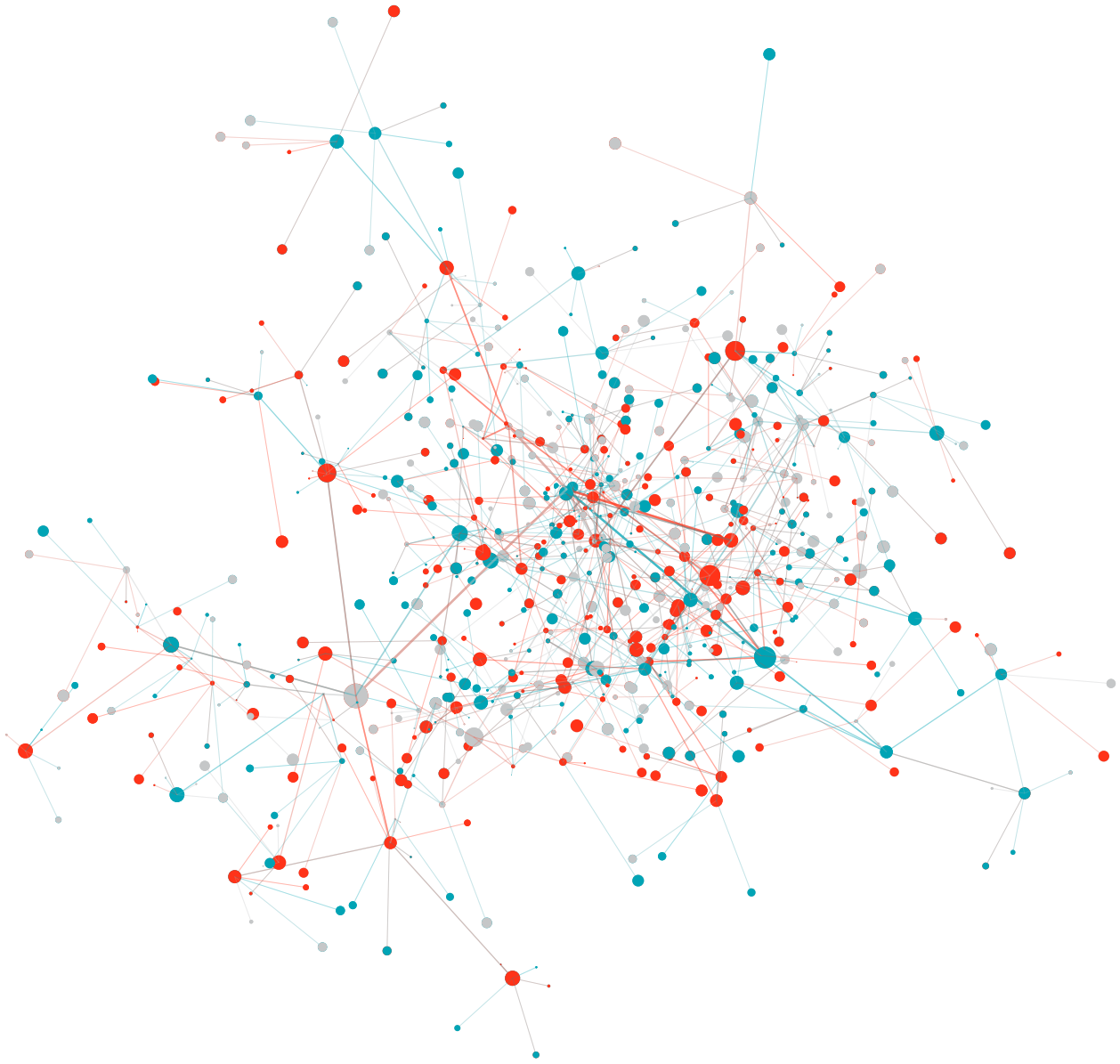
STUDIEN

ROSA LUXEMBURG STIFTUNG

LUCAS MAASER
UND STEPHANIE VERLAAN

BIG TECH ZIEHT IN DEN KRIEG

EINSICHTEN IN DIE WACHSENDE ROLLE US-AMERIKANISCHER UND EUROPÄISCHER TECHNOLOGIEFIRMEN IM MILITÄRISCH-INDUSTRIELLEN-KOMPLEX



LUCAS MAASER UND STEPHANIE VERLAAN

BIG TECH ZIEHT IN DEN KRIEG

EINSICHTEN IN DIE WACHSENDE ROLLE US-AMERIKANISCHER UND EUROPÄISCHER TECHNOLOGIEFIRMEN IM MILITÄRISCH-INDUSTRIELLEN-KOMPLEX

Studie im Auftrag der Rosa-Luxemburg-Stiftung

LUCAS MAASER ist Programmmitarbeiter der NGO Corruption Tracker. Nach seinem Studium im Fach Interkulturelles Konfliktmanagement war er als Koordinator im International Peace Bureau (IPB) tätig. Im Mittelpunkt seiner Forschungsarbeiten stehen die Themen Korruption, postkoloniale Perspektiven auf die Außenpolitik und der militärisch-industrielle Komplex.

STEPHANIE VERLAAN arbeitete zuletzt als Koordinatorin im International Peace Bureau (IPB). Nach dem Erwerb eines Masters im Fach Interkulturelles Konfliktmanagement schließt sie derzeit ihr Studium im Fachgebiet Internationale Menschenrechte und humanitäres Recht ab. Verlaan ist Mentee im Young Women in Non-Proliferation and Disarmament Mentorship Program des Europäischen Konsortiums für Nichtverbreitung und Abrüstung. Ihre Forschung konzentriert sich auf Massenvernichtungswaffen, Abschreckung und «Gemeinsame Sicherheit».

IMPRESSUM
STUDIEN 4/2022
wird herausgegeben von der Rosa-Luxemburg-Stiftung
V. i. S. d. P.: Albert Scharenberg
Straße der Pariser Kommune 8A · 10243 Berlin · www.rosalux.de
ISSN 2194-2242 · Redaktionsschluss: November 2022
Illustration Titelseite: Frank Ramspott/iStockphoto
Übersetzung: Gegensatz Translation Collective
Korrektorat: TEXT-ARBEIT, Berlin
Layout/Herstellung: MediaService GmbH Druck und Kommunikation
Gedruckt auf Circleoffset Premium White, 100 % Recycling

Erstellt mit finanzieller Unterstützung des Auswärtigen Amtes (AA). Für diese Publikation ist allein die Herausgeberin verantwortlich. Die hier dargestellten Positionen geben nicht den Standpunkt des Zuwendungsgebers wieder. Die Publikation wird kostenlos abgegeben und darf nicht zu Wahlkampfzwecken verwendet werden.

ABSTRACT

Die vorliegende Studie untersucht verschiedene Vertragsbeziehungen zwischen dem globalen Verteidigungssektor und den mächtigsten privaten Technologieunternehmen der Welt sowie die Auswirkungen dieser Beziehungen auf den sich entfaltenden militärisch-industriellen Komplex (MIK). Ein Großteil der Fallstudien konzentrierte sich auf den Verteidigungsbereich der USA, da diese über den größten Verteidigungshaushalt der Welt verfügen, während die anschließende Diskussion darüber hinaus die Entwicklung der Beziehungen im europäischen Kontext betrachtet. Zu den in die Untersuchung einbezogenen Vertragsprojekten gehören Project Maven (Google LLC), JEDI (Microsoft, AWS), JWCC (Microsoft, AWS, Oracle, Google Cloud) und GAIA-X (ein Konsortium aus über 300 europäischen und internationalen Unternehmen). Die Untersuchung wurde anhand von vier Interviews sowie von aktueller, einschlägiger Literatur und relevanten Medienbeiträgen erarbeitet. Zwei der Interviews wurden mit aktivistischen Forscher*innen aus zivilgesellschaftlichen Organisationen mit einem entsprechenden Fokus und zwei mit ehemaligen Google-Mitarbeiter*innen geführt. Die Studie befasst sich mit den Folgen der Zusammenarbeit zwischen dem Verteidigungssektor und Tech-Unternehmen und bezieht sowohl den «Krieg gegen den Terror» als auch Dual-Use-Technologien, digitale Bias und Anhaltspunkte dafür mit ein, dass sich mit der Expansion des Silicon Valley über die USA hinaus ähnliche Trends in Europa fortsetzen. Ziel der Studie ist es, eine Diskussion im europäischen Kontext anzustoßen und die Aufmerksamkeit der europäischen Zivilgesellschaft auf dieses Thema zu lenken. Als Grundlage dafür können aktivistische Erfahrungen dienen, die in den USA mit den ethischen Auswirkungen dieser Technologieverbreitung ohne ausreichende Aufsichts- und Rechenschaftsmechanismen gemacht wurden.

INHALT

1 EINLEITUNG

Stellen Sie sich vor, Sie werden von Ihrem Arbeitgeber beauftragt, ein Produkt zu entwickeln, das dazu dient, Krieg zu führen oder sogar das Leben eines anderen Menschen zu beenden. Stellen Sie sich vor, der Zweck des Produkts würde Ihnen erst mitgeteilt, nachdem Sie zu seiner Herstellung beigetragen haben. Wären Sie bereit gewesen, mitzuarbeiten, wenn Sie es gewusst hätten? Was würden Sie tun, wenn man von Ihnen verlangen würde, mit niemandem außerhalb des Unternehmens über die Situation zu sprechen? Würden Sie als gewöhnliche*r Zivilist*in weiter für ein Unternehmen arbeiten wollen, das Krieg, das Leiden anderer und den Tod von Menschen befördert?

Bekanntlich nimmt das US-Militär weltweit eine führende Rolle in der Entwicklung modernster Technologien ein. In der Tat wird ihm die Entwicklung des Advanced Research Projects Agency Network (ARPANET) zugeschrieben, das gemeinhin als Prototyp des Internets gilt. Andere Technologien, die ursprünglich für das US-Militär und von ihm entwickelt wurden, wie GPS oder Satellitenbilder, haben unser alltägliches Leben tiefgreifend verändert. In den letzten 30 Jahren wurde das US-Militär jedoch von den wichtigsten Akteuren der privaten Tech-Industrie von seiner Schlüsselposition für technologische Innovation verdrängt.[1] Um auf Augenhöhe mit seinen Kontrahenten zu bleiben, sah sich das Pentagon gezwungen, eine eigene Beziehung zum Silicon Valley aufzubauen.

Um diese Beziehung aufrechtzuerhalten, müssen die staatlichen Stellen umfangreiche finanzielle Mittel zur Verfügung stellen. Im Jahr 2020 belief sich das Budget, das Staaten weltweit für ihre militärischen Aktivitäten aufbrachten, auf 1,981 Billionen US-Dollar. Mit einem Anstieg von 2,6 Prozent gegenüber dem Vorjahr setzt diese Entwicklung angesichts der anhaltenden Corona-Pandemie nicht nur einen langjährigen weltweiten Trend steigender Militärbudgets fort; mit geschätzten 778 Milliarden US-Dollar und einem Anteil von 39 Prozent an den weltweiten Militärausgaben festigen die USA damit ihre Position als unangefochtener Spitzenreiter auf der Liste.

Vorhaben wie das Projekt Maven[2] und die Joint Enterprise Defense Infrastructure (JEDI)[3] zeigen, dass das US-Militär bei der Entwicklung neuer, entscheidungszentrierter militärischer Strategien verstärkt auf Künstliche Intelligenz (KI) setzt und dass die großen Technologieunternehmen bereit sind, zu diesen Bemühungen beizutragen. Dabei werden selbst auferlegte ethische Verpflichtungen wie Googles «Don't be evil»[4] geschickt umgangen, um einen Anteil an den lukrativen Regierungsaufträgen[5] zu erhalten, während gleichzeitig ein altruistisches Image in der Öffentlichkeit gefördert und Talente aus einer politisch bewussteren, liberalen Arbeitnehmer*innenschaft angeworben werden. Zwischen 2004 und 2021 haben allein das US-Heimatschutzministerium und das US-Verteidigungsministerium mehr als 44 Milliarden US-Dollar in die Dienste von Google, Amazon, Facebook, Microsoft und Twitter investiert.[6] Die Bestrebungen des Silicon Valley, enge Beziehungen zu staatlichen Auftraggeber*innen aufzubauen, sind jedoch nicht auf Staatsgrenzen beschränkt, wie ihr Beitrag zur europäischen Cloud-Computing-Initiative GAIA-X zeigt, die von Frankreich und Deutschland vorangetrieben wird.

Während der öffentliche Diskurs über den öffentlich-privaten militärischen Innovationsraum in den USA gereift zu sein scheint und sich dazu eine bemerkenswerte zivilgesellschaftliche Opposition entwickelt hat, scheint es in Europa und Deutschland weitgehend an Strukturen zur Untersuchung dieser Verbindungen zu mangeln. Mit dieser Studie wollen wir mit dem Aufbau entsprechender Ressourcen beginnen und Strategien aufzeigen, mithilfe derer sowohl intransparente Kooperationspraktiken untersucht als auch sinnvolle zivilgesellschaftliche Bündnisse zu deren Beobachtung geschaffen werden können. Unsere Arbeit richtet sich gleichermaßen an Wissenschaftler*innen und Aktivist*innen, Politiker*innen und Privatpersonen, die sich mit Fragen des privat-öffentlichen militärischen Innovationstransfers beschäftigen.

Die drastische Eskalation der Gewalt infolge der aktuellen russischen Invasion in der Ukraine, die am 24. Februar 2022 begann und zum Zeitpunkt der Erstellung dieser Studie noch andauerte, führte zu einer deutlichen Veränderung der traditionell restriktiven deutschen Regierungspolitik in Bezug auf Militärausgaben. Ob die geplante Aufrüstung der deutschen Militärtechnik auch auf KI-Innovationen in Form einer erhöhten Anzahl von Verträgen mit privaten Technologieunternehmen ausgedehnt wird, bleibt abzuwarten, da die Vergabe von Mitteln bislang hauptsächlich für schwere Waffen wie Panzer, Düsenjäger und Munition vorgesehen ist.[7]

In der vorliegenden Untersuchung betrachten wir diese jüngsten Entwicklungen zunächst vor dem Hintergrund der allgemeinen Geschichte der technologischen Innovation im Namen von Verteidigung und Si-

1 Chin, Warren: Technology, war and the state: past, present and future, in: International Affairs 4/2019, S. 765–783, hier S. 770–772; unter: https://academic.oup.com/ia/article/95/4/765/5513164. **2** Peitz, Dirk: Google wird einfach ersetzt, in: Die Zeit, 8.7.2018, unter: www.zeit.de/digital/internet/2018-06/maven-militaerprojekt-google-ausstieg-ruestungsexperte-paul-scharre. **3** Übertroffen von den Joint Warfighter Cloud Capability (JWCC)- und Indefinite Delivery-Indefinite Quantity (IDIQ)-Programmen. Vgl. beispielsweise US Department of Defense: Future of the Joint Enterprise Defense Infrastructure Cloud Contract, 6.7.2021, unter: www.defense.gov/Newsroom/Releases/Release/Article/2682992/future-of-the-joint-enterprise-defense-infrastructure-cloud-contract/. **4** «Tue nichts Böses» war lange Zeit das Motto von Google (Anm. d. Ü.). **5** Vgl. beispielsweise Brewster, Thomas: Google Promised Not To Use Its AI In Weapons, So Why Is It Investing In Startups Straight Out Of ‹Star Wars›?, in: Forbes Magazine, 22.12.2020, unter: www.forbes.com/sites/thomasbrewster/2020/12/22/google-promised-not-to-use-its-ai-in-weapons-so-why-is-alphabet-investing-in-ai-satellite-startups-with-military-contracts/?sh=30ba15537595. **6** Vgl. zu den Daten, die im Rahmen der Kampagne «Big Tech Sells War» veröffentlicht wurden, https://bigtechsellswar.com/. **7** Rauwald, Christoph/Wilkes, William/Patel, Tara: Europe is Re-arming, and Its Defence Firms Stand To Profit, in: Bloomberg Quint, 28.2.2022, unter: www.bloombergquint.com/business/europe-is-rearming-and-its-defense-firms-stand-to-profit.

cherheit, um anschließend aufzuzeigen, wie einige der lukrativsten Verträge zwischen Big-Tech-Firmen und dem US-Militär zum Ausbau der Kriegsmaschinerie beitragen. Dazu haben wir Fallstudien ausgewählt, die sich auf die sogenannten «Big Five» – Google, Apple, Facebook, Amazon und Microsoft – als Hauptvertreter des verbraucherorientierten technologischen Innovationsraums beziehen, und die große Zahl anderer, scheinbar unbedeutenderer privatwirtschaftlicher Akteure hervorgehoben, die an wichtigen Verträgen der letzten Jahre beteiligt waren. In einer Analyse des europäischen und des deutschen Marktes werden außerdem Hintergründe genannt, warum wir uns um die US-amerikanischen Innovationssysteme in unserer Region kümmern sollten und wie sich die Zivilgesellschaft in Vergangenheit organisiert hat, um Widerstand dagegen zu leisten und ihrer Stimme Gehör zu verschaffen.

In unserer Forschung orientierten wir uns an den folgenden vier Hauptfragen:
Welche Formen der Zusammenarbeit gibt es zwischen dem europäischen und US-amerikanischen Verteidigungssektor und den «Big Five»?
Was sind die (potenziellen) negativen Folgen dieser Zusammenarbeit?
Welche Strategien können die Friedens- und andere soziale Bewegungen anwenden, um dieser Entwicklung wirksam zu begegnen?
Welche Bündnisse und Netzwerke lassen sich für zukünftige Projekte und Vorhaben entwickeln?

Die Beschränkung auf die untersuchten fünf großen US-Unternehmen ist in erster Linie dem begrenzten Umfang dieser Studie geschuldet. Andere große Akteure wie IBM und HP Inc. Wurden daher – obwohl sie nicht weniger bedeutend sind – nicht berücksichtigt. Auch wenn wir die vielschichtige Struktur des Informationstechnologiesektors – von Halbleiterherstellern über Anbieter von Telekommunikationsausrüstung bis hin zu Netzwerk-, Anschluss- und Serviceanbietern – anerkennen, ergab die Analyse von Auftragsvergaben sowie von öffentlich zugänglichen Daten keine ausreichenden Bezüge zu diesen Bereichen, weshalb sie im Rahmen dieser Studie nicht berücksichtigt wurden. Da wir mit unserer Studie eine Grundlage für die weitere Untersuchung der in diesem Bereich auftretenden Fragen bieten wollen, laden wir andere Forscher*innen ausdrücklich dazu ein, unsere Arbeit im Hinblick auf diese Gesichtspunkte zu ergänzen.

2 THEORETISCHER RAHMEN

2.1 TECHNOLOGIE, KRIEG UND STAAT – VON DER FRÜHEN NEUZEIT BIS ZUM MILITÄRISCH-INDUSTRIELLEN KOMPLEX (MIK)

Die Verbindung zwischen privater Innovation und militärischer Anwendung ist keine Erscheinung des 21. Jahrhunderts. Um die Strukturen zu verstehen, die durch die Überschneidungen zwischen den beiden Sektoren entstanden sind, werden wir die aktuell zu beobachtenden Phänomene in ihrer historischen Entwicklung betrachten und uns dabei auf Dual-Use-Technologien konzentrieren.

In seiner Untersuchung der Zusammenhänge zwischen Technologie, Krieg und Staat in ihrem historischen Verlauf attestiert Warren Chin eine «synergetische Beziehung»[8] zwischen Kriegshandlungen und dem Wohlergehen des Staates, die dazu führte, dass sich beide von der frühen Neuzeit bis zur Mitte des 20. Jahrhunderts stark entwickelten. Diese für beide Seiten vorteilhafte Beziehung dürfte sich nach dem Zweiten Weltkrieg vordergründig abgeschwächt und Raum für «neue politische und wirtschaftliche Prioritäten»[9] geschaffen haben, die die Rolle des Nationalstaates erheblich beeinflussten. Mit dem entstehenden Gefüge internationaler Institutionen, das sich vor dem Hintergrund der Schrecken des Krieges entwickelte, so Chin, bedeutete diese Entwicklung jedoch eher eine Verschiebung hin zu einer subtileren Form des Krieges, die sich durch die Vermeidung zwischenstaatlicher Konfrontationen und eine erhöhte Komplexität auszeichnet.[10]

Mit der Umstellung auf die nukleare Abschreckungspolitik nahm die Bedeutung von Technologie – neben den Fortschritten in der nuklearen Kriegsführung – erheblich zu. Chin stellt fest, dass «die technologische Entwicklung die Möglichkeiten für einen Krieg verringerte, das dadurch ausgelöste Wettrüsten jedoch auch neue Technologien hervorbrachte, die neue Konfliktformen begünstigten».[11]

In diesem Spannungsfeld übernahmen die Vereinigten Staaten eine Schlüsselrolle bei der Finanzierung technologischer Forschung im Verteidigungsbereich. Dies war keine völlig neue Erscheinung, da die Fortentwicklung militärischer Erfordernisse seit dem Ende des 19. Jahrhunderts zu einem stetig wachsenden Interesse der Staaten an technischen Lösungen geführt hatte.[12] Bis 1945 war die staatlich geförderte Innovation weitgehend an die Anforderungen von Quantität statt Qualität auf dem Schlachtfeld gekoppelt und erforderte «die Mobilisierung der Gesellschaft und der Wirtschaft durch den Staat».[13] Ebenfalls erforderlich war ein Bildungs- und Gesundheitssystem, das die für eine offene Konfrontation nötigen Ressourcen bereitstellte.[14] Im postmodernen Zeitalter hingegen verlagerte sich der Schwerpunkt zunehmend auf eine differenziertere Sichtweise des Krieges, bei der die Grenzen, innerhalb derer sich Frieden und Konflikt vollziehen, neu definiert und dekonstruiert wurden, «um Krieg als politisches Instrument in einer nuklearen Welt einzusetzen».[15] Das Aufkommen des Kalten Krieges verstärkte die Notwendigkeit eines verbesserten nicht-militärischen Instrumentariums und erweiterte den Bereich der Verteidigung auf die psychologische, politische, soziale und wirtschaftliche Sphäre.[16]

Als die nukleare Abschreckung zum Hauptantrieb der globalen Machtdynamiken aufstieg, so folgert Chin, «wurden Rituale im Bereich der Organisation, Planung und Demonstration der nuklearen Kampffähigkeit zur Abschreckung potenzieller Gegner und damit zur Verhinderung eines möglichen Krieges zum Ersatz für die organisierte Gewalt».[17] Im Narrativ des Kalten Krieges wurde Sicherheit somit zum Synonym für das verfügbare Atomwaffenarsenal und die nuklearen Verteidigungsmittel, was die Notwendigkeit für den Staat erhöhte, in technologische Fortschritte beider Bereiche zu investieren.

Vor dem Hintergrund einer vermeintlich allgegenwärtigen nuklearen Bedrohung waren die ständig steigenden Haushaltsmittel für die Rüstungsforschung staatlicherseits leicht zu rechtfertigen. Die Bereitstellung staatlicher Mittel für sich abzeichnende technologische Innovationen beschleunigte deren Entwicklung erheblich und schuf durch komplexe Programme für Forschung und Entwicklung (F&E) solide Verbindungen zwischen privaten Unternehmen und dem Staat.[18] 1961 prägte der damalige US-Präsident Dwight D. Eisenhower den Begriff des militärisch-industriellen Komplexes (MIK), um auf mögliche Absprachen hinzuweisen, die sich aus gemeinsamen Interessen in diesem Umfeld zwischen Akteur*innen aus Politik, Verteidigungsindustrie und Militär mit dem Ziel ergeben, die Militärausgaben weiter zu erhöhen.[19]

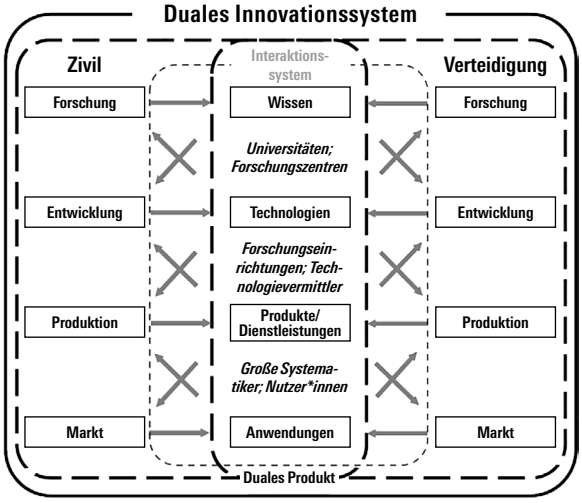
2.2 DAS AUFKOMMEN VON DUAL-USE-TECHNOLOGIEN

Die Verbindung zwischen dem militärischen und dem privaten Sektor hatte auch Auswirkungen auf den gemeinsamen Raum, in dem Forschungsergebnisse geteilt wurden, und wirkte sich auf die «Mechanismen des Technologietransfers vom zivilen in den Verteidigungsbereich *(spin-in)* und vom Verteidigungsbereich in den zivilen Bereich *(spin-off)*»[20] aus. François-Xavier Meunier stellt in seiner Untersuchung der «militärischen/zivilen Dualität im Technologiebereich» einen Wendepunkt in dieser Dynamik zwischen 1970 und 1980 fest.

8 Chin: Technology, war and the state, S. 765. **9** Ebd. **10** Vgl. ebd. **11** Ebd. **12** Vgl. ebd. **13** Ebd., S. 768. **14** Vgl. ebd. **15** Ebd. **16** Vgl. ebd. **17** Ebd., S. 769. **18** Vgl. ebd. **19** Vgl. Eisenhower, Dwight D.: Military-Industrial Complex Speech, 1961, unter: https://avalon.law.yale.edu/20th_century/eisenhower001.asp. **20** Meunier, François-Xavier: Construction of an Operational Concept of Technological Military/Civilian Duality, in: Journal of innovation Economics & Management 2/2019, S. 159–182, hier S. 162; unter: https://doi.org/10.3917/jie.029.0159.

Angesichts der anhaltenden nuklearen Bedrohung und einer wachsenden internationalen Friedensbewegung, die sich gegen die verteidigungspolitischen Strategien der großen staatlichen Kontrahenten wandte, waren ständig steigende Rüstungsausgaben mit dem Militär als Haupttriebkraft der Innovation immer schwerer zu rechtfertigen. In diesem Umfeld wurde der Begriff *dual use* erstmals in den USA eingeführt, um «zivile F&E-Ausgaben für Verteidigungsbudgets beizubehalten und damit die Regeln der [Welthandelsorganisation] zu umgehen»,[21] so Meunier. Durch die Bildung dieser vermeintlich für beide Seiten vorteilhaften Verflechtung zwischen dem zivilen und dem militärischen Markt trug die Doppelnutzungsstrategie zur Normalisierung der engen Beziehung zwischen den zwei Bereichen bei.

Abbildung 1: Duales Innovationssystem



Quelle: Meunier 2019, S. 172

Seit den 1980er-Jahren löste sich das Konzept der Dualität «allmählich von der einfachen Strategie zur Umgehung internationaler Handelsregeln»[22] und entwickelte sich, wie es Guichard und Heisbourg beschreiben, «zu einer Methode des Forschungs-, Innovations- und Produktionsmanagements von Verteidigungssystemen, die darauf abzielte, Skaleneffekte, Produktvielfalt und Wechselwirkungen mit dem zivilen Sektor zu erzielen».[23]

Meunier unterscheidet zwischen den Konzepten «duale Nutzung» und «duale Innovation». Im Falle der dualen Nutzung kann eine Technologie sowohl zivile als auch militärische Anwendungen haben, für die «das Ziel der Dualität darin besteht, den Transfer von einer Sphäre in die andere zu erleichtern, und zwar unter Berücksichtigung der Probleme der technologischen Anpassung, die dieser Vorgang hervorrufen kann».[24] Umgekehrt besteht in einem «dualen Innovationsprozess», wie ihn Meunier beschreibt, «die Herausforderung der Dualität darin, die technologische Koproduktion zwischen dem zivilen und dem militärischen Bereich zu erleichtern. Der Transfer ist kein Problem mehr, da die Besonderheiten der militärischen und zivilen Bereiche im Innovationsprozess berücksichtigt werden».[25] In beiden Fällen impliziert die «Bewältigung der Dualität […] einen Governance-Modus, der öffentliche Behörden, Privatunternehmen und Forschungszentren miteinander verbindet»,[26] wobei die Politik die Grenzen für die Verbreitung von Wissen und Technologie festlegt und gleichzeitig die Möglichkeiten der zunehmend globalen Märkte nutzt.

2.3 NEUE GRENZEN DER KRIEGSFÜHRUNG – DER FORTBESTAND DES MIK NACH DEM KALTEN KRIEG

Am Ende des Kalten Krieges im Jahr 1992 führte der plötzliche Wegfall der allgegenwärtigen militärischen Bedrohung zu einem starken Rückgang des Verteidigungshaushalts und der staatlichen Beteiligung an Forschungs- und Entwicklungsprogrammen, was es privaten Unternehmen ermöglichte, sich stärker in der Verteidigungsindustrie zu etablieren. Dies bedeutete auch einen weitreichenden Wandel der politischen Rahmensetzung. Während der Staat während des Kalten Krieges der wichtigste Innovationsmotor für technologische Errungenschaften wie das Internet und die Satellitenüberwachung gewesen war, fiel diese Verantwortung nun den großen Akteuren auf dem privaten Technologiemarkt zu.

«Die anschließende Nutzung von [militärischen] Technologien durch den privaten Sektor», so Chin, «spiegelt eine bewusste politische Entscheidung der meisten westlichen Regierungen wider, die darin bestand, die Ausgliederung von Spitzentechnologien aus der Verteidigungsforschung in die Wirtschaft im weiteren Sinne zu fördern, um so Wohlstand zu schaffen.» Dies führte zu einer Welle von Dual-Use-Innovationen sowie Spin-off-Produkten von Technologien aus dem Kalten Krieg auf dem zivilen Markt. Die Nachfrage nach diesen Produkten verschaffte dem privaten Sektor das nötige Kapital, um die technologische Innovation selbst zu gestalten, sodass er eine immer zentralere Rolle in der informationstechnologischen Revolution einnehmen konnte.[27]

In diesem Umfeld, so Chin, «stützte sich die militärische Macht zunehmend auf den vorhandenen Pool an technologischem Wissen innerhalb der Wirtschaft insgesamt».[28] Mit der zunehmenden Forderung nach Qualität statt Quantität auf dem Schlachtfeld und dem daraus resultierenden steigenden Bedarf an komplexen Systemen für militärische Operationen wurden private Unternehmen für den Bereich der militärischen Innovation unverzichtbar. In der Folge «lagerten westliche Staaten […] die Bereitstellung von Werkzeugen für die innere und äußere Sicherheit zunehmend in den privaten Sektor aus».[29]

21 Ebd., S. 160. **22** Ebd., S. 161. **23** Guichard, Renelle/Heisbourg, François: Recherche militaire: vers un nouveau modèle de gestion?, Paris 2004, S. 97. **24** Meunier: Construction of an Operational Concept, S. 163–164. **25** Ebd., S. 164. **26** Ebd., S. 166. **27** Chin: Technology, war and the state, S. 770. **28** Ebd. **29** Ebd.

Neue technologische Fortschritte und ihre Auswirkungen auf die Kriegsstrategien erlaubten es dem Staat, militärische Operationen auch dann fortzusetzen, wenn es im Inland keinen Konsens über eine direkte Beteiligung an bewaffneten Einsätzen gab, was das Interesse des Staates an der Aufrechterhaltung des MIK als tragfähigem verteidigungspolitischen Instrument zwischen dem Ende des Kalten Krieges und dem Beginn des «Kriegs gegen den Terror» aufrechterhielt. Der «Krieg gegen den Terror» leitete dann eine neue Entwicklungsstufe in der Kriegsführung ein, die sich auf weniger risikobehaftete, aber kapitalintensivere Mittel wie Satelliten und Drohnen stützte.[30] Parallel zu den verbesserten Fähigkeiten dieser technologischen Neuerungen verlagerte sich ihre Anwendung stärker ins Inland, was die staatlichen Möglichkeiten der technologischen Machtausübung über die Bürger*innen verstärkte. Während der technische Fortschritt und die Innenpolitik ein Umfeld schufen, in dem offene Überwachung und Kontrolle mit dem Argument der Terrorismusbekämpfung gerechtfertigt werden konnten, schaute der Staat weiter nach Möglichkeiten, die Kontrolle über Einzelpersonen mithilfe von Technologien, die für zivile Dienste bestimmt waren, verstärkt durchzusetzen.[31]

Das Umfeld, in dem diese Entwicklung erfolgte, wird heute als vierte industrielle Revolution bezeichnet, wie es Klaus Schwab 2017 erstmals formulierte.[32] Sein Konzept besagt, dass digitale Technologien, die Computer-Hardware, -Software und -Netzwerke umfassen, sowie die extreme Komplexität, mit der sie miteinander interagieren, unsere Gesellschaften und globalen Wirtschaftsnetze neu definieren. Das Entscheidende dabei ist ihre Fähigkeit, digitale, physische und biologische Räume zu verknüpfen und damit bisher relativ getrennte technologische Dimensionen miteinander zu verbinden, was ein vollkommen neues Spektrum an Möglichkeiten eröffnet. Diese neu gewonnenen Funktionen erstrecken sich auf unterschiedlichste Bereiche, in denen nun eine Vielzahl von Technologien eingesetzt werden kann, darunter «ein weitaus allgegenwärtigeres und mobileres Internet, […] kleinere und leistungsfähigere Sensoren, die preiswerter geworden sind, und […] leistungsfähige künstliche Intelligenz (KI) sowie maschinelles Lernen.»[33] Es ist die Verschmelzung dieser Bereiche, die den Beginn einer neuen Ära der technologischen Innovation eingeläutet hat.

Dieser Rahmen beleuchtet bereits einige der zentralen Ansätze, auf denen die Third Offset Strategy (TOS) des Pentagon beruht. Die TOS wurde 2014 vorgestellt und schlägt neue Prioritäten in der US-amerikanischen Innovationspolitik im Verteidigungsbereich als Reaktion auf potenzielle Bedrohungen durch gegnerische Mächte wie Russland und China vor. Die Strategie zielt darauf ab, sowohl den Zugang des Verteidigungssektors zu Wissen zu gewährleisten, das von kommerzieller sowie ziviler Forschung und Entwicklung auf internationaler Ebene generiert wurde, als auch Möglichkeiten zu finden, wie dieses Wissen für die Aufrechterhaltung der militärischen Überlegenheit der USA genutzt werden kann. Dies beinhaltet auch die jüngsten zivilen technologischen Innovationstrends wie KI und maschinelles Lernen.[34] Die Gründung der im Silicon Valley ansässigen Defence Innovation Unit im Jahr 2015 kann als ein Symptom für dieses Bestreben angesehen werden.

Indessen wurde diese strategische Entwicklung vom Drängen privater Akteure aus dem Silicon Valley begleitet, eine an den Kalten Krieg angelehnte Arbeitsbeziehung zwischen dem zivilen Sektor und dem Staat wiederherzustellen, was den von Eisenhower formulierten Bedenken hinsichtlich eines MIK neuen Auftrieb gab. Eines von vielen Beispielen für diese Dynamik stellt die Silicon Valley Defense Group dar – an der wichtige Anbieter ziviler marktbezogener Dienstleistungen wie Microsoft, Amazon Web Services (AWS) und Google aktiv mitwirken –, die das «erodierte Vertrauen» beklagt, das durch die immer größer werdende Kluft zwischen Industrie und Staat entstanden sei, und sich für höhere Investitionen sowie einen liberaleren Regulierungsrahmen einsetzt.[35]

30 Vgl. ebd., S. 772. **31** Vgl. Graham, Stephen: Cities Under Siege. The New Military Urbanism, Kapitel 3: The military urbanism, Abschnitt: Tracking: citizen–consumer–soldier, London/New York 2011. **32** Schwab, Klaus: The Fourth Industrial Revolution, London 2017. **33** Ebd., S. 7. **34** Meunier: Construction of an Operational Concept, S. 773. **35** Silicon Valley Defense Group: Unlocking New Sources of Techno-Security Advantage. Fall 2020 Roundtable Series Insight Paper, 2020, S. 6, unter: https://static1.squarespace.com/static/5f82250a85dd3125aeba053d/t/600081281ec43d45da33b4cf/1610645802845/SVDG+Fall+2020+Roundtable+Insights+Jan+2021.pdf.

3 DER PRIVAT-ÖFFENTLICHE INNOVATIONSTRANSFER IN DEN USA – EINE FALLSTUDIENANALYSE

In den folgenden Abschnitten geht es um einige zentrale Tendenzen dieser Beziehung. Anhand der Analyse einschlägiger Vergaben wird eine Vielzahl von Aspekten beleuchtet, die für die Ethik von Projektvorhaben, die Vergabe von Regierungsaufträgen, unerwünschte Einmischungsversuche und technologische Bias von Belang sind. Die Auswahl der untersuchten privaten Technologieunternehmen erfolgte in erster Linie nach dem Grad ihrer Kapitalausstattung auf dem Verbrauchermarkt und dem öffentlichen Bekanntheitsgrad sowohl in den USA als auch in Europa. Aus diesem Grund wurden Unternehmen wie IBM und HP Inc. trotz des Erhalts von Aufträgen in großem Umfang nicht berücksichtigt. Wir möchten jedoch zur Analyse entsprechender Fälle ermutigen, wie etwa der Beiträge von IBM zum IT-Modernisierungsprojekt ITES-2S des US-Militärs, für das zwischen dem Beginn der Initiative im Jahr 2005 und Mai 2020 Aufträge im Wert von schätzungsweise eine Milliarde US-Dollar vergeben wurden,[36] oder des Vertrags mit HP über drei Milliarden US-Dollar für die Bereitstellung von IT-Unterstützung für die US-Marine im Jahr 2017.[37]

3.1 PROJEKT MAVEN

Das Projekt Maven ist eines der bekanntesten Beispiele für die Zusammenarbeit eines großen zivilen Unternehmens mit dem US-Militär in den letzten Jahren. Das Vorhaben wurde mit dem Ziel konzipiert, durch die automatisierte Analyse riesiger Bild- und Videodatenbestände autonom «Objekte von Interesse» zu identifizieren.[38] Das auf ein Jahresbudget von 250 Millionen US-Dollar geschätzte Projekt[39] erlangte 2018 Berühmtheit, als Mitarbeiter*innen von Google LLC mit einer Arbeitsniederlegung gegen die Beteiligung ihres Arbeitgebers protestierten und einen Verstoß gegen die ethische Verpflichtung von Google geltend machten, keinen aktiven Beitrag zu Technologien zu leisten, die für den Krieg eingesetzt werden können.[40]

Im April 2017 begann der damalige stellvertretende Verteidigungsminister Bob Work mit der Zusammenstellung eines bereichsübergreifenden Teams für algorithmische Kriegsführung. Das selbsterklärte Ziel war es, künstliche Intelligenz und maschinelle Lerntechnologien effizienter in die bestehenden Ressourcen des Verteidigungsministeriums zu integrieren, um «[dessen] Vorteile gegenüber zunehmend leistungsfähigeren Gegnern und Konkurrenten»[41] zu erhalten. Dieses Vorhaben könne nur «mit kommerziellen Partnern an unserer Seite»[42] realisiert werden, sagte Drew Cukor, Oberst des Marine Corps und Chef des neu gegründeten Teams, bei einer Präsentation 2017.

Einer dieser kommerziellen Partner war Google, das die Initiative unterstützte, indem es dem Pentagon seine Open-Source-KI-Software TensorFlow zur Verfügung stellte. «Das US-Militär verwendet [TensorFlow] nicht in Waffensystemen und schon gar nicht in angeblich autonomen Systemen. Aber die bloße Tatsache, dass Google mit dem US-Militär zusammenarbeitet, hat zu Protesten von Mitarbeiter*innen und letztlich dazu geführt, dass das Unternehmen seinen bestehenden Vertrag mit dem Verteidigungsministerium nicht verlängert hat», sagte 2018 der US-Sicherheitsexperte und Senior Fellow am Center for a New American Security, Paul Scharre.[43] Um den Schaden zu begrenzen, den die Affäre sowohl intern als auch extern verursachte, verpflichtete sich Google-CEO Sundar Pichai in einem Blogbeitrag von 2018 mit dem Titel «AI at Google: our principles» dazu, «keine KI zu entwickeln oder bereitzustellen», die für «Waffen oder andere Technologien, deren Hauptzweck oder Einsatz darin besteht, Menschen Schaden zuzufügen oder einen solchen direkt zu begünstigen»,[44] bestimmt sei.

Diese selbst auferlegten Verpflichtungen erlaubten es Google, die eigenen ethischen Standards selbstständig zu formulieren, und ermöglichen dem Unternehmen dadurch erhebliche Ausnahmen für die Überwachung und andere KI-gestützte Technologien im Zusammenhang mit dem Verteidigungssektor. Es ist durchaus denkbar, dass sogar das Projekt Maven als legitimes Projekt unter Googles neuem KI-Prinzip gelten könnte, vermutet Laura Nolan, ehemalige Google-Mitarbeiterin und Gründungsmitglied der «Campaign to Stop Killer Robots»[45] – einer großen globalen Initiative, die ein Verbot von tödlichen autonomen Waffen fordert.

«Niemand hat gesagt, dass Maven eine Waffe ist. Maven ist ein Informationssystem, mit dem man Ziele auswählen kann. Die Waffe ist ein relativ trivialer Teil – die Spitze des Speers. Was Google also tatsächlich sagte, war: ‹Wir bauen den Speer und das Verteidigungsministerium liefert die Spitzen.› Googles Versäumnis, auf das Thema Überwachung einzugehen, war ebenfalls äußerst enttäuschend, da Maven im Wesentlichen darauf abzielt. Es handelt sich um ein Überwachungsprojekt, nicht um eine Waffe. Aber das Paradigma der personenbezogenen Kriegsführung hängt sehr stark von einer Massenüberwachung ab, die für sich ge-

36 Moss, Sebastian: IBM gets $18.8m contract modification for ongoing US Army IT modernization award, ITES-2S, Data Center Dynamics, 1.5.2020, unter: www.datacenterdynamics.com/en/news/ibm-gets-188m-contract-modification-ongoing-us-army-it-modernization-award-ites-2s. **37** Bylund, Anders: Meet Hewlett-Packard, the Defense Contractor, The Motley Fool, 6.4.2017, unter: www.fool.com/investing/value/2010/07/09/meet-hewlett-packard-the-defence-contractor.aspx. **38** Pellerin, Cheryl: Project Maven to Deploy Computer Algorithms to War Zone by Year's End, 21.7.2017, unter: www.defense.gov/News/News-Stories/Article/Article/1254719/project-maven-to-deploy-computer-algorithms-to-war-zone-by-years-end/. **39** Brewster: Google Promised. **40** Vgl. Wakabayashi, Daisuke/Shane, Scott: Google Will Not Renew Pentagon Contract That Upset Employees, in: The New York Times, 1.6.2018, unter: www.nytimes.com/2018/06/01/technology/google-pentagon-project-maven.html. **41** Pellerin: Project Maven. **42** Ebd. **43** Peitz, Dirk: Google wird einfach ersetzt, in: Die Zeit, 8.6.2018, unter: www.zeit.de/digital/internet/2018-06/maven-militaerprojekt-google-ausstieg-ruestungsexperte-paul-scharre. **44** Pichai, Sundar: AI at Google: our principles, 7.6.2018, unter: www.blog.google/technology/ai/ai-principles/. **45** «Kampagne Killer-Roboter stoppen» (Anm. d. Ü.).

nommen bereits gefährlich ist. Es gibt Menschen, die seit Jahren unter ständiger Überwachung leben, was dazu führt, dass ganze Gemeinschaften auseinanderbrechen. Man trifft sich nicht mehr in Gruppen, man schickt seine Kinder nicht mehr zur Schule, man geht nicht mehr zu den Beerdigungen der anderen. Was macht das mit einer Gemeinschaft, wenn sich diese Situation über ein Jahrzehnt hinzieht?»[46]

Das Ausmaß, in dem ethische Erwägungen lediglich ein strategisches Mittel darstellten, um in der durch die Beteiligung an Maven ausgelösten Krise weiteren Schaden vom Unternehmen abzuwenden, wird durch den Rückgriff auf patriotische Narrative deutlich, mit denen interne Bedenken im Zusammenhang mit dem Vertrag vor der Veröffentlichung von Pichais Blogbeitrag angesprochen wurden. Im Verlauf interner Versammlungen, die von der Google-Führung im März 2018 angesetzt wurden, um auf die Bedenken der Mitarbeiter*innen bezüglich des Projekts einzugehen, stützten sich die Entscheidungsträger*innen stark auf das Argument einer «Unterstützung unserer Truppen», um zu rechtfertigen, dass Google weiterhin zu diesem Projekt beitrug, so Nolan. «Ich würde sagen, dass nur eine Minderheit der Leute dachte, es sei eine gute Sache, ‹unsere Truppen zu unterstützen›. Google ist ein sehr internationales Unternehmen, und für die meisten Mitarbeiter*innen waren es keineswegs ‹unsere Truppen›. Aber so hat es die Führung in den USA immer formuliert.»

Indem Google signalisiert, dass es bereit ist, Forderungen nach verbesserten ethischen Richtlinien zu berücksichtigen und einzuhalten, kann es das Image eines verbraucherorientierten Unternehmens mit altruistischen Maximen aufrechterhalten – nicht nur gegenüber der Öffentlichkeit, sondern vor allem gegenüber der Belegschaft. «Google zieht seit Jahren eine vergleichsweise liberale, relativ links ausgerichtete und auch sehr internationale Belegschaft an. Selbst wenn man in die US-Büros geht, insbesondere in die Entwicklungsbüros, kommen sehr viele Mitarbeiter*innen nicht aus den USA. Google hat sehr viele Mitarbeiter*innen aus der ganzen Welt eingestellt. Es gibt also eine Menge Nicht-US-Amerikaner*innen, die für Google arbeiten, und eine Menge US-Amerikaner*innen, die mit Anti-Kriegs-Ideen sympathisieren»,[47] so Nolan.

Mit den selbst auferlegten und vermeintlich verbesserten Ethik-Richtlinien nahm zudem der Druck auf die Gesetzgeber ab, den Raum, in dem private Technologieunternehmen mit dem Militär zusammenarbeiten, weiter zu regulieren. Angesichts einer hochentwickelten und gut funktionierenden Lobby für privat-militärische Forschungs- und Entwicklungsvorhaben sind die Hindernisse für die Entwicklung eines stärkeren rechtlichen Rahmens in den USA zumeist unüberwindbar.

Als Reaktion darauf, dass Google die Verbindung zu Project Maven löste, während es weiter an Project Dragonfly arbeitete, einer Suchmaschine, die mit der Innenpolitik der chinesischen Regierung im Einklang steht, bezeichnete Paypal-Mitbegründer und Trump-Spender Peter Thiel das Verhalten von Google als «offensichtlich hochgradig verräterisch».[48] Diese Kritik machte sich auch der damalige Vorsitzende des Vereinigten Generalstabs, General des US-Marine Corps Joseph Dunford, zu eigen.[49]

Eine aktuelle Analyse des Forbes-Mitarbeiters Thomas Brewster ergab, dass AWS und Microsoft die von Google hinterlassene Lücke im Jahr 2019 füllten und sich seitdem Pentagon-Verträge im Wert von insgesamt 50 Millionen US-Dollar gesichert haben.[50] Er stellte außerdem fest, dass Pichai, seit Ende 2019 CEO der Google-Muttergesellschaft Alphabet Inc., trotz seines verstärkten ethischen Engagements keinerlei Konsequenzen für die florierenden Investitionen in Start-ups wie Orbital, Planet und ClarifAI zog, die über Alphabets Risikokapitalsparte GV Satellitenbilddaten und Analysedienste für das Militär anbieten.[51] Nicht nur das Fachgebiet selbst erinnert an Googles Beitrag zum Projekt Maven – offenbar schloss Orbital sogar einen eigenen Vertrag unter dem Maven-Dach ab und erhielt insgesamt 1,8 Millionen US-Dollar für die Entwicklung von «multispektralen Modellen für Standbilder aus großer Höhe.»[52]

Mit Rebellion Defense gesellt sich Orbital ein weiteres Start-up hinzu, das an Maven arbeitet und direkte Verbindungen zu dem in Mountain View ansässigen Tech-Giganten unterhält. Das vom ehemaligen Google-CEO Eric Schmidt[53] gegründete Unternehmen Rebellion Defense hat sich zum Ziel gesetzt, «KI-Produkte zu entwickeln, die speziell für die Verteidigung in einer Ära bestimmt sind, in der die Überlegenheit der Software den nationalen Sicherheitsvorteil bestimmt».[54] Schmidt hat sich den Ruf erworben, die Kluft zwischen dem Silicon Valley und dem Verteidigungssektor zu überbrücken. Seine Mitgliedschaft in zwei Beratungsgremien des Verteidigungsministeriums, die der Verbesserung dessen KI-Technologien dienen, hat Bedenken in Bezug auf mögliche Interessenkonflikte aufkommen lassen, während er gleichzeitig seine Rolle als technischer Berater bei Alphabet beibehält und Aktien des Google-Mutterkonzerns im Wert von 5,3 Milliarden US-Dollar hält.[55]

46 Interview mit Laura Nolan («Campaign to Stop Killer Robots»), geführt von den Autor*innen am 18. Februar 2022, unter: https://docs.google.com/document/d/1uado2xvqcdTs5yIDljbxD7N6QBmmc5bu/edit?usp=sharing&ouid=113280576371631986367&rtpof=true&sd=true. **47** Ebd. **48** Chafkin, Max: Peter Thiel Urges U.S. Probe of Google's ‹Seemingly Treasonous› Acts, in: Bloomberg, 14.7.2019, unter: www.bloomberg.com/news/articles/2019-07-15/thiel-urges-u-s-probe-of-google-s-seemingly-treasonous-acts. **49** Magnuson, Stew: Dunford Slams Google for Working with China, But Not U.S. Military, in: National Defense, 18.11.2018, unter: www.nationaldefensemagazine.org/articles/2018/11/18/dunford-slams-google-for-working-with-china-but-not-us-military. **50** Brewster, Thomas: Project Maven: Amazon And Microsoft Scored $50 Million In Pentagon Surveillance Contracts After Google Quit, in: Forbes Magazine, 8.9.2021, unter: www.forbes.com/sites/thomasbrewster/2021/09/08/project-maven-amazon-and-microsoft-get-50-million-in-pentagon-drone-surveillance-contracts-after-google/?sh=52af312f6f1e. **51** Brewster: Google Promised. **52** Brewster: Project Maven. **53** Rebellion Defense wurde nicht von Schmidt persönlich, sondern von seinem Unternehmen Innovation Endeavors mitbegründet. **54** Vgl. Selbstbeschreibung der Produkte von Rebellion Defense unter: https://rebelliondefence.com/rebellion-products. **55** Conger, Kate/Metz, Cade: «I Could Solve Most of Your Problems»: Eric Schmidt's Pentagon Offensive, in: The New York Times, 2.5.2020, unter: www.nytimes.com/2020/05/02/technology/eric-schmidt-pentagon-google.html.

Chris Lynch, CEO und Mitbegründer von Rebellion Defense, ist auch Gründungsdirektor des Defense Digital Service (DDS), eines «Rapid Response Team»[56] des Pentagon, das die Joint Enterprise Defence Infrastructure (JEDI) initiierte – eine Initiative, die vor allem durch die rechtliche Pattsituation zwischen Google und AWS im Zusammenhang mit dem 10-Milliarden-US-Dollar-Projekt bekannt wurde und im Mittelpunkt des folgenden Kapitels dieser Studie steht.[57] Die Gründungspartner*innen von Lynch, Nicole Camarillo und Oliver Lewis, teilen seine umfangreiche Erfahrung im Sicherheitssektor.[58]

Diese Dynamik fügt sich nicht nur in die Geschichte von Google ein, das aktiv dem Geld für Pentagon-Verträge folgt und gleichzeitig hart daran arbeitet, sein Image als «Don't be evil»-Innovator im Bereich der Verbrauchertechnologie aufrechtzuerhalten; es ist auch ein Hinweis auf die weitverbreitete Drehtür-Einstellungspraxis zwischen dem US-Rüstungssektor und dem Silicon Valley,[59] eine Dynamik, die im folgenden Kapitel noch genauer beleuchtet wird.

3.2 JOINT ENTERPRISE DEFENCE INFRASTRUCTURE, DIE DREHTÜRPRAXIS UND IHRE AUSWIRKUNGEN AUF DIE ZIVILE EINFLUSSNAHME IM INLAND

3.2.1 Joint Enterprise Defence Infrastructure (JEDI)

Noch bevor der Rechtsstreit zwischen konkurrierenden Auftragnehmern für öffentliche Aufmerksamkeit sorgte, offenbarte JEDI einen weiteren wichtigen Entwicklungsbereich, für den das Verteidigungsministerium die Unterstützung des zivilen US-Technologiemarkts suchte. JEDI war ein Multi-Cloud-Computing-Projekt, das für eine verbesserte Kommunikation zwischen dem Pentagon und den Streitkräften im Feld sowie zwischen den verschiedenen Verteidigungsbehörden sorgen sollte. Der Vertrag, für den AWS der erwartete Auftragnehmer gewesen war, wurde schließlich wegen angeblicher Interessenkonflikte im Zusammenhang mit dem AWS-Mitarbeiter Deap Ubhi an Microsoft vergeben.

Aufgrund früherer Bedenken hatte der JEDI-Mitbewerber Oracle eine Klage beim U.S. Court of Federal Claims eingereicht, in der das Unternehmen den Vorwurf erhob, dass AWS das Ausschreibungsverfahren durch Ubhis Beschäftigung beim Pentagon erheblich beeinflusst habe.[60] Ubhi hatte AWS im Jahr 2016 verlassen und war zum Verteidigungsministerium gewechselt, wo er auch am JEDI-Vertrag mitarbeitete. In dieser neuen Rolle bezeichnete er sich selbst immer wieder als «Amazonier» und vertrat Positionen, die die zuvor kritisierte Einzelvergabe begünstigten. Im Jahr 2017 zog er sich dann von seiner Rolle am Vergabeprozess von JEDI zurück, während er ein Tech-Startup leitete, das darauf abzielte, Restaurants zusätzliche Ressourcen für Online-Geschäfte zur Verfügung zu stellen, was die Aufmerksamkeit von AWS erregte. Ubhi verabschiedete sich dann vollständig von seiner Arbeit an JEDI und führte mögliche Interessenkonflikte aufgrund von Partnerschaftsverhandlungen mit seinem früheren Arbeitgeber an. Während die Auswirkungen dieser Vereinbarungen unklar bleiben, verließ Ubhi das Pentagon, um kurz darauf wieder bei AWS einzusteigen.[61]

Das Verteidigungsministerium wurde beauftragt, Ubhis Mitwirkung am JEDI-Vertrag weiter zu untersuchen, und setzte die Auftragsvergabe für die Dauer der Untersuchung aus. Das Ministerium kam zu dem Schluss, dass Ubhis «Beteiligung an der Vergabe die Rechtmäßigkeit der Auftragserteilung nicht beeinträchtigte und auch im Fortgang nicht beeinträchtigen könne»[62] sowie dass seine Mitwirkung am Vertrag zulässig war, «weil sein Arbeitsverhältnis mit Amazon mehr als ein Jahr vor Beginn der Vergabe geendet hatte».[63] Oracle kritisierte die oberflächliche Prüfung des Falls, da sie die mangelnde Aufsicht über den Vertrag durch das Verteidigungsministeriums außer Acht gelassen und Ubhis Beschäftigung bei AWS nach seinem Ausscheiden aus dem Pentagon nicht berücksichtigt hatte.[64] AWS focht später die Entscheidung, den Auftrag an Microsoft zu vergeben, vor Gericht an.

Im Juli 2021 gab das Verteidigungsministerium dann bekannt, dass es den JEDI-Vertrag im Wert von zehn Milliarden US-Dollar auflöse, weil er nicht mehr den Bedürfnissen des Ministeriums entspreche. Abgesehen von den potenziellen Auswirkungen der Kontroverse auf die Realisierbarkeit des Vertrags könnte diese Entscheidung auch das rasante Tempo widerspiegeln, in dem der Markt für militärische Innovationen operiert. Darüber hinaus hatte der Rechtsstreit zwischen den Anbietern den Zeitplan für die Lieferung über ein akzeptables Maß hinaus verschoben. Unmittelbar nach der Auflösung von JEDI kündigte das Verteidigungsministerium das Projekt Joint Warfighting Cloud Capability (JWCC) als Ersatz an. JWCC unterscheidet sich von JEDI dadurch, dass keine Cloud-Entität über einen einzigen Anbieter entwickelt wird, sondern der Vertrag an mehrere Cloud-Service-Anbieter vergeben wird, die nach Ansicht des Verteidigungsministeriums in der Lage sind, die Anforderungen zu erfüllen. Jeder Anbieter wird damit beauftragt, eine Cloud-Einheit mit einem spezifischen Anwendungszweck zu entwickeln. Mit diesem Ansatz soll sichergestellt werden, dass die einzelnen Clouds besser geschützt sind und Sicherheitslü-

56 Vgl. Selbstbeschreibung von DDS unter: www.dds.mil/. **57** Conger, Kate/Sanger, David E.: Pentagon Cancels a Disputed $10 Billion Technology Contract, in: The New York Times, 6.7.2021, unter: www.nytimes.com/2021/07/06/technology/JEDI-contract-cancelled.html. **58** Brewster: Google Promised. **59** Für eine weitere Analyse vgl. Die Kampagne «Big Tech Sells War» (https://bigtechsellswar.com), und das Projekt «Big Tech Sells War: A Revolving Door» (https://littlesis.org/oligrapher/7155/share/a8e846a75c90f5a6d14e). **60** Gregg, Aaron/Greene, Jay: Fierce backlash against Amazon paved the way for Microsoft's stunning Pentagon cloud win, in: The Washington Post, 30.10.2019, unter: www.washingtonpost.com/business/2019/10/30/fierce-backlash-against-amazon-paved-way-microsofts-stunning-pentagon-cloud-win. **61** Davenport, Christian/Gregg, Aaron: Pentagon to review Amazon employee's influence over $10 billion government contract, 24.1.2019, unter: www.seattletimes.com/business/pentagon-to-review-amazon-employees-influence-over-10-billion-government-contract. **62** Gregg/Greene: Fierce backlash against Amazon. **63** Ebd. **64** Davenport/Gregg: Pentagon to review.

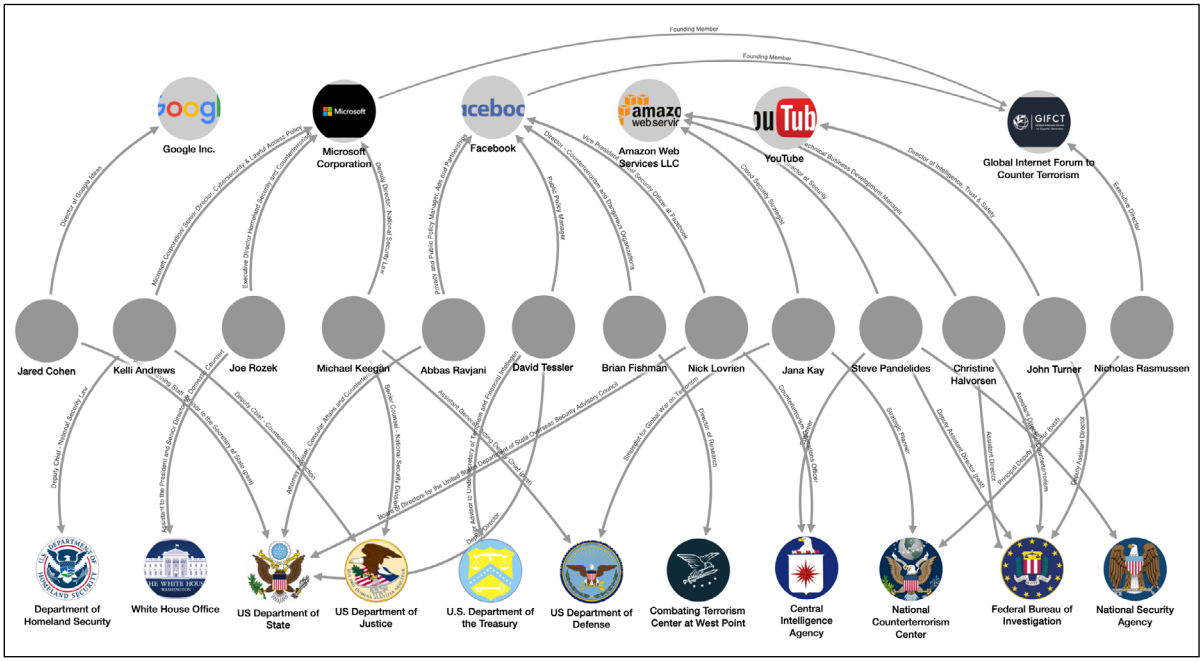
cken leichter vermieden werden können. Die Aufträge sollen in Form eines IDIQ-Vertrags («indefinite delivery indefinite quantity») vergeben werden, der eine unbestimmte Menge von Dienstleistungen innerhalb eines bestimmten Zeitrahmens vorsieht. Das Verteidigungsministerium kündigte im November 2021 an, dass es beabsichtige, jeweils einen IDIQ-Vertrag an Microsoft und AWS zu vergeben. Es forderte auch Google Cloud und Oracle auf, sich an der Unternehmung zu beteiligen und entsprechende Vorschläge einzureichen.

Die Arbeitsniederlegung der Google-Mitarbeiter*innen wegen der Beteiligung an Maven war der Auslöser für die Entscheidung des Unternehmens, sich nicht um den JEDI-Auftrag zu bewerben. Thomas Kurian, CEO von Google Cloud, erklärte in einem Blogbeitrag vom 12. November 2021, dass die Entscheidung, sich von JEDI zurückzuziehen, darauf beruhe, dass man sich nicht sicher gewesen sei, ob diese Unternehmung nicht gegen die eigenen KI-Ethikgrundsätze verstoßen würde, er jedoch davon überzeugt sei, dass ein Beitritt zum JWCC diesen Kodex nicht verletzen würde. Er räumte allerdings ein, dass sicherlich nicht alle Mitarbeiter*innen dieser Ansicht seien.[65] Kurian versuchte, das Vorgehen zu rechtfertigen, indem er zwischen JEDI und JWCC unterschied und auf andere verteidigungsbezogene Projekte verwies, bei denen das Unternehmen erfolgreich mit dem Verteidigungsministerium zusammengearbeitet hatte, ohne gegen den eigenen Ethikkodex zu verstoßen. Kurians Blogbeitrag war eine Antwort auf Fragen, die in einer unternehmensweiten Besprechung aufgeworfen worden waren, bei der über 1.000 Mitarbeiter*innen die Beteiligung von Google an JWCC in Zweifel gezogen hatten.[66] Bis zum Zeitpunkt der Abfassung der vorliegenden Studie hat AWS keine internen Kontroversen oder ethischen Bedenken im Zusammenhang mit der Zusammenarbeit mit JEDI oder JWCC bekanntgegeben.

3.2.2 Die Drehtür als Katalysator der «Antiterror»-Politik

Die Kontroverse um Deap Ubhi fand in einem Umfeld statt, in dem es zu einem regen Austausch von Personal und Fachwissen zwischen dem privaten Technologie- und dem staatlichen Verteidigungssektor kommt, wie Munira Lokhandwala bestätigt, Leiterin der Abteilung Technologie und Ausbildung beim zivilgesellschaftlichen Beobachtungsnetzwerk LittleSis. Im Rahmen der Kampagne «Big Tech Sells War» – einer gemeinsamen Initiative von LittleSis, MPower Change und dem Action Center on Race and Economy – analysierte und kartierte Lokhandwala 13 Fälle, in denen Einzelpersonen wiederholt zwischen der privaten Tech-Industrie und dem Pentagon gewechselt hatten.

Abbildung 2: Big Tech verkauft Krieg – die Drehtürpraxis



Quelle: Lokhandwala 2021[67]

65 Kurian, Thomas: Update on Google Cloud's work with the U.S. Government, 12.11.2021, unter: https://cloud.google.com/blog/topics/inside-google-cloud/update-on-google-clouds-work-with-the-us-government. **66** Elias, Jennifer: Google's pursuit of military cloud deal was among top issues at last week's all-staff meeting, in: CNBC, 15.11.2021, unter: www.cnbc.com/2021/11/15/google-pursuit-of-jwcc-among-issues-of-top-concern-at-tgif-meeting-.html. **67** Lokhandwala, Munira (2021), erstellt mit LittleSis Oligrapher; unter: https://littlesis.org/oligrapher/7155/share/a8e846a75c90f5a6d14e.

«In den 20 Jahren des sogenannten globalen Krieges gegen den Terror haben wir eine massive Expansion des Technologiesektors erlebt. Es gibt private Unternehmen, die Geschäfte machen und Produkte herstellen. Gleichzeitig haben wir eine riesige Industrie um sie herum, die ihre Agenda unterstützt. Mit Big Tech Sells War wollten wir herausfinden, wie sich diese beiden Bereiche auf Ebene der Lobbyarbeit zueinander verhalten. Das ist es, was wir – im Kontext der USA – die Drehtür zwischen dem öffentlichen und dem privaten Sektor nennen»,[68] heißt es in der Einführung zu ihrem Kampagnenbeitrag.

«Krieg gegen den Terror» ist ein Ausdruck, der von der Bush-Regierung nach den Anschlägen vom 11. September 2001 geprägt wurde. Er war der Anstoß für den 20 Jahre währenden Krieg der USA in Afghanistan. Einer der wichtigsten Aspekte von «Big Tech Sells War» ist sein Beitrag zum MIK-Diskurs, in dem der Zusammenhang zwischen dem Aufstieg von Big Tech und dem Beginn des «Kriegs gegen den Terror» aufgezeigt wird. Außerdem gelang es der Kampagne, eine direkte Verursachung durch Big Tech sowie deren Motive aufzuzeigen. Begleitet wurde «Big Tech Sells War» von einer weiteren Kampagne mit dem Titel «WhoseTube», die die Mitverantwortung von YouTube, das Google gehört, für die Verbreitung antimuslimischer Narrative anprangert. Die Plattform hat die Verbreitung islamfeindlicher Inhalte zugelassen und damit die öffentliche Unterstützung für eine aggressive Haltung der Regierung gegenüber der muslimischen Bevölkerung angeheizt und die Entwicklung von Waffen für den «Krieg gegen den Terror» befördert. Indem der Mutterkonzern Google im Ergebnis die Voraussetzungen dafür schafft, dass Muslime gefürchtet und daher als legitime Ziele angesehen werden, steigert er seine Gewinnmöglichkeiten durch den Verkauf von Technologien an die US-Regierung, die bei den Kampfeinsätzen im Rahmen des Kriegs gegen den Terror zum Einsatz kommen.[69]

Einer der wichtigsten Aspekte bei der Konzeption des Projekts war die Veranschaulichung der Vielzahl von Aspekten, die von der Drehtür betroffen sind, erklärt Lokhandwala. «Wir wollten Beispiele anführen, die deutlich machen, auf welch unterschiedliche Weise Technik die politische Entscheidungsfindung und die verschiedenen Akteure in diesem ‹globalen Krieg gegen den Terror› beeinflusst. Es geht nicht nur um das Verteidigungsministerium. Es gibt Leute, die 20 Jahre lang beim FBI gearbeitet haben, und Leute, die bei der CIA tätig waren – also in den verschiedenen Behörden des militärischen Überwachungskomplexes der USA – und dann in hochrangige und sehr bequeme Positionen in der Technologiebranche gewechselt sind. Wir sprechen dabei nicht nur über Technologieunternehmen. Ich denke, es ist wichtig, sich darüber klarzuwerden, dass wir, wenn wir es mit [privaten Unternehmen wie] Google zu tun haben, nicht nur über Google sprechen, sondern auch über all die anderen Unternehmen, die von Googles Existenz profitieren. Wir sprechen von Thinktanks, Wirtschaftsverbänden und sämtlichen Bereichen des Technologiesektors.»[70]

In Verbindung mit einer Denkweise, die im Rahmen einer vermeintlichen Terrorismusbekämpfung ein sehr spezielles Verständnis von Sicherheit befördert, hat diese Dynamik laut Lokhandwala sehr reale Folgen für die Zivilbevölkerung im Inland – insbesondere für nicht-weiße US-Bürger*innen. «Die Personengruppe, auf die wir uns bei unserer Untersuchung konzentriert haben, steht für eine ganz bestimmte Ideologie innerhalb des ‹Kriegs gegen den Terror›, nämlich eine, die sich auf diese Vorstellung einer Terrorismusbekämpfung konzentriert. Die Antiterrorismus-Industrie als eine Art Untersektor des ‹globalen Krieges gegen den Terror› ist riesig und hat die Erstellung von Profilen und die Überwachung von People of Color in den USA und im Ausland gerechtfertigt. Sie hat damit ihr eigenes Monster geschaffen.»[71]

3.2.3 Gesichtserkennung, Bias und der Staat

Ein Mittel zur Umsetzung dieser nationalen Profiling- und Überwachungsmaßnahmen sind Gesichtserkennungstechnologien (Facial Recognition Technologies/FRT). Zwar sind FRT keine neue Art von Technologie, sie spielen jedoch eine gewichtige Rolle beim Aufbau eines neuen MIK. Wie viele andere Technologien, die ursprünglich für militärische oder sehr exklusive Zwecke entwickelt wurden, ist Gesichtserkennung heute alltäglich geworden, etwa als integrierte Sicherheitsfunktion von Smartphones. Vor dieser Ausweitung waren ihr Einsatz und ihre Möglichkeiten in erster Linie nur für eine begrenzte Gruppe relevant, die in der Technologiebranche arbeitet oder ihre Entwicklung finanziert. Heute werden die Auswirkungen ihrer Nutzung auch außerhalb des rein technischen Kontexts diskutiert. Die Meinungen über die ethische Anwendbarkeit von Gesichtserkennungstechnologien und das Verständnis davon, wie ein Algorithmus erstellt wird, einschließlich seiner Verwendung in privaten oder öffentlichen Räumen oder zwischen dem Nutzer und dem FRT-Ziel, gehen in den verschiedenen Bevölkerungsgruppen weit auseinander. Während sich iPhone-Nutzer*innen womöglich nicht sonderlich für den Algorithmus interessieren, der zur Identifizierung ihres Gesichts verwendet wird, sollten Polizeibeamte – angesichts der Konsequenzen, die eine unzutreffende Übereinstimmung haben könnte – den Algorithmus sehr wohl verstehen, der zur Identifizierung von Personen verwendet wird, die eines Gesetzesverstoßes verdächtigt werden. An dieser Stelle müssen die ethischen Implikationen der in die FRT-Algorithmen eingeschriebenen Bias hinterfragt werden, und es besteht Gesprächsbedarf.

KI-Technologie simuliert menschliche Entscheidungsprozesse, indem sie eine Reihe von Algorithmen verwendet, die von menschlichen Entwickler*innen entworfen werden. In dem Maße, wie die Fähigkeiten der

68 Transkript des Interviews mit Munira Lokhandwala (LittleSis), geführt von den Autor*innen am 2. Februar 2022, unter: https://docs.google.com/document/d/1erwtg_LcvxUcRK12vu2Kp-heYtV4YYgs/edit?usp=sharing&ouid=113280576371631986367&rtpof=true&sd=true. **69** Action Center on Race & the Economy: Selbstdarstellung, 2021, unter: https://acrecampaigns.org/wp-content/uploads/2021/12/Website-2022-21-ACREI-Overview.pdf. **70** Ebd. **71** Ebd.

KI zunehmen, steigt auch die Bandbreite und Komplexität der Aufgaben, für die sie eingesetzt wird. Sie wird mehr und mehr in das alltägliche Funktionieren der Gesellschaft integriert und ist in der Lage, Handlungen und Prozesse auszuführen, die traditionell nur von Menschen erledigt werden konnten. Derartige Technologien werden eingesetzt, um die menschlichen Fähigkeiten in einigen Bereichen zu unterstützen und in anderen Bereichen die Notwendigkeit menschlicher Mitwirkung vollständig zu überwinden. In einigen Anwendungsbereichen wurde der Einsatz algorithmisch gestützter Technologie als Lösung für die Überwindung subjektiver Bias angepriesen, die oft als Hindernis für den gleichberechtigten Zugang zu Ressourcen und Chancen angesehen wurde. Algorithmen können beispielsweise dazu verwendet werden, die Eignung einer Person für einen Kredit zu bestimmen, ein Prozess, der in der Vergangenheit von einem Bankangestellten durchgeführt wurde, der möglicherweise persönliche und vorgefasste Einstellungen gegenüber bestimmten Personengruppen wie Personen mit Vorstrafen, Alleinerziehenden oder People of Color hatte. Bei einem algorithmischen System wird der Kreditantrag der betreffenden Person mithilfe einer Risikoanalysesoftware bearbeitet, die eine Reihe von Prognosen über das finanzielle Risiko und die Zuverlässigkeit der Person liefert. Finanzinstitute behaupten, dass dieses Verfahren gerechter sei, da es nicht mehr von ihren Mitarbeiter*innen durchgeführt werde. Dennoch haben Studien gezeigt, dass die vor dem Einsatz von Algorithmen beobachteten Probleme bei der Kreditvergabe fortbestehen, was die Reproduktion menschlicher Bias in von Menschen geschaffenen Algorithmen verdeutlicht. Eine Untersuchung der Kreditvergabe in den USA ergab, dass Anträge von People of Color mit einer 40 bis 80 Prozent höherer Wahrscheinlichkeit abgelehnt wurden als die von weißen Antragsteller*innen mit dem gleichen finanziellen Profil.[72] Die Risikobewertung einer Person erfolgt nämlich nur zum Teil mithilfe des Algorithmus, der restliche Anteil entfällt auf jene Fachleute der Branche, die die Technologie entwickelt haben.

Der bei Algorithmen für finanzielle Risikoanalysen zu beobachtende Trend führt zu Nachteilen für bestimmte Personen, liegt aber dennoch im unteren Bereich der Folgenschwere. Doch algorithmische KI wird zunehmend in allen Bereichen eingesetzt, insbesondere bei der Polizei und beim Militär, wobei sich die eingeschriebenen Bias auf unterschiedliche Weise und in unterschiedlichem Umfang bemerkbar machen. Was als Lösung für die Beseitigung traditioneller Diskriminierungstendenzen, Vorurteile und Bias proklamiert wurde und weiterhin wird, scheint schlichtweg die immer gleichen Muster mit den immer gleichen Auswirkungen zu wiederholen, mit dem einzigen Unterschied, dass es keinen Menschen mehr gibt, der für die Entscheidungen zur Rechenschaft gezogen werden kann, sondern nur noch eine Maschine.

Alle Entwicklungen übernehmen unweigerlich gewisse Vorurteile von ihren menschlichen Entwickler*innen. Dies gilt sogar für Erfindungen, die auf Grundlage großer Datensätze entwickelt werden und somit den Anspruch eines «Universalmodells» erheben. Die Populationen, von denen diese Datensätze gesammelt werden, sind jedoch in der Regel recht klein, was den Kreis der Nutzer*innen, denen sie tatsächlich zugutekommen, einschränkt. So werden beispielsweise viele öffentliche Infrastrukturen wie Toiletten und Verkehrsmittel auf der Grundlage von Daten konzipiert, die von überwiegend männlichen Bevölkerungsgruppen erhoben wurden. Sie sind daher viel besser auf die Bedürfnisse von Männern zugeschnitten.[73] Dieser Trend ist auch bei Algorithmen zu beobachten. Da im Technologiesektor größtenteils weiße Männer arbeiten, bedeutet dies logischerweise, dass KI-Algorithmen am besten funktionieren, wenn sie auf diese Bevölkerungsgruppe angewendet werden. In Bezug auf die Gesichtserkennungstechnologie bedeutet dies, dass die Programme Gesichter mit helleren Hauttönen und männlichen Gesichtsstrukturen am besten erkennen können, während die Genauigkeit bei weißen Frauen sowie bei Schwarzen Menschen und People of Color insgesamt abnimmt. Dies stellt die Behauptung, dass der Einsatz von algorithmischer Software anstelle von Menschen in Entscheidungsprozessen fairer und neutraler ist, erheblich infrage. Der zunehmende Einsatz von Gesichtserkennungstechnologien durch die US-amerikanischen Strafverfolgungsbehörden hat bereits die ethischen Auswirkungen ihrer Bias gezeigt, die sich entlang der Race- und Geschlechtergrenzen nachteilig auswirken.[74] Im Januar 2020 wurde Robert Williams, ein Schwarzer Mann aus Detroit, als erste Person zu Unrecht verhaftet, nachdem die Polizei sein Foto unter Einsatz von Gesichtserkennungstechnologie fälschlicherweise mit dem eines Verdächtigen verwechselt hatte. Alle Anklagen wurden vor Gericht aus Mangel an Beweisen fallengelassen, doch die traumatischen Folgen für Williams und seine Familie sind nicht rückgängig zu machen.[75] Die Selbstverständlichkeit, mit der die Polizei Williams für den Täter hielt, ist nur ein Glied in einer Kette von Tausenden potenziell falschen Treffern eines neuen Verfahrens, mit dem historisch verankerte rassistische Vorurteile und damit verbundene Traumata einer neuen Generation auferlegt werden können. Zivilgesellschaftliche Gruppen und Aktivist*innen in den USA haben sich nachdrücklich gegen den Einsatz von Gesichtserkennungstechnologie durch die Polizei ausgesprochen, die sich ihrer Tendenz zu geschlechtsspezifischen und rassistischen Vorurteilen bewusst ist und sie dennoch weiterhin einsetzt. Diese Bemühungen

72 Martinez, Emmanuel; Kirchner, Lauren: The Secret Bias Hidden in Mortgage-Approval Algorithms, in: The Markup, 25.8.2021, unter: https://themarkup.org/denied/2021/08/25/the-secret-bias-hidden-in-mortgage-approval-algorithms. **73** Criado Perez, Caroline: Invisible Women. Exposing Data Bias in a World Designed for Men, Berlin 2020. **74** Grentzel, Michael: Biased Face Recognition Technology Used by Government: A Problem for Liberal Democracy, in: Philosophy & Technology 34, September 2021, S. 1639–1663, unter: https://link.springer.com/content/pdf/10.1007/s13347-021-00478-z.pdf. **75** Allyn, Bobby: The Computer Got It Wrong: How Facial Recognition Led To False Arrest Of Black Man, 24.6.2020, unter: www.npr.org/2020/06/24/882683463/the-computer-got-it-wrong-how-facial-recognition-led-to-a-false-arrest-in-michig?t=1646734852841.

waren jedoch nicht vergeblich, wie sich zum Beispiel im Juni 2020 zeigte, als Amazon ein einjähriges Moratorium für die Nutzung seiner Gesichtserkennungstechnologie durch die Strafverfolgungsbehörden verhängte, nachdem sich die Beweise dafür verdichtet hatten, dass seine Gesichtserkennungstechnologien verzerrte Ergebnisse liefern. Die Entscheidung fiel auf dem Höhepunkt der Proteste gegen Polizeibrutalität nach der Ermordung von George Floyd durch einen Polizeibeamten in Minneapolis.[76] Im Mai 2021 gab Amazon bekannt, dass das Verbot auf unbestimmte Zeit verlängert würde.[77] IBM hingegen kündigte an, sich vollständig aus dem FRT-Bereich zurückzuziehen, mit der Begründung, dass eine Technologie, die die Verletzung von Menschenrechten ermögliche, gegen die Unternehmenswerte verstoße. Analyst*innen, die die Aktivitäten von IBM beobachten, merkten jedoch an, dass das FRT-Geschäft zu den am wenigsten profitablen Geschäftsfeldern des Unternehmens gehörte, was die Vermutung nahelegt, dass die Entscheidung eher finanzieller als ethischer Natur war.[78]

Die digitale Reproduktion menschlicher Vorurteile hat sowohl in der Polizeiarbeit als auch in der Kriegsführung eine neue Dimension der Überwachung geschaffen, stellt jedoch keineswegs eine neue Entwicklung dar. Ramah Kudaimi vom Action Center on Race and Economy, einer führenden Organisation für Kampagnen zur Sensibilisierung der Öffentlichkeit für die zunehmende Rolle der Technik im MIK, zeigt auf, wie wichtig es ist, die Behauptung zu widerlegen, dass die Technik ein Mittel zur neutralen Kriegsführung sein könne: «Technik ist nie neutral, es stecken immer Menschen dahinter.»[79] Wenn wir Technologie aus diesem Blickwinkel betrachten, werden wir durch unsere Entscheidungen als Verbraucher*innen und Wähler*innen zu Kompliz*innen dieser Entwicklung. Organisationen wie das Action Center on Race and Economy sind angesichts der extremen Geheimhaltung, die die Dreiecksbeziehung zwischen Technologie, Militär und Regierung kennzeichnet, unverzichtbar für die Wahrung sozialer Gerechtigkeit und verfolgen bei ihrer Arbeit «ethische Überlegungen […] und eine bessere Welt, die wir aufbauen wollen»[80], was sich deutlich von einem juristischen Ansatz unterscheidet. Kudaimi macht unmissverständlich deutlich, dass «der Zweck der Partnerschaften für diese großen Technologieunternehmen häufig darin besteht, vom Krieg gegen muslimische und andere Gemeinschaften auf der ganzen Welt zu profitieren».[81]

Ein Punkt, den es abschließend zu beachten gilt, ist die Eignung von Gesichtserkennungstechnologien für die massenhafte Erfassung hochsensibler Daten, die in den Besitz von Drittanbietern gelangen können. Die US-Steuerbehörde (Internal Revenue Service/IRS) sah sich kürzlich gezwungen, ihre Entscheidung rückgängig zu machen, einen Vertrag mit ID.me, einem privaten Softwareunternehmen, abzuschließen. Geplant war, Gesichtserkennungstechnologien als Teil eines Anmeldeverfahrens für Steuerzahler*innen bereitzustellen, die Zugang zu bestimmten Funktionen in ihrem Steuererklärungsprozess wünschten. Von dem Moment an, als die IRS die geplante Partnerschaft ankündigte, formierte sich eine Koalition von Aktivistengruppen für soziale Rechte unter der Leitung der Algorithmic Justice League proaktiv um das Thema und initiierte eine starke und erfolgreiche Kampagne gegen den Vertrag. Zu den Kritikpunkten gehörte, dass ID.me nicht in der Lage sei, die große Menge an sensiblen und hochgradig personalisierten Daten, die gesammelt würden, sicher zu verwahren, und dass die Steuerzahler*innen gezwungen seien, der Sammlung ihrer Daten zuzustimmen, wenn sie auf die Online-Dienste zugreifen wollten. Nach der Ankündigung der IRS, den Vertrag mit ID.me nicht zu verlängern, was die Kampagne als Erfolg wertete, sagte Joy Buolamwini, Gründerin der Algorithmic Justice League: «Wir müssen uns fragen, in welcher Art von Gesellschaft wir leben wollen.»[82]

Die übergeordnete Kategorie, der Gesichtserkennungstechnologien zugeordnet werden können, sind biometrische Daten. Biometrische Daten umfassen ein breites Spektrum von Datensätzen, die sich auf das physische, biologische und mentale Wesen einer Person beziehen, darunter Fingerabdrücke, Netzhautscans, der Gang einer Person, DNA und sogar der Herzschlag. Das US-Verteidigungsministerium hat einen neuen Laser-Vibrometer entwickelt, der die einzigartige Herzsignatur einer Person aus bis zu 200 Metern Entfernung erkennen kann.[83] Immer mehr Staaten entscheiden sich dafür, unterschiedliche Arten von biometrischen Identifizierungsmethoden an ihren Grenzübergängen einzusetzen. Dies geht oft mit Vereinbarungen über den Informationsaustausch zwischen den Staaten, die die Technologien einsetzen, und den anbietenden Unternehmen einher. Darüber hinaus steigt mit der Speicherung großer Datenmengen in internationalen Datenbanken wie etwa bei Interpol[84] oder im Migration Information and Data Analysis System (MIDAS) der Internationalen Organisation für Migration (IOM)[85] oder beim Austausch der Daten zwischen Beteiligten das Risiko des Missbrauchs, des Durchsickerns oder des (versehentlichen oder anderweitigen) Abhandenkommens von Daten in die falschen Hände.

76 Allyn, Bobby: Amazon Halts Police Use Of Its Facial Recognition Technology, in: NPR, 10.6.2020, unter: www.npr.org/2020/06/10/874418013/amazon-halts-police-use-of-its-facial-recognition-technology. **77** Dastin, Jeffery: Amazon extends moratorium on police use of facial recognition software, Reuters, 18.5.2021, unter: www.reuters.com/technology/exclusive-amazon-extends-moratorium-police-use-facial-recognition-software-2021-05-18. **78** Allyn, Bobby: IBM Abandons Facial Recognition Products, Condemns Racially Biased Surveillance, in: NPR, 9.6.2020, unter: www.npr.org/2020/06/09/873298837/ibm-abandons-facial-recognition-products-condemns-racially-biased-surveillance. **79** Transkript des Interviews mit Ramah Kudaimi und Jessica Quiason («Big Tech Sells War»), geführt von den Autor*innen am 14. Dezember 2021, unter: https://docs.google.com/document/d/1pVXPnqhNroZgF1IM7CaJ9ckEp7PkWZ5a/edit?usp=sharing&ouid=113280576371631986367&rtpof=true&sd=true. **80** Ebd. **81** Ebd. **82** Metz, Rachel: Activists pushed the IRS to drop facial recognition. They won, but they're not done yet, in: CNN, 7.3.2022, unter: https://edition.cnn.com/2022/03/07/tech/facial-recognition-activists-irs/index.html. **83** Hambling, David: The Pentagon has a laser that can identify people from a distance – by their heartbeat, in: MIT Technology Review, 27.6.2019, unter: www.technologyreview.com/2019/06/27/238884/the-pentagon-has-a-laser-that-can-identify-people-from-a-distanceby-their-heartbeat. **84** Vgl. www.interpol.int/en/How-we-work/Databases/Our-19-databases.

Die Erhebung und Weitergabe von solchen Mengen an Daten hat sich nach den Anschlägen vom 11. September 2001 beschleunigt und war eines der wichtigsten Mittel, mit denen die USA und ihre Verbündeten den «Krieg gegen den Terror» führen konnten. Die Verabschiedung der Resolution 1373 durch den UN-Sicherheitsrat[86] lieferte die rechtliche Grundlage dafür, und obwohl darin nicht festgelegt wurde, mit welchen Maßnahmen die Staaten ihre Mandate erfüllen sollten, haben sich viele dafür entschieden, dem Beispiel der USA zu folgen und dies so zu interpretieren, dass es sich um umfangreiche Investitionen in Instrumente zur Personalidentifizierung handelt, wie etwa biometrische Daten. Im Jahr 2017 verabschiedete der Sicherheitsrat die Resolution 2396, die die Staaten zum ersten Mal dazu verpflichtete,

> «Systeme zur Erfassung biometrischer Daten zu entwickeln und einzuführen, zu denen potenziell Fingerabdrücke, Fotos, Gesichtserkennung und andere relevante biometrische Daten zur Identifizierung gehören, um Terroristen, einschließlich ausländischer terroristischer Kämpfer, im Einklang mit nationalen Gesetzen und den internationalen Menschenrechtsvorschriften verantwortungsvoll und ordnungsgemäß zu identifizieren.»[87]

Ähnlich der Datenschutz-Grundverordnung in Europa gibt es für diese Methoden Datenschutz-Managementsysteme, allerdings eher in Form von Leitlinien, die offen für Interpretationen, undurchsichtig und mit wenigen oder schwachen Mechanismen zur Durchsetzung ausgestattet sind. Ein Bericht des Human Rights Center der University of Minnesota aus dem Jahr 2020 hat diesbezüglich die Alarmglocken läuten lassen und insbesondere das Fehlen eines Fokus auf die Menschenrechte in UN-Resolution 2396 bemängelt.[88] In dieser Resolution und den ihr vorausgegangenen Resolutionen des UN-Sicherheitsrats (einschließlich Resolution 1373) heißt es, dass die Staaten die Bestimmungen der Resolution im Einklang mit nationalem und internationalem Recht umsetzen müssen. Das heißt, dass dies in einer Weise geschehen muss, die sowohl der wahrgenommenen Bedrohung angemessen als auch für die Eindämmung der vermeintlichen Bedrohung notwendig ist. Die Verbindlichkeit der Resolution könnte allerdings dazu führen, dass die Einhaltung der Grundsätze von Verhältnismäßigkeit und Notwendigkeit heruntergespielt oder übersehen wird. Dies gibt Anlass zur Sorge, dass die Verbindlichkeit und die erwähnten Bedenken von Staaten als eine Art Freibrief betrachtet werden könnten, jede Person ins Visier zu nehmen, deren Profilmerkmale mit denen übereinstimmen, die üblicherweise mit Terrorismus in Verbindung gebracht werden – ohne Rücksicht auf menschenrechtliche Grundsätze und ohne jegliche Befürchtung von Konsequenzen. In der Vergangenheit hat dies dazu geführt, dass unverhältnismäßig viele People of Color, Muslim*innen oder als muslimisch wahrgenommene Personen sowie Personen, die die Staatsbürgerschaft eines überwiegend muslimischen Landes und/oder eines Landes haben, aus dem bereits Terrorist*innen hervorgegangen sind, ins Visier genommen wurden.

Diese Probleme stehen im Mittelpunkt der Arbeit von zivilgesellschaftlichen Organisationen und den Aktivist*innen, die für diese Studie befragt wurden. Forscher*innen, Aktivist*innen, Menschenrechtsanwält*innen und Politiker*innen, die in diesem Bereich tätig sind, sind sich in ihrem Anliegen einig. Sie schlagen jetzt Alarm und fordern die Staaten auf, Maßnahmen zu ergreifen, um die Rechte von Personen zu wahren und zu schützen, die bereits in erheblichem Maße unter ungerechtfertigter Verfolgung zu leiden haben, und sie vor weiterem Schaden zu bewahren.

3.3 APPLE UND FACEBOOK – KLEINERE AKTEURE AUF DEM MARKT FÜR MILITÄRISCHE INNOVATIONEN

Unter den Unternehmen, mit denen das US-Verteidigungsministerium eine Zusammenarbeit anstrebt, erscheint Apple als vergleichsweise kleiner Akteur. 2015 wurde der Konzern Mitglied eines Konsortiums von 162 Unternehmen, der FlexTech Alliance, das damit beauftragt wurde, verschiedene Hardware-Technologien für Verteidigungszwecke zu entwickeln. Das Projekt im Wert von 75 Millionen US-Dollar war auf die Entwicklung flexibler elektronischer Systeme ausgerichtet, die in Materialien wie Silikon eingebunden werden können und leicht genug sind, um von Soldat*innen getragen zu werden, gleichzeitig jedoch widerstandsfähig genug, um in die Außenhülle von Flugzeugen integriert zu werden.[89] Für Apple war das die erste Zusammenarbeit mit dem Militär. Das Management war besorgt darüber, dass die Gewinne des Unternehmens stagnieren würden, sollten keine neuen und alternativen Märkte zur Expansion erschlossen werden. Traditionell macht der Verkauf von iPhones den Großteil der Unternehmensgewinne aus. Angesichts einer steigenden Zahl von Anbietern mit vergleichbaren Produkten konnte nur die Eroberung alternativer Märkte einen möglichen Einbruch des Aufwärtstrends bei der Gewinnspanne verhindern.[90] Das früher als Facebook Inc. bekannte Unternehmen Meta Platforms Inc. lässt sich, ähnlich wie Apple, mit Aufträgen des Heimatschutzministeriums im Wert von 365.000 US-Dollar und kleineren Aufträgen des Verteidigungsministeriums im Wert von 170.000 US-Dollar wohl als relativ kleiner Akteur im Kontext militärischer Ausschreibungen bewerten.[91]

85 Vgl. www.iom.int/sites/g/files/tmzbdl486/files/documents/midas-brochure18-v7-en_digitall.pdf. **86** S/RES/1373 (2001), verabschiedet am 28. September 2001, unter: www.unodc.org/pdf/crime/terrorism/res_1373_english.pdf. **87** S/RES/2396 (2017), S. 8, verabschiedet am 21. Dezember 2017, unter: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N17/460/25/PDF/N1746025.pdf?OpenElement. **88** Huszti-Orbán, Krisztina/Ni Aoláin, Fionnuala: Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business?, Human Rights Center, University of Minnesota, 2020, unter: www.ohchr.org/sites/default/files/Documents/Issues/Terrorism/Use-Biometric-Data-Report.pdf. **89** Apple, Boeing partner with US Defence for wearables, in: Itnews, 31.8.2015, unter: www.itnews.com.au/news/apple-boeing-partner-with-us-defence-for-wearables-408632. **90** Green, Adam: Apple Inc. (AAPL) Is About to Become a Military Contractor, in: LearnBonds, 9.10.2020, unter: https://learnbonds.com/news/apple-inc-aapl-is-about-to-become-a-military-contractor. **91** Vgl. Daten der Kampagne «Big Tech Sells War» unter: https://bigtechsellswar.com.

4 ANALOGIEN UND UNTERSCHIEDE ZU US-INNOVATIONS-TENDENZEN IN EUROPA UND DEUTSCHLAND

Lenken wir den Blick von den USA auf Europa und betrachten insbesondere Deutschland, macht es den Eindruck, als ob es seitens der deutschen Politik kaum Bemühungen gibt, einen Innovationsrahmen zu schaffen, der mit der Third Offset Strategy (TOS) des Pentagon vergleichbar ist. Christian Mölling, Forschungsdirektor für die Deutsche Gesellschaft für Auswärtige Politik (DGAP), kam 2018 zu dem Schluss, «dass es zwar viele staatliche und zivile Akteure gibt, die die Bedeutung von Investitionen in verteidigungsbezogene Innovation in Deutschland erkennen, dies sich allerdings nur sehr allgemein vollziehe. In Berlin existiert ein Bewusstsein dafür, dass eine wettbewerbsfähige Verteidigungsindustrie und ein leistungsfähiges Militär Investitionen in zivile Unternehmen, die Dual-Use-Technologien entwickeln, erfordern. Aktuell gibt es jedoch weder offizielle Stellungnahmen noch Einschätzungen, die einen Ansatz für die künftige Vorgehensweise enthalten. […] Um die technologische Souveränität eines Landes zu wahren, ist es allerdings notwendig, zentrale Technologien zu schützen sowie militärische Fähigkeiten und Ressourcen zu sichern.»[92]

Mit der Gründung von an die Bundeswehr angegliederten Forschungsinstitutionen wie dem Cyber Innovation Hub (CIH.Bw)[93] schon im Jahr 2017 und dem Zentrum für Digitalisierungs- und Technologieforschung (DTEC.Bw)[94] 2020 wird jedoch deutlich, dass eine militärische Innovationsstruktur, die auf den Kernelementen der TOS basiert, mittlerweile zu einer Priorität der deutschen Verteidigungspolitik geworden ist. Die aktuelle Bestandsaufnahme zum Innovationspotenzial der Bundeswehr im Kontext mit den Fortschritten am CIH.Bw spiegelt in der Tat die Auffassung von Chin und Meunier über ein sich wandelndes technologisches Innovationsumfeld wider, das vom zivilen Sektor angetrieben wird: «Während in den letzten Jahrhunderten zumeist der Staat, allen voran das Militär, entscheidender Treiber technologischen Fortschritts war, werden disruptive Innovationen heute primär durch zivile Akteure vorangetrieben. Diese werden immer weniger abhängig von kritischer Masse – für Unternehmen wird es somit immer leichter, disruptive Technologien auf den Markt zu bringen.»[95] Das DTEC.Bw-Modell, das auf einer Kooperation zwischen Bundeswehruniversitäten, privaten deutschen Stakeholdern – sowohl aus dem etablierten Unternehmenssektor als auch aus der florierenden Start-up-Szene – sowie dem Verteidigungsministerium basiert, erinnert verblüffend an die vom US-Verteidigungsministerium entwickelten Kooperationsmodelle.

Was die Wahrung der technologischen Souveränität Deutschlands angeht, so belegen Initiativen wie das großangelegte Cloud-Computing-Projekt GAIA-X, welche Anstrengungen in letzter Zeit unternommen wurden, um dieses Ziel zu erreichen. Gleichzeitig ist jedoch offensichtlich, dass die deutsche (und europäische) Führung sehr stark von externen Anbietern abhängig ist, deren Fähigkeiten die führender europäischer Technologieunternehmen übersteigen. Exemplarisch dafür ist die Zusammenarbeit mit einer großen Zahl internationaler Hyperscaler.[96] Im nächsten Kapitel wird untersucht, wie dieses Projekt ursprünglich konzipiert wurde, wie es sich im Laufe der Zeit entwickelt hat und wie es sein selbstgestecktes Ziel der Autonomie von internationalen Tech-Dienstleistern untergräbt, während es gleichzeitig Unterstützung von fragwürdigen Partnern erhält.

4.1 GAIA-X

GAIA-X wurde 2019 mit dem Ziel ins Leben gerufen, «eine vertrauenswürdige und souveräne digitale Infrastruktur nach europäischen Regeln zu entwickeln».[97] Es stellt den deutsch-französischen Versuch dar, eine europäische Open-Source-Alternative zu den Cloud-Computing-Technologien US-amerikanischer und asiatischer Unternehmen zu schaffen, die aktuell den Markt dominieren. Um das Vorhaben zu realisieren, gründeten 22 Partner*innen aus Wissenschaft, Technik und Wirtschaft im September 2020 zunächst die gemeinnützige, in Belgien registrierte Organisation GAIAX European Association for Data and Cloud AISBL, in der sich deutsche Großunternehmen wie BMW, Bosch, Deutsche Telekom, Fraunhofer Gesellschaft, SAP und Siemens zusammenfanden.[98] Während eine militärische Anwendung in der öffentlichen Darstellung nicht als Hauptzweck des Projekts beschrieben wird, bezeichnet BWI, der IT-Provider der Bundeswehr, GAIA-X als leistungsfähiges Hilfsmittel für die Streitkräfte, um «die erforderlichen Kontroll- und Handlungsmöglichkeiten im Cyber- und Informationsraum [aufrechtzuerhalten], um ihren verfassungsgemäßen Auftrag erfüllen zu können – selbstbestimmt und frei von ungewollter Einflussnahme Dritter».[99]

Seit ihrer Gründung wuchs die Zahl der an der Initiative beteiligten Akteure rasch auf über 300 an. Dabei hat insbesondere die Teilnahme chinesischer Partner wie Huawei oder Alibaba sowie von großen US-Konzernen Kritik nach sich gezogen. «Während viel über

92 Mölling, Christian: Defense Innovation and the Future of Transatlantic Strategic Superiority: A German Perspective, The German Marshall Fund, 23.3.2018, unter: www.gmfus.org/news/defense-innovation-and-future-transatlantic-strategic-superiority-german-perspective#_ftnref2. **93** Vgl. www.cyberinnovationhub.de. **94** Vgl. https://dtecbw.de/home. **95** Bundesverband der Deutschen Industrie: Digitale Innovationen für die Bundeswehr, 15.5.2019, unter: https://bdi.eu/artikel/news/digitale-innovationen-fuer-die-bundeswehr. **96** Ein Hyperscaler ist ein Cloud-Computing-Anbieter mit der Fähigkeit zu einer massiven Skalierbarkeit der Infrastruktur (Anm. d. Ü.). **97** Knoll, Andreas: European Association for Data and Cloud - GAIA-X AISBL is officially founded, in: Elektroniknet.de, 9.2.2021, unter: www.elektroniknet.de/international/gaia-x-aisbl-is-officially-founded.183417.html. **98** Für eine vollständige Liste der Gründungsmitglieder vgl. ebd. **99** BWI: Digitale Souveränität für Deutschland und Europa: Der Weg zwischen Autarkie und Abhängigkeit, 24.9.2020, unter: www.bwi.de/news-blog/blog/artikel/digitale-souveraenitaet-fuer-deutschland-und-europa-der-weg-zwischen-autarkie-und-abhaengigkeit.

Cloud-Souveränität geredet wird, stützen sich die aktuellen Pläne europäischer Regierungen im Rahmen von GAIA-X noch immer auf US-Technologien von AWS, Google und Microsoft, die einer ausländischen Überwachung ausgesetzt sind»,[100] so der Kommentar der European Cloud Industrial Alliance (EUCLIDIA), die 2020 von 23 Unternehmen aus der Branche gegründet wurde und die Entwicklung begleitet.[101]

Jack Poulson, ehemals Google-Datenanalyst und Gründer von Tech Inquiry,[102] hebt die zentrale Rolle hervor, die Verträgen im Bereich des Cloud-Computings dabei zukomme, privatwirtschaftliche Technologiebeiträge zu Regierungsaufträgen zu entpolitisieren und sie als irrelevant für militärische oder inländische polizeiliche Anwendungen zu deklarieren. Vor diesem Hintergrund beleuchtet er mögliche Konsequenzen und betont den Handlungsbedarf für zivilgesellschaftliche Akteure.

«Wenn diese Tech-Unternehmen Cloud-Computing als ethisch neutral hinstellen, wie wir es seit Maven gesehen haben, wie können wir aufzeigen, wozu sie aktiv beitragen? Welche Rechenschaftsmöglichkeiten existieren in dieser Phase überhaupt, abgesehen von Leaks der internen Kommunikation durch Angestellte? Je eher wir in der Lage sind, zu zeigen, welche Wirkung diese sogenannten Black-Box-Verträge haben, desto eher können wir dem Narrativ, wonach diese materielle Unterstützung für Streitkräfte und Geheimdienste weltweit nicht mehr ist als die Lieferung einer Ladung Rohstahl, etwas entgegensetzen und aufzeigen, dass Cloud Computing einen tatsächlichen und direkten Beitrag zu deren Aktivitäten darstellt.»[103] Obwohl die GAIA-X-Initiative das grundsätzlich unstrittige Ziel einer unabhängigeren und sichereren digitalen Infrastruktur in einer von der Datenschutz-Grundverordnung regulierten Umgebung verfolgt, ist offensichtlich, dass eine genaue Prüfung ihrer Ausgestaltung von entscheidender Bedeutung sein wird, um zu verhindern, dass Anwendungen die individuellen Freiheiten europäischer Bürger*innen einschränken und/oder die demokratische Grundordnung der europäischen Mitgliedsstaaten gefährden.

Noch größere Bedenken rief die Beteiligung von Palantir hervor, einem Unternehmen, das auf die Integration großer Datenmengen spezialisiert ist und den US-Geheimdiensten zuarbeitet. Im Dezember 2020 verkündete das Unternehmen, «stolzes Mitglied von GAIA-X seit Tag 1» zu sein,[104] ein Vorgang, der Beobachter*innen zufolge «bei den Menschen in Europa zumindest ein Stirnrunzeln hervorrufen sollte».[105] Angesichts der lautstarken Proteste aus der Opposition und sogar aus der Wirtschaft sollte man meinen, dass dies tatsächlich der Fall war. Die Referentin für Netzpolitik der Linksfraktion im Bundestag, Anne Roth, kommentierte auf Twitter: «Und das war's dann mit dem Vertrauen in die europäische Souveränität.»[106]

Das von Peter Thiel mitgegründete Palantir hat den Ruf, sowohl für Regierungen in liberalen Demokratien als auch für autokratische Staaten KI-Werkzeuge zu entwickeln, mit denen Bürger*innen und Grenzen überwacht werden können.[107] Christopher Soghoian, technischer Experte der US-Bürgerrechtsorganisation American Civil Liberties Union (ACLU), nannte das Unternehmen «eine bedeutende Kraft im überwachungsindustriellen Komplex».[108] GAIA-X ist nicht der erste große Deal des Überwachungsunternehmens in Europa. Seit 2016 nutzt Europol dessen Anti-Terror-Werkzeug Gotham für Ermittlungen.[109] Seit 2017 ist die Software unter dem Namen Hessendata auch in Hessen im Einsatz.[110]

Im Oktober 2020, noch vor der GAIA-X-Ankündigung von Palantir, sagte Sophie in't Veld, niederländisches Mitglied des Europäischen Parlaments und Mitglied der Fraktion Renew Europe: «Ein Unternehmen mit einer Bilanz wie Palantir sollte für kein EU-weites Projekt als Partner in Betracht gezogen werden, und die Europäische Kommission weiß das. Das Handeln dieses heimlichen Konzerns steht im Widerspruch zu den europäischen Werten, die vielen EU-Bürgern wichtig sind, wie etwa Datenschutz, Grundfreiheiten und eine transparente Regierungsarbeit – ganz zu schweigen, was es bedeuten könnte, mit einem Auftragnehmer von US-Geheimdiensten zu kooperieren.»[111] Neben Bedenken hinsichtlich der Datensouveränität zeigen jüngste Berichte auch, dass das GAIA-X-Projekt an einem Übermaß an Bürokratie krankt, an mangelndem Fokus und chaotischen Zuständen angesichts gegensätzlicher Interessen. Vor diesem Hintergrund beschloss der französische Cloud-Provider Scaleway, seinen Vertrag mit dem Projekt im November 2021 nicht zu verlängern.[112]

Ungeachtet der engen transatlantischen Beziehungen Deutschlands bezeugt der Vertrag die inhärente Ungleichheit zwischen dem Maß an Kooperation mit den US-amerikanischen Partnern aus dem Silicon Valley einerseits und der Fähigkeit der europäischen Regierungen andererseits, ihre strategische Autonomie

100 Vgl. EUCLIDIA: Background: European tech innovation, o. J., unter: www.euclidia.eu/background. **101** Vgl. Steins, Teresa/Kerkmann, Christof: Gaia-X-Gipfel in Mailand: Das Cloud-Projekt wird zum Problemfall, in: Handelsblatt, 18.11.2021, unter: www.handelsblatt.com/politik/deutschland/datensouveraenitaet-gaia-x-gipfel-in-mailand-das-cloud-projekt-wird-zum-problemfall/27809120.html?ticket=ST-56859-kZqD5Q9O2MZjdewebntt-cas01.example.org. **102** Tech Inquiry ist eine gemeinnützige Organisation, die abgeschlossene Vergaben analysiert, um die Verbindungen zwischen US-Regierung und privaten Tech-Dienstleistern transparenter zu machen. **103** Vgl. Interview mit Jack Poulson (Tech Inquiry), von den Autor*innen am 22. November 2021 geführt, unter: https://docs.google.com/document/d/1uado2xvqcdTs5yIDljbxD7N6QBmmc5bu/edit?usp=sharing&ouid=113280576371631986367&rtpof=true&sd=true. **104** Palantir: Palantir and GAIA-X, 18.12.2020, unter: https://blog.palantir.com/palantir-and-gaia-x-85ab9845144d. **105** Vgl. Interview mit Jack Poulson (Tech Inquiry). **106** Vgl. Anne Roths Twitter-Antwort auf Palantir und den damaligen Bundesminister für Wirtschaft und Energie, Peter Altmaier (CDU), unter: https://twitter.com/annalist/status/1340035887619592195. **107** Malik, Kenan: Think only authoritarian regimes spy on their citizens?, in: The Guardian, 22.9.2019, unter: www.theguardian.com/commentisfree/2019/sep/22/think-only-authoritarian-regimes-spy-on-their-citizens, letzter Zugriff: 13. Dezember 2021. **108** Hardy, Quentin: Unlocking Secrets, if Not Its Own Value, in: New York Times, 31.5.2014, unter: www.nytimes.com/2014/06/01/business/unlocking-secrets-if-not-its-own-value.html. **109** In't Veld, Sophie: Palantir is not our friend, in: about:intel – European Voices on Surveillance, 20.10.2020, unter: https://aboutintel.eu/palantir-eu-independence. **110** Von Bebenburg, Pitt: Polizei in Hessen: Datenschützer prüft Palantir-Einsatz, in: Frankfurter Rundschau, 10.5.2021, unter: www.fr.de/rhein-main/landespolitik/polizei-in-hessen-datenschuetzer-prueft-palantir-einsatz-90530135.html. **111** In't Veld: Palantir. **112** Mahn, Jan: Gaia-X: Cloudprovider Scaleway zieht die Reißleine und tritt aus, in: heise online, 18.11.2021, unter: www.heise.de/news/Gaia-X-Cloudprovider-Scaleway-zieht-die-Reissleine-und-tritt-aus-6271342.html.

weiter auszubauen. Während sich die europäische Führung darum bemüht, eine technologische Infrastruktur nach US-amerikanischem oder chinesischem Vorbild aufzubauen, zementiert sie, indem sie den Kooperationsraum zwischen privaten Tech-Innovatoren aus aller Welt und den europäischen Regierungen stetig weiter vergrößert, gleichzeitig die Bindungen, die sie so verzweifelt zu kappen versucht. Ganz offensichtlich vermittelt dieser Raum ein trügerisches Gefühl der Autonomie und Sicherheit. Er bietet aber darüber hinaus auch reichlich Gelegenheiten, Kontakte zu europäischen F&E-Sektoren im privaten und staatlichen Bereich zu vertiefen sowie den Zugang zu ihnen im Sinne der Erreichung nationaler TOS-Ziele auszuweiten. Jack Poulson beschreibt, bis zu welchem Grad das im öffentlich-privaten Innovationsraum in Europa bereits eine Realität darstellt.

«Dass US-Tech-Giganten ein europäisches Konsortium unterwandern, dessen einziger Zweck es war, der Macht der US-Tech-Giganten entgegenzuwirken, hat etwas Kolonialistisches an sich», sagt Poulson. «Natürlich tauchen an allen Ecken und Enden Menschenrechtsfragen auf, etwa wenn Palantir hier Fuß fassen und Technologien verkaufen will, mit denen der Grenzschutz verschärft oder Abschiebungen erleichtert werden können. Zudem kann davon ausgegangen werden, dass diese Unternehmen enge Beziehungen zu Geheimdiensten in ganz Europa unterhalten.»[113] In Bezug auf das Engagement von US-Unternehmen bei der Intensivierung dieser Beziehungen, führt Poulson weiter aus: «Ich sehe wirklich nicht, warum es sich grundlegend anders entwickeln sollte als in den USA, auch wenn man annehmen könnte, dass Europa versuchen wird, seine eigenen Entsprechungen für diese Unternehmen zu schaffen.»[114]

4.2 ÜBER GAIA-X HINAUS – DIE ZUKUNFT DES MILITÄRISCHEN INNOVATIONSRAUMS IN DEUTSCHLAND

Während der verstärkte Ausbau von Ressourcen, die insbesondere auf eine Infrastrukturverbesserung für militärische Innovation in Deutschland abzielen, bislang nicht auf der Unterstützung durch zivile Dienstanbieter wie Google beruht, ähneln diese Ressourcen doch in starkem Maße Investitionsstrukturen für F&E, wie sie in den USA etabliert wurden. Diese Strategie setzt auf ein gemeinsames Verständnis davon, in welche Richtung sich zukünftige Strategien auf dem Schlachtfeld entwickeln werden. In ihrer vergleichenden Untersuchung zum Kooperationspotenzial zwischen Deutschland und Großbritannien identifizieren Becker, Mölling und Schütz drei zentrale übergeordnete Trends, die die deutsche Strategie der militärischen Innovation kennzeichnen:

– der «Aufklärungs-Feuer-Komplex, bei dem das Netzwerk wichtiger ist als einzelne Assets»;[115]
– das «vollständig transparente Schlachtfeld durch den zunehmenden Einsatz von Sensoren sowie Kommando- und Kontrollkapazitäten, die in der Lage sind, die Fülle von Informationen aus diesen Sensoren zu verarbeiten»[116] sowie
– die «menschliche Rolle bei dieser Art von Kriegsführung», insbesondere aufgrund des Umstands, dass «der Einsatz von Systemen mit Personenbesatzung sowie von menschlichem Bedienungspersonal eine wachsende Gefahr darstellt – sowohl für deren Leben als auch für die militärische Effizienz».[117]

Die Autor*innen betonen jedoch, dass «der Mensch seine Funktion als Entscheidungsträger beibehalten muss»[118] – nicht allein aus ethischen Gründen, sondern auch um zu vermeiden, dass es im Rahmen einer Debatte über vollständig autonome Systeme zu öffentlichem Widerspruch kommt. Daraus entstehende Kontroversen könnten potenziell negative Auswirkungen auf der politischen Ebene und damit auch für die Finanzierung nach sich ziehen. Um den Herausforderungen, die aus diesen zu erwartenden Entwicklungen entstehen, wirksam begegnen zu können, versuchen Initiativen wie das CIH.Bw und das DTEC.Bw, die Verbindungen zum privaten Sektor zu fördern und Räume für eine zivile Zusammenarbeit aus verschiedenen, sich gegenseitig unterstützenden Blickwinkeln zu schaffen.

Während das CIH.Bw darauf abzielt, «innovative Technologien in der Start-up-Welt [zu] identifizieren, mit den Nutzern weiter[zu]entwickeln und möglichst schnell im Alltag nutzbar [zu] machen»,[119] arbeitet das DTEC.Bw darauf hin, ein universitäres Innovationsumfeld aufzubauen, das von den beiden deutschen Bundeswehruniversitäten in München und Hamburg geleitet wird. Ein Beispiel dafür ist die Zusammenarbeit des DTEC.Bw mit der privatwirtschaftlichen Hensoldt AG bei der Entwicklung eines fortgeschrittenen KI-gestützten Entscheidungswerkzeugs für den militärischen Gebrauch. Diese Initiative ist Teil des DTEC.Bw-finanzierten Projekts «Ghostplay»,[120] das die Fortschritte bei automatisierten Waffensystemen direkt mit der deutschen Privatwirtschaft verknüpft.

Mit der Ausweitung ausschließlich europäischer Partnerschaften auf internationale Beteiligungen im Rahmen von GAIA-X erscheint es durchaus plausibel, dass die aktuelle Beschränkung der Forschungsvorhaben auf deutsche Unternehmenspartner zugunsten einer Einbindung US-amerikanischer oder internationaler Akteure aufgegeben werden könnte, um künftig noch bessere Ergebnisse zu erzielen. Die Initiative für solche Großprojekte könnte tatsächlich vom Silicon Valley ausgehen. Munira Lokhandwala kommt auf Grundlage ihrer Beobachtungen zum US-amerikanischen Tech-Innovationsmarkt zu dem Schluss, dass es «in den USA einen Sättigungspunkt geben wird, ab

113 Vgl. Interview mit Jack Poulson (Tech Inquiry). **114** Ebd. **115** Becker, Sophie/Mölling, Christian/Schütz, Torben: Learning together: UK-Germany cooperation on military innovation and the future of warfare, hrsg. von Hanns-Seidel-Stiftung (CSU), The Policy Institute und King's College London, London 2020, S. 2, unter: https://dgap.org/sites/default/files/article_pdfs/uk-germany_military_innovation_.pdf. **116** Ebd. **117** Ebd. **118** Ebd. **119** Bundesverband der Deutschen Industrie: Digitale Innovationen. **120** Vgl. DTEC.Bw: GhostPlay – Simulation für KI-basierte Entscheidungsverfahren, o. J., unter: https://dtecbw.de/home/forschung/hsu/projekt-ghostplay.

dem nicht mehr so viel Geld [aus staatlichen Auftragsvergaben in den USA] zu holen sein wird, um weiteres Wachstum und Gewinne zu gewährleisten. Sie werden sich dann nach Aufträgen außerhalb der USA umsehen. Und ich denke, dass es sehr wichtig sein wird, diese Entwicklung im Auge zu behalten, wie es bereits zahlreiche Organisationen weltweit tun, da die Werkzeuge, die sie an anderen Orten der Welt bauen wollen genauso gefährlich und genauso bedenklich sind wie jene, die sie aktuell in den USA entwickeln.»[121]

Ein zentraler Unterschied zwischen den USA und Europa liegt im Rechtsrahmen, in Europa ist die Grenze zwischen militärischer und ziviler technologischer Innovation strenger definiert. Die 2018 eingeführte Datenschutz-Grundverordnung (DSGVO) legt eine hohe Messlatte dafür an, wann und in welcher Form Daten innerhalb von Europa genutzt werden können, und findet in allen Mitgliedsstaaten Anwendung. Ihre umfassenden Rechtsverordnungen gelten weltweit als der beste Schutz für personenbezogene Daten.[122] Sie enthält wichtige Schutzbestimmungen wie das Recht auf Vergessenwerden (Artikel 17),[123] das besagt, dass eine Person das Recht hat, die Löschung ihrer Daten zu verlangen, wenn der ursprüngliche Zweck ihrer Erhebung entfallen ist. Zum Thema algorithmischer Bias ist Artikel 22[124] «Automatische Entscheidungen im Einzelfall einschließlich Profiling» von besonderer Relevanz, der Personen das Recht zuspricht, keiner ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden, die sie in erheblicher Weise rechtlich beeinträchtigen könnte. Die DSGVO sieht auch Schutzmechanismen vor wie etwa die Anforderung, dass die Prozesse jeglicher Systeme, die unter die DSGVO-Zuständigkeit fallen, den Grundsatz des eingebauten Datenschutzes (Privacy by Design/PbD) zu berücksichtigen haben. Dazu gehört, dass personenbezogene Daten automatisch geschützt werden und keine weiteren Schritte dafür erforderlich sind. Des Weiteren legt die DSGVO fest, dass jede staatliche oder öffentliche Einrichtung, die personenbezogene Daten erhebt, eine Datenschutz-Folgenabschätzung (DSFA) durchzuführen hat, ein Prozess, der die Risiken identifiziert, die mit der Erhebung und Speicherung der Daten einer Person verbunden sind. Diese Komponente ist besonders wichtig für Bereiche wie die Nutzung von Gesichtserkennungstechnologien durch Strafverfolgungsbehörden, da sie sicherstellen soll, dass der Prozess kontrolliert wird und die Datenerhebung gerechtfertigt ist.[125] Die DSFA ist aber auch deswegen von besonderer Bedeutung, weil sie Einrichtungen und Unternehmen dazu zwingt, die von ihnen verwendeten Algorithmen zu analysieren und zu verstehen, um die Datenerfassung zu rechtfertigen. Ein zusätzlicher Bestandteil der DSFA ist die Vorschrift, dass jede öffentliche Einrichtung, deren Kerntätigkeit die umfangreiche und systematische Erfassung personenbezogener Daten umfasst, insbesondere wenn es um strafrechtliche Fragen geht, auch Datenschutzbeauftragte einstellen muss, eine Art eingebaute*r Whistleblower*in. Die Rolle der Datenschutzbeauftragten besteht darin, die Einhaltung der DSGVO der jeweiligen Institution zu überwachen und sie zu beraten sowie jegliche Verstöße dem oder der nationalen Datenschutzbeauftragten zu melden. Die Durchsetzung der Datenschutzregulierung der DSGVO erstreckt sich jedoch auch auf Gebiete außerhalb Europas, da alle Einrichtungen und Unternehmen, die innerhalb der EU agieren oder Verträge mit EU-Institutionen eingehen wollen, selbst wenn sie ihren Sitz außerhalb der EU haben, ebenfalls die DSGVO einhalten müssen.[126]

121 Vgl. Interview mit Munira Lokhandwala (LittleSis), von den Autor*innen am 2. Februar 2022 geführt, unter: https://docs.google.com/document/d/1erwtg_LcvxUcRK12vu2Kp-heYtV4YYgs/edit?usp=sharing&ouid=113280576371631986367&rtpof=true&sd=true. **122** Almeida, Denise/Shmarko, Konstantin/Lomas, Elizabeth : The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of US, EU, and UK regulatory frameworks, in: AI and Ethics 2/2022, S. 377–387, unter: https://link.springer.com/article/10.1007/s43681-021-00077-w. **123** Artikel 17, DSGVO, unter: https://dsgvo-gesetz.de/art-17-dsgvo. **124** Artikel 22, DSGVO, unter: ebd. **125** Almeida u. a.: The ethics of facial recognition. **126** Ebd.

5 MÖGLICHE PERSPEKTIVEN

5.1 DEN WIDERSTAND ORGANISIEREN – HERAUSFORDERUNGEN UND CHANCEN FÜR WHISTLEBLOWER*INNEN

Die vielfach belegten engen Verbindungen zwischen großen US-Tech-Unternehmen und militärischen Projekten – sowohl in den Vereinigten Staaten als auch international – werfen die Frage auf, wie wir mit ihren Auswirkungen auf nachhaltige Weise umgehen können. Dabei gibt es eine Vielzahl an möglichen Vorgehensweisen. Der Weg eines ehemaligen Tech-Mitarbeiters, der bei der Analyse und Veröffentlichung potenziell bedenklicher Verträge behilflich war, verdeutlicht jedoch vielleicht am besten die Schwierigkeiten und Fallstricke, die mit einem solchen Unterfangen verbunden sind, sowie die Ressourcen, die erforderlich sind, um sie zu überwinden. Nahezu alle verfügbaren investigativen Berichte zu diesem Thema basieren auf Informationen, die von Jack Poulsons gemeinnütziger Organisation Tech Inquiry bereitgestellt wurden. Jack Poulson kündigte 2018 aus Protest gegen Googles Projekt Dragonfly, eine mit der Zensurbehörde kooperierende Suchmaschine für den chinesischen Markt, das später eingestellt wurde. Rückblickend bemerkt er, dass der Schritt in den Nonprofit-Sektor nicht unmittelbar erfolgte. «Etwa eineinhalb Jahre lang haben wir in überaus maschinenstürmerischer Manier unseren gesamten Fokus darauf gelegt, mit Journalisten zu sprechen und die Öffentlichkeit für ein Thema zu sensibilisieren, mit dem Menschen im Nonprofit-Sektor seit Längerem vertraut waren.»[127]

Der Ansatz, sowohl die Bedingungen für Vergaben als auch die Verbindungen zwischen den Auftragnehmern zu untersuchen, entsprang einer Beobachtung der Branche. «Bei Gesprächen mit Führungskräften wurde mir klar, dass Menschenrechtsbedenken sie nicht großartig interessierten. Es ging ihnen vielmehr darum, die engen Bande zwischen Militär und US-Tech-Firmen aufrechtzuerhalten»,[128] erinnert er sich. «In diesem Zusammenhang wurde mir immer bewusster, wie viel Bürokratie diese Beziehungen umgibt, ob es sich nun um das Defense Innovation Board,[129] die Defense Innovation Unit,[130] die National Security Commission on Artificial Intelligence,[131] In-Q-Tel[132] oder andere handelte. Ich begann, Anfragen nach dem Freedom of Information Act zu einigen dieser Beziehungen zu stellen, und kam zu dem Schluss, dass die Beziehungen zwischen diesen Unternehmen einfach nicht gut dokumentiert sind.»[133]

Tech Inquiry ist aus dieser Praxis heraus entstanden und beherbergt weitere ehemalige Mitarbeiter*innen aus der Technologieindustrie, die sowohl im Vorstand sitzen als auch zur Forschung der gemeinnützigen Organisation beitragen. Obwohl ihre Arbeit nicht explizit auf Abrüstung ausgerichtet ist, schlagen einige Mitglieder durch ihr Engagement in antimilitaristischen Kampagnen eine Brücke zu pazifistischen Bewegungen. Ein bekanntes Beispiel ist die bereits erwähnte «Campaign to Stop Killer Robots». «Mehrere Mitglieder sowie einige Vorstandsmitglieder von Tech Inquiry haben dabei eine wichtige Rolle gespielt. Liz O'Sullivan beispielsweise verließ ClarifAI wegen dessen Mitwirkung an der Drohnenüberwachung, Laura Nolan verließ Google wegen dessen Beteiligung am Projekt Maven.»[134]

5.2 ANTWORTEN AN UNERWARTETER STELLE

Die Verbindungen zwischen großen US-Tech-Unternehmen und der US-Regierung allein daraufhin zu betrachten, welche Auswirkungen sie im militärischen Bereich haben, wäre aber nicht sonderlich hilfreich, um herauszufinden, wie Tech-Unternehmen ihre Geschäfte führen, sagt Poulson. «Ich neige zu der Ansicht, dass Tech-Unternehmen ihre Technologien schlicht überall verkaufen wollen. Von einer anderen Warte aus betrachtet erscheinen sehr viele militärische Werkzeuge wiederum als weiterentwickelte Technik, die später in die Hände des Heimatschutzministeriums gelangt. Dazu gehören Drohnenüberwachung, automatische Systeme zur Grenzüberwachung, Gesichtserkennung usw. Und solche Systeme gelangen dann nach und nach in die Hände lokaler Behörden.»[135]

Eine Ausweitung der Analyse auf ein breiteres Spektrum von Verträgen kann Probleme in Bereichen aufdecken, die sonst vielleicht unberücksichtigt bleiben würden, findet Poulson. «Meiner Meinung nach führen eine genauere Untersuchung der Vergabepraxis sowie ein tieferes Verständnis der Bürokratie im US-Apparat zu der Erkenntnis, dass die Geheimdienste mit vielen Behörden sehr viel enger zusammenarbeiten, als vielen bewusst ist.»[136]

Diese Vorgehensweise trägt weiter dazu bei, die vermeintliche ethische Neutralität von Verträgen in der öffentlichen Wahrnehmung neu zu kontextualisieren. Ein Bereich, auf den sich dies besonders auswirken könnte, sei das Cloud-Computing, so Poulson. «Einer unserer größten Erfolge war der Nachweis, dass Google Cloud an ein Unternehmen namens Thundercat Technology verkauft wurde, einem sehr umtriebigen Vertragsnehmer der US-Zoll- und Grenzschutzbehörde. Wir fanden Beweise, wonach Thundercat plante, die KI von Google Clouds zu nutzen, um Wärmebilder aus der

127 Vgl. Interview mit Jack Poulson (Tech Inquiry). **128** Ebd. **129** Rat für Innovationen im Verteidigungsbereich; unabhängiges Gremium, das das US-Verteidigungsministerium berät. Den Vorsitz hatte jahrelang der ehemalige Google-CEO Eric Schmidt inne (Anm. d. Ü.). **130** Einheit für Innovationen im Verteidigungsbereich; Abteilung des US-Verteidigungsministeriums, das das Ministerium bei der Einbindung neuer kommerzieller Technologien berät (Anm. d. Ü.). **131** Nationaler Sicherheitsausschuss zu Künstlicher Intelligenz»; ehemaliges unabhängiges Gremium, das den US-Präsidenten und den Kongress zu KI-Fragen beriet. Den Vorsitz hatte der ehemalige Google-CEO Eric Schmidt inne (Anm. d. Ü.). **132** Privates Unternehmen, das dafür sorgt, dass die US-Geheimdienste stets mit aktuellster IT-Technologie ausgestattet sind (Anm. d. Ü.). **133** Vgl. Interview mit Jack Poulson. **134** Ebd. **135** Ebd. **136** Ebd.

intelligenten Grenzüberwachungssoftware von Anduril Industries zu verarbeiten, was ziemlich genau der Positionierung widerspricht, die Google in Bezug auf die eigene Tätigkeit für den US-Grenzschutz formuliert hat. Dies wirft eine interessante Frage auf, wenn man bedenkt, welche entscheidende Rolle Cloud-Computing in finanzieller und technologischer Hinsicht spielt. Denn diese Technik ist ein zentrales Element in den Verkäufen im Verteidigungssektor und eine wichtige Quelle für neue Umsatzsteigerungen großer Tech-Konzerne.»

5.3 DER AUFBAU VON STRUKTUREN FÜR EINE STARKE GEGENBEWEGUNG

Angestellte, die bei ihrer Arbeit unethische Praktiken erleben, finden sich häufig in einem Spannungsfeld zwischen dem, was richtig ist, und dem Streben nach einer langfristigen Karriere wieder – ein Konflikt, den Tech Inquiry durch den Schutz der Identität von Whistleblower*innen zu entschärfen versucht. Doch auch ohne diese Sicherheitsvorkehrung gibt es für Tech-Angestellte Möglichkeiten, die Stimme zu erheben. «Man muss nicht zwangsläufig namentlich erscheinen. Wer Informationen an die Presse weitergeben möchte, kann dies auch anonym tun»,[137] erklärt Poulson.

Doch auch mit den zusätzlichen Ressourcen, die der Nonprofit-Sektor bereitstellt, kann der innere Druck, der aus diesem Spannungsfeld erwächst, Angestellte dazu veranlassen, sich für einen weniger konfrontativen Ansatz zu entscheiden, um die von ihnen wahrgenommenen Missstände anzugehen. Eine Praxis, die vom Management sehr gern als Gelegenheit genutzt wird, untätig zu bleiben, so Poulson. «Das verweist auch auf den Kern einer Debatte um Organizing versus Protest. Ich denke, dass Organizing offensichtlich einer der nachhaltigeren Ansätze ist. In gewisser Weise baut er auch Gegenmacht auf. Ich denke, dass sollte in Whistleblower-Kreisen öfter zur Sprache kommen. Das ist etwas, wofür ich mich sehr stark eingesetzt habe. Einer der Fallstricke, denen ich begegnet bin, besteht darin, dass viele der leitenden Angestellten, die ich kannte, nicht annähernd das taten, was wir traditionell als Organizing bezeichnen würden. Das Narrativ vom ‹Wandel von innen› wird häufig als Ausrede dafür genutzt, warum es okay ist, nichts zu tun. Darüber wird aus meiner Sicht viel zu wenig gesprochen. Eine Frage wäre in diesem Zusammenhang, wie wir es schaffen können, zu verhindern, dass Leute, die das Narrativ vom ‹Wandel von innen› auf böswillige Weise einsetzen, damit durchkommen».[138] Das ist ein Prozess, bei dem gewerkschaftliche Organisierung eine wichtige Rolle spielen könnte.

Poulson zufolge können Gewerkschaften bei der Lösung dieser Problemstellungen jedoch nur ein Teil einer viel umfassenderen Herangehensweise sein. «Die Schwierigkeit besteht darin, dass Gewerkschaften häufig die Interessen der Arbeitenden vertreten, die sich von den Interessen der Öffentlichkeit jedoch drastisch unterscheiden können. Ich denke daher, dass es sich immer wieder zu betonen lohnt, dass wir neben den Gewerkschaften auch Bündnisse brauchen, einschließlich solcher mit unabhängigen Organisationen aus der Zivilgesellschaft.»[139] Daraus folgt auch, dass die Zusammenarbeit zwischen gemeinnützigen Organisationen auf dem Gebiet besser koordiniert werden müsste, so Poulson weiter. «Das bedeutet nicht, niemals etwas zu kritisieren. Aber wenn Nonprofit-Organisationen zusammenkommen und ihre Stärken gemeinsam zum Einsatz bringen, statt miteinander zu konkurrieren, führt das in der Regel zu unglaublichen Resultaten.»[140]

Um das dauerhaft leisten zu können, bedarf es der Unterstützung einer breiteren Öffentlichkeit. «Eines der Probleme im Nonprofit-Bereich ist, dass der Großteil des Geldes von eben jenen Tech-Milliardären stammt, die man kritisieren will. Wenn der Einfluss von Tech-Milliardären ernsthaft beschränkt werden soll, müssen wir wirklich in der Lage sein, uns selbst zu finanzieren. Selbst bei den angesehensten Organisationen gibt es immer wieder hochrangige Persönlichkeiten, die zu Tech-Firmen wechseln, weil diese so viel Macht ausüben und gemeinnützige Organisationen, ehrlich gesagt, in der Regel nicht sehr gut zahlen. Daher gibt es wohl keine Alternative dazu, die Zivilgesellschaft zu einem Ort zu machen, wo Menschen tatsächlich Karriere machen können. Und das kann letzten Endes nur mit Steuergeldern finanziert werden, und vor allem mit Spenden von der Basis.»[141]

137 Ebd. **138** Ebd. **139** Ebd. **140** Ebd. **141** Ebd.

6 SCHLUSSFOLGERUNGEN

Der rasche und massive technologische Fortschritt im Rahmen des militärisch-industriellen Komplexes und die damit verbundenen Auswirkungen auf die künftige Gestaltung von Kriegs- und Polizeitaktiken lassen sich beispielhaft in den USA beobachten. Angesichts einer derart schnellen Weiterentwicklung und zunehmenden Zahl von Gegnern waren das Pentagon und seine Behörden gezwungen, die Forschung und Entwicklung in diesem Bereich an private Unternehmen auszulagern. Denn diese verfügen über ausreichend Personal und Expertise, um der Entwicklung stets einen Schritt voraus zu sein. Die Auswirkungen, die dies auf Bereiche hat, die seit Langem mit chronischen Menschenrechts- und Ethikproblemen behaftet sind, dehnen sich auf eine neue und relativ unerforschte digitale Welt aus. Es gibt gute Gründe, davon auszugehen, dass ähnliche Muster der Verletzung von Menschenrechten und ethischen Richtlinien, die aktuell in den USA auf diesem neuen Feld zu beobachten sind, auf Europa übertragen werden, wenn Projekte wie GAIA-X weitergeführt werden und dieselben Unternehmen beteiligt sind.

Initiativen wie das Projekt Maven belegen, wie stark zivile Unternehmen von einer Kooperation mit Behörden aus dem Verteidigungssektor profitieren können. Die Reaktion von Google-Angestellten auf die Beteiligung an Maven verdeutlicht aber auch die Uneinigkeit zwischen der Unternehmensführung und ihren Angestellten. Die Unternehmensführung, die sich gegenüber ihren Aktionär*innen verpflichtet sieht und den Auftrag hat, ein kontinuierliches Wachstum der Gewinnspannen zu gewährleisten, scheint bereit zu sein, dieses Ziel um jeden Preis zu erreichen, selbst wenn dies bedeutet, vom eigenen ethischen «Don't be evil»-Prinzip abzuweichen oder es gar komplett fallenzulassen. Tatsächlich wurde dieser Prozess von Google 2018 bereits in Gang gesetzt. Im Zuge der Proteste gegen das Projekt Maven wurde der Satz – zusammen mit dem Großteil des ursprünglichen Vorworts – aus dem Verhaltenskodex entfernt und durch die allgemeineren Begriffe «ethisches Geschäftsverhalten» und «Googles Werte» ersetzt. Die Verpflichtung findet sich jedoch weiterhin im Dokument, und zwar in der letzten Zeile: «Und denken Sie daran […]: Tue nichts Böse, und wenn Sie etwas sehen, das Ihrer Meinung nach nicht in Ordnung ist, sprechen Sie es an! »[142]

Profite und ein gesteigerter Einfluss bieten Tech-Unternehmen und Behörden im Verteidigungsbereich enorme Anreize, gemeinsame Sache zu machen. Das sollte bei der Zivilgesellschaft alle Warnglocken läuten lassen. Denn die Vorteile einer solchen Zusammenarbeit überwiegen bei Weitem die negativen Konsequenzen, zumindest für diejenigen, die direkt von der Verwirklichung der Projekte profitieren. Die Drehtür zwischen den beiden Sektoren, durch die Beamte des Verteidigungsministeriums und Tech-CEOs konstant gehen, zeigt, in welchem Ausmaß es zu Absprachen kommt. Diese Allianzen, die das LittleSis-Projekt aufgedeckt hat, und ihre Auswirkungen, die die Kampagne «Big Tech Sells War» kritisiert, erklären die großzügige und drastische Aufstockung der Verteidigungshaushalte.

Was die technologische Entwicklung in Deutschland angeht, so gibt es zwar einige junge Unternehmen, doch handelt es sich dabei im Vergleich zum Silicon Valley um kleine Akteure, die nach wie vor auf von US-basierten Tech-Giganten entwickelte technologische Grundlagen zurückgreifen. Dasselbe gilt auch für europäische Regierungen, die stark von externen Ressourcen abhängig sind. Das zeigte sich exemplarisch an der Beteiligung von AWS, Google und Microsoft, aber auch von chinesischen Unternehmen wie Huawei und Alibaba am GAIA-X-Projekt. Dies ist ein frühes Signal dafür, dass es äußerst schwierig sein wird, die Souveränität Europas und Deutschlands im Technologiebereich zu bewahren, wenn die Entwicklung in dem selbst auferlegten Tempo weitergehen soll.

Die Tatsache, dass menschliche Vorurteile auf einen automatisierten digitalen Bereich übertragen werden, ist ein Aspekt, der zivilgesellschaftlichen Organisationen und Menschenrechtsaktivist*innen in diesem Entwicklungsbereich größten Anlass zur Sorge gibt. Ob es sich nun um Technologien handelt, die die Polizeiarbeit im Inland unterstützen, oder um solche, die auf ausländischen Kriegsschauplätzen zum Einsatz kommen – Bias gegen bestimmte Bevölkerungsgruppen sind in keiner Form eine wünschenswerte Entwicklung. Noch beunruhigender ist, dass diese Problematik bekannt ist. Es ist bekannt, dass solche digitalen Bias existieren, sich mithilfe neuer Technologien weiter ausbreiten und unübersehbare Konsequenzen haben. Dennoch hat dies bislang kaum die gebührende öffentliche Beachtung gefunden. Trotz der intensiven Bemühungen von Einzelpersonen und Organisationen, wie den für die Untersuchung befragten, Aufmerksamkeit und Bewusstsein für das Thema zu schaffen sowie Veränderung herbeizuführen, haben diejenigen, die über Gelder entscheiden und das Sagen haben, das Problem bislang kaum anerkannt, geschweige denn Schritte zu seiner Behebung unternommen. Auf der anderen Seite stellt die DSGVO zweifellos einen gewichtigen Schritt in die richtige Richtung dar, mit dem die europäischen Staaten zumindest eine Reihe von Schutzmechanismen integrieren konnten. Dies sollte jedoch nur als Ausgangspunkt verstanden werden, auf dem nun rasch aufgebaut werden muss.

142 Alphabet Inc.: Google Code of Conduct, 2022, unter: https://abc.xyz/investor/other/google-code-of-conduct.

Zentrale Erkenntnisse:

- Einige der profiliertesten Player im privaten Tech-Bereich sind Google LLC, Amazon Web Services, Oracle und Microsoft. Facebook und Apple stellen vergleichsweise kleine Akteure in diesem Bereich dar. Projekte von anderen großen Konzernen wie IBM und HP Inc. wurden wegen ihres relativen engen Fokus auf verbraucherorientierte Dienste sowie aufgrund des begrenzten Umfangs der vorliegenden Untersuchung nicht berücksichtigt.
- Der Großteil der staatlichen Aufträge macht nur einen geringen Teil der Einnahmen dieser Unternehmen aus. Die Vergaben stellen vielmehr eine kontinuierliche Einnahmequelle dar sowie die Möglichkeit, Ergebnisse militärischer Innovationsprozesse auf den privaten Markt zu überführen, während die Haupteinnahmequelle der Unternehmen weiterhin der Verkauf von zivilen Konsumgütern bleibt.
- Die Auftragsvermittlung erfolgt häufig über ein undurchsichtiges Netzwerk privater Akteure. Dadurch werden die Verbindungen zwischen großen Tech-Innovatoren und dem Pentagon verwischt, was es den großen Unternehmen ermöglicht, sich von möglichen Auswirkungen zu distanzieren und Haftbarkeit auszuschließen.
- Technologien, die im Rahmen des militärisch-privaten Innovationstransfers entwickelt werden, lassen sich in der Regel nicht direkt als (automatisierte) Waffen oder Technologien zur Tötung von Menschen beschreiben. Stattdessen tragen Technologien, die im Zuge solcher Verträge entwickelt werden, indirekt zu neuen Formen der Kriegsführung bei, etwa durch die automatisierte Datenverarbeitung für gezielte Aufklärung oder durch Cloud-Computing-Ressourcen. Es wurden zwar keine Belege dafür gefunden, dass diese Art von Technologie direkt mit der automatisierten Tötung verbunden ist, aber es konnte festgestellt werden, dass die untersuchten Verträge dezidiert folgende Ziele verfolgten:
  - Die Technologien sollen sowohl für den Einsatz bei militärischen Operationen als auch in der Polizeiarbeit im Inland angewandt werden können.
  - Sie sollen es allgemein ermöglichen, eine größere Rolle bei der automatischen Entscheidungsfindung sowie für automatisierte Waffensysteme zu spielen.
- Der deutsche/europäische Innovationsmarkt entwickelt sich in eine Richtung, die der Entwicklung in den USA sehr ähnelt. Dies bedeutet in erster Linie, dass es zu engeren Verbindungen zwischen dem deutschen/europäischen Verteidigungssektor und dem privaten Technologiemarkt kommt und es verstärkte Bemühungen gibt, eine Zusammenarbeit anzustreben, wie hier am Beispiel von GAIA-X veranschaulicht.
- Die Datenschutz-Grundverordnung (DSGVO) in Europa gilt aktuell als das weltweit umfassendste Regelwerk zum Schutz personenbezogener Daten. Sie liefert ein gesetzliches Fundament, in das grundlegende Menschenrechte eingeschrieben sind und das zukünftigen Bestimmungen als Vorbild dienen könnte.
- Tech-Angestellte sehen sich verstärktem Druck ausgesetzt, ihre ethischen Bedenken gegenüber der Beteiligung an Vergaben aus dem militärischen Kontext nicht zu äußern, da dies ihre Karriere gefährden könnte. Ihre Überzeugung, sich zu äußern, wird häufig durch «Wandel von innen»-Erzählungen und Beschwichtigungen von Kolleg*innen und Vorgesetzten gebremst. Diesem Druck stehen in der Regel keine Anreize im Non-Profit-Umfeld entgegen, Informationen anonym weiterzugeben oder eine Karriere innerhalb des gemeinnützigen Bereichs einzuschlagen.

Möglichkeiten, um dieser Entwicklung etwas entgegenzusetzen:

- Neben der Arbeit von Gewerkschaften braucht es ein breiteres Unterstützungsnetzwerk, das von zivilgesellschaftlichen Akteur*innen getragen wird. Derzeit wird die meiste Aufklärungsarbeit im Nonprofit-Bereich durch die Analyse von abgeschlossenen Vergaben, von Anfragen nach dem Freedom of Information Act und von öffentlich verfügbaren Daten geleistet. Dies ist eine sehr ineffiziente Arbeitsweise, die durch verstärkte Zuarbeit von Whistleblower*innen deutlich erleichtert werden könnte.
- Das Thema Diskriminierung muss in allen F&E-Prozessen stärker Berücksichtigung finden.
  - Die neuen digitalen Anwendungen reproduzieren die Diskriminierung von Personengruppen, die historisch bereits marginalisiert wurden, etwa entlang von Kategorien wie *race,* Gender oder Religion.
  - Die Forschung im Nonprofit-Bereich muss ihren Fokus stärker auf dieses Thema legen und für eine größere Öffentlichkeit sorgen, indem intersektionale Bündnisse zwischen unterschiedlichen Akteur*innen geschmiedet werden.

Um das zu ermöglichen und wirkungsvolle Bündnisse im Sinne eines nachhaltigen und organisierten Korrektivs der Zivilgesellschaft zum kriegerischen Geschäft des Tech-Sektors aufzubauen, sind allerdings zuallererst Diskurs- und Austauschräume erforderlich. In diesen Räumen wird es darum gehen, Krieg sowohl aus interdisziplinärer als auch aus intersektionaler Perspektive zu erfassen und die Perspektiven jener Menschen aufzugreifen, die am stärksten von Kriegstechnologien betroffen sind: von Communitys in aktiven Kriegsgebieten über Geflüchtete, die an den europäischen Außengrenzen sterben, bis hin zu den im Inland am stärksten marginalisierten und polizeilich kontrollierten Personengruppen.

Erst eine solche Debatte kann eine Bewegung hervorrufen, die Tech-Unternehmen für ihre Handlungen auf Grundlage der Menschenrechte und nicht aufgrund selbst auferlegter ethischer Verpflichtungen zur

Rechenschaft ziehen kann. Dabei geht es um eine Bewegung, die sich nicht darauf beschränkt, Google für die Umgehung der eigenen ethischen Richtlinien ins Visier zu nehmen, sondern auch die Frage aufwirft, warum nicht mehr Unternehmen eben solche Richtlinien formulieren.

Technologie ist eine menschliche Erfindung, deren Zweck und Verwendung von uns kontrolliert wird. Vor diesem Hintergrund gibt es keine Grundlage für die Behauptung, dass sie neutral sei. Technologie war schon immer politisch und wird es auch in Zukunft sein. In einer Welt, in der alle Menschen, die verbraucherorientierte Dienste von Firmen aus dem Silicon Valley nutzen, zu ihrem Datenbestand und ihren Einnahmen beitragen, gibt es keine Ausrede dafür, untätig zu bleiben – weder in den USA noch in Europa oder weltweit.

GLOSSAR

A

Advanced Research Projects Agency Network (ARPANET): Ein vom US-Verteidigungsministerium in den 1960er-Jahren finanziertes Forschungsprojekt, bei dem das erste Computernetzwerk zwischen Endgeräten an verschiedenen Universitäten geschaffen wurde.

Algorithmische Kriegsführung: Der kombinierte Einsatz von Systemen und Technik, deren Anwendung sich auf Algorithmen stützt. Dazu gehören autonome Waffen, Künstliche Intelligenz (KI) und die Analyse von Big Data.[143]

Autonome Waffensysteme: Das US-Verteidigungsministerium definiert ein autonomes Waffensystem als «ein Waffensystem, das nach seiner Aktivierung Ziele ohne weiteres Eingreifen eines menschlichen Bedieners ansteuern und treffen kann. Dazu gehören auch von Menschen überwachte autonome Waffensysteme, die so beschaffen sind, dass der Einsatzvorgang des Waffensystems manuell kontrolliert werden kann, die jedoch nach ihrer Aktivierung für die Ansteuerung und den Angriff des Ziels ohne weitere menschliche Bedienung auskommen.»[144] Diese Definition wird indessen in der wissenschaftlichen Debatte häufig kritisiert, da unklar ist, was die «Auswahl» von Zielen beinhaltet und wie die Unterscheidung zwischen «autonomen» und «automatisierten» Waffen getroffen wird.[145]

B

Big Tech: Sammelbegriff für die größten, dominantesten und renommiertesten Technologieunternehmen der Welt. Die meisten dieser Unternehmen haben ihren Sitz in den USA und in der Regel bezieht sich der Begriff insbesondere auf die fünf wichtigsten Unternehmen: Apple, Microsoft, Amazon, Google und Facebook.

E

Entscheidungszentrierte Kriegsführung: Diese militärische Strategie beruht auf der Schwächung gegnerischer Streitkräfte durch den militärischen Einsatz künstlicher Intelligenz und autonomer (Waffen-)Systeme bei der Identifizierung und Priorisierung von Zielen. Ein aktuelles Beispiel für entscheidungszentrierte militärische Strategien ist das Konzept der Mosaic Warfare der US Defense Advanced Research Projects Agency (DARPA). Es basiert auf der Prämisse, dass die Integration von autonomer und bemannter Militärtechnik unter KI-gestützter menschlicher Entscheidungsfindung in der Lage ist, einen Krieg effektiver zu führen und dabei potenziell weniger Verluste bei den Truppen zu riskieren.[146]

G

Gesichtserkennungstechnologie: Die ursprünglich für das Militär entwickelte Gesichtserkennungstechnologie zielt darauf ab, Personen anhand von Video- oder Fotomaterial auf Basis spezifischer Gesichtsmerkmale zu identifizieren.

K

«Krieg gegen den Terror»: Eine laufende internationale Militärkampagne unter der Leitung der US-Regierung infolge der Terroranschläge vom 11. September 2001.

Künstliche Intelligenz: Ein Teilbereich der Informatik, der sich mit der Entwicklung von Maschinen beschäftigt, die in der Lage sind, Aufgaben auszuführen, die üblicherweise menschliche Intelligenz erfordern.

M

Maschinelles Lernen: Ein Prozess, bei dem eine digitale Maschine mithilfe von Algorithmen und Erfahrungswerten lernt und ihre Fähigkeiten verbessert.

Materialschlacht: Auf dem Einsatz von militärischem Personal und Ausrüstung beruhende militärische Strategie zur schrittweisen Schwächung gegnerischer Streitkräfte. Materialschlachten setzen in der Regel die Bereitschaft voraus, erhebliche Verluste an Material und Truppen in Kauf zu nehmen. Ein Beispiel für diese Kriegsführung sind die Operationen der alliierten Streitkräfte gegen Deutschland während des Zweiten Weltkriegs.

Militärisch-industrieller-Komplex (MIK): Ein Begriff, der ursprünglich von US-Präsident Dwight D. Eisenhower im Jahr 1961 geprägt wurde, um auf mögliche Absprachen hinzuweisen, die sich aus gemeinsamen Interessen in diesem Umfeld zwischen Akteur*innen aus Politik, Verteidigungsindustrie und Militär mit dem Ziel ergeben, die Militärausgaben weiter zu erhöhen.

T

Third Offset Strategy (TOS): Ein Begriff, der das Bestreben der Entwicklung und des Erwerbs von Hochtechnologien auf dem Feld der Rüstung meint. Als Strategie einer technologisch führenden Macht zielt sie darauf die eigene technologische Überlegenheit gegenüber aufstrebenden Staaten beizubehalten, damit ihr qualitativer Vorsprung auf dem Feld der Rüstung gewahrt bleibt.

143 Layton, Peter: Algorithmic Warfare. Applying Artificial Intelligence to Warfighting, Commonwealth of Australia, Canberra 2018, S. iii, unter: https://airpower.airforce.gov.au/publications/algorithmic-warfare-applying-artificial-intelligence-warfighting. **144** US Department of Defense: Directive re Autonomy in Weapon Systems, 21.11.2012, S. 13, unter: www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/300009p.pdf. **145** Conn, Ariel: The Problem of Defining Autonomous Weapons, The Future of Life Institute, 30.11.2016, unter: https://futureoflife.org/2016/11/30/problem-defining-autonomous-weapons. **146** Clark, Bryan/Patt, Dan/Walton, Timothy: Implementing Decision-Centric Warfare: Elevating Command and Control to Gain an Optionality Advantage, Hudson Institute, 3.3.2021, unter: www.hudson.org/research/16729-implementing-decision-centric-warfare-elevating-command-and-control-to-gain-an-optionality-advantage.

WWW.ROSALUX.DE