-artificial-intelligence-strategy/defence-artificial-intelligence-strategy (letzter Zugriff: 29.9.2022).

NATO (2022). NATO Launches Innovation Fund. In: *NATO.int*, 30.6.2022. https://www.nato.int/cps/en/natohq/news_197494.htm?selectedLocale=en (letzter Zugriff: 29.9.2022).

NATO (2022). NATO sharpens technological edge with innovation initiatives. In: *NATO.int*, 7.4.2022. https://www.nato.int/cps/en/natohq/news_194587.htm (letzter Zugriff: 29.9.2022).

NATO (2022). Press Conference by NATO Secretary General Jens Stoltenberg ahead of the meetings of NATO Defence Ministers on 21 and 22 October at NATO Headquarters. In: *NATO.int*, 20.10.2021. https://www.nato.int/cps/en/natohq/opinions_187622.htm?selectedLocale=en (letzter Zugriff: 29.9.2022).

NATO (2021). Summary of the NATO Artificial Intelligence Strategy. In: *NATO.int*, 22.10.2021. https://www.nato.int/cps/en/natohq/official_texts_187617.htm (letzter Zugriff: 29.9.2022).

Die Bundesregierung (2020). Strategiepapier der Bundesregierung zur Stärkung der Sicherheits- und Verteidigungsindustrie vom 12.2.2020. https://www.bmwk.de/Redaktion/DE/Downloads/S-T/strategiepapier-staerkung-sicherits-

und-verteidigungsindustrie.pdf?__blob=publicationFile&v=4 (letzter Zugriff: 29.9.2022).

Actualisation stratégique et revue stratégique 2017. In: *Defense.Gouv.fr, 2021*, https://www.defense.gouv.fr/dgris/politique-defense/actualisation-strategique-revue-strategique-2017 (letzter Zugriff: 29.9.2022).

ASD Concept Paper Meaningful Human Control. https://www.asd-europe.org/ (letzter Zugriff: 29.9.2022).

Amt für Heeresentwicklung (2019). Künstliche Intelligenz in den Landstreitkräften. In: *Bundeswehr.de*. https://www.bundeswehr.de/de/organisation/heer/aktuelles/kuenstliche-intelligenz-in-den-landstreitkraeften-156226. (letzter Zugriff: 29.9.2022).

Bossong, Nora et al. (2022). Deutschlands Sicherheit: Künstliche Intelligenz für die Landesverteidigung. In: *Faz.net*. https://www.faz.net/aktuell/wirtschaft/in-welchem-rahmen-ist-ki-sinnvoll-fuer-die-verteidigung-17765528.html (letzter Zugriff: 29.9.2022).

Clarck, Laurie (2021). Meps Are Preparing To Debate Europe's AI Act. These Are The Most Contentious Issues. In: *Tech Monitor*. https://techmonitor.ai/policy/meps-are-preparing-to-debate-europes-ai-act-these-are-the-most-contentious-issues (letzter Zugriff: 29.9.2022).

United States (2012). Department of Defence DIRECTIVE 3000.09. https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/300009p.pdf (letzter Zugriff: 29.9.2022).

Dirk Reiners, et al. (2021). The Combination of Artificial Intelligence and Extended Reality: A Systematic Review In: *Frontiers in Virtual Reality*, vol. 2. https://doi.org/10.3389/frvir.2021.721933.

Europäische Kommission (2021). Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union. In: *Europa.eu*. https://op.europa.eu/de/publication-detail/-/publication/e0649735-a372-11eb-9585-01aa75ed71a1 (letzter Zugriff: 29.9.2022).

European Commission (2020). Europe: The Keys To Sovereignty – European Commission. In: *Europa.eu*, 11.9.2020. https://ec.europa.eu/commission/commissioners/2019-2024/breton/announcements/europe-keys-sovereignty_en (letzter Zugriff: 29.9.2022).

European Defence Agency (2016). Handbook For Defence Related SMEs. In: *Europa.eu*, 3.3,2016. https://eda.europa.eu/publications-and-data/brochures/handbook-for-defence-related-smes (letzter Zugriff: 29.9.2022).

European Investment Bank (2021). EIB Investment Report 2020/2021: Building a smart and green Europe in the COVID-19 Era. In: *Eib.org*. https://www.eib.org/en/publications/investment-report-2020 (letzter Zugriff: 29.9.2022).

Franke, Ulrike Esther (2019). Not smart enough: The poverty of European military thinking on artificial intelligence. European Council on Foreign Relations. In: *Ecfr.eu*, 18.12.2019. https://ecfr.eu/publication/not_smart_enough_poverty_european_military_thinking_artificial_intelligence/ (letzter Zugriff: 29.9.2022).

Franke, Ulrike (2021). Artificial Intelligence Diplomacy. In: *Europarl.Europa.eu*. https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662926/IPOL_STU(2021)662926_EN.pdf (letzter Zugriff: 29.9.2022).

Franke, Ulrike (2020). Europe Needs A Plan For AI In The Military Realm. In: *The Security Times*. https://www.the-security-times.com/europe-needs-plan-ai-military-realm/ (letzter Zugriff: 29.9.2022).

Hunter Christie, Edward (2022). Defence Cooperation in Artificial Intelligence: Bridging the Transatlantic Gap for a Stronger Europe In: *European View*, vol. 21, no. 1, SAGE Publications, pp. 13–21. doi:10.1177/17816858221089372.

Michael Veale, and Frederik Zuiderveen Borgesius (2022). Demystifying the Draft EU Artificial Intelligence Act. Cornell University Library, arXiv.org. doi:10.9785/cri-2021-220402.

Ministère des Armées (2019). Rapport De La Task Force IA Septembre 2019. https://www.defense.gouv.fr/sites/default/files/aid/20200108-NP-Rapport%20de%20la%20Task%20Force%20IA%20Septembre.pdf (letzter Zugriff: 29.9.2022).

Mölling, Christian (2020): Vom Flickenteppich Deutscher Sicherheitspolitik. In: *Internationale Politik*, 75 (5), S. 79–83.

Mueller, Benjamin (2021). How Much Will the Artificial Intelligence Act Cost Europe? In: *Report – Information Technology and Innovation Foundation*, 26.7.2021. https://itif.org/publications/2021/07/26/how-much-will-artificial-intelligence-act-cost-europe/ (letzter Zugriff: 29.9.2022).

Nelson, Nicholas/Luzum, Nico (2022). Helping NATO to embrace Artificial Intelligence. In: *CEPA.org,* 3.5.2022. https://cepa.org/helping-nato-to-embrace-artificial-intelligence/ (letzter Zugriff: 29.9.2022).

Reintjes, Thomas (2022). Kalter Intelligenter Krieg – Wie Algorithmen die geostrategische Lage Verändern. In: *Deutschlandfunk*. https://www.deutschlandfunk.de/ki-kuenstliche-intelligenz-waffensysteme-100.html (letzter Zugriff: 29.9.2022).

McKinsey (2017). Smartening up with Artificial Intelligence (AI) – What's in it for Germany and its Industrial Sector? In: *McKinsey.com*, 4.2017. https://www.mckinsey.com/de/~/media/mckinsey/locations/europe%20and%20middle%20east/deutschland/news/presse/2017/2017-04-24/170419_mckinsey_ki_final_m.pdf (letzter Zugriff: 29.9.2022).

Villani, Cédric/Bonnet, Yann/Rondepierre, Bertrand. 2018. For a Meaningful Artificial Intelligence: Towards a French and European Strategy. Paris: Conseil National du Numérique (French Digital Council).

Voß, Oliver (2017). Wie gefährlich ist Künstliche Intelligenz? In: *Tagesspiegel.de*. https://www.tagesspiegel.de/politik/killerroboter-und-co-wie-gefaehrlich-ist-kuenstliche-intelligenz/20602292.html (letzter Zugriff: 29.9.2022).

Yordanova, Katerina (2022). The EU AI Act – Balancing Human Rights and Innovation Through Regulatory Sandboxes and Standardization. Competition Policy International. In: *Competitionpolicyinternational.com,* 3.2022. https://www.competitionpolicyinternational.com/wp-content/uploads/2022/03/8-The-EU-AI-Act-Balancing-Human-Rights-and-Innovation-Through-Regulatory-Sandboxes-and-Standardization-Katerina-Yordanova.pdf (letzter Zugriff: 29.9.2022).

Zhao, Zhijiang (2020). Germany Needs to Consider Military AI. In: *AICGS.org*, 23.9.2020. https://www.aicgs.org/2020/09/germany-needs-to-consider-military-ai/ (letzter Zugriff: 29.9.2022).

Zühlke, Karin (2022). Vbw Zum Geplanten EU AI Act: KI Braucht Innovationsfreundlichen Rechtsrahmen – Strategien & Trends. In: *Elektroniknet.de*. https://www.elektroniknet.de/elektronikfertigung/strategien-trends/ki-braucht-innovationsfreundlichen-rechtsrahmen.197467.html (letzter Zugriff: 29.9.2022).