

**Wir, das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung, der Arbeitskreis gegen bewaffnete Drohnen und die Informationsstelle Militarisation fordern die Ächtung von Praktiken des *Targeted Killing* mit unterstützenden Systemen wie *Lavender* als Kriegsverbrechen.**

\* \* \*



\* \* \*

## *Targeted? Killing*

Menschen, Dinge und Ereignisse werden zu „programmierbaren Daten“. Es geht um 'Input' und 'Output', Variable, Prozentzahlen, Prozesse und dergleichen, bis jeglicher Zusammenhang mit konkreten Dingen wegabstrahiert ist und nur noch abstrakte Graphen, Zahlenkolonnen und Ausdrücke übrigbleiben.

*Joseph Weizenbaum*

*Der folgende Artikel kritisiert die technologische Rationalisierung von Krieg durch automatisierte Datenanalysen und -Entscheidungsfindungen. Er beruht auf Informationen des vergangenen War on Terror und investigativen Recherchen zur aktuellen Kriegsführung im Nahen Osten.*

Zahlreiche Artikel in den letzten Tagen berichteten über das KI-basierte System *Lavender*, das die israelischen Streitkräfte (IDF) einsetzen, u.a. um Hamas-Offiziere zu *identifizieren* und als menschliche Ziele (*human targets*) zu *markieren*. Die Markierungen werden an die jeweiligen IDF-Einheiten weitergegeben und ein weiteres System, *Where's Daddy?*, wird daraufhin aktiviert, um die Zielpersonen zu *verfolgen*. Sobald sie ihre jeweiligen Wohnhäuser betreten haben, werden sie bombardiert. Meist nachts und in Anwesenheit ihrer Familien.

Die Medien hierzulande, wie *der Spiegel*, *heise.de*, die *taz*, *Zeit online*, *der Freitag*, die *Berliner Morgenpost* oder auch sehr ausführlich *nd-aktuell*, bezogen sich auf die *investigative Recherche des israelischen Journalisten und Filmemacher Yuval Abraham*<sup>1</sup>. Er veröffentlichte diese im israelisch-palästinensischen Magazin +972 in Zusammenarbeit mit der unabhängigen, auf hebräisch erscheinenden Nachrichtenseite Local Call.

<sup>1</sup> Yuval Abraham, „‘Lavender’: The AI Machine Directing Israel’s Bombing Spree in Gaza“, +972 Magazine, 3. April 2024, <https://www.972mag.com/lavender-ai-israeli-army-gaza/>.

Bereits im November 2023 machte Abraham ein KI-gestütztes Befehls-, Kontroll- und Entscheidungsunterstützungssystem der IDF publik, dessen Einsatzzweck an der Markierung von Gebäuden und Strukturen, aus denen heraus militante Hamas-Kämpfer operieren sollen, ausgerichtet war: *The Gospel*<sup>2</sup>. *Lavender* hingegen markiert laut Zeugenaussagen Menschen. Es stellt keine Koordinaten von Stützpunkten, sondern von Wohnhäusern zur Verfügung. Es erstellt eine Liste von Personen, die getötet werden sollen. Eine *Kill list*.

Nicht wenige Formulierungen, die Yuval Abraham und die interviewten Soldaten benutzen, verweisen uns in Gedanken unweigerlich zurück zu der Hoch-Zeit des „*Global War on Terror*“ der US nach dem elften September. Das Töten von Familien als Kollateralschäden<sup>3</sup> – maschinell generierte Todeslisten – die Senkung der Bewertungsschwelle bei der Definition eines Militanten oder Terroristen – die militärisch und technisch erzeugte psychische Distanz zu den potenziellen Opfern in den Köpfen der Soldaten – die Farce des *targeted killings*, dass ausgereifere Technologien gezieltere Tötungen mit weniger zivilen Opfern ermöglichen sollen; es liest sich fast wie ein *Upgrade* des von den US geführten Drohnenkrieges. Aber irgendwie auch wiederum nicht. Die massive Fehleranfälligkeit komplexer informationsverarbeitender Systeme zur Überwachung, Identifizierung und zur Erfassung von Individuen konnte seither nicht behoben werden. Und das, obwohl die KI-Forschung und -Entwicklung in den letzten fünfzehn Jahren Quantensprünge machte. *Lavender* ist solch ein repräsentatives und zugleich prägnantes *Upgrade*, das aus jenen *Trial&Error* Zonen (s.u.) entsprang, die im *War on Terror* errichtet wurden, um Kriegstechnologien zu erforschen – in Afghanistan, im Jemen, in Somalia und vielen weiteren zivilen Räumen der Welt, die als Kriegsgebiete oder als *Combat Zones*<sup>4</sup> ausgewiesen wurden.

## High Tech Krieg

So ist auch *Lavender* den verfügbaren Informationen zufolge eines jener militärischen Systeme, die *Machine Learning* nutzen, eben jenen Teilbereich der KI, der algorithmisch bzw. mit statistischen Methoden Daten analysiert, um Muster in ihnen zu erkennen. Diese Muster dienen als Basis für automatisierte Empfehlungen an Führungs- und Einsatzkräfte, um sie auf verschiedenen Ebenen der Befehlskette bei der Lösung halbstrukturierter und unstrukturierter Entscheidungsprozesse zu unterstützen. Aus diesem Grund spricht man bei dieser Technologie auch von einer datengetriebenen: *data driven*. Zusammen mit Systemen wie *Gospel* und seinen Begleitsystemen *Fire Factory*<sup>5</sup>, das durch Zeitplan- und Priorisierungsfunktionen Angriffe vorbereitet, mit *Depth of Wisdom*, das das Tunnelnetz

<sup>2</sup> Yuval Abraham, „‘A Mass Assassination Factory’: Inside Israel’s Calculated Bombing of Gaza“, +972 Magazine, 30. November 2023, <https://www.972mag.com/mass-assassination-factory-israel-calculated-bombing-gaza/>.

<sup>3</sup> Der Begriff *Kollateralschaden* ist ein Euphemismus für zivile Opfer durch militärische Operationen. Nach dem humanitären Völkerrecht handelt es sich um einen ungewollten, aber zur Erreichung eines legalen Angriffs auf ein militärisches Ziel unvermeidbaren *Nebenschaden*, wie etwa das Zubruchgehen von Fensterscheiben eines dem Ziel naheliegenden Gebäudes.

<sup>4</sup> Eine *Combat Zone* ist ein Gebiet, das vom US-Präsidenten per Executive Order als ein Gebiet bezeichnet wird, in dem US-Streitkräfte an Kampfhandlungen teilnehmen oder teilgenommen haben. Afghanistan (und der darüber liegende Luftraum) wurde durch *Executive Order No. 13239* ab dem 19. September 2001 als *Combat Zone* ausgewiesen. In den Jahren darauf folgten die Länder Jordanien, Kirgisistan, Pakistan, Tadschikistan, Usbekistan, Philippinen, Dschibuti, Somalia, Syrien und weitere. Vgl.: Internal Revenue Service, „Combat Zones Approved for Tax Benefits“, zugegriffen am 14. April 2024, <https://www.irs.gov/individuals/military/combat-zones>.

von Gaza kartiert, *The Alchemist*, das Warnungen vor möglichen Bedrohungen in Echtzeit an die *Tablets* der befehlshabenden Offiziere sendet, zeigt diese weitere Publimachung von *Lavender* auch ein weiteres Mal, dass die Hemmschwelle, sich bei militärischen Operationen auf komplexe informationsverarbeitende Systeme zu verlassen, drastisch gesunken ist.

Die aktive und groß angelegte Entwicklungsphase bei diesem Ansatz zur Erfassung und Identifikation von Personen begann kurz nach der Jahrtausendwende im Zuge der Reaktionen auf die Terroranschläge am 11. September 2001, bei denen laut offiziellen Angaben 2996 Menschen in *New York City* und in *Washington* starben. Angesichts der gänzlich neuen Formen von Terroranschlägen und Attentaten wurden zahlreiche sicherheitsrelevante Förderprogramme vom Pentagon erlassen, u.a. im Bereich der rechnergestützten *sozialen Netzwerkanalyse*, bzw. den *Computational Social Science (CSS)*<sup>6</sup> und dem *Natural Language Processing (NLP)*<sup>7</sup>, der komputativen Verarbeitung natürlicher Sprache. Datenanalyse-Unternehmen wie *Palantir Technologies Inc.*, die auch im Jemen, im Irak, in Syrien, in der Ukraine, in Gaza und vielen weiteren Kriegen und Konflikten derzeit eine bedeutende Rolle spielen, begannen damals ihre kleinen, aber nicht zu unterschätzenden Imperien aufzubauen. Es waren eben jene IT-Unternehmen, die sich schnell auf die Überwachung von Individuen und die Analyse und Zusammenführung eigentlich getrennter Datenbestände spezialisierten, die in diesem Jahrtausend zu bedeutenden Playern wurden<sup>8</sup>. Der weltweite Einsatz von Drohnen (UAVs) als technische Objekte ist somit seit Beginn des Jahrtausends nicht mehr trennbar von den technischen Systemen zur Überwachung, Aufklärung und für Kampfhandlungen, wie bspw. der Ausführung von *signature strikes*<sup>9</sup>.

## War on error

Spätestens im Juni 2011, als der damalige US-Präsident Barack Obama ankündigte, seine Truppen schrittweise aus Afghanistan abzuziehen, begann sie, die militärische Ära von Identifizierungen und gezielten Tötungen (*Targeted Killings*) von Feinden mittels Drohnen. Sie wurden zur *Waffe der Wahl*,

<sup>5</sup> Marissa Newman, „Israel Quietly Embeds AI Systems in Deadly Military Operations“, *Bloomberg.Com*, 16. Juli 2023, <https://www.bloomberg.com/news/articles/2023-07-16/israel-using-ai-systems-to-plan-deadly-military-operations>.

<sup>6</sup> CSS stellt einen jungen Bereich der Wissenschaft dar, in dem soziokulturelle Phänomene mit Hilfe von neuartigen Datentypen (Big Data) und neuer Technologien untersucht werden: *Maschinelles Lernen, Text- und Data Mining*, sowie der sozialen Netzwerkanalyse.

<sup>7</sup> NLP ist eine Mischwissenschaft. Das Feld besteht anteilig aus Computer Linguistics, Computer Science und Artificial Intelligence, also der Wissenschaft der algorithmischen Verarbeitung von Sprache, der Wissenschaft von der Verarbeitung von Daten und der Wissenschaft vom künstlichem, intelligenten Verhalten.

<sup>8</sup> Vgl. Teil 2 Kapitel I Social Network Analysis in: Pratap Chatterjee und Christian Stork, „INC. Marketing the Illusion of Precision Killing“, CorpWatch Bericht, 2017, <http://www.killchain.org/>.

<sup>9</sup> Als *signature strikes* werden Tötungen von mutmaßlichen militanten Personen bezeichnet, deren Identität nicht vollkommen bekannt ist. Diese Tötungen basieren auf einer Lebensmuster-Analyse (*Life pattern*), d.h. auf Erkenntnissen über das Verhalten von Personen, die darauf hindeuten, dass es sich bei ihnen um militante Kämpfer handelt. Dieses Vorgehen wurde vom ehemaligen US-Präsidenten Bush 2008 in Pakistan erstmals abgesegnet und daraufhin auch in Afghanistan, im Jemen und in Somalia erlaubt. Das Pentagon gab offen zu, dass mit *Signature Strikes* häufig unbekannte Personen nur wegen ihres „verdächtigen Verhaltens“ getötet wurden. Vgl. Wolfgang Jung, „Die Befehlskette für die gezielten Tötungen, Die tödliche Bürokratie hinter Obamas Drohnen-Krieg, Luftpost, 30. Oktober 2015, [https://www.luftpост-kl.de/luftpost-archiv/LP\\_13/LP20115\\_301015.pdf](https://www.luftpост-kl.de/luftpost-archiv/LP_13/LP20115_301015.pdf). Deutsche Übersetzung des Artikels „The Kill Chain: The Lethal Bureaucracy behind Obama’s Drone War“, von Cora Currier, *The Intercept*, 15.10.2015, <https://theintercept.com/drone-papers/the-kill-chain/>.

zu einem zentralen Element des *High Tech Krieges*. Ohne Afghanistan, Jemen, Somalia u.v.w. Ländern, die im *War on Terror* zu *Combat Zones* mutierten, die quasi als sicherheitsbehördlich forcierter Nebeneffekt als *Trial&Error Zone* dienten, wäre diese Waffengattung heute in ihrer erweiterten und weit ausgereiften Form nicht denkbar gewesen. Systeme und Forschungsprojekte wie *Project Maven*<sup>10</sup>, *SKYNET*<sup>11</sup>, *Gorgon Stare*<sup>12</sup> im Drohnenkrieg, *Palantirs MetaConstellation*<sup>13</sup> in der Ukraine oder die *Artificial Intelligence Platform AIP for Defense*<sup>14</sup>, welche mit großer Wahrscheinlichkeit derzeit auch in Gaza zum Einsatz kommt<sup>15</sup>, zeigen der zivilen Öffentlichkeit den Weg auf, den Staaten und Technologieunternehmen im *War on Terror* einschlugen.

Der afghanische Journalist Emran Feroz sagte in einem Interview im Jahr 2021 mit *Democracy Now!*: „*We see how the war on terror in Afghanistan started and how it is ending now: It's with drones and civilian casualties*“. Bereits der allererste Angriff am 7. Oktober 2001 traf nicht Taliban-Chef Mullah Omar, sondern namenlose Afghanen (Namen der Opfer von Drohnenangriffen wurden in der Regel geheimgehalten<sup>16</sup>), so Feroz weiter. „*Dieses Szenario hat sich stets wiederholt. Bis heute.*“<sup>17</sup> Dies sagte er kurz nachdem publik wurde, dass die Opfer des letzten US-DrohnenSchlags im Afghanistankrieg

<sup>10</sup> *Project Maven* war ein Forschungsprojekt des Pentagons, bei dem versucht wurde, mit Hilfe von *Machine Learning*, die Fülle von Nachrichten-, Überwachungs- und Aufklärungsdaten im Drohnenkrieg zu sortieren und mit jenen im Ministerium und bei den Nachrichtendiensten abzugleichen. Google ging 2017 eine Partnerschaft mit dem leitenden Team des Pentagons, dem „Algorithmic Warfare Team“ ein.

<sup>11</sup> Christian Grothoff und J.M. Porup, „The NSA’s SKYNET Program May Be Killing Thousands of Innocent People“, *Ars Technica*, 16. Februar 2016, <https://arstechnica.com/information-technology/2016/02/the-nsas-skynet-program-may-be-killing-thousands-of-innocent-people/>.

<sup>12</sup> *Gorgon Stare* war einer der ersten publik gemachten Fälle, das trotz eines Wissens um die Fehlerhaftigkeit des Großraumüberwachungssystems in der Überwachung und Identifizierung von Personen, „aus Kosten- und Zeitgründen“ gebilligt und in Kampfhandlungen integriert wurde. Vgl. William Welsh, „Air Force test of Gorgon Stare reveals serious problems“, *Defense Systems*, 28. Januar 2011, <https://web.archive.org/web/20110128031208/http://defensesystems.com/articles/2011/01/24/gorgon-stare-test-shows-serious-glitches.aspx>.

<sup>13</sup> David Ignatius, „Opinion | How the Algorithm Tipped the Balance in Ukraine“, *Washington Post*, 19. Dezember 2022, <https://www.washingtonpost.com/opinions/2022/12/19/palantir-algorithm-data-ukraine-war/>.

<sup>14</sup> *AIP for Defense* ermöglicht die Verknüpfung und Analyse großer Mengen von Daten aus unterschiedlichen Quellen, um so komplexe Zusammenhänge und Muster aufzudecken. So „erkennt“ es unter anderem feindliche Stellungen. Durch eine Chatfunktion, ähnlich dem Interface von ChatGPT, schlägt es in Interaktion dann Gegenmaßnahmen vor. Eine Einstellung erlaubt es auch, Maßnahmen autonom auszuführen. Siehe: Palantir, „Palantir AIP for Defense“, Homepage, <https://www.palantir.com/platforms/aip/defense/>.

<sup>15</sup> *Palantir Technologies Inc.* ging im Januar 2024 eine strategische Partnerschaft mit dem israelischen Verteidigungsministerium ein. Sie zielt darauf ab, „das israelische Verteidigungsministerium bei der Bewältigung der aktuellen Situation in Israel maßgeblich zu unterstützen.“ Vgl. Marissa Newman, „Palantir Supplying Israel With New Tools Since Hamas War Started“, *Bloomberg*, 10. Januar 2024, <https://www.bloomberg.com/news/articles/2024-01-10/palantir-supplying-israel-with-new-tools-since-hamas-war-started>.

<sup>16</sup> Das *Bureau of Investigative Journalism* wirkte mit ihrem Projekt *Naming the Dead* öffentlichkeitswirksam dem Fakt entgegen, dass die US-Regierung sich vehement weigerte, Namen von Opfern durch Drohnenangriffe der CIA und des Pentagons preiszugeben. Das Projekt konzentrierte sich auf die Menschen in Pakistan, wo bis dato die meisten verdeckten Drohnenangriffe der USA stattgefunden haben. Das *Bureau* versuchte über Ortsansässige biografische Informationen von Getöteten zu sammeln, egal ob zivil oder militant, soweit möglich auch Fotos, Zeugenaussagen und amtliche Unterlagen, um diese zu veröffentlichen. Siehe: „Introducing the Naming the Dead project“, *The Bureau of Investigative Journalism*, <https://airwars.org/archives/bij-drone-war/namingthedead/?lang=en>.

<sup>17</sup> „U.S. Winds Down Afghanistan Occupation Like It Began, with Drone Strikes & Civilian Casualties“, 20. August 2021, *Democracy Now!*, [https://www.democracynow.org/2021/8/30/emran\\_feroz\\_afghanistan\\_us\\_withdrawal](https://www.democracynow.org/2021/8/30/emran_feroz_afghanistan_us_withdrawal).

vom 29. August 2021 nahe des Kabuler Flughafens keine IS-K Kämpfer waren, wie vom US-Geheimdienst vermutet<sup>18</sup>, sondern Zemari Ahmadi, langjähriger Mitarbeiter einer US-Hilfsgruppe, drei seiner Kinder, Zamir (20), Faisal (16) und Farzad (10), Ahmadis Cousin Naser (30), drei Kinder von Ahmadis Bruder Romal, Arwin (7), Benyamin (6) und Hayat (2) und zwei 3-jährige Mädchen, Malika und Somaya.

## Multi Domain Operationen

Der Drohnenkrieg geht weiter, in einer unaufhörlichen Dynamik. Auch die Bundeswehr rüstet in Sachen unbemenschter Systeme auf<sup>19</sup>. Unter Ausschluss der Zivilgesellschaft wurde die Vereinbarung im Koalitionsvertrag 2021, dass Drohnen der Bundeswehr nur unter verbindlichen und transparenten Bedingungen und unter Berücksichtigung ethischer und sicherheitspolitischer Aspekte bewaffnet werden können, missachtet. Der Haushaltsausschuss des Bundestags genehmigte am 6. April 2022 die Beschaffung von Präzisionsraketen aus Israel, die noch in diesem Jahr an die Bundeswehr für die *Heron TP* Drohnen geliefert werden sollen<sup>20</sup>. Auch zur Abwehr von Drohnenschwärmen werden derzeit Systeme mit *Machine Learning* Komponenten bei der Bundeswehr entwickelt. Ziel von *GhostPlay* bspw., einem Simulationssystem zur „KI-basierten Entscheidungsfindung in Maschinengeschwindigkeit“<sup>21</sup>, ist es, während des Gefechts so schnell Daten aufarbeiten zu können, dass Soldatinnen und Soldaten mehr Zeit bekommen, „ethische und informierte Entscheidungen zu treffen“ – so zumindest die militärische Vision von Gary Schaal, dem Leiter des BW-Forschungsprojekts.

Wie *Lavender* reiht sich auch *Ghostplay* in diesen Forschungs- und Entwicklungsstrang von sicherheitstechnologischen bzw. militärischen Systemen zum *Man Machine Teaming* (MMT) ein: komplexe informationsverarbeitende Systeme zur Navigation, Durchführung und zur effektiveren Entscheidungsfindung in multidimensionalen Einsatzgebieten. Diese Einsatzgebiete werden von der Bundeswehr als *gläserne Gefechtsfelder* bezeichnet, von den US und der NATO als *Transparent Battlefields*, und die dort notwendige Operationspraxis als *Multi Domain Operations* (MDO)<sup>22</sup>. Auf diesem Konzept, MDO, baut auch die am 4. April 2024 vorgestellte Strukturreform der Bundeswehr auf: auf komplexe militärische Operationen zu Land, zu Wasser, in der Luft, im Weltraum und im Cyberspace. Das Planungsamt der Bundeswehr beschreibt ihren Umbruch mit folgenden Worten: „Mit

<sup>18</sup> Matthieu Aikins u.a., „Times Investigation: In U.S. Drone Strike, Evidence Suggests No ISIS Bomb“, *The New York Times*, 10. September 2021, <https://www.nytimes.com/2021/09/10/world/asia/us-air-strike-drone-kabul-afghanistan-isis.html>.

<sup>19</sup> Vgl. Christian Heck, „Unbemenschte Systeme bei der Bundeswehr– Beobachtungen zweiter Ordnung“, in FIF-Kommunikation 2/2023, Hrsg. Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FifF) e.V. (Bremen: 2023). <https://ground-zero.khm.de/portfolio/unbemenschte-systeme-bei-der-bundeswehr/>.

<sup>20</sup> Vgl. Elsa Rassbach, „Bewaffnete Drohnen“, *Friedensforum* 2/23, April 2023, <https://www.friedenskooperative.de/friedensforum/artikel/bewaffnete-drohnen>.

<sup>21</sup> dtec.bw, „GhostPlay“, Homepage, <https://www.ghostplay.ai/>.

<sup>22</sup> Die NATO-Mitgliedstaaten einigten sich auf folgende Definition von MDO: „Orchestration of military activities, across all domains and environments, synchronized with non-military activities, to enable the Alliance to create converging effects at the speed of relevance.“ Vgl.: Planungsamt der Bundeswehr, „Multi Domain Operations für die Bundeswehr. Eine kurze Einführung.“, November 2023, <https://www.bundeswehr.de/resource/blob/5712296/ee4e4d36425e5366cec987225f3752e9/broschuere-data.pdf>.

*Multi-Domain Operations verbinden sich neben der Technik mehrere mindestens genauso wichtige nicht-technische Aspekte: Fragen zur Führungsphilosophie, angepasste Führungsverfahren und -prozesse, Ausbildung und die Einstellung der Menschen (mindset).“<sup>23</sup>*

## Mindsets

*Lavender* spielte – den Recherchen von +972 zufolge – insbesondere in den ersten Wochen nach dem Überfall der Hamas auf Israel am 7. Oktober 2023, bei dem, u.a. auch durch intelligente Waffensysteme und Kamikazedrohnen, 1200 Männer, Frauen und Kinder ermordet und rund 240 Menschen entführt und als Geiseln genommen wurden, eine zentrale Rolle für die israelischen Streitkräfte. Die IDF setzte offenbar großes Vertrauen in die möglichst fehlerfreie und zielgerichtete Finalität, die *Lavender* eingeschrieben zu sein schien. Doch so wie auch im US-amerikanischen Drohnenprogramm, in dem technische Fehler zu unzähligen zivilen Todesopfern im Laufe der Jahre führten, so war laut den von Yuval Abraham zitierten Zeugen ein Wissen um diese faktische Fehleranfälligkeit, zumindest in Geheimdienstkreisen und der militärischen Führungselite, auch bei den Einsätzen mit *Lavender* vorhanden. Israelische Geheimdienstmitarbeiter:innen überprüften den Zeugen zufolge direkt nach dem 7. Oktober die Genauigkeit von *Lavender*. Sie führten manuelle Zufallsstichproben von jeweils mehreren hundert Zielen durch, die von dem Programm markiert wurden.

Die methodische Umsetzung und die völkerrechtlichen Maßstäbe dieser stichprobenhaften *händischen Überprüfung* sind jedoch unbekannt, sodass aus der Recherche heraus nicht mehr zu schließen ist, als dass die 90%ige Treffergenauigkeit, die sich aus den Testdurchläufen ergeben hat, nach den eigenen Maßstäben der IDF als tolerierbar erachtet wurde. Mit anderen Worten: 10 Prozent der zur gezielten Tötung unter Inkaufnahme weiterer ziviler Opfer vorgesehenen menschlichen Ziele waren keine Kämpfer des militärischen Flügels der Hamas. Insbesondere Verwandte, Nachbarn, Zivilschutzbeamte und Polizisten wurden fälschlicherweise von *Lavender* markiert, da ihre Verhaltens- und Kommunikationsmuster jenen bekannter Hamas-nahen Militanten glichen. Auch Personen, die zufällig denselben Namen oder Spitznamen trugen oder ein Mobilfunktelefon benutzten, das zuvor einem Hamas-Kämpfer gehörte, wurden häufig falsch markiert. Mit der Zeit wurden auch jene, die rangniedrigeren Hamas-Mitgliedern glichen, markiert, da die israelische Armee ihre Trainings-Datenbank zum *maschinellen Lernen* sehr schnell mit Datensätzen nicht-befehlshabender Hamas-Kämpfer und Mitarbeiter der Zivilverwaltung erweiterte. Auf diese Weise gerieten Abertausende *per default* in den Kreis der Verdächtigen. Laut +972 an manchen Tagen bis zu 37.000.

## Collateral Murder

Den interviewten Soldaten zufolge entschied die Armee in den ersten Kriegswochen, dass bei jedem, der als niedrigrangiger Hamas markiert worden war, 5–20 zivile Todesopfer toleriert werden können, wobei die konkrete Zahl der tatsächlich anwesenden und getöteten Zivilist:innen während eines

<sup>23</sup> „DWT-Tagung: Multi-Domain Operations - Herausforderungen aus der Nutzerperspektive“, 3. November 2022, <https://www.bundeswehr.de/de/organisation/weitere-bmvg-dienststellen/planungsamt-der-bundeswehr-/dwt-tagung-multi-domain-operations-herausforderungen-aus-der-nutzerperspektive-5520056>.

Angriffs in der Praxis mit ziemlicher Sicherheit kaum überprüft und erfasst wurde. Bei ranghohen, bspw. einem Bataillons- oder Brigadekommandeur, sollen laut Bericht in +972 sogar mehr als 100 zivile Opfer zulässig gewesen sein. Diese Rechnung auf 37.000 Personen anzuwenden mit einer Fehlerquelle von 10% erscheint grausam. Doch nach den Berichten wurde diese Abwägung gemacht und in Teilen der israelischen Armee wurde demnach eine hohe Zahl zivile Opfer billigend in Kauf genommen. Eine der erschreckenden Erkenntnisse, wenn man diese Rechnung aus dem abstrakten Rechenraum ins Konkrete überführt, ist, dass *„die meisten Menschen, die sie getötet haben, Frauen und Kinder waren“*. Denn markierte Personen wurden in der Regel nachts und in ihren Wohnhäusern durch *signature strikes* angegriffen, während auch die gesamte Familie anwesend war. Dies geschah angeblich aus dem einfachen Grund, dass die Ziele auf diese Weise leichter zu lokalisieren waren.

Daniel Hale, ein ehemaliger Geheimdienstanalyst der *US Air Force*, der am 27. Juli 2021 zu 45 Monaten Gefängnis verurteilt wurde, nachdem er sich schuldig bekannt hatte, Regierungsdokumente durchgesickert zu haben, die das Innenleben und die schweren zivilen Kosten des US-Drohnenprogramms in den angegriffenen Gebieten aufgedeckt haben, sagte vor Gericht, er glaube, es sei *„notwendig, die Lüge zu zerstreuen, dass Drohnenkriege uns schützen und dass unser Leben mehr wert ist als ihres.“*<sup>24</sup> Er führte weiter aus, dass *„bei der Drohnenkriegsführung manchmal neun von zehn Getöteten unschuldig“* seien: *„Du musst einen Teil deines Gewissens töten, um deinen Job zu machen.“*<sup>25</sup>

Offenbar wird bei Soldatinnen und Soldaten aktiv versucht (nicht nur in *High Tech* Kriegen), es ihnen unmöglich zu machen, sich mit der Arendt'schen inneren Frage zu konfrontieren: *„Kann ich mit dem, was ich getan habe, noch weiterleben?“*<sup>26</sup>. Chelsea Manning, Edward Snowden, Brandon Bryant, Daniel Hale und viele weitere Soldatinnen, Soldaten und Geheimdienstmitarbeiter:innen, die zu Deserteuren oder Whistleblowern wurden, schafften es dennoch.

Denn diese Erkenntnis ist nicht wegzuleugnen: Eine *psychologische Distanz* zu den potentiellen zivilen Opfern muss Soldatinnen und Soldaten nicht nur antrainiert werden, sie muss auch kontinuierlich aufrechterhalten bleiben, um strategisch solch unverhältnismäßig hohe Zahlen an unschuldigen Opfern mit einzuberechnen und diese taktisch in Militärschläge einbauen zu können. Die Zivilgesellschaft lernte u.a. von Whistleblowern wie dem ehemaligen US-Drohnenpiloten Brandon Bryant: Auch ein Töten auf abstrakter Ebene und mit räumlicher Distanz lässt einen nicht einfach kalt - niemanden. Maschinen jedoch haben kein Herz. Sie sind kalt. Sie lösen die Verantwortung vom Menschen, der in seinem Herzen Mitleid empfindet, selbst wenn es voll Trauer und hasserfüllt ist. So die Aussage eines Soldaten im Gespräch mit +972: *„Der statistische Ansatz hat etwas an sich, das Soldaten an eine bestimmte Norm und einen bestimmten Standard festlegt. Bei diesen Operationen kam es zu einer unlogischen Anzahl von Bombenangriffen. Das ist in meiner Erinnerung beispiellos. Und ich habe mehr Vertrauen in einen statistischen Mechanismus als in einen Soldaten, der vor zwei Tagen einen*

<sup>24</sup> Ryan Devereaux, „Rep. Ilhan Omar Calls on Biden to Pardon Daniel Hale for Drone Leak“, The Intercept, 26. August 2021, <https://theintercept.com/2021/08/26/daniel-hale-pardon-ilhan-omar-drone-leak/>.

<sup>25</sup> Ryan Devereaux und Hussain Murtaza, „Daniel Hale Sentenced to 45 Months in Prison for Drone Leak“, The Intercept, 27. Juli 2021, <https://theintercept.com/2021/07/27/daniel-hale-drone-leak-sentencing/>.

<sup>26</sup> Hannah Arendt, *Über das Böse. Eine Vorlesung zu Fragen der Ethik* (München: Piper Verlag, 2006).

*Freund verloren hat. Alle dort, mich eingeschlossen, haben am 7. Oktober Menschen verloren. Die Maschine hat es kaltherzig gemacht. Und das hat es einfacher gemacht.“*

## Maschinenmoral?

Dieser Gedankengang führt uns unweigerlich zu jenen Ansätzen in der *Maschinenethik*, die davon überzeugt sind, dass Künstliche Intelligenzen nicht nur Soldatinnen und Soldaten zu ethischen Entscheidungen in multidimensionalen Gefechtsfeldern verhelfen können, sondern dass unbemenschte KI-Systeme auch selbst dazu in der Lage seien, „auf dem Schlachtfeld in ethischerer Weise zu handeln als menschliche Soldaten (...). Sie werden sich in schwierigen Umständen menschlicher verhalten können als menschliche Wesen“<sup>27</sup>, so der bekannte Robotiker und Pentagonberater Ronald C. Arkin.

Künstliche Intelligenz hat kein Gewissen. Für Drohnenpilot:innen oder Soldat:innen in den Einsatzzentralen wiederum, die sich auf sie verlassen müssen, ist es vermutlich nur schwer mit dem eigenen Gewissen vereinbar, sich oft ausschließlich auf die Auswertungs(un)genauigkeit solcher komplexer informationsverarbeitender Systeme verlassen zu müssen und auf die vorhergehenden formalen Befehls- und Ereignisketten angewiesen zu sein, während (Un-)Fälle, wie die von Zabet Amanullah, ihren Kamerad:innen tagtäglich passieren. Amanullah war ein im Wahlkampf stehender Zivillist, der im Jahr 2011 durch eine US-Drohne „versehentlich“ getötet wurde, da die Drohnenpilot:innen „keinen Namen gejagt haben, sondern auf ein Mobiltelefon zielten“, dessen Telefonnummer unter einem wichtigen Taliban-Anführer verzeichnet war.<sup>28</sup>

Ein Wissen um die hohe Fehleranfälligkeit von datengetriebenen technischen Systemen zur Erfassung und Identifizierung von Personen ist ihr stetiger Begleiter. Auf der anderen Seite sind sie mit dem Fakt konfrontiert, ständig sinnlich und geistig bei der Analyse von unsagbaren Massen an Informationen an ihre Grenzen zu stoßen. Nicht selten mit tödlichen Folgen: „Als bei einem Hubschrauberangriff im Februar 2011 dreiundzwanzig Gäste einer afghanischen Hochzeit getötet wurden, konnten die in Nevada auf Knöpfe drückenden Bediener der Aufklärungsdrohne die Schuld für ihren Irrtum auf die Informationsüberflutung schieben und sich darauf berufen, daß ihre Bildschirme mit Daten »vollgerotzt« würden – sie verloren den Überblick, gerade weil sie auf die Bildschirme schauten. Zu den Opfern des Bombardements gehörten auch Kinder, aber das Bedienpersonal »hatte sie inmitten des Strudels von Daten übersehen« – »wie ein Büroangestellter, dem in den täglichen Mailfluten eine dringliche Nachricht entgeht«. Und dem niemand vorwerfen könnte, daß er sich damit unmoralisch verhalten habe...“<sup>29</sup>

<sup>27</sup> Ronald C. Arkin, „Ethical robots in warfare“, IEEE Technology and Society Magazine 28, Nr. 1 (2009): 30–33, <https://doi.org/10.1109/MTS.2009.931858>.

<sup>28</sup> Kate Clark, „The Takhar attack: Targeted killings and the parallel worlds of US intelligence and Afghanistan“, Afghanistan Analysts Network, 10. Mai 2011, <https://www.afghanistan-analysts.org/en/special-reports/the-takhar-attack-targeted-killings-and-the-parallel-worlds-of-us-intelligence-and-afghanistan/>.

<sup>29</sup> Z. Bauman, D. Lyon, und F. Jakubzik, „Daten, Drohnen, Disziplin: Ein Gespräch über flüchtige Überwachung“ (Berlin: Suhrkamp Verlag, 2013).

Die Bilder, die sich von jedem Aspekt des Lebens abgetrennt haben, verschmelzen in einem gemeinsamen Lauf, in dem die Einheit dieses Lebens nicht wiederhergestellt werden kann.

Guy Debord

## Was tun?

Wir sehen: Genauso wenig wie Drohnen sind auch Systeme wie *Lavender* nicht einfach nur Werkzeuge, um etwas zu tun, sondern ihnen steht eine Finalität eingeschrieben. Eine Finalität, die sich jedoch erst durch technische, zweckgerichtete, in diesem Falle durch militärische Handlungen in Welt manifestiert. Dieser Zweck steht oft jenseits des Herstellungsprozesses der technischen Systeme selbst, was die Kontrolle über die Forschung, Entwicklung und Verbreitung dieser Technologien erschwert, bisweilen gar unmöglich macht. Bereits Max Weber, der Begründer der Soziologie als Wissenschaft, die in Verbindung mit den Computerwissenschaften Bereiche wie die *Computational Social Science* erst denkbar und Systeme wie *Lavender* somit auch erst entwerfbar machte, wies bereits vor 100 Jahren darauf hin, dass wir in der westlichen Welt meist nicht wissen, wie unsere moderne technische Lebenswelt funktioniert.<sup>30</sup> Es sei denn, wir sind Designer:innen, Programmierer:innen oder Ingenieur:innen, die sie entwerfen, oder eben Fachkräfte, die sie gestalten. Ansonsten, im Berufs- und Alltagsleben wissen wir meist ausschließlich, wie wir unser jeweiliges Verhalten anpassen müssen, damit unsere technischen Objekte ihre jeweiligen Funktionen erfüllen können. Ob nun eine militärische Handlung im gläsernen Gefechtsfeld, oder eine zivile Handlung in sozialen Netzwerken: „*Marketing or death by drone, it's the same math ... You could easily turn Facebook into that. You don't have to change the programming, just the purpose of why you have the system*“ (Chelsea Manning)<sup>31</sup>. Bei *Deep Learning*<sup>32</sup> jedoch können sich nicht einmal mehr die Fachkräfte selbst die inneren Funktionsweisen erklären bzw. wie die KI sich beim *Lernen* verhält.

Die Lehren, die die Zivilgesellschaft aus solch einer weiteren Veröffentlichung wie der von +972 zu *Lavender* ziehen kann, ist die, dass die technischen Fehler trotz Quantensprüngen in der technologischen Entwicklung noch stets dieselben tödlichen Fehler sind wie vor 15 Jahren. Was sich jedoch in den *High Tech Kriegen* unserer Zeit bedeutend weiterentwickelt und manifestiert hat, ist der Glaube, in einer technisch erzeugten Kriegswirklichkeit unabhängig von ihren Erzeugungstechnologien autonome, informierte und auch ethische Entscheidungen treffen zu können.

Systeme wie *Lavender* funktionieren letztendlich nicht anders als eine große ungenaue Bombe. In diesem Wissen können Soldat:innen die Verantwortung für ihre Tötungsentscheidungen nicht an Maschinen und Systeme delegieren. Das muss auch *technologiebegeisterten* Militärs und

<sup>30</sup> Max Weber, *Wissenschaft als Beruf*, (München: Duncker & Humblot, 1919). <http://archive.org/details/max-weber-1919-wissenschaft-als-beruf>.

<sup>31</sup> Carole Cadwalladr, „I spent seven years fighting to survive’: Chelsea Manning on whistleblowing and WikiLeaks, The Guardian, The guardian, 7. Oktober 2018, <https://www.theguardian.com/us-news/2018/oct/07/chelseamanning-wikileaks-whistleblowing-interview-carole-cadwalladr>.

<sup>32</sup> Die Technologie des *Deep Learning* begann sich um die Jahrtausendwende zu entfalten. Es begann bald darauf die Zeit von *Big Data* (dem Anstieg der Datenmengen durch die Verbreitung der Internettechnologien) und es wurden erhebliche Fortschritte in den Computertechnologien (in der Rechenkapazität, *GPUs* und preiswerten Speichertechnologien) erzielt. Erst durch diese technische Infrastruktur wurde die Weiterentwicklung der *Künstlichen Neuronalen Netze* (KNN) hin zum *Deep Learning* im Forschungs- und Anwendungsbereich möglich. Von dieser Technologie sprechen wir heute in erster Linie, wenn von Künstlicher Intelligenz zu hören ist: der *subsymbolischen Künstlichen Intelligenz*.

Politiker:innen und der Zivilgesellschaft bewusst sein. Insofern treffen diese eine grundlegende ethische Entscheidung, nämlich den Befehl zum Einsatz der Systeme.

---

29. April 2024

Der **Arbeitskreis gegen bewaffnete Drohnen** ist ein 2019 gegründetes Bündnis aus Organisationen, Netzwerken und Kampagnen der bundesweiten Friedensbewegung. Unser Ziel ist es, die gesamte Bandbreite zivilgesellschaftlicher Bewegungen zu vernetzen, die sich gegen Verletzungen grundlegender Menschenrechte durch militärische Drohnen zu Überwachung und bewaffneten Einsätzen engagieren. Der Arbeitskreis klärt auf über Forschung und Entwicklung neuer Technologien für autonome Waffensysteme sowie die Maschinenlesbarkeit gesellschaftlicher Subjekte durch diese. Das Bündnis informiert über die Robotisierung von Waffensystemen mit und durch Künstliche Intelligenz und weiteren „Machine-Learning-Techniken“. Weitere Informationen unter <http://drohnen.frieden-und-zukunft.de/>

Das **Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FifF) e. V.** ist ein deutschlandweiter Zusammenschluss von Menschen, die sich kritisch mit Auswirkungen des Einsatzes der Informatik und Informationstechnik auf die Gesellschaft auseinandersetzen. Unsere Mitglieder arbeiten überwiegend in informatiknahen Berufen, vom IT-Systemelektroniker bis hin zur Professorin für Theoretische Informatik. Das FifF wirkt in vielen technischen und nichttechnischen Bereichen der Gesellschaft auf einen gesellschaftlich reflektierten Einsatz von informationstechnischen Systemen zum Wohle der Gesellschaft hin. Zu unseren Aufgaben zählen wir Öffentlichkeitsarbeit sowie Beratung und das Erarbeiten fachlicher Studien. Zudem gibt das FifF vierteljährlich die „FifF-Kommunikation – Zeitschrift für Informatik und Gesellschaft“ heraus und arbeitet mit anderen Friedens- sowie Bürgerrechtsorganisationen zusammen. Hier finden sich unsere 10 Werte: <https://blog.fiff.de/about/>

Die **Informationsstelle Militarisierung (IMI) e.V.** versteht sich als Schnittstelle zwischen kritischer Friedensforschung und Friedensbewegung. Sie finanziert sich nahezu ausschließlich über Mitgliedsbeiträge und Spenden. Gegründet wurde sie Mitte der 1990er-Jahre in Reaktion auf eine offensichtliche Militarisierung der deutschen Außenpolitik. Bis heute ist die IMI der Auffassung, dass Tendenzen der Militarisierung am besten vor der eigenen Haustüre und gegenüber der „eigenen“ Regierung und Öffentlichkeit entgegengetreten werden sollte. Aus diesem Verständnis heraus hat sie u.a. 2013 ihren Drohnenforschungsatlas veröffentlicht, kritisiert die sicherheitspolitisch motivierte Beforschung und Entwicklung „Autonomer Systeme“ und „Künstlicher Intelligenz“ kontinuierlich - u.a. im Rahmen der sog. Sicherheitsforschung und der konkreten Auseinandersetzungen um Zivilklauseln. Auch in der Frage der Autonomisierung der Kriegsführung sieht die IMI keinen reinen Automatismus oder auch nur unhinterfragbare Pfadabhängigkeiten. Weitere Informationen unter <https://www.imi-online.de/>