Z Außen Sicherheitspolit (2019) 12:213–235
https://doi.org/10.1007/s12399-019-00770-z

ZFAS Zeitschrift für Außen- und Sicherheitspolitik

STUDIE

Autonomie in Waffensystemen: Chancen und Risiken für die US-Sicherheitspolitik

Aaron Hansen · Frank Sauer

Online publiziert: 24. September 2019

Zusammenfassung Der Artikel analysiert die sich aus Autonomie in Waffensystemen ergebenden sicherheitspolitischen Implikationen. Er fragt am Beispiel der USA nach Chancen und Risiken, insbesondere mit Blick auf Proliferation und neue Verwundbarkeiten sowie Eskalations- und Instabilitätsdynamiken. Der Artikel schlussfolgert, dass die Strategie der USA mit Blick auf Autonomie in Waffensystemen mittel- und langfristig keinen Sicherheitsgewinn erzeugt. Abschließend werden die Hürden beleuchtet, denen sich multilaterale Rüstungskontrolle im Rahmen der UN aktuell gegenübersieht.

Schlüsselwörter Third Offset Strategy · Autonomie · Drohnen · Roboter · Künstliche Intelligenz

Autonomy in Weapon Systems: Opportunities and Risks for US Defence

Abstract The article analyses the security implications resulting from the current increase of autonomy in weapon systems. Drawing on the example of the US, the article weighs gains and risks, particularly with regard to proliferation and new vulnerabilities as well as dynamics of escalation and instability. The article concludes that the US's strategy regarding autonomy in weapon systems will not yield a net gain in security over the medium and long run. In closing, the article considers the hurdles that multilateral arms control within a United Nations framework is currently facing.

A. Hansen (✉) · Dr. F. Sauer
Universität der Bundeswehr München, Werner-Heisenberg-Weg 39, 85577 Neubiberg, Deutschland
E-Mail: aaron.hansen@unibw.de

Dr. F. Sauer
E-Mail: frank.sauer@unibw.de

Keywords Third Offset Strategy · Autonomy · Drones · Robots · Artificial intelligence

1 Einleitung

Mit dem Fortschreiten von Informationszeitalter und Digitalisierung wachsen Umfang und Komplexität der Aufgaben, die vom Menschen an Computer und Maschinen delegiert werden. Künstliche Intelligenz (KI)[1] und Robotik sind gegenwärtig die Schlüsseltechnologien in diesem Prozess. Die dadurch wachsende Bedeutung von Algorithmen und maschineller Autonomie sind mit der digitalen Assistentin Siri des Hard- und Softwareherstellers Apple oder dem Fahrassistenzsystem Autopilot des Automobilherstellers Tesla längst ins Bewusstsein der breiten Öffentlichkeit gerückt. Auch das Militär macht sich diesen Trend zunutze. Ein für die militärische Anwendung betriebener *spin-in* von im zivilen Sektor forcierten Robotik- und KI-Entwicklungen ist bereits seit einigen Jahren beobachtbar.

In diesem Zuge warnen führende Expert*innen aus der Forschung und zivilen Technologieunternehmen unter großer medialer Aufmerksamkeit, dass sich mit der Militärrobotik und der Entwicklung sogenannter autonomer Waffensysteme (AWS)[2] ein risikobehafteter sicherheitspolitischer Paradigmenwechsel in den internationalen Beziehungen abzeichne (FLI 2015, 2017).

Als AWS gelten, hier einleitend kurz und in Anlehnung an die Autonomiedirektive des Pentagons (DoD 2012, S. 13) umrissen, Waffensysteme, die nach der Aktivierung mithilfe von Sensoren und Software selbständig, also im Unterschied zu ferngesteuerten Systemen ohne jedwede menschliche Kontrolle, einen kompletten Entscheidungszyklus durchlaufen. Dies bedeutet konkret: Ziele aktiv finden, fixieren, verfolgen und diese – was von besonderer Bedeutung für die aktuelle Diskussion ist – auch ohne menschliches Eingreifen auswählen und bekämpfen (*find, fix, track, target, engage, assess*, F2T2EA).[3]

Vorreiter in der aktuellen Entwicklung bzw. Weiterentwicklung dieser Waffentechnologie sind neben China, Russland und Israel insbesondere die USA, die KI und Robotik zu zwei Pfeilern ihrer sogenannten Third Offset Strategy deklariert haben. Mit ihr soll, durch die weiter forcierte Nutzung von Hochtechnologie, und zwar insbesondere die Nutzung von Autonomie und Schwarmverhalten in Waffensyste-

[1] Unter dem weiten Begriff der Künstlichen Intelligenz werden eine Vielzahl unterschiedlicher softwarebasierter Techniken und Verfahren (von traditionellen Entscheidungsbäumen bis hin zu *deep learning* – maschinellem Lernen mit neuronalen Netzen) zur Automatisierung von Aufgaben subsumiert, deren Bewältigung zuvor menschliche Intelligenz erforderte. Im Folgenden wird, der Empfehlung des International Panel on the Regulation of Autonomous Weapons folgend (iPRAW 2017), auf den unscharfen KI-Begriff weitestgehend verzichtet. Stattdessen werden stets die konkreten, für die Diskussion mit Blick auf die Funktionen in autonomen Waffensystemen jeweils relevanten Techniken benannt, etwa maschinelle Bilderkennung.

[2] Häufig, insbesondere im Kontext der Vereinten Nationen, findet auch das Akronym LAWS (für *lethal autonomous weapon systems*) Verwendung.

[3] In Kapitel 3 werden wir die Frage der AWS-Definition und den *Neuigkeitswert* von Autonomie in Waffensystemen gesondert adressieren. Siehe grundlegend Scharre (2018).

men (bzw. in *systems of systems*), der gegenwärtige militärtechnologische Vorsprung der USA ausgebaut und gehalten werden. Während Befürworter*innen von AWS sich Effizienzgewinne und sogar eine Humanisierung der Kriegsführung versprechen, geben Kritiker*innen zu bedenken, dass die völkerrechtlichen, ethischen und sicherheitspolitischen Risiken und Schattenseiten solche (erhofften) Vorteile mittel- bis langfristig zunichtemachen könnten.

Die international einflussreichste, von Staatenvertretern*innen, Zivilgesellschaft und Wissenschaft hinsichtlich eventueller multilateraler Rüstungskontrolle für AWS geführte Diskussion findet gegenwärtig bei den UN in Genf im Rahmen der Convention on Certain Conventional Weapons (CCW) statt. Dort erzeugte das Thema 2014 mit einem *informellen Expertentreffen* erstmals auf dem diplomatischen Parkett erhebliche Resonanz, angeregt durch die aus zahlreichen Nichtregierungsorganisationen und Expertengruppen bestehende Campaign to Stop Killer Robots. Die Staatengemeinschaft bei der CCW diskutiert das Thema seither zunehmend intensiv, wozu seit 2017 auch formelle Gespräche im Rahmen einer Group of Governmenal Experts (GGE) zählen. Da sich aber diese diplomatische Diskussion um AWS wie auch der Großteil des rasch wachsenden interdisziplinären wissenschaftlichen Literaturkorpus in diesem Feld primär mit Technik, Kriegsvölkerrecht und Ethik beschäftigt, blieb die sicherheitspolitische Dimension des Themas bisher eher unterbelichtet (Altmann und Sauer 2017).

Dieser Artikel geht deshalb den sicherheitspolitischen Implikationen autonomer Waffensysteme nach, indem er antizipativ fragt, welche Chancen auf militärischen Sicherheitsgewinn welchen Risiken (etwa der Instabilität oder Eskalation) gegenüberstehen. Unter Sicherheit wird dabei im klassischen Sinne äußere (militärische) Sicherheit verstanden. Sicherheitspolitik ist demnach, in Ermangelung einer allgemein anerkannten Definition, das Vorhalten von Mitteln zur Durchsetzung legitimer nationaler Interessen mit dem Ziel, ein friedliches und stabiles internationales Umfeld zu wahren, eigene Verwundbarkeiten zu identifizieren und Risiken für das eigene Wohl zu reduzieren. Diese Ziele würden von einem ungeregelten Einsatz autonomer Waffensysteme berührt und dabei, so wird im Folgenden argumentiert, in Summe negativ beeinflusst.

Antworten sucht der Artikel am Beispiel der USA, da diese, wie bereits erwähnt, einerseits technologisch führend und andererseits der Entwicklung von AWS in besonderer Weise zugeneigt sind. Denn während inzwischen 29 Staaten bei den UN in Genf ein völkerrechtliches Verbot von AWS gefordert haben,[4] beharren die USA auf Erhalt und Ausbau ihrer technologischen Vormachtstellung. Für die USA ist demzufolge die Frage nach den sicherheitspolitischen Chancen und Risiken von AWS wichtiger und drängender als für jeden anderen Staat. Die im Folgenden entwickelten Überlegungen, wenngleich auch für andere Staaten bedeutsam, hätten also vor allem dann besonderes Gewicht, wenn sie im Falle der USA Geltung beanspruchen könnten.

Um zunächst die Bedeutung von AWS für die USA historisch herzuleiten und zu untermauern, wird in Kapitel 2 die exponierte Rolle von Technologie in der

[4] Ein Ziel, das auch NATO-Verbündete wie Deutschland teilen – zumindest gemäß der letzten beiden Koalitionsverträge (Bundesregierung 2013, S. 178, 2018, S. 149).

US-Sicherheitspolitik rekonstruiert. Kapitel 3 widmet sich dann AWS im Detail. Deren spezifische Vorteile sowie die doktrinären Beschränkungen ihres Einsatzes stehen daraufhin im Zentrum von Kapitel 4, ebenso wie die Lücken in dieser US-Doktrin und der sich daraus ergebende inhärente Widerspruch. Kapitel 5 untersucht daraufhin AWS-spezifische sicherheitspolitische Risiken. In Kapitel 6 erfolgt eine Schlussbetrachtung.

2 Hightech-Rüstung als Schlüsselmerkmal der US-Sicherheitspolitik

Der *American way of war* bzw. die typisch westliche Kriegsführung fußen auf vielfältigen gesellschaftlichen, politischen und ideologischen Grundlagen. Alternde und postheroische westliche Gesellschaften sind so beispielsweise stets auf die Vermeidung von Opfern bedacht, wozu insbesondere solche unter den eigenen Streitkräften, aber auch gegnerische Verluste zählen (Münkler 2015, S. 184-185, 204).

Bedient man sich der Theorie des demokratischen Friedens, oder genauer ihren „Antinomien" (Müller 2004), als Heuristik, dann rücken die spezifischen Anforderungen in den Fokus, die Gesellschaften in liberalen Demokratien an ihre gewählten Entscheidungsträger*innen stellen. Demokratische Außen- und Sicherheitspolitik, so zeigt sich, muss bestimmte Regeln befolgen, um Kriege führen zu können (Geis et al. 2010, 2013).

Eine Schlüsselregel ist dabei der Transfer von politischen Kosten bzw. Risiken, so dass diese nicht auf die – in einer Demokratie abwählbaren – Entscheidungsträger*innen zurückfallen. Die USA sind hier insofern typisch, als sie sich zum Beispiel bevorzugt auf ihre wenig verlustanfälligen Luftstreitkräfte (bisweilen in Verbindung mit lokalen Alliierten oder privaten Militärdienstleistern am Boden) stützen, wodurch das Leiden und Sterben der eigenen Bürger*innen in Uniform räumlich und gedanklich auf Distanz zur Heimatgesellschaft gehalten, der Feind aber zugleich diskret, schnell und effizient bekämpft werden soll. Auch wenn der Schutz des zivilen Lebens dabei nicht die gleiche Priorität wie jener der eigenen Streitkräfte genießt, so muss doch in der Öffentlichkeit der Eindruck eines weitestgehend sauberen, unblutigen, *chirurgisch präzisen* Krieges gewahrt bleiben. Der Anreiz zu stetem technologischem Vorsprung in der Rüstungstechnologie besteht in den USA also nicht nur aufgrund der daraus resultierenden militärischen Überlegenheit nach außen. Er entspringt, nicht weniger wichtig, auch aus der Notwendigkeit, Kriege nach innen demokratisch legitimierbar zu machen (Shaw 2005, S. 82-84, 88-89; Kaag und Kreps 2014; Sauer 2014; Dickow 2015, S. 17-18; Sauer und Schörnig 2012, S. 368-369).

Diese herausgehobene Bedeutung von Technologie für die US-Sicherheitspolitik lässt sich bereits anhand weniger Beispiele aus der jüngeren Vergangenheit untermauern. So führte etwa die Operation Desert Storm im Jahr 1991 die Narrative der Präzisionskriegsführung und der Revolution in Military Affairs (RMA)[5] ein. Zu-

[5] Unter Revolution in Military Affairs wird eine tiefgreifende Umwälzung der Kriegsführung verstanden. Häufig liegt bei der Verwendung des Begriffs ein Fokus auf neuen Technologien und den im Rahmen ihrer militärischen Anwendung stattfindenden Änderungen von Strategien, Taktiken und Doktrinen.

gleich läutete sie einen radikalen Wandel in der konventionellen Kriegsführung ein (Mahnken 2008, S. 157, 167). Auch wenn der Begriff als solcher nicht unumstritten blieb,[6] bleibt doch festzuhalten, dass sich die USA in den letzten knapp drei Dekaden im Zuge der RMA eine beispiellose militärtechnologische Dominanz sicherten. Bereits im Kosovokrieg wurde der Grundstein für die Nutzung von unbemannten fliegenden Waffensystemen *(Drohnen)* gelegt, unter anderem mit dem System Predator, das man als Konsequenz dieses Konflikts und unter dem Eindruck der terroristischen Anschläge vom 11. September 2001 bewaffnete (Cordesman 2000, S. 320-322). Weltweite Aufmerksamkeit erfuhren Drohnen dann spätestens mit ihrem massiven Einsatz im sogenannten Krieg gegen den Terror, der ohne diese unbemannten Waffensysteme nicht in der bekannten Form führbar wäre (Mahnken 2008, S. 201; Sauer 2014; Kaag und Kreps 2014). Technologische Lösungen sind dabei zwar keine militärische Erfolgsgarantie, aber ein verlässlicher Hebel:

> Better technology hardly makes for certain victory against determined and clever foes – consider Korea, Vietnam, Iraq, or Afghanistan – but it has been something the US has been able to count on, and has taken for granted, at every level of conflict from grand strategy to squad tactics. (Freedberg 2012b)

Der Verlass auf Hochtechnologie und unbemannte Waffensysteme findet sich somit auch in der eingangs bereits erwähnten Third Offset Strategy wieder, die in der Administration des ehemaligen US-Präsidenten Barack Obama durch Ex-US-Verteidigungsminister Chuck Hagel 2014 angekündigt, dann maßgeblich von Ex-Vize-Verteidigungsminister Robert Work in ihrer Umsetzung weiter forciert und jüngst durch die Administration von US-Präsident Donald Trump, wenngleich weniger prominent hervorgehoben, erneut bekräftigt wurde (Mehta 2018). Anlass für die versuchte *Absatzbewegung* ist nicht etwa die Terrorismusbekämpfung, sondern die in den USA empfundene Bedrohung durch die *near peer competitors* China und Russland. Die Third Offset Strategy soll also im Rahmen der strategischen Umstellung von *Terrorismusbekämpfung* auf *Großmachtkonflikt* die US-Vorherrschaft in der militärischen Hochtechnologie halten und weiter ausbauen (Hagel 2014; Eaglen 2016b; Freedberg 2016).

Tatsächlich investieren China und Russland ihrerseits in die Modernisierung ihrer konventionellen Streitkräfte. Im Südchinesischen Meer besteht so beispielsweise für China aufgrund seiner neuen *Anti-Access and Area Denial*-Fähigkeiten die Möglichkeit, US-amerikanische Machtprojektion zu unterbinden, also Zugang zu verwehren und militärische Handlungsmöglichkeiten einzuschränken (Eaglen und Birkey 2012, S. 4-5; Bitzinger 2016; Overhaus 2015, S. 8, 21). In Reaktion auf derartige neue Herausforderungen liegt der Fokus der Third Offset Strategy neben Cyberfähigkeiten, *stealth* (Tarnkappentechnologie) und *hypervelocity vehicles*[7] insbesondere auf (Schwärmen aus) autonomen Waffensystemen, mit denen das US-Militär zukünftig

[6] Zur Diskussion um den Begriff der RMA siehe Shaw (2005, S. 32) und Singer (2009, S. 181).

[7] *Hypervelocity vehicles* bewegen sich mit Geschwindigkeiten von Mach 5, also fünffacher Schallgeschwindigkeit, oder mehr. Unter den Sammelbegriff fallen Marschflugkörper ebenso wie *glide vehicles*, die mit ballistischen Raketen verbracht werden.

global handlungsfähig bleiben möchte (Overhaus 2015, S. 15; Eaglen 2016a, 2016b; Hammes 2018).

In diesem Zuge ist in den USA auch ein Wandel im Verhältnis zwischen privaten Unternehmen und Militär beobachtbar. Wie einleitend bereits angedeutet, sind militärisch relevante technische Innovationen keine exklusive Domäne der Verteidigungsindustrie oder etwa der Defense Advanced Research Projects Agency (DARPA) des Pentagon mehr. Der zivile Sektor ist der primäre Innovationsmotor bei der Erforschung neuer, auch für den Verteidigungssektor bedeutsamer Schlüsseltechnologien. Zivile Entwicklungen, wie etwa Algorithmen für Bilderkennung oder autonom operierende Roboter, werden häufig zuerst für kommerzielle Zwecke entwickelt und dann für militärische adaptiert; nicht umsonst sucht das Pentagon mit seiner Dependance Defense Innovation Unit Experimental (DIUx) im Silicon Valley schon seit einer Weile gezielt die Nähe zu zivilen Technologieunternehmen (Hagel 2014; Work und Brimley 2014, S. 35; Kaplan 2016; Sauer 2018a).

Die Entwicklung von AWS in den USA folgt also einem *evolutionären*, für die US-Sicherheitspolitik schon seit Jahrzehnten kennzeichnenden Pfad. Das wiederum bedeutet jedoch keinesfalls, dass die zukünftigen Folgen dieser Entwicklung nicht *revolutionär* sein könnten. Dies führt zu der Frage, was genau die AWS-Entwicklung ausmacht und welche Chancen und Risiken sie aus US-Sicht birgt.

3 Autonomie in Waffensystemen

Waffensysteme, die *selbstständig* Ziele bekämpfen, existieren schon länger. So werden bereits seit Jahrzehnten Verteidigungssysteme gegen Raketen, Artilleriegeschosse oder Mörsergranaten eingesetzt, die anfliegende Munition – unter Zeitdruck ggf. ohne menschliches Eingreifen *(terminal defense)* – bekämpfen.[8] Solche in der Regel stationären *Sense and React to Military Objects*-Systeme (SARMO) führen allerdings nur die immer gleichen vorprogrammierten Aktionen automatisch und in wiederholter Form aus. Sie sind aufgrund ihrer Schutzfunktion sowie der Tatsache, dass sie sich primär gegen Material, also in aller Regel gegen unbelebte Ziele richten,[9] im Rahmen der AWS-Diskussion auch weitgehend unumstritten (Amoroso et al. 2018).

Als AWS werden demgegenüber häufig solche mobilen Systeme bzw. Waffen(plattformen) verstanden, die ohne menschliche Steuerung oder Aufsicht ggf. über längere Zeit in dynamischen, unstrukturierten, offenen Umgebungen operieren und sich dabei durch die Verarbeitung von Sensorsignalen und Algorithmen zur *Entscheidungsfindung* an Bord vollumfänglich selbst steuern und den gesamten einleitend erwähnten *targeting cycle* des *find, fix, track, target, engage, assess*

[8] Selbst Minen werden bisweilen unter ein breites Verständnis von Waffenautonomie subsumiert – zumindest solche, die anhand bestimmter Signaturen eine *Zielauswahl* treffen und nicht nur auf einem primitiven, opferaktivierten An-/Aus-Mechanismus ohne Selbstregulierungsschleife beruhen. Wir danken den anonymen Gutachter*innen für den Hinweis.

[9] Auch Verteidigungssysteme (genannt sei hier beispielhaft das Luftabwehrsystem Patriot) können natürlich mitunter belebte Ziele (etwa bemannte Flugzeuge) bekämpfen. Dieses Kriterium ist also nicht unbedingt trennscharf. Die Frage der AWS-Definition ist insgesamt außerordentlich diffizil, wie in diesem Kapitel herausgearbeitet werden soll.

absolvieren.[10] Im Drohnensektor existieren mit der US-amerikanischen X-47B, der britischen Taranis und der französischen nEUROn bereits mit dieser Zielsetzung entwickelnde Technologiedemonstratoren.

Eine trennschärfere Definition und Eingrenzung des Autonomiebegriffs fehlt aber bisher sowohl im diplomatischen als auch im wissenschaftlichen Strang der AWS-Diskussion (UNIDIR 2014, S. 3) – das verwundert nicht, denn die Grenzen sind fließend. So liegt etwa die Unterscheidung zwischen dem, was aktuell unter AWS diskutiert wird, und bereits existierenden *loitering munitions*[11] nicht unbedingt auf der Hand – als Beispiel sei dafür auf die israelische Anti-Radar-Munition Harpy verwiesen, die zumindest für ihren begrenzten Einsatzzweck (Kreisen über einem Gebiet und Bekämpfung gegnerischer Luftabwehr anhand von Radarsignaturen) den *targeting cycle* bereits selbständig durchläuft (und somit als AWS gelten kann, Scharre 2016a, S. 21).

Auch die oben eingeführte, auf den ersten Blick recht hilfreiche Kontrastierung von *nur* automatischen SARMO-Systemen (der Vergangenheit) und autonomen Systemen mit offensiven Fähigkeiten (der Zukunft) ist, wenngleich griffig und nicht selten in der Literatur anzutreffen (Sauer 2016, S. 8-9), aufgrund der Entwicklung von Autonomie an verschiedenen Stationen des breiten Funktionsspektrums moderner Waffensysteme nicht tragfähig (Dickow et al. 2015).

Vor dem Hintergrund der Definitionsproblematik ist es sinnvoll, zwei Vorschläge aufzugreifen. *Erstens* scheint es geboten, fortan von *Autonomie in Waffensystemen* (das praktische Akronym AWS kann beibehalten werden) statt von *autonomen Waffensystemen* zu sprechen (Boulanin 2016). Damit wird dem Missverständnis vorgebeugt, Autonomie sei als Eigenschaft gebunden an die Hardware des Waffensystems, das sie behaust. Das mag im Fall der oben genannten autonomen Testdrohnen X-47B, Taranis und nEUROn so sein, muss aber nicht immer gelten. Autonomie kann auch über ein *systems of systems*, also etwa einen Verbund verschiedener Waffensysteme oder einen Schwarm aus gleichartigen Systemen, verteilt und somit nicht an ein spezifisches, eindeutig identifizierbares Stück Hardware gebunden sein. *Zweitens* erscheint es sinnvoll, dem Vorschlag des Internationalen Komitees des Roten Kreuzes (ICRC 2016a) zu folgen und Autonomie in Waffensystemen insbesondere hinsichtlich der sogenannten *kritischen Funktionen*, dem selbständigen Auswählen und Bekämpfen von Zielen, in den Blick zu nehmen. Auch zahlreiche Exemplare der oben angeführten Verteidigungssysteme sind dazu grundsätzlich befähigt und wären nach dieser Definition *autonom*, was abermals die Schwierigkeit des Ziehens klarer Trennlinien unterstreicht. Die falsche Schlussfolgerung daraus wäre, den etablierten und wenig umstrittenen Verteidigungssystemen nun urplötzlich ein Autonomieproblem zu attestieren. Richtig ist stattdessen, mit Blick auf Autonomie in Waffensystemen zu fragen, *wann* menschliche Kontrolle *in welchem Umfang* im Rahmen

[10] Siehe mit Blick darauf die Entwicklung verschiedener Waffentypen bei Roff (2016); siehe des Weiteren Slijper (2017) für einen hilfreichen Überblick über jene Waffensysteme und Prototypen, die in der AWS-Diskussion derzeit eine Rolle spielen.

[11] Hierbei handelt es sich um Waffen, die zunächst ohne Ziel gestartet werden, um dann innerhalb eines definierten Einsatzgebietes, in dem sie sich über längere Zeit aufhalten, Ziele entweder zugewiesen zu bekommen oder sich diese anhand vorher festgelegter Merkmale selbstständig zu suchen.

welcher Funktionen eines Systems (aus Systemen) reduziert oder gänzlich verdrängt wird und was jeweils die Konsequenzen daraus sind. Die Frage nach Autonomie in Waffensystemen zielt also nicht auf eine spezifische *neue Waffenkategorie*. Sie zielt vielmehr auf bestimmte militärische Praktiken bei der *Anwendung* autonomiefähiger Waffensysteme. Dabei wirft, kurz gesagt, die Praxis der autonomen Abwehr von Mörsergranaten eben weniger völkerrechtliche, ethische und sicherheitspolitische Fragen auf als die eines zukünftig womöglich autonom geführten Gefechts gegen Panzer, Flugzeuge und Infanterie (Sauer 2018b).

Entscheidend ist in diesem Zusammenhang weiterhin, dass der Schlüssel zum Umgang mit kritischen Funktionen in modernen Waffensystemen nicht in der Hardware, sondern in der Software zu suchen ist. Man denke an die vielen Software-Updates, die das Patriot Luftabwehrsystem, das in den 1960er Jahren entwickelt wurde, bis heute einsatzfähig halten (Defense Science Board 2012, S. 10). Auch beim Third Offset ist folglich zuhauf die Rede von der Implementierung neuer Software, wenn es um AWS geht. Die Software Control Architecture for Robotic Agent Command and Sensing wurde etwa dafür entwickelt, existierende bewaffnete Schnellboote in einem autonom operierenden Schwarm zusammenzuführen, der Schiffsverbände schützen und Angreifer abwehren kann (Smalley 2014). Das Beispiel unterstreicht *erstens*, dass die Frage, was autonome Waffensysteme sind, tatsächlich weniger zielführend ist als die Frage, mit wie viel Autonomie beliebige (auch bereits existierende) Systeme – bis hin zu den kritischen Funktionen des *Wirkmitteleinsatzes* – militärisch genutzt werden können. Es verdeutlicht *zweitens*, dass die Entwicklung von autonomen Waffensystemen – besser: von Autonomie bis hin zu den kritischen Funktionen in Waffensystemen – in dem hier beschriebenen Sinne bereits ein gutes Stück vorangeschritten und somit keine *Zukunftsdiskussion* mehr ist.

Besonders virulent ist die AWS-Definitionsfrage mit Blick auf eine eventuelle völkerrechtliche Regelung (durch die CCW) und potenzielle Rüstungskontrollinstrumente. Denn man muss wissen, was genau verregelt oder gar verboten werden soll, bevor man zur Tat schreiten kann. In der Schlussbetrachtung wird diese Frage noch einmal aufgegriffen; für das hier im Zentrum stehende Nachdenken über sicherheitspolitische Implikationen ist ein fortgesetztes Erörtern der Definitionsproblematik hingegen nicht nötig.[12] Im Folgenden werden zunächst weitere, eng mit Autonomie in Waffensystemen zusammenhängende Trends vorgestellt. Anschließend werden die sicherheitspolitischen Chancen und Risiken dieses Bündels an Entwicklungen analysiert.

Neben dem auf Autonomie fußenden Trend zu *swarming* (Hurst 2017; Dickow 2015, S. 13), der im US-Drohnenbereich mit der Erprobung der Systeme Perdix (Air Force) und Locust (Navy) verspricht, den Gegner mit einem überwältigenden Angriff zu konfrontieren, gegen den er sich nur äußerst schwer verteidigen kann, zeichnen sich des Weiteren lernende und adaptivere Systeme sowie solche ab, die so klein sind, dass sie selbst urbane Operationen unbemerkt durchführen können

[12] Für eine ebenso aktuelle wie wohldurchdachte Aufbereitung der AWS-Definitionsfrage aus ethischer und völkerrechtlicher Sicht siehe Amoroso und Tamburrini (2017).

(Altmann und Sauer 2017, S 123, 128; Schörnig 2013, S. 19-20; Defense Science Board 2016, S. 61).

All diesen Entwicklungen gemeinsam ist, dass der Grad an menschlicher Kontrolle weiter zurückgehen wird, ja muss, wenn AWS Verbreitung finden und das dadurch gesteigerte Operationstempo für menschlichen Input keine Zeit mehr lässt (Scharre 2016a; Altmann und Sauer 2016, 2017). Kurz, Autonomie in Waffensystemen erzwingt – auf Kosten menschlicher Kontrolle – mehr Autonomie, wenn nur noch AWS innerhalb des gegnerischen Entscheidungszyklus des F2T2EA handeln können (DoD 2012, S. 53, 58). Warum genau der Verlust dieser *meaningful human control*, wie es im UN-Duktus heißt (Moyes 2016; Human Rights Watch 2016), mit AWS einhergeht und wie sich dies sicherheitspolitisch auswirkt, wird im folgenden Kapitel beleuchtet.

4 AWS: Sicherheitspolitische Chancen und Vorteile

Autonomie in Waffensystem birgt aus Sicht der US-Sicherheitspolitik zahlreiche Vorteile. Ganz allgemein sollen autonome Waffensysteme Aufgaben übernehmen, die für Menschen zu eintönig, zu unangenehm oder zu gefährlich sind, was nicht zuletzt Kostensenkungspotenziale verspricht (Dickow 2015, S. 10, 12; Gubrud 2013). Im Konkreten sind darüber hinaus drei weitere Vorteile zu nennen.

Erstens macht Autonomie Steuerungs- und Kommunikationsverbindungen optional. Solche sind störungs- und kaperungsanfällig und geben mitunter den Aufenthaltsort von Systemen preis. Auch liegt zwischen menschlichen Fernsteuerbefehlen und ihrer Ausführung stets eine Zeitverzögerung. Auf diese Verbindungen nicht angewiesene AWS versprechen demgegenüber zahlreiche Vorteile. Sie könnten, um weiter beim Beispiel der Drohnen zu bleiben, im umkämpften Luftraum besser bestehen (Franke 2013, S. 35-36), da sie anders als ferngesteuerte Systeme den Luftkampf latenzfrei selbst führen könnten (Sayler 2015, S. 27; Altmann und Sauer 2017, S. 123) – mit G-Kräften, die menschliche Pilot*innen im Cockpit körperlich überfordern würden (Carafano 2014, S. 3). Autonomie in Waffensystemen könnte des Weiteren in Operationsgebieten, wo Kommunikation schwierig, unmöglich oder ungewünscht ist, neue Handlungsoptionen eröffnen: etwa in der Tiefsee (Dickow 2015, S. 16; Sauer 2016, S. 9; Sharkey 2010, S. 377; UNIDIR 2015, S. 2; Brixey-Williams 2016), in den Weiten des Westpazifik (Dickow 2015, S. 14) sowie dank *Stealth*-Eigenschaften in feindlichem Gebiet. Darüber hinaus erleichtert Autonomie potentiell die Durchführung unbemerkt bleibender grenzüberschreitender Operationen im Krieg gegen den Terror (Altmann und Sauer 2017, S. 130-131; Petermann und Grünwald 2011, S. 209, 225; Sayler 2015, S. 32).

Zweitens sind AWS vor allem auch als Kräftemultiplikator attraktiv: Ein Soldat soll in Zukunft viele autonome Systeme oder Schwärme führen (Schörnig 2014, S. 28; Sharkey 2010, S. 378), was zudem die Abschreckungswirkung erhöhen soll, die die Hightech-Streitkräfte der USA gegenüber anderen Staaten entfalten (Borrie 2016).

Drittens soll das Zusammenspiel von Echtzeitaufklärung, Entscheidungsgeschwindigkeit vor Ort und präzisem Waffeneinsatz ohne Zeitverzögerung helfen,

die Zahl ziviler Opfer zu reduzieren und Schäden an ziviler Infrastruktur vorzubeugen. Gegen Angst, Stress und Überreaktion immune autonome Systeme lassen AWS-Befürworter*innen auf eine Kriegsführung hoffen, die womöglich den Vorgaben der Diskriminierung und Proportionalität des humanitären Kriegsvölkerrechts besser gerecht würde. AWS könnten dank fehlendem Selbsterhaltungstrieb im Extremfall mit dem Zurückschießen länger warten; weniger Kriegsleid könnte, so die Hoffnung, die Folge sein (Arkin 2010).

Aus Sicht des in Kapitel 2 skizzierten *American way of war* erscheint Autonomie in Waffensystemen in Summe also ein sicherheitspolitisch attraktives Versprechen. AWS ermöglichen laut ihren Befürworter*innen einen unblutigen, günstigen Krieg im Verborgenen mit geringeren politischen und militärischen Risiken. Sie eröffnen demnach neue Möglichkeiten, gegnerisches konventionelles Militär zu besiegen und potentielle neue Herausforderer abzuschrecken. Das US Defense Science Board bewertet in seinen Studien Entwicklung und Einsatz von AWS entsprechend optimistisch.[13] Zugleich spiegelt jedoch das zentrale *Policy*-Dokument der US-Sicherheitspolitik auch Vorsicht und Zweifel wider.

4.1 Vorsichtsmaßnahmen: Department of Defense Directive 3000.09 *Autonomy in Weapon Systems*

Die Direktive 3000.09 *Autonomy in Weapon Systems* des US-Verteidigungsministeriums hat zum Ziel, das militärische Potenzial von Autonomie möglichst auszuschöpfen und dabei ungewünschte Nebeneffekte zu vermeiden (DoD 2012, S. 1). Im Wesentlichen soll das durch die Bewahrung von „appropriate levels of human judgment“ (DoD 2012, S. 2) erreicht werden: Tötungsentscheidungen dürfen nach dieser Direktive – auf den ersten Blick – nicht durch einen Algorithmus allein getroffen werden, wenn etwa die Kommunikation zum menschlichen Bediener abbricht. Darüber hinaus sollen Handel und Proliferation von autonomen Waffensystemen beschränkt werden (DoD 2012, S. 2-3).

Die US-Autonomiedirektive war die erste ihrer Art und die erste, in der sich die Absicht zur Wahrung der menschlichen Kontrolle über kritische Waffensystemfunktionen widerspiegelt (Human Rights Watch 2013). Eine genaue Lektüre offenbart allerdings, dass die in ihr angemahnte Maxime der „appropriate levels of human judgment over the use of force“, die „informed and appropriate decisions in engaging targets“ (DoD 2012, S. 2) sicherstellen soll, durchaus bedeuten kann, dass in bestimmten Situationen *keine* menschliche Kontrolle für angemessen deklariert werden kann (Gubrud 2013, 2014, S. 5-6). Inzwischen wird daher in gezielter Abgrenzung dazu die Forderung nach der oben erwähnten robusteren und weniger leicht entsagbaren *meaningful human control* über Waffensysteme erhoben.[14]

[13] In der Studie von 2012 wird noch vor der Anfälligkeit gegen Cyberangriffe und vor Proliferation gewarnt, in der *Summer Study* von 2016 dagegen beschäftigt sich nur ein Kapitel mit den Cybersicherheitsaspekten; die Risiken werden im Fazit dann nicht mehr erwähnt (Defense Science Board 2012, S. 14, 73-75, 2016, S. 27-29, 98-102).

[14] Einen kritischen Überblick über die verschiedenen in der Diskussion anzutreffenden Konzepte bietet Ekelhof (2019).

Zudem formuliert die Direktive eine Ausnahmeregel, die eine Entwicklung und Nutzung von Autonomie in Waffensystemen außerhalb der von ihr gesetzten Beschränkungen sehr wohl erlaubt:

> [S]ystems intended to be used in a manner that falls outside the policies [...] must be approved by the Under Secretary of Defense for Policy (USD(P)); the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)); and the CJCS [Chief of the Joint Chiefs of Staff]. (DoD 2012, S. 3)

Die Direktive fungiert somit kaum als Autonomiemoratorium. Vielmehr gibt sie, *erstens* der US-Rüstungsindustrie einen rechtlichen Rahmen für die Entwicklung von AWS. *Zweitens* gibt sie – in Verbindung mit Studien im Auftrag des US-Verteidigungsministeriums, die bezeugen, dass angemessene menschliche Kontrolle prinzipiell möglich sei – den politischen Startschuss für die AWS-Rüstung (Altmann 2013, S 55). Insofern repräsentiert die mit dem menschlichen Entscheidungs- und Kontrollverlust hadernde Direktive die Ambivalenz einer US-Sicherheitspolitik, die die Chancen der Autonomie zwar maximal auszunutzen plant, dabei jedoch die nichtintendierten Effekte und Risiken von Waffenautonomie bereits antizipiert hat.

4.2 Der *human-on-the-loop*: Die Illusion menschlicher Kontrolle

Stellt man die Chancen und Vorteile, die AWS versprechen, der in Direktive 3000.09 formulierten Maxime der Bewahrung menschlicher Kontrolle gegenüber, so wird ein Widerspruch erkennbar. Wie oben bereits angedeutet, zieht, wenn die Entscheidungsgeschwindigkeit von Menschen hinter die von Maschinen zurückfällt, Autonomie mehr Autonomie nach sich, weil Geschwindigkeit, definiert als die Fähigkeit zum Handeln innerhalb des gegnerischen Entscheidungszyklus, entscheidende Vorteile verspricht (Clark 2016; Defense Science Board 2016, S. 4; Freedberg 2015; Gubrud 2014, S. 33).

So bleibt der abgehängten menschlichen Kognition bestenfalls eine Aufsichtsfunktion *(human-on-the-loop)*. Damit wächst das Risiko, dass der menschliche Bediener nicht mehr rechtzeitig eingreifen kann, wenn Fehler geschehen oder nicht intendierte und ungewünschte Handlungen zu unterbinden wären (Scharre 2016a, S. 8). Mit immer weiter ansteigender Systemgeschwindigkeit wird also aus dem Menschen *on-the-loop* ein Mensch *out-of-the-loop* (Human Rights Council 2013, S. 8). Dies wird auch am Beispiel des kniffligen *handover* bei Fahrassistenzsystemen deutlich:

> The speed of interactions matters significantly, however. Giving the human operator the ability to grab the wheel of an autonomous vehicle traveling at highway speeds in dense traffic, particularly if the operator is not paying attention, is merely the illusion of control. (Scharre 2016a, S. 11).

Dies gilt nicht zuletzt deshalb, weil Menschen nicht multitaskingfähig sind und vermeintlich parallel ausgeführte Operationsprozesse realiter im Hirn sequentiell (und zwar mit verminderter Kapazität) ablaufen (Schörnig 2014, S. 28; Singer 2009, S. 126). Somit lässt sich festhalten, dass eine *angemessene* oder *bedeutsa-*

me menschliche Kontrolle über kritische Funktionen in Waffensystemen aufgrund mangelnder Zeit- und Informationsressourcen unmöglich wird, sobald die Vorteile der Autonomie voll ausgeschöpft werden sollen (Article36 2014; Moyes 2016).

Ließe sich die menschliche Kontrolle aber womöglich bereits zuvor im Entscheidungszyklus des F2T2EA nachhaltig verankern? Diese Idee firmiert unter dem Begriff des *wider loop*, in dem der Mensch, wenn schon, wie oben erläutert, aus dem *narrow loop* der Zielauswahl und -bekämpfung ausgeschlossen, die Kontrolle behält (AIV und CAVV 2015; Ekelhof 2019). Doch bisher ist weder plausibel demonstriert, wie damit menschliche Kontrolle im Entscheidungszyklus weiter bis zur Autonomie bei *target selection* und *engagement durchgereicht* würde, noch trägt das Konzept angemessen der Tatsache Rechnung, dass sich auch auf Ebene des *finding* und *fixing* aufgrund des vermehrten Zusammenspiels von Menschen mit computergestützten Führungsunterstützungssystemen die Qualität menschlicher Kontrolle im militärischen Entscheidungszyklus ebenfalls verändert. Nicht nur mit Blick auf maschinell assistierte oder gänzlich an Maschinen delegierte Entscheidungsfindung, sondern schon mit steigendem Grad der Echtzeitaufbereitung von Informationen nimmt schließlich der Gesamtanteil menschlicher Urteilskraft ab (Schörnig 2014, S. 33). Als Beispiel sei hier ein Algorithmus genannt, der im Videofeed einer Drohne Bewegung relativ zum Boden erkennt und das Erkannte als Person oder Fahrzeug klassifiziert (wie etwa in der Google-Pentagon-Kooperation Maven, die Google aufgrund von Protesten allerdings nicht weiterführt). Um Missverständnisse zu vermeiden: Diese Entwicklung *muss* nicht zwingend ein Problem darstellen, aber sie beherbergt die Gefahr des schleichenden Kontrollverlusts; sie anzuerkennen macht die Idee unplausibel, ausgerechnet hier eine Art archimedischen Punkt für bedeutsame menschliche Kontrolle zu suchen.

Womöglich könnte man menschliche Kontrolle noch früher zu verankern versuchen, etwa im Entwicklungs- und Produktionsvorgang autonomer Waffensysteme. Doch spätestens mit der Einführung von lernenden Systemen würde auch dieser Einfluss schwinden. Darüber hinaus werden moderne KI-Agenten/Roboter schon heute von anderen KI-Agenten/Robotern in komplexen Simulationen getestet und eventuell in Zukunft auch entwickelt (Gubrud 2014, S. 34).[15]

Wenn die von der US-Sicherheitspolitik erwarteten Vorteile von AWS auch tatsächlich genutzt werden sollen, ist es vor dem Hintergrund der hier angestellten Überlegungen unabdingbar, dass der Mensch aus dem *targeting cycle*, insbesondere den taktisch entscheidenden kritischen Funktionen, ausgeschlossen wird. Der *human-on-the-loop* ist realiter nicht mit den erhofften Einsatzmöglichkeiten von AWS vereinbar. Auch der ehemalige US-Vize-Verteidigungsminister Robert Work kam so zu dem Schluss, dass in der Binnenlogik der Waffenautonomie das vollständige Abtreten menschlicher Kontrolle bis hin zum Wirkmitteleinsatz letztendlich unausweichlich sein wird (Mehta 2016). Was wären nun die damit einhergehenden sicherheitspolitischen Risiken?

[15] Siehe in diesem Zusammenhang auch die Unterscheidung zwischen „control by design“ und „control in use“ in den Berichten des International Panel on the Regulation of Autonomous Weapons (https://www.ipraw.org/focus-on-reports/).

5 AWS: Sicherheitspolitische Risiken

Im Folgenden werden zunächst mit AWS einhergehende Risiken der Proliferation und neuer Vulnerabilität sowie daraufhin Eskalations- und Instabilitätsrisiken näher untersucht.

5.1 Proliferation und Vulnerabilität

Um antizipativ eine Vorstellung von der Proliferation im Bereich AWS zu erhalten, bietet sich zunächst der Blick auf die gegenwärtige Drohnentechnologie an: Die Verve, mit der die USA in den letzten Jahren Drohnen zur Aufklärung und Bekämpfung von Zielen eingesetzt haben, beschleunigte deren Ausbreitung, wobei insbesondere China in diese Technologie investiert und sie auch exportiert (Defense Science Board 2012, S. 69-71). Der Datensammlung der New America Foundation (2018) zufolge nutzen inzwischen 28 Staaten bewaffnete Drohnen, des Weiteren mehrere nicht staatliche Akteure wie Hamas, Hisbollah, die Huthi-Rebellen und der sogenannte Islamische Staat.

Drohnentechnologie ist proliferationsanfällig, weil sie einen ausgeprägten *Dual Use*-Charakter hat. Da Autonomie in Waffensystemen auf beliebig vervielfältigbarer und per Cyberangriff besonders diebstahlanfälliger Software beruht (Freedberg 2015; Mahnken 2008, S. 123), wird sie sich insbesondere in diesem mit Hardware reich bestückten Sektor rasch verbreiten. Denn auch Autonomie ist ein *Dual Use*-Produkt – sie wird schließlich auch in zahllosen Unternehmen und Universitäten des zivilen Sektors entwickelt (vgl. Kapitel 2); in erheblichem Umfang außerhalb der USA, was die *Third Offset*-Hoffnung, als „fast leader" (Work et al. 2018) einen Vorsprung bei Autonomie in Waffensystemen zu etablieren und zu halten, negiert (Defense Science Board 2016, S. 45).

Neue Verwundbarkeiten ergeben sich aus US-Perspektive also durch die Weiterverbreitung von dieser in besonderem Maße diffusionsanfälligen Hard- und Software. Nicht nur das allgemeine Selbstverständnis als führende Technologienation wird damit in Frage gestellt. Es drohen auch konkrete neue Risiken aus dem Luftraum, wenngleich nicht die für den risikoarmen *American way of war* essentielle Lufthoheit insgesamt wegfallen wird. Zukünftig wieder ernsthaften Bedrohungen von oben ausgesetzt zu sein, stellt einen Paradigmenwechsel für die am Boden kämpfenden US-Truppen dar, die sich nach Ende des Kalten Krieges bisher stets auf die Deckung durch Luftstreitkräfte hatten verlassen können (Sayler 2015, S. 29). Dementsprechend bauen US-Armee und -Marinekorps ihre Luftabwehrkapazitäten aktuell (wieder) aus, dabei auch auf Laser und Mikrowellen setzend. Der Grund: konventionelle Abwehrlösungen, etwa mit Stinger-Raketen, sind für die Abwehr von Schwärmen billiger Wegwerfdrohnen nicht nur wenig geeignet, sie stehen auch in keinem akzeptablen Kostenverhältnis. Ob die neuen Abwehrsysteme ausreichend schnell Wirkung im Ziel entfalten können, um damit große Zahlen angreifender Systeme zu bekämpfen, ist aber noch fraglich (Roblin 2018). Die in Zukunft erwartbare

Kombination aus billigen unbemannten Systemen, Autonomie und Schwarmverhalten erzeugt also greifbare Risiken für die US-Streitkräfte.[16]

Die besondere Täuschanfälligkeit autonomer Systeme ergibt ein weiteres Bündel an Verwundbarkeiten. Zwar ist der Wegfall von Kommunikationsverbindungen – und damit Angriffsvektoren – einer der Anreize für mehr Autonomie in Waffensystemen, doch die Kehrseite dessen sind Angriffsszenarien wie etwa das Einspielen falscher Navigationsinformationen durch *spoofing* von GPS-Daten, für die ferngesteuerte Systeme dank menschlicher Kontrolle nicht in gleicher Weise anfällig sind. Dem Iran gelang es auf diese Weise nach aktuellem Kenntnisstand bereits im Jahr 2011, eine autonom navigierende US-Drohne zu entführen (Dickow 2015, S. 11; Freedberg 2012a).

Auf *deep neural networks* beruhende Mustererkennungssysteme, die derzeit den Stand der Technik im Bereich maschineller Bilderkennung darstellen, sind darüber hinaus in besonderem Maße manipulationsanfällig.[17] Was in der Domäne des geregelten und nicht von feindlich gesinnten Akteuren bevölkerten Straßenverkehrs ein am Ende bewältigbares Problem beim Betrieb selbstfahrender Autos darstellen mag, erzeugt in Form von AWS auf dem Schlachtfeld größere Unwäg- und Verwundbarkeiten (Klincewicz 2015; Schörnig 2013, S. 21; Nguyen et al. 2015). Die derzeit an der Schnittstelle zwischen maschinellem Lernen und Computersicherheit unter dem Schlagwort *adversarial examples* (Evtimov et al. 2017) betriebene Forschung legt nämlich nahe, dass maschinelle Bilderkennung Gegnern insofern neue Angriffsflächen bietet, als dass diese der Maschine verlässlich falsche Tatsachen vorgaukeln (wodurch etwa Schildkröten als Gewehr klassifiziert werden, vgl. Athalye et al. 2017) oder sie sogar, im Falle von im Feld lernenden Systemen, durch wiederholtes Täuschen gezielt „umtrainieren" können (Defense Science Board 2016, S. 28; Kozyulin 2016; Scharre 2016a, S. 14).

Mit steigender Komplexität der Waffensysteme steigt des Weiteren die Anzahl an Software-Bugs. Diese Programmierfehler können kritische Auswirkungen haben, bis hin zu Verlusten durch Eigenbeschuss (Scharre 2016a, S. 21). Die Theorie der *normal accidents* (Perrow 1984) legt nahe, dass Fehler grundsätzlich unvermeidlich sind. Sogar in Bereichen mit extrem hohen Vorsichts- und Sicherheitsstandards wie Atomkraftwerken oder der bemannten Raumfahrt treten sie auf (Borrie 2016; Scharre 2016a). Die Softwareindustrie kann die Zahl der Bugs maximal auf 0,1 bis 0,5 Fehler pro 1000 Zeilen Code reduzieren, was bedeutet, dass komplexe Systeme mit mehreren Millionen Zeilen Code, wie heute etwa der F-35 Kampfjet, tausende unentdeckte Softwarefehler beherbergen (Scharre 2016a, S. 13). Zudem müssen auch unbemannte Systeme Updates unterzogen werden (UNIDIR 2015, S. 8). Hier liegt die Quelle für neue Bugs, wenn ein Update beispielsweise unter Zeitdruck entworfen wird oder sich aus der Interaktion mit alter Software neue Fehler ergeben.

[16] Die Nutzung von simplen, kommerziellen und im Eigenbau bewaffneten Drohnen durch den sogenannten Islamischen Staat (Waters 2017) sowie der bisher nicht gänzlich geklärte Angriff durch 13 (wohlgemerkt ebenfalls ferngesteuerte und nicht schwärmende) Drohnen auf einen russischen Stützpunkt in Syrien (MacFarquhar 2018) stützen die These solch neuer (und natürlich nicht ausschließlich auf US-Seite entstehender) Verwundbarkeiten.

[17] Für eine kritische Bestandsaufnahme im Bereich *deep learning* insgesamt siehe Marcus (2018).

Verkompliziert wird dieser gesamte Sachverhalt weiter, wenn neben konventionell programmierter Software auch maschinelles Lernen in Waffensystemen zum Einsatz kommt. Denn auf maschinellem Lernen beruhende Systeme erzeugen Software-*Black Boxes*, die aufgrund ihrer Intransparenz nicht wie herkömmliche Software *debugged*, also gezielt von Fehlern befreit werden können (Marcus 2018, S. 10-11).

Zu guter Letzt evozieren AWS eine neue Qualität der Fehleranfälligkeit, was die (bzw. den übrig bleibenden Rest an) Interaktion mit menschlichen Kommandeur*innen betrifft. Denn hier kommen kognitive Defizite wie etwa *automation bias* ins Spiel, also das unkritische, unbegründete Vertrauen in die Funktion des Systems.[18] Autonome Systeme können also unbemerkt fehlerhaft operieren (Scharre 2016a, S. 31; Schörnig 2014, S. 28; Sharkey und Suchman 2013, S. 16-17). Ein Mensch, der Fehler macht, kann diese nach ihrem Erkennen verstehen und korrigieren; er vertraut sich selbst in der Regel nicht blind, im Gegensatz zu AWS, die er vermeintlich überwacht, deren Entscheidungen er jedoch nicht in Echtzeit kritisch reflektieren kann (Defense Science Board 2012, S. 15). Unmittelbar daran schließen Eskalationsrisiken an.

5.2 Eskalation und Instabilität

Die für Autonomie in Waffensystemen vorgesehenen Techniken – insbesondere maschinelles Lernen – bringen Besonderheiten mit sich, die, wie im vorherigen Kapitel bereits erwähnt, neue Verwundbarkeiten erzeugen. Mit ihnen geht zugleich eine neue Form der Unberechenbarkeit einher, die sich aus der Interaktion zwischen AWS und ihrer Umwelt ergibt, was wiederum neue Eskalationsrisiken nach sich zieht (Haider und Catarrasi 2016, S. 10; ICRC 2016b, S. 3).

Insbesondere die Interaktion zweier oder mehrerer autonomer Systeme ist dabei zu betrachten. Im mit Computern betriebenen Hochfrequenzhandel an der Börse *(high frequency trading)* (Shorter und Miller 2014) treten häufig unvorhergesehene Interaktionsprozesse zwischen zwei oder mehr autonom operierenden Handelsalgorithmen auf, was nicht selten sogar kurz andauernde, starke Kurseinbrüche *(flash crashes)* und somit finanziellen Schaden verursacht. Dem kann an den Finanzmärkten regulativ begegnet werden; ohne eine kriegsvölkerrechtlich verbindliche und verifizierte Regulierung von AWS auf dem Schlachtfeld bedeutet dies aber, dass mit der Konfrontation generischer AWS zukünftig nicht intendierte Wechselwirkungen drohen, bis hin zu ungewolltem Waffengebrauch (Dickow 2015, S. 19; Altmann und Sauer 2017, S. 129). Ein *flash war* würde so womöglich durch autonome Angriffe und Gegenangriffe eskalieren, bevor ein Mensch korrigierend eingreifen kann (Scharre 2016a, S. 53, 2016b). „Thus a key element of risk in autonomous systems is the time between when a system begins failing [...] and when the human operator can undertake corrective action“ (Scharre 2016a, S. 10).

Trotz seiner kognitiven Defizite, wie dem bereits diskutierten *automation bias*, sprechen mit Blick auf das Risiko der Eskalation Heterogenität und Diversität für den Menschen, da sie Resistenz gegen Massenfehler erzeugen. Der *langsamere* Mensch ist daher der bessere Krisenmanager; seine Kontrolle ist zwar bisweilen Fehler-

[18] Für das Beispiel Patriot siehe Hawley (2017).

quelle, im Zweifel aber aufgrund seiner Kapazitäten zum Verständnis von Kontext doch überlegener *Fail-Safe*-Mechanismus und somit einer in Krisen unkontrollierbar davongaloppierenden Waffensystemautonomie vorzuziehen (Altmann und Sauer 2016, 2017; Scharre 2016a, S. 23). Auch hier lässt sich aus der Geschichte lernen. Denn eindrücklich belegt hat diesen Zusammenhang das Handeln des kürzlich verstorbenen sowjetischen Oberstleutnant Stanislaw Petrow im Jahre 1983. Als das laut Diagnose fehlerfrei arbeitende sowjetische Frühwarnsystem eine Sonnenreflexion auf einer Wolke als Blitz startender US-Interkontinentalraketen interpretierte und einen atomaren Erstschlag meldete, bewertete Petrow dies als Fehlalarm und verhinderte so eine Kettenreaktion, die im nuklearen Schlagabtausch hätte enden können. Der gesunde Menschenverstand verhinderte die nukleare Eskalation (Gubrud 2014, S. 39; Sietz 2008).

Nicht nur auf nuklearer Ebene, aber dort mit potenziell besonders gravierenden Konsequenzen, befördert Autonomie in Waffensystemen auch Instabilitätsrisiken (Geist und Lohn 2018). Unter dem Stichwort *entanglement* (Acton et al. 2017) werden so inzwischen Effekte diskutiert, die aus den zunehmenden Kapazitäten konventioneller Waffensysteme – darunter Autonomie – für die strategische Ebene erwachsen, etwa „non-nuclear threats to nuclear weapons and their associated command, control, communication, and information (C3I) systems“ (Acton et al. 2017, S. 1). Konkret bringt Autonomie so etwa im Bereich der Seekriegsführung neue Möglichkeiten zur U-Boot-Bekämpfung mit sich. Mit der inzwischen bei der US Navy im Test befindlichen Sea Hunter wurde etwa im Rahmen des DARPA Anti-Submarine Warfare Continuous Trail Unmanned Vessel (ACTUV) Programms ein autonomer Trimaran entwickelt. Seine Fähigkeit, getauchte U-Boote (mit ballistischen Raketen) zu detektieren und zu verfolgen, schränkt die gesicherte nukleare Zweitschlagfähigkeit anderer Nuklearstaaten ein. Sea Hunter ist dabei nur ein Aspekt in der Diskussion um die durch Autonomie *transparenter* werdenden Ozeane und der Auswirkungen dieser Entwicklung auf die nukleare Stabilität insgesamt (Brixey-Williams 2016; Dickow 2015, S. 15).[19]

Verschärft wird das *Entanglement*-Problem durch die zunehmende Bereitschaft, nicht nukleare Angriffe – wozu neben den Waffen selbst, wie oben gesehen, auch Frühwarn- und Kontrollsysteme gezählt werden (Acton 2018) – nuklear zu vergelten. Signifikante, nicht nukleare strategische Angriffe, wie es in der *Nuclear Posture Review* der Trump-Administration heißt (DoD 2018, S. 21), sollen durch die USA neuerdings auch nuklear beantwortet werden können. Diese Haltung fand sich auf russischer Seite aufgrund des konventionellen rüstungstechnologischen Vorsprungs der USA schon länger; nun spiegeln die USA sie ihrerseits zurück, was der Stabilität zwischen den beiden größten Nuklearmächten weiter abträglich sein dürfte.

[19] Aus Sicht der US-Sicherheitspolitik wäre mit dem *transparent ocean* nur ein Bein der nuklearen Triade einem neuen Risiko ausgesetzt. Im Falle anderer Nuklearwaffenstaaten – etwa Großbritannien oder Frankreich – wäre die gesamte Zweitschlagfähigkeit in Frage gestellt.

6 Schlussbetrachtung: Rüstungskontrolle statt Autonomiewettlauf?

Aus Sicht der US-Sicherheitspolitik gibt es auf den ersten Blick zahlreiche Gründe, die für die möglichst weitreichende Nutzung von Autonomie in Waffensystemen sprechen. AWS versprechen konkrete Chancen auf Überlegenheit gegenüber herkömmlichen unbemannten und bemannten Systemen im Gefecht sowie das Multiplizieren der eigenen militärischen Stärke. Sie fügen sich insgesamt nahtlos in die Tradition ein, Sicherheit durch fortschrittliche Rüstungstechnologien zu erzeugen.

Autonomie in Waffensystemen ist nicht per se neu, wie etwa die Existenz bestimmter SARMO-Systeme zur Verteidigung nahelegt. Eine darüber hinaus reichende *Autonomisierung* im Arsenal der US-Streitkräfte würde allerdings, wie auf den zweiten Blick leicht erkennbar ist, neue Risiken mit sich bringen. Mit bestimmten doktrinären Vorsichtsmaßnahmen wird in den USA vor diesem Hintergrund versucht, die Vorteile von Autonomie in Waffensystemen auszuschöpfen und zugleich die Risiken einzudämmen, insbesondere den drohenden Verlust menschlicher Kontrolle über die kritischen Funktionen von Waffensystemen.

Diese in sich widersprüchliche Strategie des *have your autonomy-cake and eat it too* ist zum Scheitern verurteilt, so zumindest der hier präsentierte Argumentationsgang. Darüber hinaus ist das mit der Third Offset Strategy angestrebte Ziel der USA, *fast leader* im Bereich AWS zu werden und zu bleiben, angesichts der besonderen Proliferationsanfälligkeit von AWS unrealistisch. Ein weit verbreiteter Einsatz von Autonomie in Waffensystemen würde vielmehr auf Seiten der US-Streitkräfte neue Verwundbarkeiten erzeugen sowie auf internationaler Ebene Risiken der Eskalation und Instabilität nach sich ziehen, die strategische Ebene eingeschlossen. Den Sicherheitsnachteil hätten somit auch die momentan noch technologisch führenden USA.

Im Anschluss an diese Abwägung von Chancen und Risiken ist allerdings fraglich, ob es in Reaktion gelingt, die Binnenlogik des Autonomiewettlaufs zu überwinden. Rüstungskontrollmaßnahmen, etwa mittels eines CCW-Protokolls, könnten den Risiken durch AWS vorbeugen und auf diese Weise mehr Sicherheit für alle Mitglieder der Staatengemeinschaft erzeugen. Dies wäre einer unregulierten Rüstungsdynamik mit dem Endergebnis erhöhter allgemeiner Unsicherheit allemal vorzuziehen. Die damit verbundenen rüstungskontrollpolitischen Herausforderungen sind jedoch groß, nicht zuletzt, weil Autonomie in Waffensystemen eine militärisch ungleich bedeutendere Entwicklung darstellt als der vergleichsweise begrenzte aber häufig zitierte Fall der Blendlaser, die mittels eines CCW-Protokolls erfolgreich präventiv völkerrechtlich bindend verboten wurden.

Meinungsumfragen (in den USA und weltweit) deuten zwar auf die Ablehnung von Autonomie in Waffensystemen durch die Mehrheit der Bevölkerung hin (Carpenter 2013; ORi 2015)[20] und die *scientific communities* in den Feldern der KI und Robotik, unterstützt von den Nichtregierungsorganisation der Campaign to Stop Kil-

[20] Für eine kritische Betrachtung siehe Horowitz (2016).

ler Robots, stehen AWS öffentlichkeitswirksam kritisch gegenüber.[21] Doch bei den UN in Genf zeigen die technologisch führenden Staaten trotz des zivilgesellschaftlichen Drucks an Regulierung bisher kein Interesse.

Ein über unverbindliche politische Absichtserklärungen hinausreichendes Ergebnis wird sich daher nur dann erreichen lassen, wenn ein international gewichtiger Spieler sich die Forderung der zivilgesellschaftlichen Akteure zu eigen macht. Ein solcher *champion state* (Garcia 2015) könnte entweder dem CCW-Prozess neue Dynamik verleihen oder diesen außerhalb des CCW-Rahmens zu einem Abschluss bringen. Österreich fordert (als bisher einziges europäisches Land) umgehend und lautstark ein völkerrechtlich verbindliches Verbot von AWS. Ob es aber die Rolle des *champion state* annimmt, ist bisher noch offen.

Darüber hinaus müsste der Knoten im Definitionsstrang der Debatte – sprich: *was* soll *wie* reguliert werden? – gelöst werden, da dieser inzwischen zu einer Behinderung des gesamten Prozesses geworden ist. Ein vielversprechender Vorschlag dazu liegt mit dem Konzept der „levels of human supervisory control" (Amoroso et al. 2018, S. 14) vor, mit dem, den Automatisierungsgraden 0 bis 5 im Automobilbereich nicht unähnlich, Mensch-Maschine-Beziehungen systematisch unterschieden und waffensystemspezifisch (etwa mit Ausnahmen für SARMO-Systeme) verregelt werden könnten. Zu guter Letzt bedarf die Frage der Verifikation, um den Einhalt eines eventuellen völkerrechtlich bindenden Regulierungsinstruments überprüfen zu können, einer Antwort, denn (vermeintliche) Verifikationshindernisse können erfahrungsgemäß den politischen Willen in Rüstungskontrollprozessen schwinden lassen (siehe z. B. die scheiternde Ratifikation des Umfassenden Teststoppvertrags in den USA). *Shared ledger technology* (gemeinhin als Blockchain bezeichnet) wird im Bereich der nuklearen multilateralen Rüstungskontrolle inzwischen als neues Verifikationshilfsmittel erforscht (Frazar et al. 2018), und auch die Verifikationsproblematik im Bereich Autonomie wäre mittels solch innovativer Ansätze womöglich in den Griff zu bekommen (Gubrud und Altmann 2013; Altmann und Sauer 2017, S. 132-136). Angesichts der Liste an Herausforderungen bleibt aber abschließend festzuhalten, dass die multilaterale Rüstungskontrolle (ganz gleich ob im Rahmen der UN oder außerhalb), die Geschwindigkeit deutlich erhöhen muss, wenn sie auf den Autonomiewettlauf überhaupt noch einwirken will.

Literatur

Acton, J. (2018). Command and control in the Nuclear Posture Review: Right problem, wrong solution. War on the Rocks. https://warontherocks.com/2018/02/command-and-control-in-the-nuclear-posture-review-right-problem-wrong-solution/. Zugegriffen: 05. Feb. 2018.

Acton, J. M., Arbatov, A., Dvorkin, V., Topychkanov, P., Li, B., & Tong, Z. (2017). Entanglement. Chinese and Russian perspectives on non-nuclear weapons and nuclear risks. Carnegie Endowment for International Peace. http://carnegieendowment.org/files/Entanglement_interior_FNL.pdf. Zugegriffen: 05. Feb. 2018.

[21] Ein besonders öffentlichkeitswirksamer Ausdruck der Bemühungen, von wissenschaftlicher Seite weiter Druck auf die Staatengemeinschaft auszuüben, ist das federführend vom prominenten KI-Forscher Stuart Russell produzierte und im Rahmen der CCW-GGE-Sitzung im November 2017 in Genf präsentierte Video *Slaughterbots* (auf YouTube verfügbar).

AIV – Advisory Council on International Affairs, & CAVV – Advisory Committee on Issues of Public International Law. (2015). Autonomous weapon systems. The need for meaningful human control. https://aiv-advies.nl/download/606cb3b1-a800-4f8a-936f-af61ac991dd0.pdf. Zugegriffen: 05. Feb. 2018.

Altmann, J. (2013). Bewaffnete unbemannte Fahrzeuge – Beschränkungen dringend nötig. In Heinrich-Böll-Stiftung (Hrsg.), High-Tech-Kriege. Frieden und Sicherheit in den Zeiten von Drohnen, Kampfrobotern und digitaler Kriegsführung (Demokratie, Bd. 36) (S. 53–65). https://www.boell.de/sites/default/files/endf_high-tech-kriege.pdf?dimension1=division_asp. Zugegriffen: 23. Juli 2019.

Altmann, J., & Sauer, F. (2016). Speed kills: Why we need to hit the brakes on 'killer robots'. Duck of Minerva. http://duckofminerva.com/2016/04/speed-kills-why-we-need-to-hit-the-brakes-on-killer-robots.html. Zugegriffen: 14. Jan. 2017.

Altmann, J., & Sauer, F. (2017). Autonomous weapon systems and strategic stability. *Survival*, *59*(5), 117–142.

Amoroso, D., & Tamburrini, G. (2017). The ethical and legal case against autonomy in weapons systems. Global Jurist. https://doi.org/10.1515/gj-2017-0012. Zugegriffen: 13. Aug. 2019.

Amoroso, D., Sauer, F., Sharkey, N., Suchman, L., & Tamburrini, G. (2018). Autonomy in weapon systems: The military application of artificial intelligence as a litmus test for Germany's new foreign and security policy. Heinrich-Böll-Stiftung. https://www.boell.de/sites/default/files/boell_autonomy-in-weapon-systems_1.pdf?dimension1=division_oen. Zugegriffen: 19. Juli 2019.

Arkin, R. C. (2010). The case for ethical autonomy in unmanned systems. *Journal of Military Ethics*, *9*(4), 332–341.

Article36. (2014). Key areas for debate on autonomous weapons systems. Article36 Briefing Paper. http://www.article36.org/wp-content/uploads/2014/05/A36-CCW-May-2014.pdf. Zugegriffen: 19. Juli 2019.

Athalye, A., Engstrom, L., Ilyas, A., & Kwok, K. (2017). Synthesizing robust adverserial examples. https://arxiv.org/pdf/1707.07397.pdf. Zugegriffen: 05. Juli 2018.

Bitzinger, R. A. (2016). Why China should fear the US military's Third Offset Strategy. The National Interest. http://nationalinterest.org/blog/the-buzz/why-china-should-fear-the-us-militarys-third-offset-strategy-17505?page=show. Zugegriffen: 11. Nov. 2016.

Borrie, J. (2016). Security, unintentional risk, and system accidents. United Nations Institute for Disarmament Research. http://www.unog.ch/80256EDD006B8954/(httpAssets)/6FFBF5CB7ECC2403C1257F9B00525F91/$file/2016_LAWS+MX_presentations_security_borrienotes.pdf. Zugegriffen: 14. Jan. 2017.

Boulanin, V. (2016). Mapping the development of autonomy in weapon systems. A primer on autonomy. Stockholm International Peace Research Institute. https://www.sipri.org/sites/default/files/Mapping-development-autonomy-in-weapon-systems.pdf. Zugegriffen: 19. Juli 2019.

Brixey-Williams, S. (2016). Will the Atlantic become transparent? British Pugwash. https://www.basicint.org/wp-content/uploads/2018/06/Pugwash_Transparent_Oceans_update_nov2016_v3b_April2018-1.pdf. Zugegriffen: 19. Juli 2019.

Bundesregierung. (2013). Deutschlands Zukunft gestalten. Koalitionsvertrag zwischen CDU, CSU und SPD. 18. Legislaturperiode. https://www.cdu.de/sites/default/files/media/dokumente/koalitionsvertrag.pdf. Zugegriffen: 13. Aug. 2019.

Bundesregierung. (2018). Ein neuer Aufbruch für Europa. Eine neue Dynamik für Deutschland. Ein neuer Zusammenhalt für unser Land. Koalitionsvertrag zwischen CDU, CSU und SPD. 19. Legislaturperiode. https://www.bundesregierung.de/resource/blob/656734/847984/5b8bc23590d4cb2892b31c987ad672b7/2018-03-14-koalitionsvertrag-data.pdf?download=1. Zugegriffen: 13. Aug. 2019.

Carafano, J. J. (2014). Autonomous military technology: Opportunities and challenges for policy and law. The Heritage Foundation. https://www.heritage.org/defense/report/autonomous-military-technology-opportunities-and-challenges-policy-and-law. Zugegriffen: 23. Juli 2019.

Carpenter, C. (2013). Beware the killer robots. Inside the debate over autonomous weapons. Foreign Affairs. https://www.foreignaffairs.com/articles/united-states/2013-07-03/beware-killer-robots. Zugegriffen: 24. Juli 2013.

Clark, C. (2016). Pentagon study urges 'immediate action' on thinking weapons; VCJCS Selva cautious. Breaking Defense. http://breakingdefense.com/2016/08/pentagon-study-urges-immediate-action-on-thinking-weapons-vcjcs-selva-cautious/. Zugegriffen: 14. Nov. 2016.

Cordesman, A. H. (2000). The lessons and non-lessons of the air and missile campaign in Kosovo. Center for Strategic & International Studies. https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/kosovolessons-full.pdf. Zugegriffen: 19. Juli 2019.

Defense Science Board. (2012). The role of autonomy in DoD systems. Task Force Report. U.S. Department of Defense. https://fas.org/irp/agency/dod/dsb/autonomy.pdf. Zugegriffen: 19. Juli 2019.
Defense Science Board. (2016). Summer study on autonomy. U.S. Department of Defense. https://www.hsdl.org/?view&did=794641. Zugegriffen: 22. Juli 2019.
Dickow, M. (2015). Robotik – ein Game-Changer für Militär und Sicherheitspolitik? SWP-Studie. Stiftung Wissenschaft und Politik. https://www.swp-berlin.org/fileadmin/contents/products/studien/2015_S14_dkw.pdf. Zugegriffen: 22. Juli 2019.
Dickow, M., Dahlmann, A., Alwardt, C., Sauer, F., & Schörnig, N. (2015). First steps towards a Multidimensional Autonomy Risk Assessment (MARA) in weapons systems. FG Sicherheitspolitik Working Paper, 5. Stiftung Wissenschaft und Politik. https://www.swp-berlin.org/fileadmin/contents/products/arbeitspapiere/FG03_WP05_2015_MARA.pdf. Zugegriffen: 22. Juli 2019.
DoD – U.S. Department of Defense. (2012). Directive 3000.09. Autonomy in weapon systems. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/300009p.pdf. Zugegriffen: 22. Juli 2019.
DoD. (2018). Nuclear posture review 2018. https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-NUCLEAR-POSTURE-REVIEW-FINAL-REPORT.PDF. Zugegriffen: 05. Feb. 2018.
Eaglen, M. (2016a). A sneak preview of President Obama's last defense budget. Part I, winners. American Enterprise Institute. https://www.aei.org/publication/a-sneak-preview-of-president-obamas-last-defense-budget-part-i-winners/. Zugegriffen: 14. Nov. 2016.
Eaglen, M. (2016b). What is the Third Offset Strategy? American Enterprise Institute. https://www.aei.org/publication/what-is-the-third-offset-strategy/. Zugegriffen: 14. Nov. 2016.
Eaglen, M., & Birkey, D.A. (2012). Nearing coffin corner: US air power on the edge. National Security Outlook, 1. American Enterprise Institute. http://www.aei.org/wp-content/uploads/2012/03/-national-security-outlook-march-2012_133237930128.pdf. Zugegriffen: 14. Nov. 2016.
Ekelhof, M. (2019). Moving beyond semantics on autonomous weapons: Meaningful human control in operation. Global Policy. https://doi.org/10.1111/1758-5899.12665. Zugegriffen: 13. Aug. 2019.
Evtimov, I., Eykholt, K., Fernandes, E., Kohno, T., Li, B., Prakash, A., Rahmati, A., & Song, D. (2017). Robust physical-world attacks on deep learning models. https://arxiv.org/pdf/1707.08945.pdf. Zugegriffen: 22. Juli 2019.
FLI – Future of Life Institute. (2015). Autonomous weapons: An open letter from AI & robotics researchers. https://futureoflife.org/open-letter-autonomous-weapons/. Zugegriffen: 12. Sep. 2019
FLI. (2017). An open letter to the United Nations Convention on Certain Conventional Weapons. https://futureoflife.org/autonomous-weapons-open-letter-2017/. Zugegriffen: 25. Sep. 2017.
Franke, U.E. (2013). Verbreitung von unbemannten Flugzeugen für den militärischen Gebrauch. *Aus Politik und Zeitgeschichte*, *63*(37), 33–38.
Frazar, S.L., Jarman, K.D., Joslyn, C.A., Kreyling, S.J., Sayre, A.M., Schanfein, M.J., West, C.L., & Winters, S.T. (2018). Exploratory study on potential safeguards applications for shared ledger technology. Pacific Northwest National Laboratory. https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-26229.pdf. Zugegriffen: 15. Jan. 2018.
Freedberg, S.J. (2012a, 10. Aug.). Drones need secure datalinks to survive vs. Iran, China. Breaking Defense. http://breakingdefense.com/2012/08/drones-need-secure-datalinks-to-survive-vs-iran-china/. Zugegriffen: 11. Nov. 2016.
Freedberg, S.J. (2012b, 21. Dez.). The end of advantage: Enemies may catch up with US technology – or surpass it. Breaking Defense. http://breakingdefense.com/2012/12/the-end-of-advantage-enemies-may-catch-up-with-us-technology/. Zugegriffen: 14. Nov. 2016.
Freedberg, S.J. (2015). Robot wars: Centaurs, skynet, & swarms. Breaking Defense. http://breakingdefense.com/2015/12/robot-wars-centaurs-skynet-swarms/. Zugegriffen: 14. Nov. 2016.
Freedberg, S.J. (2016). The next war? Trench warfare with smart bombs. Breaking Defense. http://breakingdefense.com/2016/10/the-next-war-trench-warfare-with-smart-bombs/. Zugegriffen: 14. Nov. 2016.
Garcia, D. (2015). Humanitarian security regimes. *International Affairs*, *91*(1), 55–75.
Geis, A., Müller, H., & Schörnig, N. (2010). Liberale Demokratien und Krieg. Warum manche kämpfen und andere nicht. Ergebnisse einer vergleichenden Inhaltsanalyse von Parlamentsdebatten. *Zeitschrift für Internationale Beziehungen*, *17*(2), 171–201.
Geis, A., Müller, H., & Schörnig, N. (Hrsg.). (2013). *The militant face of democracy. Liberal forces for good*. Cambridge: Cambridge University Press.
Geist, E., & Lohn, A.J. (2018). How artificial intelligence could increase the risk of nuclear war. RAND Corporation. https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE296/RAND_PE296.pdf. Zugegriffen: 26. Apr. 2018.

Gubrud, M. (2013). US killer robot policy: Full speed ahead. Bulletin of the Atomic Scientists. http://thebulletin.org/us-killer-robot-policy-full-speed-ahead. Zugegriffen: 14. Nov. 2016.
Gubrud, M. (2014). Stopping killer robots. *Bulletin of the Atomic Scientists*, *70*(1), 32–42.
Gubrud, M., & Altmann, J. (2013). Compliance measures for an autonomous weapons convention. ICRAC Working Paper, 2. International Committee for Robot Arms Control (ICRAC). https://www.icrac.net/wp-content/uploads/2018/04/Gubrud-Altmann_Compliance-Measures-AWC_ICRAC-WP2.pdf. Zugegriffen: 14. Aug. 2019.
Hagel, C. (2014). Reagan National Defense Forum keynote. U.S. Department of Defense. http://www.defense.gov/DesktopModules/ArticleCS/Print.aspx?PortalId=1&ModuleId=2575&Article=606635. Zugegriffen: 11. Nov. 2016.
Haider, A., & Catarrasi, M. B. (2016). Future unmanned system technologies. Legal and ethical implications of increasing automation. Joint Air Power Competence Center. https://www.japcc.org/wp-content/uploads/Future_Unmanned_System_Technologies_Web.pdf. Zugegriffen: 22. Juli 2019.
Hammes, T. X. (2018). America is well within range of a big surprise, so why can't it see? War on the Rocks. https://warontherocks.com/2018/03/america-is-well-within-range-of-a-big-surprise-so-why-cant-it-see/. Zugegriffen: 12. Juni 2018.
Hawley, J. K. (2017). Patriot wars. Automation and the Patriot air and missile defense system. Center for a New American Security. https://www.cnas.org/publications/reports/patriot-wars. Zugegriffen: 22. Juli 2019.
Horowitz, M. C. (2016). Public opinion and the politics of the killer robots debate. *Research and Politics*, *3*(1), 1–8.
Human Rights Council. (2013). Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions, Christof Heyns. A/HRC/23/47. https://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A-HRC-23-47_en.pdf. Zugegriffen: 22. Juli 2019.
Human Rights Watch. (2013). USA: Verbot vollständig autonomer Waffen. US-Richtlinie zu autonomen Waffensystemen ist die erste in der Welt. https://www.hrw.org/de/news/2013/04/16/usa-verbot-vollstandig-autonomer-waffen. Zugegriffen: 14. Nov. 2016.
Human Rights Watch. (2016). Killer robots and the concept of meaningful human control. Memorandum to Convention on Conventional Weapons (CCW) delegates. https://www.hrw.org/news/2016/04/11/killer-robots-and-concept-meaningful-human-control. Zugegriffen: 13. Jan. 2017.
Hurst, J. (2017). Robotic swarms in offensive maneuver. *Joint Forces Quarterly*, *87*(4), 105–111.
ICRC – International Committee of the Red Cross. (2016a). Autonomous weapon systems: Implications of increasing autonomy in the critical functions of weapons. https://www.icrc.org/en/publication/4283-autonomous-weapons-systems. Zugegriffen: 22. Juli 2019.
ICRC. (2016b). Views of the International Committee of the Red Cross (ICRC) on autonomous weapon systems. https://www.icrc.org/en/download/file/21606/ccw-autonomous-weapons-icrc-april-2016.pdf. Zugegriffen: 12. Jan. 2017.
iPRAW – International Panel on the Regulation of Autonomous Weapons. (2017). Computational methods in the context of LAWS. "Focus on" Report, 2. https://www.ipraw.org/wp-content/uploads/2017/11/2017-11-10_iPRAW_Focus-On-Report-2.pdf. Zugegriffen: 24. Jan. 2018.
Kaag, J., & Kreps, S. (2014). *Drone warfare*. Cambridge: Polity.
Kaplan, F. (2016). The Pentagon's innovation experiment. MIT Technology Review. https://www.technologyreview.com/s/603084/the-pentagons-innovation-experiment/. Zugegriffen: 24. Jan. 2018.
Klincewicz, M. (2015). Autonomous weapons systems, the frame problem and computer security. *Journal of Military Ethics*, *14*(2), 162–176.
Kozyulin, V. (2016). International and regional threats posed by the LAWS: Russian perspective. PIR Center for Policy Studies. http://www.unog.ch/80256EDD006B8954/(httpAssets)/77058244E836364EC1257F9A0049F24A/$file/2016_LAWS+MX+Presentations_SecurityIssues_Vadim+Kozyulin.pdf. Zugegriffen: 11. Nov. 2016.
MacFarquhar, N. (2018). Russia says its Syria bases beat back an attack by 13 drones. The New York Times. https://www.nytimes.com/2018/01/08/world/middleeast/syria-russia-drones.html. Zugegriffen: 24. Jan. 2018.
Mahnken, T. G. (2008). *Technology and the American way of war since 1945*. New York: Columbia University Press.
Marcus, G. (2018). Deep learning: A critical appraisal. https://arxiv.org/ftp/arxiv/papers/1801/1801.00631.pdf. Zugegriffen: 05. Feb. 2018.
Mehta, A. (2016). Work: Autonomy in flight likely before ground. Defense News. http://www.defensenews.com/story/defense/land/army/2016/03/30/bob-work-autonomy-flight-ground-systems-robot-ai/82427024/. Zugegriffen: 11. Nov. 2016.

Mehta, A. (2018). Selva: FY19 budget sees 'increasing' investments in AI, machine teaming. Defense News. https://www.defensenews.com/congress/budget/2018/01/30/selva-fy19-budget-sees-increasing-investments-in-ai-machine-teaming/. Zugegriffen: 31. Jan. 2018.
Moyes, R. (2016). Key elements of meaningful human control. Articel36 Background Paper. http://www.article36.org/wp-content/uploads/2016/04/MHC-2016-FINAL.pdf. Zugegriffen: 26. Sep. 2017.
Müller, H. (2004). The antinomy of democratic peace. *International Politics*, *41*(4), 494–520.
Münkler, H. (2015). *Kriegssplitter. Die Evolution der Gewalt im 20. und 21. Jahrhundert*. Berlin: Rowohlt.
New America Foundation. (2018). World of drones. https://www.newamerica.org/in-depth/world-of-drones/. Zugegriffen: 24. Jan. 2018.
Nguyen, A., Yosinski, J., & Clune, J. (2015). Deep neural networks are easily fooled: High confidence predictions for unrecognizable images. Proceedings of the 2015 IEEE Conference on Computer Vision and Pattern Recognition. https://ieeexplore.ieee.org/document/7298640. Zugegriffen: 22. Juli 2019.
ORi – Open Roboethics initiative. (2015). The ethics and governance of lethal autonomous weapons systems: An international public opinion poll. http://www.openroboethics.org/wp-content/uploads/2015/11/ORi_LAWS2015.pdf. Zugegriffen: 11. Dez. 2015.
Overhaus, M. (2015). Die Verteidigungspolitik der USA. Grundlegende Trends und ihre Auswirkungen auf das transatlantische Verhältnis. SWP-Studie. Stiftung Wissenschaft und Politik. https://www.swp-berlin.org/fileadmin/contents/products/studien/2015_S11_ovs.pdf. Zugegriffen: 22. Juli 2019.
Perrow, C. (1984). *Normal accidents. Living with high-risk technologies*. Princeton (NJ): Princeton University Press.
Petermann, T., & Grünwald, R. (2011). Stand und Perspektiven der militärischen Nutzung unbemannter Systeme. Arbeitsbericht, 144. Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag. https://www.tab-beim-bundestag.de/de/pdf/publikationen/berichte/TAB-Arbeitsbericht-ab144.pdf. Zugegriffen: 22. Juli 2019.
Roblin, S. (2018). The U.S. Army needs more anti-aircraft weapons – and fast. Ground troops are vulnerable to drones. War is Boring. http://warisboring.com/the-u-s-army-needs-more-anti-aircraft-weapons-and-fast/. Zugegriffen: 24. Jan. 2018.
Roff, H. M. (2016). Weapons autonomy is rocketing. Foreign Policy. http://foreignpolicy.com/2016/09/28/weapons-autonomy-is-rocketing/. Zugegriffen: 12. Sep. 2019.
Sauer, F. (2014). Einstiegsdrohnen. Zur deutschen Diskussion um bewaffnete unbemannte Luftfahrzeuge. *Zeitschrift für Außen- und Sicherheitspolitik*, *7*(3), 343–363.
Sauer, F. (2016). Stopping 'killer robots'. Why now is the time to ban autonomous weapons systems. *Arms Control Today*, *46*(8), 8–13.
Sauer, F. (2018a). *Großmächte und Digitalisierung – welche Folgen für unsere Weltordnung? Metis Studie, 8*. Universität der Bundeswehr München. https://metis.sowi.unibw-muenchen.de/img/publications/08_10-2018_grossmaechte_und_digitalisierung.pdf. Zugegriffen: 01. Apr. 2019.
Sauer, F. (2018b). Künstliche Intelligenz in den Streitkräften: Zum Handlungsbedarf bei Autonomie in Waffensystemen. Arbeitspapier Sicherheitspolitik, 26. Bundesakademie für Sicherheitspolitik. https://www.baks.bund.de/sites/baks010/files/arbeitspapier_sicherheitspolitik_2018_26.pdf. Zugegriffen: 01. Apr. 2019.
Sauer, F., & Schörnig, N. (2012). Killer drones. The 'silver bullet' of democratic warfare? *Security Dialogue*, *43*(4), 363–380.
Sayler, K. (2015). A world of proliferated drones: A technology primer. Center for a New American Security. https://s3.amazonaws.com/files.cnas.org/documents/CNAS-World-of-Drones_052115.pdf?mtime=20160906082154. Zugegriffen: 22. Juli 2019.
Scharre, P. (2016a). Autonomous weapons and operational risk. Ethical Autonomy Project. Center for a New American Security. https://s3.amazonaws.com/files.cnas.org/documents/CNAS_Autonomous-weapons-operational-risk.pdf?mtime=20160906080515. Zugegriffen: 22. Juli 2019.
Scharre, P. (2016b). Flash war. Autonomous weapons and strategic stability. Center for A New American Security. http://www.unidir.ch/files/conferences/pdfs/-en-1-1113.pdf. Zugegriffen: 15. Nov. 2016.
Scharre, P. (2018). *Army of none: Autonomous weapons and the future of war*. New York: W. W. Norton & Company.
Schörnig, N. (2013). Noch Science Fiction, bald Realität? Die technische Leistungsfähigkeit aktueller und zukünftiger Drohnen. *Internationale Politik*, *68*(3), 15–21.
Schörnig, N. (2014). Automatisierte Kriegsführung – Wie viel Entscheidungsraum bleibt dem Menschen? *Aus Politik und Zeitgeschichte*, *64*(35-37), 27–34.
Sharkey, N. (2010). Saying 'No!' to lethal autonomous targeting. *Journal of Military Ethics*, *9*(4), 369–383.
Sharkey, N., & Suchman, L. (2013). Wishful mnemonics and autonomous killing machines. *Proceedings of the AISB*, *136*(5), 14–22.

Shaw, M. (2005). *The new western way of war. Risk-transfer war and its crisis in Iraq*. Cambridge: Polity.
Shorter, G., & Miller, R. S. (2014). High-frequency trading: Background, concerns, and regulatory developments. CRS Report. Congressional Research Service. https://fas.org/sgp/crs/misc/R43608.pdf. Zugegriffen: 29. Sep. 2017.
Sietz, H. (2008). Petrows Entscheidung. Wie ein Oberstleutnant der sowjetischen Armee vor 25 Jahren den Untergang der Welt verhinderte und dafür zum Dank tausend Dollar erhielt. Zeit Online. http://www.zeit.de/2008/39/A-Petrow. Zugegriffen: 15. Jan. 2017.
Singer, P. W. (2009). *Wired for war. The robotics revolution and conflict in the twenty-first century*. New York: Penguin.
Slijper, F. (2017). Where to draw the line. Increasing autonomy in weapon systems – technology and trends. Pax. https://www.paxforpeace.nl/media/files/pax-report-where-to-draw-the-line.pdf. Zugegriffen: 12. Sep. 2019.
Smalley, D. (2014). The future is now. Navy's autonomous swarmboats can overwhelm adversaries. Office of Naval Research. http://www.onr.navy.mil/Media-Center/Press-Releases/2014/autonomous-swarm-boat-unmanned-caracas.aspx. Zugegriffen: 14. Nov. 2016.
UNIDIR – United Nations Institute for Disarmament Research. (2014). Framing discussions on the weaponization of increasingly autonomous technologies. UNIDIR Resources, 1. http://www.unidir.org/files/publications/pdfs/framing-discussions-on-the-weaponization-of-increasingly-autonomous-technologies-en-606.pdf. Zugegriffen: 23. Juli 2019.
UNIDIR. (2015). The weaponization of increasingly autonomous technologies in the maritime environment: Testing the waters. UNIDIR Resources, 4. http://www.unidir.org/files/publications/pdfs/testing-the-waters-en-634.pdf. Zugegriffen: 23. Juli 2019.
Waters, N. (2017). ISIS is building bombs to arm its drone air force. War is Boring. http://warisboring.com/isis-is-building-bombs-to-arm-its-drone-air-force/. Zugegriffen: 24. Jan. 2018.
Work, R. O., & Brimley, S. (2014). 20YY. Preparing for war in the robotic age. Center for a New American Security. https://s3.amazonaws.com/files.cnas.org/documents/CNAS_20YY_WorkBrimley.pdf?mtime=20160906082222. Zugegriffen: 23. Juli 2019.
Work, R. O., Smith, J., & Townsend, J. (2018, 11. Jan.). Robert Work talks NATO's technological innovation and the DoD. Center for a New American Security. https://www.cnas.org/publications/podcast/robert-work-talks-natos-technological-innovation-and-the-dod. Zugegriffen: 04. Feb. 2018.