Künstliche Intelligenz als Cloud Service

Folgen für Gesellschaft, Geheimdienst und Militär

von Arkadi Schelling

Im Mai 2018 gab es einen kleinen Skandal um Überwachungstechnologie. Die amerikanische Bürgerrechtsvereinigung ACLU kritisierte den Cloud Anbieter Amazon Web Services (AWS) für den Betrieb des Internetdienstes *Rekognition*.[1] Mit dem seit Ende 2016 bestehende Softwaredienst des umtriebigen Onlinehandelsriesen können unter anderem Objekte, Gesichter, Basisemotionen und Laufwege in Fotos und Videos erkannt und analysiert werden. Diesen Dienst bewirbt AWS erfolgreich bei Strafverfolgungsbehörden. Interne Dokumente zeigen, dass unter anderem Washingtoner Kreispolizist*innen mit einer App die Bilder von Verdächtigen gegen eine Datenbank von ehemaligen Gefängnisinsassen abgleichen können. Die Videokameras des Gebiets sind ebenfalls mit Amazons System verbunden. Als nächsten Schritt rät der Cloud Anbieter zu vernetzten Bodycams, also an Polizist*innen befestigte Überwachungskameras. Die Bürger*innen vor Ort wurden vor der Einführung 2017 freilich weder gefragt noch informiert. Sogar behördeninterne Stimmen sagten korrekt vorher, dass die ACLU diesen Schritt als eine schlüpfrige Affäre von der Regierung mit Big Data sehen würde.[2] Die Kritik der Bürgerrechtler*innen verlief entlang mehrerer Linien. Die grundlegende Kritik an automatisierter und anlassloser Massenüberwachung ist klar. Menschen verhalten sich unfreier, wenn sie beobachtet werden. Seit Trump müssten selbst die gutgläubigsten US-Amerikaner*innen ihre Zweifel haben, dass solche Systeme niemals für persönliche Zwecke oder staatliche Repression missbraucht werden. Außerdem betreffen polizeiliche Maßnahmen und Überwachung überproportional viele Menschen, die Minderheiten angehören. Um diesen Punkt zu unterstreichen, veröffentlichte die ACLU einen zweiten Blogpost, in dem sie die Bilder von Kongressabgeordneten gegen eine selbst erstellte Häftlingsfotodatenbank abgleichte. Im Ergebnis zeigte sich, dass People of Color ein doppelt so hohes Risiko haben fälschlicherweise verdächtigt zu werden. Die Entwickler*innen von *Rekognition* verweisen ihrerseits verschnupft auf die inkorrekte Kalibrierung ihrer Bilderkennungssoftware und vergleichen das Experiment mit einer verbrannten Pizza aufgrund zu heißer Ofentemperatur.[3]

Künstliche Intelligenz in der Cloud

Ein Kern von *Rekognition* ist sogenannte Künstliche Intelligenz. Das aktuell wichtigste Werkzeug ist Maschinelles Lernen, welches eine Sammlung statistischer Verfahren und Softwaretechniken ist. Dabei wird ein Modell mit bekannten Daten trainiert, um für unbekannte Daten Vorhersagen zu treffen. Alle Daten über Menschen enthalten jedoch gesellschaftlich bedingte Verzerrungen, beispielsweise die überproportional häufigen People of Color auf Häftlingsfotos. Essentiell ist zudem die Optimierung des Modells anhand einer einzigen Kennziffer, die die Entwickler*innen festlegen müssen. Es macht einen Unterschied, ob die Gesichtserkennung im Training eine gesellschaftsagnostische Gesamtgenauigkeit optimiert, oder Genauigkeiten für Minderheiten mit verrechnet werden. So versteckt sich hinter vermeintlich neutraler Mathematik eine Weltsicht und politische Vision. Die Verwendung von Maschinellem Lernen auf der Grundlage personenbezogener Daten für sozial relevante Entscheidungen ist somit kritisch zu hinterfragen.

Viele KI-basierten automatisierten Entscheidungsfindungen führen außerdem zu Problemen aufgrund fehlender Interpretierbarkeit, Geheimhaltung und dem Entzug gesellschaftlicher Kontrolle. Frank Pasquale beschreibt in seinem Buch Black-Box Society solche Blackbox-Algorithmen, die nicht öffentlich sind, obwohl sie die Gesellschaft stark beeinflussen. Ein Beispiel ist die Beförderung der Banken- und Wirtschaftskrise von 2008 durch automatisierten Aktienhandel und Risikoabschätzungen von komplexen Finanzprodukten. Aktuell breit diskutiert werden auch die Google-Suche und Facebook-Timeline, die die Weltsicht und politischen Überzeugungen vieler Menschen prägen. Weitere Beispiele gehen von der Ablehnung eines neuen Handyvertrags aufgrund einer schlechten Schufa-Auskunft bis zur Einflussnahme auf einen Richterspruch durch vorhergesagte Rückfälligkeitswahrscheinlichkeit eine*r Straftäter*in. Manche dieser undurchsichtigen Algorithmen sollen lediglich als nicht-bindende Entscheidungshilfe für einen Menschen verwendet werden. Eine Gefahr besteht dabei in einer Fehlinterpretation der Vorhersage, dessen Begründung aufgrund der Blackbox verschleiert ist. Ebenso ist der psychologische Effekt des Automation Bias bekannt, der besagt, dass Menschen dazu neigen, einer automatisierten Entscheidung übermäßig viel zu vertrauen. Aufgrund dieser Verschleierung und der Vorurteile sowohl in der Datengrundlage als auch der menschlichen Entscheidungsträger*innen haben Blackbox-Algorithmen ein großes Potential für unvorhergesehene Eskalation gesellschaftlicher Ungerechtigkeiten.

Der rasante Aufstieg des Maschinellen Lernens in den letzten zwanzig Jahren kann durch die größeren Rechenleistung und die steigende Vernetzung mit höheren Datenmengen erklärt werden. Ein weiterer Faktor ist der wirtschaftliche Anreiz werbefinanzierter Produkte. Gekoppelt mit Verhaltenspsychologie ist Maschinelles Lernen ein Baustein, um in großem Maßstab die Verweildauer und Klickfreudigkeit von Nutzer*innen zu vergrößern und damit die Werbeeinnahmen zu optimieren. Die psychologische Manipulierbarkeit der User verleitete bereits manche zum Ausruf eines vermeintlichen “Endes der Theorie”[4], vor allem zeigt sich hier aber das Menschenbild der Konzerne, welches durch den Euphemismus “User Experience” verschleiert wird. Die größere Nachfrage nach komplexer Mathematik und Software, die für diesen finanziellen Erfolg nötig ist, wird auch durch immer einfacher nutzbare Implementierungen ermöglicht. In diesem Licht ist sowohl das Beispiel “AWS Rekognition” als auch der generellere Dienst “Machine Learning as a Service” zu interpretieren, wie er inzwischen von allen großen Cloud Anbietern angeboten wird. Die Technik wird damit deutlich mehr Unternehmen zugänglich gemacht, die vorher aufgrund fehlender Größe oder Expertise nicht mit Machine Learning arbeiteten. So sind selbst die privaten Unternehmen, die an erwähnten Blackbox-Algorithmen Geld verdienen, selbst nur Nutzerinnen von Blackboxen. Verstärkt wird dieser Trend zum Unverständnis durch die Verwendung von Techniken wie Transfer Learning, wo bestehende Modelle

angepasst werden, um eine neue Aufgabe zu lösen. So können beispielsweise höhere Erkennungsraten von Hauterkrankungen erreicht werden, wenn als Grundlage ein allgemeineres Modell zur Objekterkennung auf Fotos verwendet wird, wie sie beispielsweise von Google zur freien Verfügung gestellt wird. Ob es sich um dasselbe Modell handelt, welches für seinen rassistischem Bias bekannt ist, bleibt dabei unerwähnt.[5]

Die Kritik an den einfach verfügbaren neuen Werkzeugen für Massenüberwachung und für psychologische Beeinflussung geht nicht an den Unternehmen vorbei. Während von Amazon und Microsoft vor allem Lippenbekenntnisse kommen,[6] verweist Google im Guide zur Transfer-Learning-Plattfrom *TensorflowHub* selbst auf die Problematik unbekannter Trainingsdaten und ihre firmeneigene Forschung und Empfehlungen zu »fairem Maschinellem Lernen«. Während solche selbst gegebenen Richtlinien ein erster Schritt sind, stellt sich doch die Frage, wer hier definiert, was »fair« ist.[7] Facebook unterstützt mit 6,5 Millionen Euro ein Institut der TU München zur Untersuchung ethischer Fragen bei der Anwendung von KI. Zwar werden keine inhaltlichen Vorgaben gestellt, dennoch wird der Institutsleiter ein Interesse an einer Fortführung des auf fünf Jahre begrenzten Programms haben.

In der einleitenden Geschichte zeigen sich beispielhaft alle diese grundlegenden Probleme bei der Anwendung sogenannter Künstlicher Intelligenz zur Lösung gesellschaftlicher Aufgaben. Im Grundsatz hat sich die technokratische Utopie, gesellschaftliche Aufgaben allein mit neuer Technik zu lösen, im letzten Jahrhundert nicht erfüllt. Im Gegenteil kann die Konzentration von Technik und Wissen die kapitalistische Ausbeutung oder staatliche Kontrolle verstärken. In dem geschilderten Fall werden sozial ausgegrenzten Menschen durch eine stärkere Überwachung keinesfalls weniger, sondern nur noch weiter ausgegrenzt. Sei es durch verstärkte polizeiliche Kontrolle oder ein Ausweichen auf weniger sichtbare Räume. Dass die bloggenden Entwickler*innen von AWS mit profanen Pizza-Vergleichen die sozialen Probleme ihrer Arbeit von sich schieben, erstaunt nicht angesichts der jüngst immer lauter werdenden Vorwürfe von Sexismus und Rassismus im männlich und weiß dominierten Silicon Valley.[8]

Polizei, Geheimdienste und Militär

Ein weiterer Aspekt, der sich in der ACLU Geschichte zeigt, ist die mangelnde Scheu vor einer Zusammenarbeit mit Strafverfolgungsbehörden. Diese automatisierte Überwachung ist ein Teil von *Predictive Policing*.[9] Dieser Begriff beschreibt Maschinelles Lernen zur Vorhersage von Straftaten, beispielsweise Einbrüchen, aufgrund vieler polizeilicher und anderer Daten. Während Polizist*innen früher Stecknadeln in Stadtpläne steckten, so sollen nun kommerzielle KI-Lösungen helfen die Muster in den Taten krimineller Banden zu finden. Diese Daten sind stark gesellschaftlich geprägt. Teilweise empfehlen diese Blackbox-Algorithmen zukünftige Polizeipräsenz, sodass der Automation Bias bestehende soziale Missstände verstärken kann. Die vom Geschäftsgeheimnis geschützten Algorithmen bleiben sowohl für die Polizist*innen als auch die Gesellschaft undurchsichtig, werden jedoch hochskaliert auf große Teile der Bevölkerung angewendet. Diese neoliberale Übernahme von staatlichen Aufgaben durch Unternehmen ist keine Besonderheit, bietet in diesem Fall aber eine besonders hohe Gefahr für eine Einschränkung freiheitlicher Grundrechte sozial benachteiligter Menschen.

Amazons Selbstbeschreibung auf ihrem Facebook-Profil lautet: »Earth‘s most customer-centric company«. Diesen vermeintlich untertänigen Anspruch möchte Amazon auch für eine ganz besondere Klasse von Kunden erfüllen: Die US-Geheimdienste. Al Tarasiuk, ein Leiter der Dachorganisation der US-Geheimdienste (IC), nannte Cloud Computing »eine der Kernkomponenten der Strategie des Geheimdienstverbands, um kritische Informationen in einer Zeit von scheinbar unendlichen Daten zu entdecken, auf sie zuzugreifen und sie zu teilen.« Bereits 2013 wurde von der CIA der erstaunliche Schritt gegangen, ihre Server-Infrastruktur nicht mehr selbst zu bauen, sondern an das Unternehmen Amazon abzugeben, das sich mit dem Versprechen auf geringere Preise und schnellere Innovation unter anderem gegen IBM durchsetzte. Ein Jahr später erhielten die restlichen sechzehn Geheimdienste Zugriff auf die AWS-eigene Hardware hinter Firewalls der Geheimdienste. Die Dienste können damit ihre diversen Datenquellen wie überwachte Kommunikation, Kameras und Satelliten in einem einzigen Framework zusammenbringen, speichern, verknüpfen, verarbeiten und seit ein paar Jahren auch mit KI-Methoden Vorhersagen treffen.[10]

Doch nicht nur Geheimdienste brauchen Server, Festplatten und Datenanalysen. Beim Militär erscheint das Outsourcen von Aufgaben an Unternehmen nach dem Erstarken von Söldnerarmeen weniger überraschend. Das Ideal einer günstigeren Alternative wird dabei weniger erfüllt als die geringere gesellschaftliche Kontrolle und Verantwortung.

Laut eigener Aussage suchen die Armeen in der Zusammenarbeit mit den Cloud Providern nach größerer »Situational Awareness« und versuchen durch die Zusammenführung vieler Informationen den »Nebel des Krieges« zu lichten. Neu ist an einer solchen Entscheidungsfindung nicht nur der Maßstab, sondern auch die Automatisierung. Eine Werbebroschüre zeigt Tablets mit computerspielhaften topografischen Karten. Ähnlich dem Predictive Policing sollen hier die immer verbreiteteren Sensoren von militärischem Gerät verwendet werden, um eine militärische Gesamtsituation übersichtlich zu visualisieren. Die logistische Optimierung von Nachschub und automatische Empfehlungen von Truppenbewegungen und Angriffen sind ein geplanter Schritt auf dem angedeuteten Weg zu automatisierten Generäl*innen. Offenbar birgt dieser Ansatz ebenso große moralische Probleme in sich wie die aktuell verhandelten autonomen tödlichen Waffen, deren Tötungsentscheidungen typischerweise per Knopfdruck, »in-the-loop«, bestätigt oder zumindest, »on-the-loop«, von einem Menschen überwacht würden. Die einzelnen Tötungsentscheidungen bleiben potentiell bei den menschlichen Soldat*innen, also ein Mensch-Maschine-Verhältnis, was in Analogie als »under-the-loop« beschrieben werden kann und damit das Prinzip autonomer Waffen auf den Kopf stellt. Gepaart mit Drohnen und anderen autonomen Waffen auf dem Kriegsfeld entsteht selbst durch eine nur teilweise Automatisierung der Kriegstaktik ein kaum zu durchsteigendes Geflecht, in dem es schnell unmöglich wird nachzuvollziehen, wer noch Verantwortung für welche Entscheidungen trägt. Der bereits erreichte Erfolg von Computern in Logistik macht ein kollaboratives Szenario von taktischer KI und menschlichen Generäl*innen deutlich greifbarer als die Horrorvorstellungen von Terminatoren und Killerrobotern oder mordenden Drohnenschwärmen, die noch lange an einer Unterscheidung von Verbündeten, Verfeindeten und Zivilist*innen scheitern werden.[11]

Entsprechend fing im März 2018 das dem US-Verteidigungsministerium unterstellte Transportation Command an, seine Daten in die Amazon GovCloud zu migrieren. Ein Service,

der zusammen mit der Amazon Secret Region aus der Kooperation mit den Geheimdiensten entstand. Kurz nach dieser Logistikabteilung des Militärs folgte das National Ground Intelligence Center nach, welches Informationen über feindliche Bodenkräfte sammelt.[12]

Die größte Veränderung in der IT-Struktur des US-Verteidigungsministeriums steht jedoch im April 2019 durch das mit bis zu zehn Milliarden Dollar dotierte Joint Enterprise Defense Infrastructure Programm (JEDI) bevor. Der Digitalbeauftragte des Ministeriums, David Lynch, beschreibt den Weg zur obigen Vision wie folgt: »Wir möchten das Verteidigungsministerium um die kommerzielle Cloud herumbiegen«. Zwar warfen zu Bewerbungsschluss einige Cloud Anbieter ihren Hut in den Ring, doch selbst IBM werden nur geringe Chancen gegen die erfahrene Cloud-Dienstleisterschaft von Amazon eingeräumt. Etwas Konkurrenz bietet die Firma Microsoft, die das Militär mit Betriebssystemen und vernetzten Office-Anwendungen unterstützt und dafür ebenfalls Freigaben für die Verwahrung hochklassifierter Geheimdokumente in ihrer Cloud erhalten hat. Die Motivation der US-Armee, sich so abhängig von einem einzigen Unternehmen zu machen, bleibt dabei unklar.[13]

Bei Google hingegen machte im April 2018 der öffentliche Protest von 3.100 Mitarbeiter*innen gegen das Militärprojekt Maven von sich Reden, in welchem die Objekterkennung der Firma für Drohnen der Armee benutzt wird. In der Folge entschied sich die Konzernführung gegen eine Verlängerung der Zusammenarbeit und zog im Oktober ebenfalls seine, vermutlich chancenlose, Bewerbung um das JEDI Programm zurück. Ebenfalls Zweifel daran, dass Google sein von »Don‘t be evil« in »Do the right thing« umgeändertes Firmenmotto ernst meint, weckt ein weiterer Protest aus dem letzten Sommer. Sehr ähnlich zu Maven wandten sich hier Mitarbeitende gegen den Wiedereintritt der Suchmaschine in den chinesischen Markt. Die von unternehmensinternen Kritikern veröffentlichten Details zur vorgegebenen Zensur geht dabei deutlich über Schwarze Listen mit Wörtern wie Menschenrechte und Falun Gong hinaus und enthalten beispielsweise auch eine direkte Anbindung an offizielle chinesische Luftqualitätswerte. Die ethischen Prinzipien des Unternehmens bleiben somit fraglich.[14]

Das Autor*innenkollektiv çapulcu mutmaßt, dass Google sich nach dem Ausstieg aus dem Project Maven mit einem Outsourcing-Manöver wieder ins Militärgeschäft bringt.[15]

Tatsächlich begann im April 2018 eine Kooperation zwischen Google und Atos. Dieser französische IT-Konzern bietet vor allem Produkte rund um Cybersecurity, Informationssysteme und Rechenzentren an. Die Abteilung dieses französischen Konzerns spezialisiert sich auf Grenzkontrollen, Überwachung und Informationssysteme für Armeen. Zudem ist Atos einer der größten IT-Dienstleister der Bundeswehr und betreut deren zentrale Rechenzentren. Von der Kooperation mit Google erhofft sich Atos offenbar genau die KI-Fähigkeiten, die sich das Pentagon von JEDI erträumt. Ebenfalls von Atos stammt die oben erwähnte Broschüre zur Automatisierung der Kriegstaktik. Implementiert werden viele der Ideen bereits im Bull Battle Management System, welches von der französischen Armee genutzt wird. Da ergänzt es sich ausgezeichnet, dass Googles Tochter DeepMind, deren neuronale Netze bereits Schach und Go gemeistert haben, inzwischen auch im Echtzeitkriegsspiel Starcraft brilliert.[16]

Kriegssimulatoren werden schon seit vielen Jahren für die Soldat*innenausbildung immer weiter verfeinert. Die von menschlichen Soldat*innen in ihren Simulatorstunden generierten Daten sind bereits eine wertvolle Ressource, um Kriegsfähigkeiten wie Schießen und Fahren für KI lernbar zu machen. Nun kann dieselbe Technik, welche Starcraft erlernte, in diesen Simulatoren Kriegstaktik erlernen. Die EFF warnt Militärs vor der leichtfertigen Annahme, dass der Sprung in die echte Welt zu unvorhergesehenem und unerwünschtem Verhalten führen wird.[17] Technisch gesehen stehen die Entwickler*innen der Software zudem vor der Frage, welche einzelne Kennziffer optimiert werden soll. Für die mathematische Formel muss unter anderem entschieden werden, in welcher Gewichtung tote Zivilist*innen zu eigenen und feindlichen Soldat*innen stehen? Welches Gewicht haben dabei militärisches Gerät und Treibstoff? Die eigentlich dahinter stehende Frage heißt “Was ist ein militärischer Sieg?” und wurde bisher allein von Menschen beantwortet und verantwortet.

Anmerkungen

1 Sog. *Cloud Services* bieten Dienste eines Rechenzentrums über das Internet an, von Festplattenspeicher über virtuelle Server bis hin zu höheren Softwarefunktionen. Das Marktvolumen wurde 2017 von Synergy auf etwa 150 Mrd. Dollar geschätzt.

2 Matt Cagle und Nicole Ozer: Amazon Teams Up With Government to Deploy Dangerous New Facial Recognition Technology, aclu.org, 22.05.2018

3 Jacob Snow: Amazon’s Face Recognition Falsely Matched 28 Members of Congress With Mugshots, aclu.org, 26.07.2018, Thoughts On Machine Learning Accuracy, aws.amazon.com

4 Chris Anderson: The End of Theory. The Data Deluge Makes the Scientific Method Obsolete, wired.com , 23.06.2008

5 Tom Simonite: When It Comes to Gorillas, Google Photos Remains Blind, wired.com, 01.11.2018

6 Brad Smith: Facial recognition: It’s time for action, blogs.microsoft.com, 06.12.2018

7 Fairness, ml-fairness.com

8 Tamsin McMahon: What’s behind the tech industry’s toxic masculinity problem? Inside the Valley of the Bros, theglobeandmail.com, 21.11.2017

9 Einen Überblick über Predictive Policing in Deutschland gibt heise online:Ulrike Heitmüller: Predictive Policing: Die deutsche Polizei zwischen Cyber-CSI und Minority Report, heise.de, 17.04.2017

10 Frank Konkel: The Details About the CIA’s Deal With Amazon, theatlantic.com, 17.07.2014

11 Connected Defense: Vision for 2020, atos.net

12 Frank Konkel: Another Defense Agency to Tap CIA’s Commercial Cloud, nextgov.com, 31.05.2018

13 Ron Miller: Why the Pentagon’s $10 billion JEDI deal has cloud companies going nuts, techcrunch.com, September 2018

14 Ryan Gallagher, Google Dragonfly, theintercept.com

15 Çapulcu: Delete! – Der technologisch-militärische Angriff, S. 13, capulcu.blackblogs.org

16 Christoph Marischka: Cloud-Anbieter für Bundeswehr, CIA und Pentagon, IMI-Standpunkt 2018/036 - in: AUSDRUCK (Dezember 2018), imi-online.de, 05.11.2018; Bull Battle Management System. Share combat information everywhere on the battlefield, atos.net, Juli 2016; Atos and Google Cloud form a global partnership to deliver secure hybrid Cloud, machine learning and collaboration solutions to the enterprise, atos.net, 24.04.2018; AlphaStar: Mastering the Real-Time Strategy Game StarCraft II, deepmind.com

17 Peter Eckersley: The Cautious Path to Strategic Advantage: How Militaries Should Plan for AI, Electronic Frontier Foundation, eff.org, August 2018