# Die Kampfdrohne als Peripheriegerät des Internets

*von Christoph Marischka*

„Wie eine Computermaus ist die Kampfdrohne ein Peripheriegerät des Internets“. Mit dieser frei übersetzten Aussage der ehemaligen US-Soldatin und Whistleblowerin Lisa Ling lässt sich das Thema einer Konferenz auf den Punkt bringen, die Ende November im Berliner Kunstquartier Bethanien stattfand. Thema war die „Kill Cloud“, im Prinzip die Fusion zwischen ziviler digitaler Infrastruktur und Kriegführung, zwischen Tech-Unternehmen und Rüstung. Eingeladen hatte das Disruption Network Lab, selbst eine Mischung aus Kunstprojekt, NGO und Netzwerk.

Lisa Ling erzählte dort in einem leicht nachvollziehbaren Ton ihre „autoethnographische Geschichte“ der Digitalisierung der Kriegführung. Dabei verbinden sich persönliche mit ihren professionellen Erfahrungen und mit der Geschichte des Internets. Sie zeigte Fotos von Kommandozentralen der Air Force zu Beginn ihrer Laufbahn und zehn Jahre später und von typischen Kommunikationsmitteln zur jeweiligen Zeit: Einige überdimensionierte Röhrenbildschirme und Telefone mit Wahlscheiben auf der einen Seite, den durchdigitalisierten Situation Room mit Großbild-Flachbildschirmen und verschiedenen mobilen Endgeräten auf der anderen Seite. Der Unterschied zwischen beiden: Plötzlich war alles auch ein Sensor und niemand wusste mehr, welche Daten damit in jene Cloud eingespeist werden, aus der – mittlerweile – Entscheidungen über Leben und Tod getroffen werden.

In einem eigens für die Konferenz eingereichten Paper zitiert Ling auch Meredith Whittaker, KI-Forscherin und seit September 2022 Präsidentin des verschlüsselten Messengers Signal. Whittaker erhielt den Helmut-Schmidt-Zukunftspreis 2024 und weil Die Zeit zu jenen Institutionen gehört, die den Preis vergeben, hat sie auch die bemerkenswerte Preisrede Whittakers unter dem Titel „Das KI-Märchen“ dokumentiert. Im Kern beschreibt sie darin, wie vermeintlich harmlose Algorithmen zur gezielten Werbung nun zur Identifikation vermeintlich legitimer militärischer Ziele – mit beträchtlichen „Kollateralschäden“ – verwendet werden: „Es [wird] berichtet, dass die israelische Armee in Gaza nach den Angriffen vom 7. Oktober neben etlichen anderen Systemen ein KI-System namens Lavender eingesetzt hat. … Lavender schaltet keine Werbeanzeigen, sondern setzt Menschen automatisch auf eine Tötungsliste, sobald ihre durch Überwachung gesammelten Datenmuster mit den Datenmustern angeblicher Kämpfer übereinstimmen.“

Den Einsatz von Lavender und anderen KI-gestützten Systemen bei Israels Krieg in Gaza hatte der Journalist und Filmemacher Yuval Abraham in mehreren Beiträgen für die Zeitschriften „+972 Magazine“ und „Local Call“ auf der Grundlage von Interviews mit aktuellen und ehemaligen Beteiligten aus den israelischen Streitkräften öffentlich gemacht. Seine Artikel eröffnen einen zuvor nie dagewesenen Einblick in die Schattenwelten algorithmischer Kriegführung. Grundlagen dafür sind im israelischen Fall die Daten, die über viele Jahre aus der Massenüberwachung der palästinensischen Bevölkerung gesammelt wurden. Anschließend wurden KI-Systeme wie Lavender mit den Daten vermeintlich bekannter Angehöriger der Hamas trainiert und wiesen anschließend nahezu jeder Person in Gaza einen Score zu, quasi die Wahrscheinlichkeit, mit der es sich um einen Anhänger einer militanten Gruppe handelt. Bis zu 35.000 Identitäten wurden so als Terroristen und vermeintlich legitime Ziele identifiziert. Die menschliche Kontrolle bestand im Wesentlichen darin, kurz mit diesen Identitäten verknüpfte Audio-Dateien anzuhören, um zu bestätigen, dass die entsprechende Person männlich ist. War dies der Fall, konnte ein Luftangriff auf die betreffende Person eingeleitet werden, vorzugsweise angeblich in der privaten Wohnung des Opfers. Bei einfachen mutmaßlichen Hamas-Angehörigen, die nur auf der Grundlage ihres Scores identifiziert wurden, wurden dabei bis zu zwanzig zivile Opfer als tolerierbar betrachtet. Die israelische Armee ging von einer Fehlerquote von zehn Prozent aus – auch das wurde als tolerierbar eingestuft.

Im August 2024 legte Abraham mit einem weiteren Bericht nach und beschrieb, wie die israelische Armee seit Oktober 2023 verstärkt auch auf kommerzielle Cloud-Anbieter, insbesondere Microsoft, Google und Amazon zurückgreift. Besonders eng sei demnach die Zusammenarbeit mit Amazon Web Services (Aws). Die

privaten Anbieter hätten dabei zweierlei zu bieten: ein nahezu unerschöpfliches Volumen an Rechen- und Speicherkapazität einerseits und fortgeschrittene, selbst der israelischen Armee angeblich überlegene KI-Anwendungen – die über Jahre mit Konsument*innen-Daten trainiert wurden.

Dass die Fusion von Tech-Industrie und westlichen Militärs kein neuer oder auf Israel beschränkter Prozess ist, stellten auch auf der Veranstaltung zur „Kill Cloud“ in Berlin verschiedene Referent*innen dar, darunter der Mathematiker Jack Poulson, der 2012 aus der KI-Forschung bei Google ausgestiegen war und seither für die NGO Tech Inquiry akribisch Dokumente auswertet, die entsprechende Verwicklungen dokumentieren. In seinem Paper, das ebenfalls im Rahmen der Berliner Konferenz zur Kill Cloud veröffentlicht wurde, zeichnet er die umfassende Kooperation zwischen Tech-Branche und Militär insbesondere in den USA anhand vieler verlinkter Quellen nach.

Nun ist die Verquickung von Militär, Rüstung und IT-Industrie keineswegs etwas Neues. Der 2011 verstorbene Medientheoretiker Friedrich Kittler etwa hatte über Jahre geradezu Spaß daran, die Unterhaltungsindustrie auf Forschung in Militärlaboren und Anwendungen im Zweiten Weltkrieg zurückzuführen und spitzte dies in der Formulierung von der „Rockmusik als Missbrauch von Heeresgerät“ zu. Auch das Internet begleiten seit seinen Anfängen zwei sehr unterschiedliche Narrative: Eine gut informierte, vielleicht auch etwas paranoide Minderheit sah darin von Anfang an ein Projekt zur Datensammlung und Auswertung durch US-Militär- und -Geheimdienstkreise auf dem Weg dahin, was seit Jahren unter dem Begriff Netzwerkzentrierte Kriegführung verhandelt wird. Diese Geschichte wird u.a. von Yasha Levine in seinem 2018 erschienenen Buch „Surveillance Valley“ nachgezeichnet. An der Oberfläche hielt sich demgegenüber ein Narrativ des durch Hippies und Tüftler geschaffenen globalen Netzwerks, das Freiräume schafft und die Welt enger zusammenrücken lässt. Sehr lange hat man Google als bis dahin wirklich beispiellose Ansammlung privater Daten sein vermeintliches Motto „Do no harm“ (Tue nichts Böses) durchaus abgenommen. Verbindungen mit Militär und Geheimdiensten gab es immer, wurden aber sehr zurückhaltend kommuniziert.

Das ändert sich seit gut zehn Jahren. Tech-Unternehmen würden im 21sten Jahrhundert eine vergleichbare Rolle spielen, wie Lockheed Martin im 20sten, prognostizierte Google CEO Eric Schmidt 2013. Im selben Jahr hat Amazon Web Services einen Auftrag im Umfang von 600 Mio. Dollar erhalten, um der CIA Cloud-Dienstleistungen bereitzustellen. 2020 wurde dieser Vertrag abgelöst durch das Projekt Commercial Cloud Enterprise, an dem neben Amazon auch die anderen großen Player beteiligt wurden: Google, Microsoft, Oracle und IBM. Neben den bekannten großen Playern drängen jedoch zunehmend Startups auf den Markt und wurden z.B. in das „Project Maven“ einbezogen, in dem das Pentagon Technologien entwickeln ließ, mit denen Drohnenaufnahmen großflächig KI-basiert ausgewertet werden können. Vergleichbare Projekte gab es auch für die Stimmerkennung, Gesichts- und Gestenerkennung aus Überwachungskameras und die KI-gestützte Zusammenführung verschiedener Datenquellen zum Profiling und Tracking von Einzelpersonen oder Netzwerken. Vieles davon ließ sich zunächst nur anhand geleakter Dokumente nachvollziehen oder wurde durch Proteste von Angestellten bekannt. Mittlerweile jedoch prahlen Unternehmen wie Palantir und Unternehmer wie Elon Musk mit ihrer (vermeintlich) zentralen Rolle im Ukraine-Krieg, Eric Schmidt philosophiert Seite an Seite mit Top-Militärs über die KI-gestützte Kriegführung im 21sten Jahrhundert. 2021 schloss Israel mit Google und Amazon einen Vertrag über 1,2 Mrd. Dollar, die daraufhin in Windeseile Rechenzentren in Israel errichteten, auf denen seither wohl ein Großteil der Daten über die palästinensische Bevölkerung gespeichert sind.

Wie die Künstliche Intelligenz z.B. durch – ausschließlich auf die palästinensische Bevölkerung angewandte – Gesichtserkennung bereits seit Jahren in den durch Israel besetzten Gebieten dazu beiträgt, Räume zu kontrollieren und Bevölkerungsgruppen auszuschließen, beschrieb im Kunstquartier Bethanien eindrücklich Matt Mahmoudi von Amnesty Tech. Den kolonialen Kontext des „Data Extractivism“ thematisierte ebenso eindrücklich auch Shona Illingworth, die an verschiedenen Orten „Airspace Tribunals“ veranstaltet, auf denen Betroffene über die vielfältigen Belastungen berichten, die aus der alltäglichen Präsenz (unbemannter) militärischer Luftfahrzeuge über ihren Köpfen resultieren. Selbst wenn diese nicht aus buchstäblich heiterem Himmel Menschen angreifen und töten, so sammeln sie doch für die Tech-Netzwerke in den ehemaligen Kolonialmächten die Daten, aus denen auf undurchdringliche Weise jene Algorithmen trainiert werden, mit denen anderswo – oft wiederum in ehemaligen Kolonien – Menschen exekutiert werden.