PROKLA 217 | 54. Jahrgang | Nr. 4 | Dezember 2024 | S. 609-625
https://doi.org/10.32387/prokla.v54i217.2144

Jutta Weber*

»Eine sorgfältig konstruierte Maschine der Gewalt«

Über algorithmische Kriegsführung, abduktive Mutmaßungen und automatisiertes »Völkerrecht«[1]

Zusammenfassung: Die generelle Entwicklung und der Einsatz von militärischer »Data Science« bzw. Künstlicher Intelligenz (KI) und ihre Konsequenzen wurden lange vernachlässigt zugunsten einer Betrachtung der Probleme autonomer Waffensysteme, ihrer möglichen Regulation und der Bedeutung einer »Meaningful Human Control«. Anschließend an frühere Arbeiten diskutiere ich die Entwicklung, Architektur, die epistemische Logik und Materialität algorithmischer Kriegsführung sowie die Konsequenzen des Einsatzes fortgeschrittener KI-gestützter Entscheidungs-, Ziel- und Tötungssysteme am Beispiel des US-amerikanischen »War on Terror« und des Gazakrieges. Ich analysiere die epistemologischen und ontologischen Prämissen algorithmischer Kriegsführung und die soziotechnischen Implikationen dieser Mensch-Maschinen-Gefüge.

Schlagwörter: Epistemologie, Künstliche Intelligenz, Krieg, Lavender, Zielfindungssysteme

»A Carefully Constructed Machine of Violence«

On Algorithmic Warfare, Abductive Assumptions and Automated »International Humanitarian Law«

Abstract: The continuous development and use of military »data science« or artificial intelligence (AI) and its consequences have long received little attention. The focus was more on the problems of autonomous weapon systems, their possible regulation and the importance of »meaningful human control«. Following on from earlier work,

Jutta Weber ist Technikforscherin und Professorin für Mediensoziologie an der Universität Paderborn. Sie leitet seit 2024 das BMBF-Forschungsnetzwerk »Meaningful Human Control. Autonome Waffensysteme zwischen Regulation und Reflexion«. Siehe auch www.juttaweber.eu

1 Mein Dank für kritische Anmerkungen und Fragen gilt Heiner Heiland und den Reviewer*innen der Zeitschrift PROKLA sowie Leonie Kraatz für die Unterstützung bei Rechtschreibung und Formatierung.

I discuss the development, architecture, epistemic logic and materiality of algorithmic warfare and the consequences of the use of advanced AI-supported decision-making, targeting and killing systems using the example of the US »War on Terror« and the Gaza War. I analyse the epistemological and ontological premises of algorithmic warfare and the socio-technical implications of these human-machine structures.

Keywords: Artificial Intelligence, Epistemology, Lavender, Targeting Systems, War

»Krieg ist eine sorgfältig konstruierte Maschine der Gewalt. [...]
Während meiner Lebenszeit.
Es gab keine Sekunde ohne Krieg auf der Welt.« (Streeruwitz 2022)

»Es ist einfach, jede Gesellschaft mit Maschinentypen in Beziehung zu setzen, nicht weil die Maschinen determinierend sind, sondern weil sie die Gesellschaftsformen ausdrücken, die fähig sind, sie ins Leben zu rufen und einzusetzen.«
(Deleuze 1993: 258)

Der Besitz von KI-basierten Entscheidungs-, Ziel- und Tötungssystemen bedeute militärisch einen ähnlichen Machtvorsprung wie taktische Atomwaffen. Das zumindest behauptet Alex Karp,[2] CEO der marktführenden KI-Sicherheits- und Rüstungsplattform *Palantir*. Auch jenseits geschmeidiger Marketingparolen wird deutlich, dass immer mehr Armeen nicht nur mit KI-gestützten Waffensystemen und kostengünstigen Drohnen arbeiten, sondern dass mithilfe militärischer und kommerzieller Datenwissenschaft auch Entscheidungs- und Zielfindungssysteme – teils mit verheerenden Konsequenzen – im Krieg eingesetzt werden.

Die Diskussion der letzten zehn Jahre drehte sich vor allem um soziopolitische, völkerrechtliche und ethische Fragen autonomer Waffensysteme (Bhuta u.a. 2016; Scharre 2018). Militärische Großmächte wie die USA, Russland, UK oder China stritten über die korrekte Definition von autonomen Waffensystemen – wahrscheinlich um einer internationalen Regulation zu entgehen – oder man diskreditierte autonome Waffensysteme als »Terminator«-Systeme bzw. ferne Zukunftsmusik (vgl. u.a. SPD u.a. 2021; kritisch hierzu We-

2 »Sogar der CEO von Palantir, Alex Karp, hat argumentiert, dass ›die Macht der fortgeschrittenen algorithmischen Kriegsführungssysteme jetzt so groß ist, dass sie mit taktischen Atomwaffen gegen einen Gegner gleichzusetzen ist, der nur über konventionelle Waffen verfügt‹« (Bamford 2024; Übersetzung J.W.).

ber 2024). Doch in den aktuellen Kriegen wie etwa in Gaza zeigt sich in aller Deutlichkeit die zentrale Bedeutung von KI-basierten Systemen zur Entscheidungs- und Zielfindung – sowie bei der Tötung, was teilweise verheerende Konsequenzen für die Zivilbevölkerung hat.

Mit heutigen KI-gestützten Systemen lassen sich – wie im aktuellen Israel-Gaza-Krieg zu beobachten ist – die Produktion und Zerstörung von Kriegszielen und damit die Tötung von Menschen massiv beschleunigen und ausweiten (Abraham 2023, 2024a; Brumfiel 2023; Davies u.a. 2024; Marischka 2024; Suchman 2024). Das System »Hapsora« – ins Englische meist mit »Gospel« übersetzt – produzierte teilweise 50 Ziele am Tag; diese Zahl wurde mithilfe von menschlichen Analyst*innen innerhalb eines Jahres erreicht (Abraham 2024a). Gleichzeitig behaupten Anwender*innen wie die Israeli Defence Forces (IDF), dass die große Zahl der Ziele nicht nur *von der KI automatisiert produziert*, sondern auch *auf ihre Konformität mit dem Völkerrecht geprüft* würden. Gleichzeitig sei immer ein »human in the loop«, insofern Militärrechtsanwält*innen diesen Prozess nochmals überprüfen würden (IDF 2024; Sylvia 2024). Allerdings ist anzunehmen, dass sie angesichts der hohen Zahl vermutlich oft nur sehr wenig Zeit dafür haben. Dennoch: Die High-Tech-KI, die vorher als nicht mehr zu kontrollierendes Problem diskutiert wurde, das einer »meaningful human control« (Roff/Moyes 2016) bedarf, wird so geschickt als ethisches Instrument rekonfiguriert. Auf Distanz werden Ziele massenweise bestimmt und nicht nur mit Präzisionswaffen zerstört bzw. getötet. Dabei verwendet man nicht nur »Präzisions«-Waffen wie Lenkflugkörper, sondern auch ungelenkte Raketen oder Freifallbomben (»dumb bombs«) aus konventionellen Bombern (Abraham 2024a; Marischka 2024). Gleichzeitig werden zunehmend tödliche Kriege in Städten und dicht bevölkerten Regionen durch die KI-Anwendungen legitimiert. Die KI-gestützte, algorithmische Kriegsführung weitet sich nicht nur aus, sondern wird als Antwort auf die massive Kritik durch NGOs und Wissenschaft zugleich »ethisch« aufgeladen und algorithmische, KI-gestützte Kriegsführung wird als neue »Normalität« konfiguriert. Tatsächlich scheinen es Algorithmen zu ermöglichen, mögliche Verbindungen zwischen Personen oder Objekten in umsetzbare Sicherheitsentscheidungen zu übersetzen (Amoore 2009: 52).

Algorithmische Kriegsführung und militärische Datenwissenschaft

Doch was bedeutet fortgeschrittene algorithmische bzw. KI-gestützte Kriegsführung, die aktuell als die neue mächtige Wunderwaffe angepriesen wird, die mit taktischen Atomwaffen gleichzieht? Der Einsatz von Algorithmen-basierter Kriegsführung, von computergestützter »Aufstands«-Bekämpfung

sowie von (Aufklärungs-)Drohnen reicht bis zum Vietnamkrieg zurück (Edwards 1996; Reichborn-Kjunnerud 2025).

Während man im Kalten Krieg noch das Unkalkulierbare, sprich den Atomkrieg via Simulationen, Kriegsspiele und Computermodelle zu kalkulieren versuchte (Weber 2014), testete man im Vietnamkrieg verschiedene Ansätze und Programme direkt vor Ort. Vietnam wurde zu einem Computerlabor. Patrouillen sammelten vor Ort Informationen über die ländliche Bevölkerung, um sie im »Hamlet Evaluation System« mit Hilfe von IBM-Großrechnern zu ordnen, zu kategorisieren und zu klassifizieren und um Statistiken und Modelle für die Vorhersage aufständischer Aktivitäten in »Echtzeit« (Belcher 2013: 183) zu erstellen und Tötungslisten zu produzieren (González 2015: 14). Das Projekt »Igloo White« in Vietnam war wiederum eine Art elektronische Mauer entlang der sogenannten McNamara-Linie, die mit Sensoren bestückt wurde. Die Sensorinformationen wurden zu einem Flugzeug und von dort weiter zum Infiltration Surveillance Center (ISC) in Thailand übertragen. Das ISC analysierte die Daten für die weitere militärische Planung und um Ziele für taktische Luftschläge in Echtzeit bereitzustellen:

> »Obwohl einfach in seiner Konzeption, war Igloo White eine kreative Erfindung, die modernste Technologien und neuartige Mensch-Maschine-Konfigurationen nutzte, um ein ferngesteuertes, vernetztes Sensor-zu-Shooter-System zu schaffen, das das Gelände berechenbar machte und den Feind in eine anonyme technische Signatur übersetzte, ähnlich wie bei einem U-Boot – lokalisierbar, aufspürbar und abschießbar« (Reichborn-Kjunnerud 2025: 158; Übersetzung J.W.).

Damit spricht Erik Reichborn-Kjunnerud ein zentrales Moment dieser Entwicklung an: Das Feindesland beziehungsweise das Schlachtfeld wird digitalisierbar und der Feind eben auf eine technische Signatur reduziert. »Igloo White« wird heute als der Beginn der High-Tech-Sensor-Kriegsführung angesehen (Tambini 2007) und als ein wesentlicher Schritt in der Entwicklung hin zu den Drohnenkriegen (Gregory 2011).

Netzwerkzentrierte Kriegsführung und Revolution in Military Affairs

Im Zuge des allmählichen Zerbröckelns des Machtgleichgewichts des Kalten Krieges und der Politik der nuklearen Abschreckung entwickelte sich im US-Militär und in der US-Außenpolitik seit den frühen 1990er-Jahren das Konzept der »Revolution in Military Affairs« (RMA). Die RMA basiert auf den Paradigmen der technologischen Überlegenheit, der Informationssouveränität

(Arquilla/Ronfeldt 2001) und der engen Vernetzung von Informationstechnologien, einschließlich des Konzepts der »netzwerkzentrierten Kriegsführung« (Cebrowski/Garstka 1998). Das Informationsnetz wird zur zentralen militärischen Einheit. Der Kern dieses Ideals von netzwerkzentrierter Kriegsführung sind intelligente, kleine, flexible und geografisch verteilte Truppen, die ständig mit einem hochleistungsfähigen Informationsnetz verbunden sind. Dieses Netz besteht aus allen geeigneten Informationsquellen und soll schnelle Führungs- und Steuerungsprozesse ermöglichen. Die Vertreter*innen netzwerkzentrierter Kriegsführung träumen davon, den berühmten »Fog of War«, die Unübersichtlichkeit auf dem Schlachtfeld aufzulösen.

Der »computer-centric approach of RMA« (Belcher 2013: 51) wurde vom US-Militär im »War on Terror« eingeführt und konfiguriert Krieg als einen »Prozess des Hightech-Tötens auf Distanz« (Graham 2011: 29). Gleichzeitig wurde mit der damit einhergehenden Rhetorik der Präzision und der chirurgischen Schläge eine Humanisierung des Krieges behauptet. Der 2003 begonnene Irak-Krieg wird von vielen als erster operativer Test für netzwerkzentrierte militärische Strategien gesehen, die auf aggressiver, proaktiver Hightech-Kriegsführung und Network Science aufbauen.

Soziale Netzwerkanalyse als Terrorismusbekämpfung aus der Ferne

Ein weiteres wichtiges Verfahren für aktuelle algorithmische Kriegsführung ist die soziale Netzwerkanalyse (SNA), die in der Soziologie noch in analoger Form schon zu Beginn des 20. Jahrhunderts entwickelt worden war. Nach den Anschlägen von 9/11 – als US-Sicherheitsbeamten und Soldat*innen vorgeworfen wurde, sie hätten die entscheidenden Informationen nicht miteinander in Zusammenhang gebracht (»connecting the dots«) – wurde sie als neues Instrument zentral. Im »berühmten« US-amerikanischen Handbuch 3-24 zur Aufstandsbekämpfung (US Army/US Marine 2006), das die Doktrin der netzwerkzentrierten Kriegsführung begründete, wird es als leistungsfähiges Instrument zur Bewertung von Bedrohungen angepriesen. Und die Analyse sozialer Netzwerke hat im 21. Jahrhundert rasch an Bedeutung gewonnen, insbesondere als Bestandteil militärischer und sicherheitspolitischer Diskurse und Praktiken.

Die SNA bedient sich der Soziometrie, der Statistik und der Graphentheorie, um soziale Strukturen zu untersuchen. Es ist gut dokumentiert, wie die militärische Human Intelligence (HUMINT) und Signals Intelligence (SIGINT) zunehmend Data-Mining- und Analysetools einsetzen, die auf dieser relationalen Perspektive basieren, um Telekommunikation, soziale Netzwerke und Video-Feeds zu durchforsten (Joint Warfighting Center 2011; Ressler 2006). Gleichzeitig ist SNA von zentraler Bedeutung für die Präzisionsrhetorik, inso-

fern sie suggeriert, »hochwertige« Ziele zu identifizieren. Mit ihr würde gezielte, computergestützte Terrorismus- und Aufstandsbekämpfung aus der Ferne möglich. So behauptete man zum Beispiel, dass man aufgrund von SNA in der Lage war, Saddam Hussein gefangen nehmen zu können (Reed/Segal 2006).

Die Datenerfassung auf Grundlage der SNA-Prinzipien erzeugt soziale Graphen, die die sozialen Beziehungen von Personengruppen bis hin zu ganzen Bevölkerungen darstellen. Eingebettet in den breiteren Rahmen der netzwerkzentrierten Kriegsführung, baut die datengesteuerte Kriegsführung auf Data-Mining mithilfe von NOSQL-Datenbanken, Optimierungsalgorithmen und Analysen sozialer Netzwerke auf (Weber 2016; Mayer/Weber 2021). Diese Ansätze sind in den letzten zwei Jahrzehnten als Teil von KI-basierten Entscheidungs-, Ziel- und Tötungssystemen allgegenwärtig geworden.

Man stützt sich auf elektronische Aufklärung und arbeitet mit Tötungslisten, die mithilfe militärischer »data science« (und den Daten sowie der Software kommerzieller Plattformen wie Google, Amazon oder Palantir) erstellt werden. Diese Ansätze stützen sich auf transklassische, nicht-deterministische Berechnungsansätze, die den Feind auf der Grundlage von Data-Mining, sozialen Netzwerkanalysen, Inhalts- und Sentiment- bzw. Emotionsanalysen etc. *definieren*, verfolgen und töten. Datengesteuerte und teilweise KI-basierte militärische Entscheidungs-, Zielfindungs- und Tötungssysteme wurden im sogenannten »War on Terror« im Jemen, in Afghanistan, Pakistan und in Somalia eingesetzt. Heute wird ähnliche Software unter anderem von Russland, der Ukraine und Israel eingesetzt.

Skynet, Disposition Matrix und die Terrorist Screening Database

Der rasante Aufstieg der algorithmischen US-Kriegsführung via elektronischer Aufklärung, Data-Mining und maschinellem Lernen hat breite Kritik provoziert: Man würde unschuldige »Menschen auf der Grundlage von Metadaten« mithilfe von Drohnenangriffen töten – wie es in geleakten Dokumenten über das NSA-Programm »Skynet« und seine »wissenschaftlich nicht fundierten Algorithmen« (Grothoff/Porup 2016) beschrieben wurde. Die sogenannte Disposition Matrix ist eine zentralisierte Tötungs- bzw. Fahndungsliste der US-amerikanischen Regierung, die unter dem US-Präsidenten Barack Obama eingeführt wurde und die unterschiedlichen Listen der CIA und des Militärs zusammenführte (Weber 2016). Sie wurde von Präsident Donald Trump abgeschafft und die Hoheit über gezielte Tötungen zurück an das Militär delegiert. Präsident Joe Biden hat sie in modifizierter Form wieder eingeführt (Ackerman 2022). Sie spielt – zusammen mit Drohnen und Spezialeinheiten – eine Schlüsselrolle im globalen »War on Terror«, in dem die systematische

Verfolgung und gezielte Tötung von Individuen institutionalisiert wurde. Die Geografen Ian Shaw und Majed Akhter (2014: 211; Übersetzung J.W.) beschreiben die »Disposition Matrix« folgendermaßen:

> »In den ›Electronic Targeting Folders‹ werden Informationen über Terrorverdächtige aus aller Welt gespeichert. Diese Dokumente befinden sich in einer Datenbank, die als ›Disposition Matrix‹ bezeichnet wird und das bürokratische Schwert des Programms der gezielten Tötungen der Regierung Obama bildet. In der Disposition Matrix werden die Namen ›gefährlicher Personen‹ den Ressourcen gegenübergestellt, die zu ihrer Tötung oder Gefangennahme durch Drohnen oder Spezialeinheiten benötigt werden. Das institutionelle Instrument vereinheitlicht die Tötungslisten, die in der US Central Intelligence Agency (CIA) und im Verteidigungsministerium existieren, und zentralisiert damit die Verwaltung von Leben und Tod im Weißen Haus«.

Diese Tötungsliste ist eine flexible Datenbank, die strukturierte und unstrukturierte Daten enthält und mittels neuerer Algorithmen zum Data-Mining systematisch durchsucht werden kann. Sie basiert auf einer Technorationalität, bei der mit der Logik des systematisierten »Tinkerings« und Ausprobierens gearbeitet wird (Weber 2016), mit der das »Unbekannte« erforscht werden soll und mit der Unmengen von Daten durchforstet, gebündelt und viele (oftmals auch sehr unwahrscheinliche) Beziehungen bzw. Korrelationen zwischen Informationen hergestellt werden, um so »Wissen« in Datenbanken zu »entdecken« (Hildebrandt/Gutwirth 2008; Kitchin 2014). Dieser auf *Entdeckung* fokussierte Ansatz arbeitet nicht mit dem Konzept der Kausalität, sondern dem der Korrelation. Dieses folgt der Annahme, dass Verbindungen bzw. Zusammenhänge, die in der Vergangenheit auftraten, auch in der Zukunft wieder auftreten. Diese Logik der Korrelation wird umso »produktiver«, je größer die Datensammlung ist, da es mehr Möglichkeiten gibt, Korrelationen herzustellen und durch Rekombination sogenanntes »Wissen« zu produzieren. Somit wird die Zentralisierung von Tötungs- und Beobachtungslisten in der »Disposition Matrix« nicht nur durch politische Strategien und Entscheidungsträger*innen, sondern auch durch die innere Logik des Data-Minings vorangetrieben.

Von der »Disposition Matrix« zu »Lavender«

Die Logik und das Verfahren der US-amerikanischen algorithmischen Kriegsführung scheinen Parallelen zu den Israeli Defence Forces (IDF) im Gazakrieg aufzuweisen. Das System »Lavender« versammelt alle potenziellen palästinensischen Terrorverdächtigen – womit seit dem letzten Gazakrieg

alle als männlich identifizierten Verdächtigen praktisch automatisch auf einer Tötungsliste gelandet sind: »Formal ist das Lavender-System darauf ausgelegt, alle verdächtigen Personen in den militärischen Flügeln der Hamas und des Palästinensischen Islamischen Dschihad (PIJ), einschließlich derjenigen mit niedrigem Rang, als potenzielle Bombenziele zu kennzeichnen« (Abraham 2024a; Übersetzung J.W.).

Die Lektüre der einschlägigen Zeitungsartikel von Yuval Abraham (2023, 2024a) über die Targeting- und Tötungspraktiken der IDF löste bei mir ein Déjà-vu-Gefühl aus: Auch hier scheint man sich auf Data-Mining und maschinelles Lernen zu stützen, um Terroristen zu identifizieren bzw. Merkmale zu erkennen, die als »typisch« für Hamas-Aktivisten gelten. Und selbst wenn »Lavender« keine Tötungsliste im Sinne der Disposition Matrix sein sollte – wie von den IDF behauptet – und es sich »nur« um ein einfaches Dateninformationssystem handelt, stellt sich dennoch die Frage, wie man denn den »Terroristen« bzw. »Feind« definiert: Was sind die eindeutigen, relevanten Merkmale der »Hamas-Aktivisten«, die man in dieser Datenbank sammelt?

Bei der Erstellung der Disposition Matrix arbeitete man unter anderem mit der Terrorist Screening Database (TSD), einer vom FBI geführten Datenbank. Schon hier versuchte man via Data-Mining aus den Bergen von Daten Merkmale und Verhaltensmuster herauszufiltern, die mit »Terrorismus« in Verbindung stehen sollen. Was erstmal einfach klingt, ist ausgesprochen kompliziert, denn es gibt keine eindeutige internationale oder rechtsverbindliche Definition von Terrorismus und die von den US-Regierungsinstitutionen verwendeten Definitionen sind sehr unterschiedlich (Schmid 2011). Entsprechend ist völlig unklar, warum jemand als Terrorist*in gilt und in Datenbanken wie der TSD landet. Diese Liste umfasst heute etwa zwei Millionen Personen, darunter einige Tausend US-Amerikaner*innen. Und in den letzten sechs Jahren hat sich ihr Umfang verdoppelt. Zehntausende von Menschen haben sich nach Angaben des Ministeriums für Heimatschutz bei der US-Regierung darüber beschwert, dass sie auf der Liste stehen. Bei 98 Prozent von ihnen handelte es sich um »False Positives«, was bedeutet, dass sie nur deshalb markiert wurden, weil ihre Namen denen anderer Personen in der Datenbank ähnelten (Cauchi/Tyab 2023).

Das bringt uns zurück zu der Frage, auf welcher Grundlage das »Lavender«-System der IDF, das Informationen über fast jede im Gazastreifen lebende Person enthält, 37.000 Palästinenser*innen (von rund zwei Millionen Menschen im Gazastreifen) als militant identifiziert hat – von denen wiederum alle Männer als Zielpersonen betrachtet werden. Abrahams Zeug*innen bzw. anonyme Quellen wiesen darauf hin, dass die vom System ermittelten Zielpersonen genauso behandelt wurden wie auf Grundlage einer menschlichen Entscheidung. Dafür gibt es mindestens zwei mögliche Erklärungen: Zum einen ist das häufig

der Effekt eines *machine bias* – also der Tendenz vieler Menschen, Maschinen bzw. maschinellen Entscheidungen eine hohe Autorität zuzuschreiben – sowie zum anderen der hohe Druck des Militärs, »genügend« Ziele zu identifizieren. Dieser Druck wird auch von den Quellen in Abrahams (2024a) Artikel beschrieben.

Verschiedene Zeug*innen von Abraham (2024a) geben an, dass bekannt war, dass das »Lavender«-System mit einer Fehlerquote von etwa zehn Prozent arbeitet. Also scheint das von der IDF als akzeptabel angesehen zu werden – was nichts anderes bedeutet, als dass man bereit ist, viele Unschuldige aufgrund von Fehlern der KI zu töten – also nicht als »Kollateralschaden« bei der Bombardierung von Aufständischen, sondern aufgrund der Unschärfe des KI-Systems bei der Identifizierung von Zielen.

Wie kommt es zu einer so hohen Fehlerrate? Vermutlich werten hier – wie schon bei der »Disposition Matrix« – Forscher*innen Informationen aus den sozialen Medien (SOCMINT) aus, von Facebook über Instagram bis hin zu TikTok, in der Hoffnung, die relevanten Zusammenhänge herzustellen (»to connect the dots«). Die Auswirkungen dieses Vorgehens sind jedoch höchst problematisch: Aus Angst, potenzielle Verdächtige zu übersehen, werden die Suchkriterien in den Erkennungsalgorithmen sehr weit gefasst, um alle möglichen Korrelationen und Muster zu erfassen. Dementsprechend werden immer mehr Daten in Watch- und Kill-Listen aufgenommen. Die Zahl der Fehlidentifizierungen steigt entsprechend rapide an, denn um eine hohe Zahl falscher Negativ- oder Positivmeldungen zu vermeiden, bräuchte man ein genau definiertes »Terroristenprofil«: »Je besser Sie definieren können, wonach Sie suchen, desto besser werden Ihre Ergebnisse sein. Data Mining nach terroristischen Plots wird immer unscharf sein, und es wird schwer sein, etwas Nützliches zu finden« (Schneier 2006). Aus Angst, die wichtigen »Datenpunkte« zu übersehen, arbeitet man mit sehr weit gefassten Definitionen und Kriterien, die die Zahl der Personen in der Datenbank in die Höhe schnellen lassen.

Die IDF erklärten, dass sie »kein System der künstlichen Intelligenz verwenden, das terroristische Agenten identifiziert oder versucht vorherzusagen, ob eine Person ein Terrorist ist. Informationssysteme sind lediglich Werkzeuge für Analysten im Prozess der Zielidentifizierung« (IDF 2024). Die angekündigte Zusammenarbeit der KI-Sicherheits- und Rüstungsplattform Palantir Technologies mit den IDF (Bamford 2024) macht es schwer, diese Behauptung zu glauben. Aber selbst, falls die IDF nur mit einer »einfachen« Datenbank und ohne Data-Mining arbeitet, führen die notwendigerweise vagen Definitionen und Kategorien automatisch zu einem massiven Anstieg der Zahl der verdächtigen Hamas-Aktivisten – und damit werden immer mehr unschuldige Menschen zu potenziellen Zielen.

Wie beschrieben, nutzt das US-Militär seit dem »War on Terror« soziale Netzwerk-, Link- oder Sentiment-Analysen, um Ziele auszuwählen und zu verfolgen. Die Datenanalyse stützt sich meist auf elektronische bzw. Signalinformationen aus Videoübertragungen, Mobiltelefonen, geografischen Informationen, E-Mails sowie Inhalten aus den sozialen Medien. Dabei werden häufig quantitative Link-Analysemethoden eingesetzt. Das bedeutet konkret: Je häufiger jemand mit einem Verdächtigen in Kontakt tritt, desto verdächtiger wird auch diese Person – selbst, wenn es sich bei der kontaktierenden Person um einen Verwandten oder einen Freund handelt, der möglicherweise nicht Teil eines »Terrornetzwerks« ist. Abfragen in Datensammlungen werden bei der »Disposition Matrix« oft über zwei (oder drei) Schritte hinweg gemacht, um Verbindungen zu anderen verdächtigen »Terroristen« oder Mitgliedern »terroristischer« Organisationen zu finden.

Aktuelle »fortgeschrittene« KI-Kriegsführung ist offensichtlich alles andere als eine neue »Wunderwaffe«, wie sie im Marketing-Jargon von Palantir und Co. angepriesen wird. Die Grundlagen für aktuelle militärische KI-basierte Entscheidungs-, Ziel- und Tötungssysteme bilden postrelationale Datenbanken, Data-Mining und Machine Learning (ML). Schon 2012 zeigte ein Forscherteam wie man Bilder mithilfe von KI klassifizieren kann und wie man mit dieser »Kombination aus leistungsstarken Computern und gigantischen Datenmengen [https://www.image-net.org/] das Leistungsvermögen von KI-Techniken signifikant steigern [kann] – wobei diese Techniken schon in den späten Achtzigerjahren entwickelt worden waren« (Whittaker 2024). Neu sind nicht die KI-Ansätze, sondern die riesigen Rechenkapazitäten und Datenvolumen des Militärs, der Geheimdienste, aber auch der großen GAFAM-Plattformen (Google, Amazon, Facebook, Apple, Microsoft) und KI-Tech-Firmen wie Palantir, mit denen diese alten Konzepte eine neue Qualität gewinnen. So konnte die Bild- und Gesichtserkennung wesentlich besser und die Weiterentwicklung von KI als Large Language Models möglich werden.

Für diese Technologien des Tötens besteht offensichtlich von Vietnam bis heute – von »Igloo White« über die gezielte Tötung in Drohnenkriegen bis zum Einsatz autonomer Waffensysteme und KI-basierter Targetingsysteme wie »Lavender« – ein ontologisches und erkenntnistheoretisches Kontinuum.

Welt-konfigurierende Praktiken der algorithmischen Modellierung

Praktiken der algorithmischen Modellierung und der Big-Data-Analytik setzen sich in einem atemberaubenden Tempo in unseren technischen, militärischen, aber auch alltagsweltlichen Diskursen und Praktiken durch. Bereits 2009 schrieb Louise Amoore (2013: 9) in ihrem Essay über den algorith-

mischen Krieg, dass wir in Gesellschaften leben, in denen »Techniken wie ›Risikoprofilierung, algorithmische Modellierung, Informationsintegration und Datenanalyse zum maßgeblichen Wissen unserer Zeit geworden sind‹«. Welche Art von Verständnis unserer Welt und von uns selbst wird mit den weltbildenden Praktiken der algorithmischen Modellierung und der Big-Data-Analytik transportiert, die im 21. Jahrhundert hegemonial werden? Der Philosoph Gilles Deleuze (1993: 258) diagnostizierte bereits Ende des 20. Jahrhunderts: »Es ist einfach, jede Gesellschaft mit Maschinentypen in Beziehung zu setzen, nicht weil die Maschinen determinierend sind, sondern weil sie die Gesellschaftsformen ausdrücken, die fähig sind, sie ins Leben zu rufen und einzusetzen«. Nicht-deterministische Software-Artefakte kodifizieren, standardisieren und sortieren unsere Welt. Welche »Grammatik des Handelns« (Agre 1994) und des Denkens weisen sie auf?

Automatisierte Verfahren zur Rekombination und Verknüpfung von Daten, die größtenteils über Signal Intelligence bereitgestellt werden, bilden die erkenntnistheoretische Grundlage für Datenanalyse und Risikomanagement. Dieses Verfahren wird auf der Grundlage vordefinierter Kategorien organisiert und von der Vorstellungskraft im Sinne der Projektion mehr oder weniger wahrscheinlicher Szenarien und Zusammenhänge beherrscht. Halbautomatische Technologien der prädiktiven Analyse und des präventiven Handelns, der Echtzeitverfolgung und des Targetings werden als geeignete Mittel angesehen, um mit der Herausforderung unvorhersehbarer Risiken umzugehen. Das ist ein Ansatz, der an den Wunsch erinnert, einen »technological fix« zu finden und damit technologische Überlegenheit zu erreichen (Weber 2016: 119) – eine Vorstellung, die aus der netzwerkzentrierten Kriegsführung kommt.

Die massiven Fehlerraten und die Vagheit von Systemen wie »Lavender« sind nicht etwa dem frühen Entwicklungsstadium des Systems geschuldet – wie man an der Entwicklung der »disposition matrix« und der TSD sehen kann. Sie liegt deren ontologischer und epistemologischer Logik bereits zugrunde. Sie ist einer Logik des systematisierten Tinkerings und des Experimentierens geschuldet, die unter anderem unbekannte Gefahren, die sich per se nicht genau definieren lassen, durch iteratives Durchsuchen von Datenbergen finden möchte und dabei alle (un-)möglichen und oft sehr unwahrscheinlichen Korrelationen von Datenpunkten erkundet. Problematisch ist diese Technorationalität, da diese Logik der Entdeckung nicht auf der Idee kausaler Zusammenhänge, sondern auf Korrelation beruht. Das bedeutet, dass man »davon ausgeht, dass eine (mögliche) Korrelation aus der Vergangenheit irgendwann in der Zukunft wieder auftauchen wird« (Weber 2016: 109). Diese Systeme sind nicht anfällig für Fehler – der Fehler ist ein eingebauter Mechanismus sogenannter »Optimierung«.

Auch Marijn Hoijtink (2022: 325; Übersetzung J.W.) weist darauf hin, dass in der aktuellen »prototypischen Kriegsführung« Scheitern zu einer produktiven Kraft wird. Man könnte sagen, dass

> »die experimentelle Art der Kriegsführung weitgehend immun gegen Misserfolge ist oder sich nicht für die Kosten oder Folgen der durchgeführten Experimente interessiert. Jedes Ergebnis stellt einen wertvollen Datengewinn dar, und so dienen Misserfolge nur dazu, weitere Experimente zu fördern. Auf diese Weise ist die experimentelle Art der Kriegsführung weitgehend von Kritik abgeschirmt, da die Militärs immer auf die gewonnenen Erkenntnisse oder das zukünftige Potenzial des ›nächsten‹ Experiments verweisen können«.

Diese experimentelle Art der Kriegsführung ist nicht nur durch die Vorstellung gekennzeichnet, dass der Krieg selbst als ein Experiment zu sehen ist und durch geförderte experimentelle Praktiken von High-Tech-Militärs entsteht, die schnell neue Prototypen einsetzen, Ideen und neue Waffen testen. Diese Logik des Prototyps und Experimentierens korrespondiert mit der immanenten Logik des Tinkerings von nicht-deterministischen Software-Artefakten, etwa selbstlernenden Algorithmen, wie man sie auch in Drohnen nutzt. Versteht man die technowissenschaftliche Grundlage der KI, dann ist es nicht überraschend, dass diese Systeme, die auf systematisiertem Tinkering (Weber 2003) beruhen, zur Tötung vieler unschuldiger Zivilist*innen führen. Überraschend ist die Tatsache, dass wir in einer Gesellschaft und in einer Zeit leben, in der zumindest in weiten Teilen der Politik und teilweise im Militär die zehnprozentige Fehlerquote eines Systems wie »Lavender« bei der Bestimmung von zu tötenden Menschen als akzeptabel (oder unvermeidlich?) gilt.

Post-relationale Datenbanken, Data-Mining und nicht-deterministische, optimierende Algorithmen wurden in den letzten zwei Jahrzehnten zum bevorzugten Medium der Geheimdienste und des Militärs, das eine als inkohärent, unberechenbar und voller Risiken wahrgenommene Welt abbilden sollte (Aradau/van Munster 2007). Überschüssige Prozesse »emergenter« Verhaltensweisen werden durch das Sammeln riesiger Datenmengen auf der Grundlage von Signal- und Social-Media-Intelligenz genutzt. Datenbanken werden, meist auf quantitativer oder assoziativer Basis, von flexiblen Algorithmen auf der Suche nach Links, Verbindungen, Ähnlichkeiten oder Mustern durchsucht. Die Logik, der hier gefolgt wird, ist nicht die von Ursache und Wirkung, sondern eher die der Vorwegnahme (»Preemption«), des Experimentierens, der Korrelation und der Entdeckung.

Man hat Angst vor unbekannten, noch nicht imaginierten Gefahren und ist deshalb bereit, auf klassische wissenschaftliche Methoden, die zumin-

dest einen Anspruch an Exaktheit und wissenschaftliche Strenge hatten, zu verzichten, sondern nutzt stattdessen automatisierte Verfahren, die auf Rekombination und Imagination mittels systematisiertem Tinkering und formalisierten Prozessen von Versuch und Irrtum setzen. Diese Wissensproduktionssysteme fokussieren sich nicht mehr auf Problemlösung, sondern arbeiten mit abduktivem Denken, also dem Versuch, neue Erklärungshypothesen zu generieren, in denen man sich auf »unbekannte Unbekannte« fokussiert und mit ihnen jongliert.[3] Sie sind die zentralen Pfeiler einer neuen Ontologie, für die man epistemologische Gewissheiten aufgibt (vgl. Weber 2016; Reichborn-Kjunnerud 2025). Innerhalb dieser experimentellen, datengetriebenen Tinkering-Logik der umfassenden (Re-)Kombination kann jeder und jede zur Zielscheibe werden, während das immer weitere Sammeln riesiger Mengen von Überwachungsdaten sine qua non wird.

Deshalb beschleunigen datengetriebene Entscheidungs- und Zielsysteme, wie die »Disposition Matrix« bzw. »Lavender« oder »Gospel«, die mehr und schneller Terroristen bzw. Ziele identifizieren, auch die Tötungs- und Zerstörungsrate (Suchman 2024). Nicht nur die technisch-wissenschaftliche Logik der Algorithmen und der behauptete Zeitdruck, sondern auch die Aura dieser Systeme als technisch-wissenschaftlich, auf Mathematik und Statistik basierend, könnte Militärjurist*innen, die den IDF-Zielfindungsprozess überwachen, dazu bringen, maschinelle Entscheidungen zu akzeptieren, die sie nicht vollständig verstehen. Diese erkenntnistheoretische Logik des Tinkerings gewinnt in einem atemberaubenden Tempo an Dynamik und hat massive Auswirkungen auf die militärische Zielsetzung, aber auch auf Diskurse und Praktiken im Allgemeinen. Tinkering bzw. experimentelle Kriegsführung, die auf der Produktivität des Scheiterns aufbaut, ist Teil eines neuen technowissenschaftlichen Regimes, das versucht, der Welt auf neue Weise einen Sinn zu geben. Auch Erik Reichborn-Kjunnerud (2025; Übersetzung J.W.) geht davon aus, dass diese Technorationalität

> »die Art und Weise widerspiegelt, in der neu entdeckte epistemische Praktiken, materielle Infrastrukturen und Datenlogiken das militärische Denken in einer Weise verändert hat, dass die Welt als im ständigen Werden und Entstehen vorstellt, die angeblich nur durch possibilistische Logiken und iteratives Basteln und Experimentieren durch Versuch und Irrtum erfassbar ist«.

3 Ich danke Susanne Maurer dafür, mich an die Ambivalenz von Abduktion erinnert zu haben, die durchaus auch konstruktive Weisen von Erkenntnis ermöglicht – auch wenn sie als automatisierte fatale Konsequenzen zeigt.

Offensichtlich leben wir in einer Welt, in der das Denken mit und durch abduktives Denken auf der Grundlage von systematisiertem Tinkering und Bottom-up-Suchheuristiken tiefgreifend umgestaltet wird. Diese neuen Formen der Wissensproduktion entwickeln sich zu Standardlösungen für komplexe Probleme. Diese Rationalität ist das Rückgrat der militärischen Datenwissenschaft bzw. der algorithmischen Kriegsführung, die die Produktion und Sammlung von Daten, Verdächtigen und Zielen vorantreibt. Jenseits der ohnehin schon komplexen Frage, wie hochautomatisierte bzw. autonome Entscheidungs-, Zielfindungs- und Waffensysteme zu regulieren oder gar zu verbieten sind, bedarf genau diese zynische Kultur des Denkens genauer Aufmerksamkeit und radikaler Kritik. Die offene Frage wäre, wie diese Kulturen der Wissensproduktion hinterfragt werden können sowie ob und wie das Konzept einer sinnvollen menschlichen Kontrolle (»meaningful human control«) Anwendung findet.

Die marketingorientierten GAFAM-Überwachungsplattformen strecken heute ihre Finger zunehmend in Richtung militärisch-industriellem Komplex aus (u.a. Abraham 2024b). Laut der Zeitung *Tech Inquiry*, betrug die maximale Investition allein der fünf größten (bekannten) US-Rüstungsaufträge an Big Tech-Unternehmen zwischen 2019 und 2022 bereits 53 Milliarden Dollar. Das liegt nahe, weil heute ein großer Teil von Big Data für die militärischen Systeme von den GAFAM-Plattformen kommt, die auf dem Geschäftsmodell der systematischen und großflächigen Überwachung und des Profilings ganzer Bevölkerungen (in Kooperation und parallel zu den Datensammelpraktiken der Geheimdienste und der Militärs) basieren und dieses wird zunehmend in einer militärischen Datenwissenschaft »produktiv«. Genau diese (teilautomatisierte) und häufig rein quantitative Analyse von SIGINT durch SNA, Weblink-Analyse, Video-, Text-, Social Media- und Sentiment-Analyse ermöglicht es, Sensor-to-Shooter- oder Battle-Management-Systeme zu füttern, automatisiert Tötungslisten zu erstellen, Ziele zu produzieren und auszuwählen sowie Menschen zu verfolgen und zu töten (Joint Warfighting Center 2011; Ressler 2006; Sageman 2004; Weber; Abraham 2023, 2024a). Vor diesem Hintergrund ist es richtig und wichtig, die Ächtung von Systemen wie Lavender zu fordern (Grabenhorst u.a. 2024). Aber genauso zentral ist es, die possibilistische und damit zynische Rationalität zu verstehen, die nicht nur dieser »sorgfältig konstruierten Maschine der Gewalt« (Streeruwitz 2022) zugrunde liegt, sondern zunehmend mehr gesellschaftlichen Bereichen und alltäglichen Kontexten. Wenn auch der Fakt, dass diese possibilistische Rationalität zunehmend auch Entscheidungen über Leben und Tod dominiert, besonders schmerzlich ist.

Literatur

Abraham, Yuval (2023): ›A mass assassination factory‹: Inside Israel's calculated bombing of Gaza (30.11.2023). In: +972Magazine (in partnership with LocalCall). URL: https://www.972mag.com/, Zugriff: 2.9.2024.

– (2024a): ›Lavender‹: The AI machine directing Israel's bombing spree in Gaza (3.4.2024). URL: https://www.972mag.com/, Zugriff: 2.9.2024.

– (2024b): ›Order from Amazon‹: How tech giants are storing mass data for Israel's war (4.8.2024). URL: https://www.972mag.com/cloud-israeli-army-gaza-amazon-google-microsoft/, Zugriff: 2.9.2024.

Ackerman, Spencer (2022): Joe Biden's Disposition Matrix (31.10.2022). URL: https://www.forever-wars.com/, Zugriff: 2.9.2024.

Agree, Philip (1994): Surveillance and Capture: Two Models of Privacy. In: The Information Society 10: 101-127. DOI: https://doi.org/10.1080/01972243.1994.9960162.

Amoore, Louise (2009): Algorithmic war: everyday geographies of the war on terror. In: Antipode: A Radical Journal of Geography 41(1): 49-69. DOI: https://doi.org/10.1111/j.1467-8330.2008.00655.x.

– (2013): The Politics of Possibility: Risk and Security Beyond Probability. Duke University Press.

Aradau, Claudia / Van Munster, Rens (2007): Governing Terrorism Through Risk: Taking Precautions, (un)Knowing the Future. European Journal of International Relations 13(1): 89-115. DOI: https://doi.org/10.1177/1354066107074290.

Arquilla, John / Ronfeldt, David (2001): Die Entstehung des Netzkriegs (Revisited). In: Netzwerke und Netzkriege: Die Zukunft von Terror, Kriminalität und Militanz. 1-25.

Bamford, James (2024): How US Intelligence and an American Company feed Israel's Killing Machine in Gaza (12.4.2024). URL: https://www.thenation.com/, Zugriff: 2.9.2024.

Belcher, Oliver (2013): The Afterlives of Counterinsurgency: Postcolonialism, Military Social Science, and Afghanistan 2006-2012. Dissertation, University of British Columbia. Vancouver.

Bhuta, Nehal u . a . (2016): Autonomous Weapon Systems. Law, Ethics, Policy. Cambridge: Cambridge University Press.

Brumfiel, Geoff (2023): Israel is using an AI system to find targets in Gaza. Experts say it's just the start (14.12.2023).URL: https://www.npr.org/, Zugriff: 2.9.2024.

Cauchi, E.D. / Tyab, Imtiaz (2023): U.S. terrorist watchlist grows to 2 million people — nearly doubling in 6 years (14.12.2023). URL: https://www.cbsnews.com/, Zugriff: 2.9.2024.

Cebrowski, Arthur K. / Garstka, John J. (1998): Netzzentrierte Kriegsführung: Ursprung und Zukunft. In: US Naval Institute Proceedings 124(1): 28-35.

Davies, Harry / McKernan, Bethan / Sabbagh, Dan (2024): ›The Gospel‹: how Israel uses AI to select bombing targets in Gaza (1.12.2023). URL: https://www.theguardian.com/, Zugriff: 2.9.2024.

Deleuze, Gilles (1993 [1991]): Postskriptum über die Kontrollgesellschaften. In: Unterhandlungen. 1972–1990. Frankfurt/M.: 254-260.

Edwards, Paul (1996): The Closed World: Computers and the Politics of Discourse in Cold War America. In: Inside Technology. Cambridge, MA. DOI: https://doi.org/10.7551/mitpress/1871.001.0001.

González, Roberto J. (2015): Seeing into Hearts and Minds. Part 2. ›Big Data‹, Algorithms and Computational Counterinsurgency. In: Anthropology Today 31(4): 13-18. DOI: https://doi.org/10.1111/1467-8322.12188.

Grabenhorst, Susanne u.a. (2024): »The Myth of Targeted Killing«: Against the Rationalization of War (9.5.2024). URL: https://berlinergazette.de/, Zugriff: 2.9.2024.

Graham, Stephen (2011): Cities under Siege: The New Military Urbanism. London. DOI: https://doi.org/10.1002/9781444395105.ch11.

Gregory, Derek (2011): Lines of descent (8.11.2011). URL: https://www.opendemocracy.net/, Zugriff: 2.9.2024.
Grothoff, Christian / Porup, J. M. (2016): The NSA's SKYNET Program May Be Killing Thousands of Innocent People (16.2.2026). URL: https://arstechnica.com/, Zugriff: 29.12.2020.
Hildebrandt, Mireille / Gutwirth, Serge (Hg.) (2008): Profiling the European Citizen. Cross Disciplinary Perspectives. Berlin. DOI: https://doi.org/10.1007/978-1-4020-6914-7.
Hoijtink, Marijn (2022): ›Prototype warfare‹: Innovation, optimisation, and the experimental way of warfare. In: European Journal of International Security 7(3): 322-336. DOI: https://doi.org/10.1017/eis.2022.12.
ICRC (International Committee of the Red Cross) (2016): Views of the ICRC on autonomous weapon systems (11.4.2017). URL: https://www.icrc.org/, Zugriff: 2.9.2024.
IDF (2024): Israel Defence Forces' response to claims about use of ›Lavender‹ AI database in Gaza (3.4.2024). URL: https://www.theguardian.com/, Zugriff: 2.9.2024.
Joint Warfighting Center (2011): Joint Doctrine Support Division. Commander's Handbook for Attack the Network. Version 1.0. Suffolk; Virginia (20.052011). URL: www.dtic.mil/, Zugriff: 2.9.2024.
Kitchin, Rob (2014): The Data Revolution. Big Data, Open Data, Data Infrastructures & Their Consequences. Los Angeles. DOI: https://doi.org/10.4135/9781473909472.
Lawton, Joel (2016): Intelligence Planning and Methods Employed: Operation Red Dawn – The Capture of Saddam Hussein (16.3.2016). URL: https://smallwarsjournal.com/, Zugriff: 2.9.2024.
Marischka, Christoph (2024): AI-based Targeting – The Case of Gaza. Paper presented at the Pre-Conference Workshop »Imaginations of Autonomy: On Humans, AI-Based Weapon Systems and Responsibility at Machine Speed« (22.5.2024). URL: https://www.imi-online.de/, Zugriff: 2.9.2024.
Mayer, Katja / Weber, Jutta (2021): From Optimizing Military Operations to Targeting Terrorist Networks: Social Network Analysis in Data- Driven Warfare. In: Burkhardt, Marcus / Shnayien, Mary / Grashöfer, Katja (Hg.): Explorations in Digital Cultures. Lüneburg.
Reed, Brian J. / David R. Segal (2006): Social Network Analysis and Counterinsurgency Operations: The Capture of Saddam Hussein. In: Sociological Focus 39(4): 251-64. DOI: https://doi.org/10.1080/00380237.2006.10571288.
Reichborn-Kjunnerud, Erik (2025): The Worlds According to Military Targeting. Martial Epistemologies and Ecologies of Operation (im Erscheinen).
Ressler, Steve (2006): Social Network Analysis as an Approach to Combat Terrorism: Past, Present, and Future Research. In: Homeland Security Affairs 2(2): 1-10.
Roff Heather M. / Moyes, Richard (2016): Meaningful Human Control, Artificial Intelligence and Autonomous Weapons. Briefing paper for delegates at the Convention on Certain Conventional Weapons (CCW) Meeting of Experts on Lethal Autonomous Weapons Systems (LAWS). URL: https://article36.org/, Zugriff: 7.10.2024.
Sageman, Marc (2004): Understanding Terrorist Networks. Philadelphia. DOI: https://doi.org/10.9783/9780812206791.
Scharre, Paul (2018): Army of None: Autonomous Weapons and the Future of War. London.
Schmid, Alex (2011): The Definition of Terrorism. In: Ders. (Hg.): The Routledge Handbook of Terrorism Research. Abingdon, Virginia: 39-99. DOI: https://doi.org/10.4324/9780203828731.
Schneier, Bruce (2006): Data Mining for Terrorists (9.3.2006). URL: https://www.schneier.com/, Zugriff: 2.9.2024.
SPD / Bündnis 90/Die Grünen / FDP (2021): [Koalitionsvertrag zwischen SPD, Bündnis 90/Die Grünen und FDP:] Mehr Fortschritt wagen (7.12.2021). URL: https://www.spd.de/, Zugriff: 2.9.2024.
Shaw, Ian / Akhter, Majed (2014): The Dronification of State Violence. In: Critical Asian Studies 46(2): 211-234. DOI: https://doi.org/10.1080/14672715.2014.898452.

Streeruwitz, Marlene (2022): Handbuch gegen den Krieg. Wien 2022.
Suchman, Lucy / Weber, Jutta (2016): Human-Machine Autonomies. In: Bhuta, Nehal u.a. (Hg.): Autonomous Weapon Systems. Law, Ethics, Policy. Cambridge: 75-102.
Suchman, Lucy (2024): The Algorithmically Accelerated Killing Machine (24.1.2024). URL: https://ainowinstitute.org/, Zugriff: 2.9.2024.
Sylvia, Noah (2024): Israel's Targeting AI: How Capable is It? (8.2.2024). URL: https://www.rusi.org/, Zugriff: 2.9.2024.
Tambini, Anthony J (2007): Wiring Vietnam: The Electronic Wall. Lanham.
US Army / US Navy (2006): Counterinsurgency Field Manual. US Army and Marine Corps.
Weber, Jutta (2014): Wild Cards. Imagination als Katastrophenprävention. In: Zeitschrift für Kulturwissenschaft 8(2): 81-95. DOI: https://doi.org/10.14361/zfk-2014-0208.
– (2016): Keep adding. On kill lists, drone warfare and the politics of databases. In: Environment and Planning D: Society and Space 34(1): 107-125. DOI: https://doi.org/10.1177/0263775815623537.
– (2024): Autonomous Drone Swarms and the Contested Imaginaries of Artificial Intelligence. In: Digital War 5: 146-149. DOI: https://doi.org/10.1057/s42984-023-00076-7.
Whittaker, Meredith (2024): Das KI-Märchen (12.6.2024). URL: https://www.zeit.de/, Zugriff: 2.9.2024.