Deutsche
Stiftung
Friedensforschung
DSF
german foundation for peace research

Algorithmen und Künstliche Intelligenz als Game Changer? Moderne Waffensysteme zwischen Erwartung und Wirklichkeit

Christian Alwardt, Sylvia Kühne

Forschung DSF № 56

Kontakt:
Deutsche Stiftung Friedensforschung (DSF)
Am Ledenhof 3-5
49074 Osnabrück
+49 541 60035-42
www.bundesstiftung-friedensforschung.de
info@bundesstiftung-friedensforschung.de

Gestaltung, Satz und Herstellung: bvw werbeagentur

Spendenkonto der Deutschen Stiftung Friedensforschung:
Sparkasse Osnabrück, IBAN DE77 2655 0105 000 0012 30

ISSN 2193-794X

Inhaltsverzeichnis

Forschung-DSF erscheint unregelmäßig.

Zusammenfassung

Die Debatte um moderne Waffensysteme sowie die zukünftige Kriegführung wird in zunehmenden Maße durch aktuelle Entwicklungen im Feld der Softwaretechnologien, wie Automatisierung, Vernetzung oder Künstlicher Intelligenz (KI) geprägt. Die innerhalb des sicherheitspolitischen Diskurses gehegten militärischen Erwartungen und die tatsächlichen softwaretechnologischen Fähigkeiten sowie militärischen Anwendungspotenziale divergieren jedoch häufig, sind bisher nur unzureichend untersucht und desto unbestimmter, je weiter der Blick in die Zukunft geht. Softwaretechnologien entfalten so zwar einen zunehmenden Einfluss, gleichwohl ist noch offen, welche Bedeutung diese Technologietrends tatsächlich für die zukünftige Kriegführung haben werden. Was für neue militärische Fähigkeiten und Anwendungsspektren werden sich durch den Einsatz von Softwaretechnologien aber ergeben und mit welchen friedens- und sicherheitspolitischen Auswirkungen werden wir hierdurch konfrontiert sein? Vor allem aber, wie können wir resultierende Risiken präventiv einhegen?

Mit diesen Fragen hat sich das explorative und interdisziplinäre Forschungsprojekt „Algorithmen und Künstliche Intelligenz als Game Changer? Moderne Waffensysteme zwischen Erwartung und Wirklichkeit“ beschäftig. Zur Analyse und Bearbeitung der Forschungsleitfragen verfolgte das Forschungsvorhaben einen sowohl disziplinären als auch interdisziplinären Ansatz, mit dem Ziel, disziplinäre Forschung zu modernen Softwaretechnologien zu verzahnen, hierauf aufbauende fächerübergreifende Analysen zu ermöglichen und damit anwendungsorientierte Erkenntnisse zu erlangen. Anhand einer sozialwissenschaftlichen Diskursanalyse wurde die militärische Erwartungshaltung hinsichtlich Softwaretechnologien untersucht und eine exemplarische naturwissenschaftlich-technische Untersuchung zeigte am Beispiel der militärischen Informationsgewinnung die kurz- bis mittelfristigen Fähigkeiten von Softwaretechnologien auf. In insgesamt drei interdisziplinären Analysen wurden zum einen ein analytischer Abgleich der militärischen Erwartungen und technischen Realitäten in Bezug auf moderne Softwaretechnologien durchgeführt. Zum anderen beschäftigte sich eine Untersuchung mit den Problemen um die Definition von Künstlicher Intelligenz sowie die zunehmende Relevanz von Daten in der softwaretechnologischen Forschung und Entwicklung. Die Forschungs- und Analyseergebnisse sind im vorliegenden Forschungsbericht dargestellt. Abgeschlossen wird dieser Bericht mit einer Einordnung und Bewertung der Forschungs- und Analyseergebnisse sowie einer generelleren interdisziplinären Betrachtung des militärischen Einsatzes moderner Softwaretechnologien, der die friedens- und sicherheitspolitischen Risiken sowie die Notwendigkeit einer Regulierung diskutiert.

Moderne Softwaretechnologien fungieren schon heute als ein militärischer „Force Multiplier“, kurzfristig wird ihnen aber wohl noch nicht der Charakter eines „Game Changers“ attestiert werden können. Realistische Prognosen hinsichtlich ihrer mittel- bis langfristigen militärischen Fähigkeits- und Anwendungspotenziale bedürfen der weiteren Untersuchung. Hierfür ist eine fortgesetzte und vertiefte interdisziplinäre Forschung essentiell, gerade unter stärkerer Einbindung der naturwissenschaftlich-technischen Perspektive als ein Korrektiv zum sicherheitspolitischen Diskurs. Die Erkenntnisse des Forschungsprojektes stellen wertvolle Grundlagen in dieser Hinsicht dar und können den qualitativen Einfluss von Softwaretechnologien auf die moderne Kriegsführung besser verstehen, internationale Verhandlungen vorantreiben sowie probate Instrumente zur Einhegung der friedens- und sicherheitspolitischen Risiken ableiten helfen. Sie werden damit also auch eine unmittelbare Bedeutung für die friedenswissenschaftliche Politikberatung sowie die interessierte Öffentlichkeit haben.

Abstract

The debate on modern weapon systems and future warfare is increasingly shaped by advances in software technologies, particularly in areas such as automation, networking or Artificial Intelligence (AI). However, military expectations cherished by the security policy discourse often diverge from the actual software capabilities and potential military applications, which have not yet been thoroughly investigated and become increasingly vague the further one looks into the future. Despite the growing importance of and reliance on software technologies, their actual impact on future warfare remains unclear. This begs several questions: What new military capabilities and applications will likely emerge and what effect will they have on peace and security policies? Above all, how can we pre-emptively mitigate potential risks?

The explorative and interdisciplinary research project "Algorithms and Artificial Intelligence as Game Changers? Modern Weapon Systems between Expectation and Reality" addressed these questions. In order to analyze and address the guiding research questions, the research project pursued a disciplinary as well as interdisciplinary approach with the goal of interlinking disciplinary research on modern software technologies, leading to interdisciplinary analyses, which in turn should result in application-oriented findings. Military expectations of software technologies were studied using discourse analytical methods, whilst potential short- to medium-term capabilities were examined through a technical investigation centred on military information gathering technologies. Three interdisciplinary analyses focussed on modern software technologies, of which one compared military expectations to technical realities, whilst the others dealt with the definitional problems surrounding AI and the increasing data reliance within software technology research and development. This report presents the results of these analyses, followed by an evaluation of the work conducted. It concludes with an interdisciplinary discussion on the peace and security policy implications, as well as a call for regulation.

Although modern software technologies already function as a military "force multipliers", they cannot yet, in the short-term, be considered as “game changers”. Further investigation would be required to reliably assess their medium- to long-term impact on military applications. For this, continued, in-depth interdisciplinary research is essential as it also provides a corrective to the security policy discourse by further integrating scientific-technical perspectives. The findings presented in this report are a valuable first step: they provide insights into the qualitative impact of software technologies on modern warfare, help to advance international negotiations, and support the derivation of proven instruments that mitigate peace and security policy risks. Thus, the results are not only directly pertinent to policy advice but also relevant for the interested public.

1. Der zunehmende Einfluss von Softwaretechnologien auf moderne Waffensysteme und die Kriegsführung: Problemstellung und wichtige Leitfragen

Neue technologische Trends wie Automatisierung, Vernetzung und das Forschungsfeld der Künstlichen Intelligenz (KI) sind die Folge rasanter Entwicklungsfortschritte im Bereich der Informationstechnologien. Antriebsmotor dieses Fortschritts ist vor allem der zivile Sektor, wenngleich resultierende Technologien überwiegend einen Dual-use Charakter aufweisen und damit auch eine militärische Verwendung finden können. Obwohl moderne Computer- und Kommunikationshardware weiterhin die entscheidende Grundvoraussetzung für diese Entwicklungen darstellen, können softwaretechnologische Fortschritte, basierend auf Algorithmen, Programmcodes und Daten, als mittlerweile wesentliche Treiber dieser Technologietrends angesehen werden. Insbesondere das Forschungsfeld der Künstlichen Intelligenz steht gegenwärtig im Mittelpunkt nationaler Forschungsrahmenprogramme.

Im militärischen Bereich ist eine zunehmende Adaption dieser Trends zu beobachten und die Debatte um die zukünftige Kriegführung wird in zunehmenden Maße durch aktuelle Entwicklungen im Feld der Softwaretechnologien geprägt. Mit ihren weitreichenden Adaptionsmöglichkeiten könnten diese Technologien einen grundlegenden Wandel militärischer Potenziale mit sich bringen – sowohl auf der Planungsebene als auch bei der Entwicklung und Beschaffung moderner Waffensysteme. Vor allem die Künstliche Intelligenz steht in diesem Zusammenhang nun auch auf der militärischen Forschungsagenda und es ist zu erwarten, dass KI zukünftig eine zentrale Rolle im militärischen Kräftemessen der Nationen spielen wird. Angesichts der Entwicklungsfortschritte in den Informationstechnologien und ihrer militärischen Adaption lassen sich auch die Fähigkeiten moderner Waffensysteme nicht länger nur über ihre Hardwarebestandteile definieren, sondern sie leiten sich vielmehr auch aus ihren softwaretechnologischen Bestandteilen ab. Softwaretechnologien entfalten somit einen zunehmenden Einfluss in der modernen Kriegsführung; aber handelt es sich bei ihnen auch um einen Game Changer, also einen kohärenten Technologieschub, der Elemente der Kriegführung revolutionieren wird?

Zwar fehlt es bislang nicht an generellen sicherheitspolitischen Überlegungen in Bezug auf moderne Waffensysteme und auch deren Vorteile und Risiken werden im Diskurs gleichermaßen erörtert. Es wird beispielsweise angenommen, dass das Ausmaß an softwaretechnologisch bedingter Autonomie in Waffensystemen (für eine Übersicht vgl. Boulanin und Verbruggen 2017: 26) zukünftig weiter zunehmen wird (vgl. zu dieser Debatte z.B. Campaign to Stop Killer Robots 2015; HRW 2012). Diese militärischen Entwicklungen werden vor allem im Hinblick auf die Notwendigkeit der Einhaltung der Prinzipien des humanitären Völkerrecht diskutiert (vgl. z.B. CCW 2019; Amoroso et al. 2018; König 2017; UNODA 2017) oder neuerdings auch verstärkt mit Blick auf die regionale und strategische Stabilität zwischen Staaten erörtert (zu dieser Debatte vgl. z.B. Topychkanov 2020; Rickli 2019; Horowitz 2019; Altmann und Sauer 2019; Amoroso et al. 2018). Der Diskurs hat dabei vor allem die resultierenden militärischen Potentiale von Waffensystemen im Blick. Die dezidierte Rolle von Softwaretechnologien und ihr Anteil an den Fähigkeiten moderner Waffensysteme findet in diesen Diskussionen bislang aber überwiegend keine gesonderte Betrachtung.

Der Einfluss von Softwaretechnologien auf die moderne Kriegsführung ist wissenschaftlich bislang kaum untersucht. Noch ist nicht klar, welche militärischen Fähigkeiten damit genau einhergehen werden und welche Bedeutung der Technologieschub für die zukünftige Kriegführung tatsächlich haben wird. Als Konsequenz ist auch das Wissen um daraus resultierende tech-

nologisch-sicherheitspolitische Wechselwirkungen und Möglichkeiten der Rüstungskontrolle von Softwaretechnologien bislang nur gering ausgeprägt.

Im Rahmen internationaler Konsultationen stellt diese fehlende Kenntnis ein wesentliches Hindernis bei den Versuchen dar, die friedens- und sicherheitspolitischen Auswirkungen und Risiken moderner Waffensysteme bereits im Vorfeld zu identifizieren und einzuhegen. Am Beispiel unbemannter und zunehmend automatisierter Waffensysteme zeigt sich bereits, wie die fehlende Kenntnis um den einerseits prospektiven Entwicklungstand militärischer Softwaretechnologien und die dadurch andererseits induzierten militärischen Fähigkeiten den sicherheitspolitischen Diskurs und internationale Verhandlungen zur Regulierung moderner Waffensysteme und zur Einhegung damit verbundener friedens- und sicherheitspolitischer Risiken hemmen. Diese Einschätzung nimmt vor allem Bezug auf die seit 2014 laufenden Expertengespräche zu Lethal Autonomous Weapon Systems (LAWS) im Rahmen des Waffenübereinkommens der Vereinten Nationen (CCW), die seit längerem stagnieren. Die Ursachen hierfür liegen darin, dass es bisher nicht gelungen ist, sich international zum einen auf geeignete Definitionen und eine Abgrenzung des Verhandlungsgegenstandes zu einigen, noch eine gemeinsame Vorstellung von dem notwendigen Maß der menschlichen Kontrolle von LAWS und deren Überprüfbarkeit zu erlangen. Neben den abweichenden staatlichen Interessen in Bezug auf eine Regulierung von LAWS, muss als Grund hierfür insbesondere ein bislang unzureichendes Verständnis des militärischen Potentials von Softwaretechnologien sowie der daraus resultierenden Fähigkeiten moderner Waffensysteme festgestellt werden.

Rüstungskontrolle und Regulierungen können immer nur an den „Verursachern" militärischer Fähigkeiten und Potentiale ansetzten (Alwardt 2019: 95 f.) und diese sind im zunehmenden Maße die Softwaretechnologien und nicht wie bisher alleine die militärische Hardware. Daher wird ein besseres Verständnis militärisch genutzter Softwaretechnologien zukünftig so wichtig sein.

Das von der DSF geförderte explorative Forschungsvorhaben „Algorithmen und Künstliche Intelligenz als Game Changer? Moderne Waffensysteme zwischen Erwartung und Wirklichkeit" half ein besseres Verständnis dieser Kenntnislücken und der Problemstellungen an sich zu bekommen. Die Forschungs- und Analyseergebnisse sollen zu einer besseren Orientierung im Feld militärischer Softwaretechnologien und moderner Waffensysteme beitragen und zielen darauf ab, neue Impulse in Hinblick auf zukünftige Forschung, Beratung und den sicherheits- und friedenspolitischen Diskurs zu ermöglichen. Die Untersuchungen im Rahmen dieses Forschungsvorhabens orientierten sich dabei an folgenden Leitfragen:

- Welches Spektrum an Fähigkeiten, Anwendungsbereichen und Technologietrends (u.a. Automatisierung, Vernetzung und KI) resultiert aus der heutigen software-technologischen Forschung und Entwicklung (F&E) und welche militärisch relevanten Potenziale lassen sich aus technischer Sicht hieraus ableiten?

- In welchem Umfang spielen Technologietrends im internationalen sicherheitspolitischen Diskurs heute eine Rolle und welche waffentechnischen Adaptionen werden diesbezüglich thematisiert? Welche Erwartungen hinsichtlich der militärischen Potenziale hegen relevante staatliche Schlüsselakteure und welchen Einfluss auf die Kriegführung und internationale Sicherheit messen diese ihnen bei?

- In welchem Maße decken sich aktuelle softwaretechnologische Entwicklungen mit den im Diskurs identifizierten Erwartungshaltungen an die militärischen Potenziale von Technologietrends? Welche gemeinsame

Schnittmenge hinsichtlich Definitionen, Fähigkeiten sowie militärischen Anwendungen bestehen und wie könnten Arbeitsdefinitionen aussehen? Wie ließe sich das Verständnis um den Einfluss von Softwaretechnologien auf die moderne Kriegführung und resultierende sicherheitspolitische Implikationen vertiefen?

Zur Analyse und Bearbeitung dieser Forschungsleitfragen verfolgte das Forschungsvorhaben einen sowohl disziplinären als auch interdisziplinären Ansatz, mit dem Ziel, disziplinäre Forschung zu modernen Softwaretechnologien zu verzahnen, hierauf aufbauende fächerübergreifende Analysen zu ermöglichen und damit anwendungsorientierte Erkenntnisse zu erlangen. Die Basis dieses Vorgehens bildeten zwei fundierte, disziplinäre Forschungsanteile, einerseits eine sozialwissenschaftliche qualitative Inhaltsanalyse und anderseits eine exemplarische naturwissenschaftliche Technologieanalyse. In der daran anschließenden Zusammenführung und interdisziplinären Analyse der disziplinären Forschungsergebnisse wurden drei Themenfelder für eine vertiefte Untersuchung ausgewählt. Das ist zum einen das Spannungsfeld von „militärischen Erwartungen an softwaretechnologische Trends" und der „technologischen Realität", zum anderen die Schwierigkeiten um die Definition, begriffliche Abgrenzung und Fähigkeiten moderner Softwaretechnologien im militärischen Feld (hier am Beispiel Künstlicher Intelligenz) sowie die herausgehobene Relevanz von Dateninformationen. Die Erkenntnisse aus diesen interdisziplinären Analysen stellen wertvolle Grundlagen für die weitere wissenschaftliche Untersuchung des Einflusses von Softwaretechnologien auf die moderne Kriegsführung und die internationale Sicherheit dar. Hierauf weiter aufbauende interdisziplinäre Analysen können helfen, internationale Verhandlungen voranzutreiben und den qualitativen Einfluss von Softwaretechnologien besser einschätzen und abgrenzen zu lernen sowie darauf basierende Instrumente zur Einhegung von friedens- und sicherheitspolitischen Risiken abzuleiten.

In diesem Forschungsbericht werden die Ergebnisse des explorativen und interdisziplinären Forschungsvorhabens dargestellt. Im Anschluss an eine kurze Skizze des methodischen Vorgehens in Kapitel 2 finden sich die disziplinären Forschungsergebnisse in Kapitel 3 zusammengefasst, die separat bereits publiziert wurden (Kühne 2020; Erz 2020). Die Erkenntnisse der exemplarisch durchgeführten interdisziplinären Analysen sind in Kapitel 4 veröffentlicht. Abgeschlossen wird dieser Bericht in Kapitel 5 einerseits mit einer Einordnung und Bewertung der Forschungs- und Analyseergebnisse. Andererseits werden in einer interdisziplinären Betrachtung des möglichen militärischen Einsatzes moderner Softwaretechnologien ihre friedens- und sicherheitspolitischen Risiken sowie die Notwendigkeit ihrer Regulierung diskutiert.

Der explorative Charakter des Forschungsvorhabens und vor allem die nur einjährige Laufzeit des Projektes ließen keine abschließende Beantwortung aller Forschungsfragen zu – sofern dies überhaupt möglich ist. Die in diesem Forschungsbericht vorgestellten Erkenntnisse können aber als eine gute Grundlage für die weitere Rüstungskontrollforschung dienen und einen hilfreichen Ausgangspunkt für den weiteren Diskurs und die internationalen Verhandlungen zur Rüstungskontrolle moderner Waffensysteme darstellen. Sie werden damit also auch eine unmittelbare Bedeutung für die friedenswissenschaftliche Politikberatung sowie die interessierte Öffentlichkeit haben.

Dieser Forschungsbericht ist Ergebnisdarstellung und -einordnung des von der DSF geförderten Forschungsprojekts „Algorithmen und Künstliche Intelligenz als Game Changer? Moderne Waffensysteme zwischen Erwartung und Wirklichkeit", das im Zeitraum Oktober 2019 bis Januar 2021 am Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg (IFSH) durchgeführt wurde. Die Projektleitung lag bei Dr. Christian Alwardt und das Projektteam bestand aus Dr. Sylvia Kühne, Hendrik Erz und Mirjam Limbrunner.

2. Ein exploratives Forschungsvorhaben auf Basis disziplinärer Grundlagen und einer interdisziplinären Analyse

Um neue Softwaretechnologien, ihren Anteil an militärischen Technologietrends und die sich daraus ergebenden Fähigkeiten moderner Waffensysteme analysieren zu können, wurde im Projekt, wie nachfolgend dargestellt, ein mehrstufiger Ansatz verfolgt. Dieser sah zunächst separate disziplinäre Forschungsanteile vor. Im weiteren Projektverlauf erfolgten auf der Grundlage einer Zusammenführung von sozialwissenschaftlichen und naturwissenschaftlich-technischen Forschungsergebnissen dann interdisziplinäre Analysen und Betrachtungen, die sich an den Forschungsleitfragen orientierten.

2.1. Disziplinärer Projektteil: Qualitative Inhaltsanalyse

Im sozialwissenschaftlichen Projektteil wurde der sicherheitspolitische Diskurs untersucht. Mittels eines an die qualitative Inhaltsanalyse (Mayring 2015) angelehnten Verfahrens wurden Definitionen, Deutungen und Erwartungen an das militärische Potential softwaretechnologischer Trends ermittelt. Als Raster lagen der Recherche und Analyse die folgenden Leitfragen zugrunde:

- Welche militärisch adaptierbaren Technologietrends spielen für staatliche Akteure eine Rolle und was ist deren Verständnis davon?

- Welche Priorität und Dringlichkeit wird einem Engagement in F&E in die Technologietrends beigemessen?

- Welche militärischen Fähigkeiten und Potentiale werden durch die militärische Adaption der identifizierten Trends erwartet oder erhofft?

Wie an anderer Stelle (Kühne 2020: 7 ff.) bereits ausführlich beschrieben, wurden mit den USA, China, Russland und Israel für die Analyse Akteure ausgewählt, die sich angesichts ihres Engagements in F&E in militärisch adaptierbare Technologietrends als maßgeblich im Feld neuer Technologien und internationale Sicherheit erweisen (vgl. Amoroso et al. 2018: 19): Sie gehören sowohl zu den größten Produzenten (und Exporteuren) von allgemeinen Waffensystemen (vgl. SIPRI 2019: 9), als auch zu den Hauptakteuren im Feld der militärischen Drohnenproduktion (vgl. NAF 2019). Ihnen wird im Hinblick auf die Adaption entsprechender Technologieentwicklungen im Bereich autonomer Waffensysteme nicht nur eine zentrale Rolle zugeschrieben, sondern sie gehören außerdem zu den Ländern, die sich seit 2014 internationalen Maßnahmen für ein Verbot autonomer Waffensysteme widersetzen (vgl. Rickli 2019: 96).

In die Untersuchung einbezogen wurden Dokumente, deren Veröffentlichungsdatum zwischen 2014 und 2020 liegt. Neben forschungspragmatischen Erwägungen ist diese Beschränkung dadurch begründet, dass die ersten informellen Expertengespräche 2014 im Rahmen der CCW den Beginn eines internationalen Interesses an der Einhegung entsprechender Softwaretechnologietrends durch Rüstungskontrolle markieren. Die Entscheidung im Jahr 2016, diese Gespräche im Rahmen einer Group of Governmental Experts (GGE) zu verstetigen, unterstreicht, dass insbesondere seit 2014 das internationale Interesse an den Auswirkungen einer neuen Reihe von Technologien auf die Kriegsführung reift (vgl. Gill 2017: 1).

Das Untersuchungsmaterial bildeten 71 Primärquellen, darunter Strategiepapiere und/oder offizielle Verlautbarungen, die eine diskursive Verknüpfung von Softwaretechnologien und entsprechenden Entwicklungen im Hinblick auf mi-

litärische Anwendungen erkennen lassen. Einbezogen wurden neben nationalen Technologiestrategiepapieren und -plänen auch Dokumente aus den jeweiligen Verteidigungsressorts. Erfasst wurden zudem Presseartikel und wissenschaftliche Veröffentlichungen. Diese 93 Sekundärquellen ergänzen das Datenmaterial insbesondere dort, wo die Verfügbarkeit von Primärdokumenten aus öffentlichkeitspolitischen oder sprachlichen Gründen (insbesondere Russland und China, zum Teil aber auch Israel) eingeschränkt war.

2.2. Disziplinärer Projektteil: Naturwissenschaftlich-technische Untersuchung

Im Mittelpunkt des naturwissenschaftlich-technischen Projektansatzes stand die Untersuchung des Forschungs- und Entwicklungstandes moderner Softwaretechnologien sowie das daraus ableitbare technologische Fähigkeits- und Anwendungsspektrum, welches Rückschlüsse auf die mögliche militärische Adaption von Softwaretechnologien und damit verbundener militärischer Potenziale, wie z.B. in Form neuer Waffensystemfähigkeiten, ermöglichen sollte. Diese systematische technologische Untersuchung orientierte sich an den folgenden drei Leitfragen, die auch für den sicherheits- und rüstungskontrollpolitischen Diskurs von besonderer Bedeutung sind:

- Welche analytischen Rückschlüsse lassen sich auf die technischen Fähigkeiten heutiger Softwaretechnologien ziehen?

- Wie sieht das mögliche Anwendungsspektrum dieser Softwaretechnologien aus?

- Für welche der Anwendungsbereich erscheint eine militärische Adaption nachweisbar oder plausibel und welche militärischen Fähigkeiten könnten damit verknüpft sein?

Für die Beantwortung dieser Fragen wurden zunächst informationstechnologische Publikationen (u.a. Zeitschriften des Institute of Electrical and Electronics Engineers, IEEE und Preprints von arXiv), Whitepaper aus der Industrie, Strategiepapiere des U.S.-Militärs sowie Medienberichte aus Informationsportalen, die sich schwerpunktmäßig mit F&E im Bereich Softwaretechnologien und/oder deren militärischen Anwendungspotenzialen beschäftigen, gesichtet. Aufgrund eines Mangels an hinreichend belastbarer Literatur zu langfristigen softwaretechnologischen Trends, von denen aus sich verlässlich auf zukünftige militärische Anwendungen schließen ließ, lag der Fokus auf der Untersuchung von kurz- bis mittelfristigen softwaretechnologischen Trends und deren möglicher militärischer Einsatz. Insgesamt war es schwierig, aussagekräftige Informationen zu den dezidierten Fähigkeiten spezialisierter Algorithmen, deren Anforderungen an die Prozessionsleistung sowie zu den Leistungsparametern moderner Hardware (Rechenleistung, Übertragungsgeschwindigkeiten etc.) zu bekommen. Im Rahmen dieses Forschungsvorhabens wurde die Untersuchung daher exemplarisch auf das Anwendungsfeld der militärischen Informationsgewinnung eingeengt, da hier zum einen die beste Informationsgrundlage identifiziert wurde, die zugrundeliegenden Prozesse gut erforscht sind und auch eine zumindest teilweise Übertragbarkeit der Untersuchungsergebnisse in Bezug auf den Einsatz moderner Softwaretechnologien in anderen militärische Anwendungsfeldern gegeben sein sollte. Nähere Informationen zu Vorgehen und Methodik finden sich in der aus dieser Untersuchung hervorgegangenen Publikation „Künstliche Intelligenz und Daten: Eine Evaluation softwarebasierter militärischer Informationsgewinnung“ (Erz 2020).

2.3. Interdisziplinärer Projektteil: Plausibilitäten, Definitionen und Daten

Die interdisziplinäre Analysephase dieses Forschungsvorhabens sollte sich durch die erkenntnisorientierte Verzahnung disziplinärer Forschung und die Generierung einer gemeinsamen, für den friedens- und sicherheitspolitischen Diskurs dienlichen, interdisziplinären Wissensbasis auszeichnen, anhand derer es zukünftig gelingen könnte, operationalisierbare Lösungsansätze im Feld der Rüstungskontrolle zu entwickeln. Hierfür war in dieser Arbeitsphase ursprünglich ein intensiver persönlicher Austausch, sowohl projektintern als auch mit externen Expert*innen verschiedener Fachdisziplinen vorgesehen. Auf diese Weise sollten einerseits die disziplinären Forschungsergebnisse diskutiert und andererseits gemeinsam (u.a. in einem Expert*innenworkshop) die für den Diskurs relevanten Problem- und Fragestellungen identifiziert und erste Lösungsansätze generiert werden. Aufgrund geltender Kontaktbeschränkungen während der überwiegenden Projektlaufzeit war diese Herangehensweise nicht umsetzbar.

Entgegen der ursprünglichen Planung fand der interdisziplinäre Analyseanteil daher in einer sehr viel individuelleren und stärker wissenschaftlichen Form statt. Es wurden drei spezifische interdisziplinäre Analysen angefertigt, die sich am sicherheitspolitischen Diskurs um den Wandel der Kriegsführung, den friedens- und sicherheitspolitischen Risiken sowie den Fragen um die Möglichkeiten ihrer Einhegung durch Instrumente wie z.B. Rüstungskontrolle orientierten. Zwar konnte der interdisziplinäre Analyseanteil so nicht in der eigentlich angedachten Breite und unter Mithilfe größtmöglicher externer Fachexpertise durchgeführt werden, mit den drei Analysen wurden aber für den weiteren Diskurs essentielle Themen behandelt. Die interdisziplinären Analysen sind in Kapitel 4 veröffentlicht.

In Kapitel 4.1 wird die technische Plausibilität ausgewählter militärischer Erwartungen an moderne Softwaretechnologien beleuchtet. Hierzu wurde ein Abgleich mit den Ergebnissen der zuvor durchgeführten naturwissenschaftlich-technischen Untersuchung (vgl. Kapitel 3.2) durchgeführt. Die Auswahl der hier untersuchten Kategorien an militärischen Anwendungsfelder und -szenarien erfolgte einerseits entlang der im sozialwissenschaftlichen Projektteil erarbeiteten Kategorien Command & Control, Situational Awareness, Early Warning, Safety & Security, Logistics und Teaming (vgl. Kapitel 3.1). Andererseits war die Auswahl von den im naturwissenschaftlich-technischen Projektteil identifizierten Softwaretechnologien geleitet, die für diese Kategorien als wesentlich identifiziert wurden.

Die zweite interdisziplinäre Analyse widmete sich den konzeptionellen Unschärfen im Diskurs über KI. Als Grundlage dafür diente eine Bestandsaufnahme von Begriffsbestimmungen im sicherheitspolitischen Diskurs (für eine ausführliche Darstellung vgl. Kühne 2020: 27ff.), die nahelegt, dass Künstliche Intelligenz weniger eine Technologie per se, als vielmehr ein Sammelbegriff ist, mit dem auf die Ermöglichung vielfältiger Anwendungen angespielt wird[1]. Diese Definitionen, ergänzt um Bestimmungen auch aus dem deutschen Diskurs um KI und Militär, wurden mit exemplarischen Bestimmungen des technischen Diskurses, entnommen aus Handbüchern und Beiträgen einschlägiger Technologieforen, und hier identifizierter prominenter Definitionsansätze kontrastiert. Die Ergebnisse der Untersuchung zu konzeptionellen Überschneidungen, aber vor allem Unterschieden werden in Kapitel 4.2 dargestellt und diskutiert.

[1] Insgesamt konnten 31 Dokumente identifiziert werden, in denen Bestimmungen vorgenommen wurden. Sie wurden in diese Teiluntersuchung einbezogen.

Drittens haben wir in Kapitel 4.3 die zunehmende Bedeutung von Dateninformationen für moderne softwaretechnologische Anwendungen untersucht, da sich einerseits die beständige Akkumulation von (Trainings-)Daten als ein zentraler Argumentationsanker im sicherheitspolitischen Diskurs erweist. Diese Untersuchung erfolgte durch eine erneute Inhaltsanalyse des im sozialwissenschaftlichen Projektteil erfassten Materialkorpus, sowie weiterer 35, vorrangig aus dem medialen Diskurs stammender Dokumente. Da Militärs für diverse Handlungsprozeduren in unterschiedlichen Bereichen zunehmend auf eine Vielzahl von Algorithmen des Maschinellen Lernens setzen, wirft dies insgesamt die Frage nach der Stärke und Genauigkeit von KI-basierten Technologien auf. Diese haben wir mit Blick auf technische Engpässe und die Risiken, die sich aus der Verarbeitung von Daten und ihrer algorithmischen Prozessierung ergeben können, reflektiert.

Die im Rahmen des Forschungsvorhabens erzielten Forschungsergebnisse und -analysen werden in Kapitel 5 zusammengeführt und einer interdisziplinären Einordnung und Beurteilung unterzogen. Außerdem findet sich hier eine abschließende interdisziplinäre Betrachtung wichtiger Fragen, die für den weiteren friedens- und sicherheitspolitischen Diskurs um den militärischen Einsatz von Softwaretechnologien und für zukünftige Rüstungskontrollbemühungen relevant sein werden.

3. Disziplinäre Forschungsergebnisse

An Softwaretechnologien richten sich hohe Erwartungen. Insbesondere spielt die F&E im Feld der Künstlichen Intelligenz spätestens seit der Jahrtausendwende eine wachsende Rolle und wird in der jüngeren Vergangenheit auch von Regierungsseite offiziell priorisiert. Wie die nachfolgenden sozialwissenschaftlichen Untersuchungsergebnisse in Kapitel 3.1 illustrieren, erwarten die staatlichen Akteure, dass KI zukünftig an Bedeutung zunehmen und stark in unterschiedliche militärische Bereiche hineinwirken wird.

Der tatsächliche militärische Einfluss von Softwaretechnologien im Allgemeinen und KI im Besonderen lässt sich aber erst an den technischen Realitäten und damit am technologischen Forschungs- und Entwicklungsstand relevanter neuer Technologien ermessen. Die in Kapitel 3.2 zusammengefassten Ergebnisse der exemplarischen Untersuchung der kurz- bis mittelfristigen technologischen Fähigkeiten von Softwaretechnologien in der militärischen Informationsgewinnung geben hierzu einige Rückschlüsse, die auf Basis einer naturwissenschaftlich-technischen Betrachtungsweise gezogen wurden.

3.1. Die Erwartungen an Softwaretechnologien

Dieses Kapitel fasst die Ergebnisse des sozialwissenschaftlichen Projektteils zusammen, in welchem die Erwartungen staatlicher Akteure an das Forschungsfeld KI im Mittelpunkt stehen (ausführlich dazu vgl. Kühne 2020: 12 ff.). Zunächst wird dargestellt, welche Priorität und Dringlichkeit die oben benannten Schlüsselakteure KI beimessen und welche sicherheits- und militärpolitischen Zielstellungen sie mit ihrem Engagement in F&E verfolgen. Daran anschließend werden Antworten auf die Frage präsentiert, welche militärischen Fähigkeiten und Potenziale sich die untersuchten Akteure von der Applikation der Technologietrends erhoffen.

3.1.1 Zielstellungen im Feld der KI

In den USA wird F&E in KI seit 2016 von Regierungsseite offiziell priorisiert. Die im selben Jahr weltweit erste Veröffentlichung einer nationalen KI-Strategie (White House 2016a) unterstreicht die strategische Relevanz, die die USA KI für Wirtschaft und Gesellschaft zuschreiben. Seither werden Langzeitinvestitionen in Hardware und Algorithmen forciert (White House 2016b: 21 f.), u.a. mit dem Ziel, die Kommerzialisierung von KI voranzutreiben (vgl. ebd.: 6f, White House 2017b; 115th Congress 2017). Im Juni 2019 wurde mit dem „National Artificial Intelligence Research and Development Strategic Plan: 2019 Update" (White House 2019a) eine Aktualisierung des „National Artificial Intelligence Research and Development Strategic Plan" (White House 2016b) vorgelegt. Im Kontext der im Februar desselben Jahres gestarteten KI-Initiative formuliert der Plan das Ziel, den USA die weltweite Technologieführerschaft im Bereich KI zu sichern. Angestrebt wird auch die Implementierung von KI zum Zweck von Verteidigung und Sicherheit. Darüber hinaus wird der Hoffnung auf einen alle Verteidigungsbereiche übergreifenden Effekt von KI-Applikationen Ausdruck verliehen, der von Logistik über Gesundheitsversorgung bis hin zu Kommunikation reichen soll (White House 2016a: 38). Dieser militärische Sicherheitsfokus bei der Technologieentwicklung korrespondiert mit der 2016 in Kraft getretenen Third Offset-Strategie des Verteidigungsministeriums, welche insbesondere die Relevanz von KI und Autonomie für die langfristige militärstrategische Ausrichtung der USA betont (ILW 2017: 1; vgl. Martinage 2014: ii, 41). Mit der Verknüpfung von militärischer Strategie, Technologie und Streitkräfteorganisation im Kontext von KI-F&E verbindet sich für die USA insofern das Versprechen auf strategische Standortvorteile (White House 2019a: 8, 24 ff.; ILW 2017: 1; White House 2016a: 3) und argumentiert wird überdies, so als Ordnungsmacht dort regulierend eingreifen zu können, wo die Anwendung der Technologie, etwa in China oder Russland, geeignet sei, internationale Normen oder Menschrechte zu gefährden (White House 2017a: 35; mit einer ähnlichen Argumentation vgl. auch U.S. Army 2019a: 3, DoD 2018: 5). Die große Bedeutung, die KI im militärischen Sicherheits-Kontext beigemessen wird, illustriert sich überdies einerseits in einer Reihe interner Forschungsverbünde (vgl. DoD 2018) und findet andererseits ihren Niederschlag in der Höhe finanzieller Investitionen: Allein für das Verteidigungsministerium (Department of Defense, DoD) hat sich das verausgabte Budget für nicht klassifizierte F&E im Bereich von „Robotics und Intelligent Systems" seit 2015 von 96,6 Mio. U.S.-Dollar (USD) (NITRD 2016: 10) auf erwartete Ausgaben von 154,5 Mio. USD (NITRD 2019: 8) im Jahr 2020 erhöht. Die erstmals für die Fiskaljahre 2018–20 ausgewiesene NITRD (Networking & Information Technology Research & Development Program) Programmkomponente „AI" (Artificial Intelligence) veranschlagt ein Budget in Höhe von 654,4 Mio. USD, wobei Angaben über Aufwendungen für das DoD und das Defense Advanced Research Project (DARPA) wiederum klassifiziert sind (ebd.: 8f.). Ausdrücklich adressiert wird in den USA der Dual-use-Charakter von KI, den die U.S. Army (2017b: 4 f.) für die Entwicklung von autonomen militärischen Systemen, auch aus Kosten- und Effizienzgründen, explizit fordert und durch Kooperationen mit zivilen Akteuren avisiert (ebd.; vgl. auch White House 2019b: 37; U.S. Army 2019a: 9): „Kommerzielle KI-Unternehmen sind in einer Vielzahl von Sektoren aktiv und die Möglichkeiten für Dual-use-Anwendungen innerhalb des DoD sind enorm" (SASC 2019: 4, eigene Übersetzung).

Im chinesischen Kontext fungiert KI gegenwärtig und mit Blick auf die nahe Zukunft als „Megaprojekt" (Ding 2018: 8 f.). Bereits mit dem „National Medium- and Long-Term Plan for the Development of Science and Technology (2006–2020)" wurde 2006 die Grundlage für die Entwicklung von „smart sensors" oder „smarts robots" gelegt (vgl. He 2017: 2). Der Terminus

Künstliche Intelligenz hat 2016 auch Eingang in Chinas „13th Five-Year Plan on National Economic and Social Development of The People's Republic of China" (State Council 2016) gefunden sowie 2017 auch erstmals in den jährlichen Arbeitsbericht der Regierung zur ökonomischen Wachstumsentwicklung der Volksrepublik. Erwartet wird, mit KI zur Erhöhung der ökonomischen Produktivität des Landes beizutragen (China Daily 2017). Mit dem „New Generation of Artificial Intelligence Development Plan"[2] (State Council 2017a) und dem „Three-Year Action Plan for Promoting Development of a New Generation Artificial Intelligence Industry (2018–2020)" (State Council 2017b) hat China einen Drei-Schritte-Plan entwickelt, um im Jahr 2030 u.a. auf dem Feld der KI im Staatenvergleich die Führung zu übernehmen bzw. bis 2020 mit zentralen Produkten in diesem Feld einen Wettbewerbsvorteil zu erringen. Zwar betont China die Förderung von KI vorrangig im Zusammenhang mit der Entwicklung einer nationalen Industrieentwicklungsstrategie. Vergleichbar mit den USA ist ihre Bedeutung aber auch sicherheitsstrategisch gerahmt und regelmäßig wird auf die explizite Verwertung des Dual-use-Charakters von Technologien, mit anderen Worten, die Verzahnung ziviler und militärischer Anwendungen in F&E verwiesen (vgl. ebd.: 6; DoD 2019b: 21; OSD 2019; Kania 2017: 18 f.). Auch China zielt auf Übertragungseffekte zwischen Privatindustrie und Staat, etwa die Entwicklung militärischer Roboter (State Council 2016) und unbemannter Systeme (vgl. Hille und Waters 2018). Aktuelle anwendungsorientierte Forschung und Entwicklung für das Militär, die sich insbesondere auf intelligente und autonome unbemannte Systeme richtet (State Council 2017b), orientiert sich in China an einer „military intelligentization" (Jinping 2017 zit. in Kania 2018)[3] – eine Zielstellung für künftige Technologiepolitik, die explizit auch in Chinas Strategiepapier für die neue Verteidigungs-Ära (State Council 2019) formuliert wird. KI bildet danach, neben „big data" oder „quantum information", eine zentrale Technologie, die den Weg hin zu einer „informatisierten" („informationized") und „intelligenten" Kriegführung bereiten soll (ebd.). China zielt insofern mit seinen militärischen KI-Ambitionen auf eine veränderte Kriegführung – eine Zielsetzung, wie sie auch im U.S.-amerikanischen Diskurs durchscheint.

In Israel lässt der bereits 2020 erwartete nationale KI-Plan, der an die 2012 durch das Nationale Cyberbüro aufgelegte Cyberstrategie anschließen soll (Berkowitz 2018), ebenfalls eine Verknüpfung ziviler und militärischer KI-Anwendungen erwarten. Dies legen Ankündigungen von Ben-Israel (zit. in Rapaport 2018), Leiter des Security Studies Programm in Tel Aviv, nahe, wonach der Plan zum einen der israelischen High-Tech-Industrie eine neue Stoßrichtung geben soll. Ein zentrales Mittel für die Zielerreichung ist die staatliche Förderung von Start-Ups. Neben der israelischen Wirtschaft soll zum anderen die nationale Sicherheit mit Hilfe eines vereinheitlichenden Konzepts der Künstlichen Intelligenz gestärkt werden (vgl. Ben Israel zit. in ebd.). Militärische KI-Anwendungen liegen auch deshalb nahe, weil sich Israel's KI-F&E auch auf verteidigungsbasierte Innovationen richtet. Erwartet werden Übertragungseffekte in den Zivilbereich, die „in akademische und private Bereiche ausstrahlen und eine Reihe von kommerziellen Anwendungen ermöglichen" können (Groth und Nitzberg 2018: 126 zit. in Groth et al. 2019: 23; vgl. Berkowitz 2018). Noch werden konkrete Forschungsergebnisse für die KI-Forschungscommunity aber nicht sichtbar (vgl. Bagon zit. in Kelly 2019). KI-F&E in Israel ist zwar in hohem Maße durch seine, insbesondere im Verhältnis zur Gesamtbevölkerungszahl, hohe Dichte an Start-Ups geprägt (vgl. Roland Berger und Asgard 2018; Groth et al. 2019: 23), für die die israelische Innovation Authority der größte öffentliche Investor ist (IDF 2017a). Laut eines Reports der Start-Up Nation Central (Korbet

[2] Mitunter findet sich auch die Bezeichnung „Next Generation AI Development Development Plan" (vgl. He 2017).
[3] Kania (2017: 17) verweist darauf, dass der zugrundeliegende Terminus auch mit „smart" übersetzt werden könne, „intelligentization" das Konzept der People's Liberation Army (PLA) „informatization" aber deutlicher werden lasse.

2019: 12) sind bereits im Jahr 2018 37 Prozent des für Start-Ups aufgebrachten Kapitals in KI-Unternehmen investiert worden, ohne KI-Plan sei allerdings keine klare KI-Forschungsförderung erkennbar, so Groth et al. (2019: 25). Demgegenüber gilt das Militär gleichwohl selbst als zentraler Innovationstreiber, aktiver Entwickler und Anwender der KI (ebd.: 26ff.) und auch das Start-Up-Personal rekrutiert sich wiederum stark aus dem Militär (vgl. Netanyahu zit. in Fox News 2018). Im Zuge einer erfolgreichen Kommerzialisierung von KI wird dann auch erwartet, zivile Anwendungen wiederum in den militärischen Bereich zu integrieren, „wo sie helfen können, gefährliche Aufgaben zu verrichten, die derzeit nur von Menschen ausgeführt werden" (IDF 2018, eigene Übersetzung). F&E in KI gilt insofern auch in Israel als ein zentrales Moment für die Steigerung der Effektivität und Effizienz der Streitkräfte (IDF 2017b), wie es auch Lt. Col. Nurit Cohen Inger vom IDF formuliert: „Wir entwickeln keine Technologie um der Technologie willen. Wir suchen nach Wegen, um wirklich etwas zu bewirken" (zit. in IsraelDefense 2017, eigene Übersetzung). Die Entwicklung unbemannter Boden- bzw. Luftfahrzeuge bilden danach wesentliche Elemente in der israelischen Technologieentwicklung im Verteidigungssektor. In Israel ist in Bezug auf KI insofern eine starke Verwobenheit zwischen der Maßgabe, die eigene High-Tech-Industrielandschaft zu stärken (vgl. Israel Innovation Authority 2019) und dem Bestreben, die stark verteidigungsbasierte Innovationsfähigkeit voranzutreiben, zu konstatieren.

Russland hat bisher als einziges der untersuchten Länder 2019 eine explizit zivile KI-Strategie aufgelegt (Office of the President of the Russian Federation 2019). Trotz Wladimir Putins Warnung 2017 (CNBC 2017) vor einer Monopolisierung der KI-Macht, in der er das disruptive Potential von KI für eine künftige Kriegführung andeutet – „wenn die Drohnen einer Partei durch Drohnen einer anderen Partei zerstört werden, wird sie keine andere Wahl haben, als sich zu ergeben" (zit. in ebd., eigene Übersetzung) – sieht die Strategie vor, die allgemeinen Voraussetzungen für KI zu verbessern. Sie zielt insbesondere auf Kooperationen zwischen der Regierung und wissenschaftlichen Organisationen. Russland setzt im Feld der KI aber auch auf internationale Kooperationen mit der Privatwirtschaft, etwa mit chinesischen Firmen, z.B. im Rahmen eines Forschungsprogramms von Huawei im Bereich der Robotik, Gesichtserkennung und KI (Elmer 2019). Zwar gilt es in wirtschaftlicher Hinsicht für Russland – so Präsident Putin –, die eigene Position auf dem internationalen KI-Markt zu verbessern. KI-Anwendungen sind aber nicht auf zivile Anwendungsbereiche beschränkt, sondern finden Präsident Putin zufolge bereits etwa in Drohnensystemen und Robotern ihre aktive Anwendung (zit. in Tass 2019c; vgl. Tsalikov zit. in Interfax 2018). Dass eine weitergehende Anwendung von KI im militärischen Sektor in Russland geplant ist, legt auch das für Anfang 2020 angekündigte Rüstungsprogramm bis 2033 nahe, in dessen Rahmen die Ausstattung des russischen Militärs und anderer Sicherheitsagenturen mit neuen Technologien auf 70 Prozent erhöht werden soll. Bereits im 2018 veröffentlichten Rüstungsprogramm bis 2027 waren die Entwicklung und der Einsatz unbemannter Luftfahrzeuge vorgesehen (Connolly und Boulègue 2018: 25). Im selben Jahr kündigte das russische Militär-Industrie-Komitee zudem an, bis zum Jahr 2030 den Einsatz von komplett ferngesteuerten und autonom agierenden Robotik-Plattformen auf 30 Prozent zu erhöhen (Eshel 2015). Auf einem Treffen des russischen Sicherheitsrats 2019 gab Präsident Putin bekannt, die KI-Nutzung im Verteidigungssektor auszuweiten und auch verstärkt auf Drohnen, Laser, Hypersonic- und Robotik-Systeme zu setzen (Tass 2019b). Im Rahmen des Armee-2020-Forums mit über 130 Delegationen wurde überdies nach Aussagen des stellvertretenden Verteidigungsministers ein Runder Tisch zum Thema KI angekündigt (Tass 2019a). Folgt man den Aussagen des ersten stellvertretenden Verteidigungsministers Taslikov (zit. in Interfax 2018), wird KI in nahezu jedem militärischen Bereich Russlands seine An-

wendung finden. Im Mittelpunkt der Rede über KI steht folglich auch in Russland die Heuristik eines allumfassenden Nutzens, der zivile und militärische Anwendungspotentiale miteinander verbinden soll. Auf der Basis des vorliegenden Materials lässt sich folgern, dass auch Russland darauf zielt, sowohl in wirtschaftlicher Hinsicht von KI-Anwendungen zu profitieren als auch im Bereich der Militärtechnik an die Fortschritte in F&E in KI anderer sicherheitspolitischer Schlüsselstaaten anzuschließen.

3.1.2 Argumentationen für die militärische Nützlichkeit von KI

Vor diesem Hintergrund lassen sich die jeweiligen Begründungen für die Notwendigkeit einer Integration von KI in militärische Anwendungsfelder auf der Basis des Materials in sechs zentrale, sich teils überlappende, Argumentationsmuster entfalten: (1) die Verbesserung von Command & Control (nachfolgend C2), (2) die Erhöhung der Situational Awareness bzw. des Lagebewusstseins, (3) die Ermöglichung von Early Warning bzw. Frühwarnung, (4) die Security bzw. der Schutz der Soldat*innen, (5) die Verbesserung der militärischen Logistik sowie (6) die Erhöhung der Agilität u.a. durch Mensch-Maschine-Interaktivität.

Command & Control: Entscheidungsprozesse automatisieren

Unter Command & Control versteht man die Ausübung von militärischer Autorität und Leitung über zugewiesene und angegliederte Streitkräfte bei der Durchführung einer Mission. Es impliziert spezifische Entscheidungsstrukturen und -prozeduren auf der Operateursebene, in die die Mechanismen der Situational Awareness und des Early Warning eingebettet sind. Für die Verbesserung des C2 wird ein übergreifender Effekt von KI erwartet, der sich insbesondere durch die Implementierung in automatisierte Systeme ergeben soll. Im Mittelpunkt steht dabei sowohl die größtmögliche Vernetzung von Daten und Systemverbünden, wie es auch im Konzept des Network Centric Warfare[4] angelegt ist, als auch eine weitgehende Automatisierung des gesamten C2-Systems. Sollen insofern die ihm inhärenten Entscheidungsprozesse automatisiert werden, reduziert sich auch die Anzahl menschlicher Operatoren, die die Systeme kontrollieren. Ein Vorteil wird etwa aus russischer und amerikanischer Perspektive darin gesehen, mittels KI die Kontrolle über automatisierte und autonome Systeme zu erhöhen (Interfax 2015; U.S. Air Force Office of the Chief Scientist 2015: 9) und auf diese Weise die taktische Mobilität zu erhöhen (vgl. White House 2016a: 10, Fn. 17).

Der Vorteil von KI liege überdies darin, große Datenmengen analysieren zu können sowie verteilte Plattformen, Sensoren und Waffensysteme zu optimieren (U.S Army 2019b: 10, 20; ebd. 2017b: 1 f.; DoD 2017: 21; Ryan und Mittal 2019; Spencer et al. 2019: 3). Im Kontext von C2 nimmt insofern die Automatisierung von Datenprozessen einen hohen Stellenwert ein, welche dazu dienen soll, Kommandeur*innen und Soldat*innen bei der Entscheidungsfindung zu unterstützen. So kündigt die U.S. Air Force (2019) in ihrer Ergänzung zur KI-Strategie des Verteidigungsministeriums an, große Datenmengen unterschiedlichster Herkunft nutzen zu wollen und zu diesem Zweck die Integration von KI zu forcieren. Erwartet wird ein die Entscheidungs- und Handlungsstrukturen grundlegend verändernder Effekt von KI. Ihr Einsatz, etwa in der Bildanalyse (DoD 2018: 11) oder im Rahmen von „Human-Machine-Interfaces" (ebd.: 15; DoD 2017: 29ff.), soll es ermöglichen von „planning and judgment" („Planung und Be-

[4] Der Begriff des Network Centric Warfare steht für ein Modernisierungskonzept des Militärs, das, Mitte der 1990er im U.S.-amerikanischen Kontext entwickelt, auf die Verteilung und Vernetzung von Informationen und Ressourcen zielt, um die Lagebeurteilung zu verbessern.

wertung") zu „reaction and autonomy" („Reaktion und Autonomie") im Rahmen von C2 überzugehen (U.S. Army 2019b: 20). Durch ein gemeinsames Verständnis der massiven, mitunter aber lückenhaften oder widersprüchlichen Datenmengen erhofft man sich die Dauer von Entscheidungskreisläufen zu reduzieren (White House 2019b: 14; DoD 2018). Eine Verbesserung des C2 durch KI wird in dieser Hinsicht mittelfristig nicht nur darin gesehen, schneller strategische Indikatoren und Warnungen zu erhalten. Ermöglicht werden soll auch der Einsatz gemischter, d.h. bemannter/unbemannter Formationen (DoD 2017: 3; ILW 2017), um auf diese Weise spezifische Verteidigungsmissionen effektiver durchzuführen, „in denen Faktoren wie Geschwindigkeit, Informationsmenge und Synchronisation die menschliche Entscheidungsfindung überfordern können" (U.S. Army 2017b: 3, eigene Übersetzung). Ein Beispiel hierfür bildet das Projekt CODE (Collaborative Operations in Denied Environment) der DARPA, das darauf abzielt, eine Gruppe von unbemannten Bodenfahrzeugen unter der Aufsicht nur einer Person zusammenarbeiten zu lassen (DARPA, Wierzbanowski o.J.). Lang- bzw. mittelfristige Zielvorstellungen reichen bis zu Plattformen unbemannter Bodensysteme (ebd.: 24) oder den „connected soldier" des IDF (2017b). Auch „Noked" (Akronym für den hebräischen Begriff für „digitaler Kampfablauf"), ein interaktives Kartensystem, zielt auf automatisierte Standortbestimmungen und eine Verbesserung des C2 (IDF 2016b). Zudem wird erwartet, durch ein solches Teaming einen kontinuierlichen Feedback-Loop zwischen Soldat*in und der KI-Lösung zu erzeugen, indem „KI-Lösungen aus diesem Einsatz lernen und dieses Wissen an andere Einheiten auf dem Schlachtfeld weitergeben, um nachfolgende Iterationen zu verbessern" (Spencer et al. 2019: 5, eigene Übersetzung; vgl. auch White House 2019b: 15).

Situational Awareness: Lagebewusstsein verbessern

Ein weiteres zentrales Argument für den Einsatz von KI in militärischen Einsatzszenarien bildet die Erhöhung des Lagebewusstseins bzw. der Situational Awareness der Soldat*innen. Sie beinhaltet nach Endsley (1995: 36) das Moment des Wahrnehmens und des Verstehens von Elementen in der Umgebung innerhalb eines Zeit- und Raumbereichs und die Projektion ihres Status in die nahe Zukunft. Die militärische Situational Awareness zielt folglich darauf, bereits im Vorfeld Gefahrenzeichen zu erkennen und durch daraus abgeleitetes präventives Handeln einen zeitlichen und taktischen Vorteil im Kampfgeschehen zu erlangen. Die besondere Bedeutung von neuen Technologien für das Lagebewusstsein liegt darin, dass sie ein neues Moment in diese klassische Anforderung eingeführt haben, die nach Chris Zebrowski (2016: 101 f.) eng mit dem Konzept des Network Centric Warfare verknüpft ist. Danach ermöglichen es neue Technologien, indem sie in die einzelnen Momente der Lagebewertung involviert werden, „Situationen" gewissermaßen erst hervorzubringen. Im Zusammenhang mit der Wahrnehmung und Informationsverarbeitung wird der Vorteil von KI dann nicht nur darin gesehen, die Datenanalyse multipler Datenbestände effektiver zu gestalten. Ihre Implementation soll auch dazu dienen, frühzeitig Indizien für eine Vielzahl von Risiken im Rahmen von „Intelligence, Surveillance Reconnaissance" (ISR) zu entdecken (vgl. Rojkes Dombe 2019; IDF 2017b, White House 2016a: 3; DoD 2018: 6, U.S. Army 2017a: 44), etwa durch die Kombination von Sensoren und Algorithmen (White House 2019a: 10, 16; ebd. 2016b: 18; DoD 2018: 7, 11). KI gilt in diesem Zusammenhang als zentraler Faktor bei der Entwicklung von „Robotic Autonomous Systems" (RAS) (ebd.; U.S. Air Force Office of the Chief Scientist 2015: iii, 2 f., 16). Die „Robotic and Autonomous Systems Strategy" der U.S.-Army (2017b: i ff.) priorisiert die Entwicklung autonomer Systeme, um einerseits Soldat*innen kognitiv zu entlasten und andererseits durch die automatisierte Datenerfassung und -analyse schneller zu operativen Entscheidungen zu gelangen (ILW 2017: 3; DoD 2017: 17, 31; U.S. Army 2017b: 3, 5). Aus Sicht der U.S. Army (2017b: 15) sind RAS vor allem des-

halb geeignet die Lagebewertung zu schärfen, da sie eine Vielzahl qualitativ variierender Daten nicht nur erfassen, sondern auch zeitnah verarbeiten und daraus Indikatoren für die Situationsanalyse ableiten könnten. Im Rahmen dieser Strategie bildet ein kurzfristiges Ziel (2017–2020), tragbare RAS für den Truppeneinsatz und unbemannte Boden- und Flugsysteme zu entwickeln (U.S. Army 2017b: 4 f.). Sensoren (U.S. Army 2017a: 44; DoN 2016: 28) bzw. sogenannte „soldier-borne sensors" (U.S. Army 2017b: 6) sollen dazu dienen, zeitsparend und über weite Strecken in Echtzeit das Lagebewusstsein zu schärfen, ohne dass sich die Soldat*innen direkt vor Ort einen Eindruck von der Lage verschaffen müssen: „Es bietet eine organische Schnellübersicht zur Situationserkennung, die sie derzeit nicht haben" (Barroso 2017, eigene Übersetzung). In diesem Zusammenhang forciert die U.S. Army (2019b: 19) langfristig eine sogenannte „robot-onrobot affair", d.h. den Einsatz von unbemannten Plattformen gegen dieselben.

Early Warning: Frühwarnung ermöglichen

Neben der Situational Awareness ist das Konzept des Early Warning zentral, das ebenfalls auf die Neutralisierung von Bedrohungen zielt. Es ist allerdings vor allem in taktischer Hinsicht relevant und hat seinen Ursprung im Aufbau von Computergestützten Frühwarn- und Entscheidungssystemen. Diese sollen es ermöglichen, den Einsatz eines atomaren Angriffs noch innerhalb der Raketenflugzeit zu erkennen. Im Kalten Krieg wurde es angesichts der potentiell massiven Bedrohung zwischen den Nuklearmächten entwickelt und es zielt darauf ab, mittels komplexer technischer und organisatorischer Systeme, Menschen bei der Entscheidungsfindung zu unterstützen.[5]

Entsprechende Befähigungen, etwa die Verbesserung der Wirksamkeit von Raketenabwehr und Zielerkennung und/oder Flugbahnberechnung, werden auch durch den Einsatz von KI erwartet. Im Kontext der Third-offset-Strategie der USA soll die Nutzung neuer Technologien wie Sensoren nicht nur der Verbesserung der Datenvernetzung und -verarbeitung dienen, sondern auch dazu, die menschliche Entscheidungsfähigkeit technisch zu unterstützen. So erwartet etwa das DoD (DoDLive o.J.) vom Einsatz sogenannter Deep Learning Systeme, Indikatoren und Warnungen in der Cyber-Abwehr, der elektronischen Kriegsführung und im Fall von Raketenangriffen mit hoher Dichte schneller als der Mensch zu ermitteln.

Auch aus der Perspektive der israelischen Streitkräfte bietet KI Möglichkeiten (IDF 2017b), Datenerfassung und -analyse zu verbessern und so Früherkennung zu ermöglichen. Mit einem vergleichbaren Ansatz werden auch mobile Radarsysteme eingesetzt, die Soldat*innen bei sich tragen und auf Beschuss reagieren (IDF 2014). Die im Carmel-Programm[6] entwickelten Lösungen, z.B. das „Iron Vision ‚See Through' Helmet Moounted Display" von Elbit Systems, zielen ebenfalls durch die Anwendung von KI darauf ab, Vernetzung, Lagebeurteilung und Frühwarnung zu verbessern (Kempinski 2019).

Security:
Sicherheit der Soldat*innen gewährleisten

Situational Awareness und das Konzept des Early Warning zielen vor allem auf die Ermittlung, Vorhersage und Abwehr strategisch-taktischer Risiken, mit anderen Worten auf das militärische Risikomanagement. Ein weiteres Sicherheitsargument fokussiert speziell den Schutz der körperlichen Unversehrtheit der Soldat*innen, der mit Hilfe von KI verbessert werden soll (vgl. Mena 2019; DoD 2018: 6; ILW 2017: 3). Danach erlauben es Datenerfassung und -verarbeitung risikoarme Situationen zu schaffen, etwa indem verborgene Gefahren schon im Vorfeld mittels Temperatur-, elektromagnetischer oder optischer Signaturen erfasst werden (White House

[5] Gleichwohl wird seit Jahrzehnten die Fehleranfälligkeit der Systeme als hoch bzw. die Möglichkeit, entsprechende Fehler innerhalb der nur kurzen Reaktionszeiten zu erkennen, als gering eingeschätzt (Bläsius und Siekmann 1987, 2019).
[6] Das 2016 gemeinsam von IDF und Teilen der israelischen Rüstungsindustrie aufgelegte Programm entwickelt militärische Einsatzfahrzeuge.

2019b: 37; U.S. Army 2017a: 25). Auch der Einsatz von RAS soll es ermöglichen, frühzeitig Situationen im Hinblick auf ihren Risikograd zu beurteilen, und darüber hinaus auch in als riskant beurteilten Situationen zu agieren, wie etwa die U.S. Army (2017b: 15) betont.

Die U.S. Army (2019a: 9) verbindet mit Autonomie, einem ihrer priorisierten Forschungsfelder, Manövrierfähigkeit und Geländegängigkeit von Plattformen. Mittelfristig realisierbar gelten diese durch eine Kombination von Sensoren und „advanced computing" (ebd.: 3). Der „Robotic and Autonomous Systems Strategy" folgend, operieren die gegenwärtig eingesetzten unbemannten Boden- und Luftfahrzeuge „zwischen Telebetrieb und Semiautonomie" (ebd.: 3). Der Vorteil unbemannter Systeme wird darin gesehen, menschliche Akteure in Situationen zu ersetzen, die sich durch ein erhöhtes Risiko, Schaden zu erleiden, auszeichnen (vgl. ILW 2017; U.S. Army 2017b: 2 ff.; DoD 2018: 5; ebd. 2017: 31 f.; White House 2016a: 37; mit derselben Argumentation vgl. IDF 2016a). Mit ihrer Hilfe sollen folglich zukünftig weniger Soldat*innen in Hochrisikosituationen eingesetzt und gleichzeitig die Performance der Truppe erhöht werden. Im israelischen Kontext dient der Einsatz des „Border Protector", ein halbautomatisierter mit Kameras und Sensoren ausgestatteter Geländewagen, dem Schutz der Soldat*innen sowie einem effektiveren Agieren der israelischen Streitkräfte in Situationen, die gekennzeichnet sind von „Scharfschützen der Hamas, Panzerabwehrraketen und Sprengstoff [...] An Orten mit hohem Risiko kann das ferngesteuerte Fahrzeug einen wesentlichen Unterschied machen"[7] (IDF 2016a, eigene Übersetzung).

Logistics: Effizienz von Nachschub und Verteilung erhöhen

Militärlogistik dient im Feld komplexer Nachschub- und Transportwege zur Sicherstellung der Versorgung sowie dem Transport und der Unterbringung von Material und militärischen Akteuren. Zur Unterstützung dieser Funktionen soll der Einsatz von KI die Soldat*innen im Einsatzgebiet entlasten (DoD 2018: 11; ILW 2017: 3; U.S. Army 2017b: i, 1, 4), etwa durch den Einsatz von RAS-Plattformen verschiedener skalierbarer Größen und Missionskonfigurationen (U.S. Army 2017b: 5), die die physische und kognitive Arbeitsbelastung der Soldat*innen reduzieren (ILW 2017: 3).

Da die logistische Verteilung überdies als ressourcenintensiv gilt, setzt die U.S. Army (2017b: 7 ff.) auch auf die Leader-Follower-Fähigkeit – eine Mischung aus bemannten und unbemannten Fahrzeugen, um Konvoi-Operationen durchzuführen. Dafür werden Kurzstreckenfunkgeräte und computergestützte Verhaltensalgorithmen verwendet, um mehrere unbemannte Lastwagen einem bemannten Führungsfahrzeug folgen zu lassen. Unbemannte Systeme, sowohl in der Luft als auch am Boden, sollen bei der Wiederversorgung der Einheiten unterstützen (ebd.). Der Einsatz von KI soll darüber hinaus genutzt werden, um den Ausfall kritischer Geräteteile vorherzusagen, die Diagnose zu automatisieren und die Wartung auf der Grundlage von Daten und Anlagenzustand zu planen. Ähnlich soll die Technologie eingesetzt werden, um die Bereitstellung von Ersatzteilen zu steuern und die Lagerbestände zu optimieren (DoD 2018: 11).

Teaming: Agilität erhöhen

Die U.S. Army (2019a: 9) erhofft sich durch den Einsatz von KI zuletzt auch Vorteile im Hinblick auf Geschwindigkeit und Agilität im Kampfgeschehen. Ein weiteres zentrales kurzfristiges Ziel bildet hierfür die Integration von automatisierten Systemen in das Kampfgeschehen (U.S. Army 2017b), etwa von autonom agierenden Maschinen bis zum Jahr 2025. Taktische Radfahrzeuge, die mit teilautonomer Leader-Follower-Technologie ausgestattet sind, sollen teilautonome Konvoioperationen durchführen können

[7] Vgl. auch das Guardium Unmanned Ground Vehicle des IDF, das mit einer 360-Grad-Kamera ausgestattet ist (IDF 2014).

(U.S. Army 2017b: 5). In diesem Zusammenhang deutet sich an, dass es im U.S.-amerikanischen Kontext eine Zielstellung bildet, Teams aus Mensch und Maschine zu entwickeln. Deren Ausformungen können mittel- bis langfristig teils alle der bis zu dieser Stelle beschriebenen Bereiche übergreifen. Entsprechende Vorstellungen reichen bis zum „Robotic Wingman" resp. zu UGS Plattformen, die nicht nur automatisiert Daten analysieren, sondern in variierendem Grad autonom und partnerschaftlich im Kampfgeschehen agieren (U.S. Army 2017a: 24).

Mit der hier geplanten Autonomie der technischen Systeme verlagert sich der Fokus auf eine facettenreiche Kooperation, sowohl was die Operateursebene betrifft, als auch im Kampfgeschehen: Die Visionen beziehen sich einerseits auf eine Zusammenarbeit zwischen technischen Systemen (z.B. Drohnenschwärme oder autonome Aufklärungssysteme) und andererseits zwischen Mensch und Maschine. Dabei kann es sich sowohl um die Automatisierung von Entscheidungsstrukturen oder geplante technische Entwicklungen handeln, etwa einzelne Sensoren, die von den Soldat*innen getragen werden oder ganze mechanische softwareunterstützte Strukturen, wie z.B. Exoskeletten, die ihre Träger*innen automatisiert und situationsgemäß unterstützen (ILW 2017: 3).

3.1.3 Diskussion der Ergebnisse

Insgesamt zeigt sich, dass die untersuchten Länder seit einigen Jahren eine gesamtgesellschaftliche Rolle von KI betonen. Gerahmt als Schlüsseltechnologie mit beinahe unbegrenzten Implementationsmöglichkeiten fungiert sie im Diskurs als omnipotenter Lösungsansatz, wie insbesondere die nationalen KI-Strategien nahelegen. In allen Ländern verknüpfen sich mit ihr Versprechen auf wirtschaftliche Vorteile, die vor allem aus der Automatisierung von Funktionen in vielzähligen gesellschaftlichen Bereichen resultieren sollen. Obzwar nicht für alle Länder Daten über Investitionen und Beschaffung vorliegen, deutet sich an, dass F&E in KI ein hoher Stellenwert beigemessen wird. Im Hinblick auf die jeweiligen militärischen Ambitionen lassen sich zwar Unterschiede dahingehend identifizieren, wie die Bedeutung, Notwendigkeit und die Implikationen einer Integration von KI in militärische Anwendungsbereiche bewertet werden. So wird von KI wohl am deutlichsten im U.S.-amerikanischen und im chinesischen Diskurs nicht nur eine Erhöhung der Effizienz der Streitkräfte erhofft. KI steht hier auch im Mittelpunkt von Veränderungen in der Militärdoktrin. Gleichwohl unabhängig davon, als wie weitreichend ihr Einfluss im militärischen Feld erwartet oder mitunter forciert wird, zielen jedoch alle Länder darauf, den Dual-use-Charakter der Technologie zu nutzen. Mit KI verbindet sich insofern das Versprechen auf Übertragungseffekte, mit denen Vorteile sowohl im zivilen als auch im militärischen Sektor verbunden werden.

KI-Systeme sollen in vielen verschiedenen Rollen auf dem gesamten Schlachtfeld eingesetzt werden. Vielfach ist geplant, sie nicht nur in einer einzelnen Waffe, sondern in viele andere militärische Systeme zu integrieren: KI soll erstens bei der Verarbeitung und Interpretation von Informationen helfen. Erwartet wird zweitens, dass sie neue Formen der Kommandoführung ermöglicht, in dem die operativen Systeme in die Lage versetzt werden, große Datenmengen zu analysieren und Vorhersagen zu treffen, um auf diese Weise menschliche Aktionen zu lenken. Drittens soll sie dazu eingesetzt werden, um physische Objekte so zu steuern, dass sie ohne menschliche Aufsicht agieren. Insofern sind die Anwendungen sehr heterogen und beziehen sich auch auf militärische Teilbereiche, die überdies nicht immer direkt mit kinetischen Wirkungen verknüpft sind (z.B. Logistiksysteme).

3.2. Softwaretechnologien in der technischen Wirklichkeit

Ob die Erwartungen und Wünsche, die an die Fähigkeiten moderner Waffensysteme und die zukünftige Art und Gestaltung der Kriegführung gestellt werden, überhaupt erfüllbar sind, hängt in erster Linie von ihrer technologischen Realisierbarkeit ab. Diese sollte zuallererst an dem kurz- bis mittelfristigen, perspektivisch aber auch am langfristigen technologischen Forschungs- und Entwicklungsstand relevanter neuer Technologien bemessen werden. Dieser wird vor allem über eine naturwissenschaftlich-technische Einschätzung und Analyse der entsprechenden Forschungsfelder zu ermitteln sein. Welche dieser Technologien oder prognostizierten technologischen Anwendungen nun eine militärische Relevanz aufweisen könnten, gilt es parallel und fortlaufend zu untersuchen – z.B. in Form einer Technikfolgenabschätzung. Aller Voraussicht nach werden es Softwaretechnologien sein, die einen zunehmend größeren Anteil an jedem zukünftigen militärischen Fähigkeitszuwachs haben werden. Die Schwierigkeit besteht nun darin, eine belastbare Aussage darüber zu treffen, inwieweit sich Fähigkeiten von Softwaretechnologien zukünftig entwickeln werden und welche militärischen Potentiale hieraus erwachsen; dieses wird umso schwerer und unbestimmter, je weiter wir in die Zukunft blicken wollen. Dieser Umstand ist vor allem der besonderen „Komplexität von Softwaretechnologien" geschuldet: Einerseits den Schwierigkeiten, auf Grundlage einer Algorithmen-basierten Forschung auf alle tatsächlichen zukünftigen Anwendungen und möglichen Fähigkeiten schließen zu können. Anderseits wegen der ungeheuren Breite und dem Dual-use-Charakter des IT-Forschungs- und Entwicklungsfeldes als auch den vielfachen Abhängigkeiten und Synergien, denen Softwaretechnologien unterworfen sind. Denn neben Programmcode und Algorithmen spielen bei Softwaretechnologien auch die zugrundeliegende Hardware (Prozessoren, Elektronik, Sensoren etc.), die verwendete Infrastruktur (Datenverbindungen, Cloud-Services) sowie benötige Datensammlungen (Trainingsdaten, Sensordaten, Informationen etc.) eine elementare Rolle. Zukünftige Softwaretechnologien werden ihr volles Potential daher nur entfalten können, wenn das „Zusammenspiel" und die bestmögliche Funktionsweise jeder ihrer Bestandteile gewährleistet ist.

Diese technologischen und funktionalen Zusammenhänge in Bezug auf die militärische Anwendung von Softwaretechnologien wurden durch Hendrik Erz exemplarisch in einer Analyse der kurz- bis mittelfristigen technologischen Fähigkeiten von Softwaretechnologien in der militärischen Informationsgewinnung untersucht (Erz 2020). Die Schlussfolgerungen dieser Analyse sind im folgenden Kapitel 3.2.1 auszugsweise und zusammengefasst wiedergegeben.

3.2.1 Softwaretechnologien in der militärischen Informationsgewinnung

Während bereits breit diskutiert wird, in welchen militärischen Bereichen sich durch den Einsatz von Softwaretechnologien Vorteile und Optimierungen versprochen werden können – beispielsweise im Bereich der Lagebildgewinnung (Situational Awareness), dem Kommando- & Kontrollbereich (C2), der Frühwarnung etc. (siehe auch Kapitel 3.1.2) – sind die dafür dediziert benötigten Softwaretechnologien sowie deren operationelle Einbindung nur unzureichend ausgeleuchtet. Vor allem mangelt es aber immer noch an dem nötigen Verständnis dessen, was technologisch überhaupt realisierbar ist und welche zukünftigen Anwendungsszenarien hieraus eigentlich erwachsen können.

Am Anwendungsbeispiel der militärischen Informationsgewinnung werden im Folgenden

die dafür benötigten Softwaretechnologien und andere notwendige technologische Bestandteile erörtert, skizzenhaft ihr Zusammenspiel aufgezeigt und ihre Fähigkeiten – soweit absehbar – angedeutet.

Ausgehend von der These, dass der Dreh- und Angelpunkt von Softwaretechnologien insbesondere Daten sind, lehnt sich diese Analyse der militärischen Informationsgewinnung an der Schrittfolge des Weges von Daten an, ihrer Erhebung, Analyse und Speicherung. Da die Datenverarbeitung zentrales Bindeglied für Softwaretechnologien ist, hat sich diese als plausible Strukturierung erwiesen. Aus dieser ersten Eingrenzung ergeben sich fünf Oberkategorien, an denen eine mögliche militärische Verwendung von Softwaretechnologien innerhalb des Prozesses der Informationsgewinnung festgemacht werden kann. Diese sind Sensorik, eingebettete und integrierte Systeme, Kommunikation, Datenprozessierung und -analyse sowie Datenspeicherung und -verwaltung. Die Sinnhaftigkeit dieser Kategorien lässt sich durch gängige schematische Darstellungen militärischer Prozesse belegen (vgl. Alberts et al. 1999: 89; U.S. Army 2003) und ist in einer vereinfachten Form noch einmal in Abbildung 3.1 wiedergegeben.

Abbildung 3.1: Prozess militärischer Informationsgewinnung (Quelle: Erz 2020: 13)

Sensorik

Mit Bezug auf die Sensorik lässt sich festhalten, dass heutige Sensoren bereits einen Großteil der Umwelt zu erfassen imstande sind. Dadurch, dass Sensoren nicht auf die menschlichen Sinne begrenzt sind, können sie wesentlich mehr Informationen erfassen; im Bereich optischer Sensoren wird dies beispielsweise bei Infrarotkameras oder gar Hyperspectral-Imagern (HSI) deutlich, die entweder das für das menschliche Auge unsichtbare Infrarotspektrum oder einen Großteil aller elektromagnetischer Strahlung erfassen können (vgl. Manolakis und Shaw 2002: 31). Mit Bezug auf das Militär sind eine Reihe von Sensoren relevant: Reguläre Kameras, Infrarotkameras, Hyperspektral Kameras, „Light Detection and Ranging" (LiDAR, selten auch Ladar, benannt in Anlehnung an Radar), Radars und Positionssensoren („Inertial Navigation" Systeme sowie „Global Positioning" Systeme).

Kameras finden vor allem mit Bezug auf die Situational Awareness Anwendung (vgl. Shi et al. 2012: 1; für einen historischen Überblick vgl. Meyer 2019); ihre prominenteste militärische Verwendung dürfte die Drohnenüberwachung mit z.B. MQ-1 und MQ-9-Drohnen (bekannt als „Predator" und „Reaper") sein, die seit den späten 2000er-Jahren durch Wide Area Motion Imagery (WAMI) Technik nochmals intensiviert wurde (vgl. Leon 2019). Insgesamt kann ein Trend zu qualitativ verbesserten Sensoren und einer höheren Präzision beobachtet werden. Gerade in Hinblick auf Navigationssensoren umfasst dieser auch, sie resistenter gegen äußere Störungen zu machen. Ein wichtiges zukünftiges Feld ist auch die abgestimmte Zusammenarbeit verschiedenartiger Sensordaten („Sensor Fusion") um so die letztendliche Informations-

dichte zu erhöhen und Anwendungen wie Kollisionsvermeidung, Flugbahnkorrektur von Projektilen oder auch eine höhere Radarauflösung zu verbessern oder möglich zu machen.

Eingebettete Systeme

Als ein weiteres Ergebnis der bisherigen Untersuchungen kann festgehalten werden, dass die Unterscheidung militärischer Hardware in „eingebettete Systeme" („Embedded Systems") und „integrierte Systeme" („Integrated Systems"), im Militärjargon „System of Systems", Sinn macht. Denn auf autark agierenden Drohnen, Schiffen und U-Booten mit begrenztem Treibstoff lassen sich nicht beliebig viele Hardwarekomponenten installieren, die ausreichend leistungsstark für die Echtzeitanalyse von Sensordaten sind, insbesondere nicht von Videodaten. Dies ist in der Industrie als SWaP-Begrenzung („Size, Weight, and Power") bekannt (vgl. bspw. ADLink 2019). Insbesondere Prozessoren können erheblich zum Stromverbrauch beitragen.[8] Daher ist die Unterscheidung in eingebettete, d.h. autarke Systeme ohne externe Stromversorgung, und integrierte Systeme, die auch auf Kommandoinfrastruktur mit erweiterbaren und hohen Serverreserven zurückgreifen können, eingängig. Die Haupteinschränkungen solcher autarken Systeme liegen in drei Kategorien: Abgesehen von der verfügbaren Prozessionsleistung sind der Speicherplatz begrenzt (obgleich schon 2014 Drohnen bis zu 20 Terabyte Daten speichern konnten, vgl. Porche et al. 2014: 13) und die Bandbreite verfügbarer militärischer Kommunikationsverbindungen („Tactical Data Links", TDL) ist limitiert. Wohl auch in absehbarer Zeit werden eingebettete Systeme wie z.B. Drohnen nicht an die Rechenleistung festinstallierter Server herankommen. Ein softwaretechnologischer Trend zeichnet sich allerdings ab. So wird schon heute daran gearbeitet, „modellbasierte Klassifizierer" (siehe Abschnitt „Datenprozessierung und -analyse") immer kompakter zu gestalten, sodass zukünftig auch mit der reduzierten Prozessions- und Speicherleistung von Drohnen zunehmend komplexere Bilderkennung betrieben werden kann. Erst einmal ist aber weiterhin ein Zusammenspiel von mobilen Waffenplattformen und leistungsstarken Rechenzentren zu erwarten, was insbesondere resiliente Kommunikationskanäle erforderlich macht.

Kommunikation

Link 16, der derzeit in NATO und US-Armee am häufigsten verwendete Datenlink hat aufgrund starker Sicherheitsvorkehrungen wie Verschlüsselung und Anti-Jam-Verhalten eine Bandbreite von maximal 1.1 MBit/s (Martinez-Ruiz et al. 2010: 1163). Das reicht ggfs. für einen Videostream, doch darf dieser nicht in maximaler Qualität übertragen werden, da sonst bis zu 240 MBit/s an Daten produziert werden (Wiegand et al. 2003: 573). Andernfalls verbraucht ein Videostream die gesamte Bandbreite (vgl. McDonough, 2010), wodurch für Kommandobefehle, die ebenfalls über diesen Weg geschickt werden müssen, kein Platz mehr wäre.

Daher nutzt das US-Militär schon seit einiger Zeit zusätzlich kommerzielle Kommunikationssatelliten, die es den Drohnen erlauben, bis zu 30 MBit/s Daten zu senden (vgl. Erwin 2017) – allerdings mit schwächeren Sicherheitsvorkehrungen. Bis vor kurzem hat das US-Militär die Videodaten nicht einmal verschlüsselt, weswegen Aufständische mit Ausrüstung im Wert von gerade einmal rund 26 Dollar sämtliche Videostreams der Drohnen mitschneiden konnten und so bestens auf etwaige Drohnenschläge vorbereitet waren (vgl. Gorman et al. 2009). Das Unternehmen SpaceX verspricht mit dem aktuellen Projekt „StarLink" satellitengestützten Internetzugang mit bis zu 100 Gbit/s (McLain und King 2017: 7, 13, Tabelle 1).

Ob Kommunikationsverbindungen zukünftig einen kritischen „Flaschenhals" für die Datenüber-

[8] Vgl. für einen Überblick eine der vielen Benchmark-Ergebnisse im Netz, bspw. diesen Blogeintrag auf der US-Hardware-Webseite Tom's Hardware: https://www.tomshardware.com/reviews/geforce-radeon-power,2122-7.html.

mittlung darstellen werden, hängt davon ab, ob der Ausbau der Bandbreite und die Entwicklung neuer Verschlüsselungsstandards mit dem Anstieg der durch militärische Einsätze generierten Datenmengen Schritt hält. Entscheidend wird auch sein, welche Kommunikationsinfrastruktur das Militär zukünftig noch exklusiv vorhalten bzw. weiterausbauen will oder ob vornehmlich auf kommerzielle Lösungen gesetzt werden soll.

Datenprozessierung und -analyse

Die anhand von Sensorik erhobenen Daten können nun durch spezifische Software analysiert werden, um auf dieser Basis auch militärische Schlussfolgerungen ziehen zu können. Hierbei können zwei fundamentale Arten von Softwarealgorithmen unterschieden werden: Auf der einen Seite leistungstechnisch vergleichsweise simple Algorithmen mit hohen Prozessierungsgeschwindigkeiten, die allerdings nur begrenzt in der Lage sind mit komplexen Informationen wie Bildmaterial zu arbeiten (vgl. Shi et al. 2012: 2512 f.). Auf der anderen Seite leistungstechnisch erheblich ‚größere und schwerfälligere' Algorithmen, meist als „neuronale Netzwerke" (hier: modellbasierte Klassifizierer) bezeichnet, die in der Lage sind, nicht-maschinenlesbare Daten in solche umzuwandeln.

Für eine einfache Zielerfassung über Wärmesignaturen ist beispielsweise nur relevant, dass der Algorithmus ein Ziel immer wieder auf den Videodaten der Infrarotkamera identifizieren kann, d.h. nach warmen Regionen suchen muss, während er aber nicht analysiert, was genau er dort findet (vgl. Cao et al. 2015: 5; Wu et al. 2019: 12). Solche einfachen Algorithmen können optimiert werden und sind bereits heute zumeist auf mobilen Waffenplattformen mit ihren begrenzten Ressourcen lauffähig.

Anders sieht es beispielsweise mit WAMI-Anwendungen aus, wenn z.B. bewegliche als auch unbewegliche Objekte gefunden werden müssen, was ohne komplexe modellbasierte Klassifizierer schlicht nicht möglich ist. Diese beanspruchen erheblich höhere Rechenleistung, wie sie derzeit nur durch Server geliefert werden können. Es gibt hier aber bereits erste Optimierungsbemühungen, um auch diese Klassifizierer auf mobiler Hardware lauffähig zu machen. Allerdings sind die hier aufgezeigten Grenzen nicht trennscharf, sondern dienen vor allem der Veranschaulichung.

Datenspeicherung

Aber nicht nur Algorithmen und Softwareanwendungen sind wichtig für das Militär, sondern zentrale Probleme lassen sich auch in Hinblick auf die Datenspeicherung (sowohl schreiben als auch lesen) ausmachen. In dieser Hinsicht haben somit Paradigmen in Bezug auf die infrastrukturelle und methodische Planung der Datenspeicherung eine hohe Bedeutung. Zwei davon sind besonders mit Blick auf die sich derzeit anbahnende Einführung zunehmend größerer Datenbestände im US-Militär relevant, die über den JEDI-Vertrag des Verteidigungsministeriums mutmaßlich durch Microsoft auf Basis seiner Azure-Cloudplattform erfolgen wird: verteilte Dateisysteme wie „Apache Hadoop" und verteilte Datenbanken, die mittels „Sharding" auf hoher Geschwindigkeit betrieben werden können.

Im Falle verteilter Dateisysteme ist das zu lösende Hauptproblem die Bereitstellung großer Dateien. Dazu verwendet Apache Hadoop (das Hadoop Distributed File System, HDFS), ähnlich dem Google Distributed Filesystem (GDFS), sogenannte Knoten, auf welche größere Dateimengen geschrieben werden können (ein Ansatz, wie dieses Schreiben funktioniert, nennt sich „MapReduce", vgl. Dean und Ghemawat 2008). Die Geschwindigkeitsvorteile gegenüber herkömmlichen Dateisystemen werden dadurch erreicht, dass größere Dateien direkt auf die Knoten gestreamed werden, d.h. nicht am Stück transportiert werden, sondern Block für Block. Besonders für das spätere Öffnen und Lesen der Dateien ist dies von Vorteil, da Terabytegroße Dateien nicht in den Arbeitsspeicher eines Computers passen und so stattdessen Stück

für Stück entweder angeschaut, analysiert oder bearbeitet werden und die Änderungen direkt wieder zurückgeschrieben werden können.

Anders verhält es sich bei verteilten Datenbanken. Hier ist das Problem nicht die Verwaltung weniger sehr großer Dateien, sondern sehr vieler und sehr kleiner Dateien, nämlich Datenbankeinträgen – ähnlich einem Excel-Sheet. Da ab einer gewissen Menge nicht mehr alle Einträge in eine Datenbank passen und zumal eine einzelne Datenbank unter der Last der Anfragen zusammenbrechen würde, hat sich die Praktik durchgesetzt, große Mengen solcher Datenbankeinträge auf mehrere Datenbanken zu verteilen. Das zugrundeliegende Prinzip nennt sich „Sharding" (vgl. Aizman et al. 2019) und versucht, mittels sinnvoller Annahmen sowohl den Schreib- als auch den Suchaufwand möglichst zu reduzieren (vgl. für einen generellen Überblick Venkateswaran und Changder 2017; ein aufschlussreicher Algorithmus findet sich in Swart 2004). Das US-Unternehmen Instagram hat in einem Blogeintrag beschrieben, wie effizientes „Sharding" funktioniert (Instagram Engineering 2012).

Das Ergebnis beider Paradigmen ist, dass große Datenbestände mit hoher Geschwindigkeit verwaltet werden können, was vor allem für die Echtzeitüberwachung des Schlachtfeldes notwendig wäre — denn eine taktische Karte in einem Kommandozentrum hat nur einen geringen Nutzen, wenn relevante Daten erst um einige Minuten zeitverzögert auf dieser dargestellt werden. Verteilte Systeme wie die oben angesprochenen Dateiserver und Datenbankserver sind in Zeiten einer immer größeren Datenflut auch für das Militär von erheblichem Vorteil. Ein aktuelles Beispiel hierfür bietet das U.S.-Sicherheitsunternehmen Clearview (Hill 2020).

Zusammenfassung

In Bezug auf die militärische Informationsgewinnung wurden in dieser Analyse exemplarisch fünf Kategorien relevanter (Software-)Technologien beleuchtet – Sensorik, Kommunikation, die Besonderheiten von eingebetteten und integrierten Systemen, Datenprozessierung/-analyse und die Datenspeicherung. In diesen Gebieten zeigt sich, dass das Militär bereits auf vergleichsweise fortschrittliche Technologien zurückgreifen kann. Nichtsdestotrotz zeigten sich auch zahlreiche Einschränkungen. So können beispielsweise modellbasierte Klassifizierer bisher nicht auf eingebetteten Systemen laufen und Bildmaterial muss nach wie vor von Analyst*innen und/oder Computersystemen in Command & Control-Stützpunkten analysiert werden. Die Kommunikationsverbindungen stellen dabei heute einen wesentlichen „Flaschenhals" dar. Bei der Übertragung der Bilddaten von unbemannten Systemen wie Drohnen muss so zum Beispiel eine Abwägung zwischen Geschwindigkeit und Sicherheit getroffen werden. Insgesamt scheint sich dieser „Flaschenhals" aber mit der fortlaufenden Technologieentwicklung und den Investitionen in die Infrastruktur nach und nach zu weiten. Aus der bisherigen Analyse zur Rolle von Softwaretechnologien in der militärischen Informationsgewinnung lassen sich allerdings nur kurz- bis mittelfristige Einschätzungen ableiten, anhand deren sich bestenfalls ein grober Eindruck der kommenden Entwicklungen der nächsten Jahre abzeichnet. Eine profunde Analyse langfristiger Trends konnte im Rahmen dieser Analyse nicht durchgeführt werden.

Es ist sehr schwer zu einer verlässlichen Einschätzung der langfristigen Trends zu gelangen, denn die Literatur bleibt hier zumeist nur vage. Prognosen über längerfristige technologische Entwicklungen können am ehesten durch langjährige Expert*innen der jeweiligen Technologiefelder getroffen werden. Es gilt dann aber immer auch plausible, zukünftige militärische Anwendungen parallel mitzudenken, um zu einer langfristigen Einschätzung des zukünftigen Potentials militärischer Softwaretechnologien gelangen zu können.

In den kommenden Jahren sollte ein besonderes Augenmerk vor allem auf die Entwicklung

von Kommunikationstechnologie gelegt werden, ebenso auf die Fortschritte im Bereich des Zusammenspiels von Datenprozessierung und -analyse sowie Datenspeicherung. Doch auch die Entwicklung eingebetteter Systeme muss stärker in den Blick genommen werden, da hier mit Fortschritten und ggfs. Durchbrüchen zu rechnen ist.

4. Interdisziplinäre Analyse der Forschungsergebnisse

Auf der Grundlage der disziplinären Forschungsergebnisse und aufbauend auf den Forschungsleitfragen fokussierte der interdisziplinäre Projektteil des Forschungsvorhabens auf drei zentrale Themenkomplexe, die für den weiteren friedens- und sicherheitspolitischen Diskurs um den militärischen Einsatz von Softwaretechnologien und moderne Waffensysteme als essentiell erachtet werden und nur über eine interdisziplinäre Betrachtungsweise sinnvoll diskutiert werden können. Zum einen ist dies ein analytischer Abgleich der militärischen Erwartungen und technischen Realitäten in Bezug auf moderne Softwaretechnologien, der auf den disziplinären Ergebnissen dieses Forschungsvorhaben fußt (Hendrik Erz). Zum anderen eine Untersuchung der Probleme um die Definition von Künstlicher Intelligenz (Sylvia Kühne) sowie eine Analyse zum Themenfeld „Künstliche Intelligenz und Daten" (Sylvia Kühne und Mirjam Limbrunner). Die ausformulierten Ergebnisse dieser drei interdisziplinären Analysen finden sich im Folgenden.

4.1. Interdisziplinäre Analyse I: Softwaretechnologien – militärische Erwartungen und technische Realitäten

Ebenso wie der Forschungs-und Entwicklungsstand relevanter neuer Technologien den Blick auf die zukünftige Art der Kriegführung schärfen kann, lassen sich auch bereits heute absehbare militärische Anwendungsfelder und -szenarien auf spezifische technologische Schlüsselfaktoren untersuchen und als Ausschnitte einer potentiellen Zukunft bewerten. Im Rahmen des interdisziplinären Forschungsanteils dieses Projekts wurde daher versucht, entlang exemplarischer Kategorien möglicher militärischer Anwendungsfelder und -szenarien, die Plausibilität und Konsistenz der dort mit Softwaretechnologien jeweils verknüpften Erwartungen abzuschätzen.

Der nachfolgende Text von Hendrik Erz war von der Frage geleitet, inwiefern sich die militärischen Erwartungen an softwaretechnologische Anwendungen und die kurz- bis langfristigen technischen Realitäten decken oder widersprechen? Er fasst seine explorative interdisziplinäre Analyse hierzu entlang der im sozialwissenschaftlichen Forschungsteil identifizierten Kategorien (siehe Kapitel 3.1) zusammen. Die dargestellten Überlegungen gewähren nur einen kleinen und exemplarischen Einblick in die komplexe Thematik und beschränken sich wesentlich auf den kurz- bis mittelfristigen Zeithorizont.

4.1.1 Command & Control

Bei Command & Control (C2) geht es zentral um die Führung von Streitkräften, was Kommunikation impliziert. Die reichhaltigste Textstelle aus dem Bereich Command & Control findet sich bei Spencer et al. (2019: 6) und beschreibt den Ablauf einer sogenannten Multi-Domain Operati-

on (MDO, also eine Mission über mehrere Wirkungsräume hinweg) zum Ausschalten feindlicher Luftabwehrstellungen (Anti-Access/Area Denial (A2/AD) Systeme). Es handelt sich hier um einen komplexen Prozess mit zahlreichen beteiligten Softwarelösungen (vielfach als Teil eines eingebetteten Systems), Kommandoinfrastruktur und der Notwendigkeit zur komplexen Koordination: Nachdem ein*e Kommandeur*in den in diesem Beispiel voll automatisch ablaufenden Prozess zur Zielerfassung und eliminierung gestartet hat, soll ein „cyber system" ein Ziel „stimulieren". Dieses „cyber system" wird leider nicht spezifiziert, doch mit Bezug auf den im Paper angesprochenen A2/AD-Prozess ließe sich hier vermuten, dass es sich um ein System handelt, welches eine Drohne automatisiert in die Zielreichweite („Deep Maneuver Area") des A2/AD-Systems sendet und den Abschuss einer Boden-Luft-Rakete provoziert. Entsprechend günstige und daher für den Zweck des Abschusses einsetzbare Drohnen existieren bereits und haben die ausreichende Marktreife, um in das Zielgebiet gesteuert zu werden: Durch die Existenz der israelischen Luftmine „Harpy" ist belegt, dass sich Drohnen ohne menschliches Zutun in eine bestimmte, geographische Region (hier die Reichweite der Luftabwehrstellung) bewegen können. Die Verwendung von Luftminen wird an anderer Stelle auch bereits als zukünftige Taktik der U.S. Army genannt (U.S. Army 2018: 39).

Zur Lokalisierung der so provozierten A2/AD-Stellung erwarten Spencer et al. (ebd.), dass Daten aus mehreren Quellen zusammengeführt werden sollen. Auch dies ist mit den bisherigen Möglichkeiten der Technik bereits umsetzbar: Der Abschuss einer Boden-Luft-Rakete erzeugt Wärme, sodass der Abschuss auf Infrarotbildern wie auch auf Hyperspektral-Bildern klar erkennbar sein sollte (vgl. Erz 2020: 18 f.). Die Daten von Satelliten, ggfs. auch von AWACS-Flugzeugen, können mittels Datenprozessierung im Command & Control-Stützpunkt ausgewertet werden. Wichtig hierfür ist, dass den Bildern auch Koordinaten zugeordnet werden, was mittels Sensor Fusion (vgl. ebd.: 8 f.) möglich ist (mittels eines Positionssensors, vgl. ebd.: 19 ff.). Im nächsten Schritt erwarten Spencer et al. (ebd.), dass Software in der Lage sein soll, die geeignete Einheit für einen Angriff zu lokalisieren, allen anderen Einheiten mitzuteilen, sich aus der Schusslinie zu bewegen und den Satelliten anzuweisen, die Position zu beobachten. Bei dem Problem der Auswahl des „Best Shooter" handelt es sich um ein Optimierungsproblem (vgl. das Kapitel zu Problem-Solving in Russell et al. 2010: 64 ff.). Software muss für diese Fähigkeit die aktuelle Position aller im Gebiet befindlichen Einheiten sowie ihre aktuelle Bewaffnung kennen, um daraus den „Best Shooter" ermitteln zu können, d.h. die Einheit, die entsprechende Munition (mutmaßlich kommen nur Raketen infrage) besitzt und am schnellsten in einer günstigen Schussposition ist. Ist diese Entscheidung getroffen, kann die voraussichtliche Flugbahn berechnet werden und den entsprechenden Einheiten kommuniziert werden, sodass diese sich aus dem Weg bewegen.

Hier fallen bereits einige Probleme auf, die sich wahrscheinlich in einer realen Situation stellen. Implizit setzen Spencer et al. (ebd.) hier voraus, dass die Kommunikation unter den Einheiten und mit Command & Control stets funktioniert, wovon aber aufgrund von (feindlichen oder natürlichen) Störsignalen nicht immer ausgegangen werden kann (vgl. Erz 2020: 26 ff.). Zudem ist denkbar, dass einzelne Einheiten im Einsatzgebiet Funkstille wahren sollen und daher ihre Position nicht übermitteln können. Werden diese Einheiten von der Software „vergessen", kann es zu potenziell tödlichen Unfällen kommen. Zum anderen existieren trotz aller Fortschritte noch Inkompatibilitäten unter den Systemen – so können ältere AEGIS-Systeme beispielsweise nicht mit allen taktischen Datenlinks (TDL) kommunizieren (vgl. ebd.: 24 f.) – was darauf hindeuten könnte, dass vor allem älteres und neueres für dieses Szenario relevante Equipment mögliche Kompatibilitätsprobleme besitzen könnte. Spencer et al. (2019: 3 f.) sind sich dessen allerdings bewusst: „Without a well-defined set of

data standards and architecture, many aspects of MDO cannot be operationalized".

Die letzten beiden Handlungen, die in diesem Szenario geäußert werden, sind die Versorgung mit neuer Munition und das „Lernen" aus der Begegnung. Die Versorgung mit Munition ist Teil von Logistics, und zumindest das Erstellen einer Order (z.B. „Einheit X benötigt Y neue Raketen") ist maschinell sehr einfach umsetzbar (vgl. den Abschnitt zu Logistics). Der zweite Punkt allerdings – das Lernen – erscheint unrealistisch. Zum einen könnte sich die Vielzahl an unterschiedlichen Parametern, mit welchen die einzelnen Systeme angelernt werden müssen, als äußerst komplex und damit schwierig in der Praxis umsetzbar herausstellen. Zum anderen sind die Dinge, welche gelernt werden sollen, nicht notwendigerweise operationalisierbar, oder es stellen sich gewichtige ethische Probleme: Welche Kriterien sollen herangezogen werden, um den Erfolg bzw. Misserfolg dieser Auswahl zu operationalisieren? Ob das Ziel mit dem ersten Schuss bereits neutralisiert wurde? Über die Zeit, welche die Einheiten brauchten, sich in Position zu bringen? Dies sind relevante Fragen, die sich vor der eigentlichen Implementation stellen. Weiterhin gilt: Je komplexer diese Systeme werden, desto unberechenbarer ist der Lernprozess, sodass das System als Ganzes auch falsche Zusammenhänge lernen kann, die in bestimmten Situationen zu tödlichen Zwischenfällen führen könnten.

Als nächstes soll es um einen Auszug aus der „Unmanned Systems Integrated Roadmap 2017–2042" des Department of Defense gehen. Hier werden speziell Erwartungen an Machine Learning (ML) geäußert:

„ML is a rapidly growing field within AI that has massive potential to advance unmanned systems in a variety of areas, including: C2, navigation, perception (sensor intelligence and sensor fusion), obstacle detection and avoidance, swarm behavior and tactics, and human interaction. Deep learning, a promising form of artificial neural networks, can leverage the many cores of graphical processing units (GPUs), conventional CPUs and custom neuromorphic chips to learn patterns and models in data. AI and ML will allow the development of systems that are capable of learning and making high-quality decisions autonomously. This ability to learn will directly result in the development of unmanned systems with greater levels of autonomy, which will impart expanded and improved functionality. Furthermore, autonomous unmanned systems will vastly enhance battlespace awareness maximizing the utility of AI/ML-enabled decision aids that will revolutionize battlespace management and C2." (DoD 2017: 18)

Im ersten Teil dieses Abschnittes werden durchaus realistische Erwartungen geäußert – Navigation, Wahrnehmung und das Erkennen von Hindernissen werden zunehmend von Machine Learning-Systemen übernommen, wie Bestrebungen zum autonomen Fahren zeigen (vgl. Crowe 2019; Field 2020). Der zweite Teil des Abschnitts muss jedoch diskutiert werden. Das Department of Defense erklärt hier, dass ML es erlaube, Systeme zu entwickeln, welche „high-quality decisions autonomously" treffen können. Maschinelles Lernen funktioniert, indem eine Aufgabe – beispielsweise das Erkennen der Neutralisierung einer Flugabwehrstellung – als eine Funktion mit tausenden Variablen begriffen wird. Im Lernprozess ist das Ziel, für jede dieser Variablen einen Punkt zu finden, bei welchem die Wahrscheinlichkeit am höchsten ist, dass das vorgegebene Ziel korrekt erreicht wird. Es gibt allerdings keinen mathematisch exakten Weg, wie die besten Werte für all diese Variablen zweifelsfrei gefunden werden können, und daher kann es passieren, dass das Lernen im wortwörtlichen Sinne „über das Ziel hinausschießt" (vgl. Erz 2020: 34).

Dies hat zwei Implikationen. Erstens sortiert ein modellbasierter Klassifizierer in den meisten Fällen Daten in eine begrenzte Menge vorgegebener Kategorien. Das bedeutet, dass bereits bei der Programmierung des Klassifizierers klar

sein muss, was er erkennen kann, und was nicht. Sollten unvorhergesehene Situationen auftreten (Objekte, die nicht Teil des Trainingsdatensets waren und auch nicht adäquat durch eine der vorgegebenen Kategorien beschrieben werden können), wird der Klassifizierer zwar nach wie vor Wahrscheinlichkeiten für bestimmte Kategorien ausgeben, doch je nachdem, wie anders die Situation ist, können diese Werte nicht sinnvoll interpretiert werden (vgl. hierzu Erz 2020: 33, Abb. 2). Dies führt zur zweiten Implikation: Ein solcher Klassifizierer gibt immer mehrere Wahrscheinlichkeiten aus und es gibt keine Garantie, dass das korrekte Objekt auch mit der höchsten Wahrscheinlichkeit versehen wird. Das ist besonders problematisch wenn die Systeme wirklich autonom werden sollen, denn Autonomie impliziert mindestens zwei Systeme. Zum einen wird ein solcher Klassifizierer benötigt, welcher Bild- oder andere Sensordaten klassifiziert. Dessen Ergebnisse müssen dann allerdings an ein Steuersystem weitergegeben werden, welches auf dieser Grundlage entscheidet, wie sich das System verhalten soll. Wenn die korrekte Kategorie nicht auf Platz 1 der Wahrscheinlichkeiten liegt, sondern nur auf Platz 3, würde das Steuersystem auf Grundlage der falschen Kategorie auf Platz 1 handeln und somit falsche Entscheidungen treffen.

4.1.2 Situational Awareness

Militärische Situational Awareness hat zwei Elemente: Zum einen das Erfassen der Umwelt, wie sie sich im Einsatzgebiet darstellt, und zum anderen ein gewisses vorhersagendes Element, welches mittels Analyse einschätzen soll, wie sich die so wahrgenommene Umwelt in der Zukunft darstellen wird. Hier spielen eine Reihe von technischen Kategorien eine Rolle. Zunächst ist die Sensorik wichtig, da automatisierte Computersysteme nur mittels Sensoren Informationen über die Umwelt sammeln können. Diese Daten müssen dann weiterverarbeitet, also analysiert werden, damit auf der Grundlage dieser Analyseergebnisse Prognosen gebildet werden können. Zweitens spielt also die Kategorie der Datenprozessierung eine Rolle. Die dritte Kategorie, welche hier eine Rolle spielt, sind die eingebetteten Systeme, da nur diese gemäß der Definition aus dem technischen Research Report mit Sensoren ausgestattet Daten in einem Einsatzgebiet sammeln (Erz 2020: 23). Zuletzt spielt die Kategorie Kommunikation für Situational Awareness eine Rolle, da unabhängig davon, ob die gesammelten Sensordaten bereits auf dem eingebetteten System verarbeitet werden können, oder nicht, Daten von der Plattform an C2-Stützpunkte übermittelt werden müssen (ebd.: 26).

Eine Fähigkeit, welche von militärischen Akteuren an Sensoren und unbemannte Plattformen herangetragen wird, ist die von Modularität und Skalierung. In einem Konzeptpapier der U.S. Army von 2017 wird an mehreren Stellen die Entwicklung eines modularen, skalierbaren Sensor-Netzwerks erwähnt, welche für das Verbessern von Situational Awareness unumgänglich sei (U.S. Army 2017a: 10). Die dort deutlich werdenden, zu erwartenden Fähigkeiten von Sensornetzwerken basieren sehr stark auf effektiver Kommunikation. Damit verbunden sind auch Erwartungen, in Zukunft auf die Sensornetzwerke verbündeter Kräfte zugreifen zu können, also Daten miteinander zu teilen. Insbesondere in Ermangelung neuer Sensoren sprechen die Autor*innen davon, bestehende Sensoren „kreativ“ zu nutzen – so auch auf das Internet of Things (IoT) zuzugreifen:

„Creative use of available collectors may be the option until the Army develops new sensors. Access to the Internet of things will provide needed collection in urban areas. Terrestrial and aerial layer collection will leverage common platforms to expand the sensor network. Every radio is a potential signals intelligence receiver and every sight is a potential imagery collector

in a mesh network. Using the network as a sensor requires common standards and automated reporting from non-intelligence sensors, and significantly improves situational awareness. Coalition partner collection may be uniquely capable of satisfying specific requirements in their home environment." (U.S. Army 2017a: 28)

In diesem Abschnitt wird deutlich, dass auf alle vorhandenen Sensoren (RADAR, LiDAR, Kameras, Infrarotsensoren und HSIs) zugegriffen werden soll, was vor allem durch „common standards and automated reporting" ermöglicht werden soll. Dies wird im Anschluss mit Nachdruck bestärkt:

„The sensor computing environment will establish and enforce standards to create the conditions for an integrated and interoperable sensor operating environment. The computing environment will transfer information regarding sensor data, sensor management, and collected information seamlessly to collection managers, decision makers, command posts, and other networked sensors. […] Separate systems for managing Army resources, joint and national resources, and coalition partner resources are unacceptable." (U.S. Army 2017a: 28)

Aus dieser Fähigkeitsbeschreibung gehen zwei Ansprüche an Sensor-Netzwerke hervor: Erstens sollen Sensoren modular und skalierbar sein, was kleine Plattformen impliziert, die dezentral eingesetzt werden können. Zweitens sollen diese Sensoren miteinander verschaltet werden und mittels gemeinsamen Standards kommunizieren. Im Research Report des naturwissenschaftlichen-technisch-Projektteils wurde herausgestellt, dass es vom Kommunikationsweg der eingesetzten Sensorplattformen abhängt, wie viele Daten transferiert werden können. Gängige taktische Datenlinks (TDL) können bis zu einem Megabit pro Sekunde übertragen (Erz 2020: 27 f.), was für einen Videostream in ausreichender Qualität (Schmitt et al. 2016) ausreicht. Nur kann die vollständige Bandbreite nicht genutzt werden, weil über die gleichen Kommunikationskanäle zusätzlich Steuerbefehle an die unbemannten Fahrzeuge gesendet werden müssen. Das US-Militär verwendet daher für Videostreams nicht die sicheren taktischen Datenlinks sondern Satellitenkommunikation (Erz 2020: 27). Die nötige Bandbreite ließe sich aber auch durch stärkere Vor-Verarbeitung der Sensordaten auf der Plattform reduzieren, da nicht mehr die Roh-Daten übermittelt werden müssten, sondern bereits erste Analyseergebnisse. Folglich kann die geäußerte Erwartung als realistisch betrachtet werden, allerdings auf Kosten der Sicherheit: Je mehr Daten übertragen werden müssen, desto unsicherer sind die Kanäle.

Auch an Künstliche Intelligenz werden explizite Erwartungen herangetragen. In einem Absatz aus dem „National Artificial Intelligence Research and Development Strategic Plan" von 2019 heißt es:

„Perception begins with (possibly distributed) sensor data, which comes in diverse modalities and forms, such as the status of the system itself or information about the environment. Sensor data are processed and fused, often along with a priori knowledge and models, to extract information relevant to the AI system's task such as geometric features, attributes, location, and velocity. Integrated data from perception forms situational awareness to provide AI systems with the comprehensive knowledge and a model of the state of the world necessary to plan and execute tasks effectively and safely. AI systems would greatly benefit from advancements in hardware and algorithms to enable more robust and reliable perception. Sensors must be able to capture data at longer distances, with higher resolution, and in real time. Perception systems need to be able to integrate data from a variety of sensors and other sources, including the computational cloud, to determine what the AI system is currently perceiving and to allow the prediction of future states. Detection, classification, identification, and recognition of objects remain challenging, especially under cluttered and dynamic conditions. In addition, perception

of humans must be greatly improved by using an appropriate combination of sensors and algorithms, so that AI systems can work more effectively with people." (White House 2019a: 10)

Hier werden mit Bezug auf die Situational Awareness von KI-Systemen mehrere Erwartungen geäußert. Erstens würden KI-Systeme von besserer Hardware und Algorithmen profitieren. Nicht nur beweist Googles Tensor Processing Unit die Möglichkeit, neue, spezielle Chips für bestimmte Aufgabengebiete zu designen (Sato et al. 2017), sondern auch die Algorithmen der modellbasierten Klassifizierer werden kontinuierlich weiterentwickelt und dabei immer schneller und genauer (z.B. Redmon und Farhadi 2016; Loquercio et al. 2018). Weiterhin wird erwartet, dass Sensoren über höhere Distanzen höher aufgelöste Daten in Echtzeit aufnehmen. Während an einigen Sensoren aktiv gearbeitet wird, so an Hyperspektral-Imagern und optischen Kameras, verharren Infrarotkameras seit Jahrzehnten auf einer alten, geringen Auflösung (vgl. Erz 2020: 18). Nichtsdestotrotz erscheint es als durchaus realistisch, dass auch hier Verbesserungen möglich sind – nur wird an ihnen bislang nach dem bisherigen Kenntnisstand des Projektes nicht aktiv geforscht. Die Aussage, dass Sensoren allerdings Daten in Echtzeit aufnehmen können sollten, erscheint unscharf formuliert. Denn die meisten Sensoren sind problemlos in der Lage, Echtzeitdaten zu generieren und selbst die meisten Algorithmen, abgesehen von modellbasierten Klassifizierern, arbeiten bereits in Echtzeit. Die dritte Erwartung ist, dass die besprochenen KI-Systeme zur Sensordatenintegration in der Lage sein sollten, d.h. gesammelte Daten von verschiedensten Sensoren und KI-Systemen miteinander zu verbinden. Diese Erwartung ist unspezifisch, doch mit entsprechenden, konkreten Zielsetzungen während der Implementation (z.B. „Smart Goals") erscheint es zumindest möglich, ein entsprechendes System zu gestalten. Fraglich bliebe, bis zu welchem Komplexitätsgrad ein solches Tool eingesetzt werden könnte, da selbst große KI-Systeme bislang hauptsächlich mit einfach lesbaren Datenpunkten arbeiten (bspw. die Computersysteme von Technologiekonzernen wie Google oder Facebook) und über flächendeckende Integration von Kamera- Hyperspektral- und Radardaten in einem einzigen System nichts bekannt ist.

Eine zweite „vignette" von Spencer et al. (2019: 6 f.) befasst sich etwas näher mit der oben bereits angedeuteten Notwendigkeit der Verschaltung zahlreicher Einheiten zur Verbesserung der Situational Awareness. Die generelle Idee hinter „Cooperative Sensing" (Spencer et al. 2019: 6) ist dabei, dass mehr Sensoren auch mehr wahrnehmen und es somit einfacher wird, Bewegungen im Einsatzgebiet nachzuvollziehen sowie schneller zu reagieren. Generell werden in der „vignette" zwei Erwartungen geäußert: Standardisierung der Kommunikation zwischen verschiedenen Systemen sowie generell eine größere Abdeckung mit Sensorik. Technisch betrachtet werden hier also vor allem Datenprozessierung sowie Sensorik gefordert. Die Autor*innen stellen sich den Ablauf eines Zielerfassungs-Szenarios wie folgt vor: Zunächst sollen ein Gebiet beobachtet und mittels Datenverarbeitung an Bord eingebetteter Systeme (wie z.B. Satelliten) potenzielle Ziele entdeckt werden. Wird ein Fund gemeldet, sollen weitere Systeme die Daten des Satelliten mit einer „published prioritized target list" verglichen werden, um die Wichtigkeit des Zieles bestimmen zu können. Im Anschluss werden Sensoren allociert, um das vermutete Ziel weiter zu beobachten, bis die Wahrscheinlichkeit der korrekten Identifizierung einen bestimmten Schwellwert überschreitet und das Ziel dann ausgeschaltet wird. In der Erkennung des Zieles lassen sich mehrere Technologien identifizieren: Zunächst, wie auch bei vielen anderen analysierten Textstellen ist Kommunikation relevant, aber auch eingebettete Systeme sowie Datenprozessierung. Insbesondere die Formulierung „Additional Layer II AI solutions compare this data with the published prioritized target list" (Spencer et al. 2019: 6 f.) weckt Assoziationen zu Hyperspektral-Imagern (HSI), denn Zielerkennung auf Bil-

dern von HSI-Sensoren erfolgt, indem erkannte Spektren mit einer Datenbank abgeglichen werden, um zu bestimmen, was sich derzeit im Bild befindet. Insbesondere 2017 wurden zahlreiche Paper veröffentlicht, in welchen derartige Zielerfassungsalgorithmen für HSI-Bilder vorgestellt wurden, sodass die Möglichkeit der Erkennung von Zielen mittels satellitengestützten HSIs realistisch ist (vgl. z.B. Kang et al. 2017, Taghipour und Ghassemian 2017; Adão et al. 2017, Zhao et al. 2017; für einen Überblick Erz 2020: 31). Sie erfordern zwar höhere Prozessionsleistung, doch aufgrund der Tatsache, dass diese bereits in Afghanistan auf Drohnen verwendet wurden, um Sprengstofffallen zu finden (Knight 2019) und seit mindestens 2004 für die Entfernung von Landminen eingesetzt werden (Erz 2020: 19), erscheint es bereits heute als Realität, dass solche Algorithmen Verwendung finden.

4.1.3 Early Warning

Während die Situational Awareness im Generellen darauf Bezug nimmt, dass die Situation im jeweiligen Einsatzgebiet möglichst vollständig bekannt sein soll, bezieht sich Early Warning im Speziellen darauf, dass aufgrund der Datenlage Gefahrenlagen frühzeitig erkannt werden sollen. Für Early Warning werden meist integrierte Systeme verwendet. Dies liegt daran, dass für die Frühwarnung zwei Aufgaben erfüllt werden müssen: die Warnung vor herannahenden Gefahren sowie die Abwehr ebendieser Gefahren. Ein Beispiel für ein Early Warning Szenario ist Raketenabwehr, wofür meist ein integriertes System aus zwei eingebetteten Systemen verwendet wird: Radarsysteme sowie Raketenabwehr. So äußert sich beispielsweise das U.S.-amerikanische Verteidigungsministerium wie folgt:

„The BMD Sensors Program contributes to regional missile defense through the development, delivery and deployment/redeployment of Army Navy/Transportable Radar Surveillance and Control (AN/TPY-2) radars for operations or tests. AN/TPY-2 radars can be configured to operate either as a THAAD Fire Unit Radar (terminal mode) or Forward-Based Radar. These radars are transportable, they add flexibility to respond to geographical changes in threats. Radars provide early warning tracking and discrimination data through all phases of missile flight. Through the BMDS C2BMC and coalition data links, the AN/TPY-2 provides fire control data to enable remote Standard Missile (SM)-3 engagements by Aegis BMD, and to cue deployed THAAD and U.S. and partner Patriot batteries." (DoD 2019a: 2)

Hier werden softwaregestützte Fähigkeiten geäußert, die bereits Realität sind. Das angesprochene AN/TPY-2-Radar von Raytheon ist ein sogenanntes Synthetic Aperture Radar (SAR, vgl. Erz 2020: 22), welches laut Raytheon in zwei Modi betrieben werden kann: „Terminal Mode" sowie „Forward-Based Radar". Hinter diesen Begriffen verbergen sich zwei Arten, mit den Radarsignalen umzugehen. Der „Terminal Mode" bezieht sich auf die Radarfähigkeit zur „terminal illumination", bei welcher gestartete Abwehr-Raketen (beispielsweise die im Text angesprochenen PATRIOT Boden-Luft-Raketen) in ihrer Zielfindung unterstützt werden, indem das avisierte Ziel mit Radarfeuer „angestrahlt" wird, sodass die Sensoren auf der Rakete einfacher zum Ziel finden. Während dieser Zeit ist es allerdings nicht möglich, die Radardaten auszuwerten und weitere Ziele zu finden, was im zweiten Modus, dem „Forward-Based Radar" geschieht. Laut Raytheon ist das Radar präzise genug, auch ballistische Raketen zu lokalisieren. Während das Radar immer nur in einer der Konfigurationen betrieben werden kann, ist es durchaus denkbar, dass das Umschalten zwischen diesen Modi sehr schnell vonstattengehen kann, und spätestens seit 1996 (vgl. Huizing und Bloemen 1996) gibt es auch entsprechende Algorithmen, die ein effizientes Umschalten von Radareinheiten innerhalb von Sekundenbruchteilen ermöglichen.

Diese Zeit ließe sich theoretisch durch die Etablierung eines MIMO-Radar-Systems (Multiple-In-Multiple-Out, d.h. schlicht mehrere Radarsysteme, vgl. Fishler et al. 2004) weiter minimieren, wenn ein AN/TPY-2 ständig im „Terminal Mode" und ein anderes ständig im „Forward-Based Mode" gefahren wird. Entsprechende Algorithmen zur Aufgabenverteilung sind bereits seit den 1970er Jahren in den AEGIS-Systemen der U.S. Navy im Einsatz und können damit als realistisch gelten (vgl. Erz 2020: 24, Kimmel 2009).

Wo bei Situational Awareness zunächst nur Daten gesammelt werden und anschließend nach und nach ausgewertet werden können, verlangen die Anforderungen des Early Warning, dass diese Datenauswertung besonders schnell geschieht und zudem bereits Einschätzungen abliefern solle – das heißt, hier genügt nicht die Information „an diesen Koordinaten bewegt sich ein Objekt", sondern im Idealfall wird bereits die Information mitgeliefert, wie gefährlich dieses Objekt sein könnte und ob das System reagieren sollte. In zwei Textstellen wird diesbezüglich die Erwartung an KI gestellt, dass diese in die Lage gebracht werden soll, aus den immensen Datenmengen der Situational Awareness diejenigen Datenpunkte zu extrahieren, die relevant für Entscheidungen zu Defensivmaßnahmen sind.

„These machines would be used for indications and warnings in cyber defense, electronic warfare attacks and large-density missile raids when human reactions just aren't fast enough. They would also be used for big-data analytics; for example, a deep-learning system might be able to analyze 90,000 Facebook post made by ISIL in one day, crunch that data and find patterns from it, pulling out what might be of use." (DoDLive o.J.)

In dieser Textstelle wird die Erwartung geäußert, dass KI in der Lage sein soll, Textnachrichten bzw. im Generellen Social Media-Daten auszuwerten. Dies wird bereits heute praktiziert und ist soweit realistisch. Mittels Natural Language Processing (NLP) können neuronale Netzwerke (modellbasierte Klassifizierer) in die Lage versetzt werden, natürliche Sprache zu analysieren; mit dem NLTK (Natuaral Language ToolKit) gibt es beispielsweise schon seit Langem eine Reihe von Werkzeugen, Text mit der Programmiersprache Python zu analysieren. Der unrealistische bzw. schwammige Teil dieser Erwartung schwingt in der Aussage „pulling out what might be of use" mit. Kein Computerprogramm kann arbiträr „interessante" Daten extrahieren, denn diese Fähigkeit benötigt das, was umgangssprachlich mit „Bauchgefühl" oder Erfahrung umschrieben wird. Bei Early Warning scheitern die Erwartungen der Akteure also vor allen Dingen an der nicht vorhandenen Interpretationsfähigkeit von Computersystemen. Während das Lokalisieren von Objekten genauso wie das Analysieren von Daten mittels modellbasierter Klassifizierer bereits jetzt schon möglich und mittelfristig auch großflächig einsetzbar zu sein scheinen, wird ohne operationalisierte Parameter kein Computersystem in der Lage sein, abstrakte Konzepte wie „Gefährlichkeit" oder „verdächtiges Verhalten" einzuschätzen.

4.1.4 Security

Die vierte sozialwissenschaftliche Kategorie beschreibt einen speziellen Fokus auf die körperliche Unversehrtheit von Soldat*innen im Feld. Gewissermaßen geht es im Bereich Safety & Security um die Kombination von Situational Awareness und Early Warning spezifisch für Soldat*innen, die sich außerhalb von C2-Infrastruktur im Feld bewegen.

Fundamental ist für Sicherheit natürlich das frühzeitige Erkennen von Gefahren. Dies äußert sich bei der U.S. Army (2017b: 15) in folgender Fähigkeitenbeschreibung:

„RAS contribute to AWfCs 13 [Conduct Wide Area Security] and 15 [Conduct Joint Combined Arms Maneuver] by conducting persistent sur-

veillance of enemy avenues of approach, terrain denial with anti-armor robotic platforms, and targeting data collection to support indirect and direct fires. RAS provide units and teams with protection and standoff from IEDs and other explosives through detection, diagnostics, identification, neutralization, and render-safe capabilities. RAS support operations to enhance friendly force freedom of action, shape terrain, and control enemy movement."

Hier wird die Erwartung geäußert, dass beispielsweise IEDs (Improvised Explosive Devices, also improvisierte Sprengsätze) mittels RAS (Robotic Autonomous Systems) erkannt und entschärft werden sollen. Dies ist eine sehr realistische Einschätzung, hat doch bereits das Militär bestätigt, dass das Erkennen solcher Sprengsätze mit HSIs in Afghanistan erfolgreich praktiziert wurde (Knight 2019).

Eine weitere Fähigkeit, die in einigen der recherchierten Dokumente zur Sprache kommt, ist, dass einer der Vorteile von Künstlicher Intelligenz die Entlastung von Soldat*innen im Feld sei. Der avisierte Nutzen dieser Entlastung sei, dass die Soldat*innen besser geschützt werden – einerseits, weil sie sich mehr auf die wichtigen Aufgaben konzentrieren könnten, und andererseits, da so im Generellen weniger Soldat*innen in gefährliche Situationen gebracht werden.

KI könne, so das DoD (2018), helfen, die Ausrüstung zu warten, generell operationelle Kosten zu reduzieren und die Bereitschaft zu steigern. Zusätzlich könne die Verbesserung militärischer Wahrnehmung und Präzision zu weniger zivilen Toden und Kollateralschäden führen. Während letztere Erwartung von einem analytischen Standpunkt zu unspezifisch ist, sind vor allem die Erwartungen verbesserter Wartung und der Kostenreduktion durch Computersysteme durchaus realistisch. Es hat sich bereits mehrfach gezeigt, dass neuronale Netzwerke teilweise besser als menschliche Akteure sind, kleinste Anzeichen von Problemen zu erkennen – vor allem in der Krebsforschung konnte nachgewiesen werden, dass modellbasierte Klassifizierer schneller und effizienter sind, Schäden am Gewebe zu erkennen. Somit ist es denkbar, dass diese Fähigkeit auch auf militärisches Equipment anwendbar ist.

4.1.5 Logistics

Logistik ist ein weiteres, wichtiges Feld in welchem das Militär konkrete Erwartungen an Künstliche Intelligenz und Software stellt. Dieses Feld stellt einen Kernpunkt für militärischen Nachschub dar. Die logistischen Unterstützungssysteme für Multi-Domain-Operations (MDO) müssen dabei besondere Erwartungen erfüllen, die sich in kommerziellen Kontexten nur eingeschränkt stellen. So schreiben Spencer et al. (2019: 7):

„The MDO supply chain originates from the continental United States, extends to the deep maneuver area, and must remain responsive and agile to support operations. To enable this supply chain, MDO requires logistic operations enabled by predictive analytics to analyze historical and current data to predict future requirements. The Joint Force requires resupply of supplies and equipment before the time of need, transforming resupply operations from reactive or "just in time" to "ahead of time" logistics. Underpinning a dynamic and responsive chain is real-time data available to commanders and logisticians, accounting for the effects of operating while contested. AI/ML capabilities are required to enable precision logistics at the speeds and scales required for MDO."

Der Kern, wofür KI im Bereich Logistik hier gesehen wird, ist, Modelle zu generieren, mit welchen es möglich ist, nicht nur „just in time" Nachschub an die richtigen Stellen zu bringen, sondern sogar „ahead of time". Zu diesem Zwecke, so schreiben sie, würden Echtzeit-Daten benötigt, mit

welchen Künstliche Intelligenz dann entsprechende Vorschläge machen könne – und zwar „at the speeds and scales required for MDO". Hierbei handelt es sich nicht nur um eine sehr realistische Erwartung an KI, sondern sogar um das Kernthema von KI: Optimierungsprobleme (Russell et al. 2010: 120 ff.): Wie können die eingehenden Nachschub-Anfragen so zusammengefasst werden, dass mit möglichst wenigen Fahrten bzw. Flügen möglichst viel Material auf einmal ins Einsatzgebiet verbracht werden kann?

Um Nachschub aus einem Lager zu einer Einheit zu bringen, ist im Generellen keine KI vonnöten. Eine einfache „if"-Abfrage genügt: Wenn eine Einheit Nachschub anfragt könnte dieser Algorithmus überprüfen, dass der benötigte Gegenstand, z.B. Munition, im Lager in der ausreichenden Menge vorhanden ist, und den Fahrer*innen der Transportfahrzeuge die Order mitgeben, diese an die anfragende Einheit zu liefern. Ist nicht genügend vorhanden, ließe sich eine Fehlermeldung generieren, sodass die anfragende Einheit weiß, dass kein Nachschub mehr vorhanden ist. Bei hunderten parallelen Anfragen, die gemäß einiger Erwartungen mit Bezug auf Command & Control zunehmend automatisiert, also mit noch größerer Geschwindigkeit stattfinden sollen, aber würde dieser Algorithmus sehr schnell an Grenzen stoßen. Wenn die Anfragen schlicht in eine Warteschlange eingereiht werden und eine nach der anderen abgearbeitet wird, würde es in komplexen Umgebungen schnell zu Engpässen kommen: Einige Fahrzeuge würden fast leer zu einzelnen Zielen fahren, andere wären schwer beladen.

Und genau um dieses Optimierungsproblem dreht sich Machine Learning. Die Grundannahme zahlreicher Machine Learning-Ansätze ist, dass sich das zu lösende Problem als eine unbekannte Funktion darstellen lässt und das Ziel des Machine Learnings selbst ist es, einen Algorithmus die optimale Funktion (genauer: Werte für bis zu mehrere Millionen Variablen) zur Lösung des Problems finden zu lassen (vgl. zur Veranschaulichung besonders Russell et al. 2010: 121, Abb. 4.1). Viele vor allem iterative Ansätze des Machine Learnings (d.h. Ansätze, die sich schrittweise einer Lösung annähern) von genetischen Algorithmen (Russell et al. 2010: 126 ff.) bis hin zu klassischen modellbasierten Klassifizierern basieren genau auf dieser auch für die Logistik zentralen Grundannahme, dass es eine optimale Art gibt, viele Eingabewerte (Anfragen) geschickt in Ausgabewerte (Bestellungen für die Fahrer*innen) umzuwandeln.

4.2. Interdisziplinäre Analyse II: Uneindeutige Künstliche Intelligenz

Künstliche Intelligenz ist das „Modewort der Digitalisierung" (Dukino 2019). Obwohl sich KI international immer deutlicher zu einem alle gesellschaftliche Teilbereiche übergreifenden technologischen Trend entwickelt, ist parallel dazu eine weitverbreitete Unklarheit über seinen Begriffsinhalt zu konstatieren. Mit anderen Worten wird die zunehmende Prominenz der KI als Schlüsseltechnologie gleichsam von einer abnehmenden Klarheit über den eigentlichen Begriffsinhalt begleitet. Dass der Diskurs über KI folglich durch konzeptionelle Unschärfen gekennzeichnet ist (vgl. Kühne 2020, Kap. 4) illustriert der Vergleich von Begrifflichkeiten, die im sicherheitspolitischen Diskurs verwendet werden mit technisch-naturwissenschaftlichen Ansätzen bzw. Definitionen aus den Computerwissenschaften, in denen der Begriff der KI entwickelt wurde (vgl. McCarthy et al. 1955).

Im technischen Diskurs fungiert KI als Begriff, um eine sowohl dem Feld der Computerwissenschaften zuzuordnende (Luger 2009: 1), als auch zwischen Ingenieurs- und Kognitionswissenschaft zu verortende Disziplin (Görtz et al. 2013: 1f.; vgl. Genesereht und Nilsson 1987: 1) zu bezeichnen. Es handelt sich insofern um die wohl umfassendste Möglichkeit der Bestimmung

von KI, nämlich als das, womit sich KI-Forscher*innen beschäftigen. Beispielhaft steht dafür die Definition von Luger (2009: 2, eigene Übersetzung), wonach KI „die Sammlung von Problemen und Methoden [bezeichnet], die von Forscher*innen auf dem Gebiet der Künstlichen Intelligenz untersucht werden." (vgl. in diesem Sinn auch Retti 1986: 1). KI wird danach nicht als ein Endprodukt oder spezifische Technologie verstanden, sondern als ein wissenschaftlicher Prozess, dessen Inhalt und Ziel sich gleichwohl weiter spezifizieren lassen. So wird sie weiter als ein Forschungsbereich definiert, der sich mit der Automatisierung von intelligentem Verhalten beschäftigt: „Künstliche Intelligenz (KI) kann als der Zweig der Informatik definiert werden, der sich mit der Automatisierung von intelligentem Verhalten beschäftigt" (Luger 2009: 1, vgl. auch Genesereht und Nilsson 1987: 1).

In lediglich vier von 31 Policy-Dokumenten, in denen KI-Bestimmungen vorgenommen werden, wird, wie im technischen Diskurs, KI als Wissenschaftsdisziplin bzw. Forschungsbereich definiert (Planungsamt 2013: 7; Amt für Heeresentwicklung 2019: 28; ODNI 2018: 13). Das Planungsamt der Bundeswehr (2013: 7) etwa bestimmt KI als jenen „Forschungsbereich, der sich mit der Nachbildung menschlicher Wahrnehmung und menschlichen Handelns durch Maschinen beschäftigt." Mit diesem Fokus auf der Nachbildung menschlichen Handelns sieht es KI gleichwohl nicht auf die Computer-Wissenschaft beschränkt, sondern erweitert das Forschungsfeld mit Neurologie und Psychologie auf die grundsätzliche Erforschung menschlicher Denkprozesse (ebd.).

Zentral ist in der Mehrheit der Dokumente hingegen die Definition von KI als technisches System bzw. ihre Bestimmung entlang der Befähigungen, die mit KI ausgestattete Systeme erhalten sollen. Hierzu gehören etwa Handlungen wie Mustererkennung, Erfahrungslernen, das Ziehen von Schlussfolgerungen und/oder Vorhersagen selbsttätig durchzuführen (DoD 2019b: 44). Dominiert im sicherheitspolitischen Diskurs dieser Bezug zu den Befähigungen menschlicher Intelligenz, zeigt sich die Spezifizierung der KI-Definitionen abhängig von der Art der Dokumente: Je weitreichender das Dokument, wie etwa nationale KI-Strategien, desto umfassender, aber gleich auch vager erweisen sich die Bestimmungen. Es zeigen sich aber auch Länderunterschiede: In den für den deutschen und russischen Diskurs untersuchten Dokumenten dominiert ein Verständnis von KI als einer Simulation menschenähnlichen Handelns (Office of the Russian Federation 2019: 4, BMBF 2018: 4) bzw. der Simulation von intelligentem Verhalten (Planungsamt Bundeswehr 2013: 7). Typisch für den amerikanischen Diskurs ist demgegenüber, dass in den untersuchten Dokumenten der Hoffnung Ausdruck verliehen wird, mittels KI Maschinen befreit von menschlichem Einfluss zu autonomem Handeln zu befähigen (115th Congress 2017: 3f., U.S Army 2017b: 3). Damit geht einher, dass, anders als im technischen Diskurs, diese sicherheitspolitischen Definitionen stark von menschlichen Analogien gekennzeichnet sind. Dieser Anthropomorphismus, d.h. die Vermenschlichung von KI, illustriert sich in Bestimmungen, wonach mit KI ausgestattete Systeme ihre Umwelt wahrnehmen (OECD 2019), Muster erkennen (DoD 2018: 5; U.S. Air Force 2019; U.S. Army 2017b: 3), Voraussagen (OECD 2019; DoD 2018: 5, U.S. Air Force 2019; U.S. Army 2017b: 3) oder Entscheidungen treffen (OECD 2019; U.S. Army 2017b: 3) können. Hierbei handelt es sich um einen zentralen Unterschied zwischen den Diskursen, denn im technischen Diskurs ist die Auffassung zentral, dass Intelligenz zwar ein Fähigkeitsspektrum (von Maschinen)[9] beschreiben kann. Görtz et al. (2013: 1) z.B. bestimmen KI als Disziplin, die dem Ziel folgt, „Wahrnehmungs- und Verstandesleistung zu operationalisieren und durch Artefakte, kunstvoll gestaltete technische – insbesondere informationsverarbeitende – Systeme verfügbar zu machen" (ebd.). Allerdings impliziert diese

[9] Wobei dem menschlichen Gehirn kein Sonderstatus verliehen wird.

Definition, dass das Feld von KI dadurch charakterisiert ist, dass kognitive Prozesse durch Informationsverarbeitungsmodelle simuliert werden sollen (ebd.). Intelligenz wird folglich nicht als gegebene Entität verstanden, sondern mit Blick auf die Forschungsfelder als Spektrum unterschiedlicher Befähigungen. Was wiederum die Bedingungen von Intelligenz sind, ist danach eine noch umfassend zu beantwortende Forschungsfrage (vgl. Luger 2009: 2, Elish und Hwang 2016: 8) bzw. handelt es sich dabei lediglich um Modellannahmen, die wiederum durch wissenschaftliche Methoden im Feld der KI getestet werden (vgl. Görtz et al. 2013: 2, Luger 2019: 675).

Vor allem wird KI in allererster Linie als ein Ergebnis menschlicher Einwirkung verstanden (vgl. Barocas und Selbst 2016) und den Maschinen selbst keine menschlichen Eigenschaften zugeschrieben. Danach sind mit KI ausgestattete Systeme selbst nicht intelligent bzw. das zugrunde gelegte Maß an Intelligenz bemisst sich vielmehr an operationalisierbaren kognitiven Funktionen. Diese Bestimmung entspricht dem oben angeführten Verständnis einer Simulation von Intelligenz. Berücksichtigt ist damit, dass mit den Fähigkeiten von KI gleichwohl nur ein Ausschnitt dessen beschrieben ist, was, aus einer interaktionistischen Perspektive, d.h. dem Prozess der Zuschreibung von Intelligenz im menschlichen Handlungszusammenhang, entspricht (vgl. Görtz et al. 2013: 4; Elish und Hwang 2016: 9). Mit anderen Worten wird KI als Befähigung zur Problemlösung verstanden, die sich lediglich am menschlichen Problemlösungshandeln orientiert. Dies korrespondiert mit der Definition von McCarthy et al. (1955: 1), niedergelegt in einem Förderungsantrag an die Rockefeller-Stiftung, die als begrifflicher Ursprung von KI gilt. Demnach liegt KI beispielsweise dann vor, wenn Maschinen Dinge tun, für deren Ausführung man beim Menschen Intelligenz unterstellt, etwa kognitive Aufgaben wie wahrnehmen, schlussfolgern und handeln zu bewältigen bzw. Probleme zu lösen (vgl. Steinacker 1986: 10ff.; Winston 1993: 5), wobei sich die Grenzen des vorstellbar Machbaren immer auch verschieben.[10] Dennoch weiterhin wichtig erscheint daher der Hinweis der Autor*innen der Stanford-Studie (Stone et al. 2016: 12), wonach die Subsummierung jeder Tätigkeit eines Computers, die einmal vom Menschen ausgeführt wurde, unter den Begriff Intelligenz zwar eine ausreichende, aber, auch mit Blick auf die gegenwärtig bereits sehr hohe Rechenleistung bestimmter Systeme, keine notwendige Bedingung ist.

Diese Orientierung an menschlichem Problemlösungshandeln, die sich im Begriff der Simulation von Intelligenz konkretisiert, entspricht der Hypothese schwacher KI. Demgegenüber beschreibt die starke KI-Hypothese die Möglichkeit, dass Maschinen tatsächlich denken und nicht nur das Denken simulieren (Russel und Norvig 2016: 1020). Allerdings gilt diese Hypothese, „dass Bewusstseinsprozesse nichts anderes als Berechnungsprozesse sind“ (Görtz et al. 2013: 4), aufgrund der Unmöglichkeit, Befähigungen wie Kreativität oder Bewusstsein zu operationalisieren, als nicht verifizierbar (ebd.). Zwar umfassen heutige Leistungsbestandteile der KI aus technischer Sicht Aufgaben der Informationsverarbeitung in zunehmend komplexerem Ausmaß. Aber selbst das sogenannte Maschinenlernen, das zum Ziel hat, künstlich Wissen aus Erfahrung zu generieren, gilt, in Anlehnung an Erkenntnisse über die Wirkungsweise menschlicher Intelligenz, weiterhin als Herausforderung (Luger 2009: 28). Das Diffundieren von Vorstellungen echter Intelligenz und ihrer Simulation, mithin die Vermenschlichung der KI, die in den Zuschreibungen technischer Leistungsfähigkeit im sicherheitspolitischen Diskurs zu beobachten ist, sorgt dann nicht nur dafür, dass Unterscheidungen zwischen schwacher und starker KI verschwimmen. Mitunter domi-

[10] Russel und Norvig (2016: 2 f.) zufolge gehören hierzu mit Natürlicher Sprachverarbeitung, Wissensrepräsentation, Automatisiertem Schlussfolgern, Maschinellem Lernen, Bildverarbeitung oder Robotik sowohl Funktionen des Wahrnehmens (z.B. Spracherkennung) als auch des Verstehens (z.B. Maschinenlernen).

nieren Vorstellungen starker KI im sicherheitspolitischen Diskurs, was sich etwa darin zeigt, dass mit KI befähigten Systeme u.a. zugeschrieben wird, planen (115th Congress 2017: 3 f.), denken (ebd.) oder handeln (ebd.: 3 f.; DoD 2018: 5; 115th Congress 2017: 3 f.; U.S. Airforce 2019) zu können, womit eine weitestgehende Handlungsautonomie der entsprechend ausgestatteten Systeme unterstellt wird.

Diese Erwartungen und Zuschreibungen an KI sind jedoch als riskant auszuweisen, denn eine Vermenschlichung von KI verleitet dazu, Verantwortlichkeit von menschlichen Entscheidungen zu entkoppeln und problematische Erwartungen an eine Autonomie der Systeme zu entwickeln. Es ist insofern eine zentrale Perspektive des technischen Diskurses zu wiederholen, dass technisches Wirken, etwa durch Anwendung von Algorithmen, Intelligenz lediglich simuliert (vgl. Görtz et al. 2013: 1) und insbesondere, dass der Gestaltung der Systeme menschliche Entscheidungen zugrunde liegen (vgl. Barocas und Selbst 2016):

„Gerade dann, wenn sich die direkte Kontrolle über die Werkzeuge immer weiter verliert, müssen sich die Schöpfer autonomer Systeme fragen, wie kulturelle und ethische Vorannahmen künstlich intelligente Kreationen beeinflussen. Eine solche Selbstreflexion ist notwendiger denn je, denn das präzise und bewusste Design von Algorithmen in autonomen digitalen Systemen wird zu Reaktionen führen, die auf diesem Design basieren." (IEEE 2019: 36, eigene Übersetzung).

Unsere Ergebnisse unterstreichen, dass der Begriff KI mit seinem Wechsel in andere gesellschaftliche Felder Übersetzungsprozessen unterzogen wird. Diese haben, wie etwa Roberge et al. (2020: 2, mit Bezug etwa auf Callon 1984) konstatieren, zu seiner begrifflichen Ambiguität geführt. Sie, so deuten es unsere Untersuchungsergebnisse an, prägen dann auch die teils hohen Erwartungen an auf KI basierenden Technologien und nehmen schon heute Einfluss auf die sicherheitspolitische Debatte um Vorteile und Risiken der zukünftigen Kriegführung. Ist insofern eine Präzisierung des begrifflichen Instrumentariums zu fordern und zu fördern, dann aber nicht nur deshalb, weil bereits heute ein internationaler Wettlauf um die „weltweit führende Position bei den Technologien der Künstlichen Intelligenz (KI) […] begonnen [hat]" (Groth et al. 2019: 6). Weil die diffuse Verwendung der Begrifflichkeit nicht nur zu Missverständnissen, sondern gleichermaßen zu utopischen wie auch dystopischen Erwartungen führen kann, kann die Präzisierung zu einer Versachlichung etwa in der Debatte darüber führen, inwiefern das Ausmaß an technologisch bedingter Autonomie in Waffensystemen tatsächlich wächst bzw. wachsen sollte (für eine Übersicht vgl. Boulanin und Verbruggen 2017: 26).

Eine solche Reflexion der Begriffsverwendung kann dann auch dafür sensibilisieren, die den Technologien zugeschriebene Objektivität zu hinterfragen. Hierfür muss jedoch auch die Bedeutung von Daten – ihre Erfassung, Qualität und Risiken – berücksichtigt werden – ein Thema, das sich nicht nur in der naturwissenschaftlich-technischen Analyse als Dreh- und Angelpunkt erwiesen hat. Denn auch wenn in Bezug auf den Einsatz von z.B. Algorithmen suggeriert wird, dass auf Basis etwa entsprechender Datenanalysen vermeintlich objektive Entscheidungen ermöglicht werden, ist die Konstruktion des Algorithmus selbst von vorangehenden menschlichen Entscheidungen darüber abhängig, „welche Kriterien konkret mit welchem Gewicht berücksichtigt werden sollen" (Ernst 2017: 1029; vgl. ausführlich Orwat 2019; Barocas und Selbst 2016, Barocas et al. 2014).

4.3. Interdisziplinäre Analyse III: Künstliche Intelligenz und Daten

Der zunehmende militärische Bedeutungszuwachs von neuen Softwaretechnologien geht mit weitreichenden sicherheitspolitischen Konsequenzen einher. Vor allem Risiken, die sich durch die Automatisierung militärischer Prozeduren ergeben, sind regelmäßig Gegenstand von Auseinandersetzungen etwa um das Konzept der „Meaningful Human Control". Die Basis dieser Entwicklungen – Daten und die auf ihnen basierenden Methoden der Wissensgenerierung, wie z.B. das datengetriebene Maschinelle Lernen (ML) – sind jedoch nur selten Gegenstand der Debatte im Spannungsverhältnis von Militär und Softwaretechnologien im Allgemeinen und KI im Besonderen (vgl. für eine Übersicht Chavannes et al. 2020). Dabei fehlt es nicht an Hinweisen auf ihre hohe Relevanz und gefordert wird etwa, bei der Regulierung von LAWS bereits bei der Datengrundlage und den nichtletalen Grundaktivitäten wie Überwachung, Datenerfassung und Data Mining anzusetzen (vgl. z.B. Dahlmann und Dickow 2019: 13; Shoker 2019: 2). Ein solcher Diskurs über die Herkunft von Daten, ihre Verarbeitung und die mit ihnen verknüpften Risiken wird bislang vorrangig über zivile Anwendungen geführt (vgl. z.B. Orwat 2019; Deutscher Ethikrat 2017), kann aber gleichwohl für potenzielle Risiken computergestützter Methoden der Analyse und Verarbeitung von Daten im militärischen Kontext sensibilisieren. Sie sind Gegenstand der nachfolgenden Ausführungen, die zunächst einen Überblick über zentrale Begrifflichkeiten und Technologien innovativer Datenverarbeitungsmethoden geben, bevor dann zentrale Risiken ihrer Anwendung skizziert werden. Besprochen werden einerseits sowohl ethische als auch auf den Datenschutz bezogene Problemstellungen, die ihre Grundlage in kritischen Perspektiven auf die fortschreitende Digitalisierung und Datafizierung heutiger Gesellschaften finden. Ergeben sich Risiken danach mit Blick auf Ursprung, aber auch die Qualität der erhobenen Daten, dann gehen wir andererseits der Frage nach, mit wieviel Gewissheit sich eigentlich annehmen lässt, dass durch den Einsatz von Algorithmen bei der Datenprozessierung immer auch objektive Entscheidungen ermöglicht werden. Im Anschluss an diese Problematik, die in Gestalt von Bias oder Diskriminierungsrisiken virulent wird, richten wir zuletzt den Blick auf technische Vulnerabilitäten am Beispiel sogenannter „vergifteter" Daten.

4.3.1 Daten und ihre softwaretechnologische Verarbeitung

Im Rahmen der Digitalisierung stellen Daten eine wertvolle Ressource dar, werden häufig gar als binäres Gold bezeichnet (z.B. Lobe 2019, zu Daten als Kapital vgl. Sadowski 2019). In ihrer Wechselwirkung und im Zusammenspiel mit leistungsstarker IT-Hardware und einem stetig wachsenden mathematisch-analytischen Instrumentarium (Algorithmen etc.) sind Daten – in hinreichender Qualität und Quantität – eine essentielle Voraussetzung für fast jede moderne Softwareanwendung.

Letztendliches Ziel jeder Datenanalyse ist die Gewinnung verwertbarer neuer Informationen. Daten an sich können dabei in unterschiedlicher Form vorliegen; z.B. als Rohdaten, vorprozessierte Daten oder bereits analysierte Daten. Rohdaten, z.B. Fotos, Anwendungsprotokolle oder Sensordaten, müssen zumeist erstmal vorprozessiert werden, d.h. in ein für die weitere Datenverarbeitung und -analyse passendes Format gebracht werden. Der Umfang und Aufwand der Vorprozessierung hängt dabei stark von der Art der Daten und der sich anschließenden Datenanalyse ab.

Die Verarbeitung und Analyse von Daten kann anhand verschiedener computergestützter Me-

thoden erfolgen, die u.a. auf Algorithmen-basierten statistischen Verfahren, Organisationsprinzipien oder Handlungsregeln fußen. Als wichtige Methoden können hier Big Data Analyse, Data Mining oder Maschinelles Lernen genannt werden. Big Data Analytics wird zumeist als Sammelbegriff in den Datenwissenschaften verwendet und umschreibt die automatisierte Erfassung, Zusammenführung, Aufbereitung und Verwaltung sowie die Verarbeitung und Analyse von großen und unterschiedlichen Datenmengen. Die Daten können hierbei in einem hohen Maße heterogen sein, d.h. in unterschiedlichen Formaten oder Größen vorliegen (vgl. Barocas et al. 2014: 1 f.). Die Daten können in bereits strukturierter Form vorliegen, z.B. in Zeilen und Spalten sortiert, wie man sie in einer Standardtabelle vorfindet. Demgegenüber handelt es sich bei Sensordaten oder Fotografien um unstrukturierte Daten.

Beim Data-Mining geht es insbesondere darum, die Datenmenge großer und/oder unterschiedlicher Datensätze auf mögliche statistische Zusammenhänge hin zu untersuchen, mit dem Ziel, vorher nicht bekannte Muster, Korrelationen oder Kategorisierungen ausfindig zu machen, anhand derer sich übergeordnete, neue Erkenntnisse gewinnen und ggfs. sogar Modelle generieren lassen. Dieses buchstäbliche Schürfen oder Graben in Daten erfolgt durch Algorithmen, d.h. formal festgelegten Sequenzen logischer Operationen, die Schritt für Schritt Anweisungen für Computer liefern, um Daten zu bearbeiten und so Entscheidungen zu automatisieren (vgl. ebd.: 3).

Mit dem Begriff des Maschinellen Lernens (ML) werden algorithmische Verfahren umschrieben, anhand derer die Strukturen und Zusammenhänge aus Daten erfasst werden können (vgl. Tangermann 2019: 283 ff.). Die Besonderheit des ML liegt darin, dass vorab keine detaillierte Beschreibung oder Charakterisierung des Lerngegenstandes und der zugrundeliegenden Datenkorrelationen vorliegen muss, sondern der Algorithmus sich diese anhand eines möglichst umfangreichen und alle möglichen Facetten abbildenden Trainingsdatensatz selber erschließt. Der Algorithmus wird mit Beispielen von interessierenden Fällen konfrontiert. Auf diese Weise soll er lernen, welche verwandten Attribute als potenzielle Stellvertreter für Eigenschaften oder Ergebnisse dienen können, die für den Lerngegenstand von Interesse sind. Unterschieden werden kann zwischen angeleitetem bzw. überwachtem Lernen (der Mensch steuert während des Lernprozesses Wissen bei, z.B. durch das Labeln bzw. Kennzeichnen von Daten, oder greift etwa bei der Einordnung von Beispielen in Kategorien korrigierend ein) und nicht überwachtem Lernen. Für das korrekte Erkennen und Auswerten von Bildern etwa muss das System beim nicht überwachten Lernen mit qualitativ hochwertigen, passenden und vor allem ausreichenden Sätzen roher Beispieldaten trainiert werden, um zum Beispiel Strukturen und Unterschiede in den Daten finden zu können. Ihre Beschaffung gilt als schwer und kostspielig. Insbesondere in Hinblick auf die Ergründung nicht-linearer und sehr komplexer Zusammenhänge innerhalb von Datenstrukturen gewinnen sogenannte „tiefe neuronale Netzwerke" für das Maschinelle Lernen eine zunehmende Bedeutung (Deep Learning) (ebd.). Der maschinelle Lernprozess erfolgt hier über eine Vielzahl versteckter Ebenen (Layers), die jede für sich auf die Bestimmung individueller Charakteristika trainiert werden (Goodfellow et al. 2016). Beispielhafte Anwendungen für ML liegen heute im Bereich der Bilderkennung (z.B. Gesichtserkennung), der Übersetzung und Sprachverarbeitung oder betreffen Herausforderungen bei der Automatisierung und Optimierung maschineller Prozesse in komplexen Umgebungen, wie z.B. das autonome Fahren.

Eine eindeutige Abgrenzung von Data Mining, Big Data Analyse oder ML ist nicht möglich, vielmehr gibt es hier gemeinsame Schnittmengen. Auch taucht in diesem Zusammenhang immer häufiger der Begriff Künstliche Intelligenz auf, für deren Systeme Daten ein wichtiger Treiber sind, explizit auch für ihren Einsatz im militäri-

schen Sektor. Anschließend an die Befunde aus Kapitel 4.2, liegt mit dem Begriff gleichwohl eher eine Fähigkeitsbeschreibung denn eine Methode vor, die aber stark auf den vorherig genannten Verfahrensweisen beruht. KI soll sich durch Lernen und Training manifestieren und maschinell gestützte Handlungsempfehlungen und (Teil-)Entscheidungen möglich machen und essentielle Grundlage hierfür sind Daten in einer ausreichenden Quantität und Qualität.

4.3.2 Datenentgrenzung

In quantitativer Hinsicht wächst – analog zum kommerziellen Bereich – die Menge der den Sicherheitsbehörden und Verteidigungsministerien sowie den Geheimdiensten zur Verfügung stehenden Daten immer weiter an. So werden gegenwärtig mehr Daten erfasst, als es den vorrangigen Informationsanforderungen und -bedarfen im Moment der Datenerhebung entspricht. Diese Daten werden nicht nur im „Feld" generiert, sondern Big Data-Volumina ergeben sich auch daraus, dass das Militär in immer größerem Ausmaß Zugriff auf Daten aus teilweise öffentlich zugänglichen Quellen – z.B. zwischenbehördlichen, zwischenstaatlichen, industriellen und akademischen Einrichtungen – erhält (vgl. z.B. U.S. Army 2017a: 66) bzw. erhalten soll. Besonders militärisch bedeutsam sind Bild-, Video- oder anderes visuelles Material aus der Luft, vom Boden und unter Wasser, das der räumlichen Orientierung und Lokalisierung von Objekten oder Personen dient (die sogenannte Geospatial Intelligence, GEOINT)[11] sowie Daten aus öffentlich zugänglichen Quellen, vor allem dem Internet (die sogenannte Open Source Intelligence, OSINT). In diesem Zusammenhang gilt insbesondere die Datenverfügbarkeit bei großen Unternehmen sowohl aus wirtschaftlicher als auch aus sicherheitspolitischer Perspektive als ein zentraler strategischer Standortvorteil in der KI-F&E. Aufgrund schwacher Datenschutzauflagen und angesichts zahlreicher Kooperationen zwischen Industrie und Militär wird dieser Vorteil vor allem in China und den USA gesehen (EFI 2019: 31).[12]

Wie auch unsere Analyse ergab, bildet die beständige Akkumulation von Daten einen der zentralen Argumentationsanker im sicherheitspolitischen Diskurs und einen wesentlichen Ausgangspunkt für die Möglichkeit, das vielfach konstatierte „Wettrennen" um die KI-Vormachtstellung und Vorteile in der zukünftigen Kriegführung zu gewinnen. Erhalten Daten also ganz allgemein eine zunehmende militärische und sicherheitspolitische Relevanz, dann trägt ihr kontinuierliches Anwachsen das Risiko der Datenentgrenzung in sich. Denn angesichts der vielfachen nationalen Ambitionen, auch die Ergebnisse von ziviler KI-F&E in eine militärische Nutzung zu überführen (für eine Übersicht vgl. Kühne 2020), kann dies in Widerspruch zu gesetzlich verankerten Geboten der Datenminimierung und des Datenschutzes geraten. Im europäischen Kontext stünde dies im Widerspruch zur Datenschutzgrundverordnung (DSGVO), welche Datenminimierung vorschreibt. Aber auch im U.S.-amerikanischen Kontext selbst gilt es, vielfach in ökonomischer Hinsicht, als Akzeptabilitätsrisiko von KI (vgl. z.B. DHS 2017: iii), dass die Einführung von Softwaretechnologien mit der Erfassung einer wachsenden Menge an (personenbezogenen) Daten – vom Webverkehr bis hin zu Gesichts- und Spracherkennungsdaten – einhergeht. Das Risiko der Entgrenzung

[11] Die Datensammlung erfolgt hier vorwiegend über Satelliten, (unbemannte) Luft-, Boden und Unterwasserfahrzeuge oder andere Überwachungstechnologien.

[12] So wird im Kontext von GEOINT zum Beispiel für den U.S.-amerikanischen „space layer" angestrebt, eine Sensor-Umgebung zu realisieren, die aus einem Netzwerk nationaler Koalitions-, Service- und kommerzieller Einrichtungen besteht (EFI 2019: 46). Zu diesen gehört u.a. Maxar Technologies, die seit August 2019 für weitere vier Jahre unter Vertrag bei der U.S. National Geospatial-Intelligence Agency (NGA) stehend, mit ihrem DigitalGlobe System die U.S.-Regierung mit On-Demand verfügbarem, kommerziellem und hochauflösendem Bildmaterial versorgt, um die militärische Einsatzplanung und das Lagebewusstsein zu unterstützen. Die Software basiert auf rohen Sensordaten, die über Technologien wie WorldView, GeoEye und BuckEye gesammelt und mit nicht näher definierter „third-party data" ergänzt werden (businesswire 2019).

lässt sich dann auch darin identifizieren, dass personenbezogene Daten mit anderen Daten verknüpft werden können, ohne dass jedoch das Einverständnis der Betroffenen zu diesem Monitoring eingeholt wird. Weil durch die algorithmische Korrelation die Grenze zwischen personenbezogenen und nicht personenbezogenen Daten verschwimmt, können letztere zunehmend verwendet werden, um Personen später wieder zu identifizieren oder sensible Informationen über sie abzuleiten, die über das hinausgehen, was diese Personen ursprünglich wissentlich preisgegeben haben.

Wird in nationalen Sicherheitskontexten bereits seit 2001 geradezu ein „Überschuss" an Daten produziert, stellt dieser das Militär zunehmend vor das Problem einer sprichwörtlichen Datenflut (vgl. Amt für Heeresentwicklung 2019: 7; Zelaya und Keeley 2020; Porche et al. 2014: 3). Diese forciert geradezu den Einsatz von „Big Data basierte[n] Verfahren zur Verdichtung von Information und KI-Verfahren zur Erkennung von besonders kritischen oder relevanten Mustern" (Amt für Heeresentwicklung 2019: 7), einerseits um die schiere Quantität des Datenaufkommens zu bewältigen. Andererseits wird in diesen heterogenen Datenmengen ein enormes Wissenspotential vermutet (vgl. z.B. Motta et al. 2007) und mehr oder weniger ‚fraglos' davon ausgegangen, dass diese Informationen von strategischer Bedeutung sein könnten und KI basierte softwaretechnologische Ansätze und algorithmische Entscheidungssysteme die notwendige Verlässlichkeit aufweisen, diese zu analysieren.

Rechtliche und sicherheitspolitische Bedenken lassen sich auch vor dem Hintergrund formulieren, dass KI neben Datensätzen auch algorithmische Modelle benötigt, um einen Output zu erzeugen und bei der Bereitstellung von diesen Modellen vermehrt industriell-militärisch Kooperationen angestrebt werden.[13] Mit anderen Worten liefern Industrieunternehmen nicht nur zunehmend militärisch genutzte Informationen. Sie sollen vielfach auch die Instrumente zur Verwaltung und Auswertung der exponentiell wachsenden Datenbestände bereitstellen (vgl. z.B. Keller 2018), um so, wie etwa auch auf der Fachtagung der NATO 2018 (vgl. Bell et al. 2018: 11) diskutiert, das eingangs skizzierte Problem des Auswertungsrückstandes militärischer Datenbestände zu bearbeiten. Hier wird ein Regulierungsbedarf konstatiert und etwa eine Lücke in den Ansätzen zur Behandlung des geistigen Eigentums von Daten, den Modellen und den Ergebnissen von KI-Anwendungen ausgemacht (vgl. Sheppard et al. 2018) – eine Problematik, die ihren Widerhall dann auch in der Debatte um die Verantwortlichkeit beim Einsatz von KI-Verfahren durch öffentliche Institutionen, deren Softwarelösungen wiederum durch die Industrie bereitgestellt werden, findet.[14]

Die Gemengelage von gesellschaftlicher Kontrolle und wirtschaftlicher Bemühungen im Kontext zunehmender Datensammlungsbestrebungen ist insofern kritisch zu bewerten. Allerdings stoßen bei den zugrundeliegenden Entwicklungen, wie etwa Big Data, vorhandene Regulierungsbemühungen gegenwärtig „klar an Grenzen", wie etwa der Deutsche Ethikrat (2017: 257) konstatiert. Auch Lösungsansätze, wie z.B. jene der Teilhaberechte an Daten (ebd.: 244f.), erweisen sich als begrenzt und Regulierungen scheitern etwa bei Allgemeingut-Daten, d.h. bei Daten, deren Eigentumsrecht gemeinsam von einer Gruppe (z.B. Facebook, Google oder Amazon) gehalten wird und die andere vom Zugang, der Verwaltung und der Nutzung aus-, bestimmte Gruppen jedoch einschließen kann (vgl. Prainsack 2019: 3f.).

---

[13] Ein Beispiel ist etwa die U.S.-amerikanische „Mercury Challenge", die unter der Schirmherrschaft U.S.-amerikanischer Geheimdienste 2018 ins Leben gerufen wurde, um in Zusammenarbeit mit verschiedenen Akteuren aus dem privatwirtschaftlichen sowie universitären Bereich Methoden für die kontinuierliche, automatisierte Analyse ausländischer nachrichtendienstlicher Daten zu entwickeln (vgl. IARPA 2018). Prominestes Beispiel für Neuerungen bei der Beschaffung von Softwaretechnologien, bzw. die hohe militärische Bedeutung von Big Data und militärisch-ziviler Kooperationen bei ihrer Auswertung, bleibt die Zusammenarbeit von Google mit dem U.S.-amerikanischen Verteidigungsministerium im Projekt Maven bzw. die Kontroverse um seine Fortsetzung (vgl. Boland 2017).

[14] In Deutschland etwa liegt die Verantwortlichkeit für ein Verarbeitungsverfahren gem. Art. 5 Nr. 7 Datenschutz-Grundverordnung (DSGVO) bei dem Akteur, der über Zwecke und Mittel der Datenverarbeitung entscheidet.

4.3.3 Qualität von Trainingsdaten

Für KI-Methoden und -verfahren ist eine große Anzahl von Trainingsdaten die Grundlage und ihre letztendliche Leistungsfähigkeit ermisst sich daran, wie umfassend und genau diese Daten sind. Daher muss ein Algorithmus allen relevanten Variablen – etwa Ziele oder Varianten im Betriebsumfeld – ausgesetzt werden, mit denen dieser am Ende umgehen soll. Für eine hinreichend große Stichprobe an Daten für Anwendungen des Maschinenlernens genügen im militärischen Setting nicht allein Variablen aus dem Grundbetrieb, sondern es müssen auch realistische, im militärischen Einsatz generierte Daten herangezogen werden. Militärische Einsatzfelder sind allerdings nicht per se datenreiche Bereiche (Sheppard et al. 2018: 8), sondern viele operative Umgebungen zeichnen sich geradezu durch eine „Datenarmut" aus. In der Folge können solche für das Maschinenlernen probate Daten, trotz des regelmäßig konstatierten Datenüberflusses, nicht immer im hinreichenden Maß im Feld erhoben und aufgezeichnet werden. Konstatiert wird ein Mangel an Trainingsdaten und dies insbesondere für die Entwicklung von Zielerfassungsalgorithmen (Boulanin und Verbruggen 2017: 25), für die das Training und der Test an einer großen Stichprobe von Daten, die mit dem Einsatzszenario zusammenhängen, allerdings notwendig ist. Diese Datenarmut nimmt Einfluss auf die Möglichkeiten des Maschinellen Lernens und etwa auch auf den Betrieb von Systemen, die zukünftig weitestgehend autonom agieren sollen (vgl. Sayler und Hoadley 2019). Einigen gilt Datensimulation daher als schnelle, kostengünstige und sichere Alternative zum Testen eines ML-Systems für den militärischen Anwendungsfall (ebd.). Gegen die Anwendung von Simulationstrainings wird jedoch eingewendet, dass die Validität des ML-Systems aufgrund eines Trade-off zwischen der eigentlich notwendigen Genauigkeit des Systems und dem überhaupt möglichen Realitätsgrad des Simulationstrainings leidet (Song et al. 2015: 6; Motta et al. 2007: 176). Aufgrund fehlender Daten, etwa Kenntnissen über meteorologische Variablen, Informationen über Art und Ablaufs eines feindlichen Angriffs oder über die eigenen und feindlichen Waffen- und Abwehrsystemeigenschaften ließe sich kein authentisches Simulationsumfeld generieren (Motta et al. ebd.), deren Ergebnisse auf den Einsatz im Feld übertragbar wären. Die Problematik besteht, mit anderen Worten, darin, dass es sich beim Einsatz von aus militärischen Simulationen gewonnenen Trainingsdaten immer um konkrete raumzeitliche, d.h. lediglich auf das Simulationsumfeld bezogene, Daten handelt. Entsprechend können bei der Anwendung von aus Simulationen gewonnen Daten und auf ihrer Basis entwickelte Algorithmen fundamentale Änderungen der realen Daten-Zusammenhänge zumeist nicht einfach kompensiert werden, sondern erfordern einen neuerlichen Lernprozess anhand neuer oder zumindest ergänzender Trainingsdaten. Es gilt daher als besondere Herausforderung Modelle zu generieren, die allgemein genug sind, um auf andere Daten übertragbar zu sein und gleichzeitig in der jeweiligen Anwendung eine möglichst geringe Fehlerquote zu erzielen. Bislang führt ML jedoch vor allem zu sehr spezialisiertem Wissen und Datenerfahrung, die sich überwiegend nicht „verallgemeinern" und auf andersgeartete Daten oder Probleme übertragen lassen (vgl. Danks und London 2017: 4692 f.). Insofern führen unvollständige oder nicht repräsentative Trainingsdaten zu erlerntem Wissen, dessen reale Anwendung fehlerhafte Schlussfolgerungen nach sich ziehen würde. Aufgrund einer geringen Übertragbarkeit oder Anpassungsfähigkeit von so trainierten KI-Systemen können folglich Fehler bzw. der sogenannte Training-Data-Bias (ebd.) auftreten – ein Risiko, dass etwa auch dann besteht, wenn Systeme, die in einer zivilen Umgebung entwickelt und trainiert wurden, in einer Kampfumgebung eingesetzt werden (Scharre 2017).

4.3.4 Systematische Fehler

Für Anwendungen des Maschinellen Lernens haben Daten einen großen Einfluss auf den Wert und die Qualität der Ausgabe des generierten Wissens. Mit anderen Worten ist nicht nur die Menge an Trainingsdaten mitentscheidend für die Güte von KI-Anwendungen, sondern auch die Qualität der Daten selbst, die in den verschiedenen Phasen der Datenverarbeitung Anwendung finden. In dieses softwaretechnologische „Spiel mit den Daten“[15] (Lehr und Ohm 2017) können auch Verzerrungen eingeführt werden. Denn trotz der Stärke von KI-Systemen, große Datenmengen auswerten und darin Muster und Zusammenhänge selbstständig erlernen zu können, besteht eine zentrale Herausforderung auch darin, systematische Fehler bei der Datenverarbeitung zu erkennen und diesen vorzubeugen. In der Informatik ist dies durch das gängige Sprichwort „Garbage in – garbage out“ („Müll rein – Müll raus“) simplifiziert.

Systematische Fehler oder Verzerrungen beim ML können in unterschiedlicher Weise entstehen, etwa wenn Programmierer*innen für ein Data-Mining-Modell die Ausgabevariablen des Algorithmus in einer Weise trainieren, dass Mitglieder bestimmter demografischer Gruppen mit größerer Wahrscheinlichkeit von den vorherzusagenden Ergebnissen betroffen sind (Barocas und Selbst 2016: 677 ff.). Zu einer solchen, sogenannten Stichproben-Voreingenommenheit kommt es, wenn der Trainings-Datensatz mehrheitlich nur einen bestimmten Teil der Bevölkerung (etwa hellhäutige Menschen oder Männer) umfasst, während ein anderer Teil unterrepräsentiert ist (etwa dunkelhäutige Menschen oder Frauen). Aus einer solchen verzerrten Stichprobe werden dann Rückschlüsse gezogen, die zu einer systematischen Benachteiligung der im Training gleichermaßen systematisch unterrepräsentierten Gruppen führen könnten.

Data Mining kann auch Diskriminierungsmuster reproduzieren. In technischer Hinsicht kann dies als sogenannte historische Verzerrung sichtbar werden, etwa dann, wenn ein Algorithmus anhand eines alten Datensatzes trainiert wird, der auf vergangenen Werten und Moralvorstellungen basiert (vgl. Angwin et al. 2016; Barocas und Selbst 2016: 720ff.) bzw. durch die Auswahl spezifischer Variablen, mit denen ein Konstrukt gemessen werden soll. Hierfür müssen häufig Ersatzinformationen herangezogen werden. Diese sollen zwar repräsentativ für die Eigenschaften, z.B. für menschliches Verhalten, stehen. Sie sind jedoch das Ergebnis interpretativer Leistungen und die Auswahl dieser Variablen kann diskriminierende Effekte haben. Von einer eindeutigen algorithmenbasierten Diskriminierung lässt sich dann sprechen, wenn „sie eine ungerechtfertigte Benachteiligung von Personen darstellen, die durch geschützte Merkmale (insbesondere Alter, Geschlecht, ethnische Herkunft, Religion, sexuelle Orientierung oder Behinderung) gekennzeichnet sind“ (Orwat 2019: xii). Beispiele aus dem zivilen Bereich illustrieren diese Problematik. Zum Beispiel kann die Bestimmung eines „guten Mitarbeiters“, erfasst über die Dauer von Betriebszugehörigkeiten, Frauen etwa angesichts ihrer ggfs. höheren Wechselraten, systematisch benachteiligen (ebd.: 78), oder wie im Fall des Unternehmens Amazon, diese im Rahmen eines Rekrutierungsprogramm diskriminieren.[16] Angwin et al. (2016) zeigten überdies für COMPAS, ein in den USA verwendetes datenbasiertes Risikobewertung-Programm zur Prognose künftiger Delinquenz von Straffälligen, dass eine algorithmenbasierte Diskriminierung auch dann auftreten kann, wenn auf die Erfassung ge-

[15] Lehr und Ohm verweisen mit dieser Metapher auf die verschiedenen Phasen der Datenverarbeitung mit dem Ziel, mittels KI automatisierte Entscheidungsfindungsprozesse zu etablieren. Sie betonen damit die menschlichen Einflüsse auf den Designprozess von KI und Maschinellem Lernen und insofern die möglichen Risiken, die bei der Anwendung von KI und ML berücksichtig werden müssen.

[16] Das 2018 eingestellte Programm, das einen automatisierten Auswahlprozess vorliegender Bewerbungen gewährleisten sollte, hatte, basierend auf seinen Trainingsdaten, u.a. dem Fakt, dass in IT-Unternehmen, wie auch bei Amazon, mehr Männer als Frauen arbeiten, weibliche Kandidaten als minderwertiger identifiziert (Der Standard 2018, zum Genderbias von Googles Ad Posting-Algorithmus vgl. Datta et al. 2015).

schützter Merkmale oder Konstrukte wie Rasse verzichtet wird. Dass ihrer Analyse zufolge in COMPAS erfasste Afroamerikaner*innen ein höheres Rückfallrisiko attestiert wurde als weißen Amerikaner*innen, lässt sich auf die Messung des Konstrukts Rückfallwahrscheinlichkeit selbst zurückführen. Als Datengrundlage dienten Charakteristika individueller sozialer Lagen – Merkmale, die zwischen weißen und afroamerikanischen erfassten Straftäter*innen große Unterschiede aufwiesen. Zu dieser algorithmenbasierten mittelbaren Diskriminierung (vgl. Barocas und Selbst 2016: 720ff.) kam es folglich, weil sich auf dieser Datenbasis Kriminalisierungsrisiken durch stereotype Vorstellungen über den Zusammenhang von sozialer Ungleichheit und Delinquenz fortsetzten, indem aus den Merkmalen individueller sozialer Lagen kriminovalente Faktoren abgeleitet wurden – mit weitreichenden Konsequenzen für die entlang dieser Kriterien Beurteilten. Dieses Beispiel veranschaulicht dann auch, dass Daten selbst nie „einfach da" und neutral sind, ihre (automatisierte) Verarbeitung gleichsam aber entscheidende Folgen haben kann.

Ein systematischer Bias wird auch bei Systemen der Stimmungs- und Meinungsanalyse festgestellt (Orwat 2019: 74 mit Bezug auf Kiritchenko und Mohammed 2018), schlägt jedoch am eindrücklichsten im Bereich der Personen- und Gesichtserkennung durch. Bilderkennungsprogramme übertreffen zwar die durchschnittlichen menschlichen Fähigkeiten. Sie müssen jedoch mit einer großen Menge von bereits klassifizierten Bildern trainiert werden, d.h. sie benötigen Bilder, in denen bereits ein bestimmtes Objekt identifiziert ist. Fehler können entstehen, wenn Trainingsdaten falsch gekennzeichnet werden oder lassen sich auf eine mangelnde Diversität der Bilder zurückführen, an denen die Systeme trainiert wurden (vgl. Boulamwini und Gebru 2018). Die Herausforderungen für die Validität von Gesichtserkennungssystemen zeigen sich auch mit Bezug auf Kontextfaktoren wie Lichtverhältnisse oder Hintergrund der zu erkennenden Subjekte. Auch variiert ihre Erkennungsleistung bei der Personenerkennung mit unterschiedlichen Gesichtsausdrücken (ebd.: 11f.), d.h. in Bezug auf Faktoren, die wiederum kennzeichnend sind für Situationen der realen Welt. Aufgrund der Eigenschaft, berührungslos Identitäten suchen und verifizieren zu können, gilt Gesichtserkennung einigen zwar schon als effiziente und effektive Sicherheitsmethode für den militärischen Anwendungsbereich, etwa um Kombattant*innen und Zivilist*innen in militärischen Überwachungsbildern zu unterscheiden (vgl. z.B. White House 2019b: 15). Vor dem Hintergrund der bis hierhin skizzierten Risiken lässt sich aber anzweifeln, dass Algorithmen bereits hinreichend gut und fehlerfrei trainiert sind – oder vielleicht jemals sein werden –, um diese Unterscheidung tatsächlich vornehmen zu können (vgl. Shoker 2019), nicht zuletzt, weil diese Identifizierung mitunter unter datenarmen oder herausfordernden Bedingungen stattfinden kann. Sie können zur Folge haben, dass Zielbilder z.B. unscharf sind oder unter schlechten Lichtbedingungen aufgenommen werden (vgl. Abadicio 2020). Daher besteht das Risiko, dass sich systematische Verzerrungen, mit potenziell fatalen Folgen, in den Ergebnissen niederschlagen können.

4.3.5 „Vergiftete" Daten

Überdies gelten Softwaretechnologien als Risiko für neue Arten von Schwachstellen. KI-Algorithmen sind nicht nur anfällig für Verzerrungen, sondern auch für Manipulationen, wenn Trainingsdatensätze nicht angemessen kuratiert oder geschützt sind. So könnten auch neue Einfallstore für Cyberattacken geschaffen werden, die auf die Trainingsdaten von maschinellen Lernsystemen abzielen. Dieses sogenannte Data Poisoning bezeichnet z.B. Situationen, in denen falsche Daten in den Trainingspool eines Machine Learning Modells eingeschleust werden, um

es so dazu zu bringen, etwas zu lernen, was es ursprünglich nicht lernen sollte. Poisoning-Angriffe, die das Modells beeinflussen, zielen folglich darauf ab, eine bestimmte Menge an falschen Daten in das System zu injizieren. Die häufigste Folge davon ist, dass Daten mit falschen Labels versehen werden (Moisejevs 2019). Insbesondere Datenbanken für Gesichtserkennung sind anfällig für diese Form des Data Poisoning. So haben Forscher nachgewiesen, dass jemand mit Zugang zu den Trainingsdaten eines Bildklassifikators, diesem Daten aussetzen könnte, die der Klassifikator systematisch falsch kategorisieren würde – ein Sensor dann am Ende etwa einen Freund fälschlicherweise als Feind oder als überhaupt nicht vorhanden erkennt (Allen und Chan 2017: 25). Aber bereits das Hinzufügen einer kleinen Störung, wie etwa eine Veränderung einiger bereits gelabelter Daten, kann Bildklassifizierungsmodelle täuschen (OECD 2019: 94). In einer zweiten Variante handelt es sich beim Data Poisining um Angriffe, die die Integrität des Modells negativ beeinflussen. Zum Beispiel trainierten Forscher an der New York University das neuronale Netz eines autonomen Autos mit Bilddaten eines Stoppschilds, das mit einer gelben Post-it-Notiz versehen wurde. In der Folge wurde es stattdessen als Geschwindigkeitsbegrenzungsschild klassifiziert (vgl. Barnett 2020). Diese auch als „Backdoor Attacks" bezeichneten Angriffe könnten dafür sorgen, dass Militärs mit einer nicht ‚vertrauenswürdigen' KI arbeiten bzw. können sie dazu führen, einen Algorithmus funktionsunfähig zu machen, wenn er ein bestimmtes Bild oder einen „Auslöser" sieht.

4.3.6 Schlussfolgerungen

Daten spielen für KI-Systeme in der Anwendung, beim Testen, vor allem aber beim Training eine zentrale Rolle, d.h. maschinell lernende bzw. angelernte Systeme benötigen für ihre Funktion selbst eine große Menge an Trainingsdaten, was gesellschaftlich relevante Auswirkungen haben kann. Zudem können technische Engpässe im Verhältnis militärischer Datenerfassung und -verarbeitung sowie der Anwendung des Maschinellen Lernens die vermeintliche Stärke und Genauigkeit der eingesetzten Technologien ebenso beeinflussen wie kognitive Verzerrungen, Vorurteile oder Manipulationen der Daten, die beim Training von Algorithmen zur Anwendung kommen. Fehler, das zeigt unsere Betrachtung, können dabei in allen Phasen der computerbasierten Datenverarbeitung und -analyse entstehen. Sie haben nicht nur erhebliche Auswirkungen, sondern algorithmische Verzerrungen und Fehler können sich schnell ausbreiten, wenn Entwickler*innen für unterschiedliche Anwendungen die gleichen verzerrten Datensätze zur Erstellung ihrer Algorithmen verwenden. In Kombination mit der Inventionskraft des Militärs können sie, insbesondere wenn solche Verzerrungen und Manipulationen unentdeckt bleiben und in entscheidungsunterstützende oder Systeme mit tödlicher Wirkung eingebaut werden, verheerende Folgen haben. Insofern ist das Versprechen von einer Objektivität der Technologien riskant, denn „algorithmische Verfahren [können] ihr Funktionieren nicht selbst beweisen, sondern nur performativ zur Schau stellen." (Burkhardt 2017: 59). Die im zivilen Diskurs heute schon diskutierten Risiken liefern damit zahlreiche und gewichtige Gründe dafür, zum einen für menschliche Einflussmöglichkeiten und damit auch Fehler im Designprozess von KI und ML zu sensibilisieren sowie menschliche Kontrollmöglichkeiten in der Anwendung der mit ihnen ausgestatteten Technologien zu erhalten (Lehr und Ohm 2017: 657f.). Zum anderen bedarf es, wie etwa von Zweig et al. (2018: 29 ff.) ausgeführt, konkreter Lösungsansätze, die die skizzierten Risiken direkt adressieren, sei es die Etablierung von Prüfmechanismen wie eines „Algorithmen-TÜVs", einer „Berufsethik für den Beruf des Data Scientist" oder Monitoring-Verfahren, die die Angemessenheit und Kontrolle von Algorithmen und ihrer Anwendung bewerten.

5. Eine Einordnung der Ergebnisse, die Schlussfolgerungen und eine abschließende interdisziplinäre Betrachtung

In diesem Kapitel nehmen wir einerseits eine Einordnung und Beurteilung der Forschungs- und Analyseergebnisse des Forschungsprojektes vor. Andererseits diskutieren wir in einer abschließenden interdisziplinären Betrachtung die friedens- und sicherheitspolitischen Risiken um den militärischen Einsatz von Softwaretechnologien und die Notwendigkeit einer Regulierung. Dies bietet sowohl der Öffentlichkeit als auch Entscheidungsträger*innen eine Handreiche, die zu einem besseren Verständnis der Thematik führt, den weiteren Forschungsbedarf hervorhebt und aus der Handlungsoptionen für die politische Praxis unmittelbar abgeleitet werden können.

5.1 Einordnung der Forschungs- und Analyseergebnisse in Hinblick auf die Forschungsleitfragen

Das einjährige Forschungsprojekt mit seinem dezidiert explorativen Charakter orientierte sich in seiner Forschungs- und Analysearbeit an drei breit gefassten Leitfragen, die jeweils wichtige disziplinäre (Frage 1 und 2) und interdisziplinäre (Frage 3) Forschungsfragen thematisieren. Im Folgenden behandeln wir in Kürze, inwiefern diese mit den vorliegenden Forschungs- und Analyseergebnissen – auch anteilig – beantwortet werden konnten und insbesondere, welche Fragen nach wie vor einer Klärung bedürfen oder sich neu ergeben haben.

Frage 1. Welches Spektrum an Fähigkeiten, Anwendungsbereichen und Technologietrends (u.a. Automatisierung, Vernetzung und KI) resultiert aus der heutigen software-technologischen Forschung und Entwicklung (F&E) und welche militärisch relevanten Potenziale lassen sich aus technischer Sicht hieraus ableiten?

Die Untersuchung dieser Fragestellung wurde exemplarisch am Anwendungsbeispiel der militärischen Informationsgewinnung durchgeführt. Hierfür wurden fünf Kategorien relevanter (Software)Technologien betrachtet – Sensorik, Kommunikation, die Besonderheiten von eingebetteten und integrierten Systemen, Datenprozessierung/-analyse und die Datenspeicherung. Es zeigte sich hier, dass das Militär bereits auf die heute fortschrittlichsten Technologien zurückgreift und seinen Fähigkeitsbereich erweitert hat, sich im Rahmen der betrachteten Anwendung aber auch zahlreiche Einschränkungen ergeben. So kann z.B. die Analyse von komplexem Bildmaterial bisher nicht „an Bord" der eingebetteten Systeme selber erfolgen, sondern wird nach wie vor von Analyst*innen und/oder ortsgebundenen Computersystemen durchgeführt. Einen wesentlichen „Flaschenhals" stellen heute auch die Kommunikationsverbindungen dar, sodass bei der Datenübertragung häufig eine Abwägung zwischen Datengeschwindigkeit und -sicherheit getroffen werden muss. Die fortlaufende Technologieentwicklung und Investitionen in die Infrastruktur werden aber die dafür notwendige Rechen- und Übertragungskapazitäten wahrscheinlich merklich erhöhen.

Aus der durchgeführten Untersuchung lässt sich allerdings nur ein grober Eindruck dieser Entwicklungen innerhalb der nächsten Jahre abzeichnen, denn insgesamt konnten die technologisch-orientierten Forschungsfragen so lediglich für den kurz- bis mittelfristigen Zeithorizont und auch nur teilweise beantwortet werden. Eine Hauptschwierigkeit bestand darin, auf Basis der heutigen Grundlagenforschung einerseits den mittel- bis langfristigen Fortschritt der Forschung im Bereich der Softwaretechnologien zu antizipieren. Andererseits ergab sich die

Herausforderung, vom kurz-, mittel- oder langfristigen Forschungstand auf zukünftige militärische Anwendungspotentiale schließen zu können. Das Forschungsprojekt war insofern auch mit dem Grundproblem konfrontiert, dass je weiter der Blick in die Zukunft geht, sich diese Vorhersage umso unschärfer gestaltet. Was die langfristigen Fähigkeiten, Anwendungsbereiche und Technologietrends in Hinblick auf Softwaretechnologien betrifft, blieben dann auch alle recherchierten naturwissenschaftlich-technischen Veröffentlichungen vage. Daneben musste festgestellt werden, dass es bislang praktisch keine internationalen Publikationen gibt, die eine belastbare Analyse software-technologischer F&E hinsichtlich ihrer mittel- bis langfristigen militärischen Anwendungspotentiale beinhalten und dabei über die bloße Nennung allgemeiner Anwendungsfelder wie KI, Robotik etc. hinausgehen. Um eine solche Analyse durchführen und Rückschlüsse ziehen zu können, scheint insbesondere ein tiefgehendes Fachwissen in verschiedenen softwaretechnologischen Forschungsgebieten und zugleich ein anwendungsorientiertes Verständnis zukünftiger militärischer Erfordernisse Voraussetzung dafür zu sein, sich solcherart zukunftsorientierten Abschätzungen anzunähern. Aufgrund dieser Komplexität, aber auch zeitlicher Limitierungen und begrenzt zur Verfügung stehender externer Fachexpertise, konzentrierte sich der Forschungsfokus daher nur auf die heutige software-technologische Forschung und Entwicklung (F&E), die als Basis einer Untersuchung der kurz- bis mittelfristigen militärischen Anwendungspotentiale von Softwaretechnologien diente. Dabei ist die hier durchgeführte Untersuchung, bei der vor allem die Sensordatenprozessierung und -analyse im Vordergrund stand, ein anschauliches Fallbeispiel und ein guter Anfang. Der Einsatz von Softwaretechnologien in militärischen Bereichen wie z.B. szenariengestützter Prognosen, der Command & Control sowie der Entscheidungsfindung gestaltet sich überwiegend noch komplexer und undurchschaubarer, die sich hier abzeichnenden Trends und technologischen Fähigkeiten sind daher schwieriger abzusehen und wurden noch nicht aus einer naturwissenschaftlich-technischen Perspektive untersucht.

Wichtige perspektivische Fragen bleiben daher noch weitgehend unbeantwortet. Dazu gehört insbesondere jene danach, wie die langfristige Forschung und Entwicklung im Bereich der Softwaretechnologien aussehen wird und welche neuen Anwendungsbereiche sich hierdurch eröffnen. Aber auch Antworten auf die Frage, welche Potentiale sich durch die zivile Entwicklung immer komplexerer Algorithmen und neuer Ansätze von Maschinellem Lernen ergeben werden, bedarf Antworten, ebenso wie die Frage, in welche Richtung sich die Forschung um Künstliche Intelligenz perspektivisch entwickeln wird. Wesentlich ist dabei vor allem aber, welche militärischen Anwendungsszenarien aus technologischer Sicht dadurch langfristig denkbar sein werden. Die Bearbeitung dieser Forschungsfragen wird eine kontinuierliche und gewiss Jahre überdauernde Aufgabe sein. Eine solche zukunftsorientierte technologische Trendanalyse – das ist eine unmittelbare Erfahrung dieses explorativen Forschungsprojekts – kann nur erfolgreich sein, wenn hierfür über einen interdisziplinären Ansatz sowohl die beste aktuelle software-technologische Fachexpertise (Grundlagenforschung und anwendungsorientierte Entwicklung), der gegenwärtige sicherheitspolitische Diskurs und die perspektivische strategische militärische Planung berücksichtigt werden. Nur über einen solchen intensiven und andauernden interdisziplinären Expert*innenaustausch wird sich ermessen lassen, welche militärisch relevanten Potenziale sich aus naturwissenschaftlich-technischer Sicht aus der gegenwärtigen F&E in Zukunft ableiten lassen werden.

Frage 2. In welchem Umfang spielen Technologietrends im internationalen sicherheitspolitischen Diskurs heute eine Rolle und welche waffentechnischen Adaptionen werden diesbezüglich thematisiert? Welche Erwartungen hinsichtlich der militärischen Potenziale hegen relevan-

te staatliche Schlüsselakteure und welchen Einfluss auf die Kriegführung und internationale Sicherheit messen diese ihnen bei?

Die Ergebnisse des sozialwissenschaftlichen Forschungsteils illustrieren, dass die Entwicklungsfortschritte in den Informationstechnologien stark in alle gesellschaftlichen Felder und auch in militärische Anwendungsbereiche hineinwirken. Es zeigte sich, dass insbesondere das Forschungsfeld der Künstlichen Intelligenz in jüngerer Zeit im Mittelpunkt nationaler sowie explizit militärischer Forschungspläne steht und daher zu erwarten ist, dass KI auch zukünftig eine zentrale Rolle im Wettbewerb der Nationen spielen wird. So deutet sich im Diskurs der untersuchten Akteure eine Dynamik an, wonach von einer Aufrüstungsspirale im Hinblick auf die Ausstattung mit neuen Softwaretechnologien auszugehen ist. Insofern konnte mit der Untersuchung ein allgemeiner Trend identifiziert werden, der mit der Heuristik eines allumfassenden Nutzens von KI, der zivile und militärische Anwendungspotentiale miteinander verbinden soll, einhergeht. Danach wird KI als unabwendbare Entwicklung gerahmt, was wiederum ein entsprechendes Engagement der Akteure begründet. Unterstrichen wird dies durch teils hohe Investitionsleistungen der Länder in das Forschungsfeld und das Bemühen sowohl in wirtschaftlicher Hinsicht von KI-Anwendungen zu profitieren, als auch im Bereich der Militärtechnik an die Fortschritte in F&E in KI anderer sicherheitspolitischer Schlüsselstaaten anzuschließen. Die Problematik des Dual-use-Charakters der Technologie erweist sich hierfür geradezu als zentrale Begründungslogik, denn alle untersuchten Länder setzen auf Übertragungseffekte, mit denen Vorteile sowohl im zivilen als auch im militärischen Sektor verbunden werden. Allerdings waren weitergehende Aussagen über spezifische Entwicklungstrends einerseits dadurch schwer zu treffen, da Informationen über entsprechende waffentechnische Adaptionen teils mit einem hohen Grad an Geheimhaltung einhergehen. Andererseits war eine systematische Einordnung des Engagements einzelner Akteure dadurch erschwert, dass bislang kein vollständiger Datensatz über F&E in KI vorliegt, der auch einen detaillierten quantitativen Vergleich verschiedener Staaten zulässt. Eine Vervollständigung und Systematisierung dieser Daten muss daher weiter angestrebt werden.

Die Erwartungen staatlicher Schlüsselakteure wurden entlang sechs zentraler, sich teils überlappender, Argumentationsmuster aufgeschlüsselt. Sie geben Auskunft über Begründungen für die Notwendigkeit einer Integration von KI in militärische Anwendungsfelder und bilden erste Indikatoren, um Aussagen über den potentiellen Einfluss von Softwaretechnologien auf die Kriegführung und die internationale Sicherheit zu treffen. Im Feld der Ausübung von militärischer Command & Control soll KI zur größtmöglichen Vernetzung von Daten und Systemverbünden eingesetzt werden, mit dem Ziel die Prozesse der Datenerfassung und -verarbeitung zunehmend zu automatisieren, um auf diese Weise schneller zu Entscheidungen zu gelangen. Ihre Implementation soll auch dazu dienen, frühzeitig Indizien für eine Vielzahl von Risiken zu entdecken und so das Lagebewusstsein (Situational Awareness) zu erhöhen, sowie, in taktischer Hinsicht, die Wirksamkeit der Raketenabwehr und Zielerkennung und/oder Flugbahnberechnung für eine verbesserte Frühwarnung (Early Warning) zu verbessern. Wird insofern erwartet, durch automatisierte Datenerfassung und -verarbeitung risikoarme Situationen zu schaffen, ist der Schutz der körperlichen Integrität (Security) der Soldat*innen ein weiteres zentrales Argument für den Einsatz von KI. Für alle Felder ist der vermehrte Einsatz automatisiert bzw. autonom agierender Maschinen vorgesehen. Deren Vorteile werden auch für die Verbesserung der militärischen Logistik im Besonderen gesehen sowie im Allgemeinen darin, die Geschwindigkeit und Agilität im Einsatz durch die Bildung von Teams aus Mensch und Maschine (Teaming) zu erhöhen. Insofern soll sich, so die Erwartungen, mit der avisierten Autonomie der Fokus auf eine facettenreiche Kooperation verlagern, sowohl was die Planungs- und Operateursebene betrifft, als

auch im Kampfgeschehen. KI-Systeme sollen folglich in vielen verschiedenen Rollen auf dem gesamten Schlachtfeld eingesetzt werden. Vielfach ist geplant, sie nicht nur in einer einzelnen Waffe, sondern in viele andere militärische Systeme zu integrieren: KI soll erstens bei der Verarbeitung und Interpretation von Informationen helfen. Erwartet wird zweitens, dass sie neue Formen der Kommandoführung ermöglicht, in dem die operativen Systeme in die Lage versetzt werden, große Datenmengen zu analysieren und Vorhersagen zu treffen, um auf diese Weise menschliche Aktionen zu lenken. Drittens soll sie dazu eingesetzt werden, um physische Objekte so zu steuern, dass sie ohne menschliche Aufsicht agieren.

Aufgrund der sich im Diskurs abzeichnenden Initiativen, Automatisierung und Autonomie von militärischen Systemen voranzutreiben, illustriert sich erneut die Relevanz dieser Konzepte und vor allem die Notwendigkeit, sie weiter diskursiv zu spezifizieren, um die damit einhergehenden Risiken abschätzen zu können.

Frage 3. In welchem Maße decken sich aktuelle softwaretechnologische Entwicklungen mit den im Diskurs identifizierten Erwartungshaltungen an die militärischen Potenziale von Technologietrends? Welche gemeinsame Schnittmenge hinsichtlich Definitionen, Fähigkeiten sowie militärischen Anwendungen bestehen und wie könnten Arbeitsdefinitionen aussehen? Wie ließe sich das Verständnis um den Einfluss von Softwaretechnologien auf die moderne Kriegführung und resultierende sicherheitspolitische Implikationen vertiefen?

Die interdisziplinären Analysen im Rahmen dieses Forschungsvorhabens konnten sich, wie zuvor unter Frage 1 ausgeführt, nur auf eingeschränkte naturwissenschaftliche-technische Forschungsergebnisse zu den kurz- bis mittelfristigen softwaretechnologischen Forschungs- und Entwicklungstrends stützen. Im Rahmen der durchgeführten interdisziplinären Analyse in Hinblick auf die technische Plausibilität der Erwartungen an zukünftige militärische Potentiale moderner Softwaretechnologien (Kapitel 4.1) konnten daher nur für den entsprechend absehbaren Zeithorizont Einschätzungen vorgenommen werden. Die anhand militärischer Anwendungsfelder und -szenarien exemplarisch durchgeführte Analyse identifiziert Softwaretechnologien als Ursache für eine zunehmende Automatisierung und Effizienzsteigerung militärischer Anwendungen u.a. in den Bereichen Command & Control, Situational Awareness oder Logistik. KI und maschinelles Lernen entfalten vor allem dort ihr volles Potenzial, wenn sie auf spezialisierte Probleme trainiert und mit deterministischen, ganzheitlich bekannten Umgebungen konfrontiert sind. Der Analyse zufolge sind entsprechende Fortschritte realistisch und auch bereits wissenschaftlich dokumentiert. Militärische Szenarien, in denen Softwaretechnologien in der Lage sein werden, auch komplexeste Lagebilder zuverlässig zu analysieren und computergestützte Entscheidungen auf einem menschenähnlichen kognitiven Niveau zu treffen, erscheinen aber zunächst noch unrealistisch. Insgesamt illustrieren die Anwendungsfelder und -szenarien die hohen militärischen Erwartungen an Softwaretechnologien, die aus technologischer Sicht aber auf absehbare Zeit noch auf hohe Hürden stoßen werden. Ein stärker fundiertes Wissen der mittel- bis langfristigen softwaretechnologischen Forschungs- und Entwicklungstrends sowie auch detaillierter formulierte Erwartungen an zukünftige militärische Anwendungsfelder und -szenarien, werden zukünftigen interdisziplinären Plausibilitätsanalysen bezüglich der militärischen Anwendung von Softwaretechnologien mehr Gehalt geben und auch konkretere Aussagen zu realistischen mittel- bis langfristigen militärischen Potenzialen zulassen.

Im Rahmen des Forschungsprojekts ließen sich keine abschließenden Arbeitsdefinitionen von Softwaretechnologien wie z.B. KI entwickeln. Die Auseinandersetzung mit möglichen Schnittmengen hinsichtlich Akteur-bezogener Definitionen und Fähigkeitserwartungen, insbeson-

dere im Forschungsfeld KI, hat gleichwohl interessante Beobachtungen erbracht, die die Notwendigkeit einer zukünftigen interdisziplinären Auseinandersetzung mit fächerübergreifenden Begriffsgrundlegungen unterstreichen (siehe Kapitel 4.2). Die Analyse ergab, dass KI im sicherheitspolitischen Diskurs als Sammelbegriff fungiert und sich entlang seiner inhaltlichen Vagheit hohe, teils unterschiedliche und mitunter riskante Vorstellungen von Fähigkeiten, Machbarkeit und/oder Zeithorizonten von mit ihr assoziierten Technologien entfalten. Stehen diese häufig gar im Kontrast zu den im naturwissenschaftlich-technischen Kontext gebräuchlichen Bestimmungen, illustrieren unsere Ergebnisse die Notwendigkeit weitergehender interdisziplinärer Begriffsfindungen, um zukünftig den friedens- und sicherheitspolitischen Diskurs fern ab von gleichermaßen utopischen und dystopischen Vorstellungen und in einer zunehmend gemeinsamen Sprache zu gestalten.

Wichtige Einsichten ergaben sich zudem hinsichtlich der Voraussetzungen dieser Entwicklungen, die nicht allein in der Entwicklung theoretischer Algorithmen und verbesserter Rechenleistungen zu verorten sind. Es hat sich gezeigt, dass einer ihrer wesentlicher Treiber Daten sind (siehe Kapitel 4.3). Sie fungieren als ein weiterer Anker für die Erwartungen sicherheitspolitischer Akteure an die zukünftige Kriegsführung und eröffnen auf diese Weise eine neue Dimension für die Bewertung der sicherheitspolitischen Implikationen von Softwaretechnologien. In ihrer Wechselwirkung und im Zusammenspiel mit leistungsstarker IT-Hardware und einem stetig wachsenden mathematisch-analytischen Instrumentarium sind sie zudem eine essentielle Voraussetzung für fast jede moderne Softwareanwendung und ihr analytischer Einbezug sensibilisiert für Risiken, die sich aus der Organisation und Klassifikation großer Datenmengen ergeben können. Daten vertiefen insofern das Verständnis für die Bedeutung von softwaretechnologischen Entwicklungstrends und sollten daher immer auch Bestandteil bei der weiteren Bearbeitung dieser Forschungsfragen sein.

Im Rahmen der interdisziplinären Analysen dieses Forschungsprojekts konnten folglich drei wichtige Felder beleuchtet werden, die sich um die technologische Plausibilität, Schwierigkeiten eindeutiger Definitionen und die Relevanz von Daten in Zusammenhang mit der militärischen Anwendung moderner Softwaretechnologien drehten. Ein intensiver Expert*innendiskurs zu diesen Themenfeldern und den hier erzielten Analyseergebnissen hat bisher aber nicht stattfinden können und sollte Teil weiterführender Forschungsbemühungen sein. Auch konnten die aus der militärischen Anwendung von Softwaretechnologien resultierenden friedens- und sicherheitspolitischen Risiken im Rahmen dieses Projekts nicht eingehend wissenschaftlich untersucht oder mit externen Fachexpert*innen in der Tiefe erörtert werden. Vor diesem Hintergrund schließt der Forschungsbericht stattdessen im Folgenden mit einer weitgefassten interdisziplinären Betrachtung ab, die der Öffentlichkeit und Entscheidungsträger*innen eine Policy-orientierte Handreiche mit auf den Weg gibt. Sie soll das Verständnis um die friedens- und sicherheitspolitischen Risiken des militärischen Einsatzes von Softwaretechnologien – insbesondere der vielfach angeführten Künstlichen Intelligenz – fördern und wird auf die Notwendigkeit von Regulierungen in Form der Rüstungskontrolle hinführen.

5.2. Militärische Softwaretechnologien als friedens- und sicherheitspolitischer Game Changer?

Dieses Forschungsprojekt warf mit seinem Titel die Frage auf, ob der militärische Einsatz von Algorithmen und KI einen „Game Changer" in Bezug auf zukünftige Waffensysteme und die Kriegsführung darstellen wird. Breiter gefasst, und den finalen Untersuchungsansätzen dieses Projektes etwas näher, lässt sich diese Frage auch umformulieren: Wird der militärische Einsatz von Softwaretechnologien ein friedens- und sicherheitspolitischer „Game Changer" sein? Es handelt sich insofern um keine einfache Frage, die wir, um es gleich vorweg zu nehmen, anhand der Ergebnisse unseres Forschungsprojektes nicht vollumfänglich oder gar abschließend beantworten können. Eine zugrundeliegende Schwierigkeit illustriert bereits die etymologische Bedeutung des „Games Changers": Laut dem Duden verändert ein Game Changer „bisher geltende Regeln und Mechanismen [grundlegend]".[17] Der Merriam Webster formuliert noch allgemeiner und sieht darin „a newly introduced element or factor that changes an existing situation or activity in a significant way".[18] Angewendet auf das Forschungsprojekt stellt sich somit die Frage, ob der militärische Einsatz von Softwaretechnologien die Kriegsführung in signifikanter Weise ändern wird. Nun kann diese Signifikanz sowohl in einer veränderten Art und Weise begründet liegen, in der Kriege zukünftig geführt werden, als auch von grundsätzlich neuen sicherheitspolitischen Auswirkungen oder Ergebnissen herrühren, die diese Kriegsführung mit sich bringt. Anders ausgedrückt: Wird es durch den Einsatz von Softwaretechnologien relevante neue militärische Fähigkeiten oder Taktiken, induziert insbesondere durch neue Waffenfähigkeiten, geben und könnten wir dadurch mit gewichtigen neuen friedens- und sicherheitspolitischen Auswirkungen konfrontiert sein? Welche konkreten Veränderungen dabei aber genau als „signifikant" anzusehen und wo hierzu entsprechende Grenzen zu ziehen sind, sollte auf internationaler Ebene einvernehmlich geklärt werden, um auch dort zu einem gemeinsamen Verständnis eines „Game Changers" zu kommen.

Doch zusätzlich stellt sich noch eine weitere wichtige Frage: Werden solche neuen softwaretechnologischen Fähigkeiten am Ende überhaupt eine reale militärische Anwendung erfahren oder wird man sich in Anbetracht voraussichtlich signifikanter negativer friedens- und sicherheitspolitischer Auswirkungen stattdessen für deren Regulierung oder Verbot aussprechen? So könnten militärische Softwaretechnologien zwar erst einmal einen potenziellen „Game-Changer"-Charakter aufweisen, durch umsichtiges Handeln, wie z.B. präventive Rüstungskontrolle, würde dieser Charakter aber keine Wirkung entfalten. Diese Abwägungen wurden in diesem Forschungsprojekt im Detail nicht weiter betrachtet, sondern werden Aufgabe weiterführender Forschungsarbeiten und Expert*innendiskurse sein.

Begründet dadurch, dass sich die naturwissenschaftlich-technische Untersuchung dieses Forschungsprojektes nur auf die kurz- bis mittelfristigen Trends in einem exemplarischen militärischen Anwendungsfeld beschränken musste, konnte die interdisziplinäre Analyse um den Abgleich der militärischen Erwartungen und technologischen Realitäten nur eingeschränkt durchgeführt werden. Die militärischen Erwartungen an moderne Waffensysteme und die zukünftige Kriegsführung wurde hier daher nur für den kurz- bis mittelfristigen Zeithorizont auf ihre technologische Plausibilität hin analysiert (Kapitel 4.1). Anhand der Ergebnisse dieser Analyse kommen wir hier zu dem Schluss, dass moderne Softwaretechnologien heute in der mili-

[17] Duden Webseite: https://www.duden.de/rechtschreibung/Gamechanger (Stand: 11.01.2021).
[18] Merriam-Webster Webseite: https://www.merriam-webster.com/dictionary/game%20changer (Stand: 11.01.2021)

tärischen Verwendung zwar zunehmend als ein „Force Multiplier" in Hinblick auf die Steigerung militärischer Potentiale fungieren, ihnen auf kurzfristige Sicht aber nach unserem Dafürhalten bislang noch nicht der Charakter eines „Game Changers" attestiert werden kann.

Im Rahmen dieses Forschungsprojektes konnten wir nicht schlüssig untersuchen und belegen, welche mittel- bis langfristigen militärischen Anwendungspotentiale und Waffenfähigkeiten zukünftige Softwaretechnologien mit sich bringen werden. Ebenso wenig scheint gewiss, inwieweit staatliche Akteure auch alle möglichen militärischen Entwicklungen mitgehen werden oder ob es nicht doch gelingt, als riskant erachtete Technologien oder militärische Fähigkeiten in geeigneter Weise präventiv einzuhegen. Wir müssen hier daher feststellen, dass es nach wie vor zu einem großen Teil Spekulation bleibt, wie sich die Kriegsführung anhand neuer Softwaretechnologien zukünftig verändern wird (spekuliert haben wir hierzu im folgenden Kapitel 5.3 trotzdem). Ungewiss bleibt an dieser Stelle somit insbesondere, ob diese Veränderungen „signifikant" sein werden und es auf jeden Fall verdienen, als friedens- und sicherheitspolitischer „Game Changer" betitelt zu werden.

5.3. Künstliche Militärische Intelligenz: Eine Gefahr für den Frieden?

Im Rahmen dieses Forschungsberichts ist immer wieder auch der Begriff der Künstlichen Intelligenz aufgetaucht und insbesondere die Schwierigkeiten um die Definition, Deutung und Abgrenzung von KI wurden an vielen Stellen thematisiert. Von Anfang an wurde in diesem Forschungsprojekt daher das Feld der Softwaretechnologien in der Breite betrachtet, in dem Wissen, dass Künstliche Intelligenz immer ein Teil davon ist, aber Unsicherheit darüber besteht, welchen Raum sie tatsächlich einnimmt.

Vor dem Hintergrund der hier beschriebenen Forschung und unter Berücksichtigung langjähriger Erfahrungen im Themenfeld der „Digitalisierung der Kriegsführung", soll die militärische Anwendung von Künstlicher Intelligenz (oder Künstlicher Militärischer Intelligenz?) daher hier zum Ende noch einmal in einer kurzen und vor allem anschaulicheren Form betrachtet werden. Diese Darstellung erhebt nicht den Anspruch der Vollständigkeit, noch stellt sie die einzig mögliche Betrachtungsweise dar. Weil sie aber als eine hilfreiche Handreiche für den weiteren politischen Diskurs dienen kann, soll im Folgenden eine nützliche und mittlerweile auch recht geläufige Arbeitsdefinition von KI eingeführt, denkbare militärische Anwendungsfelder zusammengefasst und mögliche Auswirkungen auf die Kriegsführung skizziert werden.

5.3.1 Was ist Künstliche Intelligenz?

Der Begriff Künstliche Intelligenz dient heute in erster Linie als Schlagwort. Es wird in Verbindung und als Synonym für aktuelle Innovationen der Informationswissenschaften und daraus resultierender Anwendungen verwendet. Künstliche Intelligenz basiert auf modernen Softwaretechnologien und kann zugleich auch als Teil dieser betrachtet werden. Bisher existiert aber keine allgemeingültige Definition dessen, was Künstliche Intelligenz genau ausmacht und Abgrenzungen ermöglicht. Vielmehr werden mit KI stark voneinander abweichende Vorstellungen und Erwartungen verbunden. Einen gemeinsamen Nenner bildet sicherlich der Umstand, dass auf KI basierende Anwendungen dazu bestimmt sind, spezifische Arbeiten und Aufgaben anstelle des Menschen durchzuführen, z.B., weil diese Anwendungen dazu in der Lage

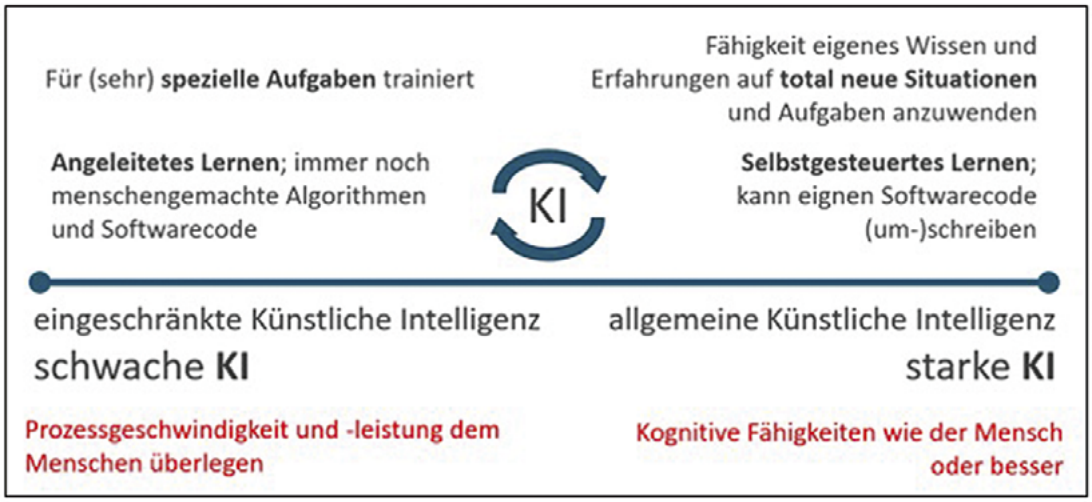

Abbildung 5.1: Spektrum Künstlicher Intelligenz

sind, diese effizienter und schneller, kostengünstiger oder genauer zu tun. Zwei Fragen, die sich in Bezug auf KI daher in diesem Zusammenhang immer aufdrängen, sind die nach dem Grad der Intelligenz und ihrem Bezugssystem, d.h. 1.) wie intelligent ist eine KI-Anwendung und im Vergleich zu „was" oder „wem" und 2.) in Bezug auf welche Arbeiten und Aufgaben kann die KI ihre kognitiven Fähigkeiten ausspielen und wo liegen die Grenzen?

Ein Ansatz, um sich die unterschiedlichen Grade an KI zu vergegenwärtigen oder begreifbar zu machen ist, die möglichen Ausprägungen Künstlicher Intelligenz innerhalb eines Spektrums zu verorten, das von einer schwachen KI auf der einen Seite hin zu einer starken KI auf der anderen Seite reicht (siehe Abbildung 5.1).

Die schwache oder eingeschränkte KI basiert diesem Modell zufolge nach wie vor auf von Menschen programmierten Algorithmen sowie Softwarecodes und wird durch angeleitetes Maschinenlernen nur für (sehr) spezielle Aufgaben trainiert. Eine schwache KI kann spezielle Aufgaben in Hinblick auf Prozessionsgeschwindigkeit und -leistung zumeist besser als ein Mensch bewältigen. Die starke oder allgemeine KI am anderen Ende des Spektrums wiederum könnte zukünftig in der Lage sein, selbständig zu lernen und ihren eigenen Softwarecode anzupassen oder umzuschreiben. Sie hätte die Fähigkeit, ihr erlangtes Wissen und ihre gesammelten Erfahrungen eigenständig auch in unvorhergesehenen Situationen anzuwenden und dabei auch völlig neue Aufgaben erfolgreich zu meistern. Die kognitiven Fähigkeiten einer solchen starken KI würden denen des Menschen entsprechen oder sogar darüber hinausgehen. Für die Gegenwart kann festgestellt werden, dass alle KI-Anwendungen auf der linken Seite des Spektrums zu verorten sind – in Nähe der schwachen KI – es sich bei ihnen also bisher nur um eingeschränkte KI handelt.

KI-Anwendungen basieren auf Softwaretechnologien. Ihre Fähigkeiten werden zwar in erster Linie durch spezifische Algorithmen und Softwarecode bestimmt, doch Rechenleistung (Computerhardware), umfangreiche Datensammlungen (zum Lernen und Trainieren der KI) sowie notwendige Infrastruktur (Datenbanken/-server, Kommunikationsverbindungen etc.) stellen wichtige Voraussetzungen dar und sind für das Funktionieren von KI-Anwendungen essentiell. Auch dem Menschen und seiner Interaktion mit der KI-Anwendung kann eine wichtige Rolle zukommen, die ggfs. berücksichtigt werden muss (siehe Abbildung 5.2). Die Rolle des Menschen erfordert insbesondere dann Beachtung, wenn es um Fragen der Mensch-Maschinen-Interaktion oder der verbliebenen menschlichen

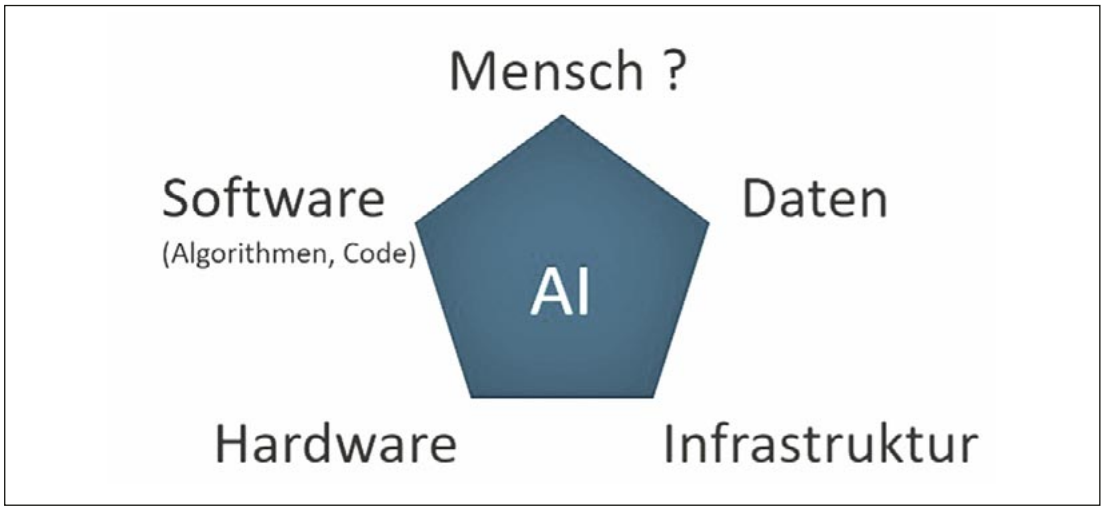

Abbildung 5.2: Was Künstliche Intelligenz ausmacht

Kontrolle von KI-Anwendungen geht. Dies gilt insbesondere auch für den militärischen Anwendungsbereich von KI, wo dem Menschen eine feste Kontrollfunktion eingeräumt werden sollte.

Die heutigen noch eingeschränkten KI-Anwendungen (schwache KI) dienen insbesondere der Informationsverarbeitung. Anwendungen und Nutzungsfelder die dabei momentan mit Künstlicher Intelligenz in Verbindung gebracht werden sind u.a. Maschinelles Lernen, Mustererkennung, Regelungstechnik, Sprach- und Bilderkennung, Steuerungsaufgaben, Robotic Process Automation (RPA) sowie Simulations- und Vorhersageanwendungen. Für sich genommen scheinen diese Anwendungsfelder erst einmal unproblematisch. Doch dienen die dort mittels KI generierten Informationen als Grundlage für wichtige menschliche Entscheidungen und fehlen dem Menschen die Möglichkeiten, diese Informationen auf Korrektheit zu überprüfen, muss diesen blind vertraut werden und der Mensch begibt sich so in eine Abhängigkeit, durch die er bereits ein Stück Kontrolle verliert.

5.3.2 Militärische KI-Anwendungen und ihre Einsatzfelder

Im Rahmen konzeptioneller Ansätze zur Digitalisierung und Automatisierung der Kriegführung werden KI-Anwendungen als ein wichtiger Baustein angesehen. Ziel dieser Konzepte – die sowohl die strategische als auch taktische militärische Ebene betreffen können – ist das Erlangen oder die Erweiterung der Fähigkeiten zur Realisierung von 1.) „schnelleren", 2.) „effizienteren" und 3) „komplexeren" militärischen Anwendungen und Operationen. Militärische Systeme, die in diesem Zusammenhang mit KI häufig Erwähnung finden sind Autonome Waffen, Verteidigungssysteme oder Gefechtsmanagementsysteme.

Im militärischen Bereich lassen sich vor diesem Hintergrund verallgemeinert drei Einsatzfelder von (zukünftigen) KI-Anwendungen abgrenzen:

Einmal die Datenverarbeitung und Lagebilderstellung, bei der es um 1.) das Sammeln, Zusammenführen, Zuordnen und Verdichten großer Datenmengen, 2.) die Datenanalyse und Informationsgewinnung sowie 3.) die Validierung, Visualisierung und Präsentation von Daten und Informationen geht.

Daneben Kommando- und Kontrollfunktionen, die der Vernetzung, Automatisierung und Handhabung bzw. Beaufsichtigung von 1.) bestimmten militärischen Funktionen oder Aufgaben, 2.)

individuellen (Waffen-)Systemen wie z.B. Autonome Waffen oder 3.) einer größeren Anzahl von (verschiedenen) militärischen Wirkmitteln und Systemen dienen.

Ein wichtiges Feld für KI-Anwendungen wird darüber hinaus die Entscheidungs-Unterstützung sein, in Form 1.) der missionsspezifischen Analyse sowie situativen Interpretation von Daten und Informationen, 2.) der Simulation und Prognose militärischer Abläufe oder Operationen sowie zukünftig 3.) der maschinellen (Teil-)Entscheidungsfindung (z.B. in Bezug auf Zielauswahl und Waffeneinsatz) unter Berücksichtigung von Informationen, den Missionskriterien und gegebenen Umgebungsbedingungen.

Neben erweiterten militärischen Fähigkeiten erhoffen sich Militärs und Sicherheitspolitiker*innen durch den Einsatz von KI auch eine Entlastung und den Schutz der eigenen Soldat*innen, indem einerseits besonders arbeits- oder zeitintensive Aufgaben an Maschinen übertragen werden und anderseits besonders gefährliche und riskante militärische Operation durch zunehmend automatisierte, unbemannte Systeme durchgeführt werden (sogenannte „Dull, Dirty, Dangerous and Dear", 4-D Einsätze). Ihren operativen Einsatz im militärischen Bereich finden KI-Anwendungen heute erst in einem sehr begrenzten Umfang und mit noch stark eingeschränkten Fähigkeiten. Exemplarisch können hier u.a. die Bild- und Signalauswertung (Beitrag zur Informationsgewinnung), die Szenarien-Erstellung und Prognostik oder der Logistik- und Organisationsbereich genannt werden.

Die zunehmenden Investitionen einiger Schlüsselstaaten in militärische KI-Anwendungen (u.a. die USA, China und Israel), vor allem aber die immensen Fortschritte im Bereich der zivilen Forschung und Entwicklung in den Informationstechnologien und ihr hohes Dual-use-Potenzial, d.h. diese Technologien können zugleich vielfach auch für militärische Zwecke einsetzt werden, lassen zukünftig einen starken Aufwuchs der Fähigkeiten militärischer KI-Anwendungen erwarten.

Als aktuelles Beispiel solcher militärischen Entwicklungsschübe wird gerne ein Experiment der Defense Advanced Research Projects Agency (DARPA) in den USA angeführt, bei dem im August 2020 erstmalig ein menschlicher Pilot in einem computersimulierten Luftkampf von einer KI besiegt wurde[19] Dieser Luftkampf wurde zwar nicht anhand echter Kampfjets ausgetragen, sondern nur virtuell durchgespielt und es mag daher erst einmal nicht überraschen, dass computergesteuerte Systeme in der Lage sind schneller und genauer als der Mensch zu reagieren, trotzdem aber wird dieses Experiment von einige Expert*innen als ein entscheidender Durchbruch für militärische KI-Anwendungen angesehen. Richtig interessant dürfte es allerdings erst werden, wenn diese computergesteuerten Systeme auch in der Lage sind eine komplexe Lagebeurteilung durchzuführen, also eine starke KI vorliegt. Aber ist eine solche Künstliche Militärische Intelligenz überhaupt eine erstrebenswerte Entwicklung?

5.3.3 Welche friedens- und sicherheitspolitischen Herausforderungen und Probleme können sich durch den Einsatz einer Künstlichen Militärischen Intelligenz ergeben?

Eine weit verbreite Vorstellung, die mit einem möglichen Einsatz Künstlicher Intelligenz im militärischen Bereich einhergeht, ist das Bild von super-intelligenten Kontroll- und Befehlsnetzwerken wie einem „Skynet" oder autonom agierenden, intelligenten Killer Robotern vom Typ „Terminator", beide bekannt aus denselben Science-Fiction-Filmen. Eine solche dystopische Zukunft, in der eine starke Künstliche Intelligenz die Macht übernommen hat, wünscht sich heute

[19] Weitere Informationen hierzu unter: https://www.darpa.mil/news-events/2020-08-26 (Stand: 11.01.2021)

niemand und sie liegt ebenso wenig im Interesse von Sicherheitspolitiker*innen und Militärs. Auch existiert eine solche starke KI bisher weder, noch ist sie in naher Zukunft absehbar.

Aber bereits heute ergeben sich durch den militärischen Einsatz von KI erhebliche Risiken. Diese liegen nicht unbedingt darin begründet, wie schwach oder stark die eingesetzte KI wirklich ist, sondern ergeben sich aus dem Maß an Kontrolle, das der Mensch bereit ist aufzugeben, um es an die KI zu übertragen. Die Gefahr eines menschlichen Kontrollverlustes und die Entkopplung des Menschen vom Gefechtsfeld stellen das Hauptrisiko beim Einsatz einer jeden KI dar. Dieses Risiko ist unmittelbar mit den eigentlichen militärischen Intentionen hinter dem Einsatz von Künstlicher Intelligenz verbunden; die Möglichkeiten für eine „schnellere", „effizientere" und „komplexere" Kriegsführung zu erlangen und die hier dem Menschen gesetzten Grenzen zu überwinden. Durch die Möglichkeiten der Vernetzung, der Anbindung an enorme Dateninformationen und stetig steigende Rechenkapazitäten werden computergestützte KI-Anwendungen dem Menschen in Bezug auf Datenverarbeitungs- und Reaktionsgeschwindigkeiten immer überlegen sein. Kurz- bis mittelfristig werden KI-Anwendungen aber nicht über die Fähigkeit verfügen, wie ein Mensch zu lernen und Erfahrungen auf neue Situationen anzuwenden, Plausibilitäten abzuschätzen und so komplexe Lagen zu beurteilen. Bevor KI-Anwendungen – wenn überhaupt – über das Äquivalent eines „gesunden Menschenverstandes" verfügen, wird wohl noch eine lange Zeit vergehen.

Eine schwache KI ist in Bezug auf die Beurteilung komplexer Lagen also auch eine „dumme" und sehr fehleranfällige KI, deren Analyseergebnisse einer menschlichen Kontrolle und Verantwortung unterliegen müssen. Werden solche KI-Anwendungen aber in der Art eingesetzt, dass enorme Datenmengen in Bruchteilen von Sekunden durch diese aufbereitet, analysiert und beurteilt werden, um dem Menschen unmittelbar als eine wichtige Entscheidungsgrundlage zu dienen, wird eine verantwortungsvolle menschliche Kontrolle der Informationen schon nicht mehr möglich sein. Der Mensch alleine könnte die Genauigkeit und Fehlerfreiheit dieser Informationen nicht in überschaubarer Zeit verifizieren. Damit stellen bereits computergeneriete Entscheidungsgrundlagen ein Risiko dar, wenn dem Menschen die Möglichkeiten zu deren Kontrolle nicht mehr gegeben sind. Verantwortungsvolle Entscheidungen sind auf dieser Basis eigentlich nicht zutreffen.

Sollte es jemals eine starke KI geben, die eine menschenähnliche Intelligenz aufweist, so ist es eine sowohl völkerrechtliche als auch ethische Frage, ob der Mensch die Verantwortung über militärisches Handel und Waffeneinsatzentscheidungen an diese KI abtreten darf oder sollte. Soll eine KI Menschen töten dürfen und kann sie für Fehler zur Verantwortung gezogen und ggfs. auch entsprechend sanktioniert werden?

Doch neben diesen ethischen und völkerrechtlichen Erwägungen sind es absehbar auch negative friedens- und sicherheitspolitische Risiken von KI-Anwendungen, die durch einen menschlichen Kontrollverlust sowie die Beschleunigung der Kriegführung zu Tage treten werden. Stark beschleunigte Reaktionszeiten, fehlerhafte oder unvollständige Entscheidungsgrundlagen sowie die Störanfälligkeit oder ein unvorhersehbares Verhalten einer KI-Anwendung (gerade auch bedingt durch die zugrundeliegenden hochkomplexen Softwaretechnologien) bergen die Gefahr von Missverständnissen und Eskalationspotenzialen, insbesondere, wenn dem Menschen kaum oder gar keine Zeit bleibt, Entscheidungen hinreichend zu überdenken. Auch könnte durch KI-Anwendungen zukünftig der Einsatz militärischer Waffensysteme einfacher und unmittelbarer ermöglicht werden, zum Beispiel, weil sich grundlegend neue Einsatzszenarien ergeben oder mittels autonom agierender Waffen das Leben eigener Soldat*innen geschont würde. Hierdurch könnte es zu vermehrten oder „leichtfertigeren" Einsätzen kommen und die Wahl militärischer Konfliktlösungen so

wahrscheinlicher werden. Nicht zuletzt kann es durch den zunehmenden und breiteren Einsatz moderner Softwaretechnologien und KI-Anwendungen zu einer Automatisierungs- und Beschleunigungsspirale in Bezug auf die Kriegsführung kommen. Staaten könnten sich gezwungen sehen, diese Entwicklung in Form verstärkter moderner Rüstung mitzumachen, um nicht ins militärische Hintertreffen zu geraten. Solche Rüstungsdynamiken können in ein Wettrüsten münden und hätten einen destabilisierenden Charakter. Insgesamt werden KI-Anwendungen und resultierende moderne Waffensysteme, wie z.B. Autonome Waffen, eine zusätzliche Gefahr für die regionale wie auch strategische Stabilität darstellen.

Angesichts der Gefahr eines menschlichen Kontrollverlustes und den friedens- und sicherheitspolitischen Auswirkungen sollte es uns Sorge bereiten, dass wir bisher nicht in der Lage sind die „Essenz" von Künstlicher Intelligenz, Autonomie oder menschlicher Kontrolle für uns allgemeingültig zu definieren, zu kategorisieren oder abzugrenzen. Denn solange das nicht gelingt, können wir auch keine Grenzen in Hinblick auf diese Entwicklungen ziehen, also entscheiden, wie weit wir bereit sind zu gehen und wo wir die Entwicklung von Künstlicher Intelligenz und Autonomie gestoppt wissen wollen. Sich alleine darauf zu verständigen, man wolle oder werde keine „unkontrollierte" Künstliche Intelligenz oder Autonomie in der Kriegsführung zulassen wird nicht ausreichen, denn ohne bereits heute festgelegte „sichtbare" Grenzen ist zu befürchten, dass ein Kontrollverlust sowie

5.4. Fazit. Regulierung militärischer Softwaretechnologien: Den Risiken verantwortungsvoll begegnen

nachteilige friedens- und sicherheitspolitischen Auswirkungen zukünftig erst festgestellt werden, wenn sie bereits eingetreten sind.

Um die Risiken und Gefahren abwägen zu können, die der militärische Einsatz moderner Softwaretechnologien mit sich bringt, gilt es zunächst zu analysieren, inwiefern der Einsatz dieser Technologien die Kriegsführung zukünftig verändern wird bzw. welches die Unterschiede zur herkömmlichen Art und Weise einen Krieg zu führen sein werden. Dieses Forschungsvorhaben hat einerseits einen Einblick in den derzeitigen Stand von militärischen Erwartungen und technischen Realitäten sowie den kurz- bis mittelfristigen Entwicklungen gegeben. Daneben wurden mögliche Problemfelder beleuchtet und wichtiger zusätzlicher Forschungsbedarf identifiziert. Leider reicht der Blick nach vorne aber nicht weit genug um verlässlich beurteilen zu können, zu welchen neuen militärischen Fähigkeiten sowie friedens- und sicherheitspolitischen Risiken moderne Softwaretechnologien mittel- bis langfristig genau führen werden. Eine fortgesetzte und vertiefte interdisziplinäre Analyse der technologischen Trends wird hierfür essentiell sein und sollte unter einer verstärkten Einbeziehung naturwissenschaftlich-technischer Fachexpertise erfolgen.

Im internationalen Diskurs wird es zukünftig unabdingbar sein, ein gemeinsames Verständnis der Entwicklungen und militärischen Anwendungsfelder rund um Softwaretechnologien, wie z.B. Künstlicher Intelligenz, Autonomie, etc. zu erlangen. Insbesondere auch in Bezug auf die zunehmend prominente Rolle, die Dateninformationen in diesem Zusammenhang spielen. Nur so wird man auch ein gemeinsames Bild der Risiken entwickeln und mit den entsprechenden technologischen Entwicklungen oder Anwendungen korrelieren können. Auf dieser Basis ließen sich dann ebenso Grenzen der technologischen Entwicklung oder militärischen Anwendung von Softwaretechnologien identifizieren, an denen internationale Regulierungsbemühungen festgemacht werden könnten.

Obgleich sich der genaue Einfluss moderner Softwaretechnologien auf die zukünftige Kriegsführung noch nicht bestimmen lässt, zeichnen sich bereits heute mögliche friedens- und sicherheitspolitische Auswirkungen hinreichend deutlich ab. Automatisierungs- und Beschleunigungsspiralen, Rüstungsdynamiken, erhöhte Eskalationspotentiale, regionale und strategische Destabilisierung oder menschlicher Kontrollverlust werden zunehmend wahrscheinlicher, sollte der militärische Einsatz von Softwaretechnologien zukünftig nicht reguliert werden. Eine vorausschauende und auf die möglichen Risiken und Gefahren abgestimmte Regulierung, z.B. in Form von Rüstungskontrolle, sollte dabei im allseitigen Interesse liegen. Solche präventive Rüstungskontrolle kann erfolgreich sein, sollte die Staatengemeinschaft darin übereinkommen, dass Gefahren und Risiken den erhofften militärischen Nutzen überwiegen, wie zum Beispiel das Übereinkommen zum Verbot von „Blendwaffen" bereits bewiesen hat.[20] Für solche Bemühungen bieten, neben den völkerrechtlichen Vorgaben, insbesondere die möglichen friedens- und sicherheitspolitischen Risiken ein bisher noch nicht ausgeschöpftes Argumentationspotenzial.

Doch die präventive Rüstungskontrolle neuer Technologien ist auch herausfordernd und gestaltet sich schwierig, wie die Verhandlungen zu tödlichen Autonomen Waffensystemen (LAWS) bei der UN in Genf zeigen. Obwohl die Gespräche in diesem Rahmen bereits seit 2014 stattfinden, herrscht seit einigen Jahren Stillstand, was insbesondere dem Unvermögen geschuldet ist, sich auf gemeinsame Definitionen zu einigen und Mechanismen zur Sicherstellung menschlicher Kontrolle zu entwickeln. Auch muss festgestellt werden, dass das Interesse technologischer Vorreiterstaaten an Rüstungskontrolle oftmals nicht sehr weitsichtig, sondern vor allem auf unmittelbare eigene militärische Vorteil fokussiert ist, die man keiner Regulierung unterwerfen möchte. Zukünftige eigene Risiken, die durch umsichtiges und rechtzeitiges Handeln verhindert werden könnten, werden dabei zu wenig in den Blick genommen oder als beherrschbar angesehen und im heutigen politischen Handeln unzureichend berücksichtigt.

Eine weitere Herausforderung für Rüstungskontrolle ergibt sich durch das hohe Dual-use Potenzial von Softwaretechnologien, deren Forschung und Entwicklung vor allem im zivilen Sektor vorangetrieben wird. Das bedeutet, eine Unterscheidung von ziviler und militärischer Nutzung ist zumeist kaum möglich, weshalb sich eine Regulierung militärischer Softwaretechnologien sehr schwer gestaltet. Obgleich erfolgreiche Rüstungskontrolle vor allem auf gemeinsamen Interessen gründet, so sehr ist sie auch von gegenseitigem Vertrauen abhängig, das vorwiegend durch geeignete Überprüfungsmechanismen von Rüstungskontrollverträgen sichergestellt wird. Eine solche Verifikation oder Kontrolle ist in Bezug auf Softwaretechnologien nur schwer zu gewährleisten und stellt ein bisher ungelöstes Problem dar, für das es bisher noch an geeigneten Lösungskonzepten fehlt.

Die heutige Zeit ist von zunehmenden internationalen Spannungen und einer geschwächten internationalen Sicherheitsarchitektur geprägt. Die Risiken, die sich aus der militärischen Verwendung von Softwaretechnologien zukünftig ergeben, stellen eine zusätzliche Gefahr für die Stabilität und den Frieden dar. Rüstungskontrolle könnte ein probates Mittel sein, um diese Risiken erfolgreich einzuhegen – eine Lehre, die aus dem Kalten Krieg gezogen werden kann, zwischenzeitlich aber in Vergessenheit geraten schien. Allerdings werden die bisherigen klassischen Ansätze von Rüstungskontrolle der Regulierung von modernen Softwaretechnologien alleine nicht mehr gerecht, vielmehr gilt es Rüstungskontrolle neu zu denken und um innovati-

[20] Zum Verbot "blind machender Laserwaffen" (Protokoll IV der UN-Waffenkonvention) siehe z.B. Informationen auf der Seite des Internationalen Komitees Vom Roten Kreuz: https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Treaty.xsp?documentId=70D9427BB965B7CEC12563FB0061CFB2&action=openDocument

ve Ansätze zu erweitern. In dieser Hinsicht ist insbesondere die interdisziplinäre Forschung verstärkt gefordert, ein besseres Verständnis der mittel- bis langfristigen softwaretechnologischen Forschung und Entwicklungen zu erlangen, mögliche militärische Potenziale hieraus abzuleiten und auf zukünftige friedens- und sicherheitspolitische Risiken zu schließen. Mit dem von der DSF geförderten Forschungsvorhaben „Algorithmen und Künstliche Intelligenz als Game Changer? Moderne Waffensysteme zwischen Erwartung und Wirklichkeit“ wurde hierzu ein erster wichtiger Beitrag geliefert, auf den es aufzubauen gilt. Doch neben der Forschung sind auch die sicherheitspolitischen und militärischen Entscheidungsträger gefragt. Einerseits indem sie die Ergebnisse der Forschung aufnehmen und andererseits die Bereitschaft zeigen, das Bewusstsein um die friedens- und sicherheitspolitischen Risiken des militärischen Einsatzes moderner Softwaretechnologien sowie den Nutzen und die Notwendigkeit von Rüstungskontrolle zu schärfen. Ein intensivierter internationaler Dialog zu diesen Themen ist essentiell und baldige Verhandlungen im Rahmen der Staatengemeinschaft sollten das Ziel sein.

Es gilt nichts zu beschönigen, dies wird kein leichter und schneller Prozess sein. In Hinblick auf die Regulierung militärischer Softwaretechnologien sind noch viele Fragen offen und kreative Lösungen müssen erarbeitet werden, so dass zukünftig auch hier der Nutzen von Rüstungskontrolle und das in sie gesetzte Vertrauen sichergestellt werden kann.

Literatur

115th Congress (2017). H.R.4625, Future of Artificial Intelligence Act of 2017, 12. Dezember 2017. https://www.congress.gov/bill/115th-congress/house-bill/4625/text (Zugriff am 14. Dezember 2019).

Abadicio, Millicent (2020). Facial Recognition in the Military. Current Application. Emerj, 17. Februar 2020. https://emerj.com/ai-sector-overviews/facial-recognition-in-the-military-current-applications/ (Zugriff am 15. August 2020).

Adão, Telmo/ Hruška, Jonáš/ Luís Pádua/ Bessa, José/ Peres, Emanuel/ Morais, Raul/ Sousa, Joaquim (2017): Hyperspectral Imaging: A Review on UAV-Based Sensors, Data Processing and Applications for Agriculture and Forestry. Remot Sensing 9(11): 1–30. https://doi.org/10.3390/rs9111110 (Zugriff am 01. Februar 2021).

ADLink. (2019). Tower in a teacup: How the small form factor transition is reshaping embedded and military computing. ADLink. http://smallformfactors.mil-embedded.com/articles/tower-in-a-teacup-how-the-small-form-factor-transition-is-reshaping-embedded-and-military-computing/ (Zugriff am 01. Februar 2021).

A**izman, Alex/ Maltby, Gavin/ Breuel, Thomas** (2019). High performance I/O for large scale deep learning, in: IEEE (Hg.), International conference on big data. https://arxiv.org/ftp/arxiv/papers/2001/2001.01858.pdf (Zugriff am 01. Februar 2021).

Alberts, David/ Garstka, John J./ Stein, Frederick P. (1999). Network Centric Warfare: Developing and Leveraging Information Superiority. CCRR Publication Series.

Allen, Greg/ Chan, Taniel (2017). Artificial Intelligence and National Security. Belfer Center for Science and International Affairs. Harvard Kennedy School, Belfer Center Study. https://www.belfercenter.org/sites/default/files/files/publication/AI%20NatSec%20-%20final.pdf (Zugriff am 15. April 2020).

Altmann, Jürgen/ Sauer, Frank (2019). Autonomous Weapon Systems and Strategic Stability. Survival. Global Politics and Strategy, 59(5): 117–142.

Alwardt, Christian (2019). Unbemannte Systeme als Herausforderung für die Rüstungs- und Exportkontrolle, in: Werkner, Ines-Jacqueline/ Hofheinz, Marco (Hg.), Unbemannte Waffen und ihre ethische Legitimierung. Wiesbaden: Springer VS, 85–109.

Amoroso, Daniele/ Sauer, Frank/ Sharkey, Noel/ Suchman, Lucy/ Tamburrini, Guglielmo (2018). Autonomy in Weapon Systems. The Military Application of Artificial Intelligence as a Litmus Test for Germany's New Foreign and Security Policy. Heinrich Böll Stiftung. Publication Series on Democracy Vol. 49. https://www.boell.de/de/2018/05/23/autonomy-weapon-systems (Zugriff am 15. Oktober 2019).

Amt für Heeresentwicklung (2019). Künstliche Intelligenz in den Landstreitkräften. Ein Positionspapier des Amts für Heeresentwicklung. Köln. https://www.bundeswehr.de/resource/blob/156024/d6ac452e72f77f3cc071184ae34dbf0e/download-positionspapier-deutsche-version-data.pdf (Zugriff am 14. April 2020).

Angwin, Julia/ Larson, Jeff/ Surya, Mattu/ Kirchner, Lauren (2016). Machine Bias. There's software used across the country to predict future criminals. And it's biased against blacks. ProPublica, 23. Mai 2016. https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing. (Zugriff am 14. April 2020).

Barnett, Jackson (2020). Army looks to block

data 'poisoning' in facial recognition, AI. Fedscoop, 11. Februar 2020. https://www.fedscoop.com/army-looks-block-data-poisoning-facial-recognition/ (Zugriff am 10. September 2020).

Barocas, Solon/ Selbst, Andrew D. (2016). Big Data's Disparate Impact. California Law Review, 104: 671–732.

Barocas, Solon/ Rosenblat, Alex/ Boyd, Danah/ Gangadharan/ Seeta Peña/ Yu, Corinne (2014). Data & Civil Rights: Technology Primer. Produced for Data & Civil Rights Conference, 30. Oktober 2014. http://www.datacivilrights.org/pubs/2014-1030/Technology.pdf (Zugriff am 13. September 2020).

Barroso, Antonia (2017). Soldier Borne Sensors (SBS) Video. https://www.youtube.com/watch?v=YqRX95AZMok (Zugriff am 10. Dezember 2019).

Bell, Andy et al. (2018). Meeting the Unmet Data Collection & Management Requirements of Big Data Analytics and AI for Military Decision Making. NATO Specialist Meeting Big Data & Artificial Intelligence for Military Decision Making. North Atlantic Treaty Organization/ Science and Technology Organization. Meeting Proceedings RDP (STO-MP-IST-160-S4-2), 06. Januar 2018. https://www.sto.nato.int/publications/STO%20Meeting%20Proceedings/Forms/Meeting%20Proceedings%20Document%20Set/docsethomepage.aspx?ID=43455&FolderCTID=&RootFolder=https://www.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-IST-160 (Zugriff am 20. Juli 2020).

Berkowitz, Uri (2018). „We'll make Israel one of world's AI leaders": Prof. Isaac Ben-Israel, who persuaded the government to invest in cybersecurity in 2010, hopes to duplicate this success in artificial intelligence. Globes Online, 12. August 2018. https://en.globes.co.il/en/article-well-make-israel-one-of-the-worlds-five-leading-countries-in-ai-1001249707 (Zugriff am 15. November 2019).

Bieker, Felix/ Bremert, Benjmin/ Hansen, Marit (2018). Verantwortlichkeit und Einsatz von Algorithmen bei öffentlichen Stellen. DuD Datenschutz und Datensicherheit, 10: 608–612.

Bläsius, Karl Hans/ Siekmann, Jörg H. (2019). Frühwarnsysteme und Cyberangriffe – gefährliche Wechselwirkungen möglich. Behördenspiegel, 35(8): 44. https://issuu.com/behoerden_spiegel/docs/2019_august (Zugriff am 14. April 2020).

Bläsius, Karl Hans/ Siekmann, Jörg H. (1987). Computergestützte Frühwarn- und Entscheidungssysteme. Informatik-Spektrum, 10: 24–39.

Boland, Barbara (2017). Algorithmic Warfare Cross Functional Team (AWCFT) To Manage Data from Drone Surveillance. GovconWire, 23. Mai 2017. https://www.govconwire.com/2017/05/algorithmic-warfare-cross-functional-team-awcft-to-manage-data-from-drone-surveillance/ (Zugriff am 20. Juli 2020).

Boulamwini, Joy/ Gebru, Timnit (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. Proceedings of Machine Learning Research, 81: 1–15.

Boulanin, Vincent/ Verbruggen, Maaike (2017). Mapping the Development of Autonomy in Weapon Systems. Stockholm: SIPRI. https://www.sipri.org/sites/default/files/2017-11/sipri-report_mapping_the_development_of_autonomy_in_weapon_systems_1117_1.pdf (Zugriff am 15. März 2020).

BMBF, Bundesministerium für Bildung und Forschung (2018). Strategie Künstliche Intelligenz der Bundesregierung. Berlin. https://www.bmbf.de/files/Nationale_KI-Strategie.pdf (Zugriff am 12. Oktober 2019).

Burkhardt, Marcus (2017): Vorüberlegungen zu einer Kritik der Algorithmen an der Grenze von Wissen und Nichtwissen, in: Friedrich, Alexander/ Gehring, Petra/ Hubig, Christoph/ Kam-

ninski, Andreas/ Nordmann, Alfred (Hg.), Technisches Nichtwissen. Jahrbuch Technikphilosophie. Baden-Baden: Nomos, 55–68.

businesswire. A Bershire Hathaway Company (2019). Maxar Technologies Awarded Four-Year Global EGD Contract by the U.S. Government for On-Demand Access to Mission-Ready Satellite Imagery. businesswire, 27. August 2019. https://www.businesswire.com/news/home/20190827005066/en/Maxar-Technologies-Awarded-Four-Year-Global-EGD-Contract (Zugriff am 15. März 2020).

Cao, Yutian/ Wang, Gang/ Yan, Dongmei/ Zhao, Zhongming (2015). Two algorithms for the detection and tracking of moving vehicle targets in aerial infrared image sequences. Remote Sensing, 8(1): 28. https://doi.org/10.3390/rs8010028 (Zugriff am 01. Februar 2021).

Campaign to Stop Killer Robots (2015). Artificial intelligence experts call for ban. http://www.stopkillerrobots.org/2015/07/aicall/ (Zugriff am 25. März 2020).

CCW, Convention on Certain Conventional Weapons (2019): Meeting of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects. Geneva, 13.–15. November 2019. Agenda item 15. https://undocs.org/CCW/MSP/2019/9 (Zugriff am 10. April 2020).

Chavannes, Esther/ Klonowska, Klaudia/ Sweijs, Tim (2020). Governing autonomous weapon systems. Expanding the solution space, from scoping to applying. The Hague Centre for Strategic Studies. https://hcss.nl/sites/default/files/files/reports/HCSS%20Governing%20AWS%20final.pdf (Zugriff am 15. November 2020).

China Daily (2017). Full text of Xi Jinping's report at 19th CPC National Congress. XI Jingping: Secure a Decisive Victory in Building a Moderately Prosperous Society in All Respects and Strive for the Great Success of Socialism with Chinese Characteristics for a New Era. Delivered at the 19th National Congress of the Communist Party of China. 18. Oktober 2017, 04. November 2017. http://www.chinadaily.com.cn/china/19thcpcnationalcongress/2017-11/04/content_34115212.htm (Zugriff am 13. November 2019).

CNBC (2017). Putin: Leader in artificial intelligence will rule world. CNBC, 04. September 2017. https://www.cnbc.com/2017/09/04/putin-leader-in-artificial-intelligence-will-rule-world.html (Zugriff am 12. November 2019).

Gorman, Siobhan/ Dreazen, Yochi J./ Cole, August (2009). Insurgents Hack U.S. Drones. In Wall Street Journal. Online verfügbar unter https://www.wsj.com/articles/SB126102247889095011 (Zugriff am 28. April 2020).

Connolly, Richard/ Boulègue, Mathieu (2018). Russia's New State Armament Programme. Implications for the Russian Armed Forces and Military Capabilities to 2027. London: Chatham House. https://www.chathamhouse.org/sites/default/files/publications/research/2018-05-10-russia-state-armament-programme-connolly-boulegue-final.pdf (Zugriff am 15. Dezember 2019).

Crowe, Steve (2019). Researchers Back Tesla's Non-LiDAR Approach to Self-Driving Cars. The Robot Report, 25. April 2019. https://www.therobotreport.com/researchers-back-teslas-non-lidar-approach-to-self-driving-cars/ (Zugriff am 01. Februar 2021).

Dahlmann, Anja/ Dickow, Marcel (2019). Präventive Regulierung autonomer Waffensysteme: Handlungsbedarf für Deutschland auf verschiedenen Ebenen. SWP-Studie, 1/2019. Berlin: Stiftung Wissenschaft und Politik (SWP) - Deutsches Institut für Internationale Politik und Sicherheit. https://doi.org/10.18449/2019S01 (Zugriff am 01. Oktober 2020).

Danks, David/ London, Alex John (2017). Algorithmic Bias in Autonomous Systems. Proceedings of the Twenty-Sixth International Joint Conference on Artificial Intelligence (IJCAI-17). https://www.cmu.edu/dietrich/philosophy/docs/london/IJCAI17-AlgorithmicBias-Distrib.pdf (Zugriff am 02. Oktober 2020).

DARPA/ Wierzbanowski, Scott (o.J.). Collaborative Operations in Denied Environment (CODE). http://www.darpa.mil/program/collaborative-operations-in-denied-environment (Zugriff am 20. April 2020).

Datta, Amit/ Tschantz, Michael Carl/ Datta, Anupam (2015). Automated Experiments on Ad Privacy Settings. A Tale of Opacity, Choice, and Discrimination. Proceedings on Privacy Enhancing Technologies, 2015(1): 92–112.

Dean, Jeffrey/ Ghemawat, Sanjay (2008). MapReduce: Simplified Data Processing on Large Clusters. Communications of the ACM, 51(1): 107. https://doi.org/10.1145/1327452.1327492 (Zugriff am 01. Februar 2021).

Der Standard (2018). Amazon streicht KI-Rekrutierungstool wegen Frauenfeindlichkeit. Der Standard web, 10. Oktober 2018. Verfügbar unter: www.derstandard.de/story/2000089096622/amazon-streicht-ki-rekrutierungstool-wegen-frauenfeindlichkeit. (Zugriff am 15. August 2020).

Deutscher Ethikrat (2017). Big Data und Gesundheit – Datensouveränität als informationelle Freiheitsgestaltung. Stellungnahme. Berlin. https://www.ethikrat.org/fileadmin/Publikationen/Stellungnahmen/deutsch/stellungnahme-big-data-und-gesundheit.pdf (Zugriff am 15. Dezember 2019).

DHS, Department of Homeland Security (2017). Narrative Analysis. Artificial Intelligence. https://info.publicintelligence.net/OCIA-ArtificialIntelligence.pdf (Zugriff am 15. Dezember 2019).

Ding, Jeffrey (2018). Deciphering China's AI Dream. Future of Humanity Institute, University of Oxford. https://www.fhi.ox.ac.uk/wp-content/uploads/Deciphering_Chinas_AI-Dream.pdf (Zugriff am 07. November 2019).

DoD, Department of Defense (2019a). Defense-Wide Justification Book. U.S. Department of Defense. https://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2020/budget_justification/pdfs/03_RDT_and_E/RDTE_Vol2_MDA%20RDTE_PB20_Justification_Book.pdf (Zugriff am 08. Dezember 2019).

DoD (2019b). Digital Modernization Strategy. DoD Information Resource Management Strategic Plan FY 19–23. https://media.defense.gov/2019/Jul/12/2002156622/-1/-1/1/DOD-DIGITAL-MODERNIZATION-STRATEGY-2019.PDF (Zugriff am 08. Dezember 2019).

DoD (2018). Summary of the 2018 Department of Defense Artificial Intelligence Strategy. Harnessing AI to Advance Our Security and Prosperity. https.//media.defense. gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF (Zugriff am 08. Dezember 2019).

DoD (2017). Unmanned Systems Integrated Roadmap. https://www.defensedaily.com/wp-content/uploads/post_attachment/206477.pdf (Zugriff am 15. Februar 2020).

DoDLive (o.J.). 3rd Offset Strategy 101: What It Is, What the Tech Focuses Are. https://www.dodlive.mil/2016/03/30/3rd-offset-strategy-101-what-it-is-what-the-tech-focuses-are/ (Zugriff am 13. Dezember 2019).

DoN, Department of the Navy (2016). Naval Aviation Vision. 2016–2025. https://www.navy.mil/strategic/Naval_Aviation_Vision.pdf (Zugriff am 10. November 2019).

Dukino, Claudia (2019). Was ist Künstliche Intelligenz? Eine Definition jenseits von Mythen und Moden. Fraunhofer IAO; 14. März 2019.

https://blog.iao.fraunhofer.de/was-ist-kuenstliche-intelligenz-eine-definition-jenseits-von-mythen-und-moden/ (Zugriff am 13. September 2020).

EFI, Expertenkommission Forschung und Innovation (2019). Gutachten zu Forschung, Innovation und technologischer Leistungsfähigkeit Deutschlands. Gutachten 2019. Berlin. https://www.e-fi.de/fileadmin/Gutachten_2019/EFI_Gutachten_2019.pdf (Zugriff am 02. Oktober 2020).

Elish, M. C./ Hwang, Tim (2016). An AI Pattern Language. Intelligence and Autonomy Initiative. New York: Data & Society.

Elmer, Keegan (2019). China and Russia plan to boostscientic cooperation with focus on artificial intelligence and other strategic areas. South China Morning Post, 28. Dezember 2019. https://www.scmp.com/news/china/diplomacy/article/3043787/china-and-russia-plan-boost-scientific-cooperation-focus (Zugriff am 09. Januar 2020).

E**ndsley, Mica R.** (1995). Toward a theory of situation awareness in dynamic systems. Human Factors, 37(1): 32–64.

Ernst, Christian (2017). Algorithmische Entscheidungsfindung und personenbezogene Daten. Juristenzeitung, 21: 1026–1036.

Erwin, Sandra (2017). Satellite Operators Push Plan to Upgrade Military Spy Drones. Spacenews, 8. November 2017. https://spacenews.com/satellite-operators-push-plan-to-upgrade-military-spy-drones/ (Zugriff am 28. April 2020).

Erz, Hendrik (2020). Künstliche Intelligenz und Daten: Eine Evaluation softwarebasierter militärischer Informationsgewinnung. Research Report 4. Hamburg: IFSH. https://ifsh.de/file/publication/Research_Report/004/20200701_Research_Report_004.pdf (Zugriff am 13. Dezember 2020).

Eshel, Tamir (2015). Russian Military to Test Combat Robots in 2016. Defense Update, 31. Dezember 2015. http://defense-update.com/20151231_russian-combat-robots.html (Zugriff am 15. Oktober 2019).

Field, Kyle. (2020). Tesla Achieved the Accuracy of Lidar with Its Advanced Computer Vision Tech. CleanTechnica, August 4, 2020. https://cleantechnica.com/2020/08/03/tesla-achieved-the-accuracy-of-lidar-with-its-advanced-computer-vision-tech/ (Zugriff am 01. Februar 2021).

Fishler, Eran/ Haimovich, Alexander R./ Blum, Rick S./ Chizhik, Dmitry/ Cimini, Leonard J./ Valenzuela, Reinaldo A. (2004). MIMO Radar: An Idea Whose Time Has Come, in: IEEE (Hg.), Proceedings of the 2004 IEEE Radar Conference, 71–78. https://doi.org/10.1109/NRC.2004.1316398 (Zugriff am 01. Februar 2021).

Fox News (2018). Interview with Benjamin Netanyahu. Fox News, 11. März 2018. https://www.foxnews.com/transcript/netanyahu-on-israels-relationship-with-the-arab-world (Zugriff am 20. Oktober 2019).

Genesereth, Michael R./ Nilsson, Nils J. (1987). Logische Grundlagen der Künstlichen Intelligenz. Braunschweig/ Wiesbaden: Friedr. Vieweg & Sohn.

Gill, Amandeep (2017). Introduction, in: UNODA, United Nations Office for Disarmament Affairs (Hg.): UNODA Occasional Papers. Nr. 30, November 2017. Perspectives on Lethal Autonomous Weapon Systems. New York, 1–4. https://www.unog.ch/80256EDD006B8954/(httpAssets)/6866E44ADB996042C12581D400630B9A/$file/op30.pdf (Zugriff am 20. März 2020).

Goodfellow, Ian/ Bengio, Yoshua/ Courville, Aaron (2016). Deep. Learning. Cambridge/ London: MIT Press. https://www.deeplearningbook.org/ (Zugriff am 02. September 2020).

Görtz, Günther/ Schneeberger, Josef/

Schmidt, Ute (2013). Handbuch der Künstlichen Intelligenz. München: De Gruyter Oldenbourg.

Groth, Olaf/ Nitzberg, Mark/ Zehr, Dan (2019). Vergleich nationaler Strategien zur Förderung von Künstlicher Intelligenz. Teil 2. Herausgegeben von Konrad-Adenauer-Stiftung e.V. Sankt Augustin/Berlin. https://www.kas.de/documents/252038/4521287/K%C3%BCnstliche+Intelligenz+Internationaler+Vergleich+Teil+2.pdf/16c82d12-898c-259b-c352-931a635fcfb3?version=1.1&t=1560420028147 (Zugriff am 12. November 2019).

He, Yujia (2017). How China is preparing for an AI-powered Future. Wilson Briefs, Juni 2017. https://www.wilsoncenter.org/sites/default/files/how_china_is_preparing_for_ai_powered_future.pdf (Zugriff am 06. November 2019).

Hill, Kashmir (2020). The Secretive Company That Might End Privacy as We Know It. The New York Times, 18. Januar 2020. https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html (Zugriff am 01. Februar 2021).

Hille, Kathrin/ Waters, Richard (2018). The power of civilian partnerships. Worried about China's rapid advances in AI and the close collaboration between the military and the country's private sector, the US is developing new tools to limit the export of frontier technologies. Financial Times (London), 09. November 2018: 7.

Horowitz, Michael C. (2019). When speed kills: Lethal autonomous weapon systems, deterrence and stability. Journal of Strategic Studies, 42(6): 764–788.

HRW, Human Rights Watch (2012). Losing Humanity: The Case against Killer Robots. Human Rights Watch, International Human Rights Council, International Human Rights Clinic, November 2012. https://www.hrw.org/sites/default/files/reports/arms1112ForUpload_0_0.pdf (Zugriff am 28. März 2020).

Huizing, Albert G./ Bloemen, Axel F. (1996). An Efficient Scheduling Algorithm for a Multifunction Radar, in: IEEE (Hg.), IEEE International Symposium on Phased Array Systems and Technology - Revolutionary Developments in Phase Arrays, 359–364.

IARPA (2018): Prize Challenges. Mercury Challenge. https://www.iarpa.gov/index.php/working-with-iarpa/prize-challenges/1118-mercury-challenge (Zugriff am 02. September 2020).

IDF, Israeli Defense Forces (2018): IDF machines are outsmarting humans, 04. Februar 2018. https://www.idf.il/en/minisites/technology-and-innovation/idf-machines-are-outsmarting-humans/ (Zugriff am 15. November 2019).

IDF (2017a). The IAF's Innovation Department is Building the Startup Culture We All Need, 17.Juni 2017. https://www.idf.il/en/minisites/technology-and-innovation/the-iaf-s-innovation-department-is-building-the-startup-culture-we-all-need/ (Zugriff am 15. November 2019).

IDF (2017b). The IDF Sees Artificial Intelligence as the Key to Modern-Day Survival, 27. Juni 2017. https://www.idf.il/en/minisites/technology-and-innovation/the-idf-sees-artificial-intelligence-as-the-key-to-modern-day-survival/ (Zugriff am 15. Dezember 2019).

IDF (2016a). These 5 Advanced Tools Keep Our Borders Safe, 10. Januar 2016. https://www.idf.il/en/minisites/technology-and-innovation/these-5-advanced-tools-keep-our-borders-safe/ (Zugriff am 10. Oktober 2019).

IDF (2016b). This IDF Startup Could Change the Battlefield Forever, 01. März 2016. https://www.idf.il/en/minisites/technology-and-innovation/this-idf-startup-could-change-the-battlefield-forever/ (Zugriff am 25. Dezember 2019).

IDF (2014). 5 Most Innovative Weapons the IDF Has to Offer (That We Can Tell You About), 20. April 2014. https://www.idf.il/en/minisites/technology-and-innovation/5-most-innovative-weapons-the-idf-has-to-offer-that-we-can-tell-you-about/ (Zugriff am 10. Oktober 2019).

IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems (2019). Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems. https://standards.ieee.org/content/ieee-standards/en/industry-connections/ec/autonomous-systems.html (Zugriff am 13. Dezember 2020).

ILW, Institute of Landwarfare (2017). Integrating Army Robotics and Autonomous Systems to Fight and Win. Arlington. https://www.ausa.org/sites/default/files/publications/SL-17-2-Integrating-Army-Robotics-and-Autonomous-Systems-to-Fight-and-Win.pdf (Zugriff am 15. November 2019).

Instagram Engineering (2012). Sharding & IDs at Instagram, 30. Dezember 2012. https://instagram-engineering.com/sharding-ids-at-instagram-1cf5a71e5a5c (Zugriff am 01. Februar 2021).

Interfax (2018). Armed Forces using cutting-edge technology – Russian Defense Ministry. Interfax, 16. März 2018.

Interfax (2015). Military robots develop ability to independently accomplish their missions. Interfax, 19. Oktober 2015.

Israel Defense (2017). The Future of Artificial Intelligence in the IDF. Israel Defense, 07. Februar 2017. https://www.israeldefense.co.il/en/node/30189 (Zugriff am 10. Oktober 2019).

Israel Innovation Authority (2019). 2018–19. Innovation in Israel overview. https://innovationisrael.org.il/en/sites/default/files/2018-19_Innovation_Report.pdf (Zugriff am 15. April 2020).

Kang, Xudong /Zhang, Xiangping /Li, Shutao/ Li, Kenli/ Li, Jun/ Benediktsson, Jon Atli (2017). Hyperspectral Anomaly Detection with Attribute and Edge-Preserving Filters. IEEE Transactions on Geoscience and Remote Sensing, 55(10): 5600–5611. https://doi.org/10.1109/TGRS.2017.2710145 (Zugriff am 01. Februar 2021).

Kania, Elsa B. (2018). The AI Titans' Security Dilemmas, in: Hoover Institution (Hg.), Governance in an emerging new world. Fall Series 2018. https://www.hoover.org/research/ai-titans (Zugriff am 15. Dezember 2019).

Kania, Elsa B. (2017). Chinese Advances in Unmanned Systems and the Military Applications of Artificial Intelligence – the PLA's Trajectory towards Unmanned, „Intelligentized" Warfare. Testimony before the U.S.-China Economic and Security Review Commission, 23. Februar 2017. https://www.uscc.gov/sites/default/files/Kania_Testimony.pdf (Zugriff am 15. Oktober 2019).

Keller, John (2018). Efficient artificial intelligence (AI) and machine learning models are focus of DARPA LwLL program. Military & Aerospace Electronics, 07. August 2018. https://www.militaryaerospace.com/computers/article/16726485/efficient-artificial-intelligence-ai-and-machine-learning-models-are-focus-of-darpa-lwll-program (Zugriff am 02. September 2020).

Kelly, Éanna (2019). Israel sets out to become the next major artificial intelligence player. Science Business, 02. Juli 2019. https://sciencebusiness.net/news/israel-sets-out-become-next-major-artificial-intelligence-player (Zugriff am 15. Dezember 2019).

Kempinski, Yoni (2019). IDF reveals technology behind its latest combat vehicles. Arutz Sheva 7, 04. August 2019. https://www.israelnationalnews.com/News/News.aspx/266911 (Zugriff am 10. November 2019).

Kimmel, Troy S. (2009). Overview of AEGIS: Overview of AEGIS. Naval Engineers Journal, 121(3): 27–35. https://doi.org/10.1111/j.1559-3584.2009.00202.x (Zugriff am 01. Februar 2021).

Knight, Will. (2019). Military Artificial Intelligence Can Be Easily and Dangerously Fooled. MIT Technology Review, 21. Oktober 2019. https://www.technologyreview.com/s/614497/military-artificial-intelligence-can-be-easily-and-dangerously-fooled/ (Zugriff am 01. Februar 2021).

König, Lucie (2017). Autonome Waffensysteme und das Humanitäre Völkerrecht. IFAR² Factsheet Nr. 11, Dezember 2017. https://ifsh.de/file-IFAR/pdf_english/IFAR2-FactSheet11.pdf (Zugriff am 14. Dezember 2019).

Korbet, Rinat (2019). Start-Up Nation Central: Finder Insights Series. The State of the Israeli Ecosystem in 2018. Start-up Nation Central. https://www.tresor.economie.gouv.fr/PagesInternationales/Pages/c6e8453d-93e0-4a99-ab14-d35e4e331d58/files/8da3fa7a-b903-4b96-a90b-d740ef193c71 (Zugriff am 05. Januar 2020).

Kühne, Sylvia (2020). Das Versprechen von Künstlicher Intelligenz. Erste Ergebnisse einer Untersuchung zu Erwartungen an modernen Waffensysteme. IFSH Research Report 3. Hamburg. https://ifsh.de/file/publication/Research_Report/003/20200525_IFSH_Research_Report_003_KI.pdf (Zugriff am 13. Dezember 2020).

Lehr, David/Ohm, Paul (2017): Playing with the Data: What Legal Scholars Should Learn About Machine Learning. University of California Davis Law Review, 51: 653–717.

Leon, Harmon (2019). Top secret military-grade surveillance drones might be coming to your neighborhood. Observer, 28. Juni 2019. https://observer.com/2019/06/gorgon-stare-aerial-surveillance-drones/ (Zugriff am 01. Februar 2021).

Lobe, Adrian (2019). Rage against the Machine. ZeitOnline, 21. Januar 2019. https://www.zeit.de/kultur/2019-01/kuenstliche-intelligenz-widerstand-angriffe-usa/komplettansicht?p (Zugriff am 13. Dezember 2020).

Loquercio, Antonio/ Maqueda, Ana I./ Blanco, Carlos R./ Scaramuzza, Davide (2018). DroNet: Learning to Fly by Driving. IEEE Robotics and Automation Letters, 3(2): 1088–95. https://doi.org/10.1109/LRA.2018.2795643 (Zugriff am 01. Februar 2021).

Luger, George F. (2009). Artificial Intelligence. Structures and Strategies for Complex Problem Solving. Boston et al.: Pearson/ Addison Wesley.

Manolakis, Dimitris/ Shaw, Gary (2002). Detection algorithms for hyperspectral imaging applications. IEEE Signal Processing Magazine 19(1): 29–43. https://doi.org/10.1109/79.974724 (Zugriff am 01. Februar 2021).

Martinage, Robert (2014). Toward a new Offset Strategy. Exploiting U.S. Global Power Projection Capability. Center for Strategic and Budgetary Assessements, 27. Oktobter 2014. https://csbaonline.org/research/publications/toward-a-new-offset-strategy-exploiting-u-s-long-term-advantages-to-restore/publication/1 (Zugriff am 20. Januar 2019).

Martinez-Ruiz, Manuel/ Artes-Rodriguez, Antonio/ Diaz-Rico, Jose Antonio/ Fuentes, Jose Blanco (2010). New initiatives for imagery transmission over a tactical data link. A case study: JPEG2000 compressed images transmitted in a Link-16 network. method and results, in: IEEE (Hg.): MILCOM, Military Communications Conference, 1163–1168. https://doi.org/10.1109/MILCOM.2010.5680102 (Zugriff am 01. Februar 2021).

Mayring, Philipp (2015). Qualitative Inhaltsanalyse. Grundlagen und Techniken. Weinheim:

Beltz.

McCarthy, John/ Minsky, Marvin L./ Rochester, Nathaniel/ Shannon, Claude E. (1955): A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence. AI Magazine, 27(4): 12. https://doi.org/10.1609/aimag.v27i4.1904 (Zugriff am 01. Oktober 2020).

McLain, Christopher/ King, Janet (2017). Future Ku-Band Mobility Satellites, in ARC (Hg.), 35th AIAA International Communications Satellite Systems Conference. Trieste. https://doi.org/10.2514/6.2017-5412 (Zugriff am 01. Februar 2021).

Mena, Middle East and North Africa Financial Network (2019). Lebanese researchers apply tech solutations to clearing landmines. Mena, 27. Januar 2019. https://menafn.com/1098028950/Lebanese-researchers-apply-tech-solutions-to-clearing-landmines (Zugriff am 15. Dezember 2019).

Meyer, Roland (2019). Operative Porträts: Eine Bildgeschichte der Identifizierbarkeit von Lavater bis Facebook. Konstanz: Konstanz University Press.

Moisejevs, Ilja (2019). Poisoning attacks on Machine Learning. Towards Data Science, 15. Juli 2019. https://towardsdatascience.com/poisoning-attacks-on-machine-learning-1ff247c254db (Zugriff am 19. August 2020).

Motta, Alexandre A./ Ebecken, Nelson/ Alves, Alexandre Soares (2007). Data Mining in Military Systems, in: Brebbia, Carlos A./ Ders. (Hg.): Computational Balistics III. Southampton/ Boston: WIT Press, 171 –180.

NAF, New America Foundation (2017). How We Became a World of Drones. https://www.newamerica.org/in-depth/world-of-drones/1-introduction-how-we-became-world-drones/ (Zugriff am 06. Oktober 2019).

NITRD, The Networking & Information Technology Research & Development Program (2019). Supplement to the President's FY 2020 Budget. https://www.whitehouse.gov/wp-content/uploads/2019/09/FY2020-NITRD-AI-RD-Budget-September-2019.pdf (Zugriff am 15. Dezember 2019).

NITRD (2016). Supplement to the President's Budget. FY 2017. https://www.nitrd.gov/pubs/2017supplement/fy2017nitrdsupplement.pdf (Zugriff am 15. Oktober 2019).

ODNI, Office of the Director of National Intelligence (2018): The AIM Strategy. A Strategy for augmenting Intelligence using Machines. https://www.dni.gov/index.php/newsroom/reports-publications/item/1940-the-aim-initiative-a-strategy-for-augmenting-intelligence-using-machines (Zugriff am 15. Oktober 2019).

OECD (2019). Künstliche Intelligenz in der Gesellschaft. Übersetzung durch den Deutschen Übersetzungsdienst der OECD. https://www.oecd-ilibrary.org/sites/6b89dea3-de/1/3/1/index.html?itemId=/content/publication/6b89dea3-de&_csp_=7dfea12ebf9400c9232c9e0f2adbd5cd&itemIGO=oecd&itemContentType=book#section-d1e763 (Zugriff am 13. September 2020).

Office of the President of the Russian Federation (2019). Decree on the Development of Artificial Intelligence in the Russian Federation. Übersetzung von Etcetera Language Group, Inc. im Auftrag des Center for Security and Emerging Technology. https://cset.georgetown.edu/wp-content/uploads/t0060_Russia_AI_strategy_EN-1.pdf (Zugriff am 05. Oktober 2019).

Orwat, Carsten (2019). Diskriminierungsrisiken durch Verwendung von Algorithmen. Herausgegeben von der Antidiskriminierungsstelle des Bundes. Berlin: Nomos.

OSD, Office of the Secretary of Defense (2019). Annual Report to Congress: Military and Secur-

ity Developments Involving the People's Republic of China 2019. https://media.defense.gov/2019/May/02/2002127082/-1/-1/1/2019_CHINA_MILITARY_POWER_REPORT.pdf (Zugriff am 18. November 2019).

Planungsamt der Bundeswehr (2013). Future Topic. Weiterentwicklungen in der Robotik durch Künstliche Intelligenz und Nanotechnologie. Welche Herausforderungen und Chancen erwarten uns? Berlin. https://www.bundeswehr.de/resource/blob/140532/4c704dc7af37a4d867a2b0663748e470/robotik-data.pdf (Zugriff am 13. September 2020).

Porche, Isaac R./ Wilson, Bradley/ Johnson, Erin-Elizabeth/ Tierney, Shane/ Saltzman, Evan (2014). Data Flood. Helping the Navy address the Rising Tide of Sensor Information. Santa Monica et al.: RAND Corporation.

Prainsack, Barbara (2019). Logged out: Ownership, exclusion and public value in the digital data and information commons. Big Data & Society, 6(1): 1–15.

Rapaport, Amir (2018). A.I. Superpower in the Making. Israel Defense, 28. September 2018. https://www.israeldefense.co.il/en/node/35798 (Zugriff am 13. Dezember 2019).

Redmon, Joseph/ Farhadi, Ali (2016). YOLO9000: Better, Faster, Stronger. Cornell University. http://arxiv.org/abs/1612.08242 (Zugriff am 01. Februar 2021).

Retti, Johannes (1986). Einleitung, in: Ders./Bibel, Wolfgang/ Buchberger, Bruno/ Buchberger, Ernst/ Horn, Werner/ Kobsa, Alfred/ Steinacker, Ingeborg/ Trappl, Robert/ Trost, Harald (Hg.), Artificial Intelligence – Eine Einführung. Stuttgart: B. G. Teubner, 1–6.

Rickli, Jean-Marc (2019). The destabilizing prospects of artificial intelligence for nuclear strategy, deterrence and stability, in: Boulanin, Vincent (Hg.), The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk. Volume I. Euro-Atlantic Perspectives. Solna: SIPRI, 91–98.

Roberge, Jonathan/ Senneville, Marius/ Morin, Kevin (2020). How to translate artificial intelligence? Myths and justifications in public discourse. Big Data & Society, 7(1): 1–13.

Rojkes Dombe, Ami (2019). The Next Generation: Tank Weapon Sights with AI Capabilities. Israel Defense, 23.August 2019. https://www.israeldefense.co.il/en/node/39881 (Zugriff am 12. Oktober 2019).

Roland Berger GmbH & Asgard Human Venture Capital (2018). Artificial Intelligence – A strategy for European startups Recommendations for policymakers. https://www.rolandberger.com/publications/publication_pdf/roland_berger_ai_strategy_for_european_startups.pdf (Zugriff am 14. Oktober 2019).

Russell, Stuart/ Norvig, Peter (2016): Artificial Intelligence: A Modern Approach. Boston et al.: Pearson.

Russell, Stuart/ Norvig, Peter/ Davis, Ernest/ Edwards, Douglas (2010). Artificial Intelligence: A Modern Approach. Upper Saddle River: Prentice Hall.

Ryan, Thomas/ Mittal, Vikram (2019). Potential for Army Integration of Autonomous Systems by Warfighting Function. Military Review, September-October. https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/SO-19/Mittal-Autonomous-Systems.pdf (Zugriff am 15. Januar 2020).

Sadowski, Jathan (2019). When data is capital: Datafication, accumulation, and extraction. Big Data & Society, January–June: 1–2.

SASC, Senate Armed Services Committee (2019). Statement by Michael Brown, Director of the Defense Innovation Unit, Before the Senate Armed Services Committee. Subcommittee on

Emerging Threats and Capabilities on „Artificial Intelligence Initiatives within the Defense Innovation Unit", 12. März 2019. https://www.armed-services.senate.gov/imo/media/doc/Brown_03-12-19.pdf (Zugriff am 13. Dezember 2019).

Sato, Kaz/ Young, Cliff/ Patterson, David (2017). An in-Depth Look at Google's First Tensor Processing Unit (TPU). Google Cloud, 12. Mai 2017. https://cloud.google.com/blog/products/gcp/an-in-depth-look-at-googles-first-tensor-processing-unit-tpu/ (Zugriff am 01. Februar 2021).

Sayler, Kelley M./ Hoadley, Daniel S. (2019). Artificial Intelligence and National Security. Updated 21. November 2019. Congressional Research Service. https://fas.org/sgp/crs/natsec/R45178.pdf (Zugriff am 14. Januar 2020).

Scharre, Paul (2017). The Lethal Autonomous Weapons Governmental Meeting, Part 1: Coping with Rapid Technological Change. Just Security, 09. November 2017. https://www.justsecurity.org/46889/lethal-autonomous-weapons-governmental-meeting-part-i-coping-rapid-technological-change/ (Zugriff am 14. Januar 2020).

Schmitt, Marwin/ Redi, Judith/ Cesar, Pablo/ Bulterman, Dick (2016). 1Mbps Is Enough: Video Quality and Individual Idiosyncrasies in Multiparty HD Video-Conferencing, in IEEE (Hg.), 2016 Eight International Conference on Quality of Multimedia Experience (QoMEX), 1–6. https://doi.org/10.1109/QoMEX.2016.7498961 (Zugriff am 01. Februar 2021).

Sheppard, Lindsey R./ Hunter, Andrew Philip/ Karlen, Robert/ Balieiro, Leonardo (2018). Artificial Intelligence and National Security. The Importance of the AI Ecosystem. A Report of the CSIS Defense-Industrial Initiatives Group. Washington: CSIS. https://www.csis.org/analysis/artificial-intelligence-and-national-security-importance-ai-ecosystem (Zugriff am 11. Oktober 2020).

Shi, Xinchu/ Ling, Haibin/ Blasch, Erik/ Hu, Weiming (2012). Context-driven moving vehicle detection in wide area motion imagery, in IEEE (Hg.), Conference Proceedings 1, 2512–2515. https://www.computer.org/csdl/pds/api/csdl/proceedings/download-article/12OmNC943Ox/pdf (Zugriff am 02. Februar 2021).

Shoker, Sarah (2019). Algorithmic Bias and the Principle of Distinction: Towards an Audit of Lethal Autonomous Weapons Systems. Working Paper. https://www.academia.edu/41125332/Algorithmic_Bias_and_the_Principle_of_Distinction_Towards_an_Audit_of_Lethal_Autonomous_Weapons_Systems (Zugriff am 12. Mai 2020).

SIPRI (2019). SIPRI Yearbook 2019. Armaments, Disarmament and International Security. Kurzfassung auf Deutsch. Friedrich Ebert Stiftung/Berghof Foundation. Verfügbar unter: https://sipri. org/sites/default/files/2019-11/yb19_summary_de.pdf (Zugriff am 10. Februar 2020).

Song, Xiao/ Ma, Yaofei/ Wu, Yulin/ Cui, Yong (2015). Military Simulation Big Data: Background, State of the Art, and Challenges. Mathematical Problems in Engineering, 2015(1): 1–20.

Spencer, David K., Duncan/ Stephen/ Taliaferro, Adam (2019). Operationalizing artificial intelligence for multi-domain operations: a first look. Proc. SPIE 11006, Artificial Intelligence and Machine Learning for Multi-Domain Operations Applications, 1100602. https://www.spiedigitallibrary.org/conference-proceedings-of-spie/11006/1100602/Operationalizing-artificial-intelligence-for-multi-domain-operations--a-first/10.1117/12.2524227.short?SSO=1 (Zugriff am 10. Dezember 2019).

State Council. The People's Republic of China (2019). China's National Defense in the New Era. The State Council Information Office of the People's Republic of China. Foreign Languages

Press Co.: Beijing. http://www.andrewerickson.com/wp-content/uploads/2019/07/China-Defense-White-Paper_2019_English.doc (Zugriff am 16. Dezember 2019).

State Council. The People's Republic of China (2017a). New Generation of Artificial Intelligence Development Plan. Übersetzung von Sapio, Fora/ Chen, Weiming/ Lo, Adrian. https://flia.org/notice-state-council-issuing-new-generation-artificial-intelligence-development-plan/ (Zugriff am 18. November 2019).

State Council. The People's Republic of China (2017b). Three-Year Action Plan for Promoting Development of a New Generation Artificial Intelligence Industry (2018–2020). Übersetzung von Triolo, Paul/ Kania, Elsa/ Webster, Graham. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinese-government-outlines-ai-ambitions-through-2020/ (Zugriff am 10. Dezember 2019).

State Council. The People's Republic of China (2016). The 13th Five-Year Plan on National Economic and Social Development of The People's Republic of China. 2016-2020. Übersetzung durch Compilation and Translation Bureau, Central Committee of the Communist Party of China. https://en.ndrc.gov.cn/newsrelease_8232/201612/P020191101481868235378.pdf (Zugriff am 18. November 2019).

Steinacker, Ingeborg (1986). Intelligente Maschinen?, in: Retti, Johannes/ Bibel, Wolfgang/ Buchberger, Bruno/ Buchberger, Ernst/ Horn, Werner/ Kobsa, Alfred/ Dies./ Trappl, Robert/ Trost, Harald et al.: Artificial Intelligence – Eine Einführung. Stuttgart: B. G. Teubner: 7–28.

Stone, Peter et al. (2016). Artificial Intelligence and Life in 2030. One Hundred Year Study on Artificial Intelligence. Report of the 2015-2016 Study Panel, Standford University, Standford, CA, September 2016. http://ai100.stanford.edu/2016-report (Zugriff am 13. September 2020).

Swart, Garret (2004). Spreading the load using consistent hashing: A preliminary report, in: IEEE (Hg.), Third International Symposium on Parallel and Distributed Computing/Third International Workshop on Algorithms, Models and Tools for Parallel Computing on Heterogeneous Networks, 169–176. https://doi.org/10.1109/ISPDC.2004.47 (Zugriff am 01. Februar 2021).

T**aghipour, Ashkan/ Ghassemian, Hassan** (2017). Hyperspectral Anomaly Detection Using Attribute Profiles. IEEE Geoscience and Remote Sensing Letters 14(7): 1136–40. https://doi.org/10.1109/LGRS.2017.2700329 (Zugriff am 01. Februar 2021).

Tangermann, Michael (2019). Maschinelles Lernen, in: Liggieri, Kevin/ Müller, Oliver (Hg.). Mensch-Maschine-Interaktion, Handbuch zu Geschichte – Kultur – Ethik. J. B. Metzler Verlag, 283–285.

Tass (2019a): Russia to invite over 130 foreign delegations to attend Army-2020 forum. Tass, 13. November 2019. https://tass.com/defense/1088423 (Zugriff am 15. November 2019).

Tass (2019b): Putin believes use of AI in defense sector should be extended. Tass, 22. November 2019. https://tass.com/defense/1091901 (Zugriff am 12. Dezember 2019).

Tass (2019c). Putin: advanced weaponry reaches 82% in Russia's nuclear triad. Tass, 24. Dezember 2019. https://tass.com/defense/1102975 (Zugriff am 03. Januar 2020).

Topychkanov, Petr (2020). Introduction, in: Ders. (Hg.): The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk. Vol. III. South Asian Perspectives. Stockholm: SIPRI, 3–8. https://sipri.org/sites/default/files/2020-04/impact_of_ai_on_strategic_stability_and_nuclear_risk_vol_iii_topychkanov_1.pdf (Zugriff am 01. Mai 2020).

UNODA, United Nations Office for Disarma-

ment Affairs (2017). UNODA Occasional Papers. Nr. 30, November 2107. Perspectives on Lethal Autonomous Weapon Systems. New York. https://www.unog.ch/80256EDD006B8954/(httpAssets)/6866E44ADB996042C12581D400630B9A/$file/op30.pdf (Zugriff am 20. März 2020).

U.S. Air Force (2019). Artificial Intelligence Annex to The Department of Defense Artificial Intelligence Strategy. https://www.af.mil/Portals/1/documents/5/USAF-AI-Annex-to-DoD-AI-Strategy.pdf (Zugriff am 15. März 2019).

U.S. Air Force Office of the Chief Scientist (2015). Autonomous Horizons. System Autonomy in the Air Force – A Path to the Future. Volume I: Human-Autonomy Teaming. https://www.af.mil/Portals/1/documents/SECAF/AutonomousHorizons.pdf (Zugriff am 15. Dezember 2019).

U.S. Army (2019a). Army Modernization Strategy: Investing in the Future Strategy. https://www.army.mil/e2/downloads/rv7/2019_army_modernization_strategy_final.pdf (Zugriff am 12. Dezember 2019).

U.S. Army (2019b). The Operational Environment and the Changing Character of Warfare. TRADOC Pamphlet 525-9. https://adminpubs.tradoc.army.mil/pamphlets/TP525-92.pdf (Zugriff am 12. Januar 2020).

U.S. Army (2018). The U.S. Army in Multi-Domain Operations 2028. United States. Army Training and Doctrine Command. 6. Dezember 2018. https://info.publicintelligence.net/**US Army**-MultidomainOps2028.pdf (Zugriff am 05. März 2020).

U.S. Army (2017a). The U.S. Army Functional Concept for Intelligence. 2020-2040. TRADOC Pamphlet 525-2-1. https://adminpubs.tradoc.army.mil/pamphlets/TP525-2-1.pdf (Zugriff am 12. April 2019).

U.S. Army (2017b). Robotic and Autonomous Systems Strategy. Maneuver, Aviation, and Soldier Division Army Capabilities Integration Center. U.S. Army Training and Doctrine Command. Fort Eustis. https://www.tradoc.army.mil/Portals/14/Documents/RAS_Strategy.pdf (Zugriff am 15. Februar 2020).

U.S. Army (2003). Mission Command: Command and Control of Army Forces. Field Manual No. 6–3. Washington: Department of the Army. https://www.bits.de/NRANEU/others/amd-us-archive/fm6(03).pdf (Zugriff am 01. Februar 2021).

Venkateswaran, Narayanan/ Changder, Suvamoy (2017). Simplified data partitioning in a consistent hashing based sharding implementation, in: IEEE (Hg.): TENCON 2017 - 2017 IEEE Region 10 Conference, 895–900. https://doi.org/10.1109/TENCON.2017.8227985 (Zugriff am 01. Februar 2021).

White House (2019a). National Artificial Intelligence Research and Development Strategic Plan: 2019 Update. https://www.whitehouse.gov/wp-content/uploads/2019/06/National-AI-Research-and-Development-Strategic-Plan-2019-Update-June-2019.pdf (Zugriff am 14. Dezember 2019).

White House (2019b). 2016–2019 Progress Report: Advancing Artificial Intelligence R&D. https://www.whitehouse.gov/wp-content/uploads/2019/11/AI-Research-and-Development-Progress-Report-2016-2019.pdf (Zugriff am 14. Dezember 2019).

White House (2017a): National Security Strategy of the United States. https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905-2.pdf (Zugriff am 13. Dezember 2019).

White House (2017b). Presidential Memorandum for the Secretary of Transportation, 25. Oktober 2017. https://www.whitehouse.gov/presidential-actions/presidential-memorandum-sec-

retary-transportation/ (Zugriff am 12. November 2019).

White House (2016a). Preparing for the Future of Artificial Intelligence. https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf (Zugriff am 12. November 2019).

White House (2016b). The National Artificial Intelligence Research and Development Strategic Plan. https://www.nitrd.gov/news/national_ai_rd_strategic_plan.aspx (Zugriff am 12. November 2019).

Wiegand, Thomas/ Sullivan, Gary J./ Bøntegaard, Gisle/ Luthra, Ajay (2003). Overview of the H.264/AVC video coding standard. IEEE Transactions on Circuits and Systems for Video Technology, 13(7): 560–576. https://doi.org/10.1109/TCSVT.2003.815165 (Zugriff am 01. Februar 2021).

Winston, Patrick Henry (1993): Artificial Intelligence. Reading MA et al.: Addison-Wesley Publishing Company.

Wu, Sijie/ Zhang, Kai/ Niu, Saisai/ Yan, Jie (2019). Anti-interference aircraft-tracking method in infrared imagery. Sensor, 19(6): 1289.

Zebrowski, Chris (2016). The Value of Resilience: Securing Life in the 21st Century. Abingdon, Oxon: Routledge.

Zelaya, David/ Keeley, Nicholas (2020). The Input-Output Problem: Managing the Military's Big Data in the Age of AI. War on the Rocks, 13. Februar 2020. https://warontherocks.com/2020/02/the-input-output-problem-managing-the-militarys-big-data-in-the-age-of-ai/ (Zugriff am 14. Oktober 2020).

Zhao, Rui/ Du, Bo/ Zhang, Liangpei (2017). Hyperspectral Anomaly Detection via a Sparsity Score Estimation Framework. IEEE Transactions on Geoscience and Remote Sensing 55(6): 3208–22. https://doi.org/10.1109/TGRS.2017.2664658 (Zugriff am 01. Februar 2021).

Zweig, Katharina/ Fischer, Sarah/ Lischka, Konrad (2018). Wo Maschinen irren können. Fehlerquellen und Verantwortlichkeiten in Prozessen algorithmischer Entscheidungsfindung. Arbeitspapier. Gütersloh: Bertelsmann Stiftung. https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/WoMaschinenIrrenKoennen.pdf (Zugriff am 15. November 2020).

Über die Autor*innen

Dr. Christian Alwardt
Dr. Christian Alwardt ist Physiker und Experte für Technikfolgenabschätzung, Rüstungskontrolle sowie für friedens- und sicherheitspolitische Fragestellungen. Seit 2008 forschte er u.a. am Institut für Friedensforschung und Sicherheitspolitik (IFSH) und der Universität Hamburg zu strategischer Stabilität, nuklearer Proliferation, zur Digitalisierung und Technologisierung der Kriegsführung (unbemannte Systemen, Weltraumbewaffnung, Cyber-Sicherheit, Raketenabwehr, Künstliche Intelligenz etc.) sowie zu den Folgen des Klimawandels. Am IFSH war Christian Alwardt zuletzt in einem Beratungsprojekt für das Auswärtige Amt beschäftigt und leitete das DSF-Projekt zu „Algorithmen und Künstliche Intelligenz als Game Changer? Moderne Waffensysteme zwischen Erwartung und Wirklichkeit". Mit seiner ausgewiesenen Expertise ist Christian Alwardt sowohl als Berater für politische Entscheidungsträger tätig als auch Ansprechpartner für Medien und die Öffentlichkeit. Christian Alwardt ist Mitglied der Vereinigung Deutscher Wissenschaftler (VDW), des Forschungsverbundes Naturwissenschaft, Abrüstung und internationale Sicherheit (FONAS) sowie der Deutschen Physikalischen Gesellschaft (DPG).
Kontakt: christian.alwardt@gmx.net

Dr. Sylvia Kühne
Dr. Sylvia Kühne ist Soziologin und hat in der Kriminologie zur Akzeptanz von Fingerabdrucktechnologien an der Universität Hamburg promoviert. Sie beschäftigt sich in ihrer Arbeit insbesondere mit techniksoziologischen Fragestellungen im Kontext von (digitalen) Sicherheitstechnologien, wie z.B. biometrischen Verfahren im Besonderen oder Künstlicher Intelligenz im Allgemeinen, und hat an unterschiedlichen Projekten an der Uni Essen und dem Institut für Friedensforschung und Sicherheitspolitik (IFSH) an der Universität Hamburg mitgewirkt. Als wissenschaftliche Mitarbeiterin an der RWTH Aachen University hat sie zuletzt zu Verfahren der Täuschungsdetektion im Projekt „Soziotechnische Systeme der antizipatorischen Wahrheitsverifikation im Feld der Flughafensicherheit" (gefördert durch DFG) geforscht."
Kontakt: skuehne@soziologie.rwth-aachen.de

DSF
Am Ledenhof 3-5
49074 Osnabrück
+49 541 60035-42
www.bundesstiftung-friedensforschung.de
info@bundesstiftung-friedensforschung.de
ISSN 2193-794X