BÜRO FÜR TECHNIKFOLGEN-ABSCHÄTZUNG
BEIM DEUTSCHEN BUNDESTAG

Reinhard Grünwald
Christoph Kehl

Autonome Waffensysteme

Endbericht zum TA-Projekt

Oktober 2020
Arbeitsbericht Nr. 187

Autonome Waffensysteme

Das Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB) berät den Deutschen Bundestag und seine Ausschüsse in Fragen des wissenschaftlich-technischen Wandels. Das TAB wird seit 1990 vom Institut für Technikfolgenabschätzung und Systemanalyse (ITAS) des Karlsruher Instituts für Technologie (KIT) betrieben. Hierbei kooperiert es seit September 2013 mit dem IZT – Institut für Zukunftsstudien und Technologiebewertung gGmbH sowie der VDI/VDE Innovation + Technik GmbH.

Reinhard Grünwald
Christoph Kehl

Autonome Waffensysteme

Endbericht zum TA-Projekt

TAB-Arbeitsbericht Nr. 187

Büro für Technikfolgen-Abschätzung
beim Deutschen Bundestag
Neue Schönhauser Straße 10
10178 Berlin

Telefon: +49 30 28491-0
E-Mail: buero@tab-beim-bundestag.de
Web: www.tab-beim-bundestag.de

2020

Umschlagbild: Bertrand Bouchez/unsplash.com

Papier: Circle*offset* Premium White
Druck: Wienands Print + Medien GmbH, Bad Honnef

ISSN-Print: 2364-2599
ISSN-Internet: 2364-2602

Inhalt

Zusammenfassung 9

1 Einleitung 29

2 Abgrenzung des Untersuchungsgegenstands 33

2.1 Definitorische Ansätze 34
2.2 Autonom, semiautonom oder automatisiert? 35
2.3 Die Definition des US-Verteidigungsministeriums 39
2.4 Die Qualität menschlicher Kontrolle über AWS 40

3 Technische Grundlagen von Autonomie 45

3.1 Autonomie aus informationstechnologischer Sicht 45
3.2 Autonome Funktionen aktueller militärischer Systeme 46
3.2.1 Autonomie für Mobilität 46
3.2.2 Autonomie für Zielerkennung/Zielbestimmung 47
3.2.3 Autonomie für Informationsgewinnung 48
3.2.4 Autonomie für die Fähigkeit zur Zusammenarbeit 49

3.3 Künstliche Intelligenz als Schlüsseltechnologie 50
3.3.1 Maschinelles Lernen 52
3.3.2 Was können KI-Systeme heute leisten? 53
3.3.3 Begrenzungen, Schwierigkeiten und Risiken bei KI-Systemen 56

4 Verbreitung, Status und Trends unbemannter Waffensysteme 67

4.1 Überblick zu einsatzreifen unbemannten (teil)autonomen Waffensystemen 70
4.1.1 Fliegende Systeme 71
4.1.2 Bodensysteme 76
4.1.3 Systeme zu Wasser 82

4.2 Forschungs- und Entwicklungstrends 85
4.2.1 USA 86
4.2.2 Europa 93
4.2.3 Weitere Schlüsselakteure 99

5 Einsatzszenarien 101

5.1 Argumente für AWS 101
5.2 Erwartete militärische Fähigkeiten 104
5.3 Missionen/Einsatzszenarien 110
5.3.1 Erwartete Missionen 111
5.3.2 Denkbare militärische Einsatzszenarien für AWS 114
5.3.3 Zwischenfazit 119

6 Sicherheitspolitische Implikationen von AWS 125

6.1 Mehr oder weniger Kriege? 126
6.2 Veränderung der Kriegsführung 127
6.3 Destabilisierende Wirkung in Krisen 130
6.4 Auswirkungen auf regionale Stabilität 131
6.5 Auswirkungen auf das strategische Gleichgewicht 132
6.6 Rüstungsdynamiken 133
6.7 Unkontrollierte Weiterverbreitung 133
6.8 Technologische Risiken 134

7 Humanitäres Völkerrecht und autonome Waffensysteme 137

7.1 Prüfungspflicht (Artikel 36 ZP I) 138
7.2 AWS im Lichte der Prinzipien des HVR 139

8 Ethische Fragestellungen im Kontext autonomer Waffensysteme 149

8.1 AWS und die Ethik des Krieges 150
8.1.1 Die Lehre vom gerechten Krieg 151
8.1.2 Ermöglichen AWS eine ethischere Kriegsführung? 153

8.2 AWS und die Würde des Menschen 162
8.2.1 Der Begriff der Menschenwürde 162
8.2.2 Verletzt der Einsatz autonomer Waffensysteme die Menschenwürde? 164

8.3 Die Frage der Verantwortung 168
8.3.1 Rechtliche Sicht 170
8.3.2 Moralische Sicht 173

8.4 Fazit 175

9 Möglichkeiten der Rüstungskontrolle 179

9.1 Rüstungs- und Exportkontrollabkommen mit Relevanz für AWS 179
9.1.1 Rüstungskontrollverträge 180
9.1.2 Transparenz und vertrauens- und sicherheitsbildende Maßnahmen 184
9.1.3 Nichtverbreitung und Exportkontrolle 185

9.2 Die Konvention über bestimmte konventionelle Waffen 189
9.2.1 Menschliche Kontrolle über AWS 191
9.2.2 Positionen wichtiger Staaten bzw. Organisationen 194
9.2.3 Gemeinsamer Vorschlag von Deutschland und Frankreich auf der CCW GGE 207
9.2.4 Ausgangslage für die weitere Diskussion im Rahmen der CCW 209

9.3 Regulierungsansätze der präventiven Rüstungs- und Exportkontrolle 212
9.3.1 Vertrauens- und sicherheitsbildende Maßnahmen 216
9.3.2 Exportkontrolle 218
9.3.3 Verbindliche Regulierung bzw. Verbot von AWS 219

9.4 Handlungsmöglichkeiten 222
9.4.1 Die Möglichkeiten innerhalb der CCW ausschöpfen 223
9.4.2 Engagement über die CCW hinaus verbreitern 224

9.5 Fazit 228

10 Literatur 229

10.1 In Auftrag gegebene Gutachten 229
10.2 Weitere Literatur 229

11 Anhang 261

11.1 Abbildungen 261
11.2 Tabellen 261
11.3 Kästen 261
11.4 Abkürzungen 262

Zusammenfassung

Robotische Waffensysteme, die ohne menschliches Zutun Ziele auswählen und bekämpfen können, waren vor nicht allzu langer Zeit ausschließlich in der Domäne der Science-Fiction beheimatet. Die enormen technologischen Fortschritte, die in den letzten Jahren in den Bereichen der Robotik und der künstlichen Intelligenz (KI) erzielt wurden, haben diese Vorstellung autonom agierender Waffen nun an die Schwelle zur konkreten Umsetzung gerückt.

Automatisierung und Autonomie werden bereits heute für eine breite Palette an Funktionen bei Waffensystemen genutzt. Dazu gehören die Suche und Identifizierung potenzieller Ziele mithilfe von Sensordaten, die Zielverfolgung, Priorisierung und Bestimmung des Zeitpunkts für den Angriff auf diese Ziele sowie die Steuerung für den Zielanflug (z. B. einer Rakete oder eines Marschflugkörpers). Bislang erfolgen jedoch die Zielauswahl, die Angriffsentscheidung und schließlich die Freigabe des Waffeneinsatzes durch einen menschlichen Kommandeur bzw. Operator.

Ein autonomes Waffensystem (AWS) wäre in der Lage, alle diese Schritte selbsttätig und ohne menschliche bzw. mit nur minimaler menschlicher Mitwirkung durchzuführen. Dies hätte zwei entscheidende militärische Vorteile: Zum einen benötigt ein autonomes System keine Kommunikationsverbindung mit einer Basisstation, zum anderen erlaubt es schnellere Reaktionszeiten in Gefechtssituationen, da keine Verzögerungen durch die Laufzeiten einer Datenübertragung und durch die Entscheidungsfindung bzw. die Reaktionszeiten eines menschlichen Operators auftreten. Die Steigerung der Autonomie von Waffensystemen steht daher in allen technologisch fortgeschrittenen Ländern auf der Agenda.

Sehr weit verbreitet ist die Auffassung, dass neue Anwendungen künstlicher Intelligenz im Begriff seien, sämtliche Wirtschafts- und Lebensbereiche grundlegend zu transformieren. In aktuellen verteidigungspolitischen und militärischen Strategiepapieren und Verlautbarungen etlicher Länder wird die Erwartung formuliert, dass diese Transformation auch vor dem Militärsektor nicht Halt machen werde und dass die zügige Einführung von KI-gestützten Waffensystemen einen entscheidenden militärischen Vorsprung verspreche.

Befürworter dieser Entwicklung argumentieren, dass mit AWS unter Umständen auch humanitäre Vorteile verbunden seien, da militärische Operationen präziser durchgeführt und somit die Zivilbevölkerung und zivile Infrastrukturen besser geschützt werden könnten. Kritiker äußern hingegen Bedenken, ob es ethisch vertretbar, politisch verantwortbar und (völker)rechtlich erlaubt sein könne, die Entscheidung über Leben und Tod von Menschen an Maschinen zu delegieren. Auch wären mit der Entwicklung und dem möglichen Einsatz von

AWS sicherheitspolitische Risiken sowie die Gefahr von Rüstungsspiralen und unkontrollierter Verbreitung potenziell riskanter Technologien verbunden.

Mit dem vorliegenden Bericht wird ein breiter Analyseansatz verfolgt und eine Vielzahl von Facetten des Themas abgedeckt: die Darstellung des technologischen Reifegrads und der Entwicklungsperspektiven von AWS, eine Bestandsaufnahme von existierenden und in der Entwicklung befindlichen Systemen sowie eine Analyse möglicher Einsatzszenarien und sich daraus ergebender sicherheitspolitischer Implikationen. Hinzu kommen ethische und völkerrechtliche Fragestellungen, die eng miteinander zusammenhängen. Schließlich werden die aktuell vor allem im Rahmen der »Convention on Certain Conventional Weapons«[1] (CCW) der Vereinten Nationen (United Nations – UN) angesiedelten diplomatischen Bemühungen um eine Einhegung der mit AWS möglicherweise verbundenen Risiken beleuchtet und daraus Überlegungen zu Möglichkeiten der präventiven Rüstungskontrolle abgeleitet.

Definition bzw. Abgrenzung des Untersuchungsgegenstands

Die Frage der Definition von AWS birgt eine erhebliche Brisanz, da sie oftmals in einen direkten Zusammenhang mit möglichen Vereinbarungen zur Rüstungskontrolle gestellt wird. Dabei wird implizit oder explizit angenommen, dass die Definition von AWS gleichzeitig den Rahmen setzt, welche Systeme ggf. zu regulieren oder gar zu verbieten sind. Daher spiegelt die Haltung der Staaten und anderer Akteure in definitorischen Fragen regelmäßig deren Eigeninteressen und Verhandlungspositionen wider.

International werden diverse Ansätze verfolgt, um AWS zu definieren und von anderen Waffensystemen abzugrenzen. Eine präzise, allgemein akzeptierte Definition existiert bis heute nicht. Ob ein Waffensystem autonom, semiautonom oder (hoch)automatisiert agieren kann, hängt nicht nur von seinen technologischen Eigenschaften ab, sondern auch von der Komplexität der Umgebung, in der es eingesetzt werden soll, sowie ganz entscheidend von der Qualität der Interaktion zwischen menschlichem Operator und technischem System. Die Zuordnung von Waffensystemen in die eine oder andere Kategorie ist in vielen Fällen strittig.

Für die hier im Zentrum stehende Analyse militärisch-strategischer, ethischer und völkerrechtlicher sowie sicherheits- und rüstungskontrollpolitischer Fragestellungen ist eine strenge Definition allerdings nicht erforderlich. Daher wurde mit einer deskriptiven Charakterisierung gearbeitet, nach der ein AWS

1 Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects (Übereinkommen über das Verbot oder die Beschränkung des Einsatzes bestimmter konventioneller Waffen, die übermäßige Leiden verursachen oder unterschiedslos wirken können)

Aufträge ohne menschliche bzw. mit lediglich schwacher externer menschlicher Kontrolle selbstständig ausführt und die Fähigkeit besitzt, in einer komplexen, dynamischen Umgebung auf unvorhersehbare Ereignisse zielgerichtet reagieren zu können. Ob ein konkretes System unter eine bestimmte strenge Definition autonomer Waffensysteme fallen würde oder nicht, kann dahingestellt bleiben.

Die CCW: internationale Bemühungen zur Regulierung von AWS

Aufgrund von Bedenken zur ethischen Vertretbarkeit und völkerrechtlichen Zulässigkeit von AWS bemüht sich die internationale Staatengemeinschaft derzeit auf Expertenebene unter dem Dach der CCW, mögliche durch AWS entstehende Risiken zu identifizieren und ggf. einzudämmen.

Eine der Kernfragen ist, welches Mindestmaß an menschlicher Kontrolle über ein Waffensystem gegeben sein muss, damit die völkerrechtlichen Anforderungen eingehalten werden können und die ethische und juristische Verantwortung jederzeit geklärt ist. Oft wird postuliert, dass es dafür ausreicht, wenn ein Mensch den Waffeneinsatz auslöst. Dies wird gerne mit der Formel »Mensch in der Entscheidungsschleife« (»human in the loop«) ausgedrückt. Bei näherem Hinsehen erweist sich dieser Ansatz jedoch als bei Weitem nicht differenziert genug, um Fragen der Handlungsurheberschaft und Verantwortung zu klären, die sich bei der Interaktion von Menschen mit immer intelligenter werdenden Maschinen stellen.

Viele Nichtregierungsorganisationen (NGOs) und eine Reihe von Ländern favorisieren das Konzept »Meaningful Human Control« (MHC; bedeutsame menschliche Kontrolle bzw. Steuerung) in der Bedeutung, dass ein Angriff nur dann statthaft ist, wenn erstens ein menschlicher Bediener bei der Planung und Bewertung eines Angriffs über adäquate Informationen zu dessen Zielsetzung, Auswirkungen und Kontext verfügt, zweitens der Angriff durch eine aktive Handlung eines Menschen initiiert wird und drittens die Menschen, die für die Planung und Durchführung des Angriffs verantwortlich sind, für die Folgen zur Rechenschaft gezogen werden können.

Andere Staaten lehnen das Konzept »Meaningful Human Control« ab. Die USA verweisen darauf, dass in bestimmten Fällen weniger menschliche Beteiligung sogar wünschenswert sei, da durch die Nutzung autonomer Funktionen eine höhere Präzision und Geschwindigkeit als bei menschlicher Kontrolle möglich sei. Daher favorisieren sie »appropriate levels of human judgement« (angemessene Niveaus menschlicher Beurteilung) beim Waffeneinsatz.

Beim zentralen Punkt der Debatten im Rahmen der CCW, ob bzw. auf welche Weise autonome Waffensysteme international reguliert werden sollten, gehen die Positionen der einzelnen Länder weit auseinander. Einige sind der Auffassung, dass eine Dehumanisierung der Kriegsführung durch AWS auf jeden Fall verhindert werden müsse, und fordern daher eine Ächtung und ein wirksames Verbot der Entwicklung, des Erwerbs, der Stationierung und/oder des

Einsatzes solcher Waffen. Andere sind der Ansicht, dass die Anwendung des bestehenden Völkerrechts ausreichende Handhaben biete, um Waffensysteme jeglicher Art – und somit auch AWS – zu regulieren. Daneben gibt es diejenigen, die sich vorstellen können, dass der Einsatz von AWS sogar humanitäre Vorteile bieten könnte, da sie sich im Gegensatz zu Menschen niemals von Emotionen wie Wut oder Rache leiten ließen und damit das Risiko von Kriegsverbrechen gesenkt würde. Schließlich vertreten einige die Position, dass noch nicht genug Wissen bereitstehe, um Fragen der Regulierung von AWS überhaupt anzugehen.

Entwicklungsstand und Trends

Autonome Waffensysteme im strengen Sinne des Wortes, also bewaffnete unbemannte Plattformen, die fähig sind, im Kampfeinsatz in einer komplexen, dynamischen Umgebung ohne jegliche menschliche Kontrolle zielgerichtet zu agieren, gibt es noch nicht. Allerdings sind in verschiedenen Waffengattungen bereits bewaffnete unbemannte Systeme einsatzreif, die über einen relativ weitreichenden Grad an Automatisierung bzw. Autonomie verfügen und deshalb als Vorläufer von AWS klassifiziert werden können. Im vorliegenden Bericht wird anhand bereits genutzter sowie in fortgeschrittenen Stadien der Entwicklung befindlicher unbemannter Waffensysteme – aufgeschlüsselt nach den Einsatzbereichen Luft, Land und Wasser – der aktuelle Stand erreichter Autonomie grob eingeordnet.

Ein Blick auf stationierte und teilweise bereits in Kampfhandlungen eingesetzte unbemannte Waffensysteme (UWS) zeigt, dass in den letzten 10 Jahren die Zahl der staatlichen und nichtstaatlichen Akteure, die damit ausgerüstet sind, stark zugenommen hat. Diese Entwicklung geht fast ausschließlich auf das Konto ferngesteuerter Kampfdrohnen, die mit Abstand zu den am häufigsten produzierten und am weitesten verbreiteten UWS gehören. Zwar wächst auch die Bedeutung von unbemannten Boden- und Wasserfahrzeugen, ihre Einsatzfähigkeiten sind derzeit jedoch noch weitgehend auf andere Zwecke als den Waffeneinsatz begrenzt (Aufklärung, Überwachung, Logistik etc.).

Noch Anfang der 2000er Jahre waren die USA die einzige Nation, die über fortschrittliche MALE-Kampfdrohnen (»medium altitude long endurance«) verfügte. Diese wurden speziell für eine mittlere Flughöhe (ca. 10 bis 15 km) und lange Reichweiten entwickelt (24 bis 48 Stunden Flugdauer); ein erster Kampfeinsatz erfolgte im Oktober 2001 in Afghanistan. In den folgenden Jahren bauten die USA ihr Drohnenprogramm massiv aus und diverse andere Länder begannen mit der Entwicklung bzw. Beschaffung von Kampfdrohnen. Es ist davon auszugehen, dass inzwischen mindestens 30 Staaten über fortschrittliche Kampfdrohnen verfügen, davon haben 10 Länder (einschließlich der USA) diese bereits unter Waffengebrauch in Kampfhandlungen eingesetzt. Deutschland besitzt bis heute noch keine Kampfdrohnen. Als fortschrittlichstes Flug-

gerät (»unmanned aerial vehicle« – UAV) setzt die Bundeswehr seit 2010 die von Israel geleaste, unbewaffnete – allerdings in der aktuellen Version bewaffnungsfähige – Drohne »Heron« der MALE-Kategorie zu Aufklärungszwecken ein.

Entwicklungsstand unbemannter (teil)autonomer Waffensysteme

Dass *Fluggeräte* in der Entwicklung am weitesten fortgeschritten und bei der Verbreitung von UWS vorherrschend sind, hängt wesentlich damit zusammen, dass Navigation, Orientierung und Funkkommunikation in der Luft relativ einfach zu bewerkstelligen sind – deutlich einfacher jedenfalls, als dies an Land bzw. auf oder unter Wasser der Fall ist. Allerdings sind die autonomen Fähigkeiten fliegender unbemannter Systeme insgesamt nach wie vor begrenzt:

- Selbst bei den fortschrittlichen Kampfdrohnen beschränkt sich die Autonomie üblicherweise auf die Flugkontrolle, auf Navigations- und Aufklärungsfunktionen sowie die eventuelle Rückkehr im Falle eines Funkabbruchs; der Waffeneinsatz geschieht in der Regel per Fernsteuerung und unterliegt somit in letzter Instanz immer noch menschlicher Kontrolle. Zu den wenigen Drohnensystemen, die mit relativ weitreichenden autonomen Angriffsfunktionen ausgestattet sind, gehören die israelische Drohne »Harpy«, die bereits in den 1990er Jahren entwickelt wurde, sowie deren Nachfolger »Harop«. Diese dienen primär dem Zweck, feindliche Flugabwehrsysteme auszuschalten. Sie suchen selbsttätig ein definiertes Gebiet nach Radarsignalen ab, lokalisieren deren Quelle und stürzen sich auf das Zielobjekt, um es durch eine Explosion zu zerstören.
- Gängige Lenkwaffen werden üblicherweise durch aktive menschliche Steuerung (z. B. per Laserstrahl) ins Ziel gelenkt, oder sie steuern selbstständig ein vorab definiertes und einprogrammiertes Ziel an. Lenkflugkörper, die bereits über weitreichende autonome Funktionen verfügen, sind beispielsweise die britische »Brimstone« sowie der Antischiffsflugkörper (»long range anti-ship missile« – LRASM), der derzeit von den USA entwickelt wird. Einmal gestartet, können sie im Prinzip völlig eigenständig auf Basis von gespeicherten Signaturen nach Zielen suchen. LRASM soll darüber hinaus die Fähigkeit besitzen, die Angriffsstrategie selbstständig mit anderen Flugkörpern in einer Salve oder einem Schwarm zu koordinieren.

Bei militärischen Robotern, die am Boden operieren, können stationäre und mobile Systeme unterschieden werden. Die verfügbaren *stationären Bodensysteme* dienen vor allem defensiven Zwecken, z. B. für:

- Personenabwehr, wie die robotischen Wachpostenkanonen, die von Israel (entlang des Gazastreifens) sowie möglicherweise von Südkorea (entlang der demilitarisierten Zone) stationiert worden sind und über alle technischen Voraussetzungen für einen vollautomatischen Betrieb verfügen sollen;

- Nahbereichsflugabwehr wie das deutsche System »MANTIS«, das US-amerikanische »Phalanx CIWS« oder das israelische »Iron Dome«. Diese Systeme sind mit weitreichenden automatisierten Funktionen ausgestattet, die sie in die Lage versetzen, auch kleine, schnell bewegliche Ziele mithilfe von Radar zu identifizieren, anhand des Radarquerschnitts zu klassifizieren und schließlich per Maschinenkanone oder Abfangrakete zu bekämpfen – alles nach ihrer Aktivierung prinzipiell ohne menschliches Zutun.

Unbemannte Bodenfahrzeuge (»unmanned ground vehicles« – UGVs) sind grundsätzlich mit deutlich komplexeren Anforderungen konfrontiert als ihre fliegenden Pendants: Sie haben keinen freien Luftraum vor sich, sondern verschiedene Arten von Hindernissen bzw. teils unwegsames, unübersichtliches Gelände. Das erschwert die Navigation, die Umgebungserfassung sowie die Verhaltensplanung und erhöht die mechanischen Herausforderungen bei der Fortbewegung vor allem in unwegsamem Terrain. Aus diesen Gründen sind autonome Funktionen bei UGVs erheblich schwieriger zu realisieren als bei UAVs. Die militärischen UGV-Systeme, die sich bereits im Einsatz befinden, sind in aller Regel nicht bewaffnet, werden aus der Nähe ferngesteuert und haben vor allem unterstützende Funktionen: Sie dienen z. B. Transportzwecken (wie das »Squad Mission Support System« – SMSS für die U.S. Army), der Aufklärung oder der Minenräumung (wie der in großer Stückzahl produzierte Kleinroboter »PackBot«).

Gleichwohl wird intensiv an bewaffneten UGVs gearbeitet, die mit komplexeren autonomen Fähigkeiten ausgestattet sind. Was Navigation und Umgebungserfassung angeht, gibt es naturgemäß große Schnittmengen mit der zivilen Forschung zum autonomen Fahren. Einer der Vorreiter in diesem Bereich ist Israel, das zur Grenzkontrolle mit einer ganzen Reihe teils bewaffneter oder zumindest bewaffnungsfähiger UGVs operiert. Ein Waffeneinsatz kann, zumindest derzeit, nur manuell ausgelöst werden.

Auf und unter Wasser, insbesondere auf hoher See, besteht im Allgemeinen mehr Raum zum Manövrieren als an Land. Außerdem sind die Meere arm an Hindernissen und weitgehend menschenleer, sodass das Risiko von Kollateralschäden gering ist. All dies würde den Unter- sowie Überwasserbereich eigentlich für den Einsatz autonomer Waffensysteme prädestinieren. Dass bislang kaum einsatzfähige seegestützte UWS existieren, hängt u. a. mit den potenziell riesigen Einsatzräumen zusammen, die vor allem mit Blick auf Energieversorgung und Kommunikation (insbesondere unter Wasser) eine große Herausforderung darstellen. Zu den wenigen verfügbaren *unbemannten Überwasserfahrzeugen* (»unmanned surface vehicles« – USVs) gehört das israelische »Silver Marlin«. Es dient vor allem der Überwachung und Aufklärung und soll autonom vorgegebene Koordinaten ansteuern können. Neben einem Radar und verschiedenen elektrooptischen Sensoren ist das Boot mit einem Maschinengewehr ausgestattet, das jedoch rein ferngesteuert ist.

Im Vergleich zu den USVs verfügen *Unterwasserfahrzeuge* (»unmanned underwater vehicles« – UUVs) über eine ungleich höhere militärstrategische Bedeutung. Ihre Verbreitung nimmt weltweit zu, wenngleich die Entwicklung bewaffneter Systeme noch in den Anfängen steckt und die militärischen Aufgaben verfügbarer Systeme sich bisher fast ausschließlich auf Aufklärung, Überwachung und Seeminenräumung konzentrieren. Beispiele sind u. a. der deutsche »Seeotter MKII«, die russische Unterwasserdrohne »Klavesin-2« oder der US-amerikanische »Echo Ranger«, der mittels eines hybriden, wiederaufladbaren Energiesystems mehrere Monate autark operieren können soll. Dennoch ist zu erwarten, dass weiträumig operierenden Unterwassersystemen perspektivisch eine hohe Bedeutung zukommen könnte, sofern sich die Probleme bei der langfristigen Energieversorgung sowie der weitreichenden Kommunikationsverbindung lösen lassen. Gerade die physikalisch bedingten Einschränkungen bei der Kommunikation unter Wasser begründen ein starkes Motiv, einen weitgehend autonomen Betrieb von UUVs zu implementieren.

Forschungs- und Entwicklungstrends

Die USA sind als Vorreiter und Treiber der Entwicklung zunehmend automatisierter Waffensysteme und als wesentlicher Wegbereiter für zukünftige autonome Waffensysteme anzusehen. Daher werden im Bericht Forschungs- und Entwicklungstrends bei AWS besonders am Beispiel der USA aufgezeigt. Ein weiterer Grund hierfür ist, dass Details über Forschungs- und Entwicklungsaktivitäten in den USA dank der vergleichsweise offenen Informationspolitik wesentlich einfacher und umfassender öffentlich zugänglich sind als in anderen Ländern.

Dass der langjährige Trend in den USA deutlich in Richtung AWS geht, spiegelt sich z. B. in den vom U.S. Department of Defense (DOD) regelmäßig publizierten militärischen Entwicklungsstrategien zu unbemannten Systemen wieder. In der aktuellen »Unmanned Systems Integrated Roadmap« von 2017 werden Autonomie und Robotik als Schlüsselfaktoren für die weitere Entwicklung unbemannter Systeme genannt, die das Potenzial hätten, die zukünftige Kriegsführung zu revolutionieren. Bereits heute investieren die USA stattliche Summen in Forschung und Entwicklung (FuE). Geforscht wird sowohl in übergeordneten Forschungsinitiativen wie dem »Science of Autonomy Program« des Office of Naval Research (ONR) als auch in kleineren spezifischen Programmen.

Es ist ein erklärtes Ziel der US-Streitkräfte, unbemannte Systeme in Schwärmen kommunizieren und kooperativ zusammenarbeiten zu lassen. Das Schwarmprinzip basiert auf der taktischen Idee, die gegnerische Abwehr dadurch zu überfordern, dass man ein bestimmtes Ziel gleichzeitig von vielen Seiten und mehrfach angreift. Davon verspricht man sich eine besonders wirkungsvolle und robuste Art der Kampfführung. Daneben ist die Entwicklung von Teams aus Mensch und Maschine (»manned-unmanned teaming« –

MUM-T) ein weiteres zentrales Ziel von U.S. Air Force, U.S. Navy und U.S. Army. So kann z. B. dem Piloten eines Kampfjets ein einzelnes bewaffnetes UAV als loyaler Flügelmann (»loyal wingman«) zur Seite gestellt werden – oder sogar ein kompletter Schwarm, der der Kontrolle des Piloten untersteht. Für die fernere Zukunft setzen die US-Streitkräfte auf unbemannte Fahrzeuge und komplexe Schwarmsysteme, die autonom agieren können, um menschliche Streitkräfte – auch in Gebieten, zu denen der Zugang aufgrund starker Verteidigungskräfte erschwert ist – zu unterstützen. Geplant ist, unbemannte taktische Fahrzeuge zukünftig als »force multiplier« einzusetzen, d. h. in unterstützender Form als Teil interaktiver Mensch-Maschine-Operationen.

Die USA engagieren sich in einer erheblichen Anzahl konkreter Entwicklungs- und Beschaffungsprojekte im Bereich unbemannter (teil)autonomer Systeme. Der klare Schwerpunkt liegt dabei auf autonomen Kampfflugzeugen. So verfolgen die US-Streitkräfte das Vorhaben, eine trägergestützte Kampfdrohne mit Tarnkappeneigenschaften zu entwickeln. Die FuE-Trends im Bereich der US-Rüstungsindustrie und des US-Militärs dienen wiederum als Vorbild für andere wichtige staatliche Akteure, die ebenfalls stark in die Drohnenentwicklung investieren (darunter z. B. China, Israel und Russland, aber auch westeuropäische Staaten). Im vorliegenden Bericht werden die FuE-Trends weiterer Schlüsselakteure überblicksartig betrachtet, insbesondere die Aktivitäten in Deutschland, Frankreich und Großbritannien.

Einsatzszenarien

Eine militärisch-strategisch bedeutsame Fragestellung lautet, für welche Art von Einsatzszenarien sich zukünftige AWS aufgrund ihrer Eigenschaften besonders eignen würden. Zwei Charakteristika kommen hierbei besonders zum Tragen. Zum einen ist dies die physische Abwesenheit eines menschlichen Operators. Dies ermöglicht u. a. kleinere und agilere Plattformen, die in Gebieten operieren können, die für Menschen nicht oder nur schwer zugänglich sind. Zum anderen soll die Fähigkeit, autonom zu operieren, schnellere und effektivere Entscheidungen in zeitkritischen Situationen gestatten. Zudem eröffnet dies neue Optionen zur Koordination in einer Gruppe (bzw. einem Schwarm) von AWS oder aber zur Kooperation zwischen AWS und Menschen (MUM-T). Die sich aus dem Fähigkeitsspektrum zukünftiger AWS perspektivisch ergebenden Einsatzmöglichkeiten werden absehbar die Aufgabenverteilung zwischen Mensch und Maschine neu definieren.

Aufgrund ihrer potenziellen Fähigkeiten und daraus resultierender militärischer Vorteile werden sich AWS insbesondere für Einsatzszenarien eignen, die für Menschen wegen der Umgebungsbedingungen problematisch oder zu gefährlich sind (z. B. Operationen unter Wasser oder auf durch starke Kräfte verteidigtem Terrain), die sehr schnelle Reaktionszeiten oder eine hohe Manövrier-

fähigkeit erfordern (z. B. Luftkampf) oder aber in einem dynamischen Umfeld ohne eine permanente Kommunikationsverbindung stattfinden (z. B. verdeckte Operationen hinter den feindlichen Linien).

Zum gegenwärtigen Zeitpunkt sind jedoch sowohl die technischen Eigenschaften als auch die Verfügbarkeit zukünftiger AWS noch spekulativ, sodass lediglich die Umrisse eines möglichen Portfolios an Einsatzszenarien in groben Zügen erkennbar sind. Dessen konkrete Ausgestaltung hängt von einem komplexen Zusammenspiel mehrerer Faktoren ab. Hierbei spielen nicht nur technologische Entwicklungen eine wesentliche Rolle, sondern auch die Wandlung der Streitkräftestrukturen, die sich im Zuge der sukzessiven Berücksichtigung von Robotik und KI in Doktrinen, Strategien sowie Taktiken, Techniken und Prozeduren abzeichnet, sowie der Konfliktypus, für den Einsatzszenarien entworfen werden.

Ein Bereich, der bisher noch wenig beleuchtet ist, aber absehbar mit einer zunehmenden Verbreitung von AWS erheblich an Bedeutung gewinnen wird, beinhaltet mögliche technologische oder operative Gegenmaßnahmen, die von Antagonisten gegen AWS getroffen werden könnten. Hardware (z. B. Sensoren) und Software von AWS werden ganz eigene Schwachstellen aufweisen, die von entsprechend innovativen Widersachern ausgenutzt werden könnten. Hierzu gehören Möglichkeiten der elektronischen Manipulation (»jamming«, »spoofing«, »hacking«), aber auch eher im Lowtechbereich angesiedelte Maßnahmen könnten ggf. sehr effektiv sein. Beispiele sind der Einsatz von Fangnetzen gegen kleine fliegende AWS, aufblasbare Attrappen oder thermische Quellen, um hitzesuchende Sensoren zu täuschen.

Sicherheitspolitische Implikationen

In fast allen technologisch fortgeschrittenen Ländern wird derzeit die militärische Nutzung von zunehmend autonomen Systemen vorangetrieben, denen ein transformatives Potenzial für die Streitkräfte zugeschrieben wird. Beispielsweise wird Autonomie – gemeinsam mit einer Handvoll weiterer Technologien – in der kürzlich veröffentlichten nationalen Verteidigungsstrategie der USA als Schlüsselfähigkeit angesehen, um »die Kriege der Zukunft zu führen und zu gewinnen«. Es ist daher essenziell, sich mit den sicherheitspolitischen Implikationen zu befassen, welche die Verbreitung und der mögliche Einsatz von AWS mit sich bringen können.

Mehr oder weniger kriegerische Gewalt?

Ob die Verfügbarkeit von AWS dazu führt, dass im Konfliktfall schneller zum Mittel der militärischen Gewalt gegriffen wird oder dass militärische Auseinandersetzungen gewaltsamer geführt werden, sind derzeit kontrovers diskutierte Fragen.

Demokratisch gewählte Regierungen stehen regelmäßig unter erheblichem Rechtfertigungsdruck, wenn eigene Soldaten gefährdet sind bzw. getötet werden können. Wenn der Einsatz von AWS das Risiko für die eigenen Soldaten erheblich verringert (u. a. da AWS Aufgaben übernehmen, die für Menschen gefährlich sind), könnte die Hemmschwelle sinken, Gewalt einzusetzen. Dies wiederum könnte dazu führen, dass die Öffentlichkeit einen Krieg nicht mehr als letzten Ausweg bzw. als einschneidendes Ereignis von nationaler Bedeutung wahrnimmt, sondern diesen als einen unter dem Primat diplomatischer und ökonomischer Abwägungen stehenden Normalfall akzeptiert. Auch unterhalb der Schwelle ausgewachsener Kriege könnten Militäreinsätze zur Durchsetzung politischer Ziele attraktiver und immer mehr zur Regel werden.

Dagegen kann argumentiert werden, dass AWS nichts grundsätzlich Neues bringen, sondern eine ohnehin vonstattengehende Entwicklung lediglich graduell verstärken würden – mit den Drohnenschlägen in Afghanistan, Somalia und anderswo als prominente Beispiele. Darüber hinaus sind Situationen vorstellbar, in denen ein schnellerer und entschlossenerer Einsatz von Gewaltmitteln viel menschliches Leid verhindern könnte, beispielsweise wenn Warlords die Bevölkerung terrorisieren bzw. ethnische Säuberungen durchführen.

Generell verliert das Argument, dass AWS zu einem häufigeren Einsatz von Gewalt führen, erheblich an Kraft, wenn man kein asymmetrisches Szenario – wie etwa gegenwärtig bei den Drohnenschlägen –, sondern eines mit Kontrahenten auf Augenhöhe betrachtet. Hier würde für die Seite, die AWS einsetzt, immer die Gefahr bestehen, dass schmerzhafte Vergeltungsmaßnahmen des Gegners folgen könnten bzw. im ungünstigsten Fall eine Eskalation zu einem ausgewachsenen Krieg mit ungewissem Ausgang eintreten könnte. Insbesondere für die Nuklearwaffenstaaten untereinander würde dieses Eskalationsrisiko stark gegen einen als lokal begrenzt intendierten Einsatz von AWS sprechen.

Auswirkungen auf regionale Stabilität und das strategische Gleichgewicht

Die Verfügbarkeit von AWS könnte sich besonders in Zeiten erhöhter Spannungen bzw. bei Krisen sowohl auf die Stabilität in regionalen Kontexten als auch auf das strategische Gleichgewicht der Nuklearmächte auswirken.

Auf der einen Seite könnten AWS die Stabilität dadurch erhöhen, indem mit ihrer Hilfe (z. B. im Rahmen von Aufklärungsmissionen) mehr Informationen in kürzerer Zeit beschafft und ausgewertet werden könnten und somit eine bessere Grundlage sowie mehr Zeit für menschliche Entscheidungsträger zur Verfügung stünden, alle Konsequenzen einer Eskalation zu durchdenken und die *richtige* Entscheidung zu treffen. Des Weiteren könnten AWS auch als defensive Systeme ausgelegt sein und so einen eskalationswilligen Akteur von einer Aggression abbringen. Eine weitere Möglichkeit, die Abschreckung zu er-

höhen, bestünde darin, dass glaubwürdig im Falle einer möglichen Aggression mit einem autonomen Gegenschlag gedroht würde.

Auf der anderen Seite sind aber auch destabilisierende Wirkungen vorstellbar. So könnten das operative Geschehen und die Entscheidungsprozesse durch AWS derart beschleunigt werden, dass Menschen kognitiv und hinsichtlich ihres Reaktionsvermögens an ihre Grenzen kämen. So könnte in einer Krise eine Eskalationsspirale automatisiert und möglicherweise ungewollt in Gang gesetzt werden. Für ein solches Szenario wurde der Begriff »flash war« geprägt.

Die potenzielle Beschleunigung des Geschehens könnte auch dazu führen, dass Akteure dazu veranlasst werden, präemptiv zuzuschlagen. Außerdem könnte der zuvor skizzierte Versuch, das Abschreckungspotenzial durch autonome Antworten zu erhöhen, auch die Stabilität unterminieren, wenn z. B. bei technischen Fehlfunktionen keine Möglichkeit der menschlichen Intervention mehr bestünde und so ein potenziell katastrophaler Schlag unbeabsichtigt geführt würde.

AWS wären auch dazu prädestiniert, proaktiveres und eventuell provokativeres militärisches Verhalten zu unterstützen, wie z. B. das Eindringen in gegnerisches Territorium, um dort Aufklärung zu betreiben. Ein gegnerischer Staat könnte gleichzeitig eine geringere Hemmung haben, eine solche unbemannte Plattform abzuschießen, woraus wiederum ein unmittelbares neues Eskalationspotenzial erwüchse.

Auf der globalen Ebene spielt das strategische Gleichgewicht zwischen den Nuklearwaffenstaaten nach wie vor eine herausragende Rolle. Es basiert wesentlich auf der gesicherten Fähigkeit eines Zweitschlags und der daraus resultierenden Abschreckung eines möglichen Erstschlags. Es wäre vorstellbar, dass sehr potente AWS zukünftig als konventionelle Erstschlagwaffen zur Zerstörung gegnerischer Nuklearwaffenarsenale eingesetzt werden könnten, die mögliche Ziele (Raketensilos oder mit Nuklearwaffen bestückte U-Boote) selbstständig aufklären, in deren Nähe unentdeckt verweilen und auf Befehl koordiniert diese Ziele angreifen und zerstören. AWS könnten auch als Trägerplattformen für Nuklearwaffen verwendet werden, beispielsweise in Form von autonomen Unterwasserfahrzeugen. Diese könnten schneller, überraschender und koordinierter als bisherige Trägersysteme zuschlagen und vorhandene Verteidigungsmaßnahmen aushebeln. Eine solche Nutzung von AWS würde die strategische Stabilität massiv infrage stellen. Dies wiederum könnte weitere nukleare Abrüstung unmöglich machen und eine Ära nuklearer Modernisierung oder gar nuklearer Aufrüstung einläuten.

Rüstungsdynamiken und unkontrollierte Weiterverbreitung

Wie zuvor ausgeführt, schreiben die Großmächte autonomen Technologien langfristig einen hohen militärischen Stellenwert zu. Technologische Durchbrü-

che einer Seite könnten das bestehende Kräftegleichgewicht fundamental erschüttern. Ein solches Bedrohungsszenario dient oftmals als Legitimation für eigene Anstrengungen auf diesem Feld. Zwischen den USA und China ist bereits heute eine beginnende Rüstungsdynamik bei zunehmend automatisierten UWS zu beobachten. Auch Russland konzentriert sich darauf, im Bereich einsatzreifer UWS den bisherigen Vorsprung des Westens aufzuholen, und scheint auch zukünftig AWS entwickeln zu wollen. Regionale Spannungsherde mit ausgeprägten Rüstungsspiralen bestehen heute u. a. zwischen Indien und Pakistan bzw. Süd- und Nordkorea. Die Beschaffung von AWS könnte hier zusätzliche Rüstungsdynamiken in Gang setzen.

Zukünftige AWS werden auf technologischen Entwicklungen basieren, die ihren Ursprung größtenteils im zivilen Sektor haben. Ein großer Teil der Hardware, vor allem aber deren Software basiert überwiegend auf Dual-Use-Technologien. Die Forschung zur künstlichen Intelligenz – einschließlich maschinellem Lernen, Big-Data-Analysen etc. – wird maßgeblich von kommerziellen Unternehmen mit Blick auf private Konsumenten und den zivilen Wirtschaftssektor vorangetrieben.

Entwicklung und Produktion von leistungsstarken AWS (mit hoher Nutzlast, Reichweite, Zuverlässigkeit etc.) werden trotz verfügbarer Dual-Use-Technologien allerdings erhebliche finanzielle und zeitliche Ressourcen erfordern. Daher könnten Staaten oder andere Akteure versuchen, in den Besitz von kleineren, weniger leistungsfähigen AWS zu gelangen, indem sie fortschrittliche zivile Technologien in bewaffnete AWS überführen, wie dies bei ferngesteuerten Drohnen (ohne autonome Fähigkeiten) bereits heute zu beobachten ist. Ob solche AWS auch für Terroristen attraktiv werden, ist derzeit noch nicht abzusehen, zumal ähnliche Wirkungen auch mit sehr viel einfacheren Mitteln und geringerem Aufwand erreichbar sind, wie Anschläge des IS (Islamischer Staat) in der jüngsten Zeit gezeigt haben.

Bereits heute existiert eine scharfe internationale Konkurrenz um den Export von bewaffneten UAVs, besonders China und Israel sind hier sehr aktiv. Um ihre Wettbewerbsposition zu stärken, haben jüngst auch die USA ihre bisher strengen Exportvorschriften gelockert. Der Wettbewerb um Rüstungsexporte könnte zukünftig in analoger Weise auch die Weiterverbreitung von Systemen mit mehr und mehr autonomen Funktionen beschleunigen.

Völkerrechtliche und ethische Aspekte

Die Entwicklung und der mögliche Einsatz von zunehmend autonom agierenden Waffensystemen schaffen große normative Unsicherheiten, die sich in der Kernfrage zuspitzen, ob und inwiefern es erlaubt sein soll, Maschinen über Tod oder Leben von Menschen entscheiden zu lassen. Diese Fragestellung erscheint nur mit Blick auf die besondere Situation, wie sie im Kriegsfall herrscht,

überhaupt zulässig. Doch selbst in Kriegen gibt es Grenzen des moralisch wie auch völkerrechtlich Erlaubten, die sicherstellen sollen, dass ein gewisses Maß an Menschlichkeit gewahrt bleibt. Obwohl noch nicht abzusehen ist, ob und wann autonome Waffensysteme einsatzfähig sein werden, wird bereits seit einigen Jahren intensiv über ihre normativen Implikationen diskutiert.

AWS im Lichte der Prinzipien des humanitären Völkerrechts

Wie jedes Waffensystem sind auch AWS im Kontext der geltenden Normen des humanitären Völkerrechts (HVR) zu betrachten. Das HVR soll im Falle eines internationalen bewaffneten Konflikts den größtmöglichen Schutz von Zivilisten, nichtmilitärischen Gebäuden und Infrastrukturen sowie der natürlichen Umwelt gewährleisten und intendiert somit, eine Balance zwischen humanitären Erwägungen und militärischen Notwendigkeiten zu schaffen. Das HVR bezieht sich nicht primär auf technologische Systeme als solche, sondern zielt darauf ab, die Art und Umstände ihres Einsatzes einzuschränken.

Zukünftige AWS werden sich gegenüber bisherigen Waffensystemen, inklusive der heutigen unbemannten Waffensysteme, dadurch auszeichnen, dass sie in einem sich dynamisch verändernden, nicht vorhersehbaren Umfeld autonom agieren können, bis zu einem gewissen Grad also selber *Handlungsentscheidungen* treffen müssen, ohne dabei einer direkten menschlichen Steuerung bzw. Kontrolle zu unterliegen. Ob ihr Einsatz völkerrechtlich zulässig sein könnte, muss bereits im Vorfeld, und zwar »bei Prüfung, Entwicklung, Beschaffung oder Einführung« geprüft und festgestellt werden. Hierzu haben sich die Vertragsparteien gemäß Artikel 36 des Zusatzprotokolls I (ZP I) der Genfer Konventionen, die eine wichtige Komponente des HVR sind, verpflichtet. Der Kernbereich des HVR fußt auf drei Prinzipien, die dabei in Betracht zu ziehen sind:

- *Unterscheidungsgebot*: Das HVR gebietet, dass Kampfhandlungen sich nur gegen militärische Ziele – Kombattanten und militärische Objekte – richten dürfen; die Zivilbevölkerung und zivile Objekte sind zu schützen und zu schonen. Darüber hinaus dürfen gegnerische Kräfte nicht angegriffen werden, die außer Gefecht (»hors de combat«) sind. Darunter fallen u. a. Soldaten, die ihre Intention, sich zu ergeben angezeigt haben, und solche, die aufgrund einer Verletzung, Bewusstlosigkeit oder Ähnlichem nicht in der Lage sind, sich zu verteidigen. Ein AWS, das völkerrechtskonform eingesetzt werden soll, müsste also legitime militärische Ziele zuverlässig und mit hoher Trefferquote unter realen Gefechtsbedingungen identifizieren können, auch bei ggf. ungünstigen Lichtverhältnissen (Tag/Nacht), Wetter- und Umweltbedingungen, sich schnell ändernden Gefechtslagen, extremem Zeitdruck sowie trotz möglicher Gegenmaßnahmen des Kontrahenten (einschließlich Tarnen, Täuschen, Blenden von Sensoren). Da auch Menschen

bei dieser komplexen Aufgabe regelmäßig Fehler unterlaufen, wird man in der Praxis sicherlich auch bei AWS keine Unfehlbarkeit bei der Identifikation legitimer Ziele erwarten können. Die eigentliche Problematik ist jedoch anders gelagert, denn für die Entscheidung, ob Objekte oder Personen legitime militärische Ziele darstellen, reicht deren zuverlässige Identifizierung bei Weitem nicht aus. Hierfür sind ein umfassenderes Lagebild erforderlich sowie die Einschätzung von Verhaltensweisen und letzten Endes der Intentionen des Gegners. Aufgrund dessen sind Zweifel angebracht, dass softwarebasierte Systeme wie AWS in absehbarer Zeit in der Lage sein werden, dem Unterscheidungsgebot des HVR Genüge zu leisten.

- *Prinzip der Verhältnismäßigkeit*: Das Unterscheidungsgebot stellt zwar hohe Anforderungen an militärische Angriffe, allerdings bedeutet dies nicht, dass generell von Angriffen abgesehen werden muss, wenn dabei Zivilisten bzw. zivile Einrichtungen in Mitleidenschaft gezogen werden könnten. Derartige Kollateralschäden dürfen in Kauf genommen werden, allerdings nur in einem Umfang, der nicht exzessiv ist in Relation zu dem konkreten und direkten militärischen Nutzen der Operation. Die Anwendung dieser Norm gehört zu den schwierigsten Aufgaben im Kontext des HVR, denn es gilt, höchst unterschiedliche, im Kern inkommensurable, also nicht vergleichbare Kategorien – militärische und humanitäre Ziele – gegeneinander abzuwägen. Deswegen bestehen begründete Zweifel, ob softwaregestützte Systeme wie AWS in der Lage sein könnten, die erforderlichen Abwägungen zur Verhältnismäßigkeit eines Angriffs zufriedenstellend und zuverlässig durchzuführen. Der dafür erforderliche Umfang an Kontext- und Weltwissen sowie die Fähigkeit, die Aktionen von Menschen zu interpretieren und zu verstehen, dürften auf absehbare Zeit nicht im Rahmen ihrer Möglichkeiten liegen.
- *Vorsorgeprinzip*: Das Vorsorgeprinzip verpflichtet den Angreifer, dasjenige Mittel zu wählen, das der Zivilbevölkerung bzw. zivilen Objekten den geringsten Schaden zufügt. Darüber hinaus besteht die Verpflichtung, die Zivilbevölkerung vor Angriffen zu warnen, die sie tangieren können, soweit dem kein gewichtiger Grund entgegensteht. Der Maßstab dieser Verpflichtung ist subjektiv, da die konkret in der Situation verfügbaren Optionen abgewogen werden müssen. Streitkräfte, die hochpräzise Wirkmittel zur Verfügung haben, sind somit einem höheren Standard unterworfen als schlechter ausgerüstete Gegner ohne diese Möglichkeiten. Die Abwägungen gemäß dem Vorsorgeprinzip wären von den hier beschriebenen Prinzipien des HVR wohl am ehesten durch AWS erfüllbar.

Die ethische Debatte

Im vorliegenden Bericht wird die weitverzweigte ethische Debatte über AWS dargestellt. Im Fokus stehen drei maßgebliche Diskussionsstränge, die aus unterschiedlichen Blickwinkeln die Frage behandeln, ob und ggf. inwiefern die eigentliche Bestimmung von AWS, nämlich die autonome Anwendung tödlicher Gewalt, moralisch zulässig ist.

Im Zentrum der ethischen Debatte über AWS stehen Fragen, die die Implikationen dieser neuen Waffentechnologie für die *Ethik des Krieges* betreffen. Einer der wichtigsten theoretischen Bezugspunkte dabei ist die sogenannte Lehre vom gerechten Krieg, die antike Wurzeln hat und deren Maßstäbe Eingang in das HVR gefunden haben. Ziel ist es, Kriterien zu finden, unter denen die Anwendung militärischer Gewalt als Mittel der Konfliktlösung im äußersten Fall gerechtfertigt werden kann. Befürworter autonomer Waffentechnologie sehen die Chance, dass AWS sogar zu einer Verbesserung der humanitären Situation gegenüber dem Status quo beitragen könnten. So wären sie diesem Ansatz zufolge dank ihrer überlegenen sensorischen und datenverarbeitenden Fähigkeiten insgesamt besser als menschliche Kämpferinnen und Kämpfer in der Lage, zwischen Kombattanten und unbeteiligten Zivilisten zu unterscheiden (Unterscheidungsgebot) und Waffengewalt so präzise und gleichzeitig zurückhaltend einzusetzen, dass unverhältnismäßige Kollateralschäden ausgeschlossen wären (Verhältnismäßigkeitsgebot). Kritiker wenden dagegen ein, dass diese Annahme auf der falschen Prämisse beruhe, aus den komplexen und interpretationsbedürftigen Anforderungen an eine ethische Kriegsführung – wie sie beispielsweise in den völkerrechtlichen Geboten zum Ausdruck kommen – ließen sich eindeutige Verhaltensregeln ableiten, die eins zu eins in Programmcodes transferiert werden können. Von der Frage, ob sich ethische und rechtliche Erwägungen maschinell angemessen implementieren lassen, hängt ab, ob ein ethisch vertretbarer Einsatz von AWS prinzipiell möglich erscheint. Nicht zuletzt entscheidet sich dies auf der technischen Ebene. Klar ist: Zum jetzigen Zeitpunkt ist der Entwicklungsstand in den relevanten Bereichen (KI, Robotik, Sensorik etc.) bei Weitem noch nicht ausgereift genug, um ethisch vertretbare bzw. völkerrechtskonforme AWS zu konstruieren. Ob und inwiefern dies in der Zukunft anders sein wird, muss zum jetzigen Zeitpunkt offenbleiben.

Im zweiten Diskussionsstrang stehen Überlegungen im Vordergrund, die genuin ethischer Art sind, also weniger auf empirischen Erwägungen beruhen und stattdessen stärker von normativen Vorgaben und begrifflichen Festlegungen geleitet sind. Zur Debatte steht dabei der grundsätzliche Zweck derartiger Waffensysteme: die Fähigkeit, autonom über Leben und Tod zu entscheiden. Dabei wird vor allem über die Frage diskutiert, ob und inwiefern die Tötung von Menschen durch autonome Systeme mit der *Menschenwürde* vereinbar ist. Mit der Idee der Menschenwürde, die in Deutschland und in vielen anderen

freiheitlich-demokratischen Gesellschaften als besonders schützenswerter Grundwert gilt, ist eine zentrale Verpflichtung verbunden: Der Mensch darf nicht zum Objekt gemacht werden. In der Debatte wird das Argument vorgebracht, dass der Einsatz letaler Gewalt durch AWS ethisch grundsätzlich inakzeptabel sei, weil er genau dies impliziere: Die Opfer würden entwürdigt, indem sie in einem rein technischen Prozess zu Zielobjekten degradiert würden, ohne dass dabei die Aussicht auf Achtung ihrer Würde bestünde. Das Argument bringt die starken moralischen Vorbehalte zum Ausdruck, die gegenüber einer solchen Dehumanisierung des Krieges bestehen. Es ist jedoch theoretisch und begrifflich sehr voraussetzungsreich und seine Reichweite entsprechend umstritten.

Schließlich ist mit Blick auf AWS auch die *Frage der Verantwortung* von besonderer Brisanz. Denn je autonomer Waffensysteme agieren, je weniger sie also direkter menschlicher Steuerung unterliegen, desto weniger eindeutig lassen sich ihre Aktionen einem menschlichen Akteur zuordnen. Das wird immer dann problematisch, wenn solche Systeme zivile und unverhältnismäßige militärische Schäden anrichten, was selbst bei völkerrechtskonformen AWS nie ganz auszuschließen wäre. Wer trägt dann die Verantwortung? Diese Frage wird virulent, da es wenig sinnvoll erscheint, die Maschinen selbst zur Rechenschaft zu ziehen, zumindest solange sie nicht über Handlungsvermögen im menschlichen Sinne verfügen. Eine sich möglicherweise abzeichnende Verantwortungslücke hat zum einen rechtliche Implikationen, denn je mehr sich Waffensysteme menschlicher Steuerung entziehen, desto schwieriger wird es, menschliche Entscheidungsträger für die von diesen Systemen begangenen Vergehen oder Verbrechen zivil- oder strafrechtlich zur Rechenschaft zu ziehen. Zum anderen stellen sich aber auch moralische Fragen, da die Entscheidung, einen anderen Menschen zu töten, eine der moralisch schwerwiegendsten ist, die man treffen kann. Insofern ist die Vorstellung, dass niemand für eine solche Entscheidung (bzw. die anschließende Tat) die moralische Verantwortung zu übernehmen hätte, durchaus beunruhigend. Durch den Einsatz von AWS könnte so eine Situation entstehen, in der sich das technisch vermittelte Töten von Menschen wie ein zufälliges Naturereignis oder ein Unfall ausnimmt. Es gäbe dann niemanden mehr, der dies mit seinem Gewissen vereinbaren müsste, was als Grund dafür ins Feld geführt wird, dass AWS ethisch verwerflich wären und nicht eingesetzt werden sollten.

Insgesamt zeigt sich, dass, obwohl autonome Waffensysteme in ethischer Hinsicht durchaus kontrovers diskutiert werden, die Zweifel an ihrer Zulässigkeit und Legitimität deutlich überwiegen. Allerdings ist es nicht Anspruch der Ethik, kategorische Urteile über die ethisch-moralische Bedenklichkeit oder Unbedenklichkeit einer Technologie zu fällen. Die Ethik vermag die mit dem technologischen Wandel verbundenen normativen Unsicherheiten nicht aufzulösen, sie kann sie nur reflektieren und zu klären versuchen.

Handlungsmöglichkeiten zur präventiven Rüstungskontrolle

Präventive Rüstungskontrolle dient der Identifikation und Ausarbeitung von rüstungskontrollpolitischen Regulierungsansätzen für zukünftige, bisher nichtstationierte Waffensysteme, mit dem konkreten Ziel, der destabilisierenden Wirkung von potenziellen Rüstungswettläufen und den Gefahren militärischer Eskalationsmechanismen bereits im Vorfeld zu begegnen. Dies ist ein breitangelegter Prozess, der darauf abzielt, die möglicherweise problematischen Konsequenzen technologischer Entwicklungen frühzeitig zu erkennen, für die in politischer Verantwortung stehenden Entscheidungsträger beurteilbar zu machen und durch Institutionen und Verfahren auf nationaler und internationaler Ebene in ihren Risiken zu begrenzen.

Die Bemühungen um eine Regulierung von AWS speisen sich aus zwei zentralen Argumentationssträngen. Der eine behandelt die Frage, ob der Einsatz von AWS mit den Prinzipien des humanitären Völkerrechts vereinbar wäre. Die internationale Debatte dazu hat innerhalb der CCW eine adäquate Plattform gefunden. Der andere schließt die Auswirkungen der Entwicklung, Stationierung oder des Einsatzes von AWS für die internationale Sicherheit ein. Die zentrale Frage hier ist, wie mit möglichen sicherheitspolitischen Implikationen, wie z. B. Rüstungsdynamiken, zwischenstaatlichen Spannungen oder strategischen Instabilitäten, umgegangen werden kann. Der Austausch zu dieser Frage befindet sich ganz am Anfang und hat bisher noch kein geeignetes internationales Forum gefunden.

Für beide Fälle bestehen für die deutsche Politik vielfältige Ansätze, um angesichts schnell voranschreitender technologischer Entwicklungen sowie verstärkter militärischer Rüstungsbemühungen mögliche Risiken einzuhegen und damit zur Krisenstabilität und internationalen Sicherheit beizutragen.

Die Möglichkeiten innerhalb der CCW ausschöpfen

Um das von Deutschland und einer Reihe anderer Staaten und NGOs erklärte Ziel einer Ächtung von Waffensystemen zu erreichen, die dem Menschen die Entscheidungsgewalt über Leben und Tod entziehen, ist es ratsam, dass Deutschland sein bisheriges Engagement im Rahmen der CCW aktiv fortführt. Die gemeinsam mit Frankreich ergriffene Initiative, als ersten Schritt eine politische Erklärung und das Bekenntnis zum HVR-konformen Einsatz von AWS anzustreben, wurde international vielbeachtet.

Da für Beschlüsse im Rahmen der CCW die Einstimmigkeit aller Vertragsstaaten erforderlich ist, ist bei den derzeit weit auseinanderliegenden Positionen der einzelnen Staaten abzusehen, dass es sich bei der Konsensfindung um einen Prozess handelt, der einen langen Atem erfordert. Es ist daher zu erwarten, dass

zunächst nur kleine Schritte als Minimalkonsens vereinbart werden können, z. B. in Form von eher *weichen* vertrauens- und sicherheitsbildenden Maßnahmen.

Diese eher auf langfristige Erfolge angelegte Vorgehensweise birgt allerdings die Gefahr, dass mit verstreichender Zeit die Entwicklung, Verbreitung oder sogar der Einsatz von AWS stark vorangeschritten sein könnte. Damit würden Tatsachen geschaffen, die eine Einigung im Rahmen der CCW erschweren könnten.

Engagement über die CCW hinaus verbreitern

Insbesondere wenn die Fortschritte im Rahmen der CCW als zu langsam und/oder nicht hinreichend bewertet werden, ist anzuraten, auch weitere Möglichkeiten ins Auge zu fassen, mit denen der internationale Dialog gestärkt, Vertrauen aufgebaut und dem Sicherheitsbedürfnis aller Staaten Rechnung getragen wird. Im Gegensatz zur CCW wäre hierfür ein Konsens aller relevanter Staaten keine Voraussetzung. Daher könnten Initiativen von ad hoc zu bildenden Koalitionen von Staaten, NGOs und internationalen Organisationen getragen werden, die ein gemeinsames Ziel verfolgen und möglichst zügig auf eine Ausformulierung und Verabschiedung entsprechender Regeln zur Einhegung der Risiken von AWS hinarbeiten. Dies könnte eine Sogwirkung entfalten, sodass sich sukzessive immer mehr Staaten dieser Vorgehensweise anschließen. Für solch ein Vorgehen bietet der Prozess bis zur Umsetzung der Ottawa-Konvention[2] in internationales Recht Orientierung, der im Ergebnis zum völkerrechtlichen Verbot von Antipersonenminen führte. Allerdings wäre ein Abkommen zu AWS, dem die rüstungstechnisch führenden Staaten nicht beitreten würden, sicherlich kaum hilfreich. Die Wahrscheinlichkeit für eine breite Partizipation möglichst aller relevanter Staaten könnte ggf. durch die Wahl weniger ambitionierter Maßnahmen und Verbotstatbestände erhöht werden.

Noch weitreichender wäre die Möglichkeit, unilateral voranzugehen und einen Verzicht auf den Einsatz, die Beschaffung und/oder die Entwicklung von AWS verbindlich und nachprüfbar zu erklären. Diese Strategie könnte sich auf die in Bezug auf die Achtung der Menschenwürde vorgebrachten ethischen Argumente stützen und der herausgehobenen Rolle der Menschenwürde im Katalog der Grundrechte Rechnung tragen. Die Glaubwürdigkeit solchen Handelns würde gestärkt, wenn sie mit anderen Politikbereichen in Einklang gebracht wird. Zu nennen sind insbesondere die Forschungsförderung sowie die Exportpolitik. Auch hier wäre ein Leitmotiv, auf die Vorbildfunktion und eine eintretende Sogwirkung zu setzen, mit dem Ziel, dass weitere Staaten diesem Vorgehen folgen.

2 Übereinkommen über das Verbot des Einsatzes, der Lagerung, der Herstellung und der Weitergabe von Antipersonenminen und über deren Vernichtung

Zur Stärkung des internationalen Dialogs zu bislang vernachlässigten Themen (u. a. Rüstungsdynamiken, zwischenstaatliche Spannungen bzw. strategische Instabilitäten) sind diverse Formate bilateraler und multilateraler Foren denkbar, die ggf. als Nukleus für konkretere und verbindlichere Übereinkünfte dienen könnten. Das Design der Diskursformate könnte sich an erfolgreiche Beispiele aus anderen Politikbereichen anlehnen. So begann etwa das Wiener Übereinkommen zum Schutz der Ozonschicht als relativ weiche Vereinbarung und gewann Verbindlichkeit erst im Laufe der Zeit vor allem durch das Montreal-Protokoll[3] und dessen Zusätze. Als geeignete Plattform für den internationalen Austausch kommt z. B. auch die OECD (Organisation for Economic Co-operation and Development) infrage. So wäre etwa ein AWS-Forum analog zur BNCT (Working Party on Biotechnology, Nanotechnology and Converging Technologies) denkbar, die sich für eine verantwortbare Entwicklung dieser Technologien einsetzt.

Ein weiteres wesentliches Handlungsfeld ist die Revitalisierung der konventionellen Rüstungskontrolle. Dies wäre angesichts der heute vorherrschenden sicherheitspolitischen Lage auch losgelöst vom Thema AWS von enormer Bedeutung für eine Entspannung. Allerdings sind die Bedingungen hierfür aktuell alles andere als einfach – u. a. angesichts der Aufkündigung des Mittelstrecken-Nuklearstreitkräfte-Vertrags (INF-Vertrag; Intermediate-Range Nuclear Forces Treaty) zum Verbot landgestützter Kurz- und Mittelstreckenraketen zum August 2019 und der Ankündigung von US-Präsident Trump im April 2019, den Vertrag über den Waffenhandel (Arms Trade Treaty – ATT) nicht weiter zu unterstützen. Die Ausarbeitung und die Umsetzung von Rüstungskontrollvereinbarungen bedeuten einen langen und steinigen Weg. Die diffizile Aufgabe besteht darin, nachvollziehbar und glaubwürdig eine rote Linie zu definieren, um erlaubte bzw. gewünschte militärische Anwendungen der künstlichen Intelligenz und Robotik von nicht statthaften zu unterscheiden. Von enormer Bedeutung für den Erfolg von Rüstungsbeschränkungen ist die Konzeption verlässlicher Verifikationsmechanismen. Da Autonomie eine im Wesentlichen softwarebasierte Funktion ist, sind viele traditionelle Mittel der Verifikation (z. B. Inspektionen militärischer Einrichtungen zur Feststellung der Einhaltung numerischer Obergrenzen für bestimmte Waffentypen) hierfür kaum geeignet.

Eine wichtige Rolle könnte die Ausarbeitung von Exportregeln für kritische Technologien spielen. Mit dem ATT, dem Wassenaar Arrangement[4] (nachfolgend auch als Wassenaar-Abkommen bezeichnet) sowie dem MTCR (Missile Technology Control Regime) existieren bereits Instrumentarien, die durch die Kontrolle der Ausfuhr von Gütern und Technologien die Proliferation bestimmter Waffen einschränken. Teilweise fallen bereits Komponenten und

3 Montreal-Protokoll über Stoffe, die zu einem Abbau der Ozonschicht führen
4 Wassenaar Arrangement zu Exportkontrollen für konventionelle Rüstungsgüter und Dual-Use-Güter (Waren, Software und Technologie)

Technologien, die auch für AWS genutzt werden könnten, unter diese Abkommen oder sie könnten relativ leicht einbezogen werden. Gleichzeitig besteht die Schwierigkeit, dass die kritischen Technologien, insbesondere auf dem Gebiet der KI, ganz wesentlich im kommerziellen Sektor entwickelt werden und eine klare zivile und militärische Doppelnutzbarkeit aufweisen (»dual use«). Die Herausforderung besteht darin, Regularien zu schaffen, die unerwünschte militärische Nutzungen einschränken, aber den zivilen Nutzen der Technologien unangetastet lassen.

Fazit

Die zunehmende Nutzung von automatisierten oder zukünftig autonomen Waffensystemen könnte einen Paradigmenwechsel darstellen, der die Kriegsführung im 21. Jahrhundert revolutionieren würde. AWS werfen zahlreiche Fragen auf, sowohl was ihre Übereinstimmung mit den Prinzipien des humanitären Völkerrechts angeht als auch die Auswirkungen, die ihre Verbreitung und ihr Einsatz entfalten könnten, gerade auch in Bezug auf potenzielle Rüstungsdynamiken, die internationale Sicherheit sowie regionale und strategische Stabilität. Die internationale Staatengemeinschaft hat begonnen, sich dieser Themen anzunehmen.

Derzeit existiert ein *Fenster von Möglichkeiten*, um mit einem international abgestimmten, zielgerichteten Vorgehen die möglichen Gefahren einzuhegen, die AWS mit sich bringen könnten. Dieses Fenster schließt sich sukzessive mit fortschreitender technologischer Entwicklung sowie der kontinuierlichen Integration autonomer Funktionen in Waffensysteme aller Art. Damit werden Strukturen gefestigt und Fakten geschaffen, die regulierende Eingriffe erschweren oder sogar verhindern. Dieses Fenster von Möglichkeiten zu nutzen, ist keine einfache Aufgabe, denn die Schwierigkeiten, die sich bei der Rüstungskontrolle im Hinblick auf AWS stellen, sind groß. Im Lichte der Implikationen, mit denen die internationale Gemeinschaft durch autonome Waffensysteme zukünftig konfrontiert werden könnte, erscheint es dringend geboten, diese Herausforderungen unverzüglich anzugehen und Lösungen zu entwickeln. Diesbezügliche politische und diplomatische Initiativen erfordern einen langen Atem und einen breiten Diskurs unter Einbezug von Wissenschaft und Zivilgesellschaft.

1 Einleitung

Beeindruckende technologische Fortschritte im Bereich der künstlichen Intelligenz ermöglichen eine Fülle neuer Anwendungen, die im Begriff sind, sämtliche Wirtschafts- und Lebensbereiche zu durchdringen und grundlegend zu transformieren. Diese Entwicklung macht auch vor dem Militärsektor nicht Halt. Weltweit laufen intensive Forschungs- und Entwicklungstätigkeiten, die darauf abzielen, den Grad der Autonomie militärischer Systeme sowie die militärische Nutzung der KI zu steigern. Bereits heute sind unbemannte Waffensysteme im Einsatz, die über hochautomatisierte und autonome Funktionen verfügen, z. B. zur Navigation, zur Zielerkennung oder zur Steuerung des Zielanflugs von Raketen. Bislang liegen jedoch die Zielauswahl, die Angriffsentscheidung und schließlich die Freigabe des Waffeneinsatzes noch in der Verantwortung eines menschlichen Kommandeurs bzw. Operators.

Ein autonomes Waffensystem wäre in der Lage, auch diese Schritte selbsttätig und ohne oder mit nur minimaler menschlicher Mitwirkung durchzuführen. Aus militärischer Sicht ist dies vor allem aus zwei Gründen attraktiv: Erstens benötigt ein autonomes System keine Kommunikationsverbindung mit einer Basisstation, zweitens erlaubt es schnellere Reaktionszeiten in Gefechtssituationen, da keine Verzögerungen durch die Laufzeiten einer Datenübertragung und durch die Entscheidungsfindung bzw. die Reaktionszeiten eines menschlichen Operators auftreten. Die Steigerung der Autonomie von Waffensystemen steht daher in allen technologisch fortgeschrittenen Ländern auf der Agenda und hat eine weltweite Debatte ausgelöst.

Mit fortschreitender Autonomie von Waffensystemen wird vor allem eine zentrale Frage virulent: Kann es ethisch vertretbar, politisch verantwortbar und (völker)rechtlich erlaubt sein, die Entscheidung über Leben und Tod von Menschen an Maschinen zu delegieren? Oder anders gefragt: Wie muss die menschliche Kontrolle bzw. Steuerung von Waffensystemen beschaffen sein, damit diese Waffen im Einklang mit ethischen, politischen bzw. (völker)rechtlichen Prinzipien eingesetzt werden dürfen?

Vor diesem Hintergrund hat der Ausschuss für Bildung, Forschung und Technikfolgenabschätzung das Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB) 2017 beauftragt, ein TA-Projekt zum Thema AWS durchzuführen. Ziel der Untersuchung war es, technologische, militärisch-strategische, völkerrechtliche, ethische und nicht zuletzt rüstungskontrollpolitische Aspekte von AWS aufzuarbeiten, um Orientierungs- und entscheidungsrelevantes Wissen in diesem schwierigen und hochaktuellen Themenfeld bereitzustellen. Gleichzeitig konnte so das Monitoring des Themenfelds »Neue Technologien und Rüstungskontrolle« fortgesetzt werden, das 2001 vom Ausschuss für Bildung, Forschung und Technikfolgenabschätzung beschlossen

worden war. Bislang erschienen in dieser Reihe »Militärische Nutzung des Weltraums und Möglichkeiten der Rüstungskontrolle im Weltraum« (TAB 2003) sowie »Stand und Perspektiven der militärischen Nutzung unbemannter Systeme« (TAB 2011).

Aufbau des Berichts

Zu Beginn werden Definitionsansätze für AWS im Überblick dargestellt (Kap. 2). Dabei zeigt sich, dass eine klare und allgemein akzeptierte Abgrenzung von autonomen zu semiautonomen und hochautomatisierten Waffensystemen bis heute nicht möglich ist.

In Kapitel 3 werden die technischen Grundlagen für Autonomie behandelt. Es wird ein Überblick über den technologischen Stand bei autonomen Funktionen aktueller militärischer Systeme gegeben. Anschließend werden die Möglichkeiten und Begrenzungen beleuchtet, die sich beim aktuellen Entwicklungsstand von KI und maschinellem Lernen ergeben.

Im Anschluss werden in Kapitel 4 die Verbreitung und der Entwicklungsstand von unbemannten (semi)autonomen Waffensystemen zu Land, zu Wasser und in der Luft beschrieben. Daraufhin folgt eine Analyse der Forschungs- und Entwicklungstrends mit Bezug zu AWS. Ziel ist, eine Vorstellung von Entwicklungspfaden zu vermitteln sowie Anhaltspunkte über potenzielle Fähigkeiten von zukünftigen AWS zu geben.

Auf Grundlage der erwarteten Fähigkeiten werden in Kapitel 5 mögliche militärische Missionen und denkbare Einsatzszenarien für AWS aufgezeigt, die wiederum als Basis dafür dienen, sicherheitspolitische Implikationen von AWS zu untersuchen (Kap. 6). Dabei stehen Fragen im Mittelpunkt, wie sich mit AWS die Kriegsführung verändern könnte bzw. welche Auswirkungen auf die globale und regionale Stabilität sowie auf Rüstungsdynamiken zu erwarten sind.

In Kapitel 7 wird der Rahmen beschrieben, den das humanitäre Völkerrecht jeglichem legitimem Waffeneinsatz setzt. Darauf aufbauend wird herausgearbeitet, welche Bedingungen und Grenzen daraus für mögliche Einsätze von AWS folgen.

Die ethische Debatte um AWS wird in Kapitel 8 anhand dreier Diskussionsstränge dargestellt. Der erste behandelt die möglichen Auswirkungen von AWS auf die Ethik der Kriegsführung, insbesondere im Hinblick auf humanitäre Folgen. Im zweiten wird der Frage nachgegangen, ob es mit der Menschenwürde zu vereinbaren ist, die Entscheidung über Leben und Tod an Maschinen zu übertragen. Im dritten schließlich wird die Frage aufgegriffen, ob AWS eine Verantwortungslücke schaffen, die mit rechtlichen sowie moralischen Rechenschaftspflichten nicht in Einklang zu bringen ist.

In Kapitel 9 wird zunächst ein Überblick über Rüstungs- und Exportkontrollabkommen mit Relevanz für AWS gegeben. Im Anschluss werden die Dis-

kussionen der internationalen Staatengemeinschaft über die mögliche Regulierung von AWS behandelt, die derzeit im Rahmen der CCW geführt werden. Zum Abschluss werden Handlungsmöglichkeiten aufgezeigt, mittels derer mögliche Risiken von AWS eingehegt werden können.

Das Thema AWS ist hochaktuell und die Befassung damit während der Projektdurchführung sowohl in der wissenschaftlichen als auch in der politischen Sphäre deutlich Fahrt aufgenommen. Diese Dynamik hatte zur Folge, dass einige bedeutsame Entwicklungen erst kurz vor Abschluss dieses Berichts Ende 2018 zu verzeichnen waren. Dies betrifft in erster Linie die inhaltlichen Fortschritte, die beim Expertentreffen erzielt wurden, das im Rahmen der CCW vom 25. bis 29. März 2019 in Genf stattfand. Aber auch der Abschlussbericht des International Panel on the Regulation of Autonomous Weapons (iPRAW 2018b), die Veröffentlichung der KI-Strategie des US-Verteidigungsministeriums (DOD 2019) sowie diverse Initiativen der Trump-Administration zu KI (U.S. President 2019) und zur Rüstungskontrolle (Aufkündigung des INF-Vertrags sowie des ATT) sind hier zu nennen. Auch wenn es aus Zeitgründen nicht mehr möglich war, alle diese Entwicklungen in der erforderlichen Tiefe und Breite abzuhandeln, wurden relevante Aspekte in Form von Fußnoten und Textkästen kenntlich gemacht.

Zusammenarbeit mit Gutachtern und Danksagung

Zur fachlichen Fundierung dieses Berichts wurden drei Gutachten vergeben:

- Technologien für autonome Waffensysteme – Stand und Perspektiven. Jürgen Altmann, Mark Gubrud, Köln
- Sicherheitspolitische Implikationen und Möglichkeiten der Rüstungskontrolle autonomer Waffensysteme. Christian Alwardt, Lina-Marieke Hilgert, Götz Neuneck, Johanna Polle, Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg, Hamburg
- Ethische Fragestellungen im Kontext autonomer Waffensysteme. Dr. Bernhard Koch, Dr. Bernhard Rinke, Institut für Theologie und Frieden, Hamburg

Zahlreiche Elemente dieser Gutachten flossen in den vorliegenden Bericht ein. Die Analysen von Alwardt et al. (2017) bilden eine wesentliche Grundlage für die Kapitel 4 bis 6 sowie 9. Die Arbeiten von Altmann und Gubrud (2017) liegen hauptsächlich Kapitel 4 zugrunde, liefern aber auch für andere Kapitel Informationen und Materialien. Kapitel 8 zu den ethischen Fragestellungen profitiert wesentlich von der Expertise von Koch und Rinke (2017).

An dieser Stelle sei den Gutachterinne und Gutachtern für die Bereitschaft zur Kooperation und Kommunikation sowie die herausragende Qualität der vorgelegten Gutachten herzlich gedankt. Die Verantwortung für die Auswahl,

Strukturierung und Verdichtung des Materials sowie dessen Zusammenführung mit eigenen Recherchen und Analysen tragen die Verfasser. Dank gebührt auch Brigitta-Ulrike Goelsdorf für die sorgfältige redaktionelle Bearbeitung und Layoutgestaltung des Berichts.

2 Abgrenzung des Untersuchungsgegenstands

International werden diverse Ansätze verfolgt, um AWS zu definieren und von anderen Waffensystemen abzugrenzen. Eine präzise, allgemein akzeptierte Definition existiert bis heute nicht. Um den Untersuchungsgegenstand des vorliegenden Berichts zu umreißen, ist eine solche Definition jedoch nicht notwendig. Für die hier vorgenommene Analyse militärisch-strategischer, sicherheitspolitischer und ethischer Fragestellungen reicht es aus, die hierfür jeweils relevanten Charakteristika der Waffensysteme plausibel zu beschreiben. Ob diese Systeme unter eine bestimmte strenge Definition autonomer Waffensysteme fallen würden oder nicht, kann dahingestellt bleiben.

Bei der Erstellung dieses Berichts wurde daher mit einer deskriptiven Charakterisierung gearbeitet, nach der ein AWS Aufträge ohne bzw. mit lediglich schwacher externer menschlicher Kontrolle selbstständig ausführt und die Fähigkeit besitzt, in einer komplexen, dynamischen Umgebung auf unvorhersehbare Ereignisse zielgerichtet reagieren zu können. Nach Kenntnis und Einschätzung des TAB existieren solche Waffensysteme heute noch nicht. Aus der Analyse gegenwärtig existierender hochautomatisierter Waffensysteme und wissenschaftlich-technologischer Entwicklungstrends können jedoch konkrete Vorstellungen und Erwartungen entwickelt werden, wie zukünftige AWS aussehen und wann sie Realität werden könnten. Da dies ein sich sehr dynamisch entwickelndes Themengebiet ist, muss allerdings damit gerechnet werden, dass diese Vorstellungen auch rasch von der Realität überholt werden könnten. Daher sollten von diesem Bericht auch keine endgültigen Bewertungen erwartet werden, vielmehr ist eine kontinuierliche Beobachtung des Gebiets anzuraten.

Die Frage der Definition von AWS birgt allerdings eine erhebliche Brisanz, da sie oftmals in einen direkten Zusammenhang mit möglichen Vereinbarungen zur Rüstungskontrolle gestellt wird (Kap. 9.2). Hier wird oft implizit oder explizit angenommen, dass die Definition von AWS gleichzeitig den Rahmen setzt, welche Systeme ggf. zu regulieren oder gar zu verbieten sind. Daher spiegelt die Haltung der Staaten und anderer Akteure in definitorischen Fragen regelmäßig deren Eigeninteressen und Verhandlungspositionen wider. Kontroversen um Definitionen stehen vielfach stellvertretend für tiefere inhaltliche Gegensätze bzw. werden instrumentalisiert, um den Verhandlungsprozess zu hemmen. Aus diesem Grund werden im Folgenden definitorische Ansätze, Beispiele und Argumente vorgestellt und analysiert.

2.1 Definitorische Ansätze

Für die Definition von AWS existieren verschiedene Herangehensweisen. Sie gründen erstens auf den (technologischen) Charakteristika des Waffensystems, zweitens legen den verbliebenen Grad menschlicher Kontrolle zugrunde, drittens orientieren sich an Funktionen oder am intendierten Einsatzspektrum des Waffensystems oder viertens kombinieren mehrere dieser Kriterien. Jeder dieser Ansätze weist inhärente Stärken, aber auch Schwächen auf (UNIDIR 2017, S. 19 ff.):

1. Der technologiezentrierte Ansatz entspricht der konventionell in rüstungskontrollpolitischem Zusammenhang üblichen Herangehensweise und wäre somit als Grundlage entsprechender Vereinbarungen gut geeignet. Allerdings birgt er das Problem, dass die genauen technischen Spezifikationen zukünftiger AWS in gewissem Umfang spekulativ bleiben müssen. Außerdem könnte eine Definition anhand technologischer Kriterien durch wissenschaftlich-technische Fortschritte obsolet gemacht werden. Außerdem existieren gravierende Abgrenzungsprobleme. Falls beispielsweise defensive AWS (beispielsweise nach Art von »MANTIS«) als akzeptabel erachtet würden, offensive dagegen nicht, wäre dies durch eine technologiezentrierte Definition nicht abzubilden, da das gleiche System lediglich abhängig von den Operationsbedingungen einmal defensiv und einmal offensiv wirken könnte.
2. Der Ansatz, dessen Fokus auf den Grad menschlicher Kontrolle liegt, hat den Vorzug, dass er wesentliche Anforderungen des humanitären Völkerrechts aufgreift (Kap. 7) und gleichzeitig an den breitgeteilten Grundsatz anknüpft, dass Menschen die Letztkontrolle über den Einsatz tödlicher Waffengewalt behalten sollen. Andererseits entsteht das Problem, dass Test, Evaluation bzw. Verifikation des Grads menschlicher Kontrolle schwierig sind, weil hier im Prinzip der Mensch als Teil des Systems mitevaluiert werden müsste.
3. Der an den Funktionen orientierte Ansatz basiert auf dem Konzept sogenannter kritischer Funktionen auf. Damit sind die Zielauswahl (einschließlich Detektion, Identifikation, Verfolgung, Priorisierung) und -bekämpfung (d. h. der Waffeneinsatz) gemeint. Ein System, das diese Funktionen selbsttätig ausfüllen kann, wäre demnach ein AWS. Dieser Ansatz hat den Vorzug, dass er recht einfach ist. Allerdings ist er sehr breit angelegt, da zum einen auch existierende hochautomatisierte Systeme (ein Beispiel wäre die radarsuchende Drohne »Harpy«) damit erfasst würden und zum anderen insbesondere für die Zielauswahl verschiedene räumlich verteilte Subsysteme (einschließlich Global Positioning System – GPS) genutzt werden, die dem AWS zugerechnet werden müssten.

4. Eine sequenzielle Kombination der drei Ansätze hat das Potenzial, zu einer umfassenden präzisen Definition zu führen. Nach einer Festlegung der angemessenen bzw. notwendigen menschlichen Rolle sowie der Bestimmung der kritischen Funktionen könnten technologische Fragen zielgerichtet angegangen werden. Erfolgversprechend ist ein solches Vorgehen allerdings nur, wenn die Definitionsfrage klar getrennt behandelt werden kann von der Frage, welche Kategorien von AWS möglicherweise reguliert oder gar verboten werden sollen. Anderenfalls würden absehbar strategische und politische Motive die Diskussion bestimmen und eine Einigung unwahrscheinlich machen.

2.2 Autonom, semiautonom oder automatisiert?

Ein Knackpunkt bei den verschiedenen Definitionen ist die Frage, wie autonome von semiautonomen und (hoch)automatisierten Waffensystemen abgegrenzt werden sollen. Um sich dieser Problematik anzunähern, müssen zunächst einige zentrale Begriffe geklärt werden.

Relativ unproblematisch sind die Begriffsbestandteile Waffe und System zu definieren. Eine Waffe ist ein Gerät oder System, das eine Form von Materie, Energie (und möglicherweise Information beispielsweise bei Cyberwaffen, die jedoch im vorliegenden Bericht ausgeklammert bleiben) freisetzen oder lenken soll, die funktionsunfähig machende, schädigende oder zerstörende Wirkungen auf Personen oder Dinge haben. Vor allem im Zusammenhang mit der CCW wird oft von »lethal[5] autonomous weapons systems« (LAWS/letale autonome Waffensysteme) gesprochen, um deren tödliche Wirkung zu betonen. Die Verwendung des Begriffs System betont, dass nicht nur das Wirkmittel bzw. der Träger des Wirkmittels betrachtet werden sollen, sondern der Blick geöffnet wird für alle Komponenten, die für das Funktionieren der Waffe von Bedeutung sind, also auch beispielsweise Startvorrichtungen, Steuerungs- und Navigationssysteme. Was im konkreten Fall zum AWS hinzugerechnet und was abgegrenzt wird, ist allerdings stark vom Kontext abhängig.

Nicht nur die öffentliche Debatte, sondern auch die Fachdiskussion krankt oftmals daran, dass der verwendete Autonomiebegriff nicht hinreichend expliziert und/oder schwammig gehalten wird. Dies kann zu gravierenden Missverständnissen führen, etwa wenn kategorische Aussagen getroffen werden wie: »Autonome Waffensysteme müssen verboten werden«, aber nicht ausgeführt wird, in welcher Bedeutung der Begriff autonom genau verwendet wird. Dessen Bedeutungsspektrum ist sehr weit: Auf der einen Seite kann er im Sinne der Philosophie der Aufklärung als Möglichkeit verstanden werden, selbstbestimmt

5 Allerdings wird im englischsprachigen Fachdiskurs »lethal« oft nicht im Sinne von tödlich, sondern von physisch zerstörend verwendet. Ursprünglich sollte der Zusatz »lethal« wohl nur Cyberwaffen ausschließen.

in Freiheit und Vernunft nach eigenen Gesetzen zu handeln (Kasten 2.1). Die Realisierung von Waffensystemen, die in diesem Sinne autonom sind, ist nach allgemeinem Verständnis mindestens in absehbarer Zeit nicht zu erwarten. Möglicherweise bleiben solche terminatorähnlichen Waffen auch dauerhaft der Domäne der Science-Fiction vorbehalten.

Kasten 2.1 Der Autonomiebegriff aus philosophischer Sicht

Autonomie ist ein Schlüsselbegriff der Philosophie und der Aufklärung, der maßgeblich durch die moralphilosophischen Schriften Immanuel Kants geprägt wurde (z. B. Pauen 2011). Gemäß Kant bedeutet Autonomie im Kern die Fähigkeit zum moralischen Urteil, zu dem nur vernunftbegabte, freie Wesen imstande sind, die sich die Gesetze ihres sittlichen Handelns selbst aufzuerlegen vermögen. Dazu reicht es nicht aus, nur in einer Art Wirkkausalität zu einer Bewegung oder dergleichen veranlasst zu sein; vielmehr gehört dazu wesentlich der intentionale Bezug auf das, was durch das Handeln bewirkt werden soll. Autonomie in diesem Sinne ist gleichbedeutend mit der Fähigkeit, sein Handeln aus eigenem freiem Willen zu initiieren und mithin für seine Taten verantwortlich zu zeichnen.

Ein im Gegensatz dazu deutlich einfacherer Ansatz, Autonomie zu definieren, besteht darin, den Begriff *operationell* zu fassen, d. h. als Eigenschaft eines (maschinellen) Vollzugs. Demnach sind Systeme dann autonom, wenn sie Aktionen in komplexen Umwelten bzw. sich verändernden Umgebungen ohne ständige Überwachung und Kontrolle insofern unabhängig vom Menschen ausführen können. Aus moralphilosophischer Sicht besteht der große und nicht zu überbrückende Gegensatz zur kantischen Autonomiedefinition darin, dass für Kant Autonomie auf die Handlungsurheberschaft zielt, während die operationelle Autonomiedefinition dies gerade nicht voraussetzt. Auch bei den intelligentesten Robotern ist nicht davon auszugehen, dass sie über (Selbst-)Bewusstsein und einen freien Willen verfügen und dementsprechend, dass sie verantwortlich handeln können (Neuhäuser 2014).

Zwar findet sich in der Literatur auch das Argument, dass Maschinen irgendwann mindestens genauso intelligent wie Menschen und insofern zumindest prinzipiell zu wahrer Autonomie und Handlungsurheberschaft fähig sein werden (Bostrom 2014). Voraussetzung dafür wäre allerdings, dass es gelänge, allgemeine menschliche Intelligenz (inklusive Bewusstsein) künstlich nachzubilden (sogenannte starke KI) und nicht nur Teilaspekte intelligenten Verhaltens zu simulieren (schwache KI; vgl. TAB 2016, S. 102 ff.). Dieses Szenario ist zum jetzigen Zeitpunkt jedoch (noch) rein hypothetisch-spekulativer Natur.

Quelle: Koch/Rinke 2017, S. 34 f. u. 156 f.

Auf der anderen Seite des Spektrums kann Autonomie in rein funktionaler Hinsicht bedeuten, dass ein System bestimmte Aufgaben ohne Einwirkung von außen erledigen kann. In dieser Bedeutung müsste aber auch eine einfache Landmine autonom genannt werden. Auch sind Waffensysteme, die selbstständig navigieren bzw. Ziele anhand bestimmter Kriterien suchen, identifizieren und auch bekämpfen können, Stand der Technik. Beispielsweise ist die israelische Drohne »Harpy« bereits seit vielen Jahren im Einsatz. Sie kann ein Gebiet abfliegen, nach vorgegebenen Radarsignaturen suchen, deren Quelle lokalisieren sowie diese ansteuern und mit ihrem Sprengkopf zerstören. Nach dem eben beschriebenen funktionalen Verständnis von Autonomie wäre somit »Harpy« ein Paradebeispiel für ein autonomes Waffensystem. Allerdings verfügt diese Drohne nur über ein geringes Ausmaß an implementierter Rechenleistung und folgt einem relativ starr vorgegebenen Programmablauf. Daher wird sie häufig als automatisiertes und nicht als autonomes Waffensystem bezeichnet. Eine Landmine, die nach einer einfachen Wenn-dann-Logik operiert (in der Art: »Wenn ein Gewicht höher als x kg einwirkt, löse den Zünder aus«), wäre nach diesem Sprachgebrauch ein automatisches System.

Kasten 2.2 Anmerkung zum Sprachgebrauch

In der Diskussion um AWS wird regelmäßig mit Begriffen operiert, die ursprünglich aus philosophischen, psychologischen oder pädagogischen Zusammenhängen stammen. Der zentrale Begriff »autonom« ist hier an erster Stelle zu nennen, aber auch beispielsweise »handeln«, »Entscheidungen treffen«, »Intelligenz« oder »lernen« gehören in diese Kategorie. In ihrer Ursprungsbedeutung bezeichnen sie Zuschreibungen, die nur in Bezug auf Menschen (und ggf. hochentwickelte Tiere) sinnvoll getroffen werden können.

Bei deren Verwendung in Bezug auf technische Artefakte besteht die Gefahr, dass die durch die Begriffe transportierten Konnotationen dazu führen, dass den Artefakten gewollt oder ungewollt menschliche Eigenschaften zugesprochen werden und/oder dass aus sprachlich naheliegenden, aber inhaltlich fragwürdigen Analogien irreführende Schlussfolgerungen gezogen werden.

Da es sinnvoll erscheint, den üblichen Sprachgebrauch in der Fachdiskussion aufzugreifen, war auch im vorliegenden Bericht die Verwendung der entsprechenden Begrifflichkeiten nicht ganz zu vermeiden. Beim Lesen dieses Berichts – wie auch in der gesamten populären und Fachliteratur zu AWS – sollte man sich dieser Problematik jedoch stets bewusst sein.

Die Begriffe automatisch, automatisiert und autonom befinden sich in dieser Reihenfolge auf einem Kontinuum ansteigender Komplexität, und eine trenn-

scharfe Abgrenzung zwischen ihnen ist kaum möglich. Zur Unterscheidung wurde beispielsweise vorgeschlagen, dass automatische Systeme in einer strukturierten, vorhersagbaren Umgebung operieren, autonome dagegen auch in einer komplexen, unstrukturierten und sich verändernden Umwelt sich zurechtfinden (Heyns 2013, S. 8); oder aber, dass die Aktionen automatisierter Systeme vorhersehbar sind, diejenigen von autonomen Systemen jedoch nicht in jedem Einzelfall, sondern nur in ihrer Gesamtheit (MOD 2017b, S. 13). Das US-Verteidigungsministerium definiert so: »Autonomie ist die Fähigkeit einer Entität, unabhängig verschiedene Vorgehensweisen zu entwickeln und auszuwählen um Ziele zu erreichen, basierend auf dem Wissen und Verständnis der Entität über die Welt, sich selbst und die Situation«.[6] Solche Beschreibungen bieten etwas Orientierung, allerdings bleibt ein gewisser Graubereich, und es können immer Beispiele gefunden werden, für die eine eindeutige Zuordnung nicht möglich ist.

Darüber hinaus existieren diverse Ansätze, unterschiedliche Grade an Automatisierung bzw. Autonomie zu definieren. Beispielsweise hat das US-amerikanische National Institute of Standards and Technology (NIST 2007 u. 2008) für unbemannte Systeme eine Skala von 0 (ferngesteuert) bis 10 (vollständige intelligente Autonomie) entwickelt. Für die Einordnung eines Systems auf dieser Skala wird in drei Kategorien – Komplexität der Mission, Schwierigkeit der Umwelt sowie Mensch-Roboter-Interaktion – eine Bewertung vergeben, die zum Gesamtergebnis aggregiert werden. In einem weiteren, eher schematischen Abgrenzungsansatz wird in Abhängigkeit von der Komplexität der Einsatzumgebung und dem Grad der menschlichen Kontrolle über das System zwischen sieben Automatisierungslevels unterschieden, die das Spektrum von automatischen zu autonomen Waffensystemen abdecken sollen (Alwardt/Krüger 2016).

Ein wesentlich ausgefeilterer Versuch zur Abgrenzung autonomer Waffensysteme wurde im Rahmen des Projekts »Multidimensional Autonomy Risk Assessment« (MARA) unternommen (Dickow et al. 2015a). Das resultierende formelbasierte Instrument erlaubt es, jedes heutige bzw. in der Entwicklung befindliche Waffensystem über die Bestimmung von 15 Einflussgrößen numerisch zu charakterisieren (MARA-Score), um in einem direkten Vergleich vieler so eingestufter Systeme eine Bewertung hinsichtlich des Grades autonomer Fähigkeiten vornehmen zu können.

In einer Analyse solcher Ansätze, verschiedene Grade von Autonomie zu definieren, kam ein Beratungsgremium des US-Verteidigungsministeriums allerdings zu dem Schluss, dass diese wenig hilfreich und teilweise kontraproduktiv sind, da sie zu sehr auf eine Charakterisierung von Eigenschaften des technischen Systems abzielen und dabei die viel bedeutsamere Art der Zusam

6 Im Original: »Autonomy is defined as the ability of an entity to independently develop and select among different courses of action to achieve goals based on the entity's knowledge and understanding of the world, itself, and the situation.« (DOD 2017b, S. 17)

menarbeit von Mensch und Maschine bei der Missionsausführung aus dem Auge verlieren (DSB 2012, S. 4).

In diesem Zusammenhang wurde angeregt, ob es nicht produktiver sein kann, den Fokus der zukünftigen Diskussion auf »Autonomie in Waffensystemen« zu lenken anstatt wie bisher auf »autonome Waffensysteme« als Waffenkategorie. Dies würde implizieren, den vorherrschenden plattform- oder systemzentrierten Ansatz durch einen funktionalen Blickwinkel zu ersetzen (Boulanin/Verbruggen 2017, S. 118).

Unterdessen ist zu beobachten, dass – angesichts der beschriebenen definitorischen Defizite bezüglich Autonomie einerseits und einer ablehnenden Haltung der Öffentlichkeit gegenüber intelligenten *Killerrobotern* andererseits – vor allem in militärischen und sicherheitspolitischen Fachkreisen der Begriff AWS zunehmend vermieden wird. Stattdessen ist häufiger die Rede von Systemen, die automatisierte oder teilautonome Funktionen aufweisen und im engen Verbund mit dem Menschen operieren. Schlagwörter, die in diesem Zusammenhang verwendet werden, lauten »manned-unmanned teaming« (MUM-T) oder »human-machine teaming« (DOD 2017b, S. 31 ff.; MOD 2018; Sadowski 2016; TARDEC 2017, S. 12 ff.).

2.3 Die Definition des US-Verteidigungsministeriums

Eine zentrale Rolle in der internationalen Debatte nimmt die Definition von AWS ein, die das US-Verteidigungsministerium im Rahmen einer formellen Richtlinie zu Autonomie in Waffensystemen 2012 vorgestellt hat. Dies war die erste Definition mit offiziellem Charakter, auf die seitdem immer wieder Bezug genommen wird. Demnach ist ein autonomes Waffensystem ein Waffensystem, »das nach seiner Aktivierung Ziele auswählen und bekämpfen kann ohne weitere Einwirkung durch einen menschlichen Bediener. Dies schließt von Menschen überwachte AWS ein, die es menschlichen Bedienern erlauben, das System im Betrieb zu überstimmen«.[7] Im Gegensatz dazu wird als semiautonomes Waffensystem definiert als ein Waffensystem, »das nach seiner Aktivierung dafür vorgesehen ist, lediglich einzelne Ziele oder spezifische Gruppen von Zielen, die von einem menschlichen Bediener ausgewählt wurden, zu bekämpfen«.[8] Solange menschliche Kontrolle über die Entscheidung, einzelne Ziele oder Gruppen von Zielen auszuwählen, gewahrt bleibt, sollen Waffensysteme auch

7 Im Original: »A weapon system that, once activated, can select and engage targets without further intervention by a human operator. This includes human-supervised autonomous weapon systems that are designed to allow human operators to override operation of the weapon system.« (DOD 2012, S. 13 f.)

8 Im Original: »A weapon system that, once activated, is intended to only engage individual targets or specific target groups that have been selected by a human operator.« (DOD 2012, S. 13 f.)

dann semiautonom sein, wenn sie bestimmte Funktionen autonom ausführen können. Es folgt eine Auflistung einiger dieser Funktionen (die nicht als abschließend verstanden werden soll):

- Erfassen, Verfolgen und Identifizieren möglicher Ziele
- menschliche Bediener auf mögliche Ziele aufmerksam machen
- ausgewählte Ziele priorisieren
- Bestimmung des Zeitpunkts zu feuern
- Steuerung des Endanflugs auf ausgewählte Ziele[9]

Diese Unterscheidung zwischen vollautonomen und semiautonomen Waffensystemen ist nicht überzeugend, da aus technischer Sicht ein so definiertes semiautonomes Waffensystem alle Fähigkeiten hätte, um auch vollständig autonom funktionieren zu können. Beim entscheidenden Kriterium, nämlich, dass ein Mensch die Auswahl des Ziels trifft, wird nicht weiter ausgeführt, was das genau bedeutet (Gubrud 2015). Unter anderem wird nicht definiert, wer als Bediener des AWS bezeichnet werden soll und welche Funktion und konkreten Aufgaben dieser erfüllt. Dies wirft die Frage auf, ob nicht beispielsweise auch ein Programmierer, der den Datensatz auswählt, anhand dessen das System die Zielerkennung trainiert (zur Bedeutung dieser Begrifflichkeit Kap. 3.3.1), als Bediener aufgefasst werden kann (Roff 2015). Dies führen Altmann und Gubrud (2017, S. 66) zu der Schlussfolgerung: »Es fällt schwer, ein militärisches Robotik- oder KI-Projekt zu identifizieren, das ein AWS genannt werden könnte, aber nicht auch halbautonom genannt werden könnte. Es scheint, dass es keine bedeutsame Unterscheidung zwischen ›halbautonomen‹ und ›autonomen‹ Waffensystemen gibt.«

Überlegungen dieser Art haben dazu geführt, dass sich die Diskussion von technischen Charakteristika und anderen Versuchen, AWS zu definieren, tendenziell wegbewegt und stattdessen eher der Frage zuwendet, welche Qualität die Kontrolle von Waffensystemen durch Menschen aufweist bzw. aufweisen sollte.

2.4 Die Qualität menschlicher Kontrolle über AWS

»Human in the loop« (Mensch in der Entscheidungsschleife) ist ein zentraler Begriff, der häufig im Kontext von Fragen zur Rolle des Menschen beim Einsatz von AWS und zum Ausmaß menschlicher Kontrolle verwendet wird. Der

9 Im Original: »This includes: Semi-autonomous weapon systems that employ autonomy for engagement-related functions including, but not limited to, acquiring, tracking, and identifying potential targets; cueing potential targets to human operators; prioritizing selected targets; timing of when to fire; or providing terminal guidance to home in on selected targets, provided that human control is retained over the decision to select individual targets and specific target groups for engagement.« (DOD 2012, S. 13 f.)

Begriff setzt auf dem Konzept auf, dass Handlungsmöglichkeiten im Zuge einer militärischen Operation in einer Entscheidungsschleife »beobachten, orientieren, entscheiden, handeln« entwickelt und ausgeführt werden. Um die Folgen der Handlung einschätzen und darauf reagieren zu können, wird sodann dieser Zyklus erneut, ggf. mehrfach, durchlaufen.[10]

Die Art und Weise, wie menschliche Kontrolle über ein unbemanntes Waffensystem ausgeübt wird, wird häufig in drei Kategorien eingeteilt: »human in the loop«, »human on the loop« und »human out of the loop« (Mensch in, auf und außerhalb der Entscheidungsschleife; Tab. 2.1). Ein Waffensystem, bei dem der Mensch außerhalb der Schleife ist, ist somit vollautonom zu nennen. Aber auch eines mit einem Menschen auf der Schleife kann, wenn die Einflussmöglichkeiten des Menschen nur gering sind, praktisch als vollautonomes Waffensystem bezeichnet werden (HRW 2012, S. 2).

Tab. 2.1 Menschliche Rolle bei Zielauswahl und -bekämpfung

Bezeichnung	menschliche Rolle
»human in the loop« Mensch in der Schleife	Mensch gibt Befehl
»human on the loop« Mensch auf der Schleife	Mensch überwacht und kann ggf. überstimmen
»human out of the loop« Mensch außerhalb der Schleife	ohne (bzw. nur geringe) menschliche Mitwirkung

Quelle: HRW 2012, S. 2

Etwas differenzierter geht der Robotiker Noel Sharkey (2016) vor, indem er die Zielauswahl und die Entscheidung für einen Angriff getrennt betrachtet und je nachdem, welche Rollen hierbei Mensch und Maschine spielen, fünf Kategorien definiert (Tab. 2.2). Kategorie 1 und 2 entsprechen der Zuschreibung »in der Schleife«, wobei man argumentieren kann, dass Kategorie 1 im Zeitalter von computergestützten Bildaufbereitungs- und Bilderkennungsverfahren in der Praxis nur noch eine untergeordnete Rolle spielt. Die Kategorien 3 und 4 entsprechen »auf der Schleife«, wobei hier der Unterschied zwischen einer aktiv zustimmenden und einer passiveren, bloß überstimmenden Rolle des Menschen liegt.

Eine der Stärken des Konzepts »in, auf oder außerhalb der Schleife« und der Hauptgrund für seine große Verbreitung ist, dass es für Laien intuitiv verständlich erscheint. Allerdings ist es bei Weitem nicht differenziert genug, um das

10 Im englischen Sprachraum ist vom OODA-Loop (»observe«, »orient«, »decide«, »act«) die Rede (Wikipedia 2009b).

komplexe Verhältnis von Menschen, die mit immer intelligenter werdenden Maschinen interagieren, im Detail zu beschreiben.

Tab. 2.2 Rolle von Mensch und AWS bei Zielauswahl und Angriffsentscheidung

Kategorie	Zielauswahl	Angriffsentscheidung	
1	Mensch	Mensch	
2	AWS schlägt vor, Mensch wählt aus	Mensch	»in der Schleife«
3	AWS	AWS, Mensch muss zustimmen	»auf der Schleife«
4	AWS	AWS, Mensch kann ggf. überstimmen	
5	AWS	AWS	»außerhalb der Schleife«

Quelle: Sharkey 2016

Hinzu kommt, dass es auf verschiedenen Ebenen multiple, teils ineinander verschlungene Schleifen gibt, die zum Großteil unter Mitwirkung komplexer technischer Systeme durchlaufen werden: von der Formulierung von Kriegszielen auf eher militärstrategischer Ebene, deren Priorisierung, der Missionsplanung und Vorauswahl von Zielen bis hin zur Wahl der Wirkmittel sowie Durchführungsplanung auf taktischer Ebene. Welche davon gemeint ist, wenn konstatiert bzw. gefordert wird, dass immer ein »Mensch in der Schleife« ist bzw. sein müsste, ist vielfach unklar. Daher ist das Konzept der »Schleife« nicht ausreichend, um ein Mindestmaß an menschlicher Kontrolle über Waffensysteme zu definieren.

Wie schwierig es ist, dies präzise zu fassen, wird in Kapitel 9 erläutert, wo die internationalen Verhandlungen zu autonomen Waffensystemen im Rahmen der CCW beleuchtet werden. Dort spielt das Konzept der menschlichen Kontrolle eine zentrale Rolle. Die konzeptionellen Schwierigkeiten spiegeln sich auf sprachlicher Ebene in dem Bemühen, sich auf konkrete sprachliche Formulierungen zu einigen, z. B. in Forderungen nach »meaningful human control« oder einem »appropriate level of human judgement«.

Kasten 2.3 AWS in Platos Höhle

Laut der Erkenntnistheorie, einem Teilgebiet der Philosophie, haben weder Menschen noch Maschinen einen direkten Zugang zu Objekten in der realen Welt, sondern sie kennen sie nur vermittelt durch ihren Wahrnehmungsapparat. Das heißt, die Repräsentationen, die in den Köpfen und Datenräumen entstehen, sind die Wirklichkeit, wie wir (bzw. die Maschinen) sie erfahren. Und da uns die Welt nur mittelbar zugänglich ist, besteht immer auch die Möglichkeit, dass wir uns über ihre Beschaffenheit irren können. Aus diesem Problem gibt es keinen Ausweg, wie bereits Plato mit seinem Höhlengleichnis (siehe z. B. Wikipedia 2003a) eindrucksvoll gezeigt hat. Die menschliche (wie die maschinelle) Wahrnehmung ist begrenzt, genau wie die der in der Höhle Gefangenen, die lediglich die Schatten an der Höhlenwand sehen können und diese Schatten für die Wirklichkeit ansehen.

Im Kontext von AWS ist dies äußerst relevant und durchaus keine müßige Metaphysik: Wenn die Ziele, die ein AWS angreift, immer den Realweltobjekten oder -personen entsprächen, die Menschen anzugreifen beabsichtigten, gäbe es wenig Grund zur Besorgnis. Tatsächlich sind jedoch diese »Ziele« lediglich interne Repräsentationen des Systems, die aus Sensordaten mit rechnergestützten Verfahren erzeugt werden. Dabei muss das System mit Unschärfen und Unsicherheiten umgehen, oft in der Form, dass vermeintlich kleine Restgrößen vernachlässigt werden. Aus: »Diese Infrarotsignatur entspricht zu 95 % der eines Panzers vom Typ X« wird dann: »Dies ist ein gegnerischer Panzer«. Um einem AWS mitzuteilen, welche Ziele es angreifen soll, müssen ihm zudem Zielspezifikationen übermittelt werden – durch einen menschlichen Bediener oder durch ein anderes System. Auch dies ist ein Prozess, der vielfältige Gelegenheiten für Fehler bietet.

Da am Ende der Kette die Einwirkung von Waffengewalt auf Objekte bzw. Personen in der realen Welt steht, bleibt nur die – wie ausgeführt – möglicherweise trügerische Hoffnung, dass es eine genügend starke Kopplung gibt zwischen der Modellwelt des Systems, das Gewalt anwendet, und der realen Welt, in der die Gewaltanwendung geschieht.

Quelle: Altmann/Gubrud 2017, S. 48 ff.; Gubrud 2015

3 Technische Grundlagen von Autonomie

Obwohl die aktuell zu beobachtende gesteigerte Leistungsfähigkeit unbemannter Systeme auch erheblich durch die jüngsten Fortschritte in hardwarebasierten Technologiefeldern (Leichtbau, Miniaturisierung von Komponenten, neue Materialien, Antriebstechnik, Energieversorgung, Computer- und kommunikationstechnische Hardware, Sensoren, Aktuatoren) bedingt ist (einen Überblick zu diesen Technologiefeldern gibt TAB 2011), wird der Schritt zu autonomen Systemen entscheidend durch Software getrieben (»autonomy is primarily a software endeavour«) (DSB 2012, S. 22).

Nach einem Blick auf Autonomie aus informationstechnischer Sicht werden im Folgenden autonome Funktionen in aktuellen militärischen Systemen näher betrachtet. Für die weitere Entwicklung von Autonomie in Waffensystemen sind computer- und datengestützte Verfahren wesentlich, die unter dem Schlagwort künstliche Intelligenz subsumiert werden können. Hierzu gehören insbesondere moderne Verfahren des maschinellen Lernens, deren Möglichkeiten und Grenzen hinsichtlich ihrer Leistungsfähigkeit thematisiert werden.

3.1 Autonomie aus informationstechnologischer Sicht

Aus informationstechnologischer Sicht ist Autonomie die Fähigkeit eines rechnergestützten Systems, selbstständig aus Daten, die sowohl durch Programmierung vorgegeben als auch aus der Umwelt mittels Sensoren gewonnen sein können, zielgerichtete Pläne und Aktionen zu generieren. Hierfür müssen Wahrnehmung, Entscheidungsfindung sowie Ausführung von Aktionen integriert werden (Boulanin/Verbruggen 2017, S. 7 ff.).

Wahrnehmung besteht aus den beiden Schritten Datensammeln mittels diverser Sensoren (z. B. optische, akustische, chemische) sowie Zusammenführung und Auswertung dieser Daten mittels Analysesoftware. Die Identifizierung von Objekten erfolgt meist durch Mustererkennung bzw. Abgleich mit vorgegebenen Profilen. Dies kann an Bord eines AWS oder aber durch externe Systeme erfolgen.

Die Entscheidungsfindung durch das Kontrollsystem eines autonomen Systems kann relativ simpel sein und beispielsweise auf einfachen Wenn-dann-Regeln beruhen, wie bei einer Landmine, die explodiert, wenn das auf ihr lastende Gewicht einen vorbestimmten Schwellenwert überschreitet. Bei ausgefeilteren Systemen ist ein Datensatz hinterlegt, der die Umwelt repräsentiert nebst Regeln, wie diese sich mit oder ohne Einwirkung durch das AWS verändert (Weltmodell). Hinzu kommt eine Belohnungsfunktion, die angibt, inwieweit ein gewünschter Zustand realisiert worden ist (z. B. die energieeffizienteste Route zu

einem Ziel), sowie ein System, das Handlungsalternativen generiert und diese mit der Belohnungsfunktion abgleicht, um die beste Möglichkeit zu ermitteln. Solche Systeme können äußerst flexibel sein. Insbesondere ist es nicht erforderlich, alle Eventualitäten, mit denen das System im Betrieb konfrontiert werden könnte, in der Designphase des Systems vorzugeben.

Aktionen können durch physische Aktuatoren (z. B. Motoren) vermittelt werden. Dies sind quasi die Muskeln, die es den Endeffektoren (dies können Räder, Beine, Flügel, aber auch Waffen sein) erlauben, physikalische Kraft auf die Umgebung auszuüben. Es sind allerdings auch virtuelle Aktuatoren denkbar, z. B. Softwareprogramme, die bestimmte Aktionen durchführen wie beispielsweise das Blockieren eines Schadcodes bei einem Virenschutzprogramm. Ganz wesentlich für autonomes Agieren sind Lern- und Adaptationsmechanismen, die ein System befähigen, sich an verändernde Umgebungen anzupassen bzw. neue Verhaltensweisen zu erwerben, damit es robust und unfallfrei auf neue Situationen oder plötzliche Störungen reagieren kann (TAB 2016, S. 102).

3.2 Autonome Funktionen aktueller militärischer Systeme

Autonome Funktionen werden derzeit bereits in diversen militärischen Systemen genutzt. Im Folgenden wird der Stand der Technik bei bereits eingesetzten Systemen sowie in FuE-Projekten in vier relevanten Bereichen näher beleuchtet: Mobilität, Zielerkennung bzw. Zielbestimmung, Informationsgewinnung sowie Fähigkeit zur Zusammenarbeit.

3.2.1 Autonomie für Mobilität

Eine Funktion im Bereich Mobilität, die heutzutage routinemäßig autonom ausgeführt werden kann, ist das Verfolgen eines vorausfahrenden (bzw. -fliegenden oder -gehenden) Fahrzeugs oder eines Soldaten (oft »follow me« genannt). Technisch ähnlich ist dies dem »homing in«, d. h. dem Anflug auf ein vorbestimmtes Ziel, das von vielen modernen Flugkörpern selbstständig durchgeführt werden kann. Für beides ist die Voraussetzung, dass das entsprechende Ziel bzw. das Führungsfahrzeug zuverlässig identifiziert und getrackt wird. Eine zweite Funktion, bei der die Autonomisierung bereits weit fortgeschritten ist, ist der Start bzw. die Landung von Fluggeräten. Augenscheinlich ist der Stand der Technik in diesem Bereich so weit, dass menschliche Piloten hinsichtlich Präzision und Zuverlässigkeit von autonomen Systemen übertroffen werden (Boulanin/Verbruggen 2017, S. 23). Mit der »X-47B« (Northrop Grumman 2015) wurden autonome Starts und Landungen auf einem Flugzeugträger auf hoher See demonstriert. Moderne UAVs, wie der »Global Hawk«, fliegen in

allen Phasen autonom – bis hin zur Fortbewegung auf dem Rollfeld (»taxiing«) (Williams 2006, S. 4). Sense-and-avoid-Systeme zur Vermeidung von Kollisionen mit anderen Flugobjekten sind u. a. für die Erlaubnis, in zivilem Luftraum zu fliegen, unerlässlich. Derzeit stößt die Technik bei unübersichtlichen Situationen mit einer Vielzahl von zu beachtenden Objekten noch an Grenzen. An einer Verbesserung dieser Systeme wird intensiv geforscht.

Die wichtigste Fähigkeit für die selbstständige Mobilität eines AWS ist Navigation, d. h. die Bestimmung des gegenwärtigen Aufenthaltsorts, die Planung einer Route im Einklang mit der Mission sowie die Verfolgung dieser Route. Im einfachsten Fall bewegt sich das System von einem vorgegebenen Punkt zum nächsten (»waypoint navigation«). Neuere Systeme können ohne vorgegebene Wegmarken selbstständiger planen, jedoch mit vom Operator vorgegebenen Parametern (z. B. maximale Geschwindigkeit, Flughöhe).

3.2.2 Autonomie für Zielerkennung/Zielbestimmung

Die simpelste Form der Zielerkennung wird seit den 1970er Jahren in automatisierter Zielerkennungssoftware implementiert. Sie beruht auf der Detektion von Signalen (z. B. Radar, optisch, akustisch) und dem Vergleich mit abgespeicherten Signaturen. Werden mehrere Ziele detektiert, können sie mit vordefinierten Kriterien (je nach Einsatzbedingungen) priorisiert werden. Solche Systeme können das völkerrechtliche Unterscheidungsgebot lediglich auf primitive Weise berücksichtigen (indem nur Ziele identifiziert werden, die der Signatur entsprechen, die charakteristisch für das intendierte militärische Ziel ist). Darüber hinausgehende Anforderungen des HVR können durch sie nicht erfüllt werden (u. a. die Einschätzung, ob sich das Ziel »hors de combat« befindet oder ob unverhältnismäßig große zivile Verluste zu befürchten sind, Kap. 7.2).

Derzeit wird an KI-gestützten Systemen zur Zielerkennung gearbeitet, um die Limitationen bestehender Software zu umgehen; so z. B. im Programm »Target Recognition and Adaption in Contested Environments« der Defense Advanced Research Projects Agency (DARPA o. J.a).[11] Aus zwei Gründen sind die Fortschritte in diesem Bereich noch eher moderat: Zum einen werden hierfür große und qualitativ hochwertige Datensätze benötigt, die alle möglichen Variationen der Einsatzbedingungen abdecken, um die Systeme zu trainieren. Diese Daten sind in der erforderlichen Menge und Qualität schwierig zu erzeugen bzw. zu beschaffen. Zum anderen bestehen erhebliche Schwierigkeiten hinsichtlich der Vorhersagbarkeit und Verlässlichkeit der durch KI-Systeme generierten Klassifikationen.

11 Die DARPA ist eine dem US-Verteidigungsministerium unterstellte Agentur für Forschungsprojekte im Verteidigungsbereich.

3.2.3 Autonomie für Informationsgewinnung

Die automatisierte Detektion von Objekten und Ereignissen ist etablierter Stand der Technik, sofern die Aufgabe klar strukturiert ist: z. B. die automatische Erkennung von Minen oder Sprengfallen (»improvised explosive device« – IED) oder das Aufspüren von Eindringlingen in ein Sperrgebiet (z. B. das UGS »Mobile Detection Assessment and Response System« – MDARS). Auch die Ermittlung des Ursprungsorts von Gewehr/Geschützfeuer kann mit hoher Präzision erfolgen.

Weit verbreitet, insbesondere bei Unterwassersystemen und zunehmend auch bei fliegenden Systemen, ist die Fähigkeit, aus Sensordaten (z. B. optische, Ultraschall, Radar) dreidimensionale Karten der Umgebung zu erstellen. Moderne Systeme zur Raketenabwehr wie das israelische »Iron Dome« können Bedrohungsanalysen anhand vorgegebener Kriterien autonom durchführen und anhand des vorausberechneten Einschlagortes der Raketen bzw. Granaten angepasste Gegenmaßnahmen vorschlagen. Wenn die Bedrohung als gering eingeschätzt wird, weil beispielsweise keine militärische oder zivile Einrichtung im Detonationsgebiet liegt, kann zur Einsparung von Munition auch darauf verzichtet werden, den Flugkörper zu bekämpfen (Raytheon Missiles & Defense o. J.a).

In offeneren Situationen sind die autonomen Fähigkeiten zur Objekterkennung in heute genutzten Systemen dagegen noch eher rudimentär. So kann beispielsweise das UAV »ScanEagle«, das zur Detektion von militärisch relevanten Objekten auf See verwendet wird, aktuell lediglich Wasser von Nichtwasser unterscheiden. Eine nähere Bestimmung oder Unterscheidung von Klassen von Objekten ist nicht möglich (Boulanin/Verbruggen 2017, S. 28). Die meisten heute genutzten Systeme verfügen nicht über die Fähigkeiten zur weitergehenden Analyse der gewonnenen Sensordaten. Diese müssen über eine breitbandige Datenverbindung an das Lagezentrum übermittelt werden, wo die Auswertung überwiegend durch menschliche Fachkräfte vorgenommen wird, was bei der riesigen Menge an typischerweise anfallendem Bild- bzw. Videomaterial eine große Herausforderung ist.

Eine Entwicklung der jüngeren Zeit sind Big-Data-Analysen zum Auffinden von Mustern in großen, heterogenen Datenbeständen. Aufgrund der hohen Anforderungen an die Rechnerleistung werden derartige Analysen üblicherweise nicht an Bord von mobilen Systemen durchgeführt, sondern in stationären Rechenzentren. Berichten zufolge sollen beispielsweise die USA die Metadaten von 55 Mio. pakistanischen Mobiltelefonen ausgewertet haben, um aufgrund bestimmter Muster Al-Kaida-Mitglieder bzw. -Kuriere zu identifizieren, zu lokalisieren und auf dieser Grundlage Drohnenangriffe zu planen (Robbins 2016).

3.2.4 Autonomie für die Fähigkeit zur Zusammenarbeit

Hierunter fallen alle Fähigkeiten, die es einem System gestatten, in Verbindung mit einem anderen technischen System (»machine-machine teaming«) oder einem menschlichen Operator (»human-machine teaming) zu operieren.

Eine bereits in der Praxis genutzte Basisfunktion des »machine-machine teaming« ist die Fähigkeit, Informationen zu teilen: Die Systeme sind vernetzt und nutzen Sensor- und andere Daten gemeinsam, arbeiten ansonsten aber unabhängig voneinander. Deutlich anspruchsvoller sind Formen der kollaborativen Autonomie, d. h., mehrere Systeme koordinieren ihre Aktionen, um ein gemeinsames Ziel zu verfolgen. Hierfür ist eine übergeordnete Steuerung des kollektiven Systems (»system of systems«) notwendig. Experten gehen davon aus, dass dies in den nächsten Jahren realisiert werden wird und zu neuen operativen Fähigkeiten autonomer Systeme (Stichwort: Schwarmtaktiken) führen kann (Arquilla/Ronfeldt 2000; Scharre 2014b).

Einige Ansätze zur Kollaboration werden aktuell entwickelt, die sich derzeit vorwiegend im Versuchs- und Demonstrationsstadium befinden:

- Koordinierte Bewegung in unterschiedlichen Formationen wurde beispielsweise in Flugtests des US-amerikanischen UAV »UTAP-22« der Kratos Defense & Security Solutions, Inc. demonstriert (White 2015).
- In einigen FuE-Projekten wird sich mit kollaborativen großräumigen Aufklärungsmissionen beispielsweise durch eine große Anzahl kleiner, kostengünstiger UAVs, u. a. im Projekt »Perdix«, befasst. Bei einer Demonstration dieses Projekts gelang es, 103 Mikrodrohnen aus einem fliegenden Kampfjet heraus freizusetzen, die anschließend als koordinierter Schwarm diverse Manöver durchführten (DOD 2017c).
- Anti-Access-and-Area-denial-Manöver (A2/AD) wurden beispielsweise im US-amerikanischen Projekt »Control Architecture for Robotic Agent Command and Sensing« (»CARACaS«) demonstriert: In einem Feldversuch kooperierte eine Flotte von 13 Booten, überwacht von lediglich einem menschlichen Bediener, um ein gegnerisches Boot zu identifizieren, zu stellen und einzukreisen (Tucker 2016).
- Entwickelt werden auch Funktionen für koordinierte Angriffe, bei denen z. B. Ziele zwischen mehreren beteiligten AWS untereinander verteilt werden bzw. das Vorgehen abgestimmt wird. Beispielsweise soll der für Einsätze gegen Schiffe in Entwicklung befindliche US-amerikanische Antischiffsflugkörper (»long range anti-ship missile« – LRASM) über solche Fähigkeiten verfügen (Lockheed Martin o. J.).

Für »human-machine teaming« relevante Fähigkeiten sind die bereits erwähnten koordinierten Bewegungen, wie das »follow me« oder der Formationsflug. Darüber hinaus können heutige Systeme relativ einfache vorprogrammierte

Manöver ausführen, etwa das Markieren von Zielen, die Aufklärung und Bewertung der Wirkungen von ausgeführten Schlägen oder das Abfeuern von Waffen auf Befehl des Piloten. Darüber hinausgehende, in Richtung echte (Peer-to-peer-)Kooperation gehende Fähigkeiten sind noch in einem relativ frühen Entwicklungsstadium. Die Hauptschwierigkeit, die hierfür überwunden werden muss, sind die Beschränkungen, denen die Mensch-Maschine-Kommunikation unterliegt. Daher sind verbesserte visuelle bzw. taktile Interfaces Gegenstand der Forschung. Die Königsdisziplin, an der Maschinen bislang noch scheitern, ist das Verständnis von natürlich gesprochener Sprache über simple Befehlsphrasen hinaus. Trotz beeindruckender Fortschritte in der Computerlinguistik beispielsweise beim Umsetzen von gesprochener in geschriebene Sprache oder bei Übersetzungen sind Maschinen nach wie vor nicht in der Lage, einem Gespräch zwischen Menschen zu folgen und auf abstrakter Ebene zu verstehen, wovon die Rede ist (Krischke 2018).

3.3 Künstliche Intelligenz als Schlüsseltechnologie

Für die Fortentwicklung der allermeisten zuvor beschriebenen Fähigkeiten in Richtung weitergehender Autonomie werden derzeit primär Methoden angewandt, die unter dem Oberbegriff künstliche Intelligenz subsumiert werden können. Der Begriff KI ist nicht unproblematisch, da damit computergestützte Verfahren vermenschlicht und Konnotationen transportiert werden, die für eine rationale Diskussion der Möglichkeiten und Begrenzungen der technologischen Leistungsfähigkeit jetzt und in absehbarer Zukunft nicht hilfreich sind.[12] Wegen der großen Verbreitung und Anschlussfähigkeit an die aktuelle wissenschaftliche und gesellschaftliche Debatte wird der Begriff in dem hier vorliegenden Bericht dennoch verwendet. Dass auch einige Informatiker sich mit dem Begriff etwas unwohl fühlen, illustriert das Bonmot: »Sobald etwas funktioniert, hören wir auf, es ›KI‹ zu nennen, sondern sagen stattdessen ›Software‹« (Buchanan/Miller 2017).

Der Begriff KI stammt aus der Informatik und Robotik und bezeichnet Forschungsrichtungen, die darauf abzielen, menschliche Fähigkeiten durch computergestützte Verfahren nachzuahmen. Dies betrifft Basisfähigkeiten wie z. B. das Lesen von Handschriften, das Verstehen gesprochener Sprache, das Erkennen von Objekten bzw. Personen auf Bildern und Videos bis hin zu spezielleren Aufgaben wie das Meistern logikbasierter Spiele wie Schach und Go, das Übersetzen von Texten in andere Sprachen, das Entwerfen von Handelsstrategien an

12 Aus diesen Gründen verwendet beispielsweise das iPRAW (iPRAW 2017b) diesen Begriff nicht, sondern propagiert die Nutzung des Terminus »computational methods« (computergestützte Verfahren).

Aktienmärkten, das Prognostizieren von Rückfallquoten bei Häftlingen und nicht zuletzt das Fahren von Automobilen im öffentlichen Straßenverkehr.

Kasten 3.1 Schwache und starke KI

Im Bereich der KI wird oft zwischen schwacher KI (enger KI) und starker KI (genereller KI) unterschieden. Bei schwacher KI wird sich mit relativ eng gesteckten, spezialisierten Aufgaben in einer bestimmten Anwendungsdomäne beschäftigt. Alle heutigen Anwendungen sind der schwachen KI zuzuordnen. Starke KI würde menschenähnliche Intelligenz über ein breites Spektrum von Domänen bedeuten oder sogar menschliche kognitive Fähigkeiten übertreffen. Ein mit starker KI ausgestattetes System wäre in der Lage, vorab unbekannte Aufgaben in unbekannten Umgebungen zu lösen.

Ob starke KI jemals durch technische Systeme zu erreichen ist, ist in Expertenkreisen umstritten. Umfragen zufolge ist eine Mehrheit der KI-Forscher der Ansicht, dass dies durchaus möglich ist (UNIDIR 2018b, S. 7). Eine offene Frage ist, ob dafür eine Form von Bewusstsein, Selbstwahrnehmung bzw. Empfindungsvermögen erforderlich ist (z. B. TAB 2016, S. 103 f.).

Die Entwicklung von KI vollzog sich bisher in zwei Wellen (GAO 2018, S. 16 f.; Launchbury o. J.): Die Anfänge der KI-Forschung, beginnend in den 1950er Jahren, beruhten auf regelbasierten Expertensystemen. Diese waren in der Lage, eng definierte Probleme zu lösen, wie z. B. die Ermittlung der Höhe der geschuldeten Einkommensteuer. Sie verfügten jedoch im Allgemeinen nicht über die Fähigkeit zum eigenständigen Lernen und konnten nicht adäquat mit unvorhergesehenen Situationen umgehen.

Seit den 1990er Jahren ist die zweite Welle in vollem Gange. Deren Grundlagen sind fortgeschrittene Methoden der Statistik und vor allem die rechnergestützte Auswertung riesiger Datenmengen (Big Data) sowie das sogenannte Maschinenlernen (»machine learning«, »deep learning«). Erfolgreich sind diese Methoden insbesondere beim Klassifizieren und Gruppieren von Daten, z. B. bei der Erkennung von Handschriften. Den Systemen ist es allerdings nicht möglich, Ergebnisse in einen weiteren Kontext zu stellen bzw. zu interpretieren.

Eine Richtung aktueller Forschung hat zum Ziel, eine dritte Welle der KI zu begründen, die Vorteile der ersten und zweiten Welle kombinieren und gleichzeitig deren Defizite auffangen soll (Launchbury o. J.). Allerdings stehen die angestrebten Fähigkeiten des Verständnisses abstrakterer Zusammenhänge, der Konzeptualisierung, des logischen Folgerns sowie der Herstellung von Erklärbarkeit noch relativ weit am Anfang.

Aufgaben, die sich nach dem heutigen Erkenntnisstand für die Lösung durch KI-basierte Verfahren besonders eignen, weisen einige spezifische Charakteristika auf:

- Es ist ein möglichst perfektes mathematisches Modell oder eine Simulation der Aufgabe verfügbar.
- Für das Fortschreiten auf das angestrebte Ziel hin existieren kurzfristige Indikatoren.
- Es ist eine große Menge an Daten vorhanden, z. B. mit Beispielen, wie die Aufgabe von Menschen bewältigt wurde.
- Die Aufgabe erfordert kein Modell der Welt, in die die Aufgabe eingebettet ist (kein »common sense«) (Brundage et al. 2018, S. 13).

Für etliche Alltagsaufgaben werden KI-Systeme bereits eingesetzt. Hierzu gehören etwa Empfehlungssysteme, die beispielsweise Konsumenten Produkte und Dienstleistungen auf Grundlage früherer Entscheidungen vorschlagen, Suchmaschinen und Spamfilter, Systeme zur Spracherkennung und persönliche Assistenzsysteme (z. B. »Alexa«, »Cortana«, »Google Assistant«, »Siri«), die Erkennung von Personen auf Fotos, die Erkennung von Handschriften, Fremdsprachenübersetzung, Betrugserkennung aus Nutzungsdaten von Kreditkarten und anderen Bezahlsystemen (Royal Society 2017, S. 21 ff.).

3.3.1 Maschinelles Lernen

Die beeindruckenden Fortschritte, die im Feld der KI in jüngster Zeit erzielt worden sind, sind ganz entscheidend durch Durchbrüche bei Methoden des maschinellen Lernens (ML) ermöglicht worden. Dabei handelt es sich allgemein gesprochen um Algorithmen, die sich datengetrieben verbessern können (Royal Society 2017). Es gibt verschiedene Verfahren, die für ML angewendet werden. Die wichtigsten sind (Royal Society 2017, S. 20):

- »Supervised learning«: Hierbei werden die gewünschten Outputkategorien vorgegeben (beispielsweise für die Erkennung von handgeschriebenen Zahlen die Ziffern 0 bis 9). Die Input- bzw. Trainingsdaten (z. B. Bilder von handgeschriebenen Ziffern) sind korrekt (in der Regel von Menschen) gemäß den Kategorien gelabelt (»dieses Bild zeigt eine 4«). Im Lernprozess soll der Algorithmus die Kategorisierungen nachvollziehen, um diese dann anschließend auf unbekannte Daten übertragen zu können.
- »Unsupervised learning«: Anhand der statistischen Eigenschaften der Inputdaten werden Outputkategorien vom Algorithmus selbst entwickelt (z. B. Einteilung von Konsumenten in Marktsegmente anhand vorliegender Daten zu Kaufentscheidungen). Die Kategorien sind im Allgemeinen nicht intuitiv für Menschen verständlich, hierfür ist eine Interpretationsleistung erforderlich. Im genannten Beispiel könnte ein Mensch diese Interpretation

vornehmen und etwa Marktsegmenten charakteristische Gemeinsamkeiten zuordnen und diese benennen (z. B. Gruppe 1: technoaffin, Gruppe 2: komfortbetont etc.).

- »Reinforcement learning«: Ein als Belohnung interpretierbarer Parameter wird so eingestellt, dass er umso größer wird, je näher der Output einem gewünschten Ergebnis kommt. Der Lernprozess besteht darin, den Output systematisch so zu verändern, dass die Belohnung maximiert wird. Ein Anwendungsbeispiel ist das Finden des besten Zugs in einer Schachpartie. Die »Belohnung« ist in diesem Beispiel ein Indikator dafür, wie vorteilhaft die entstehende Stellung eingeschätzt wird.

Ein zentrales Unterscheidungsmerkmal bei den verschiedenen ML-Verfahren besteht darin, ob das Lernen offline oder online geschieht. Bei einem offline lernenden System wird nach Abschluss des Trainings der entstandene Algorithmus einschließlich aller interner Parameter fixiert (eingefroren). Im Praxiseinsatz ändern sich diese Parameter nicht mehr. Im Gegensatz dazu setzen online lernende (selbstlernende) Systeme das Training auch im laufenden Betrieb fort. Ein wesentlicher Vorteil selbstlernender Systeme besteht darin, dass sie in der Praxis Erfahrungen sammeln und so im Prinzip immer besser werden können. Andererseits steht der gravierende Nachteil, dass selbstlernende Systeme nichtintendierte Verhaltensweisen lernen könnten und die Vorhersagbarkeit ihres Verhaltens im Laufe der Zeit gemindert würde. Daher kam beispielsweise die Ethik-Kommission Automatisiertes und vernetztes Fahren (Ethik-Kommission 2017, S. 30) zu dem Schluss: »Solange bei selbstlernenden Systemen keine hinreichende Sicherheit besteht, dass diese Situationen richtig einschätzen bzw. Sicherheitsanforderungen einhalten können, sollte eine Entkoppelung der selbstlernenden Systeme von sicherheitskritischen Funktionen vorgeschrieben werden. Ein Einsatz von selbstlernenden Systemen ist beim gegenwärtigen Stand der Technik daher nur bei nicht unmittelbar sicherheitsrelevanten Funktionen denkbar«. Da der Waffeneinsatz durch ein AWS offenkundig eine sicherheitskritische Funktion im Sinne der Ethik-Kommission darstellen würde, liegt der Analogieschluss nahe, dass selbstlernende Systeme für kritische Funktionen von AWS ausgeschlossen werden müssen. Nicht nur ethisch, auch völkerrechtlich wären selbstlernende AWS problematisch (Kap. 7). So ist vollkommen unklar, wie die Prüfpflicht nach Artikel 36 ZP I der Genfer Konvention, ob ein neu entwickeltes Waffensystem völkerrechtskonform ist, bei solchen Systemen umgesetzt werden könnte (IKRK 2018a, S. 15 ff.).

3.3.2 Was können KI-Systeme heute leisten?

Diverse Aufgaben, die vor wenigen Jahren noch als schwierig oder sogar unmöglich für Maschinen eingeschätzt wurden, können von heutigen KI-Systemen bewältigt werden. In etlichen spezifischen Bereichen übertreffen die Leis-

tungen von KI-gestützten Verfahren bereits heute menschliche Fähigkeiten, beispielsweise bei der Erkennung von Bildern (He et al. 2015), Handschriften (Markoff 2015) oder Stimmen (Xiong et al. 2016). Regelmäßig gehen Erfolgsmeldungen durch die Medien, dass ein KI-System in dieser oder jener Aufgabe menschliche Fähigkeiten übertroffen habe. So verkündeten beispielsweise im Januar 2018 die Alibaba Group Holding Limited (Najberg 2018) sowie unabhängig davon die Microsoft Corporation (Linn 2018), dass sie einen Algorithmus entwickelt hätten, der in einem standardisierten Test zum Leseverständnis (dem Stanford Question Answering Dataset, SQuAD) besser als Menschen abgeschnitten habe.

Im Folgenden werden einige der herausragenden Beispiele für die Fähigkeiten aktueller KI-Systeme dargestellt.

Schach, Shogi, Go

Seit Jahren bieten strategische Brettspiele wie Schach, Shogi (japanisches Schach) und Go eine ideale Bühne, um die Leistungsfähigkeit von Computerprogrammen in intellektuellen Aktivitäten, die als typisch menschlich angesehen werden, unter Beweis zu stellen. Programme zu entwickeln, die besser als Menschen spielen, galt lange als eine der Grand Challenges der KI. Ein erster Meilenstein wurde 1997 erreicht, als Schachweltmeister Garry Kasparov gegen ein auf dem Supercomputer »Deep Blue« laufendes Programm verlor. Allerdings stützte sich dieses Programm in erheblichem Umfang auf menschliches Expertenwissen, das u. a. aus umfangreichen Bibliotheken mit Eröffnungszügen und Parametern für die Beurteilung von Stellungen bestand (Campbell et al. 2002).

Im Vergleich zu Schach galt Go noch bis vor wenigen Jahren als Domäne, in der die menschliche Überlegenheit über Computerprogramme auf lange Zeit gesichert schien. Ein Hauptgrund dafür ist, dass bei Go viel mehr Zugmöglichkeiten bestehen, sodass die bei klassischen Schachprogrammen angewandte Brute-Force-Methode (Durchprobieren sämtlicher Möglichkeiten im Rahmen der vorhandenen Rechenkapazitäten und Bewertung der so entstehenden Stellungen) an ihre Grenzen stößt.[13] Daher war es eine wissenschaftliche Sensation, als 2016 das auf ML-Methoden (in erster Linie »reinforcement learning«) basierende Programm »AlphaGo« (Silver et al. 2016) den zu dieser Zeit unbestritten stärksten menschlichen Go-Spieler Lee Sedol überzeugend schlug (Wikipedia 2016).

Die mit »AlphaGo« angestoßene Entwicklung wurde unmittelbar mit einem weiteren Entwicklungsschritt, dem »AlphaZero«, fortgesetzt, der zwar deutlich weniger öffentliche Aufmerksamkeit erregte, aus technologischer Sicht aber fast

13 Betrachtet man alle theoretisch möglichen Spielverläufe, so übertrifft Go Schach um den Faktor 10^{237} (eine Eins mit 237 Nullen) (Wikipedia 2008).

noch beeindruckender ist. Dabei handelt es sich um einen Algorithmus, der sowohl Schach als auch Shogi und Go bewältigt hat. Lediglich mit den Regeln des Spiels gefüttert, steigerte er anschließend selbstständig durch Spielen gegen sich selbst seine Spielstärke. Bereits nach wenigen Stunden übertraf er das für Menschen erreichbare Niveau in allen drei Spielen und nach 24 Stunden schlug er das jeweils beste verfügbare konventionelle Programm. »AlphaZero« wird als bedeutender Schritt hin zu einem generalisierten Algorithmus gesehen, der jedes Strategiespiel lernen kann (Campbell 2018; Kasparov 2018; Silver et al. 2017).

Am Beispiel »AlphaZero« kann gut ein wesentlicher Unterschied zwischen Menschen und Algorithmen beim Lernen deutlich gemacht werden. Wenn »AlphaZero« ein neues Spiel lernt, startet er jedes Mal von null: Der Algorithmus kann nicht davon profitieren, dass in der Vergangenheit bereits ein anderes Spiel gelernt wurde. Menschen können im Lernprozess generalisiertere Erkenntnisse gewinnen, die etwa durch Analogieschlüsse für neue Aufgaben genutzt werden können.

Computerspiele und Simulationen

Ein weiteres Erfolgsbeispiel dafür, dass ML-basierte Algorithmen menschliche Fähigkeiten erreichen bzw. übertreffen können, sind Computerspiele. Dies wurde beispielsweise für eine breite Palette klassischer Atari-Spiele (z. B. Pong, Space Invaders) gezeigt. Dem Algorithmus wurden lediglich die Bildschirmpixel und der Spielstand übermittelt. Spielstrategien wurden anschließend per »reinforcement learning« vom Algorithmus selbst entwickelt (Mnih et al. 2015).

In letzter Zeit ist die Frage in den Mittelpunkt des Interesses gerückt, wie unterschiedliche Algorithmen zur Erreichung eines gemeinsamen Ziels miteinander bzw. mit Menschen kooperieren können. Bemerkenswert sind hier erste Ansätze, die u. a. beim äußerst populären Multiplayer-Echtzeit-Strategiespiel DOTA II[14] erprobt wurden. So gelang es einem Team aus fünf Bots, genannt »OpenAI Five«, ein Team aus fünf ehemaligen Profispielern zu schlagen, obwohl ihre Reaktionszeit künstlich auf menschliches Niveau herabgesetzt wurde (Hutson 2018).

Im Hinblick auf die praktische Umsetzung von AWS ist die Entwicklung eines KI-basierten autonomen Steuersystems für Flugsimulatoren bemerkenswert. Das System simuliert ein gegnerisches Kampfflugzeug im Luft-zu-Luft-Kampf und scheint selbst für erfahrene Kampfpiloten kaum bezwingbar zu sein (Ernest et al. 2016; Reilly 2016).

14 Benannt nach der 1. Folge »Defense of the Ancients«.

Poker

Eine völlig andere Domäne als Strategiespiele wie Schach ist Poker. Hier liegen buchstäblich nicht alle Informationen auf dem Tisch. Daher müssen Entscheidungen unter unsicheren Annahmen getroffen werden und der Zufall spielt eine wesentliche Rolle. Gute Pokerspieler besitzen daher viel Intuition und ein gutes Verständnis von Psychologie und Verhalten der Gegner. Für eine bestimmte Variante des Pokers (»heads up no limit Texas hold 'em«) wurde ein ML-Algorithmus »DeepStack« entwickelt, der professionelle Pokerspieler bezwingen konnte. Da Entscheidungen in der realen Welt oft unter unsicheren Annahmen getroffen werden müssen, versprechen sich die Entwickler von »DeepStack«, dass ihre Methoden weit über das Pokern hinaus Anwendungsperspektiven finden können (Moravčík et al. 2017; Riley 2017).

Jeopardy!

In der aus den USA stammenden Quizshow »Jeopardy!« werden den Kandidaten Antworten aus diversen Kategorien vorgegeben. Die Aufgabe besteht darin, schneller als die Konkurrenten eine zur Antwort passende Frage zu formulieren. Damit ein Computerprogramm diese Aufgabe bewältigen kann, muss es als Erstes den Sinn von in natürlicher Sprache gestellten Fragen erfassen und sodann in einem Wissensbestand die relevanten Fakten auffinden. Eine solche semantische Suchmaschine ist das Programm »Watson« (Wikipedia 2010a), das bereits 2011 gegen zwei menschliche Jeopardy!-Champions antrat und mit großem Abstand gewann.

Inzwischen werden von »Watson« abgeleitete Programme in einer Vielzahl von Feldern angewandt, u. a. zur Beantwortung von Onlinekundenanfragen, zur Weitergabe von Erfahrungswissen älterer Ingenieure an Nachwuchskräfte oder zur Steuerung eines intelligenten Bewässerungssystems im Weinbau (IBM o. J.). Auch in der Medizin werden enorme Anwendungspotenziale für angepasste Watson-Algorithmen erwartet. Allerdings gab es in diesem Bereich auch Rückschläge. So wurde ein Experiment abgebrochen, bei dem »Watson« Vorschläge zur personalisierten Therapie von Krebspatienten entwickeln sollte, da gravierende Fehler auftraten, die im Ernstfall Patienten empfindlich geschadet hätten (Meier 2018).

3.3.3 Begrenzungen, Schwierigkeiten und Risiken bei KI-Systemen

Den beschriebenen Erfolgen von KI-Systemen stehen beträchtliche technische und operationelle Begrenzungen, Schwierigkeiten und Risiken gegenüber, von denen einige im Folgenden dargestellt werden.

Abhängigkeit von großen Datenbeständen

Die Verfügbarkeit großer und für die konkrete Fragestellung hochwertiger Datenbestände (z. B. beim »supervised learning« korrekt gelabelte Daten) ist von entscheidender Bedeutung für die Qualität der Resultate von ML-Prozessen, oft wichtiger als die verwendeten Algorithmen selbst (Banko/Brill 2001). So hat beispielsweise das Unternehmen Waymo LLC (eine Tochter des Google-Mutterkonzerns Alphabet Inc.) 2018 bereits Daten von über 16 Mio. km autonomer Fahrten auf öffentlichen Straßen gesammelt. Darüber hinaus wurde angekündigt, über 60.000 selbstfahrende Minibusse auf die Straße zu bringen (Hu 2018). Die große Datenmenge ist essenziell, um autonomen Fahrzeugen adäquates Verhalten auch bei selten auftretenden Ereignissen antrainieren zu können.

Wie dies im analogen Fall eines geländegängigen autonomen Militärfahrzeugs geschehen könnte, damit alle Eventualitäten, denen das System im Betrieb ausgesetzt sein könnte, in den entsprechenden Trainingsdaten abgebildet sind, ist gegenwärtig unklar.

Begrenzte Übertragbarkeit von einem auf andere Bereiche

Erfolge von heutigen KI-Systemen in einem bestimmten Bereich können nicht ohne Weiteres auf einen anderen Bereich übertragen werden, auch wenn dieser aus menschlicher Sicht analog zum ersten Bereich erscheint. Dies liegt an einer charakteristischen Eigenschaft von KI-Systemen, die *katastrophales Vergessen* genannt wird. Das bedeutet, dass ein Algorithmus, der gelernt hat, eine bestimmte Aufgabe zu bewältigen, und anschließend für eine neue Aufgabe trainiert wird, seine Kompetenz zur Lösung der ersten Aufgabe verliert. Dies verhindert, dass KI-Systeme kontinuierlich Fähigkeiten hinzugewinnen können, und stellt eine wesentliche Begrenzung für die Erschließung neuer Aufgabenfelder vor allem durch ML-basierte KI dar. An der Überwindung dieses Problems wird derzeit intensiv geforscht (Kirkpatrick et al. 2017; UNIDIR 2018b, S. 6).

Eine ähnlich gelagerte Problematik tritt auf, wenn ein KI-System, das für eine bestimmte Aufgabe entwickelt wurde, für eine – nach menschlichen Maßstäben – geringfügig andere Aufgabe eingesetzt werden soll. Um den Entwicklungsaufwand zu minimieren, könnte man auf die Idee kommen, das bestehende System geringfügig zu modifizieren, um es so an die neue Aufgabe anzupassen. Dies kann allerdings zu unerwünschtem, nicht vorhersehbarem Verhalten des Systems führen, denn vor allem ML-basierte Systeme unterliegen dem sogenannten CACE-Prinzip (»changing anything changes everything«), gemäß dem jede Änderung an Teilen des Systems in schwer vorhersehbarer Weise auf das ganze System durchschlagen kann (Danzig 2018, S. 8; Sculley et al. 2015).

Bias

Algorithmen, ob auf der Basis von ML-Verfahren oder auf andere Weise erzeugt, können eine komplexe Wirklichkeit niemals objektiv, neutral und präzise abbilden, denn sie reflektieren immer die Auswahlentscheidungen, die in ihrem Design getroffen werden müssen.

Allgemein gesprochen liegt ein Bias vor, wenn die Ergebnisse eines algorithmischen Verfahrens systematisch von einem gesetzten Standard abweichen (hierzu und zum Folgenden UNIDIR 2018a). Aus diversen Anwendungsbereichen von ML-gestützten Verfahren sind Beispiele bekannt, bei denen ein Bias zu groben Fehlern und erheblichem Schaden für die Betroffenen geführt hat. Dies reicht von durch Algorithmen vorgeschlagene härtere Haftstrafen für Angehörige bestimmter Ethnien (Fefegha 2018) bis hin zu geringeren Jobchancen für Frauen bei algorithmisch gestützten Auswahlverfahren (Dastin 2018).[15] Die genaue Untersuchung solcher Fälle trägt zu einem besseren Verständnis bei, wie ein Bias entsteht, welche Auswirkungen er hat und wie er eingegrenzt werden kann. Dies liefert wertvolle Hinweise, um die möglichen Effekte von Bias auch bei AWS besser einschätzen zu können.

Es gibt unterschiedliche Arten von Bias: Ein *statistischer* Bias liegt vor, wenn der Output eines ML-Verfahrens die wahre Häufigkeit eines bestimmten Ereignisses nicht im Rahmen vorgegebener Toleranzen widerspiegelt. Beispielsweise könnte ein System zur Abschätzung des Kreditausfallrisikos dieses für bestimmte Kundengruppen systematisch zu hoch einschätzen. Ein *moralischer* Bias tritt hingegen auf, wenn der Output eines ML-Verfahrens etablierten moralischen Normen widerspricht. Beispielsweise könnte das System das Kreditausfallrisiko zwar statistisch korrekt berechnen, aber im Ergebnis bestimmte Kundengruppen, z. B. aufgrund von Geschlecht oder ethnischer Zugehörigkeit, diskriminieren. Dies könnte auftreten, selbst wenn die Information über die Zugehörigkeit zu dieser Gruppe nicht verwendet wurde, etwa weil diese mit anderen verwendeten Merkmalen korreliert.

Ein Bias kann auf unterschiedliche Art und Weise entstehen. Auf der einen Seite kann er systembedingt induziert werden, etwa durch Trainingsdaten, die für den intendierten Einsatzzweck nicht repräsentativ sind, oder durch falsche Modellannahmen im zugrundegelegten Algorithmus. Repräsentative Trainingsdaten für AWS, die sich in Gefechtsfeldern bewegen, die sich hochdynamisch verändern und von gegnerischen Aktionen geprägt sind, sind schwer bis unmöglich zu beschaffen. Um herauszufinden, ob sich ein AWS in allen Einsatzszenarien regelkonform verhält, müsste es in realistischen Umgebungen getestet werden, da bestimmte durch Bias verursachte Fehler sonst ggf. nicht rechtzeitig entdeckt werden können.

15 Weitere Fallbeispiele werden in Lischka et al. 2017 beschrieben.

Auf der anderen Seite können auch auf der Nutzerseite erhebliche Quellen von Bias entstehen. Wenn etwa ein System außerhalb des intendierten Einsatzkontexts verwendet wird (»transfer context bias«), ist oft eine überraschende bzw. fehlerhafte Funktionsweise zu beobachten. Ein Beispiel können AWS sein, die für ein offenes Terrain entwickelt wurden, aber entgegen der Spezifikation in dicht bebautem, urbanem Gelände eingesetzt werden. Schließlich sind auch Fehlinterpretationen durch den Nutzer möglich (»interpretation bias«). Beispielsweise könnte der Output eines Überwachungssystems, der die »Unsicherheit über die Identität einer Person« beschreibt, missverstanden werden als »Wahrscheinlichkeit, dass die Person ein Terrorist ist«. Diese Art von Fehler könnte man eher als Nutzerversagen beschreiben, allerdings spielen auch hier oft technische Elemente, wie das Design der Interfaces, eine tragende Rolle.

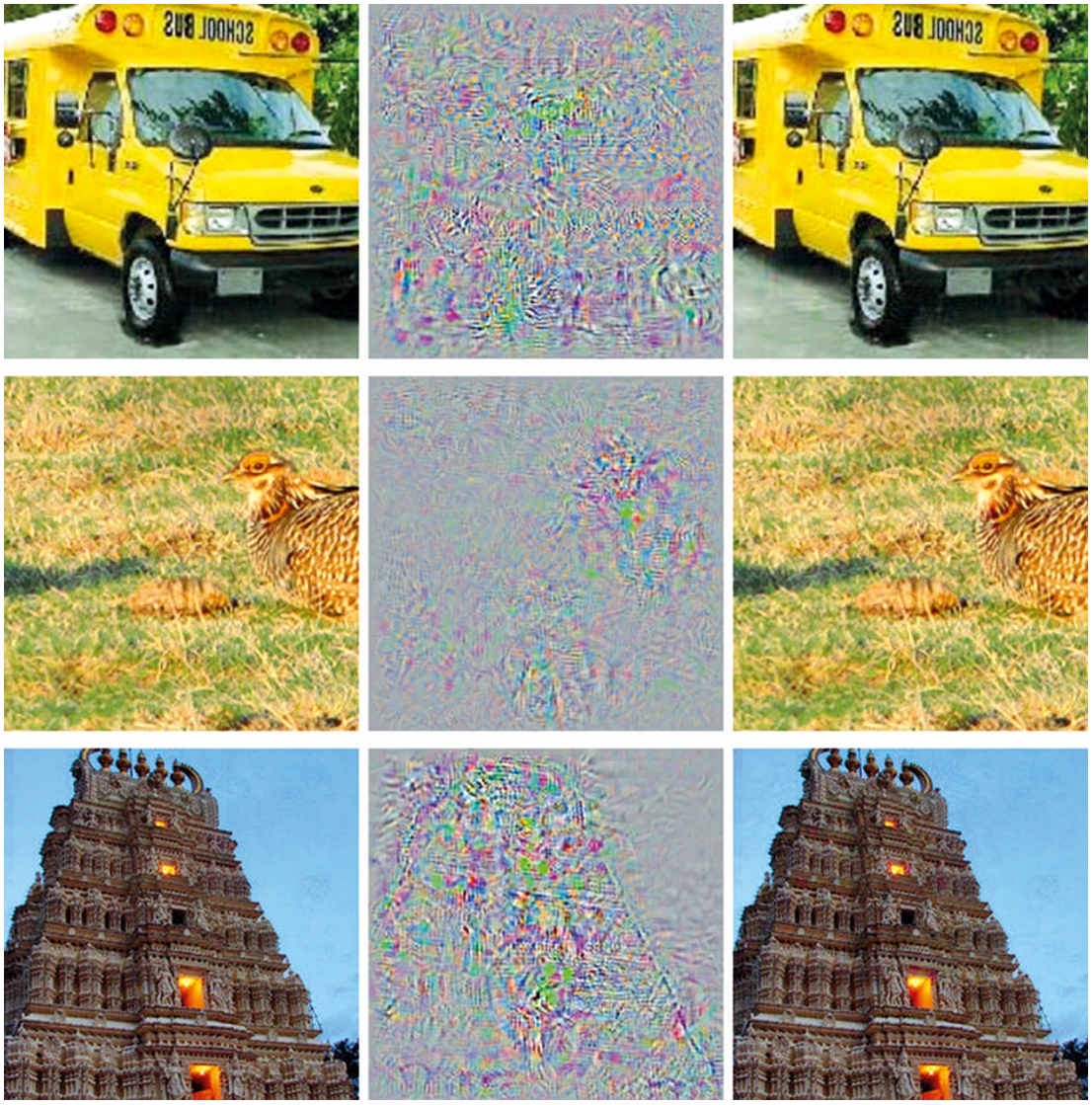
Vorhersagbarkeit und Verlässlichkeit des Verhaltens

Über die beschriebenen Auswirkungen von Bias hinaus besitzen KI-Systeme weitere Charakteristika, die die Vorhersagbarkeit ihres Verhaltens erschweren können. Im Fall von selbstlernenden Systemen, die während ihres Betriebs »im Feld« Erfahrungen sammeln und ihr Verhalten entsprechend anpassen können, ist offensichtlich, dass die Vorhersagbarkeit im Laufe der Zeit abnimmt und früher oder später nicht mehr gewährleistet werden kann.

Aber auch offline lernende ML-Systeme sind bekannt dafür, dass sie schwer vorhersagbares Verhalten produzieren können. So können etwa ML-Algorithmen, beispielsweise zur Bilderkennung, unter Umständen durch minimale Abweichungen des Inputs dazu gebracht werden, ein zuvor korrekt klassifiziertes Bild völlig falsch einzuordnen.

Ein eindrückliches Beispiel dafür zeigt Abbildung 3.1 (Szegedy et al. 2014). Einem korrekt klassifizierten Bild (linke Spalte) wurde eine kleine Störung (mittlere Spalte) überlagert. Obwohl für das menschliche Auge praktisch nicht von den Ausgangsbildern zu unterscheiden, wurden die resultierenden Bilder (rechte Spalte) vom ML-Algorithmus fälschlich als »Vogel Strauß« (Struthio camelus)« klassifiziert. Etliche weitere dieser »adversarial examples« (zu Deutsch etwa »feindliche Beispiele«) wurden generiert (Goodfellow et al. 2015). Im Extremfall reicht bereits die Änderung eines einzigen Pixels aus, um einen ML-Bilderkennungsalgorithmus zu täuschen (Su et al. 2017). Dies könnte im Praxiseinsatz problematische oder sogar katastrophale Folgen haben. Ein drastisches Beispiel wären autonome Autos, die etwa Stoppschilder, die mit kleinen Aufklebern manipuliert wurden, plötzlich als Vorfahrtsschilder interpretieren. Dass dies mehr als ein Gedankenspiel ist, zeigen Versuche mit Verkehrsschildern von Eykholt et al. (Eykholt et al. 2018).

Abb. 3.1 Täuschung eines Algorithmus zur Bilderkennung



Links: korrekt klassifiziertes Bild, Mitte: Differenz zwischen Bild links und rechts, rechts: falsch klassifiziertes Bild. Alle Bilder in der rechten Spalte wurden als »Vogel Strauß« (Struthio camelus) klassifiziert.

Quelle: Szegedy et al. 2014, S. 6

Das Generieren von Beispielen, die ML-Algorithmen täuschen können, hat mittlerweile einen eigenen Forschungszweig begründet, das Adversarial Machine Learning. Dieses hat zum Ziel, Schwachstellen von ML-Algorithmen zu finden, um diese ggf. zu verbessern. Mittlerweile sind diverse Angriffs- und Verteidigungsstrategien entwickelt worden, um ML-Algorithmen zu kompromittieren bzw. genau davor zu schützen. Die grundlegende Anfälligkeit von ML-Algorithmen konnte bisher aber nicht behoben werden (Goodfellow et al. 2017). Selbst

wenn ein ML-Algorithmus aus mathematischer Sicht verlässlich ist, weil er reproduzierbar auf einen identischen Input immer denselben Output ausgibt, wäre dies keineswegs ausreichend, um in der Praxis verlässlich zu funktionieren. Eine Bedingung hierfür wäre, dass ähnliche Inputs zu ähnlichen Outputs führen. Dies ist bei ML-Algorithmen vielfach nicht gewährleistet, weshalb ihr Verhalten oft als *brüchig* beschrieben wird (Pontin 2018).

Blackbox KI

Heutige KI-Verfahren, insbesondere ML-gestützte Verfahren, sind häufig vom Typ Blackbox. Der Input – beispielsweise bei Bilderkennungsverfahren ein Bild – erzeugt einen Output etwa in der Art: »Mit einem Korrelationskoeffizienten von 0,93 fällt der Input in die mit ›Katze‹ beschriftete Kategorie«, ohne dass ein Nutzer oder auch der Entwickler die innere Logik und die einzelnen Schritte, die zu dem Output geführt haben, nachvollziehen kann.

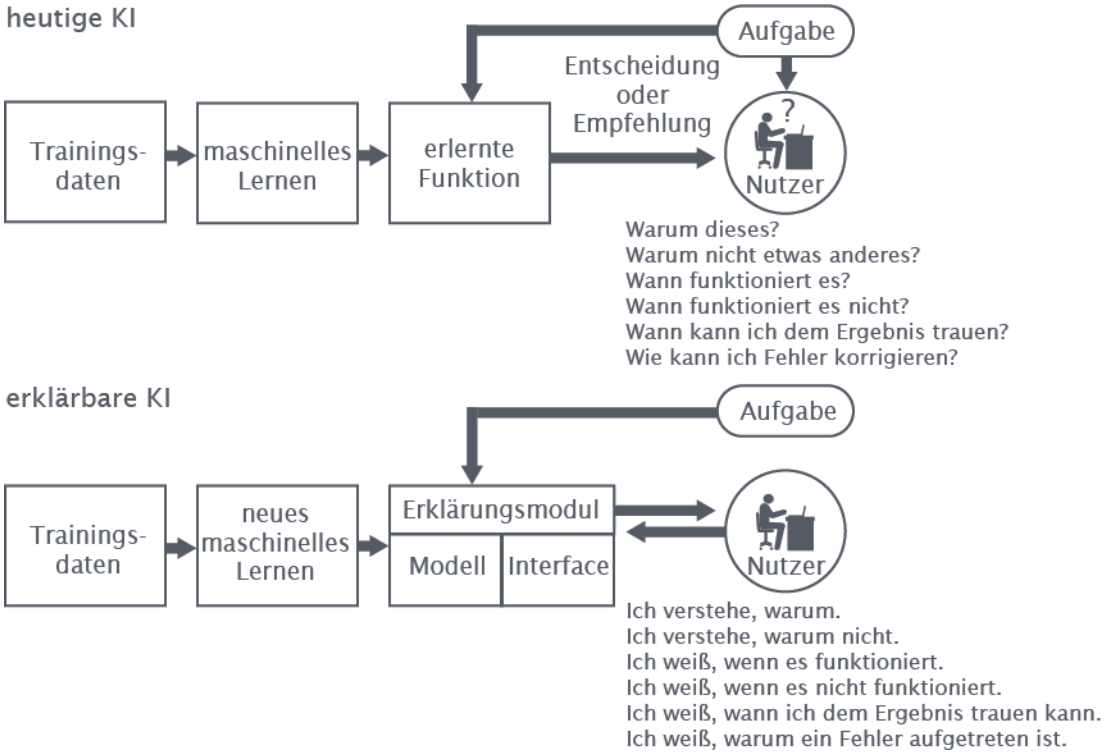
Wie bedeutsam dies ist, hängt vom Kontext ab. Für ein robustes System, das gut abgegrenzt werden kann, mag dies irrelevant sein. Für ein System, das im Kontext eines größeren Systems verwendet wird, könnte dies unlösbare Schwierigkeiten bei der Fehlersuche und -behebung verursachen (Marcus 2018, S. 11). Besonders in Anwendungsbereichen, in denen viel auf dem Spiel steht – wie in der Medizin, im Finanzsektor und natürlich beim Militär –, ist kaum vorstellbar, dass durch ein System generierte Handlungsvorschläge, die nicht nachvollzogen und begründet werden können, umgesetzt werden.

Verschiedene Ansätze sollen hier Abhilfe schaffen und neben dem eigentlichen Output entsprechende Begründungen mitliefern. *Interpretierbare Verfahren* sind so transparent gestaltet, dass ein Nutzer, der über hinreichendes technisches Verständnis bzw. Hintergrundwissen verfügt, die Entstehung des Outputs nachvollziehen und erklären kann. Im Gegensatz dazu erzeugt ein *erklärbares Verfahren* nicht nur einen Output, sondern generiert im Zuge der Berechnungen Symbole (z. B. Wörter oder Visualisierungen), die es dem Nutzer erlauben, Eigenschaften des Inputs dem Output zuzuordnen. Im Beispiel eines Bilderkennungsverfahrens wäre dies etwa: »Es hat Fell, es hat Schnurrhaare und Krallen: Es ist eine Katze«. Dies ist in Abbildung 3.2 im Kontrast zu heutigen Blackboxsystemen illustriert. Ziel dieser *erklärbaren KI* ist es, dem Nutzer zu ermöglichen, die Qualität und die Grenzen des durch die KI generierten Outputs zu bewerten.

Streng genommen liefern aber diese Verfahren keine Erklärungen, sondern sie *ermöglichen* sie lediglich, d. h., es wird charakterisiert, *wie* ein Output zustande gekommen ist, aber nicht *warum* (Doran et al. 2017; Gunning o. J. 2017). Ob diese Interpretationsleistung jemals von Maschinen erbracht werden kann, ist umstritten. Demzufolge ist derzeit noch nicht absehbar, ob diese Ansätze die Erwartungen erfüllen werden, eine Brücke zwischen Maschinensprache und

menschlicher Sprache bzw. menschlichem Verständnis zu schlagen (iPRAW 2017b).

Abb. 3.2 Erklärbare KI



Quelle: nach GAO 2018, S. 19

Problem der Verifizierung und Zertifizierung

Bevor militärische Systeme in sicherheitskritischen Bereichen in der Praxis stationiert und eingesetzt werden, müssen sie strenge Prüfprozeduren durchlaufen, damit sichergestellt ist, dass sie wie intendiert funktionieren. Eine etablierte Methode, um dies nachzuweisen, ist, die Systeme allen denkbaren Umständen auszusetzen und zu überprüfen, ob sie adäquat darauf reagieren. Dies ist für KI-Systeme schwierig zu realisieren, insbesondere wenn diese (Boulanin/Verbruggen 2017, S. 68 ff.)

- in zunehmend komplexen und dynamisch sich ändernden, schwer vorhersehbaren Umgebungen eingesetzt werden sollen,
- mit anderen autonomen Systemen oder mit Menschen interagieren,
- selbstlernende Funktionen aufweisen.

Derzeit gibt es keine Konzepte bzw. Standards, wie solche hochkomplexen autonomen Systeme verifiziert und zertifiziert werden sollen. Dies betrifft sowohl

die Algorithmen bzw. die Software als auch die Integration in ein cyberphysikalisches System (z. B. ein AWS) (DOD 2015b, S. 2 f.). Aktuelle Ansätze zur Entwicklung solcher Standards beruhen auf Modellierung und Simulation. Die Herausforderung besteht dann darin zu gewährleisten, dass diese Modelle bzw. Simulationen die relevanten Eigenschaften der realen Welt hinreichend gut abbilden (DSB 2016, S. 29 ff.). Da es sich bei der Kriegsführung oft um ein extrem schwer vorhersehbares Umfeld handelt, sind hier durchaus Zweifel angebracht, ob dies möglich ist (Danzig 2018, S. 7).

Emergente Effekte bei KI-Systemen

Die bisher beschriebenen Charakteristika von KI-Systemen waren überwiegend im engeren Bereich der Algorithmen angesiedelt. Darüber hinaus können allerdings auf der Systemebene Effekte auftreten, wenn Teile eines Systems oder verschiedene Systeme untereinander auf komplexe Art und Weise miteinander wechselwirken. Komplexität ist der zentrale Treiber dieser emergenten Effekte. Sie sind häufig auch dann schwer vorhersehbar, wenn die Eigenschaften der wechselwirkenden Komponenten gut bekannt sind (Jönsson 2007). Nicht ungewöhnlich ist bei emergenten Effekten, dass sie nur gelegentlich und nicht reproduzierbar auftreten (von Tolk [2015] »spukhaft« genannt). Bei militärischen technologischen Systemen werden emergente Effekte als einer der Hauptgründe für den Verlust von Kontrolle angesehen (Danzig 2018, S. 9 f.).

In welcher Art und Weise AWS, die auf gegnerische autonome Systeme treffen, mit diesen interagieren würden, ist eine vollkommen ungeklärte Frage. Da die genauen Charakteristika der gegnerischen Systeme vermutlich nicht bekannt sein dürften und die operationellen Umstände des Aufeinandertreffens kaum vorhersehbar sind, sind solche Begegnungen auch im Vorfeld schwer modellier- bzw. simulierbar.

Auch das Verhalten von Schwärmen wie etwa bei der sogenannten Schwarmintelligenz ist ein emergenter Effekt, der den Schwarm als Ganzes zu Aktionen befähigt, die für ein einzelnes Individuum unerreichbar sind. Dieses Verhalten zu verstehen bzw. zu steuern ist die Zielsetzung der Schwarmrobotik, die ein aktuelles Forschungsfeld ist (Şahin/Spears 2005).

Mensch-Maschine-Interaktion

Wenn menschliche Bediener nicht zuletzt aus ethischen und/oder juristischen Gründen eine wesentliche Rolle bei der Steuerung (Kontrolle, Aufsicht) von AWS spielen sollen, ist aus technologischer Sicht nicht das Ziel, ein möglichst hohes Level von Autonomie im System zu implementieren, sondern einen möglichst perfekten Mix aus Autonomie und menschlicher Mitwirkung, um eine effektive, zuverlässige und fehlerarme Ausführung der übertragenen Aufgaben zu gewährleisten. Diesen Mix herzustellen ist eine der größten

Herausforderungen der Robotik/Automatisierung und nach Ansicht des Technikhistorikers David Mindell schwieriger zu erreichen als vollständige Autonomie (Mindell 2015a, 2015b).

Ein hoher Grad an Automation führt oft dazu, dass im Normalbetrieb der Bediener kaum etwas zu tun hat, aber in kritischen Situationen plötzlich sehr viel gleichzeitig auf ihn einströmt (Geer 2018, S. 12). Die Schwierigkeit besteht dann darin, mit einer Situation umzugehen, die (Hawley 2017, S. 7) so beschreibt: »Dreiundzwanzig Stunden und neunundfünfzig Minuten Langeweile, gefolgt von einer Minute Panik«.

Es existiert eine Vielzahl von Beispielen für Fehler mit katastrophalen Auswirkungen, die in der Vergangenheit im Zuge der Interaktion von menschlichen Bedienern mit hochautomatisierten Systemen geschehen sind. (Hawley 2017) beschreibt einige davon anhand seiner langjährigen Erfahrung mit dem Flugabwehrsystem »Patriot«, das u. a. 2003 im Irakkrieg fälschlicherweise ein britisches sowie ein Kampfflugzeug der US-Navy abgeschossen hat.

Auch in der zivilen Luftfahrt existieren umfangreiche Erfahrungen mit Problemen bei der Mensch-Maschine-Schnittstelle. Dabei scheinen die großen Flugzeughersteller Boeing und Airbus unterschiedliche Philosophien zu verfolgen, welche Entscheidungen in bestimmten Situationen durch die Software bzw. den Piloten gefällt werden (Danzig 2018, S. 15). Diese Arbeitsteilung wird regelmäßig nach Unfällen öffentlich kritisiert und infrage gestellt (z. B. Economist 2019; Tagesschau 2019).

Konzeptionell entsprechen hochautomatisierte Systeme, und damit auch AWS, komplexen, eng gekoppelten technischen Systemen. In diesem Zusammenhang bedeutet eng gekoppelt, dass ein (Sub-)System ein anderes ohne Puffer direkt beeinflusst. Für solche Systeme hat Charles Perrow dargelegt, dass es auch bei höchster Sorgfalt bei Design, Bau, Betrieb und Aufsicht unvermeidlich zu unerwarteten und schwerwiegenden Fehlern kommen muss. Hierfür hat er den Begriff Normale Katastrophen geprägt (Perrow 1989).[16] Die unvorhergesehene Art und Weise, wie sich solche Fehler manifestieren können, und die fehlende Beobachtbarkeit und Steuerbarkeit systeminterner Vorgänge (z. B. der ML-Algorithmen), machen es auch für gut ausgebildete und erfahrene Bediener kaum möglich, die Quellen solcher Fehler rechtzeitig zu identifizieren und zu beheben. Entgegen der Intuition kann das Einbauen von Redundanzen, um z. B. die Möglichkeit zu haben, ein fehlerhaftes (Sub-)System durch ein Reservesystem zu ersetzen, durch Erhöhung der Komplexität sogar zu zusätzlichen bzw. schwerwiegenderen Fehlern führen (UNIDIR 2016, S. 6 ff.).

16 Eine Fülle an Beispielen findet sich in Clearfield/Tilcsik 2018.

Kasten 3.2 Militärische KI-Forschung und zivilgesellschaftlicher Protest: zwei Fallbeispiele

Dass Teile der Zivilgesellschaft der militärischen KI-Forschung äußerst skeptisch gegenüberstehen und Mittel des Protests bzw. Boykotts einsetzen, um kritisch gesehene Entwicklungen zu stoppen, zeigen zwei Fallbeispiele.

Projekt »Maven«

Die Menge des insbesondere von US-Drohnen aufgezeichneten Bildmaterials (Fotos und Bewegtbilder) steigt immer mehr an und ist aktuell dabei, die Analysekapazität der für diese Aufgabe bislang eingesetzten menschlichen Analysten zu sprengen (Pellerin 2017). Dieses Problem soll durch den Einsatz von KI-gestützten Verfahren zur Bildanalyse gelöst bzw. abgemildert werden. Das vom US-Verteidigungsministerium initiierte Projekt »Maven« hat die Zielsetzung, Bildmaterial durch Algorithmen auswerten zu lassen, um Objekte bzw. Personen zu klassifizieren, zu identifizieren sowie zu verfolgen (tracken).

Seit 2017 ist das Unternehmen Google am Projekt »Maven« beteiligt, u. a. indem die von Google entwickelte (frei verfügbare) KI-Software »TensorFlow« an die militärische Fragestellung angepasst wurde. Nachdem Tausende Google-Mitarbeiter sowie mehrere Hundert IT-Spezialisten und Ethiker dagegen protestiert hatten, entschied das Unternehmen, den bis 2019 laufenden Vertrag mit dem US-Verteidigungsministerium nicht zu verlängern (Bünte 2018; Peitz 2018).

KAIST

Hanwha Systems, ein bedeutender südkoreanischer Rüstungskonzern, hat im Februar 2018 bekanntgegeben, eine Kooperation mit der staatlichen Forschungseinrichtung Korean Advanced Institute of Science and Technology (KAIST) einzugehen, auf deren Grundlage gemeinsam an KI-Technologien für militärische Systeme geforscht werden soll (Jun 2018). Als Reaktion darauf haben mehr als 50 führende KI- und Robotikforscher einen Boykott von KAIST (d. h. einen Stopp jeglicher Kooperationen und Kontakte) angekündigt, der so lange aufrechterhalten werden soll, bis KAIST versichert, dass die zu entwickelnden Waffen stets unter menschlicher Kontrolle stehen werden. Daraufhin erklärte der Präsident von KAIST in einem Brief an die Unterstützer des Boykotts, dass KAIST sich nicht an der Entwicklung von LAWS oder Killerrobotern beteiligen würde. Daraufhin wurde der Boykott beendet (McLean 2018).

4 Verbreitung, Status und Trends unbemannter Waffensysteme

Bemühungen um unbemannte Waffensysteme[17] lassen sich bis zum Ersten Weltkrieg zurückverfolgen. Wie der historische Abriss bei Altmann und Gubrud (2017, S. 22 ff.) zeigt, wurden damals erstmals in größerem Umfang Minen sowohl zu Land als auch zur See eingesetzt, die mit ihrem automatischen Zündmechanismus als sehr einfache Varianten von AWS verstanden werden können. Außerdem wurde bereits, wenn auch nicht besonders erfolgreich, an der Entwicklung von per Kabel fernsteuerbaren Waffen (z. B. Torpedos und mit Sprengstoff bestückten Motorbooten) gearbeitet, zudem kamen erste unbemannte motorisierte Luftfahrzeuge zur Erprobung. In den folgenden Jahrzehnten waren eine stetige Automatisierung der Waffentechnik sowie etliche Innovationsschübe insbesondere bei luftgestützten unbemannten Systemen zu beobachten. Wichtige Meilensteine umfassten die »Fieseler 103«, auch bekannt als »V1«, die als erster Marschflugkörper gilt und von Nazideutschland im Zweiten Weltkrieg eingesetzt wurde, sowie die US-amerikanischen Ryan-Firebee-Aufklärungsdrohnen, die ab den 1960er Jahren in großer Zahl u. a. im Vietnamkrieg zum Einsatz kamen und als Vorläufer heutiger UAVs gelten. Im Jom-Kippur-Krieg (1973) wurden dann erstmalig bewaffnete Drohnen in größerem Umfang von Israel gegen feindliche Stellungen eingesetzt; es handelte sich dabei um mit Luft-Boden-Raketen ausgestattete Firebee-Drohnen, die per Video kontrolliert wurden. Aber erst die Fortschritte in Elektronik und Computertechnik ermöglichten schließlich ausgefeiltere und zunehmend autonome Lenkverfahren (vor allem Geländefolgeflug), was in den späten 1970er Jahren zur Konstruktion einer neuen Generation von Marschflugkörpern führte, die selbstständig Abwehrstelllungen umfliegen sowie Nuklear- oder auch konventionelle Waffen mit großer Genauigkeit ans Ziel bringen konnten.

Heute sind unbemannte Waffensysteme vor allem in Form von bewaffneten Drohnen fester Bestandteil der modernen Kriegsführung. Im Folgenden werden basierend auf den Gutachten von Altmann und Gubrud (2017) sowie Alwardt et al. (2017) die Proliferationstendenzen bei unbemannten Systemen, deren aktuelle Autonomiegrade sowie die Trends in der autonomiebezogenen FuE überblicksartig zusammengefasst.

In den letzten 10 Jahren hat die Zahl der staatlichen und nichtstaatlichen Akteure, die unbemannte Waffensysteme besitzen und teilweise auch bereits eingesetzt haben, stark zugenommen. Diese Entwicklung geht fast ausschließlich auf das Konto von Kampfdrohnen, die mit Abstand zu den am häufigsten produzierten und weitesten verbreiteten UWS gehören (dazu und zum Folgenden Alwardt

17 Umgangssprachlich oft auch als Drohnen bezeichnet.

et al. 2017, S. 16 ff.). Zwar wächst auch die Bedeutung von unbemannten Boden- und Wasserfahrzeugen (Kap. 4.1.2 u. 4.1.3). Da deren Einsatzfähigkeiten derzeit jedoch noch weitgehend auf nichtletale Zwecke begrenzt sind (Aufklärung, Überwachung, Logistik etc.) und zur Proliferation kaum öffentlich zugängliche Daten verfügbar sind, liegt der Fokus der folgenden Darstellung auf den bewaffneten UAVs. Mit Blick auf die möglichen Proliferationstendenzen zukünftiger AWS sind dabei vor allem fortschrittliche MALE-Kampfdrohnen (Kap. 4.1.1) von Interesse, die speziell für eine mittlere Flughöhe (ca. 10 bis 15 km) und lange Reichweiten entwickelt wurden (24 bis 48 Stunden Flugdauer).

Noch Anfang der 2000er Jahre waren die USA die einzige Nation, die über einen entsprechenden Drohnentyp verfügten (»MQ-1 Predator«); der erste Einsatz erfolgte im Oktober 2001 in Afghanistan (Altmann/Gubrud 2017, S. 81). In den folgenden Jahren bauten die USA ihr Drohnenprogramm massiv aus, was zur Entwicklung einer leistungsfähigeren MALE-Drohne[18] (»MQ-9 Reaper«) und zu unzähligen bewaffneten Drohneneinsätzen in Pakistan, Afghanistan sowie dem Nahen Osten führte. Das Bureau of Investigative Journalism (BIJ) schätzt, dass alleine im Zeitraum von Januar 2015 bis Oktober 2018 in Afghanistan 4.978 Drohnenangriffe stattfanden und dabei bis zu 5.346 Personen getötet wurden.[19] Hinzu gekommen sind mindestens 430 Einsätze in Pakistan (seit 2004), 324 Einsätze im Jemen (seit 2002) und 100 Einsätze in Somalia (seit 2007).

Das Vorbild der USA motivierte diverse andere Länder, selbst Kampfdrohnen zu entwickeln oder zumindest zu beschaffen (dazu und zum Folgenden Altmann/Gubrud 2017, S. 81). Während 2008 erst 3 Staaten im Besitz dieses Waffentyp waren (neben den USA noch Großbritannien und Israel), stieg die Zahl bis 2015 auf 15 (New America o. J.b). Es ist davon auszugehen, dass inzwischen mindestens 30 Staaten über fortschrittliche Kampfdrohnen verfügen (Munich Security Conference 2019, S. 52), davon haben 10 Länder (einschließlich den USA) Kampfdrohnen bereits unter Waffengebrauch in Kampfhandlungen eingesetzt (New America o. J.c).[20] Betrachtet man das Drohneninventar der einzelnen Länder genauer, fällt auf, dass eine große Anzahl von Ländern bewaffnete Drohnen importiert hat. Die USA, China sowie Israel stellen die wesentlichen Exportnationen dar. China soll z. B. bewaffnete Drohnen an Ägypten, Irak, Jordanien, Kasachstan, Myanmar, Nigeria, Saudi-Arabien, Turkmenistan und die

18 Darüber hinaus führte die U.S. Navy 2009 den unbemannten Hubschrauber »MQ-8 Fire Scout« (Naval Technology o. J.a) in den Betrieb ein und die U.S. Army 2012 das unbemannte Kampfluftfahrzeug »MQ-1C Gray Eagle« (GA-ASI o. J.). Beide können selbstständig starten und landen (Alwardt et al. 2017, S. 21).

19 https://www.thebureauinvestigates.com/projects/drone-war/charts?show_casualties=1&show_injuries=1&show_strikes=1&location=afghanistan&from=2015-1-1&to=now (1.9.2020)

20 Es gibt bislang keine umfassenden Datensammlungen über die weltweiten Drohnenprogramme. Das Programm »World of Drones« von New America ist eines der wenigen Projekte, das eine Datenliste hierzu anbietet, und wird daher häufig – auch in wissenschaftlicher Literatur – zitiert. Dennoch sind diese Daten eher als Richtwerte zu verstehen, da keine umfassenden Quellenangaben hinterlegt sind (Alwardt et al. 2017, S. 16).

Vereinigten Arabischen Emirate verkauft haben (Ewers et al. 2017, S. 12). Die USA wiederum exportieren Kampfdrohnen bisher ausschließlich an NATO-Partner, nämlich nach Frankreich, Großbritannien und Italien sowie an die Niederlande und Spanien (Cole 2016).

Tab. 4.1 Staatlicher Besitz, Beschaffung und Einsatz von fortschrittlichen Kampfdrohnen

Stand der Proliferation von Kampfdrohnen		
Besitz	Eigenproduktion	China, Georgien, Iran, Israel, Nordkorea, Pakistan, Südafrika, Türkei, Ukraine, USA
	Import/Leasing	Ägypten[c], Aserbaidschan[b], Frankreich[a, f], Großbritannien[b], Irak[c], Italien[a], Kasachstan[c], Niederlande[a, f], Nigeria[c], Saudi-Arabien[c], Spanien[a, f], Turkmenistan[c], Vereinigte Arabische Emirate[a, c]
bisherige Einsätze unter Waffengebrauch		Aserbaidschan, Großbritannien, Irak, Iran, Israel, Nigeria, Pakistan, Türkei, USA, Vereinigte Arabische Emirate
laufender Beschaffungsprozess	Entwicklung	Deutschland[e], Frankreich[e], Griechenland[d], Großbritannien, Indien, Schweden[d], Schweiz[d], Spanien[d], Südkorea, Taiwan, Vereinigte Arabische Emirate, Russland
	Import/Leasing	Australien[a, g], Deutschland[b], Indien[b], Jordanien[c], Polen[g], Schweiz[b]

a US-amerikanische Fabrikate
b israelische Fabrikate
c chinesische Fabrikate
d Entwicklung als Teil eines Konsortiums
e Entwicklung als Konsortialführer
f bisher unbewaffnete Kampfdrohne
g unsichere Informationen oder steht noch nicht fest

Wenn keine weiteren Angaben, dann handelt es sich bei den Kampfdrohnen (vorwiegend) um eigene Entwicklungen. Staaten, die bereits Kampfdrohnen produzieren, werden im Fall etwaiger weiterer Entwicklungsprogramme nicht mehr zusätzlich unter dem Punkt Entwicklung gelistet.

Quelle: Alwardt et al. 2017, S. 19

Deutschland besitzt bislang keine Kampfdrohnen vom Typ MALE (dazu und zum Folgenden Alwardt et al. 2017, S. 21 f.). Als fortschrittlichstes unbemanntes UAV setzt die Bundeswehr seit 2010 die von Israel geleaste unbewaffnete Drohne »Heron« der MALE-Kategorie zu Aufklärungszwecken in Afghanistan ein und seit November 2016 auch in Mali. Über bewaffnungsfähige Nachfolge-

modelle der »Heron« ist in den vergangenen Jahren kontrovers diskutiert worden. Als mögliche Alternativen standen zuletzt entweder US-amerikanische »MQ-9 Reaper« oder geleaste israelische »Heron-TP« zur Auswahl. Am 13. Juni 2018 bewilligte der Bundestag die Beschaffung von fünf Drohnen des Typs »Heron TP«, die jedoch vorerst nicht bewaffnet und nur zur Aufklärung eingesetzt werden sollen (BMVg 2018b). Über eine spätere Bewaffnung soll laut Koalitionsvertrag »nach ausführlicher völkerrechtlicher, verfassungsrechtlicher und ethischer Würdigung« gesondert entschieden werden (CDU/CSU/ SPD 2018). Darüber hinaus engagiert sich Deutschland in führender Rolle im Rahmen eines europäischen Konsortiums für die Entwicklung und Beschaffung einer bewaffnungsfähigen MALE-Drohne (Bundesregierung 2018e; dazu auch Kap. 4.2.2).

Zwar verfügen heute auch bereits einzelne nichtstaatliche Gruppierungen (z. B. Hamas, Hisbollah und IS) über unbemannte Waffensysteme in Form einfacher bewaffneter Drohnen (dazu und zum Folgenden Alwardt et al. 2017, S. 18). Dabei handelt es sich allerdings vorwiegend um Kleinstdrohnen sehr einfacher Bauart. Nach wie vor sind es also primär Staaten, darunter keineswegs nur die großen Militärmächte, die die Proliferation von bewaffneten UAVs vorantreiben und dies auch auf absehbare Zeit tun werden. Es wäre nicht überraschend, wenn bei einer Einführung von AWS ähnliche Erfahrungen und ein ebenso schneller Aufwuchs zu erwarten wären (Altmann/Gubrud 2017, S. 108) – schließlich ist die machtstrategische Bedeutung autonomer Waffen als sehr groß einzuschätzen und mithin die Gefahr eines Rüstungswettlaufs nicht von der Hand zu weisen (Kap. 6).

Eine nach Ländern aufgeschlüsselte Übersicht des Proliferationsstandes von Kampfdrohnen (militärisch bewaffnete Drohnen fortschrittlicherer Kategorien), untergliedert nach derzeitigem Besitz, laufender Beschaffung und dem bisherigen Einsatz findet sich in Tabelle 4.1. Es werden nur bereits stationierte Kampfdrohnen als Besitz eines Staates gelistet; anhand der vorliegenden Informationen kann jedoch nicht immer mit letzter Sicherheit abgeschätzt werden, ob eine Beschaffung nicht inzwischen schon in eine Stationierung gemündet ist.

4.1 Überblick zu einsatzreifen unbemannten (teil)autonomen Waffensystemen

Autonome Waffensysteme im strengen Sinne des Wortes, also bewaffnete unbemannte Plattformen, die fähig sind, im Kampfeinsatz ohne jegliche menschliche Kontrolle zu agieren, gibt es noch nicht. Aber zwischen Autonomie und Automatisierung besteht ein fließendes Kontinuum (Kap. 2.2), sodass in verschiedenen Waffengattungen bereits bewaffnete unbemannte Systeme vorliegen, die über einen relativ weitreichenden Grad an Automatisierung verfügen und deshalb als Vorläufer von AWS klassifiziert werden können. Im Folgenden wird anhand bereits verfügbarer oder in fortgeschrittener Entwicklung befind-

licher unbemannter Waffensysteme – aufgeschlüsselt nach den Einsatzbereichen Luft, Land und Wasser – der aktuelle Stand erreichter Autonomie grob eingeordnet. Der Überblick ist aufgrund der teils nur spärlich verfügbaren Informationen sowie der großen Zahl teilautomatisierter Waffensysteme nicht abschließend, sondern soll dazu dienen, einen exemplarischen Einblick in die aktuellen Möglichkeiten und technischen Gegebenheiten bei unbemannten Waffensystemen zu geben.

4.1.1 Fliegende Systeme

Nachdem präzisionsgelenkte Flugkörper wie der US-amerikanische »Tomahawk« und ballistische Raketen jahrzehntelang vorherrschend waren, haben seit Anfang der 2000er Jahre fortschrittliche MALE-Kampfdrohnen eine weltweite Verbreitung gefunden. Bei diesen handelt es sich um multifunktionale fliegende Plattformen, die über fortgeschrittene Aufklärungsfunktionen verfügen und zusätzlich mit Lenkflugkörpern ausgestattet werden können. Inzwischen findet sich in den Arsenalen der führenden Nationen eine beachtliche Vielfalt an unterschiedlichen Kampfdrohnentypen, die mit einer Vielzahl von Waffen bestückt sind (Military Factory o. J.a).

Dass bei der Verbreitung unbemannter Waffensysteme Fluggeräte vorherrschend sind, hängt wesentlich damit zusammen, dass Navigation, Orientierung und Funkkommunikation in der Luft relativ einfach zu bewerkstelligen sind – deutlich einfacher jedenfalls, als dies an Land bzw. auf oder unter Wasser der Fall ist (Dickow 2015, S. 14). Allerdings sind die autonomen Fähigkeiten fliegender unbemannter Systeme insgesamt nach wie vor begrenzt:

- Bei den Kampfdrohnen beschränkt sich die Autonomie üblicherweise auf die Flugkontrolle, auf Navigations- und Aufklärungsfunktionen sowie auf die eventuelle Rückkehr im Falle eines Funkabbruchs; die Waffenauslösung geschieht in der Regel per Fernsteuerung und unterliegt somit in letzter Instanz immer noch menschlicher Kontrolle (Alwardt et al. 2017, S. 19).[21]
- Gängige Lenkwaffen werden entweder durch aktive menschliche Steuerung (z. B. per Laser-, Radar- oder Infrarotstrahl) ins Ziel gelenkt, oder sie steuern selbstständig ein vorab definiertes und einprogrammiertes Ziel an (Altmann/Gubrud 2017, S. 101 f.; Boulanin/Verbruggen 2017, S. 47 ff.). Letzteres wird auch »fire and forget« genannt. Zur Anwendung kommen dabei Bilderkennung, GPS-Steuerung und Präzisionslenkung – jedoch in der Regel bloß »als Verstärkung menschlicher Steuerung [...], da sie klar dazu

21 Allerdings gibt es auch Stimmen, die spekulieren, die U.S. Air Force könnte bereits im Geheimen über einsatzfähige unbemannte Kampfdrohnen mit weitreichenden autonomen Fähigkeiten verfügen. So vertritt etwa Rogoway (2016) diese These. Die US-amerikanischen Entwicklungsprogramme, die diesen Spekulationen zugrunde liegen, werden in Kapitel 4.2.1 vorgestellt.

beabsichtigt sind, den Flugkörper zu einem vorher ausgewählten Ziel zu lenken« (Altmann/Gubrud 2017, S. 102).

Das militärische Interesse an der zunehmenden Integration autonomer Funktionen ist jedoch klar erkennbar, und es befinden sich bereits Systeme im Einsatz oder in fortgeschrittener Entwicklung, die mit weitreichender Autonomie ausgestattet sind. Dazu gehören zum einen Drohnensysteme, die im Rahmen definierter Parameter selbstständig auf die Suche nach einem Ziel gehen, um dieses dann autonom zu attackieren – im Fachjargon auch als »loitering weapon« bezeichnet (»to loiter«: verweilen, herumlungern) –, sowie zum anderen taktische Lenkflugkörper, die mit weitentwickelten autonomen Zielerfassungs- bzw. Zielsuchfunktionen ausgestattet sind.

Drohnensysteme

Zu den wenigen Drohnensystemen, die über relativ weitreichende autonome Angriffsfunktionen verfügen, gehören drei israelische Systeme: die Drohne »Harpy«, die bereits in den 1990er Jahren entwickelt wurde, deren Nachfolger »Harop« (2009; Abb. 4.1) sowie »Harpy NG« (2016), bei denen es sich im Wesentlichen um vergrößerte und technisch verbesserte Varianten von »Harpy« handelt. Die Drohnen verfügen über eine Spannweite von 2,1 m (»Harpy«) bzw. 2,5 m (»Harop«) und sind mit Sprengladungen von 32 kg (»Harpy«) bzw. 23 kg (»Harop«) bestückt. Entwickelt wurden diese Systeme von Israel Aerospace Industries (IAI).

Sowohl »Harpy« als auch »Harop« zählen zu den »loitering weapons« und dienen primär dem Zweck, feindliche Flugabwehrsysteme auszuschalten (dazu und zum Folgenden Boulanin/Verbruggen 2017, S. 50 ff.). Der Start erfolgt über an Fahrzeugen befestigte Container. Wie herkömmliche Drohnen sind sie in der Lage, in einem bestimmten Gebiet für mehrere Stunden selbstständig zu kreisen, um autonom nach vorab definierten Zielen (in diesem Falle feindlichen Radarsignalen) zu suchen. Der Unterschied zu herkömmlichen Kampfdrohnen ist darin zu sehen, dass sowohl »Harpy« als auch »Harop« nach dem Start fast komplett autonom agieren können: Sobald sie ein vorab definiertes Ziel, sprich eine feindliche Radarstation, anhand ihres spezifischen Signals detektiert haben, gehen sie in den Angriffsmodus über und stürzen sich auf das Zielobjekt, um sich in dessen Nähe zur Explosion zu bringen und es so zu zerstören – in dieser Hinsicht ähneln sie Marschflugkörpern, weshalb sie auch Kamikazedrohnen genannt werden. Dieser Selbstzerstörungseffekt hat zur Folge, dass die Drohnen hinsichtlich ihrer technischen Ausstattung eher einfach gehalten sind, auch was die Aufklärungsfunktionen betrifft. Während »Harpy« ausschließlich autonom agiert (und bei erfolgloser Suche nach einem Ziel sich selbst zerstört) (Defense Update 2006), kann »Harop« zusätzlich ferngesteuert werden und ist zu diesem Zweck mit elektrooptischen sowie Infrarotkameras ausgestattet; dies macht es möglich, auch

andere Ziele als Radarstationen anzugreifen. Im Falle einer erfolglosen Mission kann »Harop« zudem per Fallschirm gelandet werden (Bumbacher 2016).

Abb. 4.1 Drohne »Harop«

Quelle: Julian Herzog, Wikimedia Commons, CC-BY-4.0

»Harpy« wurde von Israel an China, Indien, Südkorea und die Türkei verkauft, »Harop« an Aserbeidschan, Indien, die Türkei und auch an Deutschland (Altmann/Gubrud 2017, S. 87). Bei der Bundeswehr bildet »Harop« zusammen mit der Aufklärungsdrohne »KZO« (»Kleinfluggerät Zielortung«) von Rheinmetall das Verbundsystem WABEP (Wirkmittel zur abstandsfähigen Bekämpfung von Einzel- und Punktzielen) (TAB 2011, S. 42). Da Harop sich beim Einsatz selbst zerstört, wird WABEP von der Bundesregierung nicht als Kampfdrohne eingestuft, sondern als »Wirkmittel (Munition), das dem ›Schützen‹ ermöglicht, bis kurz vor dem Einschlag das Ziel zu beobachten, nachzurichten und notfalls den Angriff abzubrechen« (Bundesregierung 2009, S. 2).

Ein anderes Beispiel für eine mit autonomen Funktionen ausgestattete »loitering weapon« ist ein »Low Cost Autonomous Attack System« (LOCAAS), das 1998 von der U.S. Air Force (mit Lockheed Martin) entwickelt wurde (dazu und zum Folgenden Altmann/Gubrud 2017, S. 161 f.). Das Ziel war es, einen kleinen, kostengünstigen Flugkörper herzustellen, der wie »Harop« eine Hybridform aus Drohne und Lenkflugkörper darstellt. Mit einer Länge von 0,9 m, einer Gesamtmasse von 45 kg und einem Multimodusgefechtskopf (Penetrator oder Splitter) von 8 kg sollte die Waffe gegen gepanzerte und ungepanzerte Fahrzeuge, anderes Material und Personen eingesetzt werden können, etwa zur Bekämpfung von mobiler Luftabwehr, mobilen Startgeräten für Boden-Boden-Flugkörper und langreichweitigen Raketensystemen. Vorgesehen war, dass das von einem Träger gestartete LOCAAS über eine Reichweite von über 200 km verfügt, sich einem vorher definierten Zielbereich mittels GPS und Trägheitsnavigation nähern und dort ungefähr eine halbe Stunde lang nach Zielen suchen kann. Diese

sollten mittels Laserradar anhand ihrer dreidimensionalen Geometrie durch Vergleich mit gespeicherten Zielsignaturen gefunden und erkannt werden. Das System sollte in der Lage sein, zwischen unterschiedlichen Typen von Zielen sowie zwischen legitimen Zielen und Nichtkombattanten zu unterscheiden (Global Security o. J.a). Für die U.S. Navy wurde der Einsatz in Schwärmen und mit optionaler Datenverbindung für einen Fernsteuerungsmodus ins Auge gefasst. Das Programm wurde Mitte der 2000er Jahre abgebrochen, offenbar aufgrund von Bedenken hinsichtlich Verlässlichkeit, Steuerbarkeit und Rechtmäßigkeit (Gubrud 2015).

Lenkflugkörper

Ein Lenkflugkörper[22], der bereits über weitreichende autonome Funktionen verfügt, ist die britische »Brimstone« von Matra BAe Dynamics Aérospatiale S.A.S (MBDA) (dazu und zum Folgenden Altmann/Gubrud 2017, S. 104 f.). Es handelt sich dabei um einen Luft-Bodenflugkörper mit einer Reichweite von 12 bis 24 km, der einen Millimeterwellen-Radarsuchkopf (MMW-Suchkopf) nutzt, um Fahrzeuge zu orten und anzufliegen (Markowitz/Gresham 2012). Die Entwicklung begann 1996, und die ersten Flugkörper wurden 2005 in Dienst gestellt. Er ist zum Einsatz gegen gepanzerte Fahrzeuge vorgesehen, mit einem Tandemgefechtskopf, in dem eine kleine Vorausladung zuerst reaktive Panzerung entfernt und ein zweiter Hohlladungsgefechtskopf schwere Panzerung durchdringt. In einem Katalog der Royal Air Force (RAF 2003, S. 87) von 2003 wird »Brimstone« als eine »völlig autonome, Feuern-und-vergessen-Antipanzerwaffe« angepriesen. Insbesondere wird bemerkt, dass die Waffe, einmal gestartet, völlig eigenständig nach gepanzerten Zielen suchen kann, auf Basis von gespeicherten Zielsignaturen. Nichtpassende Ergebnisse (wie Autos, Busse, Gebäude) werden zurückgewiesen und mit der Suche und dem Vergleich so lange fortgefahren, bis ein gültiges Ziel identifiziert ist. Analog zu den vorab beschriebenen Drohnensystemen kann der Brimstone-Flugkörper so programmiert werden, dass er erst nach Zielen zu suchen beginnt, sobald ein definiertes Zielgebiet erreicht ist (Boulanin/Verbruggen 2017, S. 49 f.). Dies soll es laut der Royal Air Force ermöglichen, freundliche Kräfte sicher zu überfliegen und Kollateralschäden zu vermeiden.

2007 bekam MBDA den Auftrag, Brimstone-Flugkörper zusätzlich zum MMW-Suchkopf mit einem halbaktiven Lasersuchkopf (»semi-active laser« – SAL) nachzurüsten (dazu und zum Folgenden Altmann/Gubrud 2017, S. 105). Grund dafür war offenbar, dass sich der vollautonome Modus (»fire and

22 Lenkflugkörper werden wie Torpedos üblicherweise nicht zu den AWS gezählt, da sie nur für den einmaligen Einsatz gedacht sind und es sich also nicht im engeren Sinne um bewaffnungsfähige Trägersysteme bzw. Plattformen handelt. Sie werden hier dennoch erläutert, da sie teilweise über fortgeschrittene autonome Funktionen verfügen und deshalb als wichtige Vorstufen von AWS anzusehen sind.

forget«) in asymmetrischen Konflikten wie dem Afghanistaneinsatz als problematisch herausstellte, da Zivilisten und irreguläre Kombattanten anhand der MMW-Signaturen kaum voneinander zu unterscheiden waren (Markowitz/Gresham 2012). Bei der neu hinzugefügten SAL-Zielsuchlenkung muss ein menschlicher Bediener einen Laserstrahl auf dem Ziel halten und der Bediener kann den Flugkörper bis einige Sekunden vor dem Aufschlag umlenken. Die SAL- und MMW-Zielanflugarten können für bessere Genauigkeit kombiniert werden, insbesondere bei bewegten Zielen. SAL kann auch einzeln benutzt werden, um den Flugkörper auf Ziele zu lenken, die durch Radar schwer zu detektieren sind (z. B. nichtmetallische Objekte) (MDBA 2018). Der Dual-Mode-Brimstone wurde in Afghanistan, Irak, Libyen und auch Syrien eingesetzt (Think Defence o. J.).

Laut Berichten von 2016 (Max 2016) plant die deutsche Luftwaffe die Anschaffung von Dual-Mode-Brimstone für den »Eurofighter«, genauere Auskünfte dazu hat die Bundesregierung (2018a) jedoch kürzlich aus Geheimhaltungsgründen verweigert. Diese Anschaffung wäre insofern brisant, als der Brimstone-Lenkflugkörper in seiner Dual-Mode-Variante zwar oft als Mensch-in-der-Schleife-Waffe angepriesen wird, der Lenkflugkörper jedoch weiterhin in seinem völlig autonomen Modus mit MMW-Suchkopfmodus benutzt werden kann – und im Gefecht offenbar auch entsprechend eingesetzt wird. So feuerte das britische Militär im Libyenkrieg 2011 erstmals eine größere Salve von ca. 24 Flugkörpern auf eine Ansammlung gepanzerter Fahrzeuge des Gaddafi-Regimes ab, wobei mehrere feindliche Fahrzeuge zerstört wurden. Laut Pressemitteilung der britischen Regierung (MOD 2011) wurde dabei nur der MMW-Suchkopf im autonomen Modus benutzt.

Ebenfalls über hochentwickelte autonome Fähigkeiten bei deutlich höherer Reichweite soll der Antischiffsflugkörper »LRASM« verfügen (offizielle Bezeichnung »AGM-158C«), dessen Entwicklung von den USA seit 2009 vorangetrieben wird (dazu und zum Folgenden Altmann/Gubrud 2017, S. 103). Obwohl er sich derzeit noch in der Testphase befindet und nur spärliche Informationen verfügbar sind, eilt ihm bereits der Ruf voraus, hinsichtlich Autonomie eines der fortschrittlichsten Waffensysteme weltweit zu sein. Hinter dem Programm »LRASM« steht das strategische Entwicklungsziel, die Reichweite der Antischiffsflugkörper der U.S. Navy vor allem im westlichen Pazifik zu vergrößern (Roblin 2018). Zu diesem Zweck wurde »LRASM«, der eine Modifikation des vorhandenen Luft-Boden-Marschflugkörpers »JASSM-ER« (»joint air-to-surface standoff missile – extended range«) darstellt, mit autonomen Funktionen ausgestattet, die es erlauben sollen, unabhängig von präzisen Informationen und funktionierenden Kommunikationsverbindungen auch weitentfernte, bewegliche Ziele zu identifizieren und zu bekämpfen. Erreicht werden soll dies mittels KI-basierter Zielidentifizierung, die mit den Daten eines multimodalen Suchkopfes gespeist wird: basierend auf passiver und aktiver Radarzielsuchlenkung, elektronischen Unterstützungsmaßnahmen (»electronic support measures« – ESM),

Infrarotbildgebung und störresistentem GPS (NavalTechnology o. J.b). Außerdem verfügt der Flugkörper über einen Datenlink, über den die Zielvorgaben während des Fluges aktualisiert werden können. Das intelligente Lenksystem von »LRASM« soll fähig sein, seinen Weg autonom zu verändern und sich mit Flugkörpern in einer Salve oder einem Schwarm zu koordinieren. Während sie zum endgültigen Angriff im Sinkflug übergehen, sollen die Flugkörper elektronische Gegengegenmaßnahmen (»electronic counter-countermeasures«) nutzen können, um feindliches Radar zu täuschen (Roblin 2018). Die erhebliche Größen- und Gewichtsbürde durch die Hinzufügung dieser Komponenten hat jedoch zur Folge, dass die Reichweite von »LRASM« mit ca. 600 km erheblich geringer ist als die des »JRASSM-ER« (930 km Reichweite), wenngleich immer noch um ein Vielfaches höher als die von »Brimstone« oder des norwegischen »Naval Strike Missile« (NSM).[23]

LRASM wurde bereits mehrfach erfolgreich getestet und offenbar wurden im Mai 2019 die ersten Exemplare an die US-Luftwaffe ausgeliefert (Defense Industry Daily 2019).

4.1.2 Bodensysteme

Militärische Roboter, die am Boden operieren, sind grundsätzlich mit deutlich komplexeren Anforderungen konfrontiert als ihre fliegenden Pendants (Altmann/Gubrud 2017, S. 83 f.; Dickow 2015, S. 14): Sie haben keinen freien Luftraum vor sich, sondern teils unwegsames, unübersichtliches Gelände. Das erschwert die Navigation, vor allem abseits von Straßen, und je nach Bodenbeschaffenheit auch die Fortbewegung. Diese Einschränkungen gelten jedoch nur für Fahrzeuge und nicht für stationäre Waffensysteme, sodass es prinzipiell einfacher ist, Letztere mit autonomen Funktionen auszustatten.

Stationäre Systeme

Bodengestützte Waffensysteme, die über keine eigene Fortbewegungsfähigkeit verfügen, haben in aller Regel ein stark eingegrenztes Funktions- und Einsatzspektrum, das meist defensiver Natur ist. In ihrer einfachsten Variante handelt es sich um Sprengfallen oder Minen, die – sofern sie direkt gegen Personen gerichtet sind (Antipersonenminen) – gemäß der Ottawa-Konvention[24] von 1997 inzwischen völkerrechtlich geächtet sind. Das Problem bei Antipersonenminen ist, dass sie nicht zwischen Kombattanten und Nichtkombattanten

23 Der »NSM« ist ebenfalls eine Antischiffswaffe und verfügt bei einer Reichweite von etwa 185 km über autonome Fähigkeiten, die dem »LRASM« vergleichbar sind. Für genauere Informationen siehe Boulanin/Verbruggen (2017, S. 50).

24 Übereinkommen über das Verbot des Einsatzes, der Lagerung, der Herstellung und der Weitergabe von Antipersonenminen und über deren Vernichtung

unterscheiden können, wofür der automatische Zündmechanismus verantwortlich ist. Mittels der Nutzung von KI und geeigneter Sensorik könnten Antipersonenminen im Prinzip jedoch so weiterentwickelt werden, dass eine entsprechende Diskriminierung möglich wird und dementsprechend der Grund für die völkerrechtliche Ächtung entfallen würde.

Ein Schritt in diese Richtung stellt das »M7 Spider Network Command Munition System« (»M7 Spider«) dar, ein vernetztes Antipersonensystem, das im Kern aus sechs sternförmig angeordneten Granatwerfern kurzer Reichweite besteht (»munition control unit« – MCU) (dazu und zum Folgenden Altmann/Gubrud 2017, S. 96 ff.).[25] Jeder dieser Granatwerfer ist mit einem Stolperdraht verbunden, dessen Aktivierung jedoch nicht direkt zur Waffenauslösung führt; stattdessen wird ein Signal an eine Fernsteuereinheit gesendet (»remote control unit« – RCU), über die mehrere MCUs aus der Distanz kontrolliert werden können (ALT 2011, S. 296 f.). Aufgrund dieser Konfiguration ist zwar grundsätzlich sichergestellt, dass sich immer noch ein Mensch in der Schleife befindet. Da die Entfernung zwischen RCU (und damit dem menschlichen Bediener) und MCU bis zu 1,5 km betragen kann, ist allerdings fraglich, ob in Gefechtssituationen ein für die Waffenbedienung ausreichendes Situationsverständnis garantiert ist.

Ebenfalls der Personenabwehr dienen robotische Wachpostenkanonen, wie sie von mindestens zwei Nationen – von Israel (entlang des Gazastreifens) sowie Südkorea (entlang der demilitarisierten Zone) – stationiert worden sind.[26] Diese fest installierten Systeme sind mit Schusswaffen ausgestattet und verwenden keine Explosivstoffe, weshalb sie nicht als Landminen gelten. Obwohl vermutlich sowohl die israelischen Sentry-Tech-Stationen als auch der südkoreanische »SGR-A1« über alle technischen Voraussetzungen für einen vollautomatischen Betrieb verfügen, werden sie – zumindest laut offiziellen Verlautbarungen – nur unter menschlicher Aufsicht betrieben (Altmann/Gubrud 2017, S. 99 f.; Cavanaugh 2016).

Hinsichtlich seiner autonomen Fähigkeiten gilt der von Samsung Techwin entwickelte »SGR-A1« als besonders fortgeschritten. Er verfügt über eine Tageslicht- sowie eine Infrarotkamera, mittels derer er potenzielle Ziele auf eine Distanz von bis zu 4 km aufspüren und überwachen können soll. Da der

25 »M7 Spider« geht auf das »intelligent munition system« (IMS) zurück, das ab 2006 im Rahmen des inzwischen eingestellten Programms »Future-Combat-Systems« (FCS) (Gubrud/Altmann 2013) der U.S. Army entwickelt wurde. Die Idee hinter IMS war, ein vernetztes, intelligentes Minensystem zu schaffen, bestehend aus Bodensensoren und Munitionsverteilern, die entweder autonom oder auf Befehl ausgelöst werden können (Altmann/Gubrud 2017, S. 97). Das IMS sollte sowohl Antipersonengranaten als auch Antipanzerstreumunition umfassen. Offiziell wurde die Entwicklung des IMS zusammen mit dem FCS 2009 beendet, woraufhin Textron Systems die Entwicklung von »M7 Spider« in Eigenregie weiterführte.

26 2016 wurde vermeldet, dass auch die Türkei begonnen hat, automatische Kanonentürme, hergestellt von der Firma Aselsan, an der Grenze zu Syrien zu installieren (Yeni Şafak 2016). Über die technische Ausstattung sowie die Fähigkeiten dieser Systeme ist jedoch fast nichts bekannt (Altmann/Gubrud 2017, S. 100).

Roboter primär für den Einsatz in der demilitarisierten Zone entwickelt wurde, in der sich kein Mensch aufhalten darf, und es sich zudem um ein stationäres System handelt, sind nur rudimentäre Diskriminierungsfähigkeiten erforderlich und auch implementiert worden. Mittels Mustererkennung soll der Roboter nicht nur fähig sein, Menschen von anderen Objekten zu unterscheiden, sondern auch einen sich ergebenden Soldaten erkennen zu können; außerdem soll er über ein Sprachinterface verfügen, über das sich nähernde Personen gewarnt und ggf. identifiziert werden können (Global Security o. J.b). Ausgerüstet mit einem leichten Maschinengewehr ist der Roboter so zumindest prinzipiell in der Lage, Angreifer automatisch zu bekämpfen, auch wenn ein derartiges Einsatzszenario wie bereits erwähnt offiziell dementiert wird (Rabinoff 2010). Auch wo und in welcher Zahl die Systeme eingesetzt werden, ist bis zum heutigen Tag noch nicht klar (Altmann/Gubrud 2017, S. 100). Über experimentelle Stationierungen entlang der koreanischen demilitarisierten Zone sowie im Irak und in Afghanistan (zum Schutz südkoreanischer Militärpräsenz) wurde berichtet, aber über Anzahl und eventuelle dauerhafte Stationierungen wurde nichts öffentlich gemacht (Cavanaugh 2016; Rabinoff 2010).[27]

Bei den hier beschriebenen robotischen Wachpostenkanonen handelt es sich im Prinzip um Sonderformen fernbedienbarer Waffenstationen (»remote weapon station« – RWS), die auf Plattformen, verschiedenen Fahrzeugen oder auch Schiffen bereits weitverbreitet zum Einsatz kommen (Cavanaugh 2016). Das Spektrum der Bewaffnung von RWS-Systemen ist breitgefächert und reicht von leichten Maschinengewehren über Granatwerfer bis hin zu Kurzstreckenflugkörpern. Um aus der Ferne bedient werden zu können, sind RWS üblicherweise mit hochentwickelten optoelektrischen Sensorsystemen ausgestattet. Dank moderner Computertechnik ist es heutzutage möglich, und dies wird auch angestrebt, grundlegende Waffenfunktionen wie Zielerfassung, -verfolgung und sogar Feuerleitung zunehmend zu automatisieren. Dies ist nicht nur zur Personenabwehr an umstrittenen Grenzverläufen nützlich, sondern vor allem und mehr noch zur Luftabwehr im Nahbereich. Die Bedienung entsprechender Abwehrsysteme erfordert nämlich so kurze Reaktionszeiten, dass Menschen damit typischerweise überfordert sind. Aus diesem Grund sind Nahbereichsflugabwehrsysteme wie das deutsche »MANTIS« (Rheinmetall Defence o. J.), das US-amerikanische Phalanx »CIWS« (Raytheon Missiles & Defense (o. J.b) oder das israelische »Iron Dome« (RAFAEL o. J.a) mit weitreichenden

27 Von der südkoreanischen DoDamm Systems Ltd. stammt das Konkurrenzsystem »Super aEgis II«. Hierbei handelt es sich ebenfalls um einen stationären Maschinengewehrturm, der menschliche Ziele auf mehr als 2 km Entfernung erkennen und bekämpfen können soll (Blain 2010). Das Gerät ist dafür ebenfalls mit zahlreichen Kameras ausgestattet und soll theoretisch – wie »SGR-A1« auch – über einen vollautonomen Einsatzmodus verfügen, wenngleich in der Regel für die Waffenauslösung eine menschliche Eingabe vorgesehen ist (Parkin 2015). »Super aEgis II« soll sich im Mittleren Osten bereits an verschiedenen Orten im Einsatz befinden.

automatisierten Funktionen ausgestattet, die sie in die Lage versetzen, auch kleine, schnellbeweglich Ziele mittels Radar zu identifizieren, anhand des Radarquerschnitts zu klassifizieren und schließlich per Maschinenkanone oder Abfangrakete zu bekämpfen – alles prinzipiell ohne menschliches Zutun (Dickow 2015, S. 9).

Das von der Rheinmetall Defence entwickelte »MANTIS« dient u. a. dem Schutz von Feldlagern vor Raketen-, Artillerie- und Mörserangriffen und wird derzeit von der Bundeswehr in Mali eingesetzt (BMVg 2018c). Es ist modular aufgebaut und besteht aus einer Bedien- und Feuerleitzentrale (BFZ), mehreren Radareinheiten und 35-mm-Geschützen (Abb. 4.2). Das Radar ist auf die Erkennung kleiner Objekte optimiert und soll in der Lage sein, Ziele in der Größe eines Tennisballs auf 20 km Entfernung zu erkennen; die maximale Reichweite des Geschützes wiederum beträgt 5 km (Wikipedia 2009a). Auch wenn »MANTIS« als hochautomatisiertes System gilt, das nach Scharfstellung prinzipiell vollständig eigenständig agieren könnte, sehen die Einsatzregeln der Bundeswehr derzeit vor, dass die Waffenauslösung unter der Kontrolle eines menschlichen Bedieners zu stehen hat (DBWV 2016).

Abb. 4.2 Geschütz des Flugabwehrsystems »MANTIS«

Quelle: Frank Vincentz, Wikimedia Commons, CC-BY-SA-3.0

Bodenfahrzeuge

Bei unbemannten Bodenfahrzeugen (UGVs) sind autonome Funktionen aus den eingangs genannten Gründen erheblich schwieriger zu realisieren als bei stationären Waffensystemen: Sowohl die Anforderungen an die Umgebungserfassung als auch an die Verhaltensplanung sind wesentlich höher, ebenso die mechanischen Herausforderungen vor allem bei der Fortbewegung in unwegsamem Terrain (Dickow 2015, S. 14). Deshalb liegt der Entwicklungsstand bei den robotischen UGVs insgesamt deutlich hinter dem von UAVs wie auch dem

von stationären Bodensystemen zurück. Die militärischen UGV-Systeme, die sich bereits im Einsatz befinden, sind in aller Regel nicht bewaffnet und haben vor allem unterstützende Funktion: Sie dienen z. B. Transportzwecken (wie das SMSS[28] von Lockheed Martin) oder der Aufklärung und Minenräumung (wie der in großer Stückzahl produzierte Kleinroboter »PackBot« [Army Technology o. J.b] der formaligen iRobot Corp.). Sowohl das SSMS wie auch der »PackBot« wurden von den USA in Afghanistan eingesetzt. Eine der wenigen bewaffneten Ausnahmen bei den komplett ferngesteuerten UGVs ist das von Qinetiq North America seit 2008 angebotene Modular »Advanced Armed Robotic System« (MAARS), ein 167 kg schwerer Kleinroboter, der optional mit Sprenggranaten und Maschinengewehr ausgerüstet werden kann und speziell für Erkundungsmissionen entwickelt wurde (Altmann/Gubrud 2017, S. 84; Qinetiq North America 2018).

Gleichwohl wird intensiv an bewaffneten UGVs gearbeitet, die mit komplexeren autonomen Fähigkeiten ausgestattet sind. Was Navigation und Umgebungserfassung angeht, gibt es dabei naturgemäß große Schnittmengen mit der zivilen Forschung zum autonomen Fahren. So spielte die DARPA eine Schlüsselrolle beim Anstoß entsprechender Entwicklungen, indem sie drei wegweisende Wettbewerbe für autonome Fahrzeuge durchführte: 2004 und 2005 die »Grand Challenges« in einer Wüste sowie 2007 den »Urban Challenge« in einer städtischen Umgebung (Siciliano et al. 2009). Ziel war es, die prinzipielle Machbarkeit des autonomen Fahrens zu demonstrieren, was auch grundsätzlich gelang (Berger/Rumpe 2008) und vor allem der zivilen Forschung sichtbaren Aufschwung gab.[29]

Inzwischen sind aber auch aus dem militärischen Bereich erste Entwicklungserfolge zu vermelden (zum Folgenden Altmann/Gubrud 2017, S. 84 f.; Alwardt et al. 2017, S. 22 f.):

Einer der Vorreiter bei UGVs ist *Israel*, das zur Grenzkontrolle mit einer ganzen Reihe teils bewaffneter oder zumindest bewaffnungsfähiger UGVs operiert. Dazu gehören das gepanzerte Fahrzeug »Guardium« (Abb. 4.3), 2008 erstmals erprobt, mit diversen Kameras und Sensoren ausgerüstet und primär für Patrouillenfahrten an der Grenze zum Gazastreifen eingesetzt, sowie das darauf

28 Das SMSS zählt zu den größten verfügbaren UGVs (Länge: 3,6 m; Gewicht: 1,7 t) und ist in der Lage, schwere Lasten zu transportieren. Es verfügt über verschiedene Steuerungsmodi: Es kann einer vorab spezifizierten Person automatisch folgen, autonom eine vordefinierte Route abfahren und auch ferngesteuert werden (Army Technology o. J.a). Laut Lockheed Martin ist die langfristige Vision, auf Basis des SMSS Varianten von autonomen UGVs aufzubauen, die jeweils unterschiedliche militärische Zwecke erfüllen und teils auch bewaffnet sein sollen (https://lockheedmartin.com/en-us/products/smss.html; 30.12.2019).

29 In Europa findet seit 2006 jährlich der »European Land-Robot Trial« (ELROB) statt, die abwechselnd militärischen und zivilen Zielen gewidmet ist (http://www.elrob.org/; 1.9.2020). Anders als die von der DARPA veranstalteten Challenges handelt es sich nicht um Innovationswettbewerbe im engeren Sinne, sondern um eine reine Leistungsschau im Bereich europäischer Landrobotiksysteme. Getestet wird jeweils anhand realistischer Einsatzszenarien.

basierende »AvantGuard«.[30] Beide Fahrzeuge können optional bewaffnet werden und sollen semiautonom – sei es einem vorausfahrenden Fahrzeug folgend oder entlang vordefinierter Routen – oder ferngesteuert ein begrenztes Gebiet überwachen können, z. B. um improvisierte Sprengkörper aufzuspüren und zu neutralisieren (Army Technology o. J.c). 2017 wurde von der israelischen Meteor Aerospace Ltd. zudem das UGV »Rambow« vorgestellt (Ahronheim 2017). Es ist mit einem leisen Elektromotor ausgerüstet und verfügt ebenfalls über semiautonome Fahrfunktionen, die optionale Bewaffnung ist aber auch – wie bei »Guardium« und »AvantGuard« – ferngesteuert (Meteor Aerospace o. J.).

Abb. 4.3 Das israelische UGV »Guardium«

Quelle: Israel Defense Forces, Wikimedia Commons, CC-BY-SA-3.0

Seit einigen Jahren zeigt sich *Russland* bei bewaffneten UGVs besonders aktiv (Hambling 2014b). Die entsprechenden Entwicklungsbemühungen passen zum offiziellen Ziel, bis etwa 2025 30 % der russischen Kampfkraft durch ferngesteuerte und robotische Plattformen bereitzustellen (Eshel 2015). Ein erster Schritt dahin ist bereits gemacht: 2014 wurde angekündigt, dass bewaffnete UGVs, die auch ohne menschliche Beteiligung schießen können sollen, für die Bewachung von mehreren Raketenbasen eingesetzt werden (Hambling 2014a). Ferner wurde 2016 der vom Kalaschnikow Konzern entwickelte Panzer »BAS-01G-Soratnik« präsentiert; ausgestattet mit Maschinengewehr und Panzerabwehrrakete soll dieser in erster Linie dem Infanterieschutz dienen (Military Factory o. J.b). Daneben gibt es eine ganze Reihe von weiteren russischen Entwicklungen im Bereich bewaffneter UGVs: Die bemerkenswertesten sind in aufsteigender

30 Die für das »Guardium« von Israel Aerospace Industries und Elbit Systems speziell gegründete Firma G-nius wurde allerdings 2016 wegen zu weniger internationaler Verkäufe geschlossen.

Gewichtsklasse »Nerekhta« (Army Recognition 2016), »Uran-9« (Army Technology o. J.d) und »Vikhr«. Diese Kettenfahrzeuge können schwere Maschinengewehre, Granatwerfer und Panzerabwehrlenkflugkörper tragen. Der »Uran-9«, der entweder eine vorprogrammierte Route abfahren kann oder über eine Distanz von bis zu 3 km per Fernsteuerung bedient wird, wurde laut Pressemeldungen bereits im Syrienkrieg eingesetzt, offenbar aber mit enttäuschendem Ergebnis (Brown 2018).

Auch asiatische Länder wie *China* und *Indien* investieren verstärkt in die militärische UGV-Entwicklung. So veranstaltete China in den Jahren 2014 und 2016 je einen Wettbewerb für autonome UGVs nach dem Vorbild der DARPA, an dem größere und kleinere unbewaffnete mobile Bodensysteme teilnahmen (Ray et al. 2016, S. 70). Das kleine, bewaffnete Kettenfahrzeug »Sharp Claw 1« (Masse 120 kg) und ein noch kleinerer »Battle Robot« wurden schon 2014 vorgestellt (Lin/Singer 2014; Wong 2014). In Indien wiederum hat die staatliche Defence Research and Development Organisation (DRDO) laut inoffiziellen Meldungen neben unbewaffneten Kleinfahrzeugen, u. a. zur Entschärfung von Sprengfallen, die zwei bewaffneten UGVs »Rudra« und »Daksh Warrior« entwickelt (Indian Defense Blog 2017).

Nicht zuletzt arbeiten auch europäische Rüstungsfirmen an UGV-Systemen: Die französische Nexter S.A. hat kürzlich den bewaffneten »Optio-X20« vorgestellt, der für Beobachtungsaufgaben und zur Feuerunterstützung gedacht ist; der Kleinpanzer soll über autonome Navigationsfunktionen und einen ferngesteuerten 20-mm-Geschützturm verfügen. Von der deutschen Firma Rheinmetall stammt der »Mission Master«, ein modular aufgebautes unbemanntes Mehrzweckbodenfahrzeug, das für unterschiedliche Aufgaben »mit verschiedenen Subsystemen« ausgestattet werden kann. Darunter befindet sich auch eine bewaffnete Version für den Schutz von Einsatztruppen (Rheinmetall Group 2018). Die zum Transport von Ausrüstung vorgesehene Version des »Mission Master« ist bereits seit 2018 einsatzbereit.[31] Sie verfügt über die gängigen semiautonomen Fahrfunktionen und kann u. a. Soldaten automatisch folgen.

4.1.3 Systeme zu Wasser

Auf und unter Wasser besteht im Allgemeinen mehr Raum zum Manövrieren als auf Land, insbesondere auf hoher See (Altmann/Gubrud 2017, S. 86). Außerdem sind die Meere arm an Hindernissen und weitgehend menschenleer, sodass das Risiko von Kollateralschäden sehr gering ist. All dies würde den Unter- sowie Überwasserbereich eigentlich für den Einsatz autonomer Waffensysteme prädestinieren. Dass bislang kaum einsatzfähige seegestützte UWS vorliegen,

31 Inwiefern die bewaffnete Version über autonome Feuerauslösung verfügt, ist nicht bekannt – es ist jedoch davon auszugehen, dass auch in diesem Fall wie bei allen anderen beweglichen UGVs für die Waffenbedienung ein menschlicher Operator vorgesehen ist.

hängt u. a. mit den potenziell riesigen Einsatzräumen zusammen, die vor allem im submarinen Bereich mit Blick auf Energieversorgung und Kommunikation eine große Herausforderung darstellen (Dickow 2015, S. 15).

Überwasserfahrzeuge

Ideen für unbemannte Überwasserfahrzeuge (USV) existieren seit den 1980er Jahren: Damals kamen Konzepte auf, Boote fern- oder programmgesteuert für Aufklärung, Minensuche, Täuschung und als Waffenträger zu nutzen (Altmann/Gubrud 2017, S. 23). In den 2000er Jahren untersuchte und entwickelte die U.S. Navy verschiedene USV-Prototypen, es war aber die israelische Elbit Systems Ltd., die 2006 mit dem »Silver Marlin« das erste einsatzfähige bewaffnete USV vorstellte. Es dient vor allem der Überwachung und Aufklärung und soll auch bei schwerem Seegang, sowohl bei Tag als auch bei Nacht, »autonom vorgegebene Koordinaten ansteuern« können (Masirske 2009). Neben einem Radar und verschiedenen elektrooptischen Sensoren ist das knapp 11 m lange Boot mit einem stabilisierten Maschinengewehr ausgestattet, das jedoch rein ferngesteuert ist (Altmann/Gubrud 2017, S. 86). Weiterentwicklungen wie das für Anti-U-Boot- und Antimineneinsätze spezialisierte »Seagull« von Elbit Systems (o. J.), oder das in verschiedenen bewaffneten Varianten erhältliche »Protector« von Rafael Advanced Defense Systems Ltd. (RAFAEL o. J.b) illustrieren Israels Ambitionen im USV-Bereich (Alwardt et al. 2017, S. 23; Opall-Rome 2016).

Insgesamt ist das Spektrum sowohl an verfügbaren wie auch in Entwicklung befindlichen USVs aber noch recht klein, vor allem im Vergleich zu den im nächsten Kapitel besprochenen Unterwasserfahrzeugen (UUVs), die eine ungleich höhere militärstrategische Bedeutung aufweisen. Die U.S. Navy beispielsweise führte zwar 2014 und 2016 Demonstrationen eines Schwarms bewaffneter Motorboote durch, bei denen autonome Bewegung und gegenseitige Koordination zentrale Ziele waren (Smalley 2016), hat aber laut eigenen Angaben keine USVs stationiert (dafür aber unbemannte Luft- sowie Unterwasserfahrzeuge; Altmann/Gubrud 2017, S. 86).

Unterwasserfahrzeuge

Obwohl Torpedos im engeren Sinne nicht zu den Unterwasserfahrzeugen gezählt werden, sind sie wichtige Vorläufer und weisen etliche technologische Parallelen zu UUVs auf. Bereits seit dem Zweiten Weltkrieg verfügen sie teilweise über eine akustische Zielsuche und damit automatisierte Steuerungsfunktionen (wie im Falle des deutschen Torpedos T5 »Zaunkönig« oder der US-amerikanischen »Mark 24 Mine«; Altmann/Gubrud 2017, S. 101). Die Fähigkeiten moderner Torpedos wie beispielsweise des US-amerikanischen »MK 54« (Raytheon Technologies o. J.) sind im Prinzip vergleichbar zu denen fortschrittlicher

Lenkflugkörper, wie sie in Kapitel 4.1.1 beschrieben wurden: Navigation, die Abwehr von Gegenmaßnahmen sowie die Suche, Identifizierung und Verfolgung von Zielen (mittels Signaturerkennung) erfolgen nach dem Abschuss weitgehend ohne menschliches Zutun.

Die sowohl in Form als auch in Funktion an Torpedos angelehnten unbemannten Unterwasserfahrzeuge, auch als Unterwasserdrohnen bezeichnet, nehmen weltweit an Verbreitung zu.[32] Ihre militärischen Aufgaben konzentrieren sich allerdings bisher weitgehend auf Aufklärung, Überwachung und Seeminenräumung (Alwardt et al. 2017, S. 17; Dean 2017).[33] Beispiele sind u. a. der Seeotter »MKII« (AUVAC o. J.) von der deutschen Atlas Elektronik GmbH, die russische Unterwasserdrohne »Klavesin-2« (Navy Recognition 2018) oder der von Boeing entwickelte »Echo Ranger«, der dank eines »hybriden wiederaufladbaren Energiesystems« (McCaney 2016) mehrere Monate autark operieren können soll. Anders als Torpedos sind diese Systeme mit der Herausforderung konfrontiert, dass für militärisch wünschenswerte Einsatzradien (idealerweise über Hunderte oder gar Tausende Seemeilen) eine langfristige Energieversorgung, möglichst über mehrere Tage oder gar Wochen, und eine weitreichende Kommunikationsverbindung sicherzustellen sind. Besonders Letzteres stellt ein Problem dar: Während die Energiefrage über unterseeische Dockingstationen oder atomare Antriebe zumindest prinzipiell lösbar erscheint (Dombe 2016; Eckstein 2016), sind die Möglichkeiten der Kommunikation und Datenübertragung – und damit auch der Fernsteuerung – aufgrund der Absorption von Funkwellen und anderen elektromagnetischen Signalen in Meerwasser grundsätzlich begrenzt (Altmann/Gubrud 2017, S. 24). Dies hat letztlich zur Konsequenz, dass bei diesen UUV-Systemen (vor allem bei bewaffneten Einsätzen, die besonders hohe Ansprüche an die Verhaltensplanung mit sich bringen) sehr weitreichende Autonomie praktisch unabdingbar ist (Dean 2017), damit sie anspruchsvolle militärische Aufgaben in den Weiten der Ozeane sinnvoll erfüllen können. Um die Kommunikationsmöglichkeiten unter Wasser zu verbessern, arbeitet die U.S. Navy mithilfe der DARPA außerdem auch an der Entwicklung einer Art Unterwasser-Internet (McCaney 2015).

Die Entwicklung bewaffneter UUVs steckt aufgrund der beschriebenen Hürden erst in den Anfängen. Dennoch ist klar, dass weiträumig operierenden Unterwassersystemen perspektivisch eine hohe strategische Bedeutung zukommen könnte (Dickow 2015, S. 15). Laut dem Chief of Naval Operations (2016, S. 14) sind autonome UUVs eine wichtige Schlüsselkomponente, um die US-

32 Die Geschichte von UUVs reicht ebenfalls relativ weit zurück (Altmann/Gubrud 2017, S. 23): In den USA wurde in den späten 1950er Jahren das »cable-controlled underwater vehicle« (CURV) entwickelt und viel genutzt, u. a. zur Bergung der in spanischen Gewässern verlorengegangenen Wasserstoffbombe. Ab 1984 setzte die U.S. Marine die kabelgesteuerte »Deep Drone« ein, sie konnte bei 3 Knoten (5,6 km/h) Geschwindigkeit bis 1.800 m tief tauchen und war mit Videokameras, Sonar und Manipulatoren ausgestattet.

33 Für einen Überblick über verfügbare Systeme http://auvac.org (1.9.2020).

amerikanische Unterwasserdominanz zu verbessern und auszudehnen – entsprechend zeigen insbesondere die USA, Großbritannien, Russland und China ein großes Interesse an deren Entwicklung und Beschaffung (Alwardt et al. 2017, S. 17; New America o. J.a). So hat die U.S. Navy im September 2017 ein erstes UUV-Geschwader aufgestellt (Altmann/Gubrud 2017, S. 86 f.) (NAVALTODAY 2017). Größeres mediales Aufsehen erregten zudem Meldungen des Pentagon im Jahr 2018, dass Russland einen »neuen interkontinentalen, nuklear bewaffneten und angetriebenen autonomen Unterseetorpedo« testen soll, das als »Ocean Multipurpose System Status-6« bezeichnet wird und über eine Reichweite von 6.200 Meilen (9.978 km) verfügen soll (Ballesteros 2018) – über technische Einzelheiten des Systems und dessen aktuellen Entwicklungsstand gibt es allerdings derzeit keine verlässlichen Informationen.

4.2 Forschungs- und Entwicklungstrends

Während einige Länder enorme Ressourcen in die FuE zunehmend automatisierter Waffensysteme investieren (z. B. die USA und China), haben andere Länder Bedenken und zögern bisher (z. B. Deutschland). In diesem Kapitel werden – basierend auf dem Gutachten von Alwardt et al. (2017, S. 24 ff.) – die FuE-Aktivitäten wichtiger staatlicher Akteure hinsichtlich der Autonomisierung von unbemannten (bewaffneten) Systemen überblicksartig dargestellt. Wegen der Fülle an Aktivitäten wird kein Anspruch auf Vollständigkeit erhoben, das Ziel ist vielmehr, eine Vorstellung von zukünftigen Entwicklungspfaden zunehmend automatisierter Waffensysteme zu vermitteln. Zugleich ergeben sich auf diese Weise auch Anhaltspunkte über die potenziellen Fähigkeiten von zukünftigen AWS.

Im Bereich der heutigen FuE und auch in der Beschaffung unbemannter Waffensysteme sind die USA der weltweite Vorreiter, weshalb die US-amerikanischen FuE-Trends im Folgenden als wichtiger Maßstab dienen und den größten Raum einnehmen. Insbesondere Großbritannien, Israel und China orientieren sich stark an den Entwicklungen im Bereich der US-Rüstungsindustrie und des US-Militärs. Neben den Genannten werden weitere Schlüsselakteure betrachtet, nämlich Deutschland, Frankreich und Russland.

Überwiegend beziehen sich die Informationen auf militärische unbemannte Systeme im Allgemeinen und nicht auf unbemannte Waffensysteme im Speziellen. Die resultierenden technologischen Trends im Hinblick auf unbemannte Systeme gelten aber erst einmal unabhängig von einer möglichen Bewaffnung, welche ggf. auch parallel oder nachträglich erfolgen kann. Neben den breiteren FuE-Trends wird exemplarisch auch auf einige konkrete Entwicklungs- und Beschaffungsprojekte von UWS eingegangen.

4.2.1 USA

Die USA sind als Vorreiter und Treiber der Entwicklungen zunehmend automatisierter Waffensysteme und als wesentlicher Wegbereiter für zukünftige autonome Waffensysteme anzusehen (dazu und zum Folgenden Alwardt et al. 2017, S. 28). Zum einen gibt es in den USA auf den Gebieten der Robotik und künstlichen Intelligenz eine Vielzahl hochkarätiger Forschungseinrichtungen und Universitäten (Boulanin 2016a). Zum anderen haben die USA mit der Policy Directive 3000.09 (DOD 2012) als erstes und bisher einziges Land damit begonnen, ein formales Regelwerk für die Entwicklung und den Gebrauch semiautonomer und autonomer Waffensysteme zu entwickeln; darin werden u. a. Bedingungen festgelegt, unter denen autonome und halbautonome Waffensysteme stationiert und eingesetzt werden dürfen (Altmann/Gubrud 2017, S. 154).

Passend dazu betonte der damalige US-Verteidigungsminister Chuck Hagel (2014) in der »Third Offset Strategy«[34] die im November 2014 von ihm angestoßen wurde, die große militär(strateg)ische Bedeutung von künstlicher Intelligenz und Autonomie (dazu und zum Folgenden Alwardt et al. 2017, S. 28; Altmann/Gubrud 2017, S. 153 ff.). Der stellvertretende US-Verteidigungsminister Robert Work wurde mit der Leitung der Initiative beauftragt (Work 2016). Er setzt dabei laut Ellman et al. (2017, S. 3) auf folgende technologischen Schlüsselbereiche: autonome Lernsysteme, kollaborative Entscheidungsfindung zwischen Mensch und Maschine, assistierte menschliche Operationen, fortgeschrittene Einsätze bemannter und unbemannter Systeme (»advanced manned-unmanned systems operations«), netzwerkfähige autonome Waffen sowie Hochgeschwindigkeitsprojektile. Ohne direkt auf die dritte Offsetstrategie Bezug zu nehmen, werden deren Schwerpunkte von der Trump-Administration offenbar fortgeführt, vor allem mit Fokus auf die Entwicklung autonomer Systeme (DOD 2018b, S. 7; Thomas 2017). So wurde vom US-Verteidigungsministerium (DOD 2019) ein neues Joint Artificial Intelligence Center (JAIC) (Pomerleau 2018) eingerichtet, das die militärische Forschung in diesem Bereich vorantreiben soll. Passend dazu unterzeichnete Präsident Donald Trump Anfang Februar 2019 eine Anordnung, die von den Regierungsbehörden mehr Engagement bei Forschung, Förderung und Ausbildung im Bereich der künstlichen Intelligenz verlangt (Pamuk/Shepardson 2019; U.S. President 2019).

Der langjährige Trend zeigt in den USA also deutlich in Richtung AWS, was sich auch in den vom DOD regelmäßig publizierten militärischen Entwick-

34 Im Deutschen sinngemäß »Dritte Kompensationsstrategie«. Darunter versteht man die asymmetrische Kompensation im militärischen Wettbewerb durch eine Kombination von militärischer Strategie, Technologie und Streitkräfteorganisation (dazu und zum Folgenden Alwardt et al. 2017, S. 25). Die erste Offsetstrategie war die Einführung von Nuklearwaffen, Bombern und Raketen unter Präsident Dwight Eisenhower angesichts der konventionellen Überlegenheit der sowjetischen Streitkräfte in den 1950er Jahren, während die zweite Offsetstrategie (1970er/1980er Jahre) auf die zunehmende Bedeutung von digitalen Mikroprozessoren, Informationstechnologien, Sensoren und Tarnkappenfähigkeit setzte.

lungsstrategien zu unbemannten Systemen (»Unmanned Systems Integrated Roadmap«) widerspiegelt. Das DOD (2013, S. 71) gibt in seiner Roadmap von 2013 an, dass die USA für den Zeitraum 2017 bis 2020 planten, »[to] move the capability further along the scale from automatic to autonomous behavior«. Auch in der aktuellen Roadmap von 2017 wird diese Linie bestätigt: Autonomie und Robotik werden dort als Schlüsselfaktoren für die weitere Entwicklung unbemannter Systeme benannt, die das Potenzial hätten, die zukünftige Kriegsführung zu revolutionieren (DOD 2017c, S. v). Entsprechendes ist ebenfalls in den Strategiepapieren der einzelnen Teilstreitkräfte zu lesen (DON 2018; U.S. Air Force 2016; U.S. Army 2017b), in denen autonomen Systemen eine entscheidende Rolle in zukünftigen Konflikten zugeschrieben wird. So stellt beispielsweise die U.S. Navy (2013, S. 4) in ihrer »Information Dominance Roadmap 2013–2028« fest, Streitkräfte könnten zukünftig unterstützt werden durch »improved robotics and remotely-guided autonomous and miniaturized weapons«. Anhand von aktuellen Strategiepapieren, Weißbüchern und Informationen staatlicher Institutionen ergibt sich so ein recht gutes Bild der mittel- und langfristigen FuE-Ziele auf dem Feld zunehmend automatisierter Systeme des US-Militärs.

Bereits heute investieren die USA stattliche Summen in entsprechende FuE (dazu und zum Folgenden Alwardt et al. 2017, S. 26). Geforscht wird sowohl in übergeordneten Forschungsinitiativen wie dem Programm »Science of Autonomy«[35] des ONR oder der »Defense Innovation Unit Experimental« (DIUx)[36] als auch in kleineren spezifischen Programmen, von denen im Folgenden einige beispielhaft genannt werden.[37] Für die dritte Offsetstrategie, die sich stark auf semiautonome und autonome Systeme konzentriert, wurden 2016 knapp 18 Mrd. US-Dollar für einen Zeitraum von 5 Jahren veranschlagt (Gady 2016). Den Angaben des DOD (2013, S. 3) zufolge sahen die USA für den Zeitraum von 2016 bis 2018 für FuE, Beschaffung und Betrieb unbemannter Systeme 14,49 Mrd. US-Dollar vor. Hinsichtlich des Plattformtyps liegt der Schwerpunkt dabei eindeutig auf UAVs, deren finanzieller Anteil in diesem Zeitraum 13,1 Mrd. US-Dollar betragen sollte. Deutlich abgeschlagen an zweiter Stelle folgten maritime Systeme, also USVs und UUVs, die mit etwa 400 Mio. US-Dollar gefördert werden sollten. Für UGVs hingegen waren im Zeitraum von 2016 bis 2018 nur etwa 164 Mio. US-Dollar vorgesehen (DOD 2013, S. 3). Trotz

35 Im Programm »Science of Autonomy« wird Grundlagenforschung in verschiedenen Themenfeldern für unbemannte Schiffe und U-Boote, insbesondere hinsichtlich neuer Konzepte für Schwärme, maschinelles Lernen und Teamfähigkeit zwischen Mensch und Maschine betrieben (ONR o. J.a).

36 Das DIU wurde 2014 vom DOD ins Leben gerufen und soll im zivilen Sektor aufkommende Technologien schneller in militärische Nutzungen überführen. Der Fokus liegt auf Themen wie Roboter, autonome Systeme, Miniaturisierung, Big Data sowie moderne Fertigungstechnologien einschließlich 3-D-Drucker (Tucker 2015).

37 Für einen detaillierten Überblick über die militärischen FuE-Programme der USA mit AWS-Bezug vgl. auch Altmann/Gubrud 2017, S. 114 ff.

dieses weitreichenden Engagements kam das DSB (2016, S. 1) zu dem Schluss, dass das Verteidigungsministerium die Erschließung (»exploitation«) der Autonomie weiter beschleunigen muss.

Diesbezüglich hat die Automatisierung von Datenprozessen mithilfe von machinellem Lernen und KI einen hohen Stellenwert (dazu und zum Folgenden Alwardt et al. 2017, S. 27 f.). Automatisierte Datenprozesse sollen Kommandeure und Soldaten zukünftig dabei unterstützen, Entscheidungen zu treffen und mittelfristig auch bei der Wahl der »richtigen« Waffen für das »richtige« Ziel behilflich zu sein (»automated battle management aids«) (U.S. Navy 2013, S. 29). In aktuellen FuE-Programmen werden u. a. neue Algorithmen für die Organisation und Zusammenführung von komplexen Daten oder Bild- und Datenverarbeitung hinsichtlich genauer Zielauswahl und autonomer Navigation entwickelt (siehe z. B. apan o. J.). In anderen Projekten wird an der selbstständigen Erfassung und Erkennung von Objekten, von U-Booten, Kleinwaffen und Luftangriffen gearbeitet.[38] Militärische Grundlagenforschung im Hinblick auf KI und maschinelles Lernen findet beispielsweise im Rahmen des Pentagonprojekts »Maven«,[39] in den Forschungsprogrammen »Computational Methods for Decision Making« (ONR o. J.b) sowie »Computational Cognition and Machine Intelligence« der U.S. Air Force Office of Scientific Research Laboratory (apan o. J.b) statt.

Trends hinsichtlich der Abmessungen

Hinsichtlich der Abmessungen von unbemannten Systemen sind zwei gegensätzliche Trends in der militärischen Forschung in den USA festzustellen. Auf der einen Seite stehen kleine kostengünstige UAVs und UGVs im Fokus, welche Soldaten bei ihren Einsätzen mitführen können oder die in großer Anzahl als Schwarm operieren sollen (dazu und zum Folgenden Alwardt et al. 2017, S. 26 f.). In dem Programm »Low-Cost UAV Swarming Technology« (LOCUST) wird gezielt darauf hingearbeitet, die Produktionskosten unbemannter Systeme zu reduzieren (Boulanin 2016b, S. 37). Der Trend zur Miniaturisierung wird anhand der Veröffentlichung einer eigenen Roadmap deutlich, dem »Small Unmanned Aircraft Systems (SUAS) Flight Plan: 2016–2036« der U.S. Air Force (2016); und im Programm »Fast Lightweight Autonomy« (FLA) arbeitet z. B. auch die DARPA (o. J.b) an kleinen und schnellen autonomen Luftfahrzeugen. Auf der anderen Seite geht der FuE-Trend zu größeren und leistungsfähigeren unbemannten Systemen, die u. a. mehr Ausdauer, Robustheit, Nutzlast oder

38 Eine strukturierte Übersicht zu US-amerikanischen FuE-Aktivitäten in Bezug auf AWS findet sich in Boulanin 2016b, S. 31 ff.

39 Ziel des 2017 gestarteten Projekts »Maven« ist die automatisierte Analyse von Bildern und Videos, die von Drohnen aufgezeichnet wurden (Pellerin 2017). Als bekannt wurde, dass Google an diesem Projekt beteiligt ist, kam es zu Protesten unter Google-Mitarbeitern, sodass die Firma die Zusammenarbeit mit dem Pentagon schließlich nicht verlängerte (Peitz 2018).

Geschwindigkeit aufweisen sollen (Boulanin 2016b, S. 31 ff.). Im Bereich der UUVs wird an großen multifunktionalen Systemen geforscht, die von Schiffen oder militärischen Basen starten können. Entsprechende Forschung findet z. B. im Programm »Large Displacement Unmanned Undersea Vehicles« statt, welches sich aktuell in der Testphase befindet (Pomerleau 2016). Das ONR und die DARPA untersuchen Möglichkeiten zur Steigerung der Ausdauer bzw. Stehzeiten militärischer Systeme im Feld, insbesondere auch für U-Boote und Schiffe, da diese sich über weite Distanzen und lange Zeiträume im offenen Meer bewegen können sollen (DOD 2013, S. 88 u. 138). Einer der Schlüsselfaktoren ist hier die Energiefrage. Es wird daran geforscht, wie sich Energie aus natürlichen Quellen wie Solarkraft oder Wellenbewegungen gewinnen lässt.[40]

Anwendungskonzepte: Schwärme sowie Mensch-Maschine-Teams

Bezüglich zukünftiger Anwendungskonzepte ist es ein wichtiges Anliegen der US-Streitkräfte, unbemannte Systeme in Gruppen kommunizieren und kooperativ zusammenarbeiten zu lassen (dazu und zum Folgenden Alwardt et al. 2017, S. 28). Teams aus unbemannten Systemen werden auch Schwärme genannt (Kasten 4.1). Das ONR forscht beispielsweise an einer Software, die es ermöglichen soll, UUVs als Schwarm zu koordinieren und autonom fahren zu lassen (Smalley 2016). Die DARPA (o. J.c) wiederum arbeitet an heterogenen Gruppen autonomer Luftfahrzeuge und das U.S. Army Combat Capabilities Development command Army Research Laboratory (CCDC ARL)[41] an schwärmenden mobilen, multifunktionalen Mikrorobotern (Luft-Boden) für Einsätze in urbanem Gelände. Im Oktober 2016 ließ die U.S. Air Force bereits 103 unbewaffnete Mikro-UAVs vom Typ »Perdix« im Schwarm fliegen (DOD 2017c). Neben der intensiveren Vernetzung ist hierbei die Weiterentwicklung von Sense-and-avoid-Technologien für komplexe Umgebungen notwendig, die dazu befähigen sollen, Hindernisse wahrzunehmen, ihnen auszuweichen und Kollisionen zu vermeiden. Insbesondere die Air Force und die Navy arbeiten an diesen Technologien (DOD 2013, S. 68).

Neben Schwarmtechnologien ist die Entwicklung von Teams aus Mensch und Maschine (MUM-T), ein weiteres zentrales Ziel von U.S. Air Force, U.S. Navy und U.S. Army (DOD 2013, S. 69; U.S. Air Force 2016, S. 17) (dazu und zum Folgenden Alwardt et al. 2017, S. 28 f.). So kann z. B. dem Piloten eines Kampfjets ein einzelnes UCAV als »loyal wingman« (U.S. Air Force 2016, S. 45) zur Seite gestellt werden – oder sogar ein kompletter Schwarm, der der Kontrolle des Piloten untersteht. Laut der »Robotic and Autonomous Systems

40 Es gibt bereits unbewaffnete Unterwasserroboter wie den »slocum thermal glider«: http://auvac.org/configurations/view/51 (1.9.2020), die aus Wassertemperaturunterschieden Energie beziehen und so bis zu 5 Jahre ohne zu tanken Meereserkundungen durchführen können.

41 https://www.arl.army.mil/www/default.cfm?page=332 (30.12.2019)

Strategy« der U.S. Army (2017b, S. 24) produziert MUM-T Synergien und führt zu asymmetrischen Vorteilen – wobei jedoch nicht weiter ausgeführt wird, worin genau diese bestehen. Auch in der Roadmap von 2013 (DOD 2013, S. 139) heißt es, das MUM-T-Konzept sieht vor, »die inhärenten Stärken bemannter Plattformen mit den Stärken der unbemannten zu kombinieren, mit Produktsynergien, die bei einzelnen Plattformen nicht zu finden sind«.[42] An MUM-T wird daher intensiv geforscht[43] – in der FuE-Budgetanfrage für das Jahr 2017 veranschlagte das US-Verteidigungsministerium dafür insgesamt 3 Mrd. US-Dollar (inklusive »human-machine collaboration«; Gady 2016).

Für die fernere Zukunft setzen die US-Streitkräfte auf unbemannte Fahrzeuge und komplexe Schwarmsysteme, die autonom agieren können, um menschliche Streitkräfte – auch in zugangsverwehrten Gebieten, dem Anti-Access-and-Area-denial-Umfeld – zu unterstützen (U.S. Army 2017b, S. 9 ff.) (dazu und zum Folgenden Alwardt et al. 2017, S. 29). Geplant ist, unbemannte taktische Fahrzeuge zukünftig als »force multiplier« einzusetzen, d. h. in unterstützender Form als Teil interaktiver Mensch-Maschine-Operationen (DOD 2013, S. 32 ff.). Laut dem Leiter der Robotikabteilung des Army Capabilities Integration Centre, ist dabei zwar autonome Navigation vorgesehen, nicht jedoch der autonome Waffeneinsatz (Magnuson 2017). Auch das U.S. Marine Corps verspricht sich perspektivisch Unterstützung durch autonome Waffensysteme, die in der Lage sind, sich in taktischer Hinsicht ähnlich wie ein Mensch zu verhalten (DOD 2013, S. 72 f.). Ebenso die Air Force: Sie will das Loyal-Wingman-Konzept so weiterentwickeln, dass kleine UAVs zukünftig in der Lage sind, bemannte Luftfahrzeuge zu begleiten und zu unterstützen (U.S. Air Force 2016, S. 12) – Fortschritte in der Autonomie spielen dabei laut U.S. Air Force eine Schlüsselrolle. Neben der Entwicklung von autonom agierenden UAV-Schwärmen sollen zudem per »multi-aircraft control« (MAC) die Möglichkeiten einzelner Piloten ausgeweitet werden, in der Luft die Kontrolle über eine größere Anzahl von Drohnen auszuüben.

Kasten 4.1 Schwärme als neue Form der Kriegsführung?

Unbemannte Systeme könnten sowohl zu Luft, zu Wasser als auch zu Land in großen koordinierten Gruppen oder Schwärmen eingesetzt werden. Die U.S. Air Force (2016, S. 45) beschreibt einen Schwarm als »eine Gruppe von autonom vernetzten kleinen UAVs, die kollaborativ operieren, um gemeinsame Ziele mit einem Betreiber auf oder in der Schleife zu erreichen«.[44]

42 Im Original: »to combine the inherent strengths of manned platforms with the strengths of UAS, with product synergy not seen in single platforms«.
43 Für Projektbeispiele vgl. Boulanin 2016b, S. 31 ff.
44 Im Original: »a group of autonomous networked SUAS operating collaboratively to achieve common objectives with an operator on or in the loop«.

Das Schwarmprinzip basiert auf der taktischen Idee, die Abwehr dadurch zu überfordern, dass man ein bestimmtes Ziel gleichzeitig von vielen Seiten und mehrfach angreifen lässt (Scharre 2014b). Da der Verlust eines oder weniger Einzelsysteme kaum Auswirkungen auf die Gesamtwirkung eines Schwarms hat, verspricht man sich davon nicht nur eine besonders wirkungsvolle, sondern auch eine besonders robuste Art der Kampfführung (Dickow 2015, S. 13).

Die erfolgversprechende Umsetzung dieses Prinzips setzt dreierlei voraus: erstens die kommunikative Vernetzung der Einheiten, was entsprechender Kommunikationsverbindungen bedarf. Zweitens müssen die Bestandteile eines Schwarms über die Fähigkeit verfügen, weitgehend autonom zu agieren – zumindest was die Navigation und Reaktion auf unvorhergesehene Ereignisse betrifft –, da die koordinierte Steuerung vieler Einheiten in Echtzeit durch einen (oder mehrere) Befehlshaber dessen Fähigkeiten, das verfügbare Personal und die Kommunikationsmöglichkeiten übersteigt. Schwarmkonzepte sehen deshalb keine zentralisierte Befehlsstruktur vor, wie im Militär ansonsten üblich. Eine weitere Bedingung ist schließlich, dass die Einheiten in möglichst großer Zahl sowie zu möglichst geringen Kosten verfügbar sind, was jedoch im Gegenzug impliziert, dass ihre Fähigkeiten eher begrenzt sind, jedenfalls im Vergleich zu teureren Systemen. Dies gilt besonders in Hinsicht auf Reichweite, Geschwindigkeit, Ausdauer und Nutzlast sowie in der Konsequenz auch für die Letalität und andere Wirkfähigkeiten.

Obwohl das Schwarmprinzip bereits im Zweiten Weltkrieg angewendet wurde – beispielsweise im U-Boot-Krieg oder in der Schlacht um Britannien (Arquilla/Ronfeldt 2000) –, bieten die Fortschritte in Robotik und KI ganz neue Möglichkeiten, unzählige Einzelplattformen in koordinierter Form miteinander zu vernetzen (Tucker 2017). Damit verbunden ist ein militärischer Paradigmenwechsel: »weg vom teuren Einzelsystem, hin zum preisgünstigen Wegwerfsystem« und weg von der zentralen zur dezentralen Steuerung (Dickow 2015, S. 13). Trotz der inzwischen vielen Demonstrationen von fliegenden Drohnenschwärmen – mit teilweise bis zu Hunderten Einheiten (DOD 2017) – und auch einiger Experimente zu Land und zu Wasser steht die Entwicklung bewaffneter Schwärme aus unbemannten Systemen noch relativ am Anfang. Offene Forschungsfragen betreffen neben der Miniaturisierung von Systemkomponenten u. a. die »effiziente Schwarmkommunikation, [die] Parallelisierung von Aufgabenbewältigung und [die] übergeordnete Steuerung durch angemessene Kompetenzverteilung« (Dickow 2015, S. 13; für Details zu einzelnen Forschungsprogrammen Kap. 4.2).

Quelle: Altmann/Gubrud 2017, S. 61 ff. u. S. 174 ff.

Entwicklungs- und Beschaffungsprojekte

Die USA engagieren sich in zahlreichen Entwicklungs- und Beschaffungsprojekten im Bereich unbemannter Systeme.[45] Dazu gehört etwa der Prototyp eines autonomen Wasserfahrzeugs mit großer Reichweite zur Aufspürung und Bekämpfung von dieselelektrischen U-Booten (»anti-submarine warfare continuous trail unmanned vessel« – ACTUV), der jüngst von der DARPA (o. J.d) zur Weiterentwicklung an die U.S. Navy übergeben wurde (Szondy 2018). Der klare Schwerpunkt der Entwicklungsaktivitäten liegt aber auf autonomen Kampfflugzeugen (dazu und zum Folgenden Altmann/Gubrud 2017, S. 107; Alwardt et al. 2017, S. 29):

- Die U.S. Air Force arbeitet bereits seit mindestens 1999 an der Entwicklung unbemannter Kampfflugzeuge, beginnend mit der »Boeing X-45«, die ihren Erstflug 2002 absolvierte und Teil des J-UCAS-Projekts (»Joint Unmanned Combat Air System«) von DARPA war (Airforce Technology o. J.).[46] Bedeutende aktuelle Projekte im Bereich unbemannter Flugsysteme sind z. B. die Hochgeschwindigkeitsplattformen »XQ-58 Valkyrie« und »UTAP-22 Mako«, beide entwickelt von Kratos (o. J.). Das etwa 9 m lange UCAV-Modell »XQ-58 Valkyrie« soll eine Traglast von ca. 227 kg und eine ungefähre Reichweite von 3.500 km haben; es könnte mit leistungsfähigen Zielsensoren und schweren_Waffen ausgestattet werden, z. B. 113-kg-Small-Diameter-Bomben (Drew 2017). Ein erster Flugtest fand im Frühjahr 2019 statt (Wright-Patterson Air Force Base 2019). Die »UTAP-22 Mako« UCAVs sollen mit bis zu 250 kg Munition ausgestattet werden können, Testflüge fanden im Sommer 2017 statt. Sowohl bei »Valkyrie« als auch bei »Mako« soll es sich um relativ kostengünstige, schwarmfähige Kampfdrohnen handeln, die bemannten Plattformen zukünftig als loyaler Flügelmann (»loyal wingmen«) in umkämpften Lufträumen (»contested airspace«) dienen können (Airforce Technology 2017).
- Die U.S. Navy verfolgt seit 2010 das Vorhaben, eine trägergestützte Kampfdrohne mit Stealth-Eigenschaften und Angriffsfähigkeiten zu entwickeln (Programm »Unmanned Carrier Launched Airborne Surveillance and Strike« – UCLASS) (Naval Drones 2016). Ergebnis war u. a. der Prototyp »X-47B« von Northrop Grumman, ein schwanzloses Unterschall-UCAV mit Düsenantrieb und verringerter Radarsignatur, das von 2011 bis 2015

45 Aufstellungen hierzu finden sich u. a. in den »Unmanned Systems Integrated Roadmaps« oder in spezifischen Dokumenten der US-Teilstreitkräfte; für einen detaillierten Überblick über US-amerikanische Forschungs- und Entwicklungsprogramme mit AWS-Bezug vgl. Altmann/Gubrud 2017, S. 114 ff.

46 Für eine detaillierte Rekonstruktion der Entwicklungsgeschichte US-amerikanischer Kampfdrohnen vgl. Rogoway 2016.

erfolgreich erprobt wurde.[47] Nachdem Zweifel an der Sinnhaftigkeit einer trägergestützten Angriffsdrohne aufgekommen waren, entschied die U.S. Navy 2016, das Beschaffungsprogramm neu auszurichten und den Fokus weg von Überwachung und Angriff und stattdessen auf Aufklärung und Luftbetankung zu legen – Aufgaben, die durch das von Boeing derzeit entwickelte Nachfolgesystem »MQ-25 Stingray« erfüllt werden sollen (Einsatzfähigkeit wird für die Mitte der 2020er Jahre erwartet; Osborn 2016).

4.2.2 Europa

Deutschland

Von deutscher Seite gab es bislang kein starkes Engagement für umfassende Investitionen in die FuE oder Beschaffung zunehmend automatisierter Waffensysteme (dazu und zum Folgenden Alwardt et al. 2017, S. 30). Ein Wandel diesbezüglich scheint sich aber abzuzeichnen. So bewilligte der Bundestag im Juni 2018 das Leasing israelischer »Heron-TP«, wenn auch vorerst nur zu Aufklärungszwecken. Verteidigungsministerin Ursula von der Leyen wiederum begründete 2014 den Bedarf einer europäischen UCAV-Entwicklung damit, dass Europa unabhängiger von anderen Staaten werden solle, insbesondere von führenden Drohnenproduktionsländern wie den USA und Israel. Es sei zudem nötig, das technologische Know-how in Europa zu kultivieren, und zwar »nicht nur unter militärischen Gesichtspunkten, sondern vor allem für die zivilen Möglichkeiten, die dahinter stecken« (Süddeutsche Zeitung 2014). Im Weißbuch zur Zukunft der Bundeswehr von 2016 werden FuE-Aktivitäten im Rüstungsbereich als »zentraler Treiber der Innovationskraft von Streitkräften und wehrtechnischer Industrie« hervorgehoben. Weiter heißt es, dass »die heutigen Herausforderungen rund um die Bereiche Cyber- und Informationsraum und Digitalisierung, autonome Systeme und Hybridisierung die Fortentwicklung und Erweiterung des klassischen FuT-Ansatzes mit Eigenmitteln« verlangen (Bundesregierung 2016, S. 131). Eine ausformulierte langfristige deutsche Strategie für teilautomatisierte oder autonome Waffensysteme gibt es jedoch nicht.

Hinsichtlich der FuE zu Automatisierungsfragen mit militärischem Bezug ist Deutschland derzeit auf EU-Ebene an einem Joint-Investment-Programm der European Defence Agency zu »Remotely Piloted Aircraft Systems« beteiligt (Alwardt et al. 2017, S. 30). Gemeinsam wollen die zehn beteiligten Staaten neue Technologien entwickeln und EU-Richtlinien schaffen, damit unbemannte Luftfahrzeuge, insbesondere solche militärischer Art, den nichtbeschränkten Luftraum nutzen können (EDA 2015; vgl. Bundesregierung 2016, S. 74). Aktuell

47 »X-47B« führte Flugzeugträgerlandungen und -starts erfolgreich aus und demonstrierte 2015 die erste autonome Luftbetankung (Spiegel Online 2013).

wirkt Deutschland in diesem Rahmen an zwei Forschungs- und Technologieprojekten mit (zum Folgenden EDA 2019):

- Das Projekt »Enhanced RPAS Autonomy« (ERA) wurde 2015 lanciert und wird von Deutschland (als federführende Nation) zusammen mit Frankreich, Polen, Schweden und Italien finanziell gefördert (Laufzeit bis 2019, Verlängerung bis 2020 in Vorbereitung; Deutscher Bundestag 2018a, S. 6320). Ziel ist es, die Automatisierung als Schlüsselfaktor für die Integration unbemannter Luftfahrzeuge in den nichtbeschränkten Luftraum technologisch voranzutreiben, vor allem in Hinsicht auf die Sicherheit und die Notfallprozeduren bei Start, Landung sowie Rollen am Boden.
- Im Projekt »MIDair Collision Avoidance System« (MIDCAS) wurde untersucht, wie unbemannte Flugfahrzeuge Hindernisse entdecken und umgehen können. Darüber hinaus wurde die Entwicklung von technischen Standards auf EU-Ebene unterstützt. Neben Schweden (als federführender Nation) und Deutschland waren auch Frankreich, Italien und Spanien beteiligt. Das Programm lief Ende 2018 aus (Deutscher Bundestag 2018a, S. 6320).

Seit 2016 engagiert sich Deutschland außerdem in führender Rolle in der Entwicklung eines europäischen UCAV der neusten Generation, das unter der Bezeichnung European MALE RPAS (»medium altitude long endurance remotely piloted aircraft system«) firmiert (Hoffmann 2015; dazu und zum Folgenden Alwardt et al. 2017, S. 30). Hauptaufgaben der »Eurodrohne« sollen Überwachungs- und Aufklärungsmissionen sein; sie soll aber auch bewaffnet werden können. An dem Entwicklungsprojekt sind neben Deutschland auch Frankreich, Italien, Spanien beteiligt. In einer zweijährigen Konzeptstudie, die im Herbst 2016 startete, wurden die jeweiligen nationalen Anforderungen an die Kampfdrohne untersucht und ein Systemdesign entwickelt.[48] Nach 10-monatiger Untersuchung einigten sich die beteiligten Länder 2017 auf eine Drohnenkonfiguration mit zwei Turboproptriebwerken, die erstmals 2018 als Eins-zu-eins-Modell auf der Internationale Luft- und Raumfahrtausstellung in Berlin vorgestellt wurde (UAS Vision 2017). Das mit der Durchführung der Studie beauftragte internationale Industriekonsortium bestand aus Airbus Defense and Space (in Deutschland und Spanien), Dassault Aviation (Frankreich) und Leonardo (Italien). Von der federführenden europäischen Organisation for Joint Armament Cooperation (OCCAR) wurde Airbus als Hauptkontraktor für die folgende Entwicklungsphase ausgewählt mit dem Ziel eines Erstflugs 2023 und der Auslieferung des ersten Systems etwa 2025. Airbus rechnet mit Entwicklungskosten von ca. 1 Mrd. Euro (Hoffmann 2015; OCCAR o. J.).

Zusammen mit Frankreich treibt Deutschland zudem zwei Rüstungsvorhaben für die Luft- und Landstreitkräfte voran, die im militärischen

48 Deutschland trug einen Kostenanteil von 18,6 Mio. Euro (31 %) an der Konzeptstudie, die anderen drei Länder jeweils 13,8 Mio. Euro (Hoffmann 2015).

Hochtechnologiebereich angesiedelt sind (BMVg 2018a). Zum einen gehört dazu die Entwicklung eines »Luftkampfsystems der Zukunft« (»future combat air system« – FCAS) bis 2040, das von Dassault Aviation und Airbus produziert werden soll. Laut dem (BMVg 2018a) handelt es sich beim FCAS um ein »Waffensystem der nächsten Generation«, das »sowohl bereits existierende als auch zukünftige bemannte und unbemannte Komponenten in einem interoperablen Verbund vereinen« wird – wobei »die unbemannten Systeme [...] die Fähigkeiten des gesamten Projekts entscheidend prägen und dessen Überlebens- und Durchsetzungsfähigkeit gewährleisten« werden. Eine erste gemeinsame Konzeptstudie wird ab 2019 erstellt (K.S. 2019). Zum anderen soll unter industrieseitiger Führung Deutschlands bis Mitte 2030 das »main ground combat system« (MGCS) entwickelt werden, das den Kampfpanzer »Leopard 2« ablösen soll. Verfolgt wird ein »Systemansatz, in dem auch unbemannte mit bemannten Systemen zusammenwirken sollen« (BMVg 2018a).

Über die geplanten Autonomiefähigkeiten sowohl des FCAS als auch des MGCS ist derzeit noch nichts bekannt – in ihrer Antwort auf eine entsprechende parlamentarische Anfrage hat die Bundesregierung jedoch erneut bestätigt, dass sie autonome Waffensysteme ablehnt und dass »bei Entscheidungen über den letalen Waffeneinsatz [...] die menschliche Kontrolle erhalten bleiben« muss (Bundesregierung 2018b).

Frankreich

Vom französischen Verteidigungsweißbuch aus dem Jahr 2013 ergibt sich kein Aufschluss über unbemannte oder autonome Waffensysteme, sondern es finden nur Überwachungs-UAVs im Zusammenhang mit automatisierter Informationsverarbeitung Erwähnung (Ministère de la Défense 2013; dazu und zum Folgenden Alwardt et al. 2017, S. 32 ff.). In einem Senatsbericht von 2016 wurde festgestellt, dass wegen der Komplexität moderner Schlachtfelder und neuer Waffentechnologien eine stärkere Automatisierung nützlich ist, vor allem damit französischen Soldaten ein besseres Lagebild und damit auch eine bessere Entscheidungsgrundlage zur Verfügung stehen (Gautier et al. 2016, S. 90). Gleichzeitig ist es Frankreich traditionell äußerst wichtig, dass es in der nationalen Verteidigung eine gewisse Unabhängigkeit bewahrt. Es hat den Anspruch, selbst über die notwendigen Technologien zu verfügen und eine wettbewerbsfähige Industrie zu haben, damit die französischen Streitkräfte ihre Aufgaben erfüllen können (Ministère de la Défense/DGA 2013, S. 3).

Die französische militärische FuE-Ausrichtung im Zeitraum 2014 bis 2019 baut auf Autonomie als eines der Mittel auf, um französische Kampfsysteme zu modernisieren, insbesondere an der Schnittstelle zwischen Mensch und Maschine, wie z. B. im Bereich der Entscheidungsfindung (dazu und zum Folgenden Alwardt et al. 2017, S. 32 f.). Die französische KI-Strategie macht

diesbezüglich deutlich, dass Frankreich zwar möchte, dass die Anwendung tödlicher Gewalt dem Menschen vorbehalten bleibt – was sich auch in dem entsprechenden Engagement in den CCW-Verhandlungen widerspiegelt (Kap. 9.2) –, gleichzeitig aber auch bei der Forschung zu »diesem wichtigen strategischen Bereich« nicht hinter andere Staaten zurückfallen möchte (Villani 2018, S. 125).

Im Themenfeld Robotik und Informatik treibt Frankreich FuE u. a. in den drei folgenden Bereichen voran: erstens Kommunikationssicherheit, zweitens Roboter und komplexe kognitive Systeme sowie drittens digitale Verarbeitung und Analyse von Big Data. Im Rahmen des letzten Bereichs wird etwa im Programm »Système d'aide à l'interprétation multicapteurs« (SAIM) geforscht. Damit verbunden ist die Weiterentwicklung von Multifunktionssensoren, von Techniken der Datenfusion sowie der Daten- und Bildverarbeitung. Ein besonderes Augenmerk soll hierbei auf der Luftfahrt liegen. Im maritimen Bereich werden als Prioritäten autonome Hochleistungsnavigationssysteme, der Bereich Entscheidungsfindung und die Seeminenräumung aufgelistet (Ministère de la Défense/DGA 2013, S. 21 u. S. 26 ff.). Das militärische Auftragswesen von Waffensystemen sowie die militärische FuE wird in Frankreich von der Direction générale de l'armement (DGA) koordiniert.

Bei der Entwicklung von unbemannten Waffensystemen setzt Frankreich hauptsächlich auf UCAVs, und das in dreifacher Hinsicht (dazu und zum Folgenden Alwardt et al. 2017, S. 32 f.):

- Erstens ist es an dem von Deutschland angeführten MALE-RPAS-UCAV-Entwicklungsprogramm beteiligt, das bereits zuvor beschrieben wurde.
- Zweitens führt es mit Dassault Aviation das internationale Entwicklungskonsortium des nEUROn-Technologie-Demonstrators für eine europäische Kampfdrohne der MALE-Klasse an, die Tarnkappentechnik und autonome Funktionen aufweisen soll (Altmann/Gubrud 2017, S. 108 ff.).[49] Das Projekt wurde 2003 von der französischen Regierung begonnen. Seit dem Erstflug 2012 hat der »nEUROn« bereits zahlreiche Testflüge erfolgreich absolviert (Dassault Aviation 2016; Tran 2016).
- Das nEUROn-Programm sollte drittens, neben dem in Entwicklung befindlichen britischen Taranis-Demonstrator von BAE Systems, eine Grundlage des Programms »Future-Combat-Air-System« sein, das seit 2014 von Großbritannien und Frankreich angestrebt wurde und ein bewaffnungsfähiges UCAV mit Tarnkappeneigenschaften zum Ziel hatte (Altmann/Gubrud 2017, S. 109 ff.; Stevenson 2016). Nach der Erstellung einer Machbarkeitsstudie scheint die diesbezügliche französisch-britische Zusammenarbeit ab 2016 jedoch zum Erliegen gekommen zu sein (Pocock 2018). Stattdessen

49 Dem Konsortium gehören außerdem Griechenland (HAI), Italien (Alenia Aermacchi), Schweden (Saab), die Schweiz (Ruag) und Spanien (Airbus Defence and Space) an.

verfolgt Frankreich die FCAS-Entwicklung wie bereits beschrieben nun in enger Kooperation mit Deutschland.

Daneben entwickelt Frankreich gemeinsam mit Großbritannien USV- und UUV-Systeme, insbesondere zur Räumung von Seeminen (L3Harris ASV 2018). Außerdem plant die französische Regierung bis 2025 die Beschaffung eines leichten Panzerfahrzeugs, wobei auch eine unbemannte, fernsteuerbare Ausführung in Betracht gezogen wird (Tran 2018).

Großbritannien

Obwohl Großbritannien im Bereich der FuE bei Weitem nicht die Größenordnung der USA erreicht hat, ist ein großes Interesse an den Forschungsfeldern automatisierter Datenprozesse, Logistik und Navigation zu erkennen (Boulanin 2016b, S. 38 ff.; dazu und zum Folgenden Alwardt et al. 2017, S. 31 ff.). Die Kooperationen zwischen Regierung und Industrie zeigen, dass intensiv an automatisierten Militärsystemen gearbeitet wird. In Großbritannien gibt es dafür eine solide industrielle Grundlage, z. B. forscht BAE Systems im Bereich Luftfahrt und QinetiQ an autonomen maritimen Fahrzeugen (POST 2015). Neben einem UCAV-Testgelände in Wales (Brooke-Holland 2015, S. 28 ff.) eröffnete das britische Verteidigungsministerium 2013 das Maritime Autonomy Centre in Portsmouth, wo (unbewaffnete) autonome Schiffe, U-Boote und andere Wasserplattformen erforscht, entwickelt und getestet werden sollen (Rees 2013).

Bisher gibt es in Großbritannien jedoch weder eine dezidierte Militärstrategie in Bezug auf autonome Waffensysteme noch offizielle Angaben darüber, welcher Anteil der nationalen Verteidigungsausgaben (ca. 45 Mrd. Euro für 2018; SIPRI 2019) für die FuE automatisierter Systeme ausgegeben wird oder in welchem Umfang Großbritannien an autonomen Waffensystemen forscht (dazu und zum Folgenden Alwardt et al. 2017, S. 31 ff.). Das britische Ministry of Defence mahnt jedoch an, dass es »bis 2035 wahrscheinlich scheint, dass automatisierte Systeme fortschrittlich und hochgradig anpassungsfähig sein werden. [...] Technologische Fortschritte werden mit ziemlicher Sicherheit Schwarmangriffe ermöglichen, sodass zahlreiche Geräte gemeinsam agieren können«.[50]

Öffentlichen Quellen zufolge gibt es in Großbritannien nur ein KI-Forschungsprogramm im Verteidigungssektor zum Thema »Information Processing and Sensemaking« (Informationsprozessierung und Sinnstiftung), das sich u. a. mit Datenverarbeitung, automatischem Lernen und Modellgenerierung befasst (dazu und zum Folgenden Alwardt et al. 2017, S. 31 ff.; GOV.UK 2015). Die britische Regierung hat aber bereits einige bilaterale Innovationsprojekte auf

50 Im Original: »[b]y 2035, it seems likely that automated systems will be advanced and highly adaptable. [...] Advances in technology will almost certainly enable swarm attacks, allowing numerous devices to act in concert.« (MOD 2015, S. 16 ff.)

dem Gebiet der Autonomie initiiert, wie z. B. die angloamerikanische »Innovation Autonomy Challenge« (MOD 2017a) oder das britisch-französische »Future Combat Air System« (POST 2015). Zusammen mit britischen Rüstungsunternehmen führt die Royal Navy das Programm »Unmanned-Warrior« durch, welches an der Datenintegration von unbemannten Flugzeugen, Schiffen und U-Booten forscht. 2016 gelang eine entsprechende Demonstration mit 50 unbemannten Fahrzeugen in den Bereichen Überwachung, Informationssammlung und Minenabwehrmaßnahmen[51] (Royal Navy 2016).

Außerdem investiert Großbritannien in Wettbewerbe und Entwicklungsprogramme zu (teil)automatisierten Systemen, die das Defence Science and Technology Laboratory (DSTL) koordiniert (Alwardt et al. 2017, S. 32 ff.). Der Schwerpunkt liegt dabei auf Plattformleistungsfähigkeit und maschinellen Datenprozessen (Boulanin 2016b, S. 38 ff.).

Rüstungspolitisch liegt der Fokus Großbritanniens, wie der der meisten anderen Länder auch, auf der Drohnenentwicklung. Bis 2021 sollen zehn zusätzliche UCAVs in die britischen Streitkräfte integriert werden, wodurch die Flotte auf 20 Plattformen anwachsen würde (Ackerman 2016; Brooke-Holland 2015, S. 17 f.; dazu und zum Folgenden Alwardt et al. 2017, S. 32 ff.). Obwohl es sich hierbei um »General Atomics MQ-9 Reaper« handelt (früher »Predator B« genannt), gab die Royal Air Force bekannt, diese »Protector« nennen zu wollen. Anstatt mit US-amerikanischen Hellfire-Raketen werden sie mit britischen Brimstone-2-Raketen bewaffnet.

Parallel dazu arbeitet Großbritannien – inzwischen offenbar auf eigene Faust, nachdem die Kooperation mit Frankreich am Future Combat Air System beendet scheint – unter dem Projektnamen »Tempest« an der Entwicklung eines Kampfflugzeugs der nächsten Generation (Wiegold 2018). Durch BAE Systems hat Großbritannien bereits einen UCAV-Demonstrator mit dem Namen »Taranis« entwickeln lassen; seinen Jungfernflug absolvierte der Prototyp 2013 (Farmer 2015). 2010 wurde das Verteidigungsministerium mit den Worten zitiert, bei »Taranis« handele es sich um ein »vollständig autonomes« Flugzeug, das »sich gegen bemannte und andere unbemannte Flugzeuge verteidigen kann« (Cartwright 2010; vgl. auch Altmann/Gubrud 2017, S. 108 f.). Allerdings wird die Serienproduktion nicht angestrebt: Bei UCAV-Prototypen wie »Taranis« (oder auch »nEUROn«) geht es vielmehr darum, eine Grundlage für zukünftige Einsatzfähigkeiten über 2030 hinaus zu schaffen und neue Konzepte zu erforschen, z. B. MUM-T mit bemannten Flugzeugen wie der »Typhoon« oder »Lightning II« (Brooke-Holland 2015, S. 21 ff.).

51 Im Original: »surveillance, intelligence-gathering and mine countermeasures«.

4.2.3 Weitere Schlüsselakteure

Russland

Russlands Engagement ist im Bereich von unbemannten Systemen, insbesondere UCAVs, noch vergleichsweise neu und liegt bei FuE, Produktion und Beschaffung weit hinter führenden Herstellerländern wie den USA und Israel zurück (Bendett 2017; dazu und zum Folgenden Altmann/Gubrud 2017, S. 110 ff.; Alwardt et al. 2017, S. 33). In den letzten Jahren soll Russland jedoch die Bandbreite seines teilautomatisierten Militärequipments erweitert haben. 2017 präsentierte Russland den düsengetriebenen Nurflügel-Unterschall-Prototypen »Skat« (mit verringerter Radarsignatur) und 2013 wurde berichtet, MiG habe einen Vertrag bekommen, basierend auf dessen Auslegung ein neues UCAV zu entwickeln (Rosenberg 2013). Allerdings legen andere Berichte nahe, das Programm »Skat« sei beendet und an die Sukhoi Holding Company übertragen worden und werde dort unter der Bezeichnung »Okhotnik« weitergeführt. Laut Meldungen könnte die tarnkappenfähige Kampfdrohne »Okhotnik-B« (Deagel.com o. J.) bald flugfertig sein (Global Security o. J.c). Allerdings unterliegen die Quellen für diese Berichte der russischen Staatskontrolle, und sie geben wenig Spezifisches preis.

Ein Schwerpunkt der russischen Entwicklungsaktivitäten scheint – hier unterscheidet sich Russland von anderen wichtigen Ländern – auf unbemannten bewaffneten Bodensystemen zu liegen, die zum Teil bereits in Syrien eingesetzt wurden (Kap. 4.1.2). Dies befindet sich im Einklang mit einer aktuellen Modernisierungsstrategie für das russische Militär, bei der die Landstreitkräfte hohe Priorität genießen. Diese sieht vor, 70 % des russischen Militärequipments bis 2020 zu erneuern (Bodner 2015). Die wichtigste staatliche FuE-Institution für neue Militärtechnologien ist die Russia Foundation for Advanced Studies. Deren Hauptinitiative ist das Programm »Robotics-2025«, das 2014 beschlossen wurde. Ziel ist es, erheblich in die Entwicklung unbemannter Land-, See- und Luftfahrzeuge zu investieren – zukünftig soll offenbar ein Drittel aller militärischen Fahrzeuge unbemannt sein (Rötzer 2016). Jedoch ist es schwierig, die zukünftigen russischen FuE-Pläne oder konkrete Programme präziser abzuschätzen, da hierüber nur sehr wenige Informationen öffentlich zugänglich sind.

China

Unbemannte Systeme spielen eine wichtige Rolle für die Zukunft des chinesischen Militärs (dazu und zum Folgenden Altmann/Gubrud 2017, S. 109; Alwardt et al. 2017, S. 34 ff.). Bereits heute werden beträchtliche staatliche Fördermittel bereitgestellt und die Chinesen forschen intensiv zu UWS an zahlreichen nationalen Instituten (DOD 2017a). In den letzten Jahren hat die chinesische Regierung insbesondere massiv in UAVs investiert. Peking orientiert sich dabei

stark an den Aktivitäten der USA, was u. a. am äußeren Erscheinungsbild chinesischer UCAV-Modelle zu erkennen ist. Die chinesischen Institutionen Shenyang Aircraft Design Institute der Aviation Industry Corporation of China, Shenyang Aerospace University und Hongdu Aviation Industry Group entwickeln derzeit das »Lijian« (scharfes Schwert), ein düsengetriebenes UCAV mit verringerter Radarsignatur, äußerlich ähnlich zu »X-47B«, »nEUROn« und »Taranis«; der Erstflug erfolgte 2013 (Lin/Singer 2017).

Zukünftige chinesische Marschflugkörper sollen ein hohes Niveau an KI und Automatisierung aufweisen (Lei 2016). Für die Zukunft sind zudem große Investitionen in unbemannte maritime Systeme – sowohl Schiffe als auch U-Boote – zu erwarten (Chen 2013). Das US-Verteidigungsministerium geht davon aus, dass China plant, zwischen 2014 und 2023 bis zu 41.800 unbemannte Luft- und Seesysteme zu produzieren (die jedoch nicht alle bewaffnet sein werden) (DOD 2015a, S. 36 ff.). Im jährlichen Bericht an den Kongress zu den militärischen und sicherheitspolitischen Entwicklungen in China von 2017 stellte das US-Verteidigungsministerium fest, dass Chinas diesbezügliche Aktivitäten im Luft- und Seebereich den »signifikanten technischen Vorteil der USA« mindern werden (DOD 2017a, S. 28 ff.).

Israel

Sowohl die Erforschung als auch die Produktion von unbemannten Systemen hat einen hohen Stellenwert in Israel, weshalb es einer der weltweit führenden Staaten auf diesem Gebiet ist (dazu und zum Folgenden Alwardt et al. 2017, S. 34). Die Entwicklung vor allem von unbemannten Luftsystemen ist eine der höchsten Verteidigungsprioritäten, um den militärischen Vorsprung in der Region zu halten (Sadot 2016). Diese Systeme werden heute schon häufig als autonom angepriesen (siehe z. B. IAI o. J.). Zwar sind Israels genaue FuE-Bestrebungen überwiegend intransparent, aber die israelische Luftwaffe arbeitet derzeit an einer UAV-Roadmap. Von dieser ist bereits bekannt, dass MUM-T eine wichtige Rolle spielen wird (Egozi 2017). Nicht nur hinsichtlich der Roadmap, sondern auch bei den Technologien orientiert sich Israel an den Entwicklungen in den USA, z. B. in Hinblick auf eine neue Generation von USVs für die israelische Marine (Opall-Rome 2016).

5 Einsatzszenarien

Aus den beschriebenen Forschungs- und Entwicklungstrends bei AWS können mögliche technische Eigenschaften und andere damit verbundene Charakteristika zukünftiger AWS eingeschätzt und daraus erwartbare operative Fähigkeiten abgeleitet werden. Auf dieser Grundlage lassen sich denkbare militärische Missionen sowie Einsatzszenarien entwickeln, bei denen die erwarteten Vorzüge von AWS besonders gut zur Geltung kommen würden. Dies dient dazu, einen plastischeren Eindruck zu gewinnen, wie bzw. auf welchen Feldern AWS zu einer neuen Aufgabenverteilung zwischen Mensch und Maschine führen und so zu einer Veränderung der Kriegsführung insgesamt beitragen könnten (Kap. 6).

Da allerdings sowohl die technischen Eigenschaften als auch die Verfügbarkeit zukünftiger AWS noch eher spekulativ sind, können hier lediglich Umrisse eines möglichen Einsatzportfolios skizziert werden. Darüber hinaus sollte bei vorausschauenden Analysen wie dieser immer im Blick behalten werden, dass die damit vielfach einhergehende Übertragung heutiger Denkweisen auf die Technologien von morgen auch fehlleiten kann, da Struktur- und Traditionsbrüche nur schwer vorherzusehen sind.

5.1 Argumente für AWS

Die drei am häufigsten genannten Argumente, warum unbemannte und in Zukunft stärker autonome Systeme eine wesentliche Rolle bei militärischen Operationen spielen könnten, werden im Folgenden dargelegt und kritisch eingeordnet:

- AWS können gefährliche, langweilige und schmutzige[52] Aufgaben übernehmen bzw. für Menschen unmögliche Missionen durchführen.
- AWS können zu einer schnelleren und besseren Entscheidungsfindung in zeitkritischen Operationen beitragen.
- AWS können zu einer Reduzierung von Kosten führen, insbesondere durch Verringerung des Personaleinsatzes.

Entlastung des Menschen von gefährlichen, langweiligen und schmutzigen Aufgaben

Das am häufigsten genannte Argument für einen verstärkten Einsatz von autonomen Systemen in den Streitkräften ist, dass Menschen von gefährlichen, langweiligen sowie schmutzigen Aufgaben entlastet werden könnten (U.S. Army 2017b, S. 3 ff.). Sowohl anstrengende körperliche Aufgaben (Tragen von Lasten)

52 englisch: »dull, dirty and dangerous«

als auch langweilige oder solche mit kognitiver Dauerbelastung (Datenauswahl und -analyse, Errechnen und Vorschlagen von Handlungsoptionen etc.) könnten Soldaten durch autonome Systeme abgenommen werden. Mit den freigewordenen Kapazitäten könnten neue Aufgaben übernommen werden oder es könnte Personal eingespart werden. Ganz generell soll dadurch die Mobilität, Effektivität und das Durchhaltevermögen von Truppen erhöht werden (U.S. Army 2017b, S. 1).

Andererseits bringt gerade die Übernahme kognitiver Aufgaben durch autonome Systeme eine neue Qualität der Interaktion zwischen Mensch und Maschine ins Spiel, die neue potenzielle Fehlerquellen zur Folge haben kann. Wenn beispielsweise Soldaten nur noch mit Systemaufsicht und -management beschäftigt sind und darauf warten, dass das System eine Auffälligkeit berichtet, schwindet die kontinuierliche Wachsamkeit und vermehrte Fehler können die Folge sein.[53] Wenn ein System dagegen vollständig eigenständig und ohne menschliche Aufsicht operiert, könnten schwerwiegende Fehlfunktionen oder Systemfehler unentdeckt bleiben (Heyns 2013, S. 18). Außerdem ist unklar, wer die Verantwortung für mögliche (Fehl-)Entscheidungen von AWS tragen soll (Kap. 8.3).

Schnellere und bessere Entscheidungsfindung

Autonome Systeme können Unmengen von Daten aus verschiedensten Quellen sammeln und KI-gestützt auswerten, organisieren und priorisieren. Bei der Verarbeitung großer Datenmengen übertreffen sie menschliche Fähigkeiten bei Weitem. Vom militärischen Einsatz solcher Systeme verspricht man sich deshalb einen wesentlich umfassenderen Gesamtüberblick über die jeweilige Situation und somit eine bessere Grundlage für schnelle Entscheidungen und Operationen (U.S. Army 2017b, S. 16). Die Leistungsfähigkeit KI-basierter Systeme wird darüber hinaus auch nicht durch Stress oder Müdigkeit beeinträchtigt, und kognitive Verzerrungen – z. B. durch zu optimistische Annahmen (Sharot 2014) bzw. Selbstüberschätzung (Johnson 2004) –, für die Menschen anfällig sind, spielen keine Rolle. Besonders in zeitkritischen Operationen sollen autonome Systeme zu schnelleren und konsistenteren Entscheidungen als Menschen fähig sein (DSB 2016, S. 1 u. 6). Allerdings sind KI-basierte Systeme oft anfällig für Bias und andere unerwünschte Eigenschaften (Kap. 3.3.3).

Aber auch auf der Ebene der Strategieentwicklung werden KI-basierten Systemen Vorteile gegenüber Menschen zugeschrieben: Sie können Muster in Daten entdecken, die ansonsten unentdeckt bleiben würden, und neuartige Strategien entwickeln, die menschlichen Gewohnheiten und (Vor-)Urteilen zuwiderlaufen. Die aktuellen Erfolge von KI über die besten menschlichen Spieler in etlichen strategischen Spielen sprechen eine deutliche Sprache (Kap. 3.2).

53 Haider (2014, S. 58 f.) berichtet, dass bei mehr als der Hälfte der Unfälle aller Art bei Predator-Missionen der U.S. Air Force, bei denen Crewmitglieder involviert waren, Fehler dieser Art der Auslöser waren.

Es ist allerdings gegenwärtig fraglich, wie robust durch KI entwickelte Strategien in realen offenen, dynamischen und feindlich dominierten Umgebungen sind. Skepsis ist angebracht, da teilweise schon minimale Veränderungen der Szenarien, an denen die KI trainiert wurde, ausreichen, um sie völlig hilflos zu machen (Marcus 2018, S. 7 ff.). Hinzu kommen das Fehlen eines echten Verständnisses für Kontexte sowie die Blackboxeigenschaft der meisten KI-Systeme, die es schwer bis unmöglich macht nachzuvollziehen, aus welchen Gründen bestimmte Entscheidungen zustande gekommen sind.[54] Dies erschwert es, Vertrauen in die Sinnhaftigkeit dieser Entscheidungen aufzubauen (DSB 2016, S. 14 ff.). Dass die Aktionen autonomer Systeme im Einzelnen oft schwer vorherzusehen sind, stellt gleichzeitig eine Hürde dafür dar, sie in militärische Kommandostrukturen zu integrieren, die darauf ausgelegt sind, dass Befehle akkurat und zuverlässig ausgeführt werden.

Reduzierung von Kosten

Ein häufig angeführtes Argument für den verstärkten Einsatz unbemannter und zukünftig autonomer Systeme sind verringerte Kosten gegenüber bemannten Systemen. Einige sind sogar der Auffassung, dass diese Entwicklung unausweichlich ist, da die Kosten für Entwicklung, Beschaffung und Unterhalt bemannter Systeme sowie die zugehörigen Personalkosten so stark ansteigen, dass sie kaum noch bewältigt werden können (Work/Brimley 2014, S. 5 f.). Bei anhaltendem Trend würden beispielsweise in den USA die Personalkosten bis 2021 ca. 46 % des gesamten Verteidigungsbudgets aufzehren (Work/Brimley 2014, S. 21). Vor diesem Hintergrund sollen AWS ein Mittel darstellen, um mit weniger Personal und Equipment dieselben (oder sogar bessere) Ergebnisse zu erreichen.

Wie begründet diese Hoffnung ist, lässt sich aus heutiger Sicht nicht abschließend beurteilen. Existierende Vergleiche von bemannten mit unbemannten Flugzeugen ergeben kein eindeutiges Bild. So kommt das britische Verteidigungsministerium zu dem Schluss, dass die Betriebskosten von unbemannten Flugzeugen auf demselben Niveau oder sogar höher als die äquivalenter bemannter Flugzeuge liegen können, aufgrund der notwendigen Bodeninfrastruktur, Vernetzung sowie logistischer Unterstützung (MOD 2013, S. 10). Dies lässt sich an einem konkreten Zahlenbeispiel aufzeigen: Die gesamten Betriebskosten pro Flugstunde betragen bei einem unbemannten »RQ-4B Global Hawk« etwa 49.000 US-Dollar, wohingegen eine »U-2 Dragon Lady« (bemanntes Spionageflugzeug) mit ca. 31.000 US-Dollar zu Buche schlägt (Thompson 2013).

Allerdings ist einer der größten Kostenfaktoren beim Betrieb bemannter Flugzeuge der Bedarf an Trainingsflügen zur Ausbildung von Piloten und zur

54 Laut dem ehemaligen Schachweltmeisters Garri Kasparov (2018): »Explainability is still an issue«.

Aufrechterhaltung ihrer Fähigkeiten.[55] Bediener von unbemannten Flugzeugen können dagegen weitgehend in Simulatoren ausgebildet werden. Daher würde eine Substitution bemannter durch unbemannte Flugzeuge die Kosten für Trainingsflüge erheblich reduzieren (Boulanin/Verbruggen 2017, S. 63). Ein weiterer Ansatz zur Reduktion der Personalkosten ist, Systeme so zu designen, dass ein menschlicher Bediener gleichzeitig mehrere Plattformen bedienen kann (DOD 2013, S. 68), was für zunehmend autonomere Systeme eine naheliegende Option ist.

Insgesamt ist es somit schwer zu sagen, ob beim Vergleich der Gesamtkosten bemannte oder unbemannte Systeme günstiger abschneiden. Hinzu kommt, dass ein direkter Vergleich oft gar nicht möglich ist, da unbemannte Systeme ein anderes Fähigkeits- und Einsatzspektrum abdecken als bemannte Systeme.[56]

5.2 Erwartete militärische Fähigkeiten

Die militärischen Fähigkeiten, die für AWS erwartet werden, umfassen auf der einen Seite die Vorteile aktueller bzw. in Entwicklung befindlicher UWS gegenüber bemannten Systemen. Diese beruhen in erster Linie darauf, dass kein menschlicher Bediener an Bord des Systems ist und daher die daraus resultierenden Beschränkungen hinsichtlich Größe, Gewicht und Ausstattung des Systems entfallen. Auf der anderen Seite unterscheiden sich die technischen Systemfähigkeiten von AWS von UWS dadurch, dass Datenprozesse und Kommunikationserfordernisse in autonomen Systemen völlig anders gestaltet sind als in unbemannten, aber mindestens partiell ferngesteuerten Systemen.

Im Folgenden werden zu erwartende Charakteristika zukünftiger autonomer Systeme dargestellt und hinsichtlich ihrer möglichen Vorteile, aber auch der gegen sie bestehenden Vorbehalte beleuchtet. Die Darstellung konzentriert sich stark auf fliegende Systeme, da die Unterschiede zu bemannten Systemen hier am prominentesten hervortreten. Außerdem befinden sich fliegende AWS weitaus näher am Stadium der Einsatzreife als boden- bzw. seegestützte Systeme. Bei den folgenden Ausführungen handelt es sich um eine überarbeitete Fassung des Gutachtens von Alwardt et al. (2017, Kap. 3).

55 Gemäß Boulanin/Verbruggen (2017, S. 63) muss ein Kampfpilot 10 bis 20 Flugstunden im Monat unter realen Bedingungen absolvieren.

56 Beispielsweise findet man im englischen Wikipediaartikel über das für Anti-U-Boot-Einsätze in der Entwicklung befindliche autonome Schiff »Sea Hunter« die Angabe, es sei mit Betriebskosten von 15.000 bis 20.000 US-Dollar pro Tag erheblich günstiger als der Betrieb eines Destroyer (deutsche Bezeichnung: Fregatte) mit 700.000 US-Dollar. Allerdings ist die »Sea Hunter« lediglich 40 m lang und hat eine Verdrängung von 135 t, ein Destroyer der Arleigh-Burke-Klasse ist hingegen etwa 150 m lang und verdrängt ca. 9.000 t (Wikipedia 2003b u. 2016b).

Gewicht

UWS – ob autonom agierend oder ferngesteuert – sparen das Gewicht des menschlichen Operators und der Innenausstattung ein (Sitz, gepanzerte Kabine, Sauerstoffversorgung etc.). Daher haben sie häufig ein geringeres Gewicht als bemannte Systeme, was u. a. zu einem geringeren Treibstoffverbrauch führen kann (Scharre 2014a, S. 12 ff.). Dadurch könnten Plattformen länger ununterbrochen eingesetzt werden. Allerdings schlägt dies umso weniger zu Buche, je größer die Plattform ist (Scharre 2014a, S. 10). Zudem müssen Gewichtseinsparungen nicht zwingend zu leichteren Systemen führen; sie können sich auch in einer höheren Nutzlast niederschlagen (Sensoren, Wirkmittel, höherer Treibstoffvorrat für größere Reichweite etc.).

Der Verzicht auf einen menschlichen Bediener an Bord erlaubt auch sehr kleine und leichte Plattformen. Hier stellt sich allerdings die Frage, ob diese bei schwierigen Operationsbedingungen (beispielsweise starker Wind, Regen etc.) robust genug sind.

Einsatzdauer

Bei unbemannten Systemen muss nicht auf menschliche Einschränkungen, z. B. hinsichtlich Beschleunigung (G-Kraft), Bedürfnisse und insbesondere Ruhephasen Rücksicht genommen werden (Heyns 2013, S. 10). Letzteres ermöglicht eine längere Einsatzdauer, was gleichzeitig auch eine größere Reichweite bedeutet, da längere Distanzen zurückgelegt werden können. Damit werden sowohl zeitlich als auch geografisch ausgedehntere Überwachungs- und Aufklärungsmissionen möglich, auch an Orten, an die bemannte Plattformen nicht gelangen können (U.S. Army 2017b, S. 1 f.). Um etwa eine Rund-um-die-Uhr-Aufklärungsmission mit durchgehend mindestens einem Flugzeug vor Ort in Libyen von einer Basis in Sizilien aus durchzuführen, würden fünf bemannte, aber nur zwei unbemannte Flugzeuge benötigt.[57] Eine Mission in Mali wäre von Sizilien aus mit vier unbemannten Flugzeugen durchführbar und mit bemannten Flugzeugen überhaupt nicht darstellbar (Scharre 2014a, S. 14 f.) (Abb. 5.1).

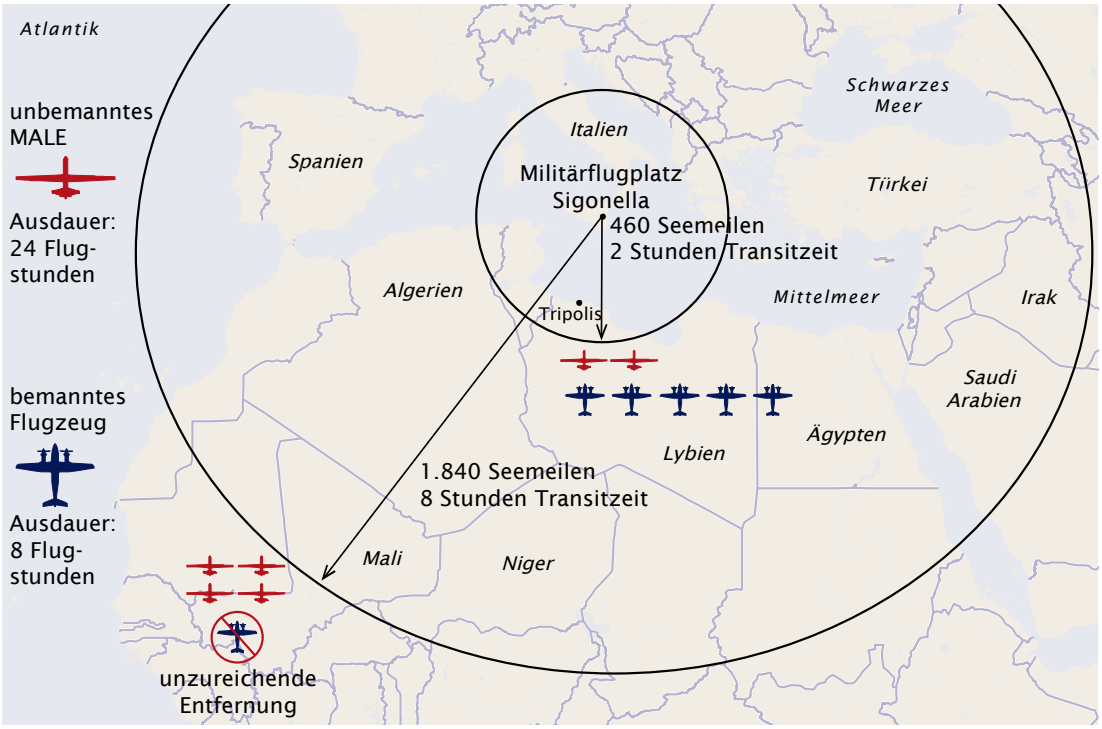
Einsatzfähigkeit

AWS werden voraussichtlich aufgrund ihrer längeren Ausdauer mobiler sein und könnten somit vom Ort ihrer Stationierung aus flexibler eingesetzt werden als bemannte Plattformen. Dies kann potenziell erhebliche Auswirkungen darauf haben, wie sich Streitkräfte in Bezug auf mögliche Einsatzgebiete rund um

57 Angenommen wurden: unbemanntes Flugzeug: Ausdauer 24 Stunden, bemanntes Flugzeug: Ausdauer 8 Stunden; Transitzeit Sizilien – Libyen: 2 Stunden, Sizilien – Mali: 8 Stunden; d. h., der Transit nach Mali würde die gesamte maximal mögliche Flugzeit des bemannten Aufklärungsflugzeugs aufzehren.

den Globus aufstellen (Work/Brimley 2014, S. 31 f.). Somit befördern autonome Systeme gemeinsam mit anderen neuen Technologien die in der aktuellen Verteidigungsstrategie der USA geplante Modernisierung der noch aus der an den Kalten Krieg anschließenden Ära stammenden Leitbilder für die globale Handlungsfähigkeit der US-Kräfte (DOD 2018b, S. 7).[58]

Abb. 5.1 Anzahl benötigter Luftfahrzeuge für 24/7-Abdeckung



Quelle: nach Scharre 2014a, S. 14 f.

Die US-Armee geht von einer rascheren Einsatzfähigkeit bzw. Abrufbarkeit von AWS aus. Langfristig soll dies eine verbesserte Integration und Synchronisierung von Teilstreitkräften und eine Flexibilisierung und Dezentralisierung von Operationen ermöglichen bis hin zu einem schnelleren Übergang zu offensiven Operationen nach Eintritt in den Gefechtsraum (U.S. Army 2017b, S. 10 ff.). Dies mag zutreffen, allerdings stellen sich auch neue Fragen bezüglich der zunehmenden Abhängigkeit von Technologie bei der Entscheidungs- und Zielfindung sowie der Operationsführung (Unfallhäufigkeit, Störanfälligkeit mit und ohne feindliche Einwirkung etc.).

58 Im Original: »A modernized Global Operating Model of combat-credible, flexible theater postures will enhance our ability to compete and provide freedom of maneuver during conflict, providing national decision-makers with better military options.«

Abstandsfähigkeit

Würden AWS künftig gefährliche Missionen übernehmen, könnten die eigenen Truppen einen größeren Sicherheitsabstand zu gegnerischen Verbänden oder gefährlichen Arealen einhalten. Dadurch verringert sich das Risiko für die eigenen Soldaten. Dies ist sowohl in Aufklärungs- und Angriffsoperationen als auch bei Versorgungsmissionen relevant, da Konvois häufig attackiert oder mit improvisierten Sprengkörpern konfrontiert werden. Demzufolge könnten autonom operierende Konvois hier große Vorteile bieten (U.S. Army 2017b, S. 2). Darüber hinaus wird oft betont, dass Roboter Arbeiten in kontaminierten Gebieten übernehmen können, z. B. nach chemischen, biologischen, radiologischen oder nuklearen Attacken (DSB 2016, S. 45).

Verlässlichkeit

Befürworter einer stärkeren Nutzung von autonomen Funktionen argumentieren, dass das Verhalten autonomer Systeme oft verlässlicher, konsistenter und vorhersehbarer als das von Menschen ist, da es auf programmierten Regeln beruht (DSB 2016, S. 1). Gleichzeitig sollen autonome Systeme die Beschränkungen von automatisierten Systemen überwinden und auch in unvorhergesehenen Situationen zielgerichtet agieren können. Dies wird wiederum damit erkauft, dass das System sich unvorhersagbar verhalten kann bzw. nicht mehr nachvollziehbar ist, warum ein System eine bestimmte Aktion durchgeführt hat (U.S. Air Force/Office of the Chief Scientist 2015, S. 5 f.). Verlässlichkeit und Überprüfbarkeit der Aktionen eines AWS wären damit infrage gestellt (UNIDIR 2018b, S. 8).

Datenprozesse

Autonome Systeme können ein großes Datenvolumen und diverse Datentypen (Bilder in allen verfügbaren Spektralbereichen, akustische, Radar- und andere elektromagnetische Signale, nachrichtendienstliche Datenanalysen etc.) selbstständig erfassen, bearbeiten, auswerten und nutzen (DSB 2016, S. 45). Der Prozess, aus Rohdaten verwertbare Informationen zu generieren, könnte somit erheblich beschleunigt werden. Aufgrund der effizienteren Datenprozesse und rascheren Kommunikation können AWS Aufgaben erledigen, die die menschliche Reaktionszeit überfordern würden. Dies könnte die Geschwindigkeit von Operationen maßgeblich erhöhen (DOD 2017b, S. 20).

Einschränkend muss jedoch festgehalten werden, dass neben einer schnellen Reaktionszeit auch die Qualität der Reaktion relevant ist. Im Gegensatz zum Menschen sind autonome Systeme weder zur Interpretation eines Kontextes noch zu reflektiertem oder moralischem Handeln bzw. zur situationsgerechten Auslegung rechtlicher Prinzipien in der Lage. Nur weil ein Ziel identifiziert und

lokalisiert wurde und die Wahrscheinlichkeit hoch ist, dass es effizient und schnell bekämpft werden kann, heißt das noch nicht, dass seine Bekämpfung im strategischen, sozialen, ethischen und rechtlichen Kontext sinnvoll oder erlaubt ist (Heyns 2013, S. 10 f.) (siehe dazu Kap. 7 u. 8).

Kommunikationsverbindung

Kommunikationsverbindungen sind ein zentrales Schlüsselelement des gegenwärtigen Paradigmas der netzwerkzentrierten Kriegsführung (in den USA »Network Centric Warfare« – NCW; Wilson 2005; in Deutschland »Vernetzte Operationsführung« – NetOpFü; BMVg 2004, S. 15). Bei unbemannten Systemen sind Daten- und Kommunikationsverbindungen zum Austausch von Sensordaten, Missionsparametern und Steuerbefehlen zwischen dem mobilen System und einer Basisstation unverzichtbar. Dies bringt mehrere Probleme mit sich, für die ein höheres Ausmaß an Autonomie oft als Beitrag zu deren Lösung dargestellt wird:

Die Schnelligkeit von heutigen Operationen mit unbemannten ferngesteuerten Systemen leidet häufig unter Verzögerungen durch die (in der Regel satellitengestützte) Datenübertragung über globale Distanzen. Dies würde entfallen, da AWS nicht auf externe Steuerbefehle angewiesen wären (zumindest nicht kontinuierlich), d. h., AWS könnten wesentlich schneller operieren (Heyns 2013, S. 10).

Die verfügbare Bandbreite der Kommunikationsverbindung begrenzt oft die Möglichkeiten der Datennutzung (z. B. keine Übertragung von hochauflösenden Echtzeitvideos möglich). Durch eigene Datenverarbeitungskapazitäten eines AWS könnten aus großen Mengen an Sensorrohdaten direkt an Bord entscheidungsrelevante Informationen gewonnen werden, sodass eine breitbandige Übertragung ggf. entbehrlich wäre.

Daten- und Kommunikationsverbindungen hinterlassen elektronische und digitale Spuren, die vom Gegner aufgespürt werden können, was dazu führen kann, dass Plattformen entdeckt und bekämpft werden. Auch die Kommunikationsverbindungen selbst können zum Angriffsobjekt werden. Beispielsweise können GPS-Signale von Satelliten durch Widersacher blockiert (»jamming«) oder gefälscht (»spoofing«) werden, damit der Pilot die Kontrolle über das ferngesteuerte Gerät verliert.[59] Denkbar ist ebenfalls, dass Systeme über die Kommunikationsverbindungen gehackt und ihre Software oder das Aufgabenprofil verändert werden. AWS könnten dagegen über einen längeren Zeitraum eigenständig operieren, womit die Kommunikation mit einer Basisstation minimiert wird. Dies würde sowohl das Entdeckungsrisiko als auch die Angriffsfläche für elektronische Attacken (»jamming«, »spoofing«, »hacking«) reduzieren.

59 Dickow (2015, S. 11) schildert ein Fallbeispiel, wie 2011 eine US-Drohne vom Typ »RQ-170 Sentinel« offenbar vom iranischen Militär durch elektronische Manipulation entführt wurde.

Direkte Kommunikation zwischen AWS (»peer to peer«) ist deutlich schwerer zu entdecken und zu manipulieren als satellitengestützter Funk und könnte die selbstständige Koordination mehrerer AWS (als Schwarm) untereinander zulassen (DSB 2016, S. 84). Dem geringeren Risiko elektronischer Attacken stehen allerdings potenziell gravierende Konsequenzen gegenüber, besonders wenn aufgrund fehlender Kommunikationsmöglichkeiten kein menschlicher Bediener in der Lage wäre einzugreifen, wenn AWS-Operationen torpediert oder manipuliert würden. Völlig ohne Kommunikationsverbindung werden die meisten AWS voraussichtlich nicht auskommen. Ein gewisser Datenaustausch wird zur Betreuung der Operation und zur Verteilung von Daten an andere an der Operation beteiligte Kräfte sowie nicht zuletzt zur Aufrechterhaltung eines gewissen Maßes an menschlicher Kontrolle benötigt. Um die Systeme und Operationen zu sichern, wären insofern hochentwickelte Verschlüsselungs- und Schutztechnologien notwendig (U.S. Air Force 2016, S. 26 ff.).

Schwarmfähigkeit

Im Kontrast zu den bisher behandelten konventionellen Eigenschaften eröffnet die Fähigkeit von AWS, aus einer Vielzahl von Einzelsystemen Schwärme zu bilden, völlig neuartige Einsatzmöglichkeiten für AWS. Schwärme können in ihrer Gesamtheit Wirkungen erzielen, die quantitativ und qualitativ weit über die eines einzelnen Systems hinausreichen. Dass eine Gruppe von Individuen sich mit Blick auf ein gemeinsames Ziel selbst koordiniert und ihre Aktionen untereinander abstimmt, ist ein in der Tierwelt verbreitetes Phänomen. Selbst mit minimaler Kommunikation untereinander und auf einfachen Regeln beruhenden Aktionen von Individuen kann ein Schwarm als Ganzes intelligent erscheinendes Verhalten ausbilden. Dieses auf KI-gestützte technische Systeme zu übertragen, ist Gegenstand intensiver Forschungsbemühungen. Bei hinreichend großer Autonomie auf Missionsebene wären keine oder nur eine kleine Anzahl menschlicher Bediener für eine große Menge an Plattformen erforderlich.

Dieser Ansatz weist wesentliche Vorteile auf. Entsprechende technologische Fortschritte vorausgesetzt, könnte dies eine Abkehr vom Paradigma einleiten, immer teurere und spezialisiertere Systeme zu entwickeln. Stattdessen könnte eine große Menge kleiner und kostengünstiger Geräte im Kollektiv ähnliche Funktionen erfüllen oder völlig neue Möglichkeiten eröffnen (Scharre 2014b, S. 13 ff.):

- Die Kampfkraft wird stärker verteilt, sodass der Gegner mit einer größeren Anzahl an Zielen konfrontiert wird.
- Durch die große Anzahl können Verteidigungssysteme überlastet werden.
- Die Überlebensfähigkeit einzelner Plattformen wird weniger wichtig. An ihre Stelle tritt die Schwarmresilienz.

- Bei Verlusten sinkt die Kampfkraft nur sukzessive, statt zusammenzubrechen, wenn eine große Einheit verlorengeht.

Durch Schwärme könnten sowohl die offensive Schlagkraft erhöht als auch die Defensive gestärkt werden. Sie könnten beispielsweise als Ablenkungsmanöver, zum »jamming« der gegnerischen Kommunikation, zum Aufbau von robusten Sensor- und Kommunikationsnetzen bzw. als Träger variabler, der Situation angepasster letaler oder sonstiger Nutzlasten eingesetzt werden (DSB 2016, S. 61 ff.). So könnte beispielsweise eine große Anzahl billiger Wegwerfsysteme einen gegnerischen Flugplatz lahmlegen, indem sie den Luftraum wie Heuschrecken quasi verminen, wenn sie vom Geräusch herannahender Flugzeuge angelockt werden. Wegwerfsysteme müssen nicht per se klein und billig sein. Ein Beispiel sind die Antischiffsmarschflugkörper »LRASM«, bei denen es sich um technisch hochentwickelte und kostspielige Plattformen handelt, die über die Fähigkeit verfügen, sich untereinander zu koordinieren (Kap. 4.1.1).

Als Gegenmaßnahme zu Schwärmen kommt der Einsatz von Gegenschwärmen in Betracht. Taktiken für solche Schwarm-gegen-Schwarm-Kämpfe sind derzeit noch Neuland. Es ist nicht unplausibel, dass die Kampfkraft von Schwärmen stärker von den Taktiken und Algorithmen für bessere Koordination bestimmt wird als von der Qualität der einzelnen Plattformen (Scharre 2014b, S. 42). Allerdings bestünde ein erhebliches Risiko zur ungewollten Eskalation, wenn in Krisensituationen gegnerische Schwärme in großer Nähe zueinander stationiert wären und auch bei fehlinterpretierten Signalen automatische Gegenreaktionen getriggert würden, ohne dass Menschen die Möglichkeit hätten, korrigierend einzugreifen (Altmann/Sauer 2017, S. 128).

5.3 Missionen/Einsatzszenarien

Vor dem Hintergrund der dargestellten potenziellen militärischen Fähigkeiten von AWS werden nun denkbare Einsatzszenarien diskutiert, in denen diese Systemfähigkeiten besonders zum Tragen kommen könnten. In der Übersicht in Tabelle 5.1 werden Typen von Missionen aufgelistet, für die laut Strategiepapieren der US-Streitkräfte potenzielle operative Vorteile von AWS in den Kategorien Geschwindigkeit, Agilität, Ausdauer, Reichweite sowie Koordination Anwendung finden.

Im Folgenden werden basierend auf dem Gutachten von Alwardt et al. (2017, S. 46 ff.) einige der erwarteten Missionstypen aus Tabelle 5.1 aufgegriffen, in denen AWS alleine, als Schwarm mit anderen AWS oder zusammen mit Menschen agieren könnten (Kap. 5.3.1). Im Anschluss werden auf dieser Grundlage fünf denkbare Einsatzszenarien für zukünftige AWS entwickelt (Kap. 5.3.2).

Tab. 5.1 Missionen, in denen operative Vorteile von AWS besonders zum Tragen kommen

Hauptvorteile der Autonomie	Art der Mission
Geschwindigkeit: Lichtgeschwindigkeit bei der Umsetzung der Schleife »beobachten, orientieren, entscheiden, handeln«	Luftverteidigung, Cyberverteidigung; elektronische Kriegsführung
Agilität: weniger Abhängigkeit von Kommando und Kontrolle	ISR-Mission, Cyberkriegsführung, elektronische Kriegsführung, U-Boot- und Minenjagd, logistische Operationen
Beharrlichkeit: konstante Leistung unbemannter Systeme für »langweilige, schmutzige und gefährliche« Einsätze	Luftverteidigung, lange ISR-Missionen, Antimineneinsatz, Evakuierung von Verletzten, logistische Operationen auf feindlichem Gebiet
Reichweite: Zugang zu GPS und Umgebungen ohne Kommunikation	ISR-Missionen in A2/AD-Umgebungen, U-Boot- und Minenjagd, Evakuierung von Verletzten, Logistikoperationen in A2/AD-Umgebungen, Schläge in A2/AD-Umgebungen
Koordinierung: Fähigkeit, große Gruppen von Waffensystemen auf strukturierte und strategische Weise zu koordinieren	Schutz der Streitkräfte, Kampfeinsätze in A2/AD-Umgebungen, ISR-Missionen in komplexen und unübersichtlichen Umgebungen

A2/AD (»anti access and area denial«) = Zugangsverweigerung und Absperrung von Gebieten; GPS = globales Positionsystem; ISR = Nachrichtengewinnung, Überwachung und Aufklärung

Quellen: Boulanin/Verbruggen 2017, S. 62; DOD 2016; Übersetzung durch das TAB

5.3.1 Erwartete Missionen

Militärische Planer und Analysten gehen davon aus, dass AWS aufgrund ihrer angenommenen Vielseitigkeit bei zahlreichen militärischen Einsatzszenarien eine wichtige Rolle spielen werden – mit oder ohne letale Waffeneinsätze. Sie könnten alleine, als Schwarm oder gemeinsam mit Soldaten im Sinne eines Mensch-Maschine-Teams (MUM-T) eingesetzt werden (DOD 2013, S. 139).

Ein wichtiger Einsatzfaktor ist die Beschaffenheit des Terrains. Gebiete, die relativ homogen sind und wenige natürliche Hindernisse aufweisen, sind dafür prädestiniert, dass weitgehend autonome Systeme dort als Erstes verwendet werden. Dies ist der Grund, warum fliegenden Systemen in der Diskussion um AWS eine herausgehobene Rolle zukommt, da der Luftraum über genau diese

Eigenschaften verfügt. Darüber hinaus sind aber auch der Weltraum, Meere (über, aber vor allem auch unter der Wasseroberfläche) sowie strukturarme Landschaften wie Wüsten für einen AWS-Einsatz besonders geeignet. Einsatzräume wie Städte oder auch solche innerhalb von Gebäuden sind hingegen wesentlich komplexer strukturiert, sodass es für Roboter dort erheblich schwieriger ist, sich zielgerichtet und effizient fortzubewegen und Missionen durchzuführen. Dennoch sind auch urbane Einsatzszenarien Gegenstand von Forschung und strategischen Überlegungen (U.S. Army 2017b, S. 6). Dass die verschiedenen Terrains nicht voneinander getrennt zu betrachten sind, zeigt das Multi-Domain-Battle-Konzept, das von den US-Streitkräften entworfen wurde, um militärische Schlagkraft in alle Domänen projizieren zu können (U.S. Army 2017a u. 2017b, S. i. ff.).

Im Folgenden werden potenzielle militärische Einsatzformen zukünftiger AWS – ohne Anspruch auf Vollständigkeit – anhand von Einsatzbeispielen erläutert.

Kampfmissionen

Im Luft-zu-Luft-Kampf werden Loyal-Wingman-Konzepte diskutiert. Dabei handelt es sich um autonome unbemannte Systeme, die im Verbund mit einem bemannten Flugzeug operieren und dessen Kampfkraft bzw. Überlebensfähigkeit steigern. AWS könnten als loyaler Flügelmann beispielsweise als Container für zusätzliche Bewaffnung bzw. Munition oder als Sensorträger für Aufklärungsmissionen dienen. Außerdem könnten sie feindliches Feuer auf sich ziehen, um das bemannte Flugzeug zu schützen (Scharre 2014b, S. 15; U.S. Air Force 2016, S. 45).

Im Luft-zu-Boden-Kampf könnten AWS die feindliche Luftabwehr angreifen (DOD 2013, S. 24). Außerdem wären Einsätze möglich, in denen autonome Luft- oder Bodensysteme unbemerkt und ausdauernd, alleine oder in Teams tief im feindlichen Gebiet hochwertige Ziele, z. B. wichtige Personen oder Gebäude, angreifen (DOD 2013, S. 24). Autonome Bodensysteme könnten Infanterietruppen dabei unterstützen, die feindliche Verteidigung zu durchbrechen, oder sie könnten bei potenziellen Nahkämpfen vorausgeschickt werden (U.S. Army 2017b, S. 10).

Elektronische Angriffe

AWS könnten elektronische Angriffe unterstützen, die ein Ziel immobil oder kampfunfähig machen, anstatt es mit physischer Gewalt auszuschalten (siehe z. B. Northrop Grumman o. J.). Mögliche elektronische Angriffsformen sind das Blockieren von Signalen (»jamming«) oder die Überforderung der feindlichen Kommunikationsnetze durch elektronische Angriffe in großer Zahl (U.S. Air Force 2016, S. 8). Die UAVs »Reaper« haben bereits ihre Fähigkeit zum

elektronischen Angriff unter Beweis gestellt (Scharre 2014a, S. 28). Auch für autonome UUVs wird erwartet, dass elektronische Angriffsmanöver in naher Zukunft zu deren Fähigkeitsspektrum gehören wird (Chief of Naval Operations 2016, S. 5, 9).

Verdeckte Operationen

Für verdeckte oder geheime Operationen würden sich (kleine) autonome Roboter besonders eignen, da sie weniger Spuren hinterlassen und unauffälliger als große bemannte Plattformen sind. Dadurch könnten sie leichter unentdeckt in feindliches Territorium eindringen. Wenn sie zudem aus kommerziell erhältlichen Komponenten bestehen und keine identifizierbaren Markierungen aufweisen, könnte eine Regierung ihre Verantwortlichkeit abstreiten, wenn die Plattform in die Hände des Gegners fällt (»plausible deniability«) (Scharre 2014a, S. 11). Im Umkehrschluss ist dies für die angegriffene betroffene Seite problematisch, denn wenn ein Angriff keinem Verantwortlichen nachweisbar zugeordnet werden kann, sind Gegenmaßnahmen schwer zu begründen und durchzuführen.

Nachrichtengewinnung, Überwachung, Aufklärung

Nachrichtengewinnung, Überwachung und Aufklärung (»intelligence«, »surveillance«, »reconnaissance« – ISR) ist bereits heute ein routinemäßiges Einsatzfeld für unbemannte Plattformen. Indem sie über lange Zeiträume und weite Strecken die Umgebung erkunden, tragen sie zu einem besseren Situationsbewusstsein von Truppen bei (U.S. Army 2017b, S. 5 ff.). Es ist wahrscheinlich, dass Aufklärungsdrohnen mit AWS synchron operieren können werden. Als Späher würden sich auch hier kleine Systeme besonders eignen, u. a. weil sie gut portabel sind und Soldaten sie zu Einsätzen mitnehmen können (Scharre 2014a, S. 11). Schwärme unbemannter Plattformen würden qualitativ hochwertige Aufklärungsresultate liefern, da sie Ziele von verschiedenen Blickwinkeln beobachten können (U.S. Air Force 2016, S. 43 f.). Außerdem könnten sehr hoch fliegende und ausdauernde unbemannte Plattformen ähnlich wie Satelliten Kommunikations- und Navigationsfunktionen übernehmen (»pseudolites«) (Scharre 2014a, S. 19).

Täuschungsmanöver

Täuschungsmanöver sind ein weiterer Missionstyp, für die AWS prädestiniert sein könnten. Diese sind oft auf einen kalkulierten Verlust oder die Beschädigung der beteiligten Plattformen ausgelegt. Darum sind kleine und günstige Plattformen, wie sie z. B. im LOCUST-Programm (Atherton 2018) entwickelt werden, hierfür attraktiver als große, teure Systeme. Als eine Art Lockvogel

könnten Kleinplattformen einen Feind ablenken und seine Truppen in eine falsche Richtung führen oder ihn zum Feuern provozieren und so seine Ressourcen (z. B. Munition) erschöpfen (Scharre 2014b, S. 14).

Sicherung militärischer Stützpunkte

Zur Sicherung von militärischen Stützpunkten sind autonome Systeme unterschiedlicher Art denkbar. Hochautomatisierte (von autonomen oft nur schwer abgrenzbare; Kap. 2.2) Nahbereichsverteidigungssysteme sichern bereits heute kritische Standorte, indem sie ohne menschliche Intervention reaktiv auf sich nähernde Ziele schießen können (beispielsweise »C-RAM«; UNIDIR 2014a, S. 5). Durch verbesserte Sensoren und zunehmende Autonomie könnte die Effizienz dieser Systeme erheblich gesteigert werden. Staaten wie Israel setzen bereits jetzt ferngesteuerte Bodenfahrzeuge zur Sicherung von Gebietsabschnitten ein (Kap. 4.1.2). Autonome maritime Waffensysteme können außerdem zur Sicherung von Häfen und kritischen Wasserwegen eingesetzt werden (DOD 2013, S. 88).

Weitere Einsatzbeispiele

Zusätzliche Operationsformen für unbemannte Boden- oder Luftsysteme, die auch für autonome Plattformen denkbar wären, sind die nichtletale Kontrolle und Lenkung von Menschenmengen (DOD 2013, S. 24) und diverse logistische Aufgaben (Bornstein 2015, S. Folie 6). Da unbemannte Luft- und Bodensysteme bereits heute erfolgreich im Umgang mit improvisierten Sprengkörpern (IEDs) verwendet werden, sollen zukünftig autonome maritime Systeme, sowohl Schiffe als auch U-Boote, nach Unterwasserminen suchen, sie neutralisieren und ggf. auch selbst legen (Chief of Naval Operations 2016, S. 4).[60] Ferner könnten unbemannte U-Boote der strategischen nuklearen Abschreckung dienen (Ballesteros 2018; Bitzinger/Leah 2016).

5.3.2 Denkbare militärische Einsatzszenarien für AWS

Auf Basis der bisherigen Betrachtungen zu möglichen Einsatzumgebungen und Operationsformen zukünftiger AWS und unter Berücksichtigung der – zum jetzigen Zeitpunkt noch spärlichen – öffentlich verfügbaren Informationen zu zukünftigen Einsatzszenarien (z. B. Chief of Naval Operations 2016, S. 4 f.; DOD 2013, S. 12 ff.; iPRAW 2017a, S. 14 f.; U.S. Air Force 2016, S. 9 f.) werden im Folgenden einige exemplarische Szenarien entwickelt und andiskutiert, in denen der Einsatz von AWS zukünftig denkbar wäre.

60 Das unbemannte Antiminenmodul (»mine countermeasures module« – MCM) soll ab 2021 einsatzbereit sein (The Maritime Executive 2019).

Maritime Einsätze

Maritime AWS wie UUVs und USVs könnten sich über lange Zeiträume hinweg in oder auf dem offenen Meer bewegen. Da sie keine Mannschaft an Bord haben, wäre ihre Ausdauer erheblich größer als die bemannter Systeme und da sie keine kontinuierliche Steuerungs- oder Kommunikationsverbindung brauchen, könnten sie eigenständig in abgelegenen Gegenden operieren. Insbesondere UUVs könnten vermehrt verwendet werden, denn sie sind tief unter der Wasseroberfläche nur sehr schwer zu detektieren und nicht den oft unwirtlichen Wetter- und Umweltbedingungen über der Wasseroberfläche ausgesetzt. Somit sind sie im Einsatz robuster als USVs. In Anbetracht weiter Strecken, die global operierende UUVs im Meer zurücklegen müssten, könnten auch extra große unbemannte Unterwasserfahrzeuge (»extra-large unmanned underwater vehicles« – XLUUVs) (siehe z. B. Baker 2019) eingesetzt werden, die eine äußerst lange Ausdauer haben – potenziell sogar mehrere Monate. Durch die Ozeane streifende UUVs könnten bei Bedarf zur Unterstützung von Fregatten und Trägerverbänden hinzugerufen werden. Sie könnten ebenfalls andere maritime Plattformen beschatten, die ihnen aufgrund ihrer Operationsparameter verdächtig erscheinen, und deren Aktivitäten ausspionieren. Weiterhin ist denkbar, dass sie z. B. für Hunter-Killer-Missionen eingesetzt werden und selbstständig feindliche U-Boote oder Kriegsschiffe aufspüren, identifizieren und durch abgefeuerte Torpedos zerstören. Da die Kommunikation zwischen bzw. mit Objekten unter Wasser sehr schwierig ist, wäre die kontinuierliche Aufsicht und Kontrolle ebenso wie die Koordination von Schwärmen von AWS erheblich erschwert. Es ist absehbar, dass Gegner ihrerseits mit verstärkten Anstrengungen zur Detektion von autonomen USVs und UUVs reagieren würden, beispielsweise durch das Ausbringen von Sensornetzwerken.

Einsatz in A2/AD-Gebieten

Bisher operieren unbemannte Systeme vor allem in offenen, also durch eigene oder befreundete Kräfte hinreichend gut kontrollierten, Gebieten (z. B. durch Luftüberlegenheit). Hier werden unbemannte Systeme für Aufklärungs-, Überwachungs- und Erkundungsmissionen sowie zur Logistikunterstützung breit genutzt. Auch für offensive Operationen sind bewaffnete UCAVs im Einsatz, um hochwertige Ziele (z. B. Infrastruktur, militärische Objekte oder Personen) direkt anzugreifen.

Seit einigen Jahren spielen auch geschlossene Gebiete, bei denen es eine starke Luftverteidigung bzw. anderweitige Abwehrmaßnahmen gibt (»anti access and area denial«), in Bezug auf den Einsatz von unbemannten Systemen eine immer größere Rolle (DSB 2016, S. 61; U.S. Air Force 2014, S. 3). Es handelt sich hierbei häufig um Territorien, deren Gebietshoheit umstritten ist bzw. bei denen starke Verteidigungskräfte den Zugang verwehren oder hemmen. Da

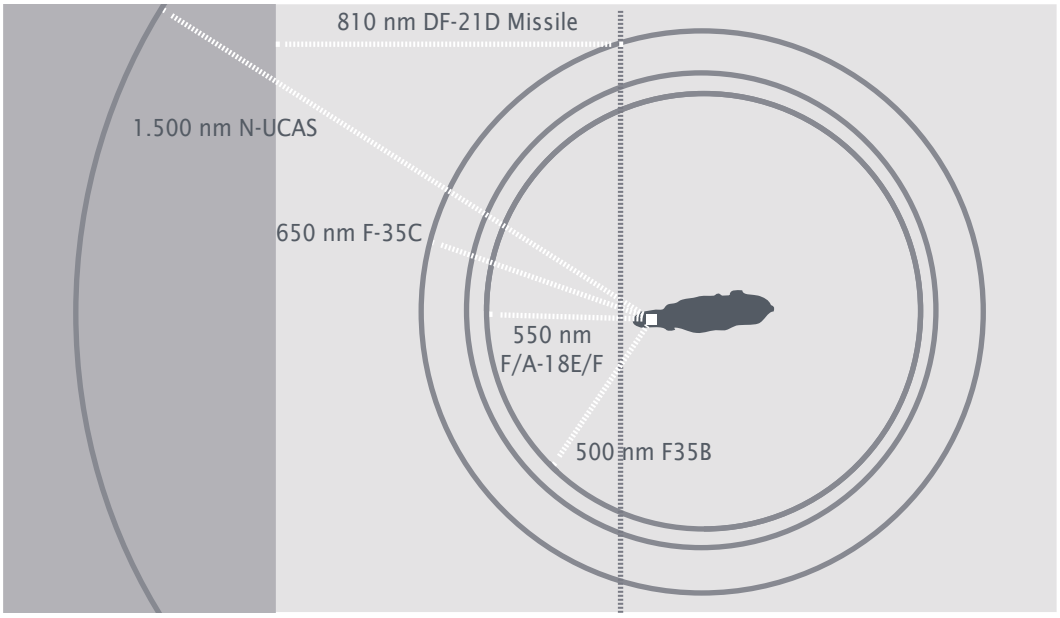
dort Kommunikationsverbindungen vom Gegner gestört oder aber anhand der elektromagnetischen Signale die eigene Position offenbart werden könnte, würde sich hier der Einsatz von AWS anbieten. Entsprechend genießt die Entwicklung dieser Fähigkeit eine hohe Priorität in gegenwärtigen strategischen Überlegungen (DOD 2013, S. 67). Das DSB (2016, S. 61) beschreibt A2/AD-Gegenmaßnahmen sogar als »ein Paradebeispiel einer Mission, die durch autonome Systeme verbessert werden könnte«.

Ein mögliches Szenario, um den militärischen Nutzen des Einsatzes von AWS in A2/AD-Umgebungen zu illustrieren, diskutiert Scharre (2014a, S. 19 ff.): Kampfdrohnen, die von Flugzeugträgern aus gestartet werden, könnten mit ihrer Reichweite von bis zu 1.500 Seemeilen (2.778 km) Landziele angreifen, ohne dass der Flugzeugträger in die Reichweite gegnerischer Antischiffsraketen mit ihrer aktuellen Reichweite von bis zu 810 Seemeilen (1.500 km) geraten würde (Abb. 5.2). Als Gegenreaktion der verteidigenden Seite wäre hier mit der intensiven Entwicklung und Verbreitung von Antischiffsraketen mit größerer Reichweite zu rechnen, die es erlauben, potenzielle Angriffe bereits im Vorfeld und in größerer Entfernung zu vereiteln.

Ein A2/AD-Einsatz ist aber weitaus anspruchsvoller als Einsätze in einer einfachen, offenen Umgebung. Die Verteidigungskapazitäten von aktuellen UCAVs in umkämpften Lufträumen sind unzureichend. In diesen Umgebungen sind sie nicht sehr widerstandsfähig, zudem sind sie aufgrund ihrer Datenverbindung aufspürbar und manipulierbar. Um potenziellen Angriffen zu entgehen, fliegen sie bei Nacht oder sehr hoch. Weder haben existierende Systeme nennenswerte Tarnkappenfähigkeiten (bei neuen Modellen wie z. B. der »Taranis« soll sich dies ändern; Kap. 4.2.2) noch können sie feindliche Angriffe ausmanövrieren oder das Feuer auf schnelle mobile Fahrzeuge eröffnen. Daher würde es z. B. ausreichen, in einem Hubschrauber neben einer UCAV herzufliegen und von dort auf sie zu schießen (Williams 2017).

Falls AWS eigenständig agieren könnten, ohne eine Kommunikationsverbindung zu unterhalten, wären sie sehr viel schwerer detektierbar. Flugzeugträger könnten autonome Luftfahrzeuge nahe an das Ziel heranbringen, von wo sie dann ins feindliche Gebiet eindringen könnten. Welche Aufgaben sie übernehmen können, hängt wesentlich von der Plattformgröße ab, da diese mit der erreichbaren Ausdauer, Nutzlast (z. B. Waffenmix) und Geschwindigkeit korreliert. Denkbar wäre, dass AWS einzeln oder als Schwarm ISR-Aufgaben erledigen oder Ziele wie Gebäude, Infrastruktur oder Menschengruppen angreifen, als unabhängige Mission oder auch als Vorhut für eine Intervention weiterer Einsatzkräfte. Weiterhin könnten Schwärme die feindliche Luftabwehr ablenken oder überlasten. Falls sie jedoch entdeckt würden, müssten sie in der Lage sein, dem gegnerischen Feuer schnell auszuweichen oder es zu erwidern. Sollten sie in die Hände des Gegners fallen, könnte der betreffende Staat die Verantwortung abstreiten.

Abb. 5.2 Kampfradien bemannter und unbemannter Flugzeuge



nm: nautische Meile; »DF-21D Missile«: Antischiffsrakete; N-UCAS (»naval uninhabited combat aircraft«): unbemanntes Kampfflugzeug der Marine; »F/A-18E/F«, »F-35B/C«: bemannte Kampfflugzeuge

Quelle: Scharre 2014a, S. 20

Spezialeinsätze

Für besondere oder verdeckte Operationen würden sich eher kleinere autonome Boden-, See- oder Luftsysteme eignen. Zudem könnten AWS auch in Zusammenarbeit mit menschlichen Soldaten ins Feld geschickt werden (MUM-T). Da sich Spezialeinsätze häufig auf hochrangige Ziele richten (ob einzelne Personen oder Gruppen, z. B. die Führungselite terroristischer Organisationen), ihnen eine intensive Vorbereitungsphase vorgeschaltet ist und die Missionserfüllung eine sehr hohe Priorität hat, wäre vermutlich das Risiko zu hoch, sich ausschließlich auf AWS zu verlassen. Stattdessen könnten Soldaten kleine, möglicherweise nur insektengroße autonome UGVs oder UAVs mit auf ihre Mission nehmen, die mit Miniaturkameras und Mikrosensoren ausgestattet sind (iPRAW 2017a, S. 14). Da sie nicht nur unauffällig, sondern auch agil sind, könnten die AWS unter der Anleitung eines Soldaten eigenständig die Umgebung ausspähen oder sichern und dabei auch als Schwarm operieren, wenn Schnelligkeit oder mehrere Blickwinkel gewünscht werden (U.S. Air Force 2016, S. 43). Auf diese Weise könnten einzelne Gegner auch gezielt ausgeschaltet werden. Derartige Einsätze könnten auch in urbanem Gelände stattfinden, wo AWS z. B. »kritische Informationen zur Position feindlicher Kämpfer und den Status von Räumen, Gebäuden, und Nachbarschaften für den Task Force Komman-

deur« ausspähen, der darauf aufbauend taktische Entscheidungen trifft (iPRAW 2017a, S. 14). Es ist davon auszugehen, dass AWS hier sowohl zu Aufklärungs- als auch zu Kampfzwecken Verwendung finden könnten.

AWS-AWS-Kampf

Wenn ein Staat von einem Gegner den Kampfeinsatz von AWS erwartet, wäre eine plausible Gegenmaßnahme, ebenfalls AWS ins Feld zu schicken, wenn diese zur Verfügung stehen. In einem symmetrischen Szenario mit Antagonisten mit vergleichbaren technologischen Fähigkeiten wären zukünftige Einsätze, in denen sich AWS in einer Kampfsituation gegenüberstehen, nicht nur denkbar, sondern sogar naheliegend. Für zeitkritische duellartige Situationen wären AWS aufgrund der möglichen schnellen Manövrierfähigkeit (die bei bemannten Flugzeugen durch die maximale Beschleunigung, die Menschen aushalten können, begrenzt ist),[61] der schnellen Reaktionszeit sowie Entscheidungsfindung prädestiniert. Im Falle von Luft-zu-Luft-Kämpfen haben KI-Systeme zumindest in Simulationen bereits unter Beweis gestellt, dass sie menschlichen Piloten überlegen sein können (Ernest et al. 2016; Reilly 2016). Boden-zu-Boden-Kämpfe stehen aufgrund der Schwierigkeiten des Terrains derzeit noch nicht im Fokus strategischer Überlegungen.

Damit wären Menschen in das direkte Kampfgeschehen nicht mehr involviert. Dem Argument, dass somit auch keine Menschen zu Schaden kommen können, stehen allerdings einige Bedenken gegenüber. Zum einen würde sich das Gefechtstempo ggf. so sehr erhöhen und quasiautomatisch ablaufen, dass eine Kontrolle oder ein Eingreifen durch menschliche Bediener nicht mehr möglich wären. Wenn der Kampf nicht in einem isolierten Teil des Schlachtfeldes stattfindet, würde diese rasante Gefechtsgeschwindigkeit und möglicherweise hohe Letalität möglicherweise anwesende Menschen gefährden (Neuneck 2014). Darüber hinaus bestünde das Risiko, dass automatisiert durch Aktion und schnelle Reaktion sich Konflikte aufschaukeln oder gar erst ausgelöst werden (Kap. 6). Wie KI- bzw. softwaregestützte Systeme unterschiedlicher Herkunft interagieren würden, ist kaum vorhersehbar und im Vorfeld auch nicht zu testen.

Nuklearszenario

Grundsätzlich ist nicht auszuschließen, dass AWS zukünftig mit Nuklearwaffen bestückt werden könnten. Szenarien, in denen unbemannte Langstreckensysteme mit nuklearer Bewaffnung eingesetzt werden, werden in Strategiezirkeln bereits durchgespielt (Bitzinger/Leah 2016). So sind beispielsweise Raketen, Marschflugkörper oder Hyperschallträgersysteme mit nuklearen Sprengköpfen

61 Diese beträgt etwa die 9-fache Erdbeschleunigung (Wikipedia 2003c).

denkbar, die im Endanflug autonom agieren. Autonome, durch Kernreaktoren angetriebene und mit Nuklearwaffen bestückte UUVs könnten mehrere Monate in den Tiefen des Meeres über den Globus verteilt versteckt ausharren, bis ein Funkbefehl sie aktiviert. Ohne eine Besatzung, die nach gewisser Zeit an Land gehen müsste, z. B. um Proviant aufzunehmen, und ohne kontinuierliche Datenverbindung zu einer Militärbasis wären sie noch schwerer auffindbar als U-Boote mit menschlicher Besatzung. Bei einem potenziellen nuklearen Erstschlag auf das Heimatland könnten sie dann aus sicherer Entfernung einen Zweitschlag durchführen. Insofern könnten autonome Nuklear-UUVs zur strategischen Abschreckung eingesetzt werden. Nach Auffassung der USA ist Russland im Begriff, ein solches autonomes nuklear bewaffnetes Unterwasserfahrzeug zu entwickeln und zu stationieren (Kap. 4.1.3).[62]

Autonome UCAVs könnten ebenfalls mit nuklearen Waffen bestückt und bei Bedarf eingesetzt werden. Wenn sie eigenständig Objekten oder auch bekannten Luftüberwachungsstützpunkten ausweichen könnten und durch Tarnkappenfähigkeiten schwerer durch Verteidigungsradare erkennbar wären, wäre dies ein nennenswerter Vorteil gegenüber bemannten oder ferngesteuerten Flugzeugen. Gleichzeitig könnten autonome nukleare Waffensysteme die Reaktionszeiten für Vergeltungsschläge nach einem nuklearen Erstschlag durch den Feind verkürzen, was einerseits der Abschreckung dienen, andererseits die Möglichkeiten zur Überprüfung der Situationslage durch den Menschen einschränken könnte (Altmann/Sauer 2017, S. 128 ff.). Aber auch das nicht geringe Unfallrisiko, mögliches Fehlverhalten oder Gegenmaßnahmen und die ohnehin hohe Anzahl von Nuklearwaffen sprechen gegen die Entwicklung nuklearwaffenfähiger AWS.

5.3.3 Zwischenfazit

Die besonderen Systemfähigkeiten zukünftiger AWS gründen sich zum einen auf die physische Abwesenheit eines Bedieners, die u. a. kleinere und agilere Plattformen ermöglicht, die in Gebieten operieren können, die für Menschen nicht oder nur schwer zugänglich sind. Zum anderen werden die Fähigkeiten durch die Möglichkeit bestimmt, autonom zu operieren, was schnellere und bessere Entscheidungen in zeitkritischen Situationen ermöglichen soll sowie neue Optionen zur Koordination in einer Gruppe (bzw. einem Schwarm) von AWS oder aber zur Kooperation zwischen einem oder mehreren AWS und Menschen (»manned-unmanned teaming«) eröffnet.

Aufgrund ihrer potenziellen Fähigkeiten und daraus resultierender militärischer Vorteile werden sich AWS insbesondere für Einsatzszenarien eignen, die für menschliche Bediener wegen der Umgebungsbedingungen problematisch

62 Im Original: »Russia is also developing at least two new intercontinental range systems, a hypersonic glide vehicle, and a new intercontinental, nuclear-armed, nuclear-powered, undersea autonomous torpedo.« (DOD 2018a, S. 9)

oder zu gefährlich sind (z. B. Unterwasserkriegsführung, durch starke Kräfte verteidigtes Terrain oder A2/AD-Räume), die sehr schnelle Reaktionszeiten oder eine hohe Manövrierfähigkeit erfordern (z. B. Luftkampf) oder aber in einer dynamischen Umgebung ohne eine permanente Kommunikationsverbindung stattfinden (verdeckte Operationen hinter den feindlichen Linien oder bei Störung der Kommunikationsverbindung). Da AWS perspektivisch vermutlich für zunehmend unterschiedliche Operationsarten eingesetzt werden können, wird durch sie auch die Aufgabenverteilung zwischen Mensch und Maschine neu definiert werden.

Zum gegenwärtigen Zeitpunkt sind jedoch sowohl die technischen Eigenschaften als auch die Verfügbarkeit zukünftiger AWS noch spekulativ, sodass die hier entwickelten möglichen Einsatzszenarien lediglich die Umrisse eines möglichen Portfolios skizzieren. Dessen konkrete Ausgestaltung hängt von einem komplexen Zusammenspiel technologischer Entwicklungen und der Wandlung der Streitkräftestrukturen ab, die sich im Zuge der sukzessiven Integration von Robotik und Autonomie in Doktrinen, Strategien sowie Taktiken, Techniken und Prozeduren abzeichnet.

Ein Feld, das bisher noch wenig beleuchtet ist, das aber absehbar mit einer zunehmenden Verbreitung von AWS erheblich an Bedeutung gewinnen wird, betrifft mögliche technologische oder operative Gegenmaßnahmen, die von Antagonisten gegen AWS getroffen werden könnten. Die Sensoren und computergestützten kognitiven Fähigkeiten von AWS werden ganz eigene Schwachstellen aufweisen, die von entsprechend innovativen Antagonisten ausgenutzt werden könnten. Hierzu gehören sowohl Möglichkeiten der elektronischen Manipulation (»jamming«, »spoofing«, »hacking«). Aber auch eher im Lowtechbereich angesiedelte Maßnahmen könnten ggf. sehr effektiv sein, beispielsweise Fangnetze gegen kleine fliegende AWS oder aber aufblasbare Attrappen oder thermische Quellen, um hitzesuchende Sensoren zu täuschen (Neuneck 2014, S. 68 ff.).

Kasten 5.1 Die militärische KI-Strategie der US-Regierung

Die USA messen der Anwendung künstlicher Intelligenz eine herausragende Bedeutung bei der Modernisierung ihrer Streitkräfte bei. In ihrer 2018 vom Verteidigungsministerium formulierten »Nationalen Verteidigungsstrategie« heißt es: »Das Ministerium wird umfangreich investieren in die militärische Anwendung von Autonomie, künstlicher Intelligenz und Maschinenlernen einschließlich der schnellen Anwendung von im kommerziellen Sektor erzielten (technologischen) Durchbrüche, um militärische Wettbewerbsvorteile zu generieren«[63] (DOD 2018b, S. 7).

63 Im Original: »The Department will invest broadly in military application of autonomy, artificial intelligence, and machine learning, including rapid application of commercial breakthroughs, to gain competitive military advantages.«

Das Verteidigungsministerium hat diese Ankündigung untermauert und konkretisiert durch die Ausarbeitung einer KI-Strategie (DOD 2019). Diese wurde am 12. Februar 2019 im Vorfeld der Münchner Sicherheitskonferenz öffentlich vorgestellt. Unterstrichen wird die hohe Priorität, die die US-Regierung der KI beimisst, durch einen Exekutiverlass zur Förderung und Priorisierung von KI, den der Präsident am Tag vor der Präsentation der militärischen KI-Strategie unterzeichnete (U.S. President 2019).[64]

Als Hauptziele der Einführung von KI im Verteidigungssektor werden in dem Strategiepapier Verbesserungen bei der Unterstützung und dem Schutz der eigenen Soldaten bzw. der Bevölkerung genannt sowie Vorteile bei der Verteidigung von Verbündeten und Partnern. Zudem könnten militärische Operationen schneller durchgeführt werden und wären erschwinglicher.[65] Als starkes Motiv wird der Wettbewerb angeführt, der weltweit um KI für militärische Zwecke entbrannt ist. Insbesondere China und Russland würden hier voranschreiten, auch bei Anwendungen, bei denen es fragwürdig ist, ob sie mit internationalen Normen und den Menschenrechten vereinbar sind. Diese Entwicklungen drohen den technologischen und operationellen Vorsprung der USA zu gefährden und die freie und offene internationale Ordnung zu destabilisieren.[66]

Die Kernelemente der Strategie sind unter fünf Überschriften zusammengefasst (DOD 2019, S. 7 f.):

Bereitstellen von KI-getriebenen Fähigkeiten für zentrale Missionen

Hierfür werden als Beispiele genannt die Verbesserung des Lagebewusstseins und der Entscheidungsfindung, die Steigerung der Betriebssicherheit von Ausrüstung, die Implementierung von vorausschauender Instandhaltung und Beschaffung sowie die Straffung von Geschäftsabläufen. Es sollen KI-Systeme priorisiert werden, die die Fähigkeiten des Personals erweitern, indem sie es von mühsamen kognitiven oder physischen Aufgaben entlasten und neue Arbeitsweisen einführen.

64 Dies erfolgte nach dem Redaktionsschluss des vorliegenden TAB-Berichts. Wegen der großen Relevanz wurde dennoch dieser Textteil aufgenommen. Es war allerdings nicht möglich, alle Kapitel eingehend auf möglichen Änderungs- bzw. Ergänzungsbedarf zu prüfen.

65 Im Original: »With the application of AI to defense, we have an opportunity to improve support for and protection of U.S. service members, safeguard our citizens, defend our allies and partners, and improve the affordability and speed of our operations.« (DOD 2019, S. 5)

66 Im Original: »Other nations, particularly China and Russia, are making significant investments in AI for military purposes, including in applications that raise questions regarding international norms and human rights. These investments threaten to erode our technological and operational advantages and destabilize the free and open international order.« (DOD 2019, S. 5)

Ausweiten der Wirkungen von KI im gesamten Geschäftsbereich des Verteidigungsministeriums durch Schaffung einer gemeinsamen Grundlage, die zu dezentraler Entwicklung und experimenteller Erprobung befähigt

Es wird erwartet, dass insbesondere von der Praxis von Nutzern in vorderster Front Impulse für die Entwicklung transformativer KI-Anwendungen ausgehen und nicht (nur) aus zentralen Entwicklungsabteilungen. Es soll eine gemeinsame Grundlage für dezentrale Entwicklung geschaffen werden, die aus gemeinsam genutzten Daten, Tools, Bezugssystemen sowie Standards in Cloud- und Edge-Diensten[67] bestehen soll. Gleichzeitig sollen bestehende Prozesse und Routinen durch Digitalisierung und Automatisierung für die Einbindung von KI vorbereitet werden, um deren Diffusion zu beschleunigen.

Kultivieren einer Belegschaft, die führend in KI ist

Um die KI-bezogenen Kenntnisse und Fähigkeiten des Personals auf das höchstmögliche Niveau zu heben, soll umfassend in Ausbildung und Training investiert werden und gleichzeitig externes Know-how von Weltklasseformat durch Rekrutierung und Bildung von Partnerschaften integriert werden.

Einbinden von kommerziellen, akademischen und internationalen Verbündeten und Partnern

Partnerschaften entlang der gesamten Innovationskette sollen gepflegt und verstärkt werden, vor allem mit dem kommerziellen Sektor, um dortige Fortschritte mit den Anforderungen des Verteidigungssektors zu verknüpfen. Auch für den Verteidigungsbereich eher unübliche Kooperationen sollen vorangetrieben werden, insbesondere mit der globalen Open-Source-Community. Bei der Interaktion mit dem kommerziellen Sektor soll die Defense Innovation Unit (DIU) eine zentrale, beschleunigende Rolle einnehmen (DOD 2019, S. 13).

Bei militärischer Ethik und KI-Sicherheit die Führung übernehmen

Die Formulierung eines Leitbildes von rechtlich zulässiger und ethisch vertretbarer Entwicklung und Nutzung von KI soll in führender Rolle vorangetrieben werden. Hierbei sollen die akademische Welt, die Privatwirtschaft und die internationale Gemeinschaft einbezogen werden, um Ethik und Sicherheit der KI im militärischen Kontext zu verbessern. FuE von KI-Systemen sollen gestärkt werden, die robust, zuverlässig und sicher sind. Forschung zu Techniken, die eine besser erklärbare KI (»explainable AI«; Kap. 3.3.3) erzeu-

67 Edge Computing bezeichnet im Gegensatz zum Cloud Computing die dezentrale Datenverarbeitung am Rand des Netzwerks (Wikipedia 2017).

gen, sollen gefördert werden. Bei der Entwicklung von Methoden für Tests, Bewertungen, Verifizierung und Validierung (»test and evaluation, verification and validation« – TEVV) soll Pionierarbeit geleistet werden.

Es soll nach Möglichkeiten Ausschau gehalten werden, KI einzusetzen, um unbeabsichtigtes Leid und Kollateralschäden durch ein gesteigertes Situationsbewusstsein und eine verbesserte Entscheidungsunterstützung zu reduzieren. Um zu fördern, dass die Entwicklung und der Einsatz von KI auch in anderen Ländern in verantwortungsbewusster Weise geschehen, sollen Ziele, ethische Richtlinien und Sicherheitsverfahren mit diesen geteilt werden (DOD 2019, S. 8, 15 f.).

Das Joint Artificial Intelligence Center

Die KI-Strategie wird institutionell unterfüttert durch die Gründung des JAIC, das als Brennpunkt für ihre Umsetzung fungieren soll. Die Arbeit des JAIC soll die eher langfristig orientierte Grundlagenforschung und Technologieentwicklung, die in bestehenden Organisationen wie der DARPA und weiteren vom Verteidigungsministerium unterstützten Forschungseinrichtungen beheimatet sind, durch kurzfristigere umsetzungsorientierte FuE komplettieren. Als Schwerpunkte des JAIC werden genannt: Prototypen identifizieren und zur Verfügung stellen, Wissenstransfer vorantreiben und Forschung mit dem praktischen Betrieb verzahnen, Prototypen zur Praxisreife fortentwickeln, laufende Unterstützung bieten (DOD 2019, S. 9 f.).

6 Sicherheitspolitische Implikationen von AWS

Aktuell ist ein Wettlauf im Gange, wer die Entwicklung und den Einsatz von KI in vielen Lebensbereichen anführt. Wie der russische Präsident Putin kürzlich ausführte: »Künstliche Intelligenz ist die Zukunft, nicht nur für Russland, sondern für die gesamte Menschheit. Sie ist mit gewaltigen Möglichkeiten verbunden, aber auch mit Gefahren, die schwer vorherzusehen sind. Wer auf diesem Feld führend ist, wird die Welt beherrschen.«[68] Oder wie es in der kürzlich veröffentlichten nationalen Verteidigungsstrategie der USA heißt: »Neue Technologien einschließlich hochentwickelte Rechenverfahren, ›Big Data‹-Analysen, künstliche Intelligenz, Autonomie, Robotik, gebündelte Energie, Überschall- und Biotechnologie – genau diese Technologien stellen sicher, dass wir in der Lage sein werden, die Kriege der Zukunft zu führen und zu gewinnen«.[69] Einschätzungen dieser Art sowie die im Kapitel 5 skizzierten militärischen Vorteile, die AWS versprechen, generieren einen hohen Anreiz, die militärische Nutzung von zunehmend autonomen Systemen voranzutreiben. In Staaten mit verantwortlich handelnder Führung wird dies zwar begrenzt durch die Schwelle, jenseits derer dies nicht mehr ethisch zu rechtfertigen scheint. Diese Schwelle ist jedoch bis heute weder national noch im internationalen Kontext klar definiert. Auch wenn dies durch rüstungskontrollpolitische Vereinbarungen (Kap. 9) geleistet würde, bestünde keine Gewähr, dass Regierungen mit weniger moralischen Skrupeln dieses als verbindliche *rote Linie* akzeptieren würden.

Um auf alle möglichen Entwicklungen vorbereitet zu sein, ist es daher essenziell, sich mit den sicherheitspolitischen Implikationen zu befassen, die die Verbreitung und der mögliche Einsatz von AWS mit sich bringen können. Risiken für die internationale Stabilität und Sicherheit lassen sich grob in drei Dimensionen unterteilen (Altmann/Sauer 2017; Scharre 2018):

Die erste ist verbunden mit der Gefahr von unkontrollierter Verbreitung und dem Triggern von Rüstungswettläufen. So würde allein die begründete Vermutung eines Staates, dass ein anderer AWS mit neuartigen Fähigkeiten anstrebt oder sogar bereits besitzt, intensive Entwicklungs- und Beschaffungsbemühungen auslösen, um nicht rüstungstechnologisch ins Hintertreffen zu

68 Rede gehalten für Schüler anlässlich der Onlineveranstaltung »Russland, Blick in die Zukunft«. Im Original: »Искусственный интеллект – будущее не только России, это будущее всего человечества. Здесь колоссальные возможности и трудно прогнозируемые сегодня угрозы. Тот, кто станет лидером в этой сфере, будет властелином мира.« (Jaroslawl 2017)

69 Im Original: »New technologies include advanced computing, ›big data‹ analytics, artificial intelligence, autonomy, robotics, directed energy, hypersonics, and biotechnology – the very technologies that ensure we will be able to fight and win the wars of the future.« (DOD 2018b, S. 3)

geraten. Diese Bemühungen würden wohl wiederum den ersten Staat veranlassen, seine Aktivitäten noch zu intensivieren, wodurch sich eine Rüstungsspirale ausbilden und immer schneller drehen könnte, die einerseits bei allen Beteiligten ein Bedrohungsgefühl erzeugen und andererseits erhebliche ökonomische Ressourcen verschlingen würde. Beide Effekte könnten dazu beitragen, Krisen zu erzeugen oder zu verschärfen. Auch wenn substaatliche Akteure (von Aufständischen bis Terrorgruppen) sich neuartige AWS beschaffen oder glaubwürdig damit drohen könnten, wären schwerwiegende sicherheitspolitische Konsequenzen zu befürchten.

Die zweite Dimension bezieht sich darauf, dass die Eigenschaften von AWS dazu führen könnten, dass die Hemmschwelle zum Einsatz von Waffengewalt sinken könnte. So könnte im Konfliktfall häufiger Waffengewalt eingesetzt werden und Krisen auf diese Weise schneller eskalieren. Dies gilt umso mehr, als der Raum für deeskalierend wirkende politische Initiativen durch die technologisch induzierte Beschleunigung des Konfliktgeschehens tendenziell schrumpfen könnte.

Die dritte Dimension bezeichnet die Gefahr, dass die neuartigen Fähigkeiten von AWS einen militärischen Erstschlag ermöglichen könnten, der einen der Kontrahenten seiner Fähigkeit zum Zurückschlagen beraubt. Selbst die begründete Vermutung, dass ein solches Erstschlagpotenzial aufgebaut werden könnte, würde in höchstem Maße destabilisierend wirken, insbesondere wenn es sich bei den Akteuren um Nuklearmächte handelt.

Einige Aspekte der sicherheits- und stabilitätspolitischen Dimensionen werden im Folgenden eingehender untersucht. Manche der Argumente sind in ähnlicher Weise schon für ferngesteuerte bzw. teilweise automatisierte unbemannte Systeme zutreffend, andere beziehen sich expliziter auf die Fähigkeit zu autonomen Operationen von AWS. Das Gutachten von (Alwardt et al. 2017) stellt eine wesentliche Grundlage für das Folgende dar.

6.1 Mehr oder weniger Kriege?

Ob die Verfügbarkeit von AWS dazu führt, dass im Konfliktfall schneller zum Mittel der militärischen Gewalt gegriffen wird oder dass militärische Auseinandersetzungen gewaltsamer geführt werden, ist derzeit eine kontrovers diskutierte Frage.

Einige Argumente sprechen für eine solche Entwicklung (Heyns 2013, S. 11 ff.): Der größere physische und psychologische Abstand vom eigentlichen Kampfgeschehen, der durch AWS ermöglicht wird, könnte die Hemmschwelle, Gewalt einzusetzen, senken. Demokratisch gewählte Regierungen stehen regelmäßig unter erheblichem Rechtfertigungsdruck, wenn eigene Soldaten gefährdet oder getötet werden. Aufgrund des durch AWS verringerten Risikos für eigene Soldaten könnte die Öffentlichkeit einen Krieg nicht mehr als letzten

Ausweg bzw. als einschneidendes Ereignis von nationaler Bedeutung wahrnehmen, sondern diesen als einen unter dem Primat diplomatischer und ökonomischer Abwägungen stehenden Normalfall akzeptieren. Auch unterhalb der Schwelle ausgewachsener Kriege können Militäreinsätze zur Durchsetzung politischer Ziele attraktiv sein und immer mehr zur Regel werden.

Andererseits können einige Argumente gegen eine wesentliche Erhöhung der Konfliktgefahr ins Feld geführt werden: Jede Technologie und militärische Praktik, die das Risiko für eigene Soldaten bzw. die Opferzahlen auf dem Schlachtfeld verringert, senkt nach der angeführten Logik die Schwelle zum Einsatz militärischer Mittel. AWS würden hier nichts grundsätzlich Neues bringen, sondern eine ohnehin vonstattengehende Entwicklung lediglich graduell verstärken. Auch sind Situationen vorstellbar – beispielsweise, wenn Warlords die Bevölkerung terrorisieren bzw. ethnische Säuberungen durchführen –, in denen ein schnellerer und entschlossenerer Einsatz von Gewaltmitteln viel menschliches Leid verhindert. Generell verliert das Argument, dass AWS zu einem häufigeren Einsatz von Gewalt führen, erheblich an Kraft, wenn man ein Szenario mit etwa gleich starken Kontrahenten betrachtet. Hier würde für die Seite, die AWS einsetzt, immer die Gefahr bestehen, dass schmerzhafte Vergeltungsmaßnahmen des Gegners folgen bzw. im ungünstigsten Fall eine Eskalation zu einem ausgewachsenen Krieg mit ungewissem Ausgang eintritt. Insbesondere für die Nuklearwaffenstaaten untereinander würde dieses Kalkül stark gegen einen beabsichtigten und als lokal begrenzt intendierten Einsatz von AWS sprechen.

6.2 Veränderung der Kriegsführung

Neue Technologien haben historisch immer auch die Kriegsführung verändert oder gar revolutioniert, sowohl in Form der zur Verfügung stehenden Wirkmittel als auch in der Art und Strategie ihres Einsatzes. Gegenwärtig sind bereits einige Umwälzungen im Gange, die sich im Wechselspiel geopolitischer Entwicklungen, strategischer Überlegungen und von technologischem Fortschritt vollziehen.

So tritt die klassische Art von Krieg, in dem zwei souveräne Staaten direkt gegeneinander kämpfen, im historischen Vergleich immer mehr hinter andere Formen der Austragung von Konflikten zurück (Pettersson/Eck 2018). AWS können hier existierende Asymmetrien zwischen Staaten, die AWS besitzen, und technologisch weniger fortgeschrittenen Ländern noch vergrößern (CCW 2016b, S. 3 Punkt 19). Auch würde der bestehende Trend durch AWS verstärkt, dass das Risiko, im bewaffneten Konflikt getötet zu werden, für das Militärpersonal technologisch fortgeschrittener Länder sinkt, für andere Beteiligte, sowohl feindliche Kämpfer als auch Zivilisten, hingegen ansteigt (Shaw 2002).

Im Folgenden werden einige Aspekte, wie AWS zu Veränderungen in der Kriegsführung beitragen können, näher betrachtet.

Digitalisierung der Kriegsführung

Die Digitalisierung der Kriegsführung, die mit einer zunehmenden Automatisierung und Vernetzung von Waffensystemen einhergeht, ist erklärtes Ziel der strategischen Überlegungen in den Streitkräften technologisch potenter Staaten. In den USA läuft dies unter dem Titel »Network Centric Warfare« (Wilson 2005), in Deutschland unter »Vernetzte Operationsführung« (NetOpFü) (BMVg 2004, S. 15). Dabei werden sukzessive Aufgaben an Maschinen bzw. Programmsoftware abgegeben, die bisher von Menschen erledigt worden sind. So werden z. B. aktuell Drohnen nicht mehr von einem Operateur direkt gesteuert, sondern dieser nimmt nur noch eine übergeordnete Kontrollfunktion wahr. Im Rahmen netzwerkzentrierter Kriegsführung wären AWS zur Durchführung komplexer Aufgaben prädestiniert, die menschliche Operateure überfordern. Hierzu zählen schnelle Reaktionen auf sich verändernde Missionsparameter oder die Koordination bzw. Steuerung komplexer Systemverbünde in Echtzeit. Außerdem könnten AWS abseits von Gefechtsfeldern in einer dynamischen, vielleicht auch zivilen Umgebung hinter den feindlichen Linien eingesetzt werden. Damit einhergehend droht dem Menschen jedoch zusehends der Einblick in die zugrundeliegenden Entscheidungsprozesse und Informationsgrundlagen verlorenzugehen, sodass er seiner Kontrollfunktion nicht mehr nachkommen kann.

Allerdings ist es keineswegs selbstverständlich, dass Streitkräfte, die auf der Grundlage von hochorganisierten Kommando- und Kontrollstrukturen operieren, in der Lage sind, Systeme mit autonomen Funktionen reibungslos in ihre Abläufe zu integrieren. Beim Militär handelt es sich kulturell zudem um eine eher konservative Institution, die durchaus skeptisch gegenüber tiefgreifenden institutionellen Veränderungen sein kann (Rosen 1991).

Verdeckte Operationen

Wie der heutige Einsatz von UCAVs im Rahmen von asymmetrischer Kriegsführung und gezielten Tötungen (»targeted killings«) vor Augen führt, können AWS sehr wirkungsvolle Instrumente für verdeckte Operationen oder geheimdienstliche Maßnahmen in Graubereichen und auch in zivilen Umgebungen sein. Damit würde der gegenwärtige Trend, dass die Grenzen zwischen zivilen und militärischen Räumen zunehmend verschwimmen, noch verstärkt und einer weiteren Entgrenzung des Krieges Vorschub geleistet.

Gegenreaktionen

Für Staaten, denen der Zugriff auf AWS verwehrt bleibt, wäre eine (radikale) Option die Anschaffung von Massenvernichtungswaffen (MVW), z. B. von Nuklearwaffen, um gegen die militärtechnische Überlegenheit von großen Mili-

tärmächten wie den USA oder China vorzugehen und etwaige Interventionen mit AWS abzuschrecken (Neuneck 2014). Derartige Entwicklungen würden sich auf die strategische Stabilität auswirken. Es ist jedoch fraglich, ob es wirklich realistischer ist, MVW statt AWS zu erwerben.

Eine weitere mögliche Reaktion ist, umfassend in die Entwicklung sowie Produktion von Anti-AWS-Mitteln zu investieren. Eventuell wären auch technologisch einfache Gegenmaßnahmen effektiv, beispielsweise Störsender, aufblasbare Panzerattrappen oder thermische Quellen, um hitzesuchende Sensoren zu täuschen. Auch wenn die Soldaten durch entsprechendes Equipment gut vor AWS geschützt sind, trifft dies nicht unbedingt auf die Zivilbevölkerung zu. Folglich könnte es unter Umständen zu höheren Kollateralschäden, d. h. zivilen Opfern kommen (Neuneck 2014).

Antiterrorismuseinsätze

In US-Strategiepapieren wird explizit darauf hingewiesen, dass Militärsysteme mit »zunehmend autonomen Funktionen« erforderlich wären, um terroristische Gruppen weltweit zu verfolgen, zu überwachen und zu bekämpfen (U.S. Air Force 2016, S. 10). UCAVs haben im Rahmen des »Global War on Terror« bereits immens an taktischer Bedeutung gewonnen. Präsident Obama bezeichnete sie im Mai 2013 als »Allheilmittel« gegen Terrorismus (Zenko/Kreps 2014, S. 10). Derzeitige UCAVs eignen sich für Antiterrorismuseinsätze besonders gut; sie operieren in Räumen, in denen sie keiner nennenswerten Luftverteidigung ausgesetzt sind. Einige Tendenzen, die heute bei der Nutzung von UCAVs in Antiterrorismusoperationen beobachtbar sind, könnten sich bei AWS weiter verstärken, z. B. verleiten bereits heutige UCAV-Einsätze vielfach dazu, verdächtige Personen in Kriegszonen und instabilen Gebieten zu töten, anstatt sie gefangen zu nehmen (Horowitz et al. 2016, S. 20).

Innerstaatliche Einsätze

Prognosen zum innerstaatlichen Einsatz von AWS konzentrieren sich häufig auf Autokratien. Autokratische Herrscher, die bestimmten Bevölkerungsteilen schaden oder sie bestrafen wollten, hätten durch AWS eine neue Handlungsoption. In der Vergangenheit kam es vor, dass sich Militärpersonal weigerte, gegen die eigene Bevölkerung vorzugehen. Laut dem stellvertretenden US-Verteidigungsminister Robert Work (2015) könnten »autoritäre Regime zu gänzlich automatisierten Lösungen tendieren«, weil sie menschlichen Sicherheitskräften nicht vertrauen.[70]

70 Rede von Robert O. Work, gehalten in Washington, D.C., 14. Dezember 2015, CNAS Defense Forum, zitiert nach Horowitz et al. (2016, S. 34).

Auch in Demokratien ist jedoch ein innerstaatlicher Einsatz nicht auszuschließen. Das Beispiel von heutigen unbemannten Systemen zeigt, dass die Einsatzhemmschwelle sinkt, wenn sich neue Technologien verbreiten und die Bevölkerung sich an sie gewöhnt. Während die Möglichkeit eines UCAV-Einsatzes gegen amerikanische Staatsbürger auf US-Territorium 2013 noch eine heftige Kontroverse ausgelöst hatte (Swaine 2013), verfügen heute zunehmend mehr Polizeieinheiten über kleine unbewaffnete Luftfahrzeuge. Im September 2015 legalisierte North Dakota dann als erster Bundesstaat die polizeiliche Nutzung von UAVs, die mit Tränengas, Gummigeschossen und Pfefferspray bewaffnet werden können (Austin 2015). In Connecticut wurde im Frühjahr 2017 ein Gesetzesvorschlag debattiert, der lokalen Polizeikräften die Ausrüstung von UAVs mit tödlichen bzw. nichttödlichen Waffen gestattet hätte (Reuters 2017). Letztendlich wurde der Vorschlag zwar abgelehnt (Smith 2017), dennoch ist es denkbar, dass auch AWS in Zukunft nicht nur in ausländischen Konflikten, sondern auch innerhalb eines Staates eingesetzt werden.

6.3 Destabilisierende Wirkung in Krisen

Zwischen Militärmächten hat es schon immer Zeiten erhöhter Spannungen gegeben, in denen Akteure bewusst Risiken der Eskalation auf sich nahmen, um politische Ziele durchzusetzen.[71] Dabei ist die Fähigkeit, diese Eskalation gezielt zu managen, entscheidend, um Ziele zu möglichst geringen (politischen und ökonomischen) Kosten zu erreichen und gleichzeitig das Ausbrechen eines Krieges zu vermeiden.

Es stellt sich die Frage, welche Auswirkungen AWS in einer solchen spannungsgeladenen Situation haben könnten. Auf der einen Seite könnten sie die Stabilität dadurch erhöhen, dass mehr Informationen in kürzerer Zeit beschafft und ausgewertet werden können und somit eine bessere Grundlage und mehr Zeit für menschliche Entscheidungsträger zur Verfügung steht, alle Konsequenzen einer Eskalation zu durchdenken und die *richtige* Entscheidung zu treffen. Außerdem könnten AWS auch als defensive Systeme ausgelegt sein und so einen eskalationswilligen Akteur von einer Aggression abbringen. Eine weitere Möglichkeit wäre, die Abschreckung zu erhöhen, indem glaubwürdig im Falle einer möglichen Aggression des Gegners mit einem massiven autonomen Zweitschlag gedroht wird, um auf diese Weise die Stabilität zu erhöhen.

Auf der anderen Seite könnten autonome Waffensysteme destabilisierend wirken, wenn deren unvorhergesehene Interaktionen mit der Umwelt, mit gegnerischen Kräften oder mit anderen autonomen Systemen unbeabsichtigt zur Eskalation führen. AWS könnten das operative Geschehen und die Entscheidungsprozesse derart beschleunigen, dass das menschliche Reaktionsvermögen

71 Die folgende Darstellung orientiert sich an Scharre (2018, S. 199 ff.).

überfordert würde. In einer Krise könnte hierdurch die zur Verfügung stehende Bedenkzeit, um z. B. mögliche Unfälle, Fehlkommunikation oder Fehlinterpretationen auszuschließen, stark verringert werden und eine Eskalationsspirale damit automatisiert und möglicherweise ungewollt in Gang gesetzt werden. In Analogie zu Kursverlusten an Devisen- und Aktienmärkten, die von automatisierten Handelsplattformen ausgelöst und unter dem Schlagwort »flash crash« (Wikipedia 2010b) bekannt geworden sind, hat Scharre (2018) für dieses Szenario den Begriff »flash war« geprägt.

Die potenzielle Beschleunigung des Geschehens könnte auch dazu führen, dass Akteure dazu veranlasst werden, präemptiv zuzuschlagen. Außerdem könnte der skizzierte Versuch, das Abschreckungspotenzial durch autonome Antworten zu erhöhen, auch die Stabilität unterminieren, wenn z. B. bei technischen Fehlfunktionen keine Möglichkeit der menschlichen Intervention mehr besteht und so ein potenziell katastrophaler Schlag unbeabsichtigt geführt würde.

AWS wären auch dazu prädestiniert, proaktiveres und eventuell provokativeres militärisches Verhalten zu unterstützen, wie z. B. das Eindringen in gegnerisches Territorium, um dort Aufklärung zu betreiben. Ein gegnerischer Staat könnte nun auch eine geringere Hemmung haben, eine solche unbemannte Plattform abzuschießen, woraus wiederum ein unmittelbares neues Eskalationspotenzial erwächst. Mögliche Situationen, in denen das Eskalationspotenzial von AWS besonders hoch sein kann, sind unterschwellige Krisen, wie z. B. ein eskalierender diplomatischer Schlagabtausch zwischen Staaten oder schwelende Grenzkonflikte (z. B. zwischen Indien und China).

6.4 Auswirkungen auf regionale Stabilität

Eine Destabilisierung einer latenten Krise zwischen regionalen Kontrahenten droht unmittelbar, falls AWS aufgrund spezifischer Fähigkeiten oder Einsatzoptionen einen bestehenden militärischen Status quo gefährden, also das Kräfteverhältnis zu verschieben drohen. Darüber hinaus kann die Stabilität innerhalb bestimmter Regionen durch Rüstungsdynamiken gefährdet werden, die durch AWS angestoßen bzw. verstärkt werden. Dies kann sich zu einer massiven gegenseitigen Aufrüstung (Wettrüsten) entwickeln, die in hohem Maße destabilisierend wirken würde.

Als Beispiel hierfür kann die Situation im Westpazifik angeführt werden. Hier stehen sich – neben einer Vielzahl weiterer Akteure – mit den USA und China auch zwei Großmächte gegenüber, die beide eine regionale Führungsrolle beanspruchen und diese auch mit politischen und militärischen Mitteln zu untermauern oder auszuweiten versuchen. Die USA operieren in diesem Gebiet bisher relativ unbehelligt, u. a. mit ihren Flugzeugträgerverbänden. In Form von verstärkten A2/AD-Kapazitäten arbeitet China bereits an robusten Maßnah-

men, mit denen es sich zukünftig in die Lage versetzen möchte, gegnerischem Militär den Zutritt zu bestimmten Gebieten des Westpazifiks zu verwehren. Neben dem heutigen Ausbau seiner maritimen Streitkräfte, von Offshore-Militärbasen und einer Verstärkung der regionalen Luftverteidigung könnten AWS zukünftig insbesondere in der See- und Luftkriegsführung ein probates Mittel für das chinesische Militär sein, um der maritimen Dominanz und Luftüberlegenheit der USA zu begegnen. Die USA werden sich ihrerseits den Zutritt zum Westpazifik mit geeigneten militärischen Mitteln sichern wollen, wozu dann sehr wahrscheinlich auch AWS zählen werden. Eine Schwächung regionaler Stabilität kann hier also sowohl aus Rüstungsdynamiken erwachsen als auch diese befeuern. Angesichts einer Vielzahl von Akteuren und Interessen im westpazifischen Raum und damit einhergehender Krisenpotenziale könnte durch AWS die Eskalationsgefahr weiter steigen und damit zur Instabilität der Region beitragen.

6.5 Auswirkungen auf das strategische Gleichgewicht

Auf der globalen Ebene spielt über den Kalten Krieg hinaus auch immer noch die strategische Stabilität zwischen den Nuklearwaffenstaaten eine herausragende Rolle. Das strategische Gleichgewicht, das seinen Ausdruck in der gesicherten Fähigkeit eines Zweitschlags findet, wird nach Ansicht einiger Staaten (u. a. Russland u. China) bereits heute durch zusehends bessere Raketenabwehrsysteme und immer zielgenauere konventionelle Präzisionswaffen (»prompt global strike« [Wikipedia 2006a] und zielgenaue Marschflugkörper) tangiert. Künftige AWS (in Form von UCAVs oder Marschflugkörpern mit KI-Suchköpfen) müssen vom jeweiligen Widersacher als eine potenzielle Bedrohung der strategischen Stabilität angesehen werden. So ist es vorstellbar, dass sehr potente AWS zukünftig z. B. als konventionelle Erstschlagwaffen zur Zerstörung gegnerischer Nuklearwaffenarsenale eingesetzt werden, mögliche Ziele (Raketensilos oder mit Nuklearwaffen bestückte U-Boote) selbstständig ausmachen, in deren Nähe unentdeckt verweilen und auf Befehl koordiniert diese Ziele angreifen und zerstören. AWS könnten auch selber als Trägerplattformen für Nuklearwaffen verwendet werden, mit der Intention, schneller, überraschender und koordinierter als bisherige Trägersysteme zuzuschlagen und vorhandene Verteidigungsmaßnahmen aushebeln zu können. Die Gefahr und die Angst vor einem möglicherweise vernichtenden Erstschlag würden durch eine solche Nutzung von AWS erheblich zunehmen und die strategische Stabilität infrage stellen. Dieses könnte weitere nukleare Abrüstung unmöglich machen und vielmehr eine Ära nuklearer Modernisierung oder sogar nuklearer Aufrüstung einläuten.

6.6 Rüstungsdynamiken

Rüstung ist im Wesentlichen ein Wechselspiel aus der Modernisierung des eigenen Waffenpotenzials (Effizienz- und Fähigkeitssteigerung) und der Reaktion auf potenzielle bzw. wahrgenommene äußere Bedrohungen (Auf- oder Abrüsten). Fühlen sich Länder bedroht oder streben eine militärische Hegemonie an, so kann es zu einem Wettrüsten oder einer Rüstungsspirale zwischen diesen Ländern kommen.

Die Entwicklung neuer Waffentechnologien verspricht eine Steigerung der militärischen Effizienz und Schlagkraft, und es werden häufig auch erweiterte militärische Einsatzszenarien möglich. Da die allermeisten Staaten danach streben, militärisch ihren potenziellen Kontrahenten mindestens ebenbürtig zu sein, führen neue Waffentechnologien häufig zu Rüstungsbestrebungen unter denjenigen Staaten, die über die entsprechenden ökonomischen und industriellen Voraussetzungen verfügen. Damit entsteht bei Kontrahenten ein Anreiz nachzuziehen und ebenfalls in die Rüstung und Entwicklung neuer Waffentechnologien zu investieren. Somit wird eine wechselseitige Rüstungsspirale angetrieben (technologisches Wettrüsten).

Wie bereits ausgeführt, schreiben die Großmächte autonomen Technologien einen langfristig hohen militärischen Stellenwert zu. Technologische Durchbrüche einer Partei können das bestehende Kräftegleichgewicht fundamental erschüttern. Ein solches Bedrohungsszenario dient verbreitet als Legitimation für eigene Entwicklungen und Anstrengungen auf diesem Feld. Zwischen den USA und China ist bereits heute eine beginnende Rüstungsdynamik im Feld zunehmend automatisierter UWS zu beobachten (Kap. 4.1.1). Auch Russland unternimmt konzentrierte Bestrebungen, um hinsichtlich heutiger UWS den bisherigen Vorsprung des Westens aufzuholen, und scheint auch zukünftig AWS entwickeln zu wollen. Indien und Südkorea wiederum sind ohnehin schon in regionalen Rüstungsspiralen mit ihren jeweiligen Nachbarn engagiert (Pakistan u. China bzw. Nordkorea), die Beschaffung von AWS könnte hier zusätzliche Rüstungsdynamiken in Gang setzen.

6.7 Unkontrollierte Weiterverbreitung

Zukünftige AWS werden auf technologischen Entwicklungen basieren, die ihren Ursprung größtenteils im zivilen Sektor haben. Die Forschung zur künstlichen Intelligenz – einschließlich maschinellem Lernen, Big-Data-Analysen – wird maßgeblich von großen Konzernen mit Blick auf private Konsumenten und den zivilen Wirtschaftssektor vorangetrieben. Bei einem großen Teil der Hardware zukünftiger AWS, vor allem aber bei der Software, handelt es sich überwiegend um Dual-Use-Technologien. Von dezidiert militärischen Bestand-

teilen – wie moderne Bewaffnung, Hochleistungsantriebe oder spezielle militärische Werkstoffe (zur Panzerung, Tarnung etc.) – einmal abgesehen, unterliegen die wesentlichen technologischen Grundlagen und das Know-how für eine zunehmende Automatisierung bzw. Autonomie militärischer Systeme keinen Beschränkungen bei der Weiterverbreitung und sind im Prinzip frei verfügbar.

Die Entwicklung und Produktion von leistungsstarken AWS wird trotz verfügbarer Dual-Use-Technologien allerdings erhebliche finanzielle und zeitliche Ressourcen erfordern. Andererseits könnten Staaten oder andere Akteure auch versuchen, fortschrittliche zivile Technologien in bewaffnete AWS zu überführen, ggf. unter Abstrichen bei der Leistungsfähigkeit (Nutzlast, Reichweite, Zuverlässigkeit etc.), aber dennoch mit weitgehend autonomen Funktionen. Auf diesem Weg könnte es auch nichtstaatlichen Akteuren gelingen, in den Besitz von kleineren AWS zu gelangen. Eine ähnliche Entwicklung ist heute bereits im Hinblick auf Drohnen zu beobachten (Kap. 4). Ob z. B. für Terroristen kleine bewaffnete kommerzielle AWS zukünftig attraktiv sein werden, ist derzeit noch nicht abzusehen, zumal ähnliche Wirkungen auch mit sehr viel einfacheren Mitteln und geringerem Aufwand erreichbar sind, wie Anschläge des IS in der jüngsten Zeit gezeigt haben.

Bereits heute existiert eine zunehmend schärfer werdende internationale Konkurrenz um den Export von UCAVs (besonders China und Israel sind hier sehr aktiv; Kap. 4). Auch die USA haben ihre bisher strengen Exportvorschriften in dieser Hinsicht jüngst gelockert (U.S. Department of State 2018). Der Wettbewerb um Rüstungsexporte könnte zukünftig auch die Weiterverbreitung von Systemen mit mehr und mehr autonomen Funktionen beschleunigen.

6.8 Technologische Risiken

Moderne Waffensysteme werden immer komplexer und deren Hardware, aber insbesondere die Software weisen vielfache Fehlerpotenziale bzw. Einfallstore für Systemmanipulationen (»hacking«) und Störungen von außen (»jamming«, »spoofing«) auf. Diese potenzielle Verwundbarkeit moderner Waffensysteme gilt generell für bemannte und unbemannte Systeme. Bemannte Systeme sind zumeist aber sehr viel ausfallsicherer konzipiert und weisen gerade bei lebenswichtigen Systemen oft Redundanzen auf. Sie haben darüber hinaus den Vorteil, über einen menschlichen Operateur zu verfügen, dem im Falle von Fehlfunktionen noch (manuelle) Eingriffsmöglichkeiten zur Verfügung stehen.

Die netzwerkzentrierte Kriegsführung setzt die Existenz und das reibungslose Funktionieren einer hochkomplexen Infrastruktur voraus, die eine hinreichende geografische Abdeckung, verlässliche Kommunikationsverbindungen und hohe Datendurchsatzraten aufweist. Diese Datennetze bieten potenziellen Gegnern Angriffsmöglichkeiten, sei es das Zerstören wichtiger Knotenpunkte

(Relaisstationen, Kommandobasen, Satelliten etc.), das Stören des Kommunikationsfrequenzspektrums als solches oder die Manipulation des Datenflusses.

Zunehmend automatisierte UWS oder zukünftige AWS zeichnen sich durch ihre immer komplexere Programmierung aus. Die Erfahrung zeigt, dass es unvermeidlich ist, dass diese Programme eine hohe Anzahl an Fehlern enthalten, deren Auswirkungen im Detail nicht abzusehen sind, Programmabstürze und unvorhersehbare Reaktionen eingeschlossen. Auch ist es unmöglich, alle Eventualitäten einer operationellen Umgebung vorherzusehen und entsprechend zu berücksichtigen. Falls zukünftige AWS die Fähigkeit zum eigenständigen Lernen haben werden, stellt sich die Frage, wie sichergestellt werden kann, dass nicht unerwünschtes Verhalten mit potenziell katastrophalen Konsequenzen erlernt wird.[72]

Hinzu kommt, dass jede Programmierung auch manipuliert werden kann (z. B. über Datenverbindungen von außen oder direkt am System) und Schadcodes sehr lange unentdeckt in einem solchen System verweilen können. So könnte im Ernstfall ohne Vorwarnung das Waffensystem z. B. gestört, manipuliert oder sogar durch den Gegner übernommen werden. Insgesamt bleibt festzuhalten, dass AWS zwar weitreichende Fähigkeiten aufweisen, diese aber mit einer erheblichen systemischen Verwundbarkeit verbunden ist.

72 Aus diesem Grund plädiert die Ethik-Kommission (2017) für automatisiertes und vernetztes Fahren dafür, selbstlernende Systeme nur für nichtsicherheitsrelevante Funktionen zuzulassen.

7 Humanitäres Völkerrecht und autonome Waffensysteme

Wie jedes Waffensystem sind auch AWS im Kontext der geltenden Normen des humanitären Völkerrechts zu betrachten. Das HVR soll im Falle eines internationalen bewaffneten Konflikts (»ius in bello«) den größtmöglichen Schutz von Zivilisten, nichtmilitärischen Gebäuden und Infrastrukturen sowie der natürlichen Umwelt gewährleisten und intendiert somit, eine Balance zwischen humanitären Erwägungen und militärischen Notwendigkeiten zu schaffen. Das HVR bezieht sich nicht primär auf technologische Systeme als solche, sondern zielt darauf ab, die Art und Umstände ihres Einsatzes einzuschränken.[73]

Im Zentrum des HVR stehen die vier Genfer Konventionen aus dem Jahr 1949 sowie zwei Zusatzprotokolle von 1977 (IKRK o. J.). Darin sind drei fundamentale Prinzipien des Waffeneinsatzes festgeschrieben:

- das Unterscheidungsgebot
- das Prinzip der Verhältnismäßigkeit
- das Vorsorgeprinzip[74]

Zusätzlich soll mittels der Martens'schen Klausel sichergestellt werden, dass Sachverhalte, die nicht explizit im HVR geregelt sind, mit dem Prinzip der Menschlichkeit und dem öffentlichen Gewissen in Einklang gebracht werden. Die Klausel wurde bereits in der Präambel der Haager Landkriegsordnung (1899) eingeführt und ist in abgewandelter Formulierung im ZP I (1977) der Genfer Konventionen (1949), Artikel 1 Absatz 2, zu finden: »In Fällen, die von diesem Protokoll oder anderen internationalen Übereinkünften nicht erfasst sind, verbleiben Zivilpersonen und Kombattanten unter dem Schutz und der Herrschaft der Grundsätze des Völkerrechts, wie sie sich aus feststehenden Gebräuchen, aus den Grundsätzen der Menschlichkeit und aus den Forderungen des öffentlichen Gewissens ergeben.«

Das Internationale Komitee vom Roten Kreuz (IKRK 2006, S. 17) legt diesen Artikel dahingehend aus, dass neue Waffensysteme den Prinzipien der Menschlichkeit und den Forderungen des öffentlichen Gewissens nicht grundlegend widersprechen dürfen.[75]

---

73 Siehe hierzu insbesondere die Artikel 35, 48, 51, 52 bis 57, ZP I (1977) der Genfer Konventionen (1949).

74 Obwohl einige Länder, u. a. auch die USA, das ZP I nicht ratifiziert haben, besteht weitreichende Übereinstimmung darin, dass die hier formulierten Grundprinzipien Eingang in das Völkergewohnheitsrecht gefunden haben und somit als allgemein verbindlich angesehen werden können (Schmitt 2012, S. 92 ff.).

75 Das IKRK spielt im HVR eine herausgehobene Rolle. Dies kommt u. a. darin zum Ausdruck, dass das IKRK in den Genfer Konventionen als einzige Institution explizit als Kontrollorgan genannt wird (siehe z. B. Wikipedia 2003d).

7.1 Prüfungspflicht (Artikel 36 ZP I)

Ob der Einsatz neu entwickelter Waffen oder Mittel und Methoden der Kriegsführung stets oder unter bestimmten Umständen durch das ZP I oder eine andere völkerrechtliche Bestimmung verboten sein könnte, muss bereits im Vorfeld, und zwar »bei Prüfung, Entwicklung, Beschaffung oder Einführung« geprüft und festgestellt werden. Hierzu verpflichten sich die Vertragsparteien in Artikel 36 ZP I (1977) der Genfer Konventionen (1949).[76] Wie dieser Prüfprozess im Detail auszusehen hat, ist im HVR jedoch nicht näher geregelt.[77]

Tatsächlich setzt derzeit nur eine kleine Anzahl von Ländern diese grundlegende Verpflichtung zur Waffenprüfung um. Das IKRK (2006) nennt Australien, Belgien, die Niederlande, Norwegen, Schweden, die Vereinigten Staaten, Frankreich, das Vereinigte Königreich und Deutschland. Dies sind alles Staaten mit einer modernen Verteidigungsindustrie. Die Prüfung wird von den Ländern sowohl prozedural als auch hinsichtlich der angewandten inhaltlichen Prüfkriterien auf sehr verschiedene Weise durchgeführt (IKRK 2006; McClelland 2003). In Deutschland wird sie im Rahmen des Beschaffungsverfahrens vom Referat Recht I 3 des Bundesverteidigungsministeriums durchgeführt und muss vor Beginn der Nutzungsphase abgeschlossen sein (BMVg 2016, S. 4). Dass auch die USA Waffenprüfungen durchführen, obwohl sie nicht Vertragspartei des ZP I sind, darf als Beleg dafür gelten, dass die in Artikel 36 ZP I formulierte Prüfverpflichtung als Teil des allgemein verbindlichen Völkergewohnheitsrechts anzusehen ist (Boulanin/Verbruggen 2017, S. 73; Nasu/McLaughlin 2014, S. 26).

Obwohl es keine Verpflichtung zur Offenlegung oder Veröffentlichung der Prüfungsergebnisse gibt, sind die Berichte in einigen Ländern öffentlich verfügbar – sofern keine für die nationale Sicherheit sensiblen Informationen enthalten sind –, z. B. in den USA und in Schweden (IKRK 2006, S. 27). In Deutschland werden die Berichte nicht veröffentlicht. Als Grund gibt die Bundesregierung zu wahrende Geheimschutzverpflichtungen, Betriebsgeheimnisse und immaterielle Rechte Dritter an (Deutscher Bundestag 2016, S. 33 f.).

Heutige UWS werden im Rahmen völkerrechtlicher Betrachtungen meist den bisherigen Waffensystemen gleichgestellt, da ihr Einsatz zurzeit überwiegend ferngesteuert ist und immer ein menschlicher Operator die Einsatzverantwortung hat (TAB 2011, S. 199 ff.; WD 2012). Andererseits können unbemannte

76 Artikel 36 ZP I (1977) der Genfer Konventionen (1949) im Original: »In the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party.«

77 Für weitere Interpretation/Hintergrundinformationen zum HVR vgl. BMVg (1992).

Systeme auch als reine Plattformen dienen. Als solche (d. h., wenn sie keine Wirkmittel oder Nutzlasten tragen, die sich auf die eigenen offensiven oder defensiven Fähigkeiten auswirken) würden sie per se keine Waffen, Mittel oder Methoden der Kriegsführung darstellen. Für diese läge eine Prüfungspflicht gemäß Artikel 36 ZP I demzufolge nicht vor (Deutscher Bundestag 2016, S. 34).

Zukünftige AWS müssen den Überprüfungen nach Artikel 36 ZP I erst noch unterzogen werden. Hierfür müsste die Konformität mit den Prinzipien des HVR in allen intendierten bzw. erwarteten Einsatzszenarien nachgewiesen werden. Eine notwendige Voraussetzung dafür ist, dass das Verhalten des AWS sehr hohen Anforderungen an Vorhersagbarkeit und Verlässlichkeit genügt. Test und Verifikation dieser Eigenschaft stellen aufgrund der speziellen Eigenschaften von AWS eine besondere, bisher ungelöste Herausforderung dar (Davison 2017, S. 9 f.).

7.2 AWS im Lichte der Prinzipien des HVR

Zukünftige AWS werden sich gegenüber jedem bisherigen Waffensystem, inklusive der heutigen unbemannten Waffensysteme, dadurch auszeichnen, dass sie in sich dynamisch verändernden, nicht vorhersehbaren Umfeldern autonom agieren können, bis zu einem gewissen Grad also selber *Handlungsentscheidungen* treffen müssen, ohne dabei einer direkten menschlichen Steuerung und Kontrolle zu unterliegen. Um die zentrale Frage zu beantworten, ob ein Einsatz von AWS völkerrechtskonform sein kann, muss zunächst untersucht werden, ob bzw. unter welchen Voraussetzungen die grundlegenden Prinzipien des HVR von AWS eingehalten werden können.

Die Natur aktueller Konflikte erschwert dabei die Aufgabe, jederzeit den Bestimmungen des HVR Rechnung zu tragen. Häufig finden diese nicht direkt zwischen Staaten und ohne klar definierte geografische Frontlinie statt. Gefechte nahe oder inmitten ziviler Gebiete mit Kämpfern, die sich absichtlich möglichst wenig von Zivilisten unterscheiden, sind mehr und mehr die Regel.

Unterscheidungsgebot

Das HVR gebietet, dass Kampfhandlungen sich nur gegen militärische Ziele – Kombattanten und militärische Objekte – richten dürfen. Die Zivilbevölkerung und zivile Objekte sind zu schützen und zu schonen (Artikel 48 bis 52 ZP I). Insbesondere verbietet Artikel 51 Absatz 2 ZP I jegliche Angriffe sowohl auf die Zivilbevölkerung generell als auch auf einzelne Zivilisten. Unterschiedslose Angriffe, die nicht gegen ein bestimmtes militärisches Ziel gerichtet werden bzw. bei denen Kampfmethoden und -mittel eingesetzt werden, die nicht gegen ein bestimmtes militärisches Ziel gerichtet werden können, sind gemäß Artikel 51 (4) ZP I verboten. Darüber hinaus dürfen gegnerische Kräfte nicht angegriffen

werden, die außer Gefecht (»hors de combat«) sind. Darunter fallen u. a. Soldaten, die ihre Intention angezeigt haben, sich zu ergeben, und solche, die aufgrund einer Verletzung, Bewusstlosigkeit oder Ähnlichem nicht in der Lage sind, sich zu verteidigen (Artikel 41 ZP I).

Ein AWS, das völkerrechtskonform eingesetzt werden soll, müsste also legitime militärische Ziele zuverlässig und mit hoher Trefferquote unter realen Gefechtsbedingungen identifizieren können, d. h. bei ungünstigen Lichtverhältnissen (Tag/Nacht), Wetter- und Umweltbedingungen, sich schnell ändernden Gefechtslagen, extremem Zeitdruck sowie trotz möglicher Gegenmaßnahmen des Gegners (einschließlich Tarnen, Täuschen, Blenden von Sensoren).

Da auch Menschen bei dieser komplexen Aufgabe regelmäßig Fehler unterlaufen, wird man sicherlich bei AWS in der Praxis auch keine Unfehlbarkeit bei der Identifikation legitimer Ziele erwarten können. Welche Fehlerquote dabei im Sinne der Einhaltung der völkerrechtlichen Normen als tolerabel angesehen wird, ist derzeit noch eine offene Frage. Wie im Kapitel 8.1.2 ausgeführt wird, vertritt Arkin (2015, S. 46) die Auffassung, dass AWS diese Aufgabe »besser als ein Mensch« erfüllen könnten.

Allerdings darf bezweifelt werden, ob dies als Maßstab tatsächlich trägt, denn erstens spielt nicht nur die Häufigkeit, sondern auch die Art der Fehler eine wichtige Rolle für die Bewertung ihrer Akzeptabilität. Wie in Kapitel 3.3 beschrieben, können beispielsweise heutige Verfahren der Bilderkennung bestimmte Aufgaben mit hoher Trefferquote bewältigen. Gleichzeitig können jedoch krasse Fehler auftreten, die der menschlichen Intuition diametral entgegenlaufen bzw. die einem Menschen niemals unterlaufen würden (in Kap. 3.3.3 wird das Beispiel genannt, dass von zwei Bildern, die sich lediglich in einem einzigen Pixel unterscheiden, eines korrekt erkannt wird und das andere nicht).

Zweitens ist unklar, wie »besser als ein Mensch« konkret zu verstehen ist. Da AWS ganz eigene, besondere Eigenschaften aufweisen, werden sie voraussichtlich auch in Einsatzszenarien Verwendung finden, die unter Einbeziehung menschlicher Bediener gar nicht in Betracht kämen. Wäre z. B. ein Angriff bei sehr schlechten Sichtbedingungen durch dichten Nebel legitim, bei dem ein AWS mittels seiner technischen Vorrichtungen nur gelegentlich ein militärisches Ziel korrekt identifizieren würde, nur weil ein Mensch hier noch schlechter abschneiden würde? Oder ist als Vergleichsmaßstab ein menschlicher Operator heranzuziehen, dem sämtliche Sensordaten und Hilfssysteme nach dem technologischen State of the Art zur Verfügung stehen? Aber wäre dieses technologisch-menschliche Hybridsystem nicht einem rein technischen AWS oftmals überlegen? Und wäre in zeitkritischen Situationen, in denen die menschliche Reaktionsfähigkeit schlicht überfordert wäre, der Einsatz jeglicher militärischer Gewalt durch AWS statthaft, wenn diese auch nur eine rudimentäre Zieldiskriminierung leisten könnten?

Die eigentliche Problematik ist jedoch anders gelagert, denn zur Entscheidung, ob ein Objekt oder eine Person ein legitimes militärisches Ziel darstellt, reicht deren zuverlässige Identifizierung bei Weitem nicht aus. Hierfür ist ein umfassenderes Lagebild erforderlich sowie die Einschätzung von Verhaltensweisen und letzten Endes der Intentionen des Gegners. So könnte zwar ein Kriegsschiff relativ problemlos von einer Zielerkennungssoftware identifiziert werden. Aber einem erfahrenen Seemann würde dabei unter Umständen auffallen, dass die Lage des Rumpfes relativ zu Wind und Strömung sowie der aus dem Maschinenraum austretende Rauch dafür sprechen, dass das Schiff sich in Seenot befindet und daher »hors de combat« ist. Wäre eine Software zur Einbeziehung derart *weicher* Kontextfaktoren und abstrakter Abwägung in der Lage? Auch ist schwer vorstellbar, auf welche Weise sich ein verwundeter Soldat einem AWS ergeben könnte. Dies würde die korrekte Deutung subtiler – auch emotionaler – Signale sowie verbaler und nonverbaler Kommunikation erfordern.

Aufgrund dieser Überlegungen sind Zweifel angebracht, ob softwarebasierte Systeme wie AWS (ausgenommen hypothetische mit menschenähnlicher, starker künstlicher Intelligenz ausgestattete, Sparrow 2016, S. 99) in absehbarer Zeit in der Lage sein werden, dem Unterscheidungsgebot des HVR Genüge zu leisten. Einige Kritiker gehen noch weiter und bestehen darauf, dass dies letztlich nur von Menschen und niemals von technologischen Systemen zu leisten ist. Noel Sharkey (2012a) fasst dies wie folgt zusammen: »Menschen verstehen einander auf eine Weise, die Maschinen nicht möglich ist. Signale können sehr subtil sein und es gibt eine unendliche Anzahl an Umständen unter denen der Einsatz tödlicher Gewalt unangemessen ist.«[78]

Prinzip der Verhältnismäßigkeit

Das Unterscheidungsgebot stellt zwar hohe Anforderungen an militärische Angriffe, allerdings bedeutet dies nicht, dass generell von Angriffen abgesehen werden muss, wenn dabei Zivilisten und/oder zivile Einrichtungen in Mitleidenschaft gezogen werden könnten. Derartige Kollateralschäden dürfen in Kauf genommen werden, allerdings nur in einem Umfang, der nicht exzessiv ist in Relation zu dem konkreten und direkten militärischen Nutzen der Operation. Dies ist das Prinzip der Verhältnismäßigkeit des HVR.[79]

78 Übersetzung durch das TAB; im Original: »Humans understand one another in a way that machines cannot. Cues can be very subtle, and there are an infinite number of circumstances where lethal force is inappropriate.«

79 Artikel 51 Absatz 5b ZP I im Original: »Among others, the following types of attacks are to be considered as indiscriminate: [...] an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated.«

Diese Norm anzuwenden ist eine der schwierigsten Aufgaben im Kontext des HVR (Schmitt 2012, S. 190). Zunächst einmal müssen höchst unterschiedliche, im Kern inkommensurable Kategorien – militärische und humanitäre – gegeneinander abgewogen werden. Wie bestimmt man beispielsweise den Wert eines Bombers, Kriegsschiffes, Panzers oder eines Aussichtspostens relativ zur Zahl der dafür geopferten zivilen Menschenleben? (Schmitt 2012, S. 139)[80] Hinzu kommt, dass die Bewertungsgrundlage während des Kriegsgeschehens durch militärische und/oder humanitäre Ereignisse einem ständigen Wandel ausgesetzt ist. Kommando- und Kommunikationsstrukturen des Gegners zu zerstören, kann am Anfang eines bewaffneten Konflikts von entscheidender militärischer Bedeutung sein. In einer Situation, wo sich Bemühungen abzeichnen, die Auseinandersetzung auf dem Verhandlungsweg zu beenden, wäre dies dagegen in höchstem Maße kontraproduktiv (Schmitt 2012, S. 139). Darüber hinaus existieren keine objektiven und global einheitlichen Standards: Die Wertebasis, auf deren Grundlage ein Kommandeur entscheidet, welches Ausmaß an menschlichem Leid in Bezug auf ein bestimmtes militärisches Ziel akzeptabel erscheint, hängt entscheidend von dessen kultureller und sozialer Prägung ab.

Dass die Anwendung der Norm nicht, wie oft fälschlicherweise dargestellt, einem präzisen Wägeprozess entspricht, wo bereits ein geringes Überwiegen der einen oder anderen Seite den Ausschlag gibt, sondern dass lediglich geprüft werden muss, ob der zu erwartende Kollateralschaden bezogen auf den militärischen Nutzen *exzessiv* ist, d. h. in keiner vernünftigen Relation steht, erleichtert die Aufgabe nicht wesentlich. Zwar wird damit die kaum je erfüllbare Anforderung beseitigt, den militärischen Vorteil sowie den Kollateralschaden präzise messen bzw. bestimmen zu müssen. Allerdings wird gefordert, dass sämtliche relevanten Umstände einzubeziehen sind und das Resultat der Abwägung eben *vernünftig* ist. Der Internationale Strafgerichtshof für das ehemalige Jugoslawien hat dies 2003 so konkretisiert: Hätte »eine durchschnittlich informierte Person (›a reasonably well-informed person‹) unter den zum fraglichen Zeitpunkt vorherrschenden Umständen und unter vernünftiger Berücksichtigung der verfügbaren Informationen [...] erwarten können, dass es durch den Angriff zu einer exzessiven Anzahl ziviler Opfer kommen würde« (Geiß 2015, S. 16 ff.)?

Deswegen bestehen begründete Zweifel, ob softwaregestützte Systeme wie AWS in der Lage sein können, die erforderlichen Abwägungen zur Verhältnismäßigkeit eines Angriffs zufriedenstellend und zuverlässig durchzuführen. Der Umfang von Kontext- und Weltwissen sowie die Fähigkeit, die Aktionen von Menschen zu interpretieren und zu verstehen, die hierfür erforderlich sind, sind auf jeden Fall auf absehbare Zeit nicht in ihrer Reichweite. Analog wie beim Unterscheidungsgebot müsste auch hierfür nach Sparrow (2016, S. 99 ff.) starke künstliche Intelligenz vorausgesetzt werden.

80 Sharkey (2012b, S. 789) nennt dies das »hard proportionality problem«.

Eine gegensätzliche Position vertritt Arkin (2008, S. 126) (Kap. 6.1), der computerbasierten Systemen mit Verweis auf ihre überlegenen sensorischen und Simulationsfähigkeiten zutraut, die Konsequenzen eines Waffeneinsatzes auf ein bestimmtes Ziel effektiver bestimmen zu können als jeder Mensch. In der Tat existieren für diesen Zweck bereits Softwaretools. So setzen beispielsweise die Streitkräfte der USA das Programm »Bugsplat« ein, um dasjenige Wirkmittel auszuwählen und so zu steuern, dass ein möglichst geringer Kollateralschaden verursacht wird. Allerdings wird damit keineswegs die gesamte Breite der Abwägungen abgedeckt, die vom Verhältnismäßigkeitsgebot gefordert sind, sondern nur der Teil, den Sharkey (2012b, S. 789 f.) als das »easy proportionality problem« bezeichnet. Dieses ist erheblich leichter durch Software zu lösen als das »hard proportionality problem«, bei dem qualitative und subjektive Entscheidungen eine wesentlich dominantere Rolle spielen. Somit bleibt Arkin letztlich eine Antwort auf die Frage schuldig, ob er das »hard proportionality problem« für durch Software lösbar hält.

Vorsorgeprinzip

Nachdem ein militärisches Ziel identifiziert wurde und dieses nach Abwägung der Verhältnismäßigkeit als legitim angesehen wird, ist als letzter Schritt vor einem Angriff dem Vorsorgeprinzip Rechnung zu tragen. Dieses verpflichtet den Angreifer, dasjenige Mittel zu wählen, das der Zivilbevölkerung bzw. zivilen Objekten den geringsten Schaden zufügt (Artikel 57 Absatz 2aii ZP I). Darüber hinaus besteht die Verpflichtung, die Zivilbevölkerung vor Angriffen zu warnen, die sie tangieren können, soweit dem kein gewichtiger Grund entgegensteht (Artikel 57 Absatz 2c ZP I).

Der Maßstab dieser Verpflichtung ist subjektiv, da die konkret in der Situation verfügbaren Optionen abgewogen werden müssen. Streitkräfte, die hochpräzise Wirkmittel zur Verfügung haben, wären somit einem höheren Standard unterworfen als schlechter ausgerüstete Gegner ohne diese Möglichkeiten. Es ist auch nicht auszuschließen, dass in einer Gefechtssituation nur eine einzige Option zur Verfügung steht und somit eine Abwägung gar nicht sinnvoll durchgeführt werden kann. Eine explizite Verpflichtung, durch Entwicklung und Einsatz neuer Technologien Optionen zu schaffen, die möglichst wenige Kollateralschäden verursachen, besteht nicht (Schmitt 2012, S. 159 ff.). Dessen ungeachtet wird dies insbesondere in Staaten mit hohem Verantwortungsbewusstsein oft als Argument für die Entwicklung von immer präziseren Waffen und Methoden der Kriegsführung angeführt.

Die Abwägungen gemäß dem Vorsorgeprinzip ähneln dem oben angesprochenen »easy proportionality problem« und wären von den hier untersuchten Prinzipien des HVR wohl am ehesten durch AWS erfüllbar, die hier ihre

Vorteile ausspielen könnten, die im voranstehenden Kapitel zum Unterscheidungsgebot aufgeführt worden sind.

Allerdings ist diese Überlegung eher theoretischer Natur, da die hier zum Zwecke der Analyse vorgenommene Trennung in drei Abwägungsschritte zu Unterscheidungsgebot, Verhältnismäßigkeit und Vorsorgeprinzip in der Praxis nicht aufrechterhalten werden kann. Im Verlauf der Planung bis zur tatsächlichen Ausführung eines Angriffs können sich wesentliche Umstände jederzeit auf unvorhersehbare Weise ändern, die dessen Konformität mit den völkerrechtlichen Anforderungen infrage stellen. In einem solchen Fall müssten Angriffe abgebrochen werden können. Daher ist eine integrierte Bewertung aller drei Aspekte unmittelbar vor der Auslösung eines Angriffs unerlässlich.

Staatenverantwortlichkeit

Die fundamental wichtige Frage, wer die Verantwortung trägt, wenn ein AWS einen völkerrechtswidrigen Angriff durchführt, wird kontrovers diskutiert. Oft wird hier eine Verantwortungslücke diagnostiziert (Sparrow 2007). Die Debatte darüber wird in Kapitel 8.3 ausführlich dargestellt. An dieser Stelle soll sie lediglich aus der Perspektive der Staatenverantwortlichkeit im Kontext des HVR beleuchtet werden.

Allgemein gilt, dass Konfliktparteien für jegliche Handlungen verantwortlich sind, die von *Personen* begangen werden, die Teil ihrer Streitkräfte sind (Artikel 91 ZP I).[81] Da AWS keine Personen, sondern Maschinen sind, könnte man sich auf den simplen Standpunkt stellen, dass für von AWS begangene Handlungen der zugehörige Staat demzufolge nicht verantwortlich ist.

Diese Haltung ist allerdings nicht überzeugend, denn das Ingangsetzen eines AWS durch einen menschlichen Bediener würde zweifellos eine Handlung darstellen, für die der zugehörige Staat in letzter Konsequenz die Verantwortung zu tragen hätte.[82] Dass die Folgen dieser Handlung nicht vollständig überschaubar sind, da das Verhalten eines AWS dem Prinzip nach zumindest punktuell unvorhersehbar ist, entlastet den menschlichen Verantwortungsträger nicht. Denn »wenn tatsächlich die Beziehung zwischen dem menschlichen Handeln und der Wirkung, die über autonome Waffensysteme erfolgt, sich so weit erstreckt, dass eine Verantwortlichkeitsbeziehung völlig willkürlich wirkt, dann ist die ethische Frage wohl weniger die, ob hier eine Verantwortlichkeitslücke entsteht, sondern vielmehr die, ob es verantwortbar ist, einen Prozess in Gang zu setzen, der sich offenkundig der Kontrolle gänzlich entzieht« (Koch/Rinke 2017, S. 159). Somit wäre eine durch ein AWS begangene Verletzung des

81 Artikel 91 ZP I im Original: »A Party [...] shall be responsible for all acts committed by persons forming part of its armed forces.«

82 Nach Maßgabe der Artikel 4 bzw. 86 Absatz 2 ZP I, die die Verantwortung des Staates für Handlungen seiner Organe und die Verantwortung eines Kommandierenden für die Handlungen eines Untergebenen regeln.

Völkerrechts dem Staat zuzurechnen, dessen Streitkräfte das Gerät eingesetzt haben (AIV/CAVV 2015, S. 27 ff.). Ob diese Argumentation im internationalen Rahmen greift, ist derzeit noch strittig.

Ebenso verhält es sich mit der Frage, ob es für die Verantwortlichkeit und letzten Endes die Haftbarkeit des Staates für Schäden darauf ankommt, dass die unmittelbare Handlung vorsätzlich oder zumindest fahrlässig begangen wurde.[83] Wenn dies bejaht wird, ergäben sich insbesondere im Falle der Fahrlässigkeit Schwierigkeiten, die analog bei der strafrechtlichen Verantwortlichkeit von einzelnen Personen greifen: Bei Fahrlässigkeitsdelikten ist nämlich Vorhersehbarkeit eine Voraussetzung für die Strafbarkeit. Wenn diese aber aus den genannten Gründen, dass AWS eben unvorhersehbar reagieren können, nicht gegeben ist, besteht die Gefahr, dass sich jedes Fehlverhalten von autonomen Systemen letztlich wie höhere Gewalt darstellt, also wie ein Ereignis, das durch Menschenhand nicht zu verhindern war.

Wie hier Unfälle oder Fehlfunktionen des Geräts aufgrund eines Defektes (die keine Verletzung des HVR darstellen würden, selbst wenn dabei Zivilisten zu Schaden kämen; CCW GGE 2017b, Punkt 30) von Fehlverhalten im Zuge spezifikationsgemäßen Funktionierens (das hochproblematisch sein kann) unterschieden werden könnten, ist völlig unklar.

Um diese Problematik zu umgehen, hat das IKRK (1987, RN 3661) in seinem Kommentar zu Artikel 91 ZP I die Möglichkeit ins Spiel gebracht, auf eine verschuldensunabhängige Gefährdungshaftung (»no fault or strict liability«) zurückzugreifen.[84] Dies ist ein probates Mittel, um das Gefahrenpotenzial bestimmter (im Prinzip erwünschter) Handlungen oder Technologien einzudämmen, und findet in Deutschland z. B. im Straßenverkehr, beim Betrieb von Kernkraftwerken oder bei der Produkthaftung Anwendung.

Als Vorbild kann beispielsweise das 1972 geschlossene Übereinkommen über die völkerrechtliche Haftung für Schäden durch Weltraumgegenstände dienen. Dort heißt es: »Ein Startstaat haftet unbedingt für die Leistung von Schadensersatz wegen eines von seinem Weltraumgegenstand auf der Erdoberfläche oder an Luftfahrzeugen im Flug verursachten Schadens«.

Da AWS technologische Risiken mit sich bringen, die heute im Einzelnen nicht überschaubar sind, würde sich die explizite Einführung einer strikten

83 Die nachstehenden Ausführungen fassen die Analysen von Geiß (2015, S. 21 f.) zu diesem Thema zusammen.

84 Gemäß der verschuldensunabhängigen Gefährdungshaftung (»strict liability« in der englischen Rechtsterminologie) kann eine Person für einen Sachverhalt verantwortlich sein, den sie kausal nicht einmal beeinflussen konnte – oder zumindest nicht unmittelbar beeinflussen konnte (dazu und zum Folgenden Koch/Rinke 2017, S. 159). Ein Verschulden im strengen Sinne liegt also nicht vor. In manchen Fällen widerspricht die Gefährdungshaftung unseren Intuitionen, aber in manchen Fällen scheint sie der einzige Weg zu sein, rechtliche Verantwortlichkeit zu sichern. Die Person, die absehbar nach der Gefährdungshaftung verantwortlich gemacht würde, steht somit unter großem Druck, im Vorfeld dafür zu sorgen, dass keine Fehler geschehen.

Gefährdungshaftung im Zuge eines internationalen Abkommens anbieten. Gegebenenfalls könnte es für einzelne Staaten auch in Betracht kommen, als vertrauensbildende Maßnahme die Übernahme einer Gefährdungshaftung unilateral zu erklären.

Kasten 7.1 »Boxed autonomy«

Aus den vorstehenden Ausführungen wird deutlich, dass erhebliche Zweifel angebracht sind, ob AWS den vom HVR gestellten Anforderungen, aber auch ganz allgemein den höchsten Standards an Zuverlässigkeit und Sicherheit unter allen möglichen operationellen und Umweltbedingungen genügen können. So schlussfolgern beispielsweise zwei Beratungsgremien der niederländischen Regierung in einem gemeinsamen Bericht: »It is clear from the above that humans will remain responsible for making assessments regarding distinction, proportionality and precaution for at least the next 10 years. The deployment of autonomous weapons will only be permitted in cases where it is almost certain that IHL [International Humanitarian Law] will not be violated« (AIV und CAVV 2015, S. 26).

Zurzeit wird in Fachkreisen unter dem Schlagwort »boxed autonomy« intensiv diskutiert, ob eine strikte räumliche und zeitliche Beschränkung des Einsatzgebietes eines AWS die zuvor ausgeführten Kritikpunkte nicht zumindest deutlich entschärfen könnte (iPRAW 2017a; Sparrow 2016, S. 100 ff.). Die Bewertung des Kontexts und die Entscheidung, ob ein Angriff dem HVR genügt, würden in Bezug auf ein begrenztes Operationsgebiet und einen bestimmten Zeitraum quasi auf Vorrat von einem menschlichen Kommandeur getroffen. Das AWS könnte sodann in diesem vorgegebenen Rahmen agieren. Dies könnte vor allem für bestimmte Operationsgebiete infrage kommen, bei denen nicht mit der Anwesenheit von Zivilisten zu rechnen ist: z. B. auf hoher See, tief unter Wasser, im Luftraum von Flugverbotszonen oder im Weltraum. Ob es ausreicht, Zivilisten vor einem Angriff lediglich zu warnen und genügend Zeit zum Abziehen zu gewähren, ist dagegen umstritten (Sparrow 2016, S. 103).

Beispielsweise kann man die Funktionsweise des bei der Bundeswehr gängigen Flugabwehrsystems »MANTIS« im automatischen Modus als »boxed autonomy« auffassen (Kap. 4.1.2). Der Operationsraum erstreckt sich hier auf die Reichweite der Sensoren, einen Radius von etwa 20 km, und die Zeit kann vom menschlichen Bediener durch An- und Abschalten des automatischen Modus bestimmt werden. Ein anderes Beispiel sind Operationen auf rein militärisch genutztem Gebiet wie etwa innerhalb eines Hauptquartiers. Diese sind vergleichbar mit dem Artilleriebeschuss eines als militärisches Ziel ausgewiesenen Gebiets (Delegation der USA zur CCW GGE 2018j, S. 3).

Eine ungeklärte Frage ist allerdings, wie weit das Gebiet (in räumlicher und zeitlicher Ausdehnung) denn sein dürfte, um erstens sicher zu sein, dass das AWS sich in der vorher bestimmten Weise verhält (d. h. nicht »aus dem Ruder läuft«), und zweitens, dass keine Veränderungen des Kriegsgeschehens bzw. im Operationsgebiet den Angriff obsolet machen. Was wäre beispielsweise, wenn in unvorhergesehener Weise doch Zivilisten im Operationsgebiet auftauchen oder wenn das anvisierte Ziel sich ergeben will? Hier würde sich ein erheblicher Graubereich auftun. Hinzu kommen Zweifel, wie realistisch die Beschränkung auf einen Boxed-Autonomy-Betriebsmodus angesichts heute dominierender Konfliktformen wäre. Gerade in komplexen und unübersichtlichen Situationen sind menschliche Soldaten ja besonders gefährdet, wodurch ein sehr hoher Anreiz besteht, sie durch AWS zu ersetzen (Geiß 2015, S. 17).

8 Ethische Fragestellungen im Kontext autonomer Waffensysteme

Obwohl noch gar nicht abzusehen ist, wann autonome Waffensysteme einsatzfähig sein werden, wird bereits seit mindestens 10 Jahren intensiv über ihre ethischen Implikationen diskutiert – und das nicht nur in Fachkreisen, sondern zunehmend auch in der Öffentlichkeit.[85] Die Debatte schließt dabei zum Teil an normative Fragen an, die sich in ganz ähnlicher Weise auch in zivilen Anwendungskontexten stellen (wie etwa der Pflege; TAB 2016, S. 146 ff.), die ebenfalls von Autonomisierungstendenzen betroffen sind: Gibt es Kernbereiche des Menschlichen, die es vor maschinellen Zugriffen zu schützen gilt? Wer ist für Schäden verantwortlich, die von autonom agierenden Robotern verursacht werden? Der besondere Einsatzzweck autonomer Waffensysteme, nämlich die militärische Gewaltanwendung, bringt es allerdings mit sich, dass sich die ethischen Herausforderungen zunehmender maschineller Autonomie auf eine Weise zuspitzen, wie es im zivilen Bereich nicht der Fall ist. Der Einsatz militärischer Kampfroboter stellt gewissermaßen ein Extremszenario der Entgrenzung von Mensch und Maschine dar, das eine Frage von existenzieller Tragweite aufwirft: Sollen Maschinen über Leben oder Tod von Menschen entscheiden dürfen?

Klar ist, dass sich mit dem Auftauchen autonomer Waffensysteme nicht nur eine »echte Revolution und [ein] Paradigmenwechsel im Bereich der Militärtechnologie« (Geiß 2015, S. 3) ankündigt, sondern grundsätzliche normative Fragen zu den Grenzen maschineller Autonomie aufgeworfen werden. Ethische Argumente und Erwägungen sind deshalb in der AWS-Debatte von besonderem Gewicht, auch und gerade in den politischen Auseinandersetzungen, die derzeit auf internationaler Ebene über ein Verbot solcher Waffensysteme geführt werden. Es ist in diesem Zusammenhang wichtig, darauf hinzuweisen, dass nicht die technisch vermittelte Tötung von Menschen das ethisch Brisante an AWS ist – dieser Aspekt ist selbstverständlicher Bestandteil moderner Kriegsführung. Kritisch ist vielmehr der Umstand, dass Waffensysteme am Horizont auftauchen, die menschlicher Kontrolle weitgehend entzogen sind, also autonom agieren, und zwar insbesondere in Bezug auf Zielauswahl sowie den Einsatz letaler Gewalt.

Im Folgenden wird, basierend auf dem Gutachten von Koch und Rinke (2017), die weitverzweigte ethische Debatte über AWS dargestellt. Dabei ist es alleine schon aus Platzgründen nicht möglich, alle Erwägungen und Überlegungen umfassend abzuhandeln. Stattdessen werden drei wichtige Diskussions-

85 So haben Tausende Forscher aus den Bereichen KI und Robotik einen offenen Brief aus dem Jahr 2015 unterschrieben, in dem ein Verbot von autonomen Waffensystemen gefordert (ca. 4.502 aus KI/Robotik und 26.215 andere; Stand Oktober 2020; FLI o. J.a).

stränge herausgegriffen, die sich aus unterschiedlichen Blickwinkeln mit der Frage befassen, ob und ggf. inwiefern die eigentliche Bestimmung von AWS, nämlich die autonome Anwendung tödlicher Gewalt, moralisch zulässig erscheint. In einem ersten Schritt werden einflussreiche Argumente betrachtet, die sich mit den möglichen Auswirkungen auf die Ethik der Kriegsführung und insbesondere den humanitären Folgen beschäftigen. Anschließend geht es um die sehr grundsätzliche Frage, ob es überhaupt mit der Menschenwürde zu vereinbaren ist, die Entscheidung über Leben und Tod an Maschinen zu übertragen. Schließlich stehen Befürchtungen im Fokus, der Einsatz von autonomer Waffentechnologie schaffe eine Verantwortungslücke, die mit rechtlichen sowie moralischen Rechenschaftspflichten nicht in Einklang zu bringen ist.

8.1 AWS und die Ethik des Krieges

Im Zentrum der ethischen Debatte über AWS stehen Fragen, die die Implikationen dieser neuen Waffentechnologie für die Ethik des Krieges betreffen. Eine der wichtigsten theoretischen Bezugspunkte dabei ist die sogenannte Lehre vom gerechten Krieg,[86] die antike Wurzeln hat und im Laufe der abendländischen Geschichte (wesentliche Impulse lieferte u. a. Thomas von Aquin) zu einem detaillierten, wenn auch keineswegs einheitlichen Regelwerk ausgearbeitet wurde, das sich mit den legitimen und illegitimen Formen zwischenstaatlicher Gewaltanwendung befasst (dazu und zum Folgenden Koch/Rinke 2017, S. 29 u. 32).[87] Ziel ist es, Kriterien zu finden, unter denen die Anwendung militärischer Gewalt als Mittel der Konfliktlösung *im äußersten Fall* gerechtfertigt werden kann.[88] Die Stoßrichtung ist somit streng genommen weniger eine kriegsethische und mehr eine friedensethische: Das Bestreben ist die Einschränkung militärischer Gewalt und nicht ihre Legitimierung. Wesentliche Postulate der Lehre vom gerechten Krieg haben deshalb, wie unten zu sehen sein wird, ihren Niederschlag im humanitären Völkerrecht gefunden. Die diesbezügliche ethische Debatte ist aus diesem Grund sehr eng mit der völkerrechtlichen verknüpft und kaum trennscharf von dieser abgrenzbar.

86 Die Lehre vom gerechten Krieg dominiert nahezu unangefochten die theoretische Debatte über die ethisch gerechtfertigte Anwendung militärischer Gewalt, die stark vom englischen Raum bestimmt ist (Koch/Rinke 2017, S. 30). Andere Denkschulen, etwa die Lehre vom gerechten Frieden, wie sie die beiden deutschen Großkirchen in ihren Lehrtexten vertreten (Hoppe/Werkner 2017), sind allenfalls von marginaler Bedeutung.

87 Traditionell gehören zum Gegenstandsbereich der Lehre vom gerechten Krieg bewaffnete Konflikte, die sich zwischen zwei souveränen Staaten abspielen. Andere Formen militärischer Gewalt, Bürgerkriege etwa, nehmen hingegen eher eine Randstellung ein (Frank 2009, S. 734).

88 Theoretische Gegenpositionen sind der Bellizismus, der kriegerische Gewalt grundsätzlich befürwortet, sowie der Pazifismus, der sie a priori verurteilt.

8.1.1 Die Lehre vom gerechten Krieg

Die Lehre vom gerechten Krieg besteht aus mindestens drei Teilen, die sich auf die hauptsächlichen Aspekte einer kriegerischen Auseinandersetzung beziehen: das Recht zum Krieg (»ius ad bellum«), das Recht im Krieg (»ius in bello«) sowie das Recht nach dem Krieg (»ius post bellum«). Diese Teilaspekte sind wiederum mit jeweils unterschiedlichen, wenn auch eng miteinander verflochtenen ethischen Fragestellungen verknüpft, die sich mit Blick auf AWS folgendermaßen grob charakterisieren lassen:

1. Beim »ius ad bellum« geht es um die Frage, wann es gerechtfertigt ist, einen Krieg zu beginnen. In der Debatte wurden zentrale Anforderungen formuliert wie das Vorliegen eines legitimen, *gerechten* Kriegsgrundes sowie das Scheitern anderweitiger Möglichkeiten der Konfliktlösung. Dass Krieg nur als Ultima Ratio zulässig ist, wird im Zusammenhang mit AWS besonders kontrovers diskutiert. Befürchtet wird, dass die Hemmschwelle zur Gewaltanwendung sinken und es zu einer »Normalisierung des Krieges« (Franke/Leveringhaus 2015) kommen kann, sollten mit der Verfügbarkeit von AWS Kriege risikoloser sein und zu geringeren gesellschaftlichen Kosten (vor allem zu weniger toten und verletzten Soldaten) führen (Kap. 6.1; Geiß 2015, S. 13 f.; Koch/Rinke 2017, S. 48 ff.).
2. Das »ius in bello« beschäftigt sich mit den Anforderungen an eine ethische Kriegsführung. Im Fokus steht hierbei die Frage, welche Mittel bei militärischen Konfliktlösungen erlaubt sind und wie diese eingesetzt werden dürfen. Zu beachten sind dabei vor allem drei, auch völkerrechtlich verankerte Gebote (Kap. 7.2). Erstens: Es dürfen nur Kombattanten, nicht jedoch die Zivilbevölkerung direkt angegriffen werden (Unterscheidungsgebot). Zweitens: Der Einsatz von Waffengewalt muss verhältnismäßig sein, d. h., tote Zivilisten und anderweitige Kollateralschäden müssen in einem angemessenen Verhältnis zum militärischen Nutzen stehen (Verhältnismäßigkeitsgebot). Und drittens: Alles Erforderliche muss getan werden, um die Zivilbevölkerung auch vorsorglich zu schützen (Vorsorgeprinzip). Kampfmittel, die diese Kriterien systematisch verletzen, gelten als ethisch unzulässig und sind völkerrechtswidrig. Insofern ist die Frage, inwieweit AWS in der Lage sind, diese Kriterien einzuhalten, sowohl von zentraler völkerrechtlicher als auch ethischer Bedeutung – die entsprechende Debatte wird in Kapitel 8.1.2 genauer dargestellt (bzw. aus völkerrechtlicher Sicht in Kapitel 7.2).
3. Das »ius post bellum« befasst sich mit der Zeit nach der kriegerischen Auseinandersetzung, speziell mit all jenen Aktivitäten, die für den Übergang in eine stabile Nachkriegsordnung sowie für deren Aufrechterhaltung erforderlich sind (Frank 2009). Die dazugehörigen Fragen sind daher eng mit denen des »ius ad bellum« sowie »ius in bello« verknüpft, da nicht zuletzt von der Legitimität des Krieges sowie der Wahl der kriegerischen Mittel

wesentlich abhängt, ob sich nach Beendigung der Kriegshandlungen eine nachhaltige Friedensperspektive eröffnet (Koch/Rinke 2017, S. 155). So wird auch mit Blick auf AWS diskutiert, inwiefern deren Einsatz friedensförderlich sein könnte oder nicht (z. B. Leveringhaus 2016, S. 20). Allerdings ist festzustellen, dass das »ius post bellum« generell zu den eher vernachlässigten Aspekten im Rahmen der Lehre vom gerechten Krieg gehört und insofern auch in der ethischen Debatte über AWS nur eine Nebenrolle spielt (Koch/Rinke 2017, S. 155).

Fragen des »ius in bello« nehmen in der ethischen AWS-Debatte bei Weitem den größten Raum ein, weshalb sie im Folgenden auch vertieft behandelt werden. Diese Sonderstellung hat ihren Grund nicht zuletzt in dem Umstand, dass das Spezifikum von AWS, nämlich die Entscheidungsgewalt über den potenziell tödlichen Waffeneinsatz außerhalb menschlicher Kontrolle zu stellen, sich nur im Rahmen von direkten Kriegshandlungen manifestieren kann – weshalb sich mithin auch die damit verknüpften ethischen Fragen primär auf das »ius in bello« beziehen (Sparrow 2016).

Mit Blick auf das »ius ad bellum« hingegen werfen AWS keine moralischen Probleme auf, die sie in besonderer Weise von anderen modernen Waffensystemen abheben. So wird die (im Übrigen eher sicherheitspolitisch als ethisch relevante) Frage, ob durch AWS die Hemmschwelle für kriegerische Gewaltanwendung sinkt, derzeit bereits im Zusammenhang mit dem sogenannten Drohnenkrieg intensiv diskutiert (Franke/Leveringhaus 2015, S. 307 f.; Geiß 2015, S. 13). Eine bestimmte Sonderrolle nimmt ein Szenario ein, in dem Aspekte des »ius ad bellum« sowie des »ius in bello« gewissermaßen verschwimmen und das von Altmann (2017, S. 799) wie folgt beschrieben wird: »In einer schweren Krise würden sich zwei Flotten autonomer Waffensysteme intensiv gegenseitig beobachten; unklare Ereignisse könnten als Angriff missverstanden werden, zum vermeintlichen Gegenangriff führen und damit eine militärische Eskalation auslösen.« Hier ist die Erhöhung der Kriegswahrscheinlichkeit direkte Folge einer Autonomisierung der Kriegsführung und des damit verbundenen menschlichen Kontrollverlustes.[89] Das Szenario verdeutlicht, dass Aspekte des »ius ad bellum« sowie des »ius in bello« häufig nicht isoliert voneinander, sondern vielmehr in ihrer wechselseitigen Verschränkung zu betrachten sind (Koch/Rinke 2017, S. 39).

Inwiefern AWS den Regeln des »ius post bellum« gemäß eine echte Friedensperspektive zu befördern imstande sind, hängt wiederum entscheidend davon ab, ob und inwiefern sie überhaupt die Bestimmungen des humanitären Völkerrechts einhalten und sich folglich in Kampfsituationen ethisch angemessen verhalten können. Die diesbezügliche Debatte, die im Folgenden genauer beleuchtet

89 Laut dem Philosophen Peter Asaro (2008) wäre ein solch versehentlich ausgelöster Krieg (»accidental war«) im Übrigen nicht rechtmäßig, da er auf keinem legitimen Kriegsgrund basiert.

werden soll, kreist maßgeblich um Argumente, die von Ronald C. Arkin, Robotikforscher am Georgia Institute of Technology, vorgebracht wurden.

8.1.2 Ermöglichen AWS eine ethischere Kriegsführung?

Aus militärischer Sicht bieten AWS, es wurde bereits darauf hingewiesen (Kap. 5), etliche Vorteile: Computer sind Menschen bei der Verarbeitung großer Datenmengen deutlich überlegen, sodass von ausgereiften Kampfrobotern prinzipiell schnelle Reaktionszeiten sowie eine effiziente und präzise Kampfführung zu erwarten wäre. Verfügen diese Systeme zudem über ausreichende Autonomie, sodass sie auch in unzugänglichen Gebieten sowie weitgehend unabhängig von menschlicher Intervention einsatzfähig wären, könnten sie die militärische Reichweite bzw. die Gefechtsdistanz substanziell erweitern. Dies wiederum würde die Möglichkeit eröffnen, »die Gefahr [eigener] menschlicher Verluste« (Geiß 2015, S. 4) zu reduzieren, indem »jene Aufgaben von Robotern übernommen werden, die den Soldaten einer zu großen Gefahr aussetzen« (Dickow 2015, S. 12). Dieses Argument hat nun nicht nur eine militärische, sondern durchaus eine ethische Komponente, da die Verringerung menschlicher Verluste moralisch in den meisten Fällen geboten scheint. Vor diesem Hintergrund hat der Philosoph Bradley Strawser (2010) im Kontext der Drohnendebatte die Auffassung vertreten, dass es unter Umständen sogar die moralische *Pflicht* eines Staates sein kann, Systeme wie Drohnen einzusetzen, welche die eigenen Soldaten unnötigen Risiken entziehen. Ganz ähnlich, wenn auch deutlich breiter, argumentiert mit Blick auf AWS Ronald C. Arkin. Die von ihm vertretene und kontrovers diskutierte These lautet, dass AWS nicht nur in der Lage sein könnten, das Leben der eigenen Soldaten zu schützen, sondern dass sie insgesamt eine *humanere* Kriegsführung ermöglichen.

Die Position Arkins

Arkin spielt insofern eine »singuläre Rolle« (Koch/Rinke 2017, S. 70), als er praktisch der einzige namhafte Experte ist, der sich im Rahmen der ethischen Debatte dezidiert für AWS ausspricht (z. B. Arkin 2010).[90] Seine Argumentation ist allerdings weniger ethisch, denn rechtlich orientiert: Arkins zentrale These lautet, dass AWS technisch so entworfen werden können, dass sie die zuvor beschriebenen Regeln des Völkerrechts insgesamt besser einzuhalten vermögen als menschliche Soldatinnen und Soldaten. Sollte dies der Fall sein, wäre ihr Einsatz moralisch geradezu geboten, so Arkin (2013, S. 7), da Kriege dadurch insgesamt humaner und mithin ethischer gestaltet werden könnten.

90 Ebenfalls ein starker Befürworter von AWS ist der deutsche Philosoph Vincent C. Müller (2016).

Arkin (2013, S. 9) selber hat immer wieder darauf hingewiesen, dass er AWS nicht per se befürwortet und insofern auch kein prinzipieller Gegner eines Verbots ist. Sein Standpunkt ist vielmehr geprägt von einem grundlegenden Pessimismus, sowohl was die Überwindbarkeit von kriegerischen Auseinandersetzungen angeht als auch hinsichtlich der Fähigkeit des Menschen, sein regelmäßig von Grausamkeit und Verbrechen geprägtes Verhalten im Krieg im Sinne des humanitären Völkerrechts nachhaltig zu verändern (Koch/Rinke 2017, S. 71). Es sind also letztlich Negativaspekte wie die Unvermeidlichkeit des Krieges sowie vor allem die gut dokumentierte Unzulänglichkeit des Menschen auf dem Schlachtfeld, die laut Arkin (2010, S. 334 ff.) für AWS sprechen und diese insgesamt als das kleinere Übel erscheinen lassen. Konkret weist Arkin (z. B. 2010, S. 333, u. 2013, S. 6 ff.) u. a. auf folgende Vorteile autonomer Kampfsysteme (gegenüber menschlichen Kombattanten) hin:

- *Kein Selbsterhaltungstrieb*: Anders als Menschen setzen AWS auf dem Schlachtfeld nicht ihr Leben aufs Spiel, wodurch sie sich deutlich zurückhaltender verhalten können. Dies gilt insbesondere hinsichtlich der Anwendung von übermäßiger und unverhältnismäßiger Gewalt, die bei Soldatinnen und Soldaten häufig zum Selbstschutz erfolgt.
- *Fehlende Emotionen*: Bei Maschinen besteht nicht die Gefahr, dass das Verhalten durch starke Emotionen wie Stress, Angst oder Zorn beeinflusst wird, die Menschen in Gefechtssituationen oftmals zu einem unethischen Verhalten (z. B. aus Rache oder Frust) provozieren.
- *Bessere Sensorik*: Die Wahrnehmungsfähigkeiten von Menschen sind aus biologischen Gründen eingeschränkt und technisch nicht beliebig erweiterbar. Dahingegen sind den sensorischen Fähigkeiten von AWS prinzipiell keine technischen Grenzen gesetzt, zudem lassen sie sich spezifisch auf die im Gefecht benötigten Anforderungen anpassen. AWS sollten deshalb besser als Menschen in der Lage sein (zumindest potenziell), sich in komplexen und unübersichtlichen Gefechtssituationen zurechtzufinden.
- *Überlegene kognitive Fertigkeiten*: Roboter sind weit besser darin, umfangreiches Datenmaterial zu prozessieren und auszuwerten – nicht nur, was die Geschwindigkeit angeht, sondern auch hinsichtlich der Integration unterschiedlicher Datentypen. Außerdem leiden sie nicht an kognitiver Voreingenommenheit und Verzerrung, von der die menschliche Urteilskraft gerade in hierarchisch geprägten Entscheidungssituationen oftmals befallen ist.[91]

91 Arkin (2015, S. 46) spricht in diesem Zusammenhang vom psychologischen Phänomen des »scenario fulfilment syndrome«: Informationen, die nicht in ein einmal gewähltes Interpretationsschema passen, werden ignoriert. Es wird vermutet, dass der Abschuss des Iran-Air-Flugs 655 durch das US-Kriegsschiff »USS Vincennes« 1988 auf dieses Phänomen zurückzuführen sei (Wikipedia 2006b).

Arkin kommt vor diesem Hintergrund zu dem bereits erwähnten Schluss, dass AWS gegenüber dem beklagenswerten Status quo der Kriegsrealität grundsätzliche Vorteile versprechen, und zwar nicht nur in militärischer, sondern auch und vor allem in humanitärer Hinsicht. So sind sie ihm zufolge durch die zuvor genannten Merkmale insgesamt besser als menschliche Kämpfer in der Lage, zwischen Kombattanten und unbeteiligten Zivilisten zu unterscheiden (Unterscheidungsgebot) und Waffengewalt so präzise und gleichzeitig zurückhaltend einzusetzen, dass unverhältnismäßige Kollateralschäden ausgeschlossen sind (Verhältnismäßigkeitsgebot). Wohlgemerkt, Arkin (2015, S. 46) erwartet von AWS diesbezüglich keine Perfektion. Er ist jedoch der festen Überzeugung, dass sie dem Menschen in dieser Hinsicht prinzipiell weit überlegen sein können, besonders unter den zeitkritischen und überaus komplexen Bedingungen des modernen Schlachtfeldes.

Kasten 8.1 Zwei Grundmodelle ethischen Argumentierens

In der Ethik lassen sich grundsätzlich folgen- und handlungsorientierte Argumentationen unterscheiden. Die jeweiligen Positionen werden als Konsequentialismus bzw. Deontologie bezeichnet:

- Konsequentialistische Argumentationsmuster bewerten eine Handlung primär danach, wie ihre Konsequenzen ausfallen. Die bekannteste konsequentialistische Theorie ist der Utilitarismus, der Handlungen danach bemisst, wie sie zur Vermehrung des allgemeinen Nutzens beitragen.
- Deontologische Argumentationsmuster verweisen dagegen auf den Handlungstyp selbst und bewerten dessen inhärente Zu- oder Unzulässigkeit. Einfache Beispiele sind Sätze wie »Du sollst nicht töten!« – ein Gebot, dessen Richtigkeit aus deontologischer Perspektive unabhängig davon gilt, welche Folgen sich aus einer Tötung ergeben und ob darunter auch günstige Folgen zu finden sind.

Wie sich die beiden Argumentationsformen genau voneinander abtrennen lassen, ist Gegenstand vielfältiger Diskussionen. So ist zwar keine ethische Theorie gegenüber den Handlungsfolgen völlig indifferent, d. h., auch deontologische Ansätze beziehen Folgenabwägungen in die Rechtfertigungsargumente mit ein. Allerdings gibt es – wie der erwähnte Utilitarismus – rein konsequentialistische Herangehensweisen.

Quelle: Koch/Rinke 2017, S. 137 f.

Deutlich wird, dass Arkins Argumentation utilitaristisch ausgerichtet ist, insofern seine ethische Beurteilung von AWS primär auf den potenziellen Nutzen rekurriert, der von ihrem Einsatz zu erwarten ist. Demnach gelten AWS u. a.

deshalb als ethisch vorteilhaft, da sie dabei helfen können, zivile Opfer zu reduzieren. Ethische Argumentationen dieser Art machen die Frage der Zulässigkeit der Nutzung eines technischen Instruments ausschließlich von den Konsequenzen abhängig, die bei der Nutzung des Instruments (bzw. bei Verzicht darauf) zu erwarten sind (Kasten 8.1).

Das Problem dabei ist, dass diese Konsequenzen nicht nur vielschichtig, sondern oft unklar sind und auf mehr oder weniger unsicheren Prognosen beruhen; dies gilt besonders für Technologien, die sich – wie AWS – erst in einem frühen Stadium der Entwicklung befinden (zur Problematik konsequentialistischer Ansätze vgl. Koch/Rinke 2017, S. 145 ff.). So ist auch die Aussage, dass der Einsatz von autonomen Waffensystemen zu weniger Kollateralopfern führen würde, derzeit noch ein reines Zukunftsversprechen.

Klar ist: Zum jetzigen Zeitpunkt ist der technologische Entwicklungsstand in den relevanten Bereichen (KI, Robotik und Sensorik etc.) bei Weitem noch nicht ausgereift genug, um ethisch vertretbare bzw. völkerrechtskonforme Kampfroboter zu konstruieren. Die entsprechenden technischen Hürden hält Arkin jedoch für überwindbar – vorausgesetzt, es wird ausreichend in FuE investiert. Einem Verbot, wie es derzeit im Rahmen der CCW diskutiert wird (Kap. 9.2), steht er äußerst kritisch gegenüber, weil es genau dies unterbindet: Es sei voreilig und basiere auf »reiner Angst und Pathos« (»pure fear and pathos«; Arkin 2013, S. 10). Stattdessen plädiert Arkin (2015, S. 47) für ein Moratorium, das sich auf den Bau und den Einsatz von Kampfrobotern beschränkt. Diese Vorgehensweise würde es ermöglichen, FuE zu AWS weiter voranzutreiben und so die Chancen auszuloten (und später ggf. zu nutzen), welche die Technologie hinsichtlich einer humaneren Kriegsführung bietet.

Arkin (2009, S. xii ff.) selbst hat als Robotiker viele Jahre an der Entwicklung »moralischer« Kampfroboter geforscht, u. a. im Auftrag des US-Verteidigungsministeriums. Seine Arbeiten lassen sich der neuen Disziplin der Maschinenethik zuordnen, die zum Ziel hat, »künstliche Systeme mit der Fähigkeit zu moralischem Entscheiden und Handeln auszustatten« (Misselhorn 2018, S. 29; Kasten 8.2). In diesem Sinne hat Arkin (2008 u. 2009) detaillierte Vorschläge gemacht, wie Kampfroboter zu gestalten sind, damit sie sich rechtlich und moralisch möglichst untadelig verhalten. Kernstück der von ihm propagierten AWS-Architektur ist der »ethical governor«, der als eine Art künstliches Gewissen fungiert und zwischen die deliberativen Komponenten des Systems sowie dessen ausführende Instanzen geschaltet ist. Zweck des »governor« ist zu prüfen, ob die vom System generierten Entscheidungen (zumindest soweit sie die Ausübung von Waffengewalt betreffen) mit dem humanitären Völkerrecht und den militärischen Einsatzregeln konform gehen (Koch/Rinke 2017, S. 72); falls dies nicht der Fall ist, könnte der »governor« die Ausführung der geplanten Aktion unterbinden. Gleichzeitig eröffnet dies grundsätzlich die Möglichkeit, so Arkin (2009, S. 203 ff.), dass die ethischen Schlussfolgerungen des Roboters von

einem menschlichen Bediener überwacht werden und so ein gewisses Maß an menschlicher Kontrolle sichergestellt wird – der Bediener könnte z. B. immer dann eingreifen, wenn er antizipiert, dass der Roboter unethisch zu agieren versucht (Koch/Rinke 2017, S. 72).[92]

Arkins Perspektive ist also primär eine designtechnische, die von dem Bestreben geprägt ist, ethische Erwägungen so zu formalisieren, dass sie sich maschinell implementieren lassen. Mit diesem maschinenethischen Vorhaben sind nicht zuletzt umstrittene Annahmen über die Natur moralischen Entscheidens und Handelns verbunden (Kasten 8.2). Unter anderem ist eine unabdingbare Voraussetzung für die Realisierung eines »ethical governor«, dass sich völkerrechtliche Vorgaben, kontextspezifische Einsatzregeln sowie ethische Prinzipien sinnvoll in Programmcodes abbilden lassen (Arkin 2008, S. 39 ff.). Besonders dieser Anspruch stößt von verschiedenen Seiten auf massive Kritik.

Kasten 8.2 Moralische Maschinen? Die neue Disziplin der Maschinenethik

Im Zuge des Fortschritts im Bereich der KI und Robotik hat sich die Maschinenethik in den letzten Jahren als »neues Forschungsgebiet an der Schnittstelle von Informatik und Philosophie« (Misselhorn 2018, S. 29) etabliert. Ausgangspunkt maschinenethischer Überlegungen bildet die Beobachtung, dass maschinelle Systeme immer autonomer werden und also nicht mehr bloß *Objekte der Moral* sind – wie herkömmliche Maschinen, die sich eindeutig menschlichen Zwecken unterordnen und deshalb über keine eigene Moral verfügen. Vielmehr treten Maschinen, je eigenständiger sie werden, verstärkt als *Subjekte der Moral* in Erscheinung, d. h. als künstliche Akteure, deren Agieren moralische Implikationen hat und entsprechend auch nach ethischen Gesichtspunkten beurteilt werden kann (und eventuell sogar muss). Vor diesem Hintergrund beschäftigt sich die Maschinenethik sowohl in theoretischer als auch gestalterischer Absicht mit der Moral autonomer Systeme, u. a. mit dem Ziel, *moralische Maschinen* zu konstruieren, die sich auch in komplexen Entscheidungssituationen möglichst im Einklang mit unseren Wertvorstellungen verhalten (Anderson/Anderson 2007; Wallach/Allen 2008). Interessante Anwendungsgebiete sind vor allem jene gesellschaftlichen Bereiche, in denen autonome Systeme zukünftig eng mit Menschen interagieren könnten: Beispiele sind etwa die Pflege (Pflegerobotik), der Verkehr (automatisiertes Fahren) oder das Militär (AWS).

92 Auch der andere Fall ist möglich: Wenn der »governor« eine Handlung aus ethischen Gründen zu unterbinden sucht, so könnte der menschliche Operator deren Ausführung dennoch zulassen und müsste dafür dann aber auch letzten Endes die Verantwortung übernehmen.

Die skizzierte maschinenethische Programmatik ist mit der grundlegenden Frage konfrontiert, ob und inwiefern es überhaupt zulässig ist, moralische Kategorien wie *gut* und *böse* auf Maschinen zu übertragen. Selbst wenn diese scheinbar intelligentes Verhalten zeigen: Ist es nicht so, dass moralisches Handeln die Fähigkeit zur Handlungsurheberschaft, Willensfreiheit und folglich genuine Autonomie im Kant'schen Sinne voraussetzt (Kasten 2.1)? Maschinenethiker wie Ronald C. Arkin (2009, S. 37) oder Oliver Bendel (2018) bestreiten dies nicht. Sie gestehen zu, dass Maschinen nur über Autonomie im operationellen Sinne verfügen – und damit nicht über eine »vollumfängliche moralische Handlungsfähigkeit, wie sie Menschen typischerweise besitzen« (Misselhorn 2018, S. 31). Auch wenn es sich derzeit bei der maschinellen Moral noch um eine künstliche Moral handelt, also eine reine Simulation menschlicher Moralfähigkeiten (analog zur künstlichen Intelligenz), so wäre es dennoch sinnvoll – alleine schon aus anwendungspraktischen Gründen –, teilautonome und autonome Maschinen so zu konstruieren, dass sie mit moralisch problematischen Situationen umgehen können.

Für Kritiker wie Noel Sharkey (2012b, S. 793 ff.) und andere hingegen beruht das maschinenethische Unterfangen auf einem unzulässigen Anthropomorphismus, der von der fälschlichen Vorstellung ausgeht, dass Moral etwas ist, was logisch formalisierbar und maschinell implementierbar ist (Royakkers/van Est 2015, S. 268). Das mag für bestimmte ethische Theorien wie den Utilitarismus sogar zutreffen; die zugrundeliegende Fähigkeit zum moralischen Urteil ist jedoch nicht auf explizite Regeln reduzierbar, sondern hat ihren Ursprung in der Subjektivität des Menschen, die das Reflektieren über Werte, das Handeln aus moralischen Gründen sowie moralische Emotionen wie Mitgefühl oder Schuldgefühle erst ermöglicht (Misselhorn 2018, S. 31 f.). Insofern birgt die anthropomorphisierende Rede von moralischen Maschinen die Gefahr, das menschliche Fundament zu untergraben, auf dem die Moralität überhaupt erst gründet (Beavers 2011). In diesem Sinne konstatiert Bernhard Koch (2017, S. 10): »Die Gefahr in der ganzen Debatte um künstliche Intelligenz besteht meines Erachtens darin, dass wir angefangen haben, die Prozesse von Maschinen mit Begriffen zu bezeichnen, die wir aus unseren lebensweltlichen Bezügen kennen [...] und dass wir dann anfangen, unser eigenes Handeln und Verhalten nach dem Modell der Maschine zu beschreiben.«

Die Gegenargumente

Kaum zu bestreiten ist: Sollte sich zeigen, dass AWS nicht nur dem Schutz der eigenen Soldaten dienen, sondern auch dabei helfen, unbeteiligte Dritte zu schützen – wie Arkin behauptet –, wäre das sicherlich ein triftiges ethisches Argument für deren Einsatz. Doch kann man Roboter tatsächlich so programmie-

ren, dass sie die Regeln des »ius in bello« (bzw. des Völkerrechts) zuverlässig einhalten? Zum jetzigen Zeitpunkt ist dies schwierig zu beurteilen, da es vollautonome Waffensysteme ja noch gar nicht gibt und vieles von der weiteren technischen Entwicklung abhängt. Dennoch wird in der Literatur mehrheitlich die Ansicht vertreten, dass Arkin die technischen Herausforderungen systematisch unterschätzt, die mit der Entwicklung und Konstruktion von »moralischen« Kampfrobotern einhergehen (Koch/Rinke 2017, S. 73 ff.). Dies betrifft vor allem die Unterscheidung von legitimen und illegitimen Angriffszielen, die ohne ein umfassendes Situationsverständnis nicht angemessen durchführbar ist (Kap. 7.2). Hinzu kommen die inhärenten Interpretationsspielräume, die das humanitäre Völkerrecht besonders hinsichtlich der Abschätzung der Verhältnismäßigkeit eines Angriffs aufwirft und die starke Zweifel wecken, ob sich dessen Regeln so operationalisieren lassen, dass sie von einem Computerprogramm verarbeitet werden können (z. B. Geiß 2015, S. 14 ff.; Sharkey 2012b, S. 789).

Vor diesem Hintergrund wird darauf hingewiesen, dass autonome Waffensysteme neue und in ihrem Ausmaß noch nicht klar bestimmbare Risiken schaffen werden (Koch/Rinke 2017, S. 148). Zum Wesenskern von AWS gehört ja, dass sie sich autonom verhalten und mithin nach Aktivierung menschlicher Kontrolle gänzlich entzogen sind. Mit AWS kommt somit ein Element der Unvorhersehbarkeit ins Spiel, das zur Folge hat, dass inakzeptable Konsequenzen, wie z. B. unverhältnismäßige Kollateralschäden, nie ganz auszuschließen wären (IKRK 2018a, S. 16 f.). Auch die nichtintendierte Auslösung eines Krieges oder bewaffneten Konfliktes, z. B. durch sensorische Fehlinterpretation eines autonomen Waffensystems (ohne dass ein menschlicher Bediener noch die Möglichkeit hat einzugreifen), stellt eine ernstzunehmende Möglichkeit dar (Koch/Rinke 2017, S. 149). Zwar gehört die Bestimmung derartiger Risiken streng genommen nicht zum Bereich der Ethik, sondern ist eine technische bzw. sicherheitspolitische Aufgabe. Mit Blick darauf, dass diese Geräte auf Tötung hin ausgelegt sind, erscheint aus ethischer Sicht dennoch zumindest naheliegend, wie Koch und Rinke (2017, S. 148 u. 158 f.) betonen, auf ein »Ingangsetzen« unkontrollierbarer Vollzüge aus einem allgemeinem Vorsichtsprinzip heraus zu verzichten – und zwar selbst dann, wenn die Eintrittswahrscheinlichkeit inakzeptabler Folgen eher gering erscheint.[93]

Es ist fraglich, ob der von Arkin vorgeschlagene Lösungsansatz, nämlich Roboter mit einem künstlichen Gewissen auszustatten – einem »ethical governor«, der alle Entscheidungen des Systems noch einmal auf ihre rechtliche und ethische Angemessenheit prüft –, hier Abhilfe zu schaffen vermag. Für Kritiker Arkins wie Asaro (2012, S. 701 f.) oder Sparrow (2016, S. 101) liegt dieser Idee die fälschliche Vorstellung zugrunde, dass sich aus moralischen wie auch rechtlichen Maßstäben eindeutige Verhaltensregeln ableiten lassen. Dies ist jedoch

93 Zur ethischen Fundierung des Vorsichtsprinzips vgl. Rath et al. 2012, S. 105 ff.

nicht der Fall; selbst das moralisch wie rechtlich sehr hoch verankerte Tötungsverbot gilt nicht absolut (wie ja gerade das Kriegsvölkerrecht zeigt), sondern kennt Ausnahmen und ist deshalb immer auslegungsbedürftig. Moralisches und rechtliches Erwägen sind aus diesen Gründen wohl noch auf längere Zeit auf menschliche Urteilskraft angewiesen, so Sparrow (2016, S. 99) – zumindest noch so lange, bis es gelingt, eine starke KI zu erzeugen, die sich nicht nur in funktioneller, sondern auch moralischer Hinsicht als autonom erweist (Kasten 2.1).

Bis es soweit ist – und ob es jemals so weit kommen wird, ist derzeit reine Spekulation –, scheint sich folgende Schlussfolgerung aufzudrängen: Ohne adäquate menschliche Supervision und Kontrolle sollten AWS bis auf Weiteres nicht eingesetzt werden dürfen, da – wie skizziert – kaum sicherzustellen ist, dass sie sich ethisch und völkerrechtlich einwandfrei verhalten, und verheerende Folgen deshalb nie ganz auszuschließen sind (Asaro 2012, S. 708; Sparrow 2016, S. 102). Ein autonomes Waffensystem, dessen Aktivitäten unter konstanter menschlicher Überwachung zu stehen hätte, wäre jedoch nicht wirklich autonom. Nun könnte man zwar den unüberwachten Einsatz von AWS auf solche Kampfgebiete beschränken, die weitgehend frei von Zivilbevölkerung und damit moralisch problematischen Entscheidungssituationen sind (Sparrow 2016, S. 102 ff.). Abgesehen davon, dass sich eine solche Begrenzung des Aktionsradius kaum kontrollieren ließe, stünde sie in gewissem Widerspruch zu den postulierten militärischen Vorteilen von AWS, die ja u. a. in der Erweiterung des Gefechtsraumes sowie der militärischen Reichweite zu sehen sind (Koch/Rinke 2017, S. 80). Und auch ein weiterer Vorschlag, der in die Diskussion eingebracht wurde, scheint wenig zielführend, nämlich den »ethical governor« als Steuerungsmodul so auszugestalten, dass er immer dann einen menschlichen Bediener involviert, wenn moralisch kritische Entscheidungen auf dem Spiel stehen (Brutzman et al. 2013; Koch/Rinke 2017, S. 77 f.; Sparrow 2016, S. 101 f.). Voraussetzung wäre, dass der »ethical governor« zuverlässig einschätzen kann, wann er mit moralischen Entscheidungssituationen konfrontiert ist, die er nicht selber zu lösen vermag; dies ist von einer Instanz, deren ethische Urteilskraft generell fragwürdig ist, freilich nicht zu erwarten.

Insgesamt bestehen also deutliche Zweifel an Arkins Postulat, dass AWS mit völkerrechtlichen Standards vereinbar sind. Unabhängig davon stellt sich die wesentlich grundsätzlichere Frage, ob die bestehenden Regeln des Kriegsvölkerrechts »überhaupt noch die richtigen Regeln sind, wenn autonome Kampfsysteme in die Konfliktführung integriert sind« (Geiß 2015, S. 17 f.). Ausgangspunkt derartiger Überlegungen ist die Feststellung, dass die aktuellen Normen des humanitären Völkerrechts von einem fundamentalen Anthropozentrismus geprägt sind, basierend auf der Prämisse, dass alle kritischen (insbesondere letalen) Entscheidungen von Menschen getroffen werden. Mit dem Aufkommen autonomer Waffen wäre hingegen eine *militärtechnologische*

Zeitenwende eingeleitet, die diesbezüglich eine ganz neue Situation schaffen würde. So kann von autonomen Waffensystemen eine außerordentlich hohe Präzision erwartet werden. Außerdem verfügen sie weder über menschliche Emotionalität und Irrtumsanfälligkeit noch agieren sie unter Einsatz des Lebens. Deshalb könnte es laut dem Völkerrechtler Robin Geiß (2015, S. 17 ff.) geboten sein, ihren Einsatz an deutlich »höhere humanitäre Schutzstandards zu binden«, als es für menschliche Kämpferinnen und Kämpfer geboten erscheint – was bis hin zu der Pflicht reichen könnte, AWS »grundsätzlich nur als nichttödliche Systeme einzusetzen«. Geiß beruft sich dabei maßgeblich auf eine Studie des Internationalen Komitees vom Roten Kreuz, das die These vertritt, dass im Krieg der Einsatz letaler Gewalt nur insoweit gerechtfertigt ist, als dies militärisch unbedingt erforderlich ist und keine anderweitigen nichtletalen Mittel zur Verfügung stehen (Melzer 2009). Käme es zukünftig nun zu einem Kampf Roboter gegen Mensch, bestünde für die Maschine, die ja kein Leben zu riskieren hat, »so gut wie nie eine zwingende Notwendigkeit, tödliche Gewalt anzuwenden« (Geiß 2015, S. 21). Jedenfalls ist das Töten einer Person alleine deshalb, weil diese eine Maschine zu beschädigen versucht, wahrscheinlich unverhältnismäßig (Koch/Rinke 2017, S. 154).

Damit ist eine zentrale Prämisse der Arkin'schen Argumentation infrage gestellt, nämlich, dass die tradierten Regeln einer ethischen Kriegsführung auch dann noch angemessen sind, sollten AWS dereinst zu einem maßgeblichen Faktor in militärischen Auseinandersetzungen werden. Doch moralische und rechtliche Maßstäbe sind nicht in Stein gemeißelt, sondern haben sich an neue Gegebenheiten anzupassen, wobei insbesondere der technische Fortschritt neue Herausforderungen aufwirft. Mit der Autonomisierung von Waffensystemen könnte sich die Kriegsführung so fundamental verändern, dass auch die traditionellen Prinzipien des »ius in bello« mit Blick auf AWS ggf. neu justiert werden müssten – etwa hinsichtlich der Frage, welche Ziele (mittels AWS) angegriffen werden dürfen oder wie die Verhältnismäßigkeit eines Einsatzes zu bewerten ist. Wie Koch und Rinke (2017, S. 154) etwa betonen, sind die Verhältnismäßigkeitsanforderungen im Laufe der Zeit aufgrund technologischer Verbesserungen stetig und deutlich angestiegen. Was im Zweiten Weltkrieg möglicherweise noch als verhältnismäßig gelten konnte, kann heute völlig unangemessen sein, da mit der Verfügbarkeit von neuen, präziseren Kampfmitteln auch die Anforderungen an Verhältnismäßigkeit neu zu bewerten sind. Ob für AWS überhaupt die gleichen völkerrechtlichen Standards gelten sollen wie für menschliche Kombattanten, ist also alles andere als klar. Deshalb dürfte auch Arkins These, dass AWS dereinst besser als Menschen in der Lage sein werden, sich gemäß den bestehenden völkerrechtlichen Standards zu verhalten, zu kurz greifen.

8.2 AWS und die Würde des Menschen

Die bisher vorgestellten Argumente kreisten um die im Wesentlichen technische Frage, ob und inwiefern AWS so konstruierbar sind, dass sie den Regularien des humanitären Völkerrechts Folge zu leisten vermögen. Doch angenommen, es gelänge, eine technisch perfekte Tötungsmaschine zu entwickeln, die diesbezüglich fehlerfrei agiert (zu diesem Gedankenexperiment Leveringhaus 2016, S. 89 ff., und Koch/Rinke 2017, S. 127 ff.). Stellt sich dann nicht dennoch »die ganz grundsätzliche Frage, ob Computeralgorithmen über Leben und Tod entscheiden sollten, ohne dass ein Mensch diese Entscheidung zumindest mitträgt und auf sein Gewissen lädt« (Schörnig 2014, S. 33)?

Im Gegensatz zu einer konsequentialistischen Denkweise, die lediglich die Folgen eines AWS-Einsatzes in den Blick nimmt, werden ethische Bedenken, die grundsätzlicher auf die Handlung selbst verweisen, deontologisch genannt (Kasten 8.1). Deontologische Argumente spielen im Zusammenhang mit AWS eine wichtige Rolle. Zur Debatte steht in diesem Kontext nämlich nichts weniger als der grundsätzliche Zweck derartiger Waffensysteme: die Fähigkeit, autonom über Leben und Tod zu entscheiden. Dabei wird vor allem über die Frage diskutiert, ob und inwiefern die Tötung von Menschen durch autonome Systeme mit der Menschenwürde vereinbar ist. Ins Spiel kommen damit Überlegungen genuin ethischer Art, die weniger auf empirischen Erwägungen beruhen (wie es bei konsequentialistischen Argumenten der Fall ist), stattdessen stärker von normativen Vorgaben und begrifflichen Festlegungen geleitet sind.

8.2.1 Der Begriff der Menschenwürde[94]

Der Begriff der Menschenwürde geht wie derjenige der Autonomie maßgeblich auf die Philosophie der Aufklärung zurück und hat von dort den Weg in die Allgemeine Erklärung der Menschenrechte sowie das deutsche Grundgesetz (GG) gefunden. So heißt es in Artikel 1 GG, dass die Würde des Menschen unantastbar ist, während sich die Erklärung der Menschenrechte in der Präambel (und an verschiedenen anderen Stellen) auf die angeborene Würde aller Menschen beruft. Interessanterweise wird jedoch in beiden Fällen, trotz der zentralen Stellung des Begriffs, nicht weiter konkretisiert oder definiert, was unter der Würde des Menschen zu verstehen ist. Zurückzuführen ist das darauf, dass sich der Gehalt des Würdebegriffs als Rechtsbegriff »mangels einer juristischen Tradition seiner Verwendung« (Stoecker 2010, S. 19) primär in moralischen Intuitionen seinen Ursprung hat, die unter dem Eindruck der Grausamkeiten des

94 Die Ausführungen in diesem Teilkapitel lehnen sich an das Gutachten von Koch/Rinke 2017, S. 166 ff. an.

Zweiten Weltkrieges – also in der Nachkriegszeit, als die beiden Dokumente entstanden –, besonders gegenwärtig waren (Gutmann 2010, S. 3).

Trotz – oder vielleicht gerade wegen – seiner intuitiven Plausibilität haben wir es bei der Menschenwürde mit einem Begriff zu tun, der äußerst voraussetzungsreich, jedenfalls nicht einfach definierbar ist (Stoecker 2010). In der christlichen Tradition besteht die Würde des Menschen darin, dass er als Gottes Ebenbild geschaffen ist. Hingegen hängt die aufklärerische Prägung des Begriffs, die vor allem auf Immanuel Kant zurückgeht, untrennbar mit der spezifischen menschlichen Fähigkeit zusammen, moralisch autonom, d. h. selbstgesetzgebend zu sein (Kasten 2.1). Als Vernunftwesen ist der Mensch nach Kant dem »Reich der Zwecke« zugehörig, was bedeutet, dass Menschen fähig sind – im Unterschied zu Maschinen oder nicht vernunftbegabten Lebewesen –, ihre Ziele zu reflektieren und ihr Handeln selbst zu bestimmen (Ulgen 2017b). Damit ist eine Einzigartigkeit des Menschen angesprochen, die diesen gegenüber anderen Lebewesen auszeichnet und jedem menschlichen Individuum somit – völlig unabhängig von persönlichen Eigenheiten – einen moralischen Status verleiht, der Respekt verdient. Kant bringt dies auf folgende Formel: »Handle so, dass du die Menschheit sowohl in deiner Person, als in der Person eines jeden andern jederzeit zugleich als Zweck, niemals bloß als Mittel brauchest« (Kant, Grundlegung zur Metaphysik der Sitten). Mit anderen Worten, der Mensch ist Zweck an sich und sollte deshalb nie bloßes Mittel sein, da dies seine Autonomie missachtet. Nach dieser kantischen Lesart[95] heißt die Würde des Menschen achten, also zunächst anzuerkennen, dass ein Mensch einen inhärenten Wert besitzt und deshalb nicht instrumentalisiert, d. h. zum Spielball subjektiver Interessen und Bedürfnisse gemacht werden darf.

Dass Menschen immer auch einen materiellen Aspekt besitzen, ist davon unbenommen. So werden Menschen von anderen Menschen zu bestimmten wirtschaftlichen Zwecken eingesetzt, beispielsweise im Rahmen einer Beschäftigung, oder sie sind auf ihre Körperlichkeit zurückgeworfen, z. B. wenn sie krank sind und medizinischer Behandlung bedürfen. Insofern ist das Zufügen von Schmerz nicht notgedrungen entwürdigend, denn die betroffene Person könnte der Handlung, die die Schmerzen verursacht, zugestimmt haben. Anders sieht es aus, wenn jemandem gegen seinen eigenen Willen Leid zugefügt wird; in vielen Fällen stellt dies eine Würdeverletzung dar – allerdings nicht wegen des zugefügten Leids, sondern weil der Wille dieser Person eklatant missachtet wurde. Das Gebot der Menschenwürde verlangt also im Kern, dass ungeachtet der physischen Aspekte des Menschseins die Anerkennung eines Menschen als selbstbestimmtes Wesen niemals verlorengehen darf.

95 Daneben existieren diverse alternative philosophische Auslegungen von Menschenwürde, die besonders in bioethischen Debatten – etwa über den moralischen Status von ungeborenem menschlichem Leben – aufeinanderprallen (z. B. Birnbacher 2001; Kettner 2004).

Insbesondere in der deutschen bioethischen Diskussion spielt der Verweis auf eine mögliche Würdeverletzung des Menschen eine wichtige Rolle. Dies ist der kantischen Tradition und natürlich der besonderen, unantastbaren Stellung der Menschenwürde im Grundgesetz geschuldet. Die Würde des Menschen fungiert dabei als zentraler Grundwert und moralischer Leitbegriff, der sich gerade aufgrund seiner intuitiven Kraft und semantischen Offenheit in vielen politisch-moralischen Handlungskontexten als anschlussfähig erwiesen hat (Birnbacher 2016). Dadurch besteht allerdings auch die Gefahr, dass Würdeverweise in normativen Debatten fast schon inflationär in Anschlag gebracht werden, was den Begriff auszuhöhlen und ihn auf eine »Leerformel« (Birnbacher 2001, S. 243) zu reduzieren droht. Angesichts der zahlreichen philosophischen Kontroversen, die um den Begriff der Menschenwürde und dessen konkurrierende Deutungen entbrannt sind, erscheint elementar wichtig, in ethischen Debatten nicht nur pauschal auf mögliche Würdeverstöße hinzuweisen, sondern deutlich zu machen, welche elementaren Momente des Menschseins jeweils auf dem Spiel stehen.

8.2.2 Verletzt der Einsatz autonomer Waffensysteme die Menschenwürde?

Aus der Idee der Menschenwürde lassen sich die Menschen- und Grundrechte ableiten, zu denen auch das Recht auf Leben und körperliche Unversehrtheit gehört (Artikel 2 GG und Artikel 3 der Allgemeinen Erklärung der Menschenrechte). Jemandem das Recht auf Leben abzusprechen, ist offensichtlich nicht mit der Achtung seiner Würde vereinbar. Ein generelles Tötungsverbot, wie es etwa im 5. biblischen Gebot formuliert wird (»Du sollst nicht töten«), lässt sich daraus jedoch nicht ableiten. Denn es sind durchaus Umstände denkbar, unter denen die Tötung eines Menschen moralisch und rechtlich legitim erscheint. Dazu gehören insbesondere Notwehr- oder Nothilfesituationen, die auch staatlicherseits den Einsatz von Gewalt als Ultima Ratio rechtfertigen können – wie im Falle des finalen Rettungsschusses durch die Polizei. Auch Kriege sind gemäß der Lehre vom gerechten Krieg (sowie entsprechend dem Völkerrecht) nur dann gerechtfertigt, wenn sie sich als Akt kollektiver Notwehr (oder Nothilfe) deuten lassen. Festzuhalten bleibt also, dass völker- und auch verfassungsrechtlich gesehen Tötungen unter ganz bestimmten Bedingungen durchaus erlaubt und mit dem Prinzip der Menschenwürde vereinbar sind. Die entscheidende Frage lautet dann, ob sich daran etwas ändert, wenn auf AWS als Gewaltmittel zurückgegriffen wird.

Um es vorwegzunehmen: Wie die Literaturanalyse von Koch/Rinke (2017, S. 105 ff.) zeigt, trifft die These, dass es die Würde des Menschen verletzt, autonome Waffensysteme gegen menschliche Ziele einzusetzen, auf breite Zustim-

mung.[96] Allerdings wird auch deutlich, dass Aspekte der Menschenwürde im Rahmen der AWS-Debatte eher marginal behandelt werden und die dazugehörigen Argumente weit weniger ausdifferenziert sind als jene, die sich mit Fragen der ethischen Kriegsführung beschäftigen. Dies hat sicherlich zum einen damit zu tun, dass die Debatte über AWS vor allem im englischsprachigen Raum geführt wird, wo der Würdebegriff nicht die gleiche Bedeutung hat wie im deutschsprachigen Kontext; zum anderen aber auch mit den konzeptionellen Schwierigkeiten, die der schwer fassbare Begriff der Menschenwürde aufwirft, der christlich-theologische, philosophische und rechtliche Facetten aufweist.

Während die christliche Perspektive in der Debatte keine nennenswerte Rolle spielt, wird dafür umso mehr auf den philosophischen Kern des Würdegedankens rekurriert. Laut Geiß (2015, S. 18) ist er darin zu sehen, dass »jeder Mensch als Individuum wahrgenommen und dementsprechend behandelt werden muss, als einzigartiges, nicht austauschbares Wesen«. Dies gilt selbstverständlich auch – und vielleicht sogar ganz besonders – dann, wenn es darum geht, das Leben eines Menschen zu beenden. Gemäß einer Entscheidung des Bundesverfassungsgerichts (BVerfG, Urteil des Ersten Senats vom 15. Februar 2006 – 1 BvR 357/05 –, Rn. 1-156) zur Verfassungskonformität des § 14 Absatz 3 Luftsicherheitsgesetzes ist es beispielsweise entwürdigend, ein entführtes Flugzeug und dessen unschuldige Insassen zum Abschuss freizugeben, um dadurch andere Personen zu schützen: »Eine solche Behandlung missachtet die Betroffenen als Subjekte mit Würde und unveräußerlichen Rechten. Sie werden dadurch, dass ihre Tötung als Mittel zur Rettung anderer benutzt wird, verdinglicht und zugleich entrechtlicht, [...].« Dabei spielt laut dem BVerfG weder eine Rolle, ob die betroffenen Passagiere sowieso mit größter Wahrscheinlichkeit dem Tod geweiht sind, noch wie groß die Zahl der Personen ist, die sich auf diese Weise retten lassen. Die Quintessenz lautet: Selbst im Angesicht des Todes dürfen Menschen also nicht als bloße Objekte, als Mittel zum Zweck behandelt werden, da dies den inhärenten Wert negiert, der ihnen als Menschen zukommt.

Natürlich lassen sich Kriegssituationen nicht mit zivilen Rettungsaktionen gleichsetzen, wie sie das Bundesverfassungsgerichtsurteil zum Gegenstand hat. Dennoch lässt sich aus dem Prinzip der Menschenwürde unmittelbar folgende ethische Minimalanforderung an Tötungshandlungen ableiten, die auch auf militärische Kontexte zutrifft: Wer einen Menschen seines Lebens beraubt, sollte dies zumindest in der Anerkenntnis tun, dass es sich bei dem Opfer um einen Menschen, also ein Wesen von inhärentem Wert handelt (Koch/Rinke 2017,

96 Die Debatte, wie sie im Folgenden nachgezeichnet wird, bezieht sich also auf einen spezifischen Einsatzzweck von AWS, nämlich das Töten von Menschen. Darum lässt sich aus den Argumenten nicht ableiten, dass es ethisch falsch ist, autonome Waffen zu entwickeln, die für andere Zwecke verwendet werden, z. B. den Angriff auf nichtmenschliche Ziele wie die Erfassung und Zerstörung unbemannter Kampfdrohnen (Koch/Rinke 2017, S. 130).

S. 168 ff.; iPRAW 2018a, S. 12). Ohne direkt auf den Würdebegriff Bezug zu nehmen, weist Sparrow (2016) ganz in diesem Sinne darauf hin, dass es auch im Krieg und zwischen Feinden in moralischer Hinsicht essenziell ist, eine zumindest rudimentäre Form des zwischenmenschlichen Respekts aufrechtzuerhalten – selbst und gerade dann, wenn tödliche Gewalt im Spiel ist.

Was folgt daraus für den möglichen Einsatz von AWS? Zum jetzigen Zeitpunkt ist mehr als zweifelhaft, ob derartige Systeme je in der Lage sein werden, die skizzierten moralischen Anforderungen an Tötungshandlungen zu erfüllen. Zwar können Kampfroboter ihre Ziele anhand bestimmter Merkmale abstrakt als Menschen klassifizieren, aber sie verfügen nicht über die Empathie, sich in Menschen einzufühlen. Das wäre aber erforderlich, um nachvollziehen zu können, was es heißt, ein Mensch zu sein, und damit auch, um den inhärenten Wert menschlichen Lebens achten zu können. Die meisten Autorinnen und Autoren stimmen deshalb darin überein, dass der Respekt und die Anerkennung, die der Würdebegriff einfordert, im Wesentlichen eine interpersonale Beziehung voraussetzen, die verlorenzugehen droht, sobald Maschinen auf dem Schlachtfeld das Regiment übernehmen (z. B. Asaro 2012; Heyns 2016; HRW 2014; Sparrow 2016; Ulgen 2017a). Die Folge einer derart dehumanisierten Kriegsführung wäre, so Geiß (2015, S. 19), dass »der Mensch [...] dann gerade nicht mehr als Individuum wahrgenommen [wird], sondern als bloßes Objekt einer mathematisch kalkulierten Tötungsentscheidung«. Das Töten von Menschen geriete, mit anderen Worten, zu einem puren, mit »gnadenloser Konsequenz ausgeführten« Automatismus. Nicht zuletzt würden so »Faktoren wie Gnade oder Mitgefühl [...] aus der Gleichung entfernt« (Geiß 2015, S. 19), die für menschliche Tötungsentscheidungen konstitutiv sind oder es zumindest sein sollten, damit überhaupt ein Anspruch auf moralische Zulässigkeit besteht.

An dieser Stelle wird in der Würdedebatte eine argumentative Brücke zur Ethik des Krieges und zum humanitären Völkerrecht geschlagen. Dessen inhärente Interpretationsspielräume (Kap. 7) sind nicht nur als Mangel zu sehen – als rechtliche Unschärfen, die der Auslegung bedürfen –, sondern als positiver Wert, insofern sich dadurch erst der Raum für moralisches Urteilen und damit die Anerkennung der menschlichen Würde eröffnen (zum Folgenden Koch/Rinke 2017, S. 112 ff.). So ist Asaro (2012, S. 700 ff.) zufolge die Interpretations- und Auslegungsbedürftigkeit des humanitären Völkerrechts auch als Appell an die Menschlichkeit der Kombattanten zu verstehen. Ganz ähnlich argumentiert Sparrow (2016, S. 107), der darauf hinweist, dass durch das im humanitären Völkerrecht verankerte Recht, nicht zur Zielscheibe eines militärischen Angriffs zu werden (z. B. durch Aufgeben), die Humanität der potenziellen Opfer gewürdigt wird. Umgekehrt gilt dann wiederum: Die algorithmische Formalisierung der völkerrechtlichen Bestimmungen, wie sie der »ethical governor« Arkins vorsieht und auch voraussetzt, würde das deliberative Moment

und damit die Möglichkeit für eine »höchstpersönliche Gewissensentscheidung bzw. -prüfung« (Geiß 2015, S. 19) durch den Angreifer eliminieren.

Das Fazit derartiger Überlegungen lautet, dass Menschlichkeit gegenüber den Opfern von Gewalt letztlich auch nur von menschlichen Gewaltanwendern ausgeübt werden kann – zumindest so lange, bis auch Maschinen über die Fähigkeit zur Empathie, ein Gewissen und moralisches Bewusstsein verfügen. Und solange dies nicht der Fall ist, ist es unethisch, den menschlichen Faktor aus Entscheidungsprozessen zu eliminieren, welche die Anwendung tödlicher Gewalt zum Ziel haben. Deshalb stimmen die meisten Autoren, die zur Würdefrage Stellung genommen haben, darin überein, dass AWS intrinsisch (d. h. von der Sache her) mit dem Würdegebot unvereinbar sind.

Allerdings bleibt vieles diffus und ungeklärt: beispielsweise die Kriterien, die vorliegen müssen, damit unter den moralischen Extrembedingungen des modernen Krieges von einem menschenwürdigen Tötungsakt die Rede sein kann. Zu Recht wenden die Philosophen Ryan Jenkins und Duncan Purves (2016) ein, dass beim Einsatz hochtechnologischer Massenvernichtungs- und Distanzwaffen von wechselseitiger zwischenmenschlicher Anerkennung – als zentraler Grundbedingung eines moralisch akzeptablen Waffeneinsatzes – ebenfalls nicht die Rede sein kann. Wenn dem so ist, kann auf dieser Basis kaum mehr von einer spezifischen moralischen Verwerflichkeit von AWS gesprochen werden, da das Argument einer Würdeverletzung auf praktisch alle modernen Waffensysteme zutrifft. Der deutsche Philosoph Dieter Birnbacher (2016) stimmt dem zu und sieht das Problem in der inflationären und zu unspezifischen Verwendung des Würdekonzepts, die auch in der AWS-Debatte zum Ausdruck komme. Seiner Ansicht nach sind autonome Waffensysteme nicht grundsätzlich mit der Würde des Menschen inkompatibel, sondern nur, insofern sie in bestimmter, nämlich entwürdigender Weise eingesetzt werden. Ausschlaggebend sind dabei die psychologischen und physischen Folgen für die Betroffenen. Die Funktionen und Charakteristika, die demütigende Einsatzszenarien wahrscheinlich machen (und im Falle von AWS besonders wahrscheinlich, wie Birnbacher zugesteht), würden autonome mit vielen konventionellen Waffensystemen teilen. Dazu zählt Birnbacher (2016, S. 116 ff.) etwa die Unvorhersehbarkeit im Verhalten (analog zu versteckten Landminen oder ferngesteuerten Drohnen), welche die potenziellen Opfer großem psychischem und potenziell traumatisierendem Stress aussetzt; dieser Aspekt der Heimtücke wird dadurch verstärkt, dass AWS das Unterscheidungs- und das Verhältnismäßigkeitsgebot vermutlich nicht zuverlässig einhalten können (was aber z. B. beim Einsatz von Distanzwaffen in analoger Weise zutreffen kann). Ob ein Waffeneinsatz die Menschenwürde verletzt, lässt sich laut Birnbacher demzufolge nicht an intrinsischen Merkmalen des eingesetzten Systems festmachen (z. B. ob autonom oder nicht). Ausschlaggebend ist vielmehr alleine die subjektive Wirkung (etwa Traumatisierung

durch andauerndes Bedrohungsgefühl), die bei den Betroffenen unter den konkreten Umständen erzeugt wird.

Insgesamt machen derartige Einwände deutlich, dass stark von der inhaltlichen Bestimmung des Würdebegriffs abhängt, inwiefern eine Würdeverletzung von AWS plausibel erscheint. So vertritt der Utilitarist Birnbacher, der dem Würdekonzept insgesamt eher skeptisch gegenübersteht, einen ethischen Ansatz, der die Würde des Menschen vornehmlich bedürfnisorientiert deutet – relevantes und einziges Kriterium für eine Würdeverletzung ist dann, ob eine Störung des subjektiven Wohlbefindens vorliegt (Birnbacher 2016, S. 120). Koch und Rinke heben hingegen hervor, dass erst dort, wo Menschen sich auf andere Menschen beziehen, Würde aktuell werden kann (dazu und zum Folgenden Koch/Rinke 2017, S. 167 f.). Für Tötungshandlungen folgt daraus, dass immer noch anerkannt werden sollte, dass es ein Mensch ist, der getötet wird. Dabei liegt auf der Hand, dass es keine definitiven äußeren Kriterien geben kann, anhand derer sich in der Praxis ablesen lässt, ob dieses Anerkennungsmoment in ausreichender Weise erfüllt ist oder nicht. Ebenfalls wird eine Tötungshandlung dadurch natürlich noch lange nicht zu einer legitimen Handlung. Doch lässt sich daraus zumindest ableiten, dass dort, wo Menschen komplett die Möglichkeit genommen wird, in ihrer Würde durch andere geachtet zu werden – und zwar ganz unabhängig von ihren subjektiven Bedürfnissen –, diese fundamental bedroht ist. Insofern AWS diese basale Anerkennung nicht erbringen können, erscheint plausibel, ihren Einsatz als entwürdigende Form roher technischer Gewalt anzusehen. Wie gezeigt hängt die Überzeugungskraft dieses Gedankengangs allerdings zentral davon ab, ob man die zugrundeliegenden moralischen Intuitionen und theoretischen Festlegungen teilt. Zu konstatieren ist deshalb, dass die Herleitung einer Würdeverletzung durch AWS an enge argumentative Grenzen stößt.

8.3 Die Frage der Verantwortung

Trotz der Schwierigkeiten, den Autonomiebegriff definitorisch einzugrenzen (Kap. 2), ist eines gewiss: Ein Gewinn an maschineller Autonomie geht schon alleine aus begrifflichen Gründen immer mit einem Verlust an menschlicher Kontrolle einher (Noorman/Johnson 2014, S. 52). Dieser Kontrollverlust ist grundsätzlich erwünscht, da von autonomen Systemen ja erwartet wird, dass sie sich flexibel und unabhängig von menschlicher Einflussnahme in neuen und unvorhergesehenen Situationen zurechtfinden (Leveringhaus 2016, S. 79). Dadurch lässt sich ein umfangreicheres Funktionsspektrum realisieren und neue maschinelle Anwendungsgebiete erschließen, womit sich im militärischen Bereich perspektivisch ganz neue strategische, operative und taktische Möglichkeiten eröffnen (Kap. 5.3).

Die Kehrseite davon ist jedoch, dass die Frage der Verantwortungszuschreibung deutlich an Brisanz gewinnt. Denn je autonomer Systeme agieren, also je weniger sie direkter menschlicher Steuerung unterliegen, desto weniger eindeutig lassen sich ihre Aktionen einem menschlichen Akteur zuordnen. Das wird immer dann problematisch, wenn solche Systeme Schaden anrichten: Wer trägt dann die Verantwortung? Diese Frage wird virulent, da die Maschinen selbst natürlich nicht zur Rechenschaft gezogen werden können, zumindest solange sie nur über operationelle Autonomie und deshalb nicht über Handlungsvermögen im strengen philosophischen Sinne verfügen (Kasten 2.1; Hilgendorf 2012; Koch/Rinke 2017, S. 157 f.). Insofern es also immer schwieriger wird, »menschliche Akteure zu den Vollzügen des Roboters in Verbindung zu bringen« (Koch/Rinke 2017, S. 156), wird zunehmend unklar, wer für die Folgen geradezustehen hat – mit weitreichenden rechtlichen und moralischen Implikationen. Dieses Problem ist auch als »Verantwortungslücke« (»responsibility gap«, siehe z. B. Johnson 2015; Sparrow 2007) bekannt. Es wird generell intensiv diskutiert, vor allem mit Bezug auf Fragen der zivilrechtlichen Haftung (für einen Überblick Hilgendorf 2014). Letztlich geht es um die Frage, wer die in ihrem Ausmaß teils noch unbekannten Haftungsrisiken, die mit dem Einsatz dieser neuen Technologien verbunden sind, zu tragen hat.

Mit Blick auf AWS ist die Verantwortungsthematik sogar von besonderer Brisanz, da wir es hier mit Geräten zu tun haben, die mit einer enormen Eingriffstiefe ausgestattet sind. Was auf dem Spiel steht, ist das Leben von Menschen. Wie bereits dargelegt wurde, ist u. a. fraglich, ob und inwiefern AWS in der Lage sein werden, die Regeln des humanitären Völkerrechts einzuhalten. Auch wenn es gelingen sollte, ein System zu schaffen, das den diesbezüglich relevanten Anforderungen Folge zu leisten vermag, sind Fehlfunktionen aufgrund von Programmierfehlern oder technischem Versagen selbstverständlich nie ganz auszuschließen – mit den entsprechenden tödlichen Folgen bis hin zu möglichen Kriegsverbrechen. Insofern ist es nicht erstaunlich, dass die Frage der Verantwortung auch in der ethischen Debatte über AWS größeren Raum einnimmt. Selbst Arkin (2010, S. 339), der ja bekanntlich die These vertritt, dass ein Einsatz von AWS die Zahl an unschuldigen Opfern verringern könnte, sieht die Frage der Verantwortung als eines der großen ungelösten Probleme an.

In der Debatte wird allerdings nicht immer klargestellt, was genau mit *Verantwortung* gemeint ist (dazu und zum Folgenden Koch/Rinke 2017, S. 157). Verantwortung fällt einem Verantwortungsträger – also einem moralischen Akteur – nicht einfach zu, sondern sie ist nur inhaltlich bestimmbar innerhalb von sozialen Verantwortungskontexten. Das heißt, es bedarf stets mehrerer Personen, die in eine soziale Praxis des Verantwortlichmachens involviert sind. Gerade auch mit Blick auf AWS ist dabei wichtig, zwischen rechtlichen und moralischen Kontexten der Verantwortungszuschreibung zu unterscheiden. Denn nicht alles, was rechtlich legitim ist, erscheint auch moralisch richtig; und um-

gekehrt ist nicht alles, was rechtlich geahndet wird, auch moralisch verwerflich. Aus rechtlicher und moralischer Sicht gehört es zwar zentral zur Verantwortungspraxis, Verantwortlichkeit an Handlungsurheberschaft (alternativ an die Urheberschaft von Handlungsunterlassungen) zu binden. Während die rechtliche Verantwortung jedoch stärker auf juristischen Normsetzungen beruht und vor allem die Folgen von Handlungen bewertet (auf Basis empirischer Evidenz), ist moralische Verantwortung primär (wenn auch nicht ausschließlich) auf die Gründe von Handlungen bezogen (Voßenkuhl 1983, S. 137). Unterschiede bestehen auch hinsichtlich des Umgangs mit Schuld und Verantwortung: Rechtliche Vergehen sind zwar üblicherweise sanktioniert, die resultierende Schuld lässt sich dafür aber im Rahmen der dafür vorgesehenen institutionalisierten Verfahren tilgen; bei moralischer Verantwortung besteht diese Möglichkeit nicht.

8.3.1 Rechtliche Sicht

Das humanitäre Völkerrecht kann seine Funktion – den Schutz von Menschen und Sachen vor Kriegsauswirkungen – letztlich nur erfüllen, wenn Rechtsverstöße geahndet und sanktioniert werden (Geiß 2015, S. 21). Die Identifizierung von Verantwortlichen ist dafür zentral. Wenn nun AWS für die von ihnen begangenen Vergehen selbst nicht zur Rechenschaft gezogen werden können, wie bereits argumentiert wurde, stellt sich die Frage, wer ansonsten haftbar gemacht werden kann. Naheliegend ist, sich dabei an die Staaten zu wenden, die die Systeme eingesetzt haben – schließlich ist das humanitäre Völkerrecht ein Regelwerk, das zwischenstaatliche Beziehungen zum Gegenstand hat und somit auch nur Staaten als Rechtssubjekte adressiert. Der Fall der Staatenverantwortlichkeit wurde bereits in Kapitel 7.2 erläutert. Hier soll nun etwas genauer beleuchtet werden, inwiefern es möglich ist, im Rahmen des Strafrechts oder des Zivilrechts auch individuelle Akteure verantwortlich zu machen (zum Folgenden Geiß 2015, S. 21 ff.):

- Kommt es durch AWS zu Verletzungen des Völkerrechts, so kommt unter bestimmten Bedingungen eine *strafrechtliche Verantwortung* derjenigen Einzelpersonen in Betracht, welche die Systeme zum Einsatz gebracht haben – das sind in der Regel die verantwortlichen militärischen Befehlshaber. Für die Verfolgung von Völkermord, schweren Kriegsverbrechen sowie Verbrechen gegen die Menschlichkeit ist seit 2002 der Internationale Strafgerichtshof in Den Haag zuständig, der allerdings nur dann tätig wird, wenn diese Delikte auf nationaler Ebene nicht verfolgt werden (Steinke 2018). Um das deutsche Strafrecht an die Statuten des Internationale Strafgerichtshofs

anzupassen (sogenanntes Rom-Statut[97]), wurde 2002 das Völkerstrafgesetzbuch (VStGB) erlassen. Demnach sind militärische Befehlshaber insoweit für Völkerrechtsverstöße verantwortlich, als sie völkerrechtswidrige Aktionen entweder selbst direkt anordnen – und zwar in vollem Bewusstsein der Konsequenzen (§ 11 Absatz 1 VStGB) – oder sich vorsätzliche oder fahrlässige Verletzungen der Aufsichtspflicht zuschulden kommen lassen (§ 14 VStGB). Ein Kommandeur, der ein autonomes Waffensystem ins Feld schickt, müsste also vorab wissen, dass es Kriegsverbrechen begehen wird oder diese zumindest fahrlässig in Kauf genommen haben – nur dann ist er strafrechtlich für dessen Verfehlungen verantwortlich.[98] Da sich AWS gerade durch weitgehende Eigenständigkeit bei der Wahl ihrer Ziele auszeichnen, dürfte es mit zunehmender Verbreitung dieses Waffentyps immer schwerer fallen, militärischen Befehlshabern eine strafrechtliche Verantwortung in diesem Sinne eindeutig nachzuweisen (siehe dazu Geiß 2015, S. 22; Sparrow 2007, S. 69 ff.).

› Außerdem können gegen den Hersteller/Programmierer eines AWS auch auf *zivilrechtlicher Ebene* Haftungsansprüche geltend gemacht werden, beispielsweise im Rahmen einer verschuldensunabhängigen Produkthaftung, wie sie in den EU-Staaten gilt.[99] Voraussetzung ist, dass ein völkerrechtlicher Verstoß eindeutig auf ein fehlerhaftes Produkt zurückzuführen ist;[100] unabhängig davon, ob der Hersteller für den Produktfehler verantwortlich ist oder nicht, kann er dann prinzipiell für den resultierenden Schaden haftbar gemacht werden. Derartige Haftungsregeln könnten die Hersteller zur Einhaltung hoher Qualitäts- und Sicherheitsstandards motivieren (Geiß 2015, S. 23). Die Schwierigkeit liegt jedoch darin, dass es im Zivilrecht den Geschädigten obliegt, eine Haftungsklage gegen den Hersteller anzustrengen und, schwieriger noch, auch den ursächlichen Zusammenhang zwischen Produktfehler und Völkerrechtsverstoß zu beweisen. Gerade Letzte-

97 Das Rom-Statut wurde bislang von 123 Staaten ratifiziert (Stand 2020; ICC o. J.). Gerade diejenigen Staaten, die über die größte militärische Macht verfügen und auch bei der Entwicklung von AWS eine entscheidende Rolle spielen, nämlich China, Russland und die USA, haben sich bislang geweigert, den Internationalen Strafgerichtshof anzuerkennen.

98 Beispielsweise durch Verletzung von Sorgfaltspflichten wie der mangelhaften Wartung/Instandhaltung oder durch Missachtung der vorgesehenen Zweckbestimmung; Ähnliches gilt im Übrigen für die Hersteller (oder Programmierer) der Waffensysteme, die ebenfalls für deren Verfehlungen im Einsatz strafrechtlich zur Verantwortung gezogen werden können – vorausgesetzt, sie haben diese Verfehlungen vorsätzlich oder zumindest fahrlässig herbeigeführt (z. B. durch absichtliche Fehlprogrammierung oder fahrlässige Missachtung von Sicherheitsstandards etc.; Geiß 2015, S. 22).

99 Auf Basis der Richtlinie 85/374 EWG zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Haftung für fehlerhafte Produkte, die in Deutschland mittels des Gesetzes über die Haftung für fehlerhafte Produkte (Produkthaftungsgesetz – ProdHaftG) umgesetzt wurde.

100 Ob Soft- oder Hardware betroffen sind, spielt dabei keine Rolle, wenn beides vom selben Hersteller stammt. Ansonsten bürgt für Softwarefehler der Softwarehersteller, für Hardwarefehler der Hersteller der Hardware.

res ist bei autonomen Waffensystemen, deren technisches Innenleben von hoher Komplexität ist und zudem noch weitreichenden Geheimhaltungspflichten unterliegen dürfte, für Einzelpersonen praktisch ein Ding der Unmöglichkeit.

Folglich lässt sich konstatieren, dass sich auf rechtlicher Ebene im Umgang mit AWS eine Verantwortlichkeitslücke deutlich abzuzeichnen beginnt. Geiß (2015, S. 22) sieht darin ein »strukturelles Problem«, da die Zuschreibung von Verantwortung bedingt, dass eine Form von Kontrolle ausgeübt wird (Betzler/Scherrer 2016). Je mehr sich Waffensysteme also menschlicher Steuerung entziehen, desto schwieriger wird es fallen, menschliche Entscheidungsträger für die von ihnen begangenen Vergehen rechtlich zur Rechenschaft zu ziehen.

Es wäre jedoch voreilig, daraus ein grundsätzliches Rechtsproblem abzuleiten. Tatsache ist: Die bestehenden straf- und zivilrechtlichen Normen stammen noch aus einer Zeit, in der das Verhalten von Maschinen mechanisch weitgehend determiniert und damit vorhersehbar war. Die beschriebene Problematik verweist demzufolge vor allem auf die Defizite des bestehenden Rechtsrahmens sowie die Notwendigkeit, diesen an die neuen technologischen Entwicklungen anzupassen (Hilgendorf 2012). Das Ziel müsste sein, neue Rechtspraktiken zu entwickeln, die der technischen Komplexität autonomer Systeme angemessen sind, und zu verlangen, dass maschinelle Autonomie transparent ausgestaltet wird (Noorman/Johnson 2014). Mögliche Lösungsansätze werden bereits seit einiger Zeit intensiv diskutiert, u. a. vom Europäischen Parlament (EP 2017) oder der Ethik-Kommission Automatisiertes und vernetztes Fahren (Ethik-Kommission 2017). Zwar geschieht dies vor allem mit Blick auf zivile Einsatzbereiche autonomer Systeme, die zugrundeliegenden Konzepte lassen sich in der Regel problemlos auf militärische Einsatzbereiche übertragen; so etwa die Idee, Roboter mit einem Modul auszustatten, in dem »die Daten über jede von der Maschine ausgeführte Aktion – einschließlich der logischen Abfolgen, die zu etwaigen Entscheidungen geführt haben – gespeichert sind« (EP 2017, S. 11).[101] Zusammen mit dem verstärkten Fokus auf ethische Technikgestaltung würde es diese Maßnahme erleichtern, nachträglich nachzuvollziehen, ob der Schadensfall auf menschliches Versagen (z. B. Programmierfehler) oder sogar Vorsatz zurückzuführen ist (Müller 2016). Zudem scheint naheliegend, dass sich künftig die rechtliche Haftbarkeit im Zusammenhang mit autonomen Systemen weniger an konkretem Verschulden und mehr an der abstrakten Gefährdung festmachen sollte, eine Praxis, die z. B. in Bezug auf Tierhalter bereits gängig ist

101 Die militärische Geheimhaltung steht diesem Verfahren zunächst entgegen. Eine Lösungsmöglichkeit könnte darin bestehen, die Maschinendaten fälschungssicher aufzuzeichnen, wie von Gubrud/Altmann (2013) vorgeschlagen, sodass sie später von einer internationalen Organisation vertraulich überprüft werden könnten (Altmann 2017, S. 802). Dieses Vorgehen ließe sich jedoch nur im Rahmen eines internationalen Abkommens etablieren.

(§ 833 Bürgerliches Gesetzbuch). Das würde dann demjenigen, der autonome Systeme zum Einsatz bringt, bei AWS also dem verantwortlichen Kommandeur, automatisch – also im Sinne einer verschuldensunabhängigen Gefährdungshaftung (Kap. 7.2) – die Verantwortung für die Risiken aufbürden, die damit verbunden sind (Geiß 2015, S. 22 f.).

8.3.2 Moralische Sicht

Was in der juristischen Praxis möglich ist, nämlich die soziale Verantwortung für einen Schaden jemandem zuzuweisen, der keine konkrete Schuld dafür trägt, ist aus moralischer Sicht keine Option. Grundlage für moralische Verantwortung ist die bereits angesprochene Handlungsurheberschaft, die wiederum eng mit der Idee der Willensfreiheit zusammenhängt (Kasten 2.1). Nur vor dem Hintergrund der Vorstellung, dass man auch hätte anders handeln können, ergibt moralische Verantwortlichkeit Sinn. Koch und Rinke (2017, S. 157) geben folgendes Beispiel: Wenn jemand geschubst, also bloß als Körper bewegt wird, wird man ihm die körperliche Bewegung nicht zuschreiben und ihn dementsprechend auch nicht für deren Folgen verantwortlich machen (allenfalls wird man ihn dafür verantwortlich machen, dass er sich in eine Situation gebracht hat, in der er leicht geschubst werden konnte). Das ist der Grund, wieso es auch keinen Sinn ergibt, autonome Maschinen für ihre Taten zu bestrafen: Sie verfügen nicht über eine Form der Selbstbestimmung, die von Freiwilligkeit und Wissen um die Konsequenzen getragen ist (Fischer/Ravizza 1998).

Was wäre die Folge, sollte die Autonomisierung der Waffentechnologie weiter voranschreiten? Bis auf wenige Ausnahmefälle, in denen sich die tödlichen Aktivitäten autonom agierender Waffensysteme klar auf menschlichen Vorsatz oder Fahrlässigkeit zurückführen lassen (sei es des Programmierers oder des Kommandeurs), würde die Frage der moralischen Verantwortung für die Opfer zunehmend diffus. Jemanden für die Opfer die moralische Verantwortung zuzuschieben, der keine konkrete Schuld daran trägt, vermag die Verantwortungslücke zwar aus rechtlicher (vgl. das Konzept der Gefährdungshaftung), nicht jedoch aus moralischer Sicht zu schließen. Denn schuldig im moralischen Sinne fühlen sich Menschen aus den zuvor genannten Gründen in der Regel nur für Dinge, die sie selbst getan haben (oder zu denen sie durch Unterlassen beigetragen haben) (Koch/Rinke 2017, S. 129).

Angesichts dessen wird in der Literatur argumentiert, dass mit dem Aufkommen von AWS eine Verantwortungslücke zu entstehen droht, die vor allem aus ethischer Sicht problematische Konsequenzen mit sich bringt (z. B. Sparrow 2007). Denn offensichtlich ist die Entscheidung, einen anderen Menschen zu töten, eine der moralisch schwerwiegendsten, die man treffen kann. Insofern ist die Vorstellung, dass niemand für eine solche Entscheidung (bzw. die anschließende Tat) die moralische Verantwortung zu übernehmen hätte, durchaus

beunruhigend. Würden AWS eingesetzt, entsteht laut Sparrow (2007, S. 68) eine Situation, in der sich das technisch vermittelte Töten von Menschen wie ein zufälliges Naturereignis oder ein Unfall ausnimmt. Es gibt dann niemanden mehr, der dies mit seinem Gewissen vereinbaren muss, was eine tiefe Missachtung des Wertes eines Menschenlebens zum Ausdruck bringt (Sparrow 2016, S. 108). Aus ähnlichen Gründen plädiert der Philosoph Alexander Leveringhaus (2016, S. 89 ff.) dafür, die menschliche Entscheidungsfähigkeit in einem bewaffneten Konflikt für ein hohes und schützenswertes Gut anzusehen (dazu und zum Folgenden Koch/Rinke 2017, S. 127 ff.). Gerade weil menschliches Leben kostbar und generell schützenswert ist, so Leveringhaus, soll es immer auch die Möglichkeit geben, von einer Tötungsentscheidung zurückzutreten. Die Fähigkeit, barmherzig zu sein und Gnade zu zeigen, ist zweifelsohne eine hohe moralische Tugend. Das heißt nicht, dass es immer richtig ist, dieser Tugend Folge zu leisten (es wäre z. B. falsch, einen Attentäter nicht zu erschießen, bevor er seinen Sprengsatz zur Detonation bringen kann). Aber selbst wenn es in einem kriegerischen Ernstfall zur Anwendung von Waffengewalt kommt, sollte dies laut Leveringhaus (2016) immer eine direkte menschliche Entscheidung sein, für die ein menschlicher Akteur letztlich auch moralisch einzustehen hat (dazu auch Asaro 2012, S. 701).

Vor diesem Hintergrund vertreten die zitierten Experten die Ansicht, dass AWS ethisch verwerflich sind und deshalb nicht eingesetzt werden sollten. Dies zeigt, dass die Implikationen der moralischen Verantwortlichkeitslücke deutlich weitreichender sind als diejenigen ihres rechtlichen Gegenstücks: Die rechtliche Verantwortungslücke wird erst relevant, wenn ein Verstoß gegen Recht und Gesetz vorliegt (beispielsweise ein Kriegsverbrechen, das es strafrechtlich zu ahnden gilt). Ein generelles Verbot von AWS lässt sich daraus schwerlich ableiten, wie bereits argumentiert wurde, sofern es gelingt, die rechtliche Praxis der Verantwortungszuschreibung an die Herausforderungen autonomer Technologien anzupassen (dazu auch Koch/Rinke 2017, S. 159 f.). Aus moralischer Sicht stellt sich die Frage der Verantwortlichkeit jedoch ganz grundsätzlich und insbesondere unabhängig davon, ob der Tötungsakt unter den gegebenen Umständen legal ist oder nicht. Das Töten selbst ist ein moralisch problematischer Akt, über den es zumindest vor dem eigenen Gewissen Rechenschaft abzulegen gilt. Tötungsmaschinen zu konstruieren und in Gang zu setzen, die mittels ihrer Autonomie genau diese menschliche Praxis des Verantwortlichmachens unterminieren, erscheint demnach als fundamental unmoralisch (Asaro 2012, S. 695).

Bei genauerer Betrachtung wird deutlich, dass die Frage nach der moralischen Verantwortlichkeit und die Frage nach der Würde des Menschen auf ähnlichen Intuitionen beruhen und eng miteinander verbunden sind (Koch/Rinke 2017, S. 105). Das Argument von der moralischen Verantwortungslücke, wie es zuvor entfaltet wurde, lässt sich auch folgendermaßen auf den Punkt bringen: Menschen zu töten, ohne dass dafür jemand verantwortlich zeichnet, heißt,

ihnen die moralische Anerkennung und Wertschätzung zu versagen, die ihnen als Wesen mit Würde zusteht. Im Umkehrschluss heißt das aber auch, dass dieses Argument ebenso voraussetzungsreich und in seiner Reichweite gleichermaßen begrenzt ist wie jenes, das eine Würdeverletzung durch AWS abzuleiten versucht. Letztlich bleiben in beiden Fällen große Unsicherheiten, die sich mit argumentativen Mitteln nicht restlos auflösen lassen (Koch/Rinke 2017, S. 166). So sieht etwa Birnbacher (2016, S. 120), der wie geschildert dem Argument einer spezifischen Würdeverletzung durch AWS skeptisch gegenübersteht, auch unter der Perspektive der Verantwortungsproblematik keinen zwingenden Grund, der gegen einen Einsatz autonomer Waffensysteme spricht. Und andere Autoren wie der Philosoph Vincent C. Müller (2016) bestreiten generell, dass die Existenz einer Verantwortungslücke den Einsatz autonomer Technologien im Allgemeinen und autonomer Waffensysteme im Speziellen moralisch ausschließt.

8.4 Fazit

Die Entwicklung und der mögliche Einsatz von immer autonomer agierenden Waffensystemen schafft große normative Unsicherheiten, die sich in der Kernfrage zuspitzen, ob und inwiefern es erlaubt sein soll, Maschinen über Tod oder Leben von Menschen entscheiden zu lassen. Es ist völlig klar, dass diese Fragestellung nur mit Blick auf die besondere Situation, wie sie im Kriegsfall herrscht, überhaupt zulässig erscheint. Doch selbst in Kriegen gibt es Grenzen des Erlaubten, die sicherstellen sollen, dass ein gewisses Maß an Menschlichkeit gewahrt bleibt. Autonome Waffensysteme fordern diese Grenzen heraus, indem sie zum einen die Entscheidungs- und Handlungshoheit des Menschen in diesem ethisch-humanitären Ausnahmebereich zu untergraben drohen (Heyns 2016, S. 13) und zum anderen den Anwender militärischer Gewalt gänzlich der Gegengewalt entziehen (Koch/Rinke 2017, S. 7). Damit stellen sie letztlich den normativen Hintergrund infrage, der bis heute für bewaffnete Konflikte geradezu selbstverständlich angenommen wird.

Der Überblick über die weitverzweigte Debatte in Koch und Rinke (2017) zeigt, dass AWS aus ethischer Sicht zwar kontrovers diskutiert werden, insgesamt aber doch die Zweifel an ihrer Zulässigkeit und Legitimität deutlich überwiegen. Im Kern dreht sich die ethische Debatte um zwei zentrale Streitpunkte:

1. Inwiefern vermögen AWS die völkerrechtlich geforderten Standards im Krieg einzuhalten? Befürworter autonomer Waffentechnologie sehen die Chance, dass AWS dank ihrer überlegenen sensorischen und datenverarbeitenden Fähigkeiten sogar zu einer Verbesserung der humanitären Situation gegenüber dem Status quo beitragen könnten. Die Kritiker wenden dagegen ein, dass diese Annahme auf der fälschlichen Prämisse beruht, die

komplexen und interpretationsbedürftigen Regularien des humanitären Völkerrechts ließen sich eins zu eins in Computercodes transferieren. Dies erscheint als starkes Argument gegen die Möglichkeit völkerrechtskonformer AWS, das es erst einmal zu widerlegen gälte. Letztlich beruht die Entscheidung in dieser konsequentialistischen Frage jedoch weniger auf ethischen Einschätzungen als auf solchen technischer Art, die zum jetzigen Zeitpunkt schwierig zu treffen sind, da sich autonome Waffensysteme erst in einem frühen Stadium der Entwicklung befinden und deshalb noch nicht klar absehbar ist, was sie zu leisten vermögen und was nicht.

2. Inwiefern ist der Einsatz von AWS mit der Würde des Menschen vereinbar? Mit der Idee der Menschenwürde, die in Deutschland und in vielen anderen freiheitlich-demokratischen Gesellschaften als besonders schützenswerter Grundwert gilt, ist eine zentrale Verpflichtung verbunden: Der Mensch darf nicht zum Objekt gemacht werden. In der Debatte wird aus deontologischer Sicht das Argument vorgebracht, dass der Einsatz letaler Gewalt durch AWS ethisch grundsätzlich inakzeptabel ist, weil er genau dies impliziert. Die Opfer werden entwürdigt, indem sie in einem rein technischen Prozess zu Zielobjekten degradiert werden, ohne dass dabei die Aussicht auf Achtung ihrer Würde besteht. Das Argument bringt die starken moralischen Vorbehalte zum Ausdruck, die gegenüber einer Dehumanisierung des Krieges bestehen. Es ist jedoch theoretisch und begrifflich sehr voraussetzungsreich und seine Reichweite entsprechend umstritten.

Die Gründe und Erwägungen, die gegen AWS vorgebracht werden, sind in ihrer Gesamtheit äußerst vielgestaltig und nicht auf einen einfachen Nenner zu bringen. Aus Sicht des TAB sprechen gegen einen Einsatz von AWS vor allem zwei Überlegungen, wobei die eine konsequentialistisch ausgerichtet, die andere relativ zu bestimmten Wertegesichtspunkten ist: Erstens gilt es die unkalkulierbaren Risiken zu bedenken, die mit dem Einsatz autonom agierender Kampfmaschinen verbunden sind (Koch/Rinke 2017, S. 171 f.). Diese Risiken betreffen technische Fehlfunktionen, die ja nie ganz auszuschließen sind und im Falle von autonom agierenden Waffensystemen dramatische Folgeschäden nach sich ziehen können. In Betracht zu ziehen ist aber auch eine Destabilisierung der internationalen Sicherheitsarchitektur, ausgelöst durch einen möglichen Rüstungswettlauf und erhöhte Kriegsrisiken (zu diesen sicherheitspolitischen Fragen siehe Kap. 6). Angesichts dessen ist höchst fraglich, ob der mit der Einführung dieser Systeme verbundene Kontrollverlust verantwortbar ist, auch wenn die Risiken in ihrem Umfang zum jetzigen Zeitpunkt noch nicht eindeutig zu bemessen sind. Zweitens hat sich Deutschland verfassungsrechtlich dazu verpflichtet, das Gebot der Menschenwürde uneingeschränkt zu achten und zu schützen. Das Argument von der Würdeverletzung ist für den deutschen Staat also von besonderem Gewicht, und selbst wenn Zweifel an der Reichweite des zugrundeliegenden Arguments bestehen, sollte die bloße Möglichkeit eines

Würdeverstoßes für die Bundesregierung und andere staatliche Akteure Anlass genug sein, von der Entwicklung und dem Einsatz dieses Waffentyps abzusehen und auf ein internationales Verbot hinzuwirken.

Gerade der letzte Punkt macht allerdings auch deutlich, dass es nicht die Aufgabe von Ethik ist, im Sinne eines »Ethik-TÜVs« (Riecke 2018) oder nach Art einer »Genehmigungsbehörde« (Grunwald 2013, S. 6) kategorische Urteile über die ethisch-moralische Bedenklichkeit oder Unbedenklichkeit einer Technologie zu fällen (dazu auch Koch/Rinke 2017, S. 6 ff.). Dies ist schon alleine deshalb so, weil ethische Urteile immer von bestimmten theoretischen und normativen Prämissen abhängen und deshalb niemals eindeutig sein können. Die Ethik vermag deshalb die mit dem technologischen Wandel verbundenen normativen Unsicherheiten nicht aufzulösen, sie kann nur deren moralische Hintergründe reflektieren und zu klären versuchen (Grunwald 2013).

Mit Blick auf AWS ist die Ethik dabei allerdings mit der besonderen Schwierigkeit konfrontiert, dass das zentrale Definitions- und Abgrenzungsmerkmal dieses Waffentyps, nämlich die Autonomie, von großen begrifflichen Unschärfen geprägt ist. So hängt die ethische Bewertung von AWS maßgeblich davon ab, welches Verständnis (moralisch oder operationell) und welcher Grad von Autonomie (teilautonom oder vollautonom) zugrunde gelegt wird. Dass man es hier mit fließenden Übergängen zu tun hat, erschwert die ethische Beurteilung außerordentlich. Klar ist, dass sich die meisten der vorab diskutierten ethischen Bedenken in Luft auflösen, sollte es gelingen, AWS zu konstruieren, bei denen eine adäquate menschliche Kontrolle des Waffeneinsatzes (inklusive Zielauswahl) sichergestellt ist. Doch wie die CCW-Verhandlungen zeigen (dazu Kap. 9.2), ist die Rede von der adäquaten menschlichen Kontrolle bislang eine ebenso unklare Formel wie die Rede von starker KI, die über menschliche Handlungsqualitäten verfügt. Diese Situation erschwert nicht nur die ethische Bewertung, sondern auch die rechtliche Regulierung der Technologie. Denn sowohl für ein generelles Verbot autonomer Waffen als auch für die Etablierung technischer und/oder operationeller Standards, die einen ethischen Umgang mit den technologischen Möglichkeiten sicherstellen sollen,[102] werden Kriterien benötigt, die Waffensysteme gemäß ihren Autonomiefähigkeiten – und damit ihrer moralischen Qualität – differenziert einzuordnen vermögen (Hellström 2013). Sich diesbezüglich auf relevante Unterscheidungs- und Klassifikationsmerkmale zu einigen, wäre deshalb ein wichtiger erster Schritt, um mit den anstehenden ethischen Herausforderungen umgehen zu können.

102 Mögliche Maßnahmen umfassen beispielsweise die Ausstattung mit einer Blackbox, die alle relevanten Betriebsdaten aufzeichnet (Kap. 9.3.3), oder technische Vorkehrungen, welche die letalen Einsatzmöglichkeiten begrenzen oder bestimmte riskante Einsatzzwecke gänzlich unterbinden (siehe die Ausführungen zu »boxed autonomy« in Kasten 7.1).

9 Möglichkeiten der Rüstungskontrolle

Autonome Waffensysteme (AWS) werden bislang von keinem Rüstungskontrollvertrag explizit erfasst. Dies ist nachvollziehbar, denn die bestimmende Eigenschaft, die AWS von anderen Waffensystemen abgrenzt, nämlich ihre *Autonomie,* war zum Zeitpunkt der Aushandlung dieser Abkommen im Bereich von Science-Fiction angesiedelt und spielt deshalb in den bestehenden Abkommen keine Rolle. Dennoch lassen sich AWS – genauso wie unbemannte (fernpilotierte bzw. -überwachte) Waffensysteme (UWS) – analog zu Marschflugkörpern, Kampfflugzeugen oder Kampfpanzern als Trägersysteme auffassen, die unter bestimmten Voraussetzungen, beispielsweise oberhalb einer bestimmten Größe oder bei Bestückung mit bestimmten Wirkmitteln, unter bestehende internationale Abkommen subsumiert werden können.

Der Fragenkomplex, ob bzw. in welcher Hinsicht Autonomie in Waffensystemen problematisch für die Erhaltung von Frieden, Sicherheit und Menschenwürde ist und wie diese ggf. reguliert werden könnte, ist derzeit Gegenstand eines intensiven Gedankenaustauschs auf internationaler Ebene. Dieser wird mit Fokus auf die Frage der Vereinbarkeit von AWS mit dem humanitären Völkerrecht im Rahmen der CCW in Genf geführt.

9.1 Rüstungs- und Exportkontrollabkommen mit Relevanz für AWS

Im Folgenden werden die relevanten Abkommen daraufhin geprüft, ob sie Sachverhalte bzw. Regelungen enthalten, die auch auf AWS anwendbar sein können.[103] Die in Bezug auf Trägersysteme oder Waffenplattformen relevanten *Rüstungskontrollverträge* sind:

- der KSE-Vertrag,
- der New-START-Vertrag,
- der INF-Vertrag sowie
- das Chemie- und das Biowaffenübereinkommen.

Im Bereich der Transparenz sowie vertrauens- und sicherheitsbildender Maßnahmen (VSBM) sind zu nennen:

- das Wiener Dokument und
- das UN-Waffenregister.

Außerdem sind im Hinblick auf die *Nichtverbreitung und Exportkontrolle* einschlägig:

103 Das folgende Kapitel stützt sich wesentlich auf das Gutachten von Alwardt et al. 2017.

- das Trägertechnologie-Kontrollregime,
- der Haager Verhaltenskodex gegen die Proliferation ballistischer Raketen,
- das Wassenaar-Abkommen und
- der Vertrag über den Waffenhandel.

9.1.1 Rüstungskontrollverträge

KSE-Vertrag

Der Vertrag über konventionelle Streitkräfte in Europa (KSE-Vertrag) wurde 1990 unterzeichnet und trat 1991 in Kraft. Er gilt innerhalb eines geografischen Bereichs, der sich »vom Atlantik bis zum Ural« erstreckt. Ausgehandelt durch die beiden Militärallianzen des Kalten Krieges, die NATO und den Warschauer Pakt, wurden im KSE-Vertrag u. a. gleiche numerische Obergrenzen für Hauptwaffensysteme festgeschrieben. Diese umfassen Kampfpanzer, gepanzerte Kampffahrzeuge, Artilleriewaffen, Kampfflugzeuge und Angriffshubschrauber. Der KSE-Vertrag kann als der erste und bisher einzige Rüstungskontrollvertrag angesehen werden, der konventionelle Waffensysteme umfassend einschränkt und über Verifikationsmechanismen (z. B. Informationsaustausch und Inspektionen) verfügt. Im November 1999 wurde der Versuch unternommen, den KSE-Vertrag an die veränderten Realitäten nach dem Ende des Ost-West-Konflikts, der Auflösung des Warschauer Pakts und der NATO-Erweiterung anzupassen (A-KSE-Vertrag). Der A-KSE-Vertrag wurde von den NATO-Staaten jedoch nicht ratifiziert, da nach ihrer Auffassung Russland nicht alle vertraglichen Verpflichtungen erfüllt hatte. Russland suspendierte den ursprünglichen KSE-Vertrag 2007. Als Gründe wurden die A-KSE-Nichtratifizierung und die US-Raketenabwehrpläne in Europa angegeben. Am 11. März 2015 wurde der Vertrag seitens der Russischen Föderation aufgekündigt.[104]

Der KSE-Vertrag ist somit de facto obsolet. Im Rahmen eines *strukturierten Dialogs* sollen im Kontext der Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE) Möglichkeiten für Nachfolgeregelungen ausgelotet werden. Der strukturierte Dialog wurde auf deutsche Initiative hin etabliert und stellt ein Forum dar, in dem sich die OSZE-Mitglieder regelmäßig über Bedrohungswahrnehmungen, militärische Übungen und Rüstungskontrollmechanismen austauschen (Heinrich 2018). Die Bundesregierung moderiert diesen Prozess.

Unbemannte Waffensysteme werden im KSE-Vertrag nicht explizit beschrieben. Da bei der Definition der jeweiligen aufgeführten Waffensysteme aber auch keine Besatzung erwähnt oder festgeschrieben wird, können die Definitionen sowohl für bemannte als auch für unbemannte Waffensysteme als

104 Formal handelt es sich nicht um einen offiziellen Rücktritt vom Vertrag nach Artikel XIX Absatz 2 oder Absatz 3, sondern um den Beschluss, »seine Handlungen im Vertrag ab 11. März 2015 vollständig einzustellen« (RT 2015).

gültig angesehen werden.[105] Im Rahmen eines Nachfolgeregimes könnten UWS/AWS explizit aufgenommen werden. Angesichts der aktuellen Spannungen zwischen dem Westen und Russland ist eine Neuregelung zurzeit jedoch nicht sehr wahrscheinlich.

New-START-Vertrag

Der New-START-Vertrag (Treaty between the United States of America and the Russian Federation on Measures for the Further Reduction and Limitation of Strategic Offensive Arms) ist ein bilateraler Rüstungskontrollvertrag zu strategischen Nuklearwaffen[106] zwischen den USA und Russland, unterzeichnet im April 2010 und in Kraft getreten im Februar 2011. Er limitiert die Anzahl der stationierten strategischen Trägersysteme (»intercontinental ballistic missile« – ICBM; landgestützte ballistische Interkontinentalraketen, auf U-Booten stationierte ballistische Raketen – SLBM und schwere Bomber) auf 700 Stück pro Land. Auf Basis der stationierten Trägersysteme wird die entsprechende Anzahl der stationierten strategischen Nukleargefechtsköpfe berechnet, die 1.550 Stück pro Seite nicht überschreiten darf. Der New-START-Vertrag listet unter Artikel 3 Absatz 8 die bis dato vorhandenen strategischen Trägersystemtypen beider Seiten auf. Der Vertrag sieht Verifikationsmechanismen vor und hat eine 10-jährige Laufzeit (bis 2021), die im Konsens um weitere 5 Jahre verlängert werden kann.

Im Zentrum des Vertrags stehen Bomber und ballistische Raketen mit großer Reichweite. Hyperschallflugkörper, die von Raketen in den Weltraum transportiert werden und auf einer eigenständigen Flugbahn ihr Bodenziel ansteuern, fallen nicht unter die Regelungen des New-START-Vertrags. Besonders von russischer Seite besteht die Sorge, dass dies eine Lücke bei der strategischen bilateralen Rüstungskontrolle darstellt, die die Stabilität der Abschreckungspotenziale unterminiert. Solche Trägersysteme mit großer Reichweite wären ähnlich wie Marschflugkörper prädestiniert für die Integration von teilautonomen Komponenten, die selbstständig Ziele ansteuern.

Neue Trägersysteme müssen auf Verlangen einer Vertragspartei nach Artikel 5 des Vertrags daraufhin geprüft werden, ob sie die Kriterien eines strategischen Trägersystems erfüllen und daher auch unter den New-START-Vertrag fallen. Dieses würde auch für unbemannte Trägersysteme wie UCAVs oder UUVs gelten, die strategische Reichweiten aufweisen und nuklear bewaffnet werden können. Solche unbemannten strategischen Flugkörper oder unbemannten, mit Raketen bestückten Unterseeboote müssten, falls sie diese

105 Artikel II KSE-Vertrag, offenbar wurde seinerzeit bewusst auf eine Erwähnung von Besatzung verzichtet, da während der Verhandlungen befürchtet wurde, künftige unbemannte Systeme könnten die Vertragsbegrenzungen aushebeln (Richter 2013, S. 2).

106 Dies bezeichnet »Kernwaffen mit großer Sprengkraft, die nicht auf dem Gefechtsfeld eingesetzt werden, sondern Ziele im gegnerischen Hinterland zerstören sollen« (Wikipedia 2002).

Kriterien erfüllen, im Rahmen des New-START-Vertrags oder eines Nachfolgevertrags berücksichtigt werden. Die Zukunft von New START über 2021 hinaus ist ungewiss, da beide Vertragsparteien eine Verlängerung derzeit offenlassen (Gramer/Seligman 2019, siehe auch AMF 2020).

INF-Vertrag

Der INF-Vertrag (Treaty Between The United States Of America And The Union Of Soviet Socialist Republics On The Elimination Of Their Intermediate-Range And Shorter-Range Missiles – INF Treaty) zwischen den USA und Russland, 1987 unterzeichnet und 1988 in Kraft getreten, ist der bisher einzige Rüstungskontrollvertrag, der eine komplette Kategorie an Trägersystemen komplett verbietet. Er umfasst bodengestützte Kurz- und Mittelstreckenraketen sowie Marschflugkörper mit Reichweiten zwischen 500 und 5.500 km, deren Bestände von den USA und Russland bis 1991 vollständig und verifiziert abgerüstet wurden. Russland reklamiert, dass UCAVs, die im INF-Vertrag zwar nicht explizit erwähnt werden, unter die Definition bodengestützter Marschflugkörper fallen würden (Thielmann/Zagorski 2017, S. 3 f.). Die USA widersprechen dem mit der Argumentation, dass unbemannte Systeme »die nicht bodengestützt sind oder aber ohne Hilfe von Startvorrichtungen abheben können und die dafür vorgesehen sind, von einer Mission zurückzukehren«,[107] nicht in die Kategorie eines bodengestützten Marschflugkörpers fallen (DOD 2009, S. 42). Insofern ist umstritten, ob UCAVs vom Geltungsbereich des INF-Vertrags erfasst werden. Nachdem sich die USA und Russland gegenseitig vorgeworfen hatten, Vertragsinhalte zu verletzen (Thielmann/Zagorski 2017), suspendierten Anfang Februar 2019 zuerst die USA und sodann auch Russland den INF-Vertrag (BBC News 2019). Nach Ablauf der 6-monatigen Kündigungsfrist zogen sich die USA am 2. August 2019 aus dem Vertrag zurück. Die Gefahr eines neuen Wettrüstens in Europa ist somit akuter denn je (Meier 2019).

Chemie- und Biowaffenübereinkommen

Das Chemiewaffenübereinkommen (CWÜ) von 1993 und das Biowaffenübereinkommen (BWÜ) von 1972 verbieten die Entwicklung, die Herstellung, den Besitz, die Weitergabe und den Einsatz chemischer bzw. biologischer Waffen. Dem CWÜ sind bisher 192 Staaten und dem BWÜ 178 Staaten beigetreten.[108] Beide Abkommen beinhalten auch ein Verbot von Munition, Gerät, Ausrüstung oder anderer Einsatzmittel, falls diese dazu bestimmt sind, diese Waffen

107 Im Original: »which are not ground launched, or take off without the aid of launching equipment, and are designed to return from mission«.
108 Für weitere Informationen www.auswaertiges-amt.de/DE/Aussenpolitik/Themen/Abruestung/BioChemie/Uebersicht-BCWaffen_node.html (1.9.2020)

auszubringen und in feindseliger Absicht einzusetzen. Entsprechend ausgerüstete oder bewaffnete unbemannte Trägersysteme, die dazu bestimmt sind, chemische oder biologische Waffen zum Einsatz zu bringen, sind somit laut dem CWÜ bzw. dem BWÜ verboten. Von diesen Verboten wären auch alle UWS oder AWS betroffen, die zur Ausbringung von chemischen oder biologischen Waffen vorgesehen sind. Im Sinne der Einhaltung dieser Bestimmungen ist es problematisch, dass viele Systeme modular konstruiert sind und beispielsweise Tanks und Sprühvorrichtungen zum Zweck der Ausbringung chemischer und/oder biologischer Agenzien relativ kurzfristig nachgerüstet werden können. Im Gegensatz zum BWÜ verfügt das CWÜ mit der Organisation für das Verbot chemischer Waffen (Organisation for the Prohibition of Chemical Weapons – OPCW) über ein aktives Implementierungs- und Verifikationsregime.

In Tabelle 9.1 sind die Rüstungskontrollverträge und die für AWS relevanten Regelungstatbestände in der Übersicht aufgeführt.

Tab. 9.1 Übersicht der für AWS relevanten Rüstungskontrollverträge

Vertrag	Rahmen	relevanter Regelungstatbestand	AWS Bestandteil des Vertrags?	Verifikation	Status
KSE	multilateral	Obergrenzen für konventionelle Waffen	ja, falls AWS der Definition einer der Hauptwaffentypen entsprechen	ja	obsolet seit 2015
New START	bilateral	Begrenzung strategischer Offensivwaffenträger	ja, autonome UCAVs oder UUVs, die über eine strategische Reichweite verfügen und zur nuklearen Bewaffnung vorgesehen sind	ja	in Kraft (Laufzeit bis 2021)
INF	bilateral	Abrüstung von Marschflugkörpern (500 bis 5500 km Reichweite)	umstritten, ob UCAVs ggf. Marschflugkörpern gleichzustellen sind	(ja) gilt seit 1991 als umgesetzt	gekündigt mit Wirkung zum 2.8.2019
CWÜ und BWÜ	UN	Verbot des Einsatzes chemischer und biologischer Waffen	ja, falls sie dazu bestimmt sind, am Einsatz chemischer oder biologischer Waffen mitzuwirken	ja (CWÜ); nein (BWÜ)	in Kraft

Quelle: Alwardt et al. 2017, S. 78; TAB 2011, S. 191

9.1.2 Transparenz und vertrauens- und sicherheitsbildende Maßnahmen

Wiener Dokument

Mit dem Wiener Dokument 2011 über vertrauens- und sicherheitsbildende Maßnahmen verpflichten sich alle 57 Mitgliedstaaten[109] der Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE 2011), regionale Maßnahmen zur Transparenz und Vertrauensbildung im Bereich der konventionellen Rüstung umzusetzen. Das Ursprungsdokument wurde 1990 von der Vorgängerorganisation der OSZE, der Konferenz über Sicherheit und Zusammenarbeit in Europa (KSZE), verabschiedet und seither regelmäßig überarbeitet und ergänzt.

Die Staaten verpflichten sich mit dem Wiener Dokument in Bezug auf ihre Landstreitkräfte und landstationierten Luftkräfte u. a. zu einem Informationsaustausch über die Anzahl, Stationierung und Bewegung von Truppen und Hauptwaffentypen, die Vorabmeldung von Großmanövern sowie die Vorführung neuer Typen von Hauptwaffensystemen. Hiermit einhergehend sind auch Überprüfungs- und Verifikationsmechanismen vereinbart. Darüber hinaus besteht im Hauptsitz der OSZE in der Wiener Hofburg bis heute ein wöchentlich tagendes Diskussionsforum zur Rüstungskontrolle, Vertrauensbildung, Wahlbeobachtung und Konfliktprävention.

Im Wiener Dokument werden insbesondere die Hauptwaffentypen des KSE-Vertrags wie Kampfpanzer, gepanzerte Kampffahrzeuge, Artillerie, Kampfflugzeuge und Angriffshubschrauber aufgeführt. Unbemannte Waffensysteme finden keine gesonderte Erwähnung. Da aber auch nirgendwo explizit von ausschließlich bemannten Systemen die Rede ist, würden AWS (bzw. bewaffnete unbemannte Systeme) jeweils unter die Waffenkategorien fallen, die in den Ziffern 10.2.5 (Landstreitkräfte) bzw. 10.5 (Luftstreitkräfte) spezifiziert werden. Daten zu AWS (bzw. unbemannten Systemen) müssten gemäß Ziffer 11.2 (»Daten über neue Typen oder Versionen von Hauptwaffensystemen und Großgerät«) spätestens dann übermittelt werden, wenn das betreffende System erstmals in Dienst gestellt wird.

UN-Waffenregister

Mehr Offenheit und Transparenz beim globalen Transfer von Waffen zu schaffen, ist das Ziel der UN (o. J.c) mit dem UN-Waffenregister (UN Register of Conventional Arms – UNROCA), das mit der Resolution der UN-Generalversammlung 46/36L vom 6. Dezember 1991 etabliert wurde (UN 1991). Das Register wird vom UN-Generalsekretär geführt und allen Mitgliedstaaten steht es frei, ihre Im-

109 Die Mongolei trat der OSZE erst am 21. November 2012 bei, übernahm aber mit dem Beitritt sämtliche im Wiener Dokument festgeschriebenen Verpflichtungen.

und Exporte im Bereich konventioneller Waffen zu melden. Dies bezieht sich primär auf die fünf Hauptwaffentypen des KSE-Vertrags sowie bestimmte Kriegsschiffe und Raketen/Raketenstartsysteme. Mehr als 170 Staaten haben seitdem entsprechende Daten geliefert. Seit 2006 sind auch leichte und Kleinwaffen mit einbezogen (von Revolvern über Maschinengewehre bis zu portablen Raketenwerfern). Nach eigener Angabe deckt UNROCA seit 2 Jahrzehnten etwa 90 % des globalen Waffenhandels ab.[110] Leider beteiligen sich nicht alle Staaten in vollem Umfang und die Daten sind teilweise widersprüchlich.[111]

Eine ausdrückliche Unterscheidung zwischen bemannten und unbemannten Waffensystemen erfolgte in den Definitionen der Waffenkategorien ursprünglich nicht. Daher würden UWS bzw. AWS bei Erfüllung der sonstigen Kriterien unter die jeweiligen Waffenkategorien fallen. Einem Vorschlag von Regierungsexperten folgend, wurden UCAVs 2016 als eine eigene Unterkategorie (IV b) aufgenommen (UN 2016b): »Unmanned fixed-wing or variable-geometry wing aircraft, designed, equipped or modified to engage targets by employing guided missiles, unguided rockets, bombs, guns, cannons or other weapons of destruction« (UN 2016a, S. 29). Über die Aufnahme von unbemannten Hubschraubern in die Liste der Waffenkategorien soll demnächst beraten werden. Boden- und seegestützte unbemannte Systeme (UGV, USV und UUV) werden bisher nicht gesondert erwähnt, sind per Definition aber auch nicht ausgeschlossen. Es ist damit bisher kein internationaler festgehaltener Konsens, sondern Auslegungssache, ob – von UCAVs abgesehen – auch andere unbemannte Waffenplattformen Bestandteil dieses Vertrags sind oder AWS es zukünftig sein werden.

9.1.3 Nichtverbreitung und Exportkontrolle

Trägertechnologie-Kontrollregime

Das Trägertechnologie-Kontrollregime (Missile Technology Control Regime – MTCR) wurde 1987 durch die G7 ins Leben gerufen. Das primäre Ziel ist es, durch die Kontrolle der Ausfuhr von Gütern und Technologien die Proliferation von Trägersystemen für alle Arten von Massenvernichtungswaffen einzuschränken. Es handelt sich hierbei um eine Gruppe von mittlerweile 35 Staaten, die auf informeller und freiwilliger Basis gemeinsame Exportstandards für ballistische Raketen, Marschflugkörper und UAVs erarbeiten und umsetzen.[112]

110 https://www.unroca.org/ (1.9.2020)

111 Ein Beispiel: Deutschland meldete für 2016 folgende Exporte in der Kategorie Kampfpanzer: 41 nach Indonesien, 33 nach Katar, 7 nach Singapur, 1 in die Schweiz. Indonesien und Katar übermittelten für 2016 keinerlei Importdaten. Singapur und die Schweiz gaben Berichte ab, meldeten aber keine Importe von Kampfpanzern aus Deutschland, und Spanien meldete den Import von 108 »Leopard 2«, die jedoch in der Exportbilanz Deutschlands nicht aufgeführt sind (UN 2016c, 2016d, 2016e u. 2016f).

112 http://mtcr.info/ (1.9.2020)

Allerdings beteiligen sich einige Schlüsselakteure nicht am MTCR, so z. B. China, Israel, Iran, Nordkorea oder Pakistan.[113] Indien trat 2016 als jüngstes Mitglied dem MTCR bei. Die MTCR-Regeln sind für die Mitgliedstaaten nicht unmittelbar rechtlich bindend, sondern werden typischerweise in nationales Recht umgesetzt. Bei Exporten zwischen den MTCR-Mitgliedstaaten, innerhalb der EU und NATO sowie in bestimmten Bereichen der zivilen Raumfahrt, werden die Richtlinien nicht angewendet.

Das MTCR (2017) unterscheidet zwei Kategorien von Gütern, die unterschiedlich strengen Restriktionen unterliegen und die im Detail im »Equipment, Software and Technology Annex« aufgeführt werden: Güter der Kategorie I sollen grundsätzlich gar nicht ausgeführt werden. Ausnahmen von dieser Regel können im Einzelfall zulässig sein, unter der Bedingung, dass der Importstaat Garantien abgibt, dass das Gut nur im Einklang mit den MTCR-Regeln verwendet wird. Dies betrifft komplette Raketensysteme und UAVs (einschließlich Cruise Missiles und Aufklärungsdrohnen), die eine Nutzlast von 500 kg oder mehr über mindestens 300 km tragen können, sowie deren Subsysteme und Komponenten (beispielsweise Triebwerke oder Steuerungssysteme). Der Export von Geräten oder Einrichtungen zur Produktion von Kategorie-I-Komponenten soll ausnahmslos verboten werden. Für den Export von Gütern der Kategorie II besteht ein Ermessensspielraum nicht zuletzt aus dem Grund, als es sich hierbei oft um Dual-Use-Güter handelt. Deren Export ist statthaft, solange sie nicht dazu gedacht sind, in Form eines Systems der Kategorie I oder zur Ausbringung von Massenvernichtungswaffen verwendet zu werden. Kategorie II umfasst Trägersysteme mit Nutzlasten unter 500 kg (bei einer Reichweite über 300 km) sowie andere festgelegte Risikotechnologien.

Kritiker werfen dem MTCR vor, dass es sich um ein diskriminierendes Regime handelt, da für einige Empfängerstaaten in der Vergangenheit bereits Ausnahmen gemacht wurden und dies vor allem dazu dienen könnte, bestimmten Staaten gewisse Technologien vorzuenthalten (Mallik 2004, S. 11).

Bestimmte Kategorien von UCAVs oder deren Bestandteile werden bereits vom MTCR erfasst, dasselbe gilt damit auch für bestimmte AWS. Der MTCR-Annex und die darin gelisteten Güter unterliegen einer ständigen Revision. Das MTCR könnte daher auch zukünftig um weitere Technologien erweitert werden, die eine Relevanz für AWS aufweisen. Ob dies eine realistische Perspektive darstellt, ist allerdings fraglich. Derzeit gibt es im Gegenteil Bestrebungen, UCAVs aus dem MTCR herauszunehmen. Diese werden maßgeblich von US-amerikanischen Herstellern von Drohnen unterstützt, mit dem Argument, das Abkommen benachteilige sie gegenüber Wettbewerbern aus Ländern, die diesem nicht angehören (vor allem China), und schneide sie von einem

113 Israel folgt den MTCR-Regeln, ohne Mitglied zu sein. China stellte 2004 einen Antrag auf MTCR-Mitgliedschaft. Dieser wurde jedoch aufgrund von Bedenken hinsichtlich des Standards der chinesischen Exportkontrollen abschlägig beschieden (ACA 2017).

milliardenschweren Zukunftsmarkt für zivile und militärische Drohnen ab (Schörnig 2017, S. 12 f.).

Haager Verhaltenskodex gegen die Proliferation ballistischer Raketen

Der Haager Verhaltenskodex gegen die Proliferation ballistischer Raketen (Hague Code of Conduct against Ballistic Missile Proliferation – HCoC) verfolgt im Prinzip dieselbe Zielsetzung wie das MTCR. Im Unterschied zum MTCR hat der HCoC mit derzeit 139 Staaten (Stand 2018) eine wesentlich breitere Mitgliederbasis. Allerdings beinhaltet er lediglich Prinzipien, Verpflichtungen und Vorschläge für vertrauensbildende Maßnahmen, z. B. die Ankündigung von Raketenstarts und die Erstellung von jährlichen nationalen Berichten über Raketenprogramme und -bestände. Eindeutige Verbotsnormen oder Kooperationsanreize enthält er hingegen nicht. Auch bezieht sich der HCoC nur auf ballistische Raketen. Cruise Missiles[114] und UAVs sind nicht Bestandteil des Abkommens.

Ein Vorschlag der Weapons of Mass Destruction Commission (WMDC 2006, S. 143) unter dem Vorsitz des ehemaligen schwedischen Außenministers und Leiters der United Nations Monitoring, Verification and Inspection Commission (UNMOVIC) (Amtszeit 2000–2003) Hans Blix, Cruise Missiles und UAVs in den HCoC einzubeziehen sowie ein multilaterales Zentrum zum transparenten Datenaustausch einzurichten, wurde bis heute von der Staatengemeinschaft nicht aufgegriffen. Daher ist der HCoC für AWS derzeit nicht von besonderer Bedeutung.

Wassenaar-Abkommen

Das Wassenaar-Abkommen (Wassenaar Arrangement zu Exportkontrollen für konventionelle Rüstungsgüter und Dual-Use-Güter [Waren, Software und Technologie]) von 1996 soll der Stärkung der Exportkontrolle im Bereich von Rüstungsgütern und sensitiven Technologien, insbesondere auch solchen mit Dual-Use-Charakter, dienen. Hervorgegangen ist es aus dem Coordinating Committee on Multilateral Export Controls (COCOM), ursprünglich während des Kalten Krieges etabliert, um die Lieferung sensitiver Güter an die Staaten des Ostblocks zu verhindern.

Heute umfasst das Wassenaar-Abkommen 41 Mitgliedstaaten. Diese erstellen Listen sensitiver Güter (Wassenaar Arrangement 2017), deren Export an

114 Cruise Missiles (Marschflugkörper) weisen technologisch viele Merkmale bewaffneter UAVs auf. Der wesentliche Unterschied ist, dass sie nicht auf Wiederverwendbarkeit ausgelegt sind, da bei ihnen das Wirkmittel und das Trägersystem eine Einheit bilden. Eine eindeutige Klassifizierung ist allerdings oft schwierig.

Drittstaaten reglementiert wird.[115] Hierbei orientieren sich die Mitglieder an gemeinsamen Best Practices (Wassenaar Arrangement Secretariat 2019). Ferner stehen sie einem freiwilligen Informationsaustausch sowohl über erfolgte als auch über verweigerte Rüstungs- und Technologieexporte.

Explizit im Wassenaar-Abkommen erwähnt sind UAVs (in Category 9: Aerospace and Propulsion) sowie unbemannte Unterwasserfahrzeuge (UUVs, in Category 8: Marine). Darüber hinaus ist eine Reihe für unbemannte Systeme unmittelbar relevanter Technologien in den Kontrolllisten aufgeführt (TAB 2011, S. 198 f.). Andere unbemannte Trägersysteme finden keine explizite Erwähnung, allerdings wird auch im Wassenaar-Abkommen nicht zwischen bemannt und unbemannt differenziert – weshalb auch UGVs, USVs und somit jegliche zukünftige AWS bei Zutreffen der entsprechenden Kriterien den Exportkontrollen des Wassenaar-Abkommens unterworfen wären.

Da bereits heute auch bestimmte Software bzw. Algorithmen in den Kontrolllisten aufgeführt sind (z. B. einige kryptografische Verfahren oder Software, um akustische, optische und andere Sensordaten auszuwerten) (Wassenaar Arrangement 2017), wäre es perspektivisch durchaus möglich, kritische Softwarekomponenten von AWS in das Kontrollregime des Wassenaar-Abkommens einzubeziehen.

Vertrag über den Waffenhandel

Der von der UN-Generalversammlung angenommene Vertrag über den Waffenhandel (Arms Trade Treaty – ATT) (UN 2013) soll helfen, weltweit gültige Standards für den Export, Import und den Transfer von konventionellen Waffen zu schaffen und somit diesen zu regulieren. Dem Vertrag sind bisher 92 Staaten beigetreten (UN o. J.a).[116] In Artikel 2 des Vertrags werden die Waffenkategorien definiert, die der ATT einschließt. Hier finden sich – analog zum UN-Waffenregister – Kampfpanzer, gepanzerte Kampffahrzeuge, schwere Artilleriewaffen, Kampfflugzeuge und Angriffshubschrauber sowie Kriegsschiffe. Der Vertrag nimmt nicht direkt auf unbemannte oder autonome Waffensysteme Bezug, verweist hingegen in Artikel 5 Absatz 3 auf die Definition konventioneller Waffen im UN-Waffenregister.[117] Da 2016 UCAVs als Unterkategorie in das UN-Waffenregister aufgenommen wurden, gilt dies wohl auch für den ATT. UGVs, USVs und UUVs werden im UN-Waffenregister nicht

115 In Deutschland ist dies vor allem durch das Gesetz über die Kontrolle von Kriegswaffen (KrWaffG) und das Außenwirtschaftsgesetz (AWG) in Verbindung mit der Außenwirtschaftsverordnung (AWV) geregelt. Die in der AWV aufgeführten Rüstungsgüter orientieren sich eng an der Liste des Wassenaar-Abkommens.

116 Im April 2019 erklärte US-Präsident Trump, dass die USA den ATT nicht weiter unterstützen werden (Smith 2019).

117 Artikel 5 Absatz 3 des ATT im Original: »National definitions of any of the categories covered under Article 2 (1) (a)–(g) shall not cover less than the descriptions used in the United Nations Register of Conventional Arms at the time of entry into force of this Treaty.«

gesondert erwähnt, aber per Definition auch nicht ausgeschlossen. Es ist damit – wie beim UN-Waffenregister – auch im Falle des ATT Auslegungssache, ob neben UCAVs auch andere unbemannte Waffenplattformen (und damit zukünftig auch AWS) bereits Bestandteil dieses Informationsabkommens sind oder ob diese in der Zukunft explizit aufgenommen werden können.

Eine Übersicht über die wichtigsten internationalen Abkommen zu VSBM, Nichtverbreitung und Exportkontrolle bietet Tabelle 9.2.

Tab. 9.2 Transparenz- und vertrauensbildende Maßnahmen, Nichtverbreitung und Exportkontrolle

Abkommen	Rahmen	AWS Bestandteil des Vertrags?	Verifikation	Art des Abkommens
Wiener Dokument	multilateral	ja, AWS im Allgemeinen*	ja	VSBM der OSZE-Staaten
UN-Waffenregister	UN	ja, autonome UCAVs wahrscheinlich AWS im Allgemeinen**	nein	internationale VSBM
MTCR	multilateral	ja, autonome UCAVs	nein	Exportregime
Wassenaar-Abkommen	multilateral	ja, autonome UCAVs; UAVs werden explizit erwähnt wahrscheinlich AWS im Allgemeinen*	nein	Exportregime
ATT	UN	ja, autonome UCAVs wahrscheinlich AWS im Allgemeinen*	nein	internationale Normen zum Waffenhandel

* analog zum KSE
** Falls AWS der Definition einer der Hauptwaffentypen entsprechen; die dortigen Definitionen schließen unbemannte Systeme nicht aus (wahrscheinlich Auslegungssache).

Quelle: Alwardt et al. 2017, S. 80

9.2 Die Konvention über bestimmte konventionelle Waffen

Das zentrale Forum für die Debatte um eine mögliche Einhegung von AWS auf internationaler Ebene ist die Konvention über bestimmte konventionelle Waffen (Convention on Certain Conventional Weapons – CCW) der UN (o. J.b).[118] Dieses UN-Abkommen wurde 1980 in Genf beschlossen, trat im Dezember

118 Vertragstext in derzeit aktueller Fassung von 2001.

1983 in Kraft und wurde bisher von 125 Staaten unterzeichnet. Das Ziel der CCW besteht darin, (neue) konventionelle Waffen daraufhin zu bewerten, ob ihr Einsatz übermäßiges Leiden verursachen oder unterschiedslos wirken kann und sie daher in erklärten Kriegen oder bewaffneten Konflikten zu verbieten oder zu beschränken sind. Neben dem eigentlichen CCW-Rahmenvertrag sind bisher fünf Protokolle verabschiedet worden, die sich mit der Reglementierung bestimmter konventioneller Waffentypen beschäftigen: Das Protokoll I (1980) verbietet den Einsatz von Waffen, die durch in Röntgenuntersuchungen nicht entdeckbare Splitter wirken; Protokoll II (1980, geändert 1996) regelt den Einsatz von Minen, Sprengfallen und andere Vorrichtungen; Protokoll III (1980) hat Brandwaffen zum Inhalt; Protokoll IV (1995) verbietet blindmachende Laserwaffen, und Protokoll V (2003) befasst sich mit explosiven Kampfmittelrückständen.

Seit 2014 steht das Thema AWS auf der Tagesordnung, anfänglich im Rahmen informeller Expertengruppen. 2016 wurde eine Group of Governmental Experts (GGE) etabliert, deren Rolle es ist, technologische und definitorische Fragen zu klären und ggf. den Weg für formale Verhandlungen über ein Verbot oder eine anderweitige Regulierung von AWS zu bereiten.

Neben einem ethischen und einem (völker)rechtlichen Diskussionsstrang standen anfänglich Versuche im Mittelpunkt, verschiedene Grade an Autonomie mithilfe technologischer Kriterien zu bestimmen und daraus Definitionen für AWS abzuleiten, die es ermöglichen sollten, diese von anderen automatischen Waffensystemen abzugrenzen. Das Fehlen einer allgemein gültigen Definition von AWS und der Umgang mit diesem Defizit bestimmten die Debatte. Einige sahen die Notwendigkeit, sich zunächst über gemeinsame Charakteristika von »lethal autonomous weapon systems« (LAWS[119]) zu verständigen, andere wiesen auf die Schwierigkeiten dieses Unterfangens hin oder bezweifelten teilweise dessen Machbarkeit.

In der Folge konzentrierte sich die Debatte verstärkt auf die Art und Weise und das Ausmaß, in dem Menschen die Kontrolle über AWS ausüben. Dies war der Erkenntnis geschuldet, dass zentrale Fragen der Völkerrechtskonformität von AWS nicht nur von technischen, sondern auch maßgeblich von operationellen und anderen Kontextfaktoren ihres Einsatzes bestimmt werden. Darüber hinaus bestand (und besteht immer noch) bei den Staatenvertretern eine breite Übereinstimmung, dass es keine autonomen Waffensysteme geben soll, die ohne menschliche Beteiligung die Entscheidung über den Einsatz von Gewaltmitteln gegen Menschen treffen können bzw. dürfen (CCW 2015, S. 4).

119 LAWS ist die im Kontext der CCW verwendete Abkürzung für autonome Waffensysteme. Das »lethal« sollte anfänglich zur Unterscheidung von »cyber« dienen, wird aber inzwischen meist als »für Menschen (zumindest potenziell) tödlich« verstanden.

9.2.1 Menschliche Kontrolle über AWS

Nicht jede Art menschlicher Kontrolle im Sinne von »human in the loop« ist ausreichend, um den politischen, ethischen und (völker)rechtlichen Mindestanforderungen für verantwortliches Handeln gerecht zu werden. Das krasseste Gegenbeispiel wäre ein Mensch, dessen Aufgabe es wäre, mittels Knopfdrucks einen Angriff freizugeben, und der als einzige Information das Aufleuchten eines Lichts hätte, das signalisierte, dass »das System« diesen Angriff priorisierte. Ausgehend von dieser Überlegung wurde das Konzept »Meaningful Human Control«[120] (MHC), von der britischen NGO Article 36 (2013, S. 3 f.) geprägt und auf folgende Weise definiert:[121]

Für die Ausübung von MHC über individuelle Angriffe müssen mindestens folgende Voraussetzungen erfüllt sein:

- *Information*: Ein menschlicher Bediener und diejenigen, die verantwortlich für die Planung eines Angriffs sind, müssen über adäquate Kontextinformationen über das Zielgebiet verfügen, darüber, warum ein bestimmtes Objekt als Ziel vorgeschlagen wird, über die Zielsetzungen der Operation sowie über die unmittelbaren und langfristigen Auswirkungen des Waffeneinsatzes in diesem Kontext.
- *Aktive Handlung*: Ein Angriff darf nur durch eine aktive Handlung eines menschlichen Bedieners initiiert werden.
- *Rechenschaftspflicht*: Wer verantwortlich dafür ist, die Informationen zu bewerten und den Angriff durchzuführen, muss für die Folgen des Angriffs zur Rechenschaft gezogen werden können.

Der Begriff MHC wurde zwar breit adoptiert, allerdings nicht von allen Akteuren im gerade skizzierten Bedeutungsumfang. Auch wird nicht immer transparent kommuniziert, wie der Terminus verstanden wird bzw. werden soll, was die Diskussion mitunter erschwert. So wird beispielsweise nicht von allen der explizite Bezug auf *individuelle Angriffe* geteilt. Dies ist sehr bedeutsam, da

120 Zu Deutsch in etwa bedeutsame menschliche Kontrolle; »control« kann im Deutschen sowohl Kontrolle als auch Steuerung bedeuten. Im Kontext MHC ist nach Ansicht des TAB Kontrolle im Sinne von situativem Verständnis plus Eingriffsmöglichkeit vorzuziehen, da Steuerung als direkte Manipulation (an einem Joystick oder Ähnlichem) missdeutet werden kann.

121 Übersetzung durch das TAB; im Original: »Requirements for meaningful human control over individual attacks include, but are not necessarily limited to:
- *Information* – a human operator, and othersresponsible for attack planning, need to have adequate contextual information on the target area of an attack, information on why any specific object has been suggested as a target for attack, information on mission objectives, and information on the immediate and longer-term weapon effects that will be created from an attackin that context.
- *Action* – initiating the attackshould require a positive action by a human operator.
- *Accountability* – those responsible for assessing the information and executing the attack need to be accountable for the outcomes of the attack.«

MHC über individuelle Angriffe eine wesentlich stringentere Kontrolle impliziert als über AWS ganz allgemein oder lediglich über kritische Funktionen (d. h. insbesondere Zielauswahl und Zielbekämpfung) von AWS (UNIDIR 2014b).

Um das gemeinsame Verständnis über AWS zu schärfen und daraus ggf. Kriterien abzuleiten, um akzeptable von unakzeptablen AWS (bzw. deren Einsatzspektrum) unterscheiden zu können, kann die Diskussion um MHC sich als nützlich erweisen. Zu klärende Fragen sind u. a. (Davison 2017; IKRK 2018a; UNIDIR 2014b, S. 3 ff.):

- Wann im Produktzyklus eines AWS ist MHC primär umzusetzen: wenn das System für den Einsatz aktiviert wird (wie bei den meisten konventionellen Waffen) oder während des Einsatzes oder wesentlich früher, z. B. wenn die Waffe entwickelt bzw. designt wird?
- In welchen Phasen eines beabsichtigten Angriffs soll MHC greifen: während der Gewinnung von Aufklärungsdaten, der Analyse des Kontextes, der Zielidentifikation, der Zielauswahl inkl. Abwägungen bezüglich des HVR (Unterscheidungsgebot, Verhältnismäßigkeit, Vorsorgeprinzip) oder der letztendlichen Entscheidung zum Angriff?
- Was soll MHC unterworfen sein: das AWS selbst, bestimmte Funktionen des AWS, jeder individuelle Angriff oder etwas anderes?
- Welche Vorkehrungen würden gewährleisten, dass MHC tatsächlich ausgeübt wird?
- Würde eine auf MHC basierende Norm ggf. bereits existierende Waffensysteme berühren?
- Wie könnte MHC ausgeübt werden, wenn keine Kommunikationsverbindung zu dem AWS existiert?
- Welches Ausmaß menschlicher Kontrolle ist erforderlich, um »meaningful« zu sein, und wie hängt dieses ab von operationellen Gegebenheiten (Art des Ziels, Umgebung etc.)?
- Wie gut muss das Verhalten von AWS vorhersagbar sein? Wie verlässlich müssen AWS sein?
- Wie kann MHC überhaupt erfolgen, wenn die Zeiträume, in denen rechnergestützte Entscheidungen gefällt werden, so kurz werden, dass Menschen dem Geschehen nicht mehr folgen, geschweige denn es kontrollieren und eingreifen können?

Zur Illustration der Komplexität und des Facettenreichtums der Diskussionen im Rahmen der CCW, bei der zum gegenwärtigen Zeitpunkt das grundsätzliche begriffliche und konzeptuelle gemeinsame Verständnis im Zentrum steht, zeigt Tabelle 9.3 eine Übersicht – erstellt vom Vorsitzenden der CCW – über verschiedene Möglichkeiten, menschliche Kontrolle über AWS begrifflich zu fassen (ohne Anspruch auf Vollständigkeit).

Tab. 9.3 Formulierungsvarianten zur menschlichen Kontrolle über AWS

maintaining (Aufrechterhaltung)	substantive (substanzieller)	human (menschlicher)	participation (Beteiligung)
ensuring (Sicherung)	meaningful (sinnvoller)		involvement (Mitwirkung)
exerting (Ausübung)	appropriate (angemessener)		responsibility (Verantwortung)
preserving (Bewahrung)	sufficient (ausreichender)		supervision (Überwachung)
	Minimum level of (Mindestniveau an)		validation (Validierung)
	Minimum indispensable (unabdingbares Mindestmaß an)		control (Kontrolle)
			judgement (Urteil)
			decision (Entscheidung)

Quelle: Zusammenfassung des CCW-Vorsitzes, CCW GGE 2018a, S. 7

Das US-Verteidigungsministerium lehnt beispielsweise das Konzept MHC ab und stellt dagegen in den Vordergrund, dass Kommandeure und Operatoren »angemessene Niveaus menschlicher Beurteilung über den Einsatz von Gewaltmitteln«[122] ausüben sollen, was – insbesondere in der deutschen Übersetzung – auf den ersten Blick recht ähnlich klingen mag.

Die USA führen weiter aus, dass es kein einheitliches festgeschriebenes *angemessenes Niveau* menschlicher Beurteilung geben kann, da dies vom Kontext abhängt. In bestimmten Fällen ist weniger menschliche Beteiligung sogar wünschenswert, da die Nutzung autonomer Funktionen höhere Präzision und Geschwindigkeit aufweisen würde, als dies bei menschlicher Kontrolle möglich wäre (beispielsweise bei SARMO-Systemen) (CCW GGE 2018j, S. 2 f.).

Kritiker befürchten wiederum, dass unter bestimmten Bedingungen auch das Ingangsetzen eines AWS ohne spezifische weitere menschliche Kontrolle als *angemessen* interpretiert werden könnte. So wird im zitierten Dokument (DOD 2012) als eine Voraussetzung für angemessene Kontrolle genannt, dass ein menschlicher Bediener »einzelne Ziele oder spezifische Gruppen von Zielen« auswählt, bevor sie angegriffen werden. Mit dieser vage gehaltenen Umschreibung kann auch ein Auftrag in der Form »Zerstöre alle feindlichen Fahrzeuge im Operationsgebiet!« konform gehen, ohne dass weitere menschliche Kontrolle gefordert wäre (Altmann/Gubrud 2017, S. 206 ff.).

122 Im Original: »appropriate levels of human judgment over the use of force« (DOD 2012).

Wie diese Diskussion sich weiterentwickelt und ob bzw. auf welche genaue Ausformulierung sich die Staaten im Rahmen der Diskussionen in der CCW verständigen könnten, ist gegenwärtig nicht abzusehen.

9.2.2 Positionen wichtiger Staaten bzw. Organisationen

Im Folgenden werden die Positionen einiger wichtiger Akteure beleuchtet, wie sie im Rahmen der CCW vorgebracht werden. Wie verstehen sie AWS und wie grenzen sie diese von anderen Waffentypen ab, welche Vorteile, Nachteile und Implikationen verbinden sie mit AWS, welche Form menschlicher Kontrolle wird als adäquat angesehen und welche Folgerungen werden daraus gezogen in Bezug auf Fragen der Regulierung von AWS? Als Grundlage hierfür diente die Zusammenstellung des United Nations Institute for Disarmament Research (UNIDIR 2017, S. 23 ff.), die ergänzt und aktualisiert wurde.

Deutschland

Die deutsche Regierung hat über zwei Legislaturperioden hinweg stets erklärt, dass sie sich »aktiv für die Ächtung letaler autonomer Waffensysteme (einsetzt), die dem Menschen die Entscheidungsgewalt über Leben und Tod entziehen« (Bundesregierung 2018f). Dies lässt einen gewissen Interpretationsspielraum offen, ob *Ächtung* beispielsweise mit *international verbindliches Verbot* gleichgesetzt werden kann.

Auf der CCW (CCW GGE 2018f) wurde die Position so umrissen: Die ultimative Entscheidung über Leben und Tod muss weiterhin ausschließlich Menschen vorbehalten sein. Daher wird ein Verzicht auf die Entwicklung bzw. Beschaffung von Waffen erklärt, die den menschlichen Faktor beim Waffeneinsatz gegen Menschen vollständig ausschließen. Konkret werden Waffensysteme abgelehnt, die dafür ausgelegt sind, tödliche Effekte oder andere Schäden gegen menschliche Wesen zu richten und die völlig ohne Interaktion bzw. Kontrolle durch Menschen Wahrnehmungen generieren, Folgerungen ziehen, entscheiden, handeln, evaluieren und lernen. Die Fähigkeit zu lernen und eine Eigenwahrnehmung zu entwickeln wird als wesentliches Attribut genannt, um eine Funktion bzw. ein System autonom zu nennen. Dabei ist man sich mit der französischen Position einig, dass heute AWS (wie hier definiert) noch nicht existieren (CCW GGE 2018e).

Dass bei der Definition die Betonung auf einen *vollständigen* Ausschluss des menschlichen Faktors beim tödlichen Waffeneinsatz gelegt wird, eröffnet allerdings ein weites Feld für autonome Systeme, die nicht unter diese Definition fallen würden, da sie eine minimale menschliche Aufsicht aufweisen, und sei sie noch so gering. Dass hier ein wesentlicher Klärungsbedarf besteht, wird von der Bundesregierung anerkannt, indem sie feststellt, dass »eine Einigung über

Mindeststandards wirksamer menschlicher Kontrolle zentrales Element in der Diskussion über Handlungsoptionen der CCW-Vertragsstaaten« (Bundesregierung 2018f) sein muss. Eine ausformulierte ressortübergreifend abgestimmte nationale Position zu diesen konzeptionellen Fragen könnte dazu beitragen, diese Diskussion inhaltlich voranzutreiben.

Deutschland spielt in den Debatten im Rahmen der CCW eine treibende Rolle und hatte u. a. 2015 und 2016 den Vorsitz der Expertentreffen dazu genutzt, Bedingungen für einen Konsens auszuloten. Diese Konsensorientierung ist im Kontext der CCW verständlich und naheliegend, da für Beschlüsse Einstimmigkeit erforderlich ist. Andererseits geht das Einnehmen dieser vermittelnden Rolle damit einher, dass darauf verzichtet wurde, die beschriebene inhaltliche Position der Bundesregierung offensiver zu formulieren und in die CCW einzubringen.

Kasten 9.1 Aktuelle deutsche Position

Das Auswärtige Amt hat auf dem Arbeitstreffen der CCW GGE im März 2019 folgende Elemente einer Definition für Autonomie in LAWS vorgestellt (AA 2019b):

- die Fähigkeit, eine Umwelt wahrzunehmen (sensorisch zu erfassen und zu interpretieren);
- die Umstände einer sich verändernden Situation evaluieren ohne Bezugnahme auf vordefinierte Ziele;
- abwägen und auswählen der geeignetsten Vorgehensweise;
- auf Basis dieser Schlussfolgerungen Aktionen initiieren;
- all dies ohne menschliche Beteiligung, nachdem das System aktiviert wurde.

Gleichzeitig wird betont, dass aus deutscher Sicht eine exakte, von allen Beteiligten geteilte Definition für den weiteren Fortschritt des CCW-Prozesses nicht notwendig ist. Das bisher erzielte gemeinsame Verständnis wäre ausreichend, um nun in Richtung auf ein Ergebnisdokument voranzuschreiten. Hierfür wären die 2018 formulierten möglichen Leitlinien (Kasten 9.5) eine gute Basis (AA 2019a, 2019c u. 2019d).

Frankreich

Frankreich hat in einem informellen Arbeitspapier im Rahmen der CCW eine sehr enge Definition für LAWS vorgebracht, die u. a. verlangt, dass überhaupt keine Kommunikationsverbindung mit der menschlichen Kommandokette vorliegt: »LAWS sollten so verstanden werden, dass sie ein vollständiges Fehlen menschlicher Aufsicht implizieren. Dies bedeutet, dass keinerlei Verbindung

(zur Kommunikation oder Kontrolle) mit der militärischen Kommandokette besteht.«[123] Zugleich wird aber konstatiert, dass solche Systeme, die sich zu 100 % auf die interne Modellierung der Umgebung verlassen müssten, beim ersten unvorhergesehenen Ereignis unvorhersehbar reagieren würden. Dies würde sie militärisch nutzlos machen (CCW GGE 2016b). Es ist kaum vorstellbar, dass Staaten mit einem gewissen Verantwortungsbewusstsein derartige Waffen anstreben bzw. entwickeln.

Gleichzeitig hat Frankreich erkannt, dass der Umgang mit der militärischen Nutzung von KI in einer nationalen KI-Strategie eine wesentliche Rolle spielen muss. Im Bericht von Villani (2018), der den Ausgangspunkt für eine französische KI-Strategie markiert, werden einige konkrete Vorschläge gemacht, wie die Proliferation von AWS eingeschränkt werden kann. Dies reicht von nationalen Exportregeln über eine internationale Beobachtungsstelle, um mögliche Gefahren durch AWS frühzeitig zu erkennen, bis hin zum Anstoß einer breiten gesellschaftlichen Debatte, die sich auch mit ethischen Fragen von KI im Militär befassen soll (Villani 2018, S. 125 ff.).

Niederlande

Die Regierung der Niederlande (Dutch Government 2016) hat ihre Position zum Themenkomplex AWS in einer Stellungnahme zu dem in ihrem Auftrag angefertigten Bericht des Adviesraad Internationale Vraagstukken (Beirat für internationale Angelegenheiten) und des Commissie Van Advies Inzake Volkenrechtelijke Vraagstukken (Beratender Ausschuss für Fragen des Völkerrechts) (AIV/CAVV 2015)[124] ausführlich dargelegt. Sie strebt an, eine international abgestimmte Definition zu erarbeiten (insbesondere im Rahmen der CCW GGE), und nimmt hierfür die Definition von AIV und CAVV als Ausgangspunkt: »[...] eine autonome Waffe ist definiert als: eine Waffe, die ohne menschliches Zutun Ziele auswählt und bekämpft, die bestimmte vorher definierte Kriterien erfüllen. Dies erfolgt, nachdem ein Mensch die Entscheidung getroffen hat, die Waffe einzusetzen, wohlwissend dass ein Angriff nicht mehr durch menschliche Intervention gestoppt werden kann, nachdem er lanciert wurde.«[125]

Diese Definition wird präzisiert, indem eine klare Trennlinie gezogen wird zwischen autonomen Waffensystemen, bei denen Menschen eine entscheidende Rolle spielen (»in the wider loop«), und vollständig autonomen Waffen-

123 Im Original: »LAWS should be understood as implying a total absence of human supervision, meaning there is absolutely no link (communication or control) with the military chain of command.« (CCW GGE 2016a)

124 AIV und CAVV sind unabhängige Gremien, die die niederländische Regierung und das Parlament beraten.

125 Im Original: »An autonomous weapon is defined as: A weapon that, without human intervention, selects and engages targets matching certain predefined criteria, following a human decision to deploy the weapon on the understanding that an attack, once launched, cannot be stopped by human intervention.« (AIV/CAVV 2015, S. 11)

systemen ohne jegliche menschliche Kontrolle. Der »wider loop« schließt über den »narrow loop« (der die konkrete Zielauswahl und -bekämpfung umfasst) hinaus Aufgaben wie Missionsplanung, Vorauswahl der Ziele, Wahl der Wirkmittel und Durchführungsplanung ein. Auch die Bewertungen der Vereinbarkeit eines Angriffs mit dem HVR betrifft den »wider loop«. Für »meaningful control« reicht nach Ansicht der niederländischen Regierung die menschliche Aufsicht über den »wider loop« aus, der »narrow loop« könnte ohne menschliche Intervention(smöglichkeit) ablaufen.

Dass vollständig autonome Waffensysteme in den nächsten Jahrzehnten entwickelt werden, wird als unwahrscheinlich eingeschätzt. Dies erfordert, wenn es denn technisch überhaupt möglich ist, erhebliche Fortschritte auf dem Gebiet der KI. Darüber hinaus wird bezweifelt, ob Staaten derartige Waffen überhaupt entwickeln wollten (AIV/CAVV 2015, S. 17).

Es wird bekräftigt, dass im Zuge einer möglichen Beschaffung von AWS diese ausführlich unter realistischen Bedingungen getestet würden. Bezüglich der Waffenprüfung gemäß Artikel 36 ZP I, ob bestimmte autonome Waffen mit dem HVR kompatibel sind, haben die Niederlande das Advisory Committee on International Law and the Use of Conventional Weapons (AIRCW) etabliert, das dafür zuständig ist. Die Existenz einer Verantwortungslücke wird abgestritten: Solange Kommandeure und Operatoren »meaningful human control« ausüben, tragen sie die volle Verantwortung. Eine entsprechende Ausbildung und das Training der Soldaten sollen sicherstellen, dass ein verantwortungsvoller Umgang mit AWS stattfindet. Ein Moratorium für die Entwicklung und den Einsatz vollautonomer Waffen wird derzeit für nicht sinnvoll bzw. nicht machbar gehalten (Dutch Government 2016).

Dessen ungeachtet ist sich die niederländische Regierung über das Potenzial von Autonomie im Verteidigungssektor wohl bewusst: »Wenn die niederländische Armee auf technologischem Feld fortschrittlich bleiben will, werden autonome Waffen jetzt und in der Zukunft eine Rolle spielen. [...] Deren Einsatz muss aber immer menschlicher Kontrolle (›meaningful human control‹) unterliegen« (Dutch Government 2016). Diese Einschätzung spiegelt auch die »Strategische FuE-Agenda« des niederländischen (Ministerie van Defensie 2016) wider, die Big Data, künstliche Intelligenz und »man-machine teaming« zum Schwerpunkt hat.

Vereinigtes Königreich

Das britische Ministry of Defence (MOD 2017b, S. 13) arbeitet mit folgenden Definitionen autonomer bzw. automatisierter Waffensysteme: »Ein automatisiertes System [...] ist so programmiert, dass es als Antwort auf eingehende Signale eines oder mehrerer Sensoren einem vorher definierten Satz von Regeln logisch folgt, um daraus ein Ergebnis zu erzeugen. Wenn der Regelsatz, mit dem es operiert, bekannt ist, ist das Ergebnis vorhersagbar.

Ein autonomes System ist fähig, Absichten und Anweisungen auf einer höheren Ebene zu verstehen. Mittels dieses Verständnisses und seiner Wahrnehmung der Umwelt kann das System geeignete Handlungen vollziehen, die einen gewünschten Zustand herbeiführen. Es ist dazu fähig, aus einer Anzahl von Alternativen eine Vorgehensweise auszuwählen, ohne auf menschliche Aufsicht und Kontrolle angewiesen zu sein, obwohl diese dennoch vorhanden sein können. Obwohl die allgemeine Aktivität eines autonomen unbemannten Fluggeräts vorhersagbar sein wird, sind dies individuelle Handlungen möglicherweise nicht.«[126]

Als Schlüsselbegriff für die Abgrenzung autonomer von automatisierten Systemen wird hier die Vorhersehbarkeit (»predictable«) verwendet. Die Aktionen automatisierter Systeme sind vollständig vorhersehbar, die von autonomen Systemen auf der Ebene individueller Handlungen nicht.

Diese Definition für AWS ist so eng gefasst (insbesondere aufgrund des Postulats von »Verständnis von Absichten und Anweisungen auf einer höheren Ebene«), dass im Weiteren konstatiert wird, derartige Systeme würden derzeit nicht und möglicherweise niemals existieren (CCW 2016c, Ziffer 5). Zudem wird Systemen, die ohne menschliche Kontrolle Waffeneinsätze durchführen können, ein militärischer Nutzen schlichtweg komplett abgesprochen (CCW 2016c, Ziffer 3).[127] Somit ist es nur konsequent, dass das Vereinigte Königreich erklärte, nicht an derartigen Systemen zu forschen.

Für die Art der menschlichen Kontrolle wird der Terminus »meaningful human control« abgelehnt, da er insbesondere beim Punkt Verantwortlichkeit nicht mit der derzeitigen Militärdoktrin in Einklang zu bringen sei. Stattdessen wird z. B. der Begriff »intelligent partnership« vorgeschlagen, allerdings ohne eine präzise Definition anzubieten (CCW 2016c, Ziffer 6).

In einem Bericht des Ausschusses zu künstlicher Intelligenz des britischen Oberhauses (House of Lords Select Committee on Artificial Intelligence 2018, S. 101 ff.), in dem die wirtschaftlichen, ethischen und sozialen Auswirkungen der Fortschritte im Bereich KI beleuchtet wurden, wurde diese Herangehensweise deutlich kritisiert. Der Definitionsansatz (»ist fähig, Absichten und Anweisungen auf einer höheren Ebene zu verstehen«) ist mit den Positionen der meisten

126 Im Original: »An automated [...] system is one that, in response to inputs from one or more sensors, is programmed to logically follow a predefined set of rules in order to provide an outcome. Knowing the set of rules under which it is operating means that its output is predictable.
An autonomous system is capable of understanding higher-level intent and direction. From this understanding and its perception of its environment, such a system is able to take appropriate action to bring about a desired state. It is capable of deciding a course of action, from a number of alternatives, without depending on human oversight and control, although these may still be present. Although the overall activity of an autonomous unmanned aircraft will be predictable, individual actions may not be.«

127 Im Original: »The UK does not believe that there would be any military utility in a fully autonomous lethal weapon system.«

anderen Regierungen weltweit nicht kompatibel. Dies würde die Möglichkeiten zu konstruktiven Beiträgen in der internationalen Debatte einschränken und Großbritannien eine Rolle als ethisch und moralisch führende Nation auf diesem Gebiet erschweren. Daher empfiehlt der Ausschuss, eine Expertengruppe einzuberufen, die zeitnah eine international anschlussfähige Definition für AWS vorlegen soll (House of Lords Select Committee on Artificial Intelligence 2018, Ziffer 345 f.).

Hinter der bisherigen Definition lässt sich die Intention erkennen, dass bereits genutzte Systeme mit einem hohen Grad operationeller Autonomie – insbesondere Abwehrsysteme gegen schnell anfliegende Flugkörper (Raketen, Granaten) vom Typ »SARMO« (»sense and react to military objects« z. B. »C-RAM«, »Phalanx«, »NBS Mantis«) oder Flugkörper mit intelligenter Zielerkennung und -identifizierung (etwa »Brimstone«) – auf keinen Fall darunter fallen sollen. Dies speist sich aus der Befürchtung, dass im Rahmen der internationalen Diskussion ggf. beschlossene Einschränkungen für AWS auch auf diese als militärisch unverzichtbar bewertete Systeme ausgedehnt werden können (Sharkey 2018).

An diesem Punkt lässt sich die Diversität der nationalen Definitionsansätze gut demonstrieren. So postuliert der französische Ansatz das vollständige Fehlen menschlicher Aufsicht als Kernkriterium für AWS, was dem britischen diametral gegenübersteht.

Hinsichtlich der Frage der Regulierung von LAWS im Rahmen der CCW vertritt die britische Regierung die Position, dass die Sorgfalt, die verantwortliche Regierungen und Militärs bereits heute bei der Überprüfung von Waffensystemen an den Tag legen, vollkommen ausreichend ist, um die Entwicklung sämtlicher neuer Waffensysteme einschließlich LAWS zu regulieren. Menschen müssen stets die Oberaufsicht über Waffensysteme ausüben, und das Ziel der CCW sollte sein, ein Einverständnis darüber zu erzielen, welche Elemente der Kontrolle über Waffensysteme Menschen vorbehalten bleiben sollen. Es wird betont, dass das Vereinigte Königreich vollständig autonome Waffensysteme weder besitzt noch entwickelt. Es wird versichert, dass jeder Waffeneinsatz unter menschlicher Kontrolle steht und stehen wird, um absolut sicherzustellen, dass menschliche Aufsicht, Befehlsgewalt und Verantwortlichkeit gewahrt sind (CCW GGE 2018i). Insgesamt ist die britische Regierung der Auffassung, dass das HVR in seiner gegenwärtigen Form für die Regulierung von LAWS ausreichend ist. Ein Bedarf für neue völkerrechtliche Regeln oder Verbote wird nicht gesehen (Bowcott 2015).

Jenseits der skizzierten Debatte um Konzepte, Definitionen und Regulierung wird die herausragende Rolle, die Autonomie in vielen Bereichen künftig einnehmen könnte, vom britischen Militär keineswegs unterschätzt. Dies kann man beispielsweise dem Strategiepapier »Future Operating Environment 2035«

des MOD (2015) entnehmen. AWS werden dort unter der Überschrift »remote and automated systems« ausführlich behandelt.

Kasten 9.2 Qualität menschlicher Kontrolle aus britischer Sicht

Die britische Regierung hat ihre Position mittlerweile weiterentwickelt und ausdifferenziert. Von der früheren Definition autonomer Systeme mit der mindestens missverständlichen Formulierung, diese wären in der Lage, »Absichten und Anweisungen auf einer höheren Ebene zu verstehen«, wurde merklich abgerückt (UK Mission 2019a). Stattdessen wird die Qualität menschlicher Kontrolle beim Waffeneinsatz in den Mittelpunkt gestellt. Der direkte Einbezug von Menschen bei jeglicher Aktion eines Systems ist weder praktikabel noch unter allen Umständen wünschenswert.

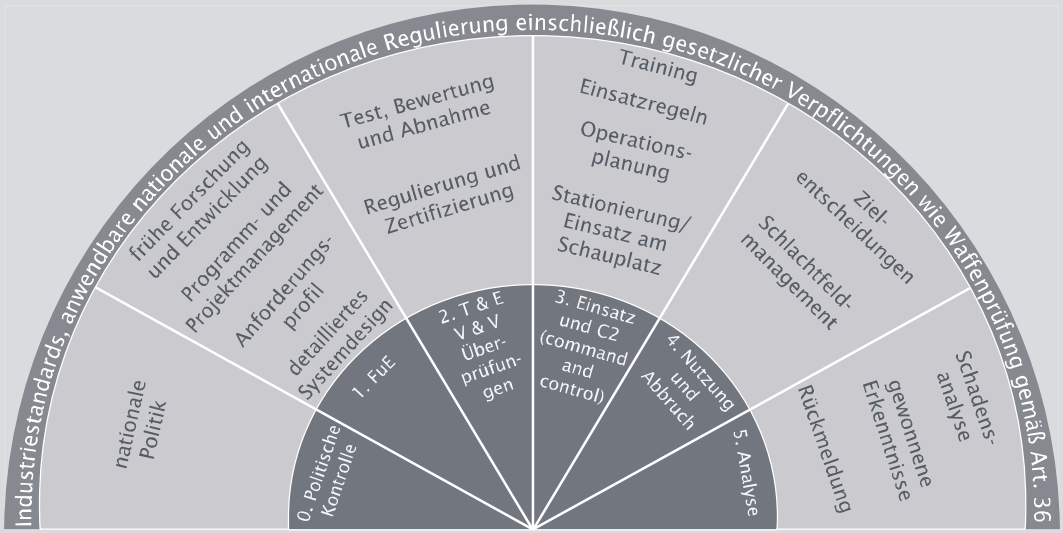
Zur Sicherstellung der menschlichen Kontrolle ist die Fokussierung auf sogenannte kritische Funktionen (vor allem Zielauswahl und -bekämpfung) zu kurz gegriffen (UK Mission 2019b). Stattdessen muss der gesamte Entwicklungs- und Nutzungszyklus einer Waffe in den Blick genommen werden, wie dies u. a. in einem Arbeitspapier dargelegt wird (CCW GGE 2018i).

Für eine detaillierte Diskussion wird vorgeschlagen, diesen Zyklus in sechs Stadien zu unterteilen, angefangen von der Konzeption politischer Grundlagen über FuE, TEVV inklusive der Waffenprüfungen nach Artikel 36 ZP I, Stationierung einschließlich der entsprechenden Kommandokette (C2: »command and control«), Entscheidungen hinsichtlich des Einsatzes bzw. Abbruchs des Einsatzes bis schließlich zur Analyse der Auswirkungen des Waffeneinsatzes. Abbildung 9.1 ordnet diesen Stadien wesentliche Aktivitäten zu. Dies dient dazu, die unterschiedlichen Blickwinkel zu verdeutlichen, unter denen menschliche Kontrolle zur Sicherstellung eines effektiven und gleichzeitig rechtlich und ethisch konformen Waffeneinsatzes betrachtet werden sollte.

Die praktizierte menschliche Kontrolle auf all diesen Ebenen reicht nach Ansicht der britischen Regierung aus, um die Entwicklung und den Einsatz jeglicher neuer Waffentechnologien einschließlich von AWS zu regulieren. Dass die Aufsichtsfunktion, Autorität, Verantwortlichkeit und Rechenschaftspflicht beim Waffeneinsatz durch Menschen wahrgenommen werden, ist im Vereinigten Königreich somit jederzeit gewährleistet (CCW GGE 2018i, S. 1)

Hinsichtlich des weiteren Vorgehens im Rahmen der CCW wird eine mögliche Zustimmung zu einer regelmäßig tagenden Expertengruppe signalisiert und es wird anerkannt, dass der deutsch-französische Vorschlag oder eine Art »code of conduct« Ausgangspunkte für die weitere Diskussion sein können. Einer darüber hinausgehenden Erteilung eines Verhandlungsmandats, um neue Instrumente zur verbindlichen Regulierung von LAWS zu implementieren, wird jedoch eine strikte Absage erteilt (UK Mission 2019c).

Abb. 9.1 Rahmen für menschliche Kontrolle im Entwicklungs- und Nutzungszyklus einer Waffe



Quelle: nach CCW GGE 2018i, S. 5

Europäische Union

In ihrem Statement auf der Sitzung der CCW GGE im April 2018 erklärte die Delegation der EU, es müsse Menschen vorbehalten sein, die Entscheidung über die Ausübung tödlicher Gewalt zu treffen. Außerdem habe das HVR für alle Waffen einschließlich LAWS in vollem Umfang zu gelten. Eine Arbeitsdefinition für LAWS begrüßte die EU-Delegation. Im Übrigen soll es in Anbetracht der Dual-Use-Eigenschaften der Technologien vermieden werden, den Fortschritt in der zivilen FuE zu behindern (CCW GGE 2018b).

Im Vergleich zu diesen weich formulierten Zielen nimmt das EU-Parlament eine wesentlich deutlichere Position ein. Bereits 2014 verabschiedete es eine Entschließung zum Einsatz bewaffneter Drohnen, die die Hohe Vertreterin für Außen- und Sicherheitspolitik, die Mitgliedstaaten und den Rat auffordert, »die Entwicklung, Produktion und Verwendung von vollkommen autonom funktionierenden Waffen, mit denen Militärangriffe ohne Mitwirkung des Menschen möglich sind, zu verbieten« (EP 2014). Dies wurde kürzlich in einer weiteren Entschließung bekräftigt, in der explizit gefordert wurde, »auf die Aufnahme internationaler Verhandlungen über ein rechtsverbindliches Instrument hinzuarbeiten, mit dem letale autonome Waffensysteme untersagt werden« (EP 2018).

Abseits von der militärischen Anwendung der Robotik regte das EU-Parlament an, ein umfassendes EU-Registrierungssystem für fortschrittliche Roboter einzuführen, wenn dies für bestimmte Kategorien von Robotern sachdienlich und notwendig ist. Eine neu einzurichtende Europäische Agentur für Robotik

und Künstliche Intelligenz kann hier die Federführung übernehmen (EP 2017, S. 9 f.). Eine analoge Initiative wäre sicher auch für AWS denkbar.

Kasten 9.3 AWS und der Europäische Verteidigungsfonds

Der 2017 ins Leben gerufene Europäische Verteidigungsfonds (European Defence Fund) soll die Wettbewerbs- und Innovationsfähigkeit der technologischen und industriellen Basis der europäischen Verteidigung steigern. Er ist pro Jahr mit etwa 500 Mio. Euro für Forschung sowie etwa 1 Mrd. Euro für Entwicklung und Beschaffung (nach 2020) ausgestattet (EK 2017).

In der Frage, ob Mittel aus dem Fonds auch für FuE von AWS bereitgestellt werden dürfen, zeichnet sich aktuell eine Einigung ab. In einem zwischen den Mitgliedsländern abgestimmten Entwurf für eine entsprechende Regulierung, der allerdings noch vom EU-Parlament sowie vom Rat formal gebilligt werden muss, ist dies explizit ausgeschlossen (General Secretariat of the Council 2019). Dort steht unter Punkt 7: »Maßnahmen zur Entwicklung von tödlichen autonomen Waffen ohne die Möglichkeit der bedeutsamen menschlichen Kontrolle über Entscheidungen zur Auswahl und Bekämpfung bei Schlägen, die sich gegen Menschen richten, sollen durch den Fonds nicht förderfähig sein, unbeschadet der Möglichkeit, die Entwicklung von Frühwarnsystemen und Gegenmaßnahmen für defensive Zwecke finanziell zu fördern.«[128]

USA

Die USA stützen sich auf ihre bereits 2012 ausgearbeitete Definition von AWS (DOD 2012, S. 13 f.): »Ein Waffensystem, das nach seiner Aktivierung Ziele auswählen und bekämpfen kann ohne weitere Einwirkung durch einen menschlichen Bediener. Dies schließt von Menschen überwachte AWS ein, die es menschlichen Bedienern erlauben, das System im Betrieb zu überstimmen«.[129]

Ausgehend von der von allen Staaten geteilten Prämisse, dass alle Waffen einschließlich LAWS vollständig konsistent mit dem HVR sein müssen, betonen die USA, dass dabei den nationalen Waffenreviewprozessen eine zentrale Bedeutung zukommen soll. Es wird festgestellt, dass Fortschritte in KI und

128 Im Original: »Actions for the development of lethal autonomous weapons without the possibility for meaningful human control over the selection and engagement decisions when carrying out strikes against humans should also not be eligible for financial support by the Fund, without prejudice to the possibility to provide funding for actions for the development of early warning systems and countermeasures for defensive purposes.«

129 Im Original: »A weapon system that, once activated, can select and engage targets without further intervention by a human operator. This includes human-supervised autonomous weapon systems that are designed to allow human operators to override operation of the weapon system.«

maschinellem Lernen nicht nur Risiken und Herausforderungen mit sich bringen, sondern dass dies die Einhaltung des HVR auch erleichtern und verbessern könnte. Daher ist es wichtig, besser zu verstehen, wie diese Technologie dazu genutzt werden kann, das Risiko für Zivilisten und verbündete Kräfte im bewaffneten Konflikt zu reduzieren.[130] Daher wäre es voreilig, in die Aushandlung eines politisch oder juristisch bindenden Dokuments einzusteigen (CCW GGE 2017d u 2018h).

Die USA sind der Ansicht, dass für den Fortgang der Diskussionen im Rahmen der CCW keine allgemein akzeptierte Definition von LAWS erforderlich ist. Dies wäre nur dann notwendig, wenn Normen oder Regularien formuliert werden sollen, was aber zum gegenwärtigen Zeitpunkt als verfrüht angesehen wird. Aktuell ist es völlig ausreichend, Charakteristika von LAWS zu identifizieren, um die Diskussion voranzubringen. Diese sollten allerdings nicht auf spezifischen technologischen Annahmen basieren, da diese durch die Fortschritte bei FuE schnell überholt sein können (CCW GGE 2017c).

Der zentrale Punkt bei der Mensch-Maschine-Interaktion bei LAWS ist, dass Maschinen die Intentionen des Kommandeurs bzw. Operators umsetzen. Dies wäre bei Einhaltung eines angemessenen Niveaus menschlicher Beurteilung beim Waffeneinsatz (»appropriate levels of human judgment over the use of force«) gewährleistet. Der in der Debatte vorgebrachte Fokus auf menschliche Kontrolle (»meaningful human control«) wäre u. a. deshalb fehlgeleitet, weil autonome Funktionen eines Waffensystems die menschliche Kontrolle über die Waffe effektiv erhöhen könnten, wie am Beispiel von smarten Bomben ausgeführt wird. Außerdem wären die Verantwortung und die Rechenschaftspflicht von Kommandeuren und Operatoren jederzeit gegeben, unabhängig vom Niveau der Autonomie der eingesetzten technischen Systeme. Wesentlich ist vor allem, wie Menschen diese Systeme nutzen und was von den Waffen erwartet wird (CCW GGE 2018j).

Russland

Das russische Verteidigungsministerium (CCW GGE 2018d) verwendet folgende Definitionen für autonome und semiautonome Waffensysteme:[131]

130 Dieser Punkt wird auch in der jüngst veröffentlichten KI-Strategie der US-Regierung betont (DOD 2019, S. 6): »AI also has the potential to enhance our implementation of the Law of War. By improving the accuracy of military assessments and enhancing mission precision, AI can reduce the risk of civilian casualties and other collateral damage.«

131 Im Original: »Autonomous weapons system – an unmanned piece of technical equipment that is not a munition and is designed to perform military and support tasks under remote control by an operator, autonomously or using the combination of these methods; Semi-autonomous weapon system – type of robotic military equipment requiring involvement of the operator.«

- autonomes Waffensystem: ein unbemanntes Gerät, das keine Munition ist und das militärische und unterstützende Aufgaben ferngesteuert durch einen Bediener, autonom oder in Kombination der beiden Modi durchführen kann;
- semiautonomes Waffensystem: ein robotisches militärisches Gerät, das die Mitwirkung eines Bedieners erfordert.

Russland stellt fest, dass die unterschiedlichen Definitionen für LAWS, die die einzelnen Staaten verwenden, die Diskussion ganz erheblich erschweren. Einige Staaten verstehen darunter auch bereits genutzte semiautonome und automatisierte Systeme; andere nur solche, die mit einem hohen Grad an künstlicher Intelligenz ausgestattet sind und die derzeit noch nicht existieren, aber in Zukunft möglich sind. Demzufolge sollen zuerst die grundlegenden Funktionen geklärt und eine Arbeitsdefinition aufgestellt werden, die als Voraussetzung für Fortschritte in den Diskussionen gesehen wird. Dabei wird Wert darauf gelegt, dass die Definition keinesfalls zu einer Einteilung von Waffensystemen in *gute* und *böse* führen darf.

Des Weiteren ist man der Ansicht, dass existierende Systeme mit einem hohen Grad an Autonomie bzw. Automatisierung nicht als LAWS klassifiziert werden sollen. Bei diesen ist sichergestellt, dass sie den Kriterien des HVR genügen. Aufgrund der Effizienz und Präzision dieser Systeme reduzieren sie das Risiko für zivile Einrichtungen und Personen. Um dies jederzeit zu gewährleisten, sollen die Staaten sich auf *jeweils eigene* Standards beziehen. Versuche, universelle Parameter für *kritische Funktionen*, d. h. Zielauswahl und -bekämpfung, festzulegen, werden nicht als erfolgversprechend angesehen. Es ist z. B. zweifelhaft, ob Kriterien für ein Mindestmaß an *Bedeutsamkeit* menschlicher Kontrolle entwickelt werden können (CCW GGE 2018d).

China

China definiert LAWS anhand von fünf Charakteristika[132] (CCW GGE 2018c):

1. Tödlichkeit, d. h. eine ausreichende Tragkraft für eine tödliche Ladung;
2. Autonomie, d. h. Abwesenheit von menschlicher Intervention und Kontrolle während des gesamten Prozesses der Ausführung einer Aufgabe;
3. Unmöglichkeit des Abbruchs, d. h., es gibt kein Mittel, das Gerät zu stoppen, nachdem es aktiviert wurde;
4. unterschiedslose Wirkung, d. h., das Gerät führt die Aufgabe der Tötung und Verstümmelung aus, ohne Rücksicht auf Bedingungen, Szenarien und Art der Ziele;

132 Leider ist im Originaltext an vielen Stellen völlig unklar, was genau gemeint ist. Über die Gründe dafür soll an dieser Stelle nicht spekuliert werden.

5. Evolution, d. h., das Gerät kann durch Interaktion mit der Umwelt lernen, seine Funktionen und Fähigkeiten in einer Weise erweitern, dass sie menschliche Erwartungen übertrifft.

China äußert die Befürchtung, dass LAWS die Schwelle für kriegerische Auseinandersetzungen senken können. Gleichzeitig würden die Kosten der Kriegsführung gesenkt (dabei bleibt in dem Statement offen, ob nur finanzielle oder auch politische Kosten und/oder der Verlust von Soldaten gemeint ist). Es wird klar formuliert, dass LAWS weder zur effektiven Diskriminierung zwischen Kombattanten und Zivilisten noch zu Einschätzungen hinsichtlich der Verhältnismäßigkeit fähig sind. Auch ist schwierig zu etablieren, wer die Verantwortung bei einem Einsatz von LAWS trägt. Daher ruft China alle Staaten auf, Vorsicht walten zu lassen. Nationale Waffenprüfungen (nach Artikel 36 ZP I) sind positiv zu bewerten, können aber keinesfalls die grundsätzlichen Bedenken ausräumen, die LAWS aufwerfen.

Aus diesem Grund befürwortet China die Entwicklung eines bindenden Protokolls zu LAWS im Rahmen der CCW, ähnlich dem über blind machende Laserwaffen (Chinese Delegation o. J., S. 1).[133] Die Bezugnahme auf dieses Protokoll ist bemerkenswert, denn es wurde geschaffen, um ein präventives Verbot für Laserblendwaffen zu installieren. Andererseits hat China bis heute weder eine schlüssige Definition noch konkrete Charakteristika für LAWS vorgebracht, die unter ein solches Protokoll fallen würden. Darüber hinaus bezieht sich der Vorschlag explizit nur auf den Einsatz von LAWS, aber nicht auf die Entwicklung, Produktion oder Beschaffung. Insgesamt betrachtet ist die Position Chinas ambivalent und schwierig zu fassen und einzuschätzen (siehe dazu auch die Analyse von Kania 2018).

Dieser Eindruck verstärkt sich, da gleichzeitig der positive Beitrag herausgestrichen wird, den KI auf die wirtschaftliche und soziale Entwicklung in vielen Ländern leistet. Aus diesem Grund wird gefordert, dass voreilige Handlungen in Bezug auf LAWS die zukünftige Entwicklung und Nutzung von KI nicht hemmen dürfen (CCW GGE 2018c). Aber auch im militärischen Bereich treibt China die Nutzung von KI dynamisch voran. KI wird als Schlüsseltechnologie gesehen, um im globalen wirtschaftlichen und militärischen Wettbewerb bestehen zu können. KI gilt als Instrument, um technologische Entwicklungsstufen überspringen zu können und mit Rivalen wie den USA technologisch gleichziehen oder sie sogar überholen zu können (Allen 2019; Kania 2017).

133 Im Original »China supports the development of a legally binding protocol on issues related to the use of LAWS, similar to the Protocol on Blinding Laser Weapons, to fill the legal gap in this regard.«

Bewegung der Blockfreien Staaten

Die Bewegung der Blockfreien Staaten[134] äußert Besorgnis, da LAWS viele ethische, moralische, rechtliche, technische sowie den internationalen Frieden und die Stabilität betreffende Fragen aufwerfen. Sie setzt sich dafür ein, dass konkrete Schritte unternommen werden einschließlich der Elemente eines rechtlich bindenden Instrumentariums zur Regulierung bzw. zum Verbot von LAWS. Weichere Instrumente wie politische Deklarationen, »codes of conduct« und andere freiwillige Maßnahmen sind nicht geeignet, rechtlich verbindliche Instrumente zu ersetzen. Die Staatengemeinschaft wird aufgefordert, bis zur Umsetzung solcher Instrumente ein Moratorium für die weitere Entwicklung und die Nutzung von LAWS zu erklären (CCW GGE 2018g).

Internationales Komitee vom Roten Kreuz

Nach Ansicht des IKRK sollte das Ziel der CCW GGE sein, sich auf Grenzen für die Autonomie von Waffensystemen zu einigen. Relevant sind dabei insbesondere die kritischen Funktionen der Zielauswahl und -bekämpfung und nicht z. B. Navigation oder Flugsteuerung. Ein Minimum an menschlicher Kontrolle ist sowohl aus ethischen als auch aus rechtlichen Erwägungen unabdingbar. Ein vollständig autonomes Waffensystem ohne jegliche menschliche Kontrolle ist deshalb unzulässig. Aber auch jenseits vollautonomer Waffensysteme besteht ein Spektrum von Risiken, das von der internationalen Staatengemeinschaft nicht übersehen werden sollte. Da technologische Entwicklungen, die die direkte menschliche Kontrolle über Waffensysteme mindern, den internationalen Diskurs über diese Fragen abzuhängen drohen, wird den Staaten angeraten, die Aufgabe, Autonomie in Waffensystemen zu beschränken, mit hoher Dringlichkeit anzugehen (IKRK 2018b).

Kasten 9.4 Aktuelle Position des IKRK

Das IKRK ist der Auffassung, dass ein Standard formuliert werden soll, der die Art und Qualität menschlicher Kontrolle definiert, die für die Einhaltung des HVR und ethischer Prinzipien erforderlich ist. Auf dem Weg zu einem solchen Standard, der der Autonomie von Waffensystemen Grenzen setzt, wird die Beantwortung einiger Schlüsselfragen als erforderlich angesehen (IKRK 2019):

134 Internationale Organisation mit derzeit 120 Mitgliedstaaten, deren Ursprung ihre Neutralität während des Ost-West-Konflikts zwischen NATO und Warschauer Pakt war; sie setzt sich für eine Gleichberechtigung zwischen den Staaten ein.

- Muss die menschliche Aufsicht über ein Waffensystem mit der Möglichkeit, einzugreifen und es ggf. zu deaktivieren, während der gesamten Operation dauerhaft gewährleistet sein? Welche Ausnahmen sind zulässig?
- Muss es verpflichtend sein, dass ein menschlicher Operator in der Lage ist, mit hoher Sicherheit vorherzusagen, dass die Waffe ein spezifisches Ziel zu einem spezifischen Zeitpunkt angreifen wird und welche Auswirkungen dies haben wird? Welche Ausnahmen sind zulässig?
- Welchen Standards hinsichtlich der Zuverlässigkeit sollen Waffen, die in ihren kritischen Funktionen über Autonomie verfügen, genügen? Wie soll dies überprüft werden?
- Angenommen, dass LAWS zur Selektion und zum Angriff materieller Ziele (d. h. Dinge) akzeptabel wären – welche operationellen Einschränkungen würden daraus folgen, insbesondere hinsichtlich ihres Operationsraums (z. B. besiedelte oder unbesiedelte Gebiete) und der Dauer ihrer Operation? Wäre dies für mobile bzw. stationäre Systeme unterschiedlich?

9.2.3 Gemeinsamer Vorschlag von Deutschland und Frankreich auf der CCW GGE

Auf dem Treffen der GGE im November 2017 ergriffen Deutschland und Frankreich die Initiative und brachten gemeinsam einen ersten konkreten Vorschlag ein, wie die internationale Gemeinschaft mit LAWS umgehen kann (CCW GGE 2017a). Ausgehend von der Prämisse, dass LAWS gegenwärtig noch nicht existieren und die Staaten sich noch kein umfassendes Bild über die Charakteristika der zu regulierenden Systeme machen konnten, wird eine umfassende Regulierung zum gegenwärtigen Zeitpunkt als verfrüht angesehen. Zudem wird der Diskussionsstand der CCW so eingeschätzt, dass »eine internationale Ächtung entsprechender Waffensysteme aufgrund der unterschiedlichen Positionierung der Vertragsstaaten der CCW aktuell nicht durchsetzbar erscheint« (Bundesregierung 2018f). Stattdessen wird eine politische Deklaration vorgeschlagen, flankiert von transparenz- und vertrauensbildenden Maßnahmen.

Im Zentrum der politischen Deklaration (CCW GGE 2017a, S. 3) soll eine Bekräftigung der Staaten stehen, dass weiterhin Menschen die letztendliche Entscheidung über den Einsatz tödlicher Gewalt treffen und ausreichende Kontrolle über tödliche Waffensysteme ausüben werden. Außerdem soll erklärt werden, dass die völkerrechtlichen Regelungen, insbesondere das HVR, uneingeschränkt auf die Entwicklung und Nutzung von LAWS anwendbar sein sollen.

Auf freiwilliger Basis können Maßnahmen getroffen werden, die die Transparenz und gegenseitiges Vertrauen (CCW GGE 2017a, S. 3 f.) stärken. Konkret genannt werden erstens die Identifikation und Austausch von Best-Practice-Beispielen für Waffenprüfungen gemäß Artikel 36 ZP I (Kap. 7.1), zweitens die Erlaubnis für Beobachter, an Demonstrationen zukünftiger LAWS teilzuneh-

men, sowie drittens der gegenseitige Austausch von Informationen. Der Vorschlag sieht darüber hinaus vor, dass auf Basis der politischen Deklaration als nächster Schritt ein »code of conduct« (CCW GGE 2017a, S. 4) entwickelt wird, der politisch bindende Regeln für die Entwicklung und die Nutzung von LAWS ausformuliert.

Zusätzlich wird vorgeschlagen, im Rahmen der CCW ein Komitee technischer Experten (CCW GGE 2017a, S. 4) einzurichten, das den Auftrag hat, die Staaten regelmäßig über neue technologische Entwicklungen mit Relevanz für LAWS zu unterrichten, damit die Staaten Maßnahmen entwickeln und umsetzen können, mit denen die spezifischen Herausforderungen durch LAWS beantwortet werden könnten.

Die Reaktionen auf den deutsch-französischen Vorschlag waren gemischt. Die meisten Stimmen begrüßten ihn als konstruktiven Schritt in die richtige Richtung. Die im Vorschlag vertretene Linie erhielt »als Mittelweg Unterstützungszusagen zahlreicher Staaten« (Bundesregierung 2018d, S. 58). Einige Delegationen und insbesondere die Akteure aus dem NGO-Segment der CCW kritisierten den Vorschlag dagegen als nicht ambitioniert genug. In der Tat drückt die von Deutschland und Frankreich angestrebte politische Deklaration im Großen und Ganzen lediglich den Minimalkonsens der Staaten aus, wie er in den Ergebnisprotokollen der CCW GGE festgehalten wurde (CCW 2016a; CCW GGE 2017e u. 2018a), und die transparenz- und vertrauensbildenden Maßnahmen sind deutlich weniger weitreichend, als es insbesondere das von den NGOs geforderte Moratorium bzw. Komplettverbot ist.

Einige Delegationen wiesen auf die Schwäche von auf Freiwilligkeit basierenden Maßnahmen hin und sahen diese lediglich als Zwischenschritt auf dem Weg zu einem rechtlich bindenden Instrumentarium, beispielsweise in Form eines neuen Protokolls der CCW[135] (ähnlich dem zum Verbot von Laserblendwaffen von 1995). Andere unterstrichen die Notwendigkeit, das Wissen und gemeinsame Verständnis der Thematik zu vertiefen, bevor eine bestimmte Handlungsoption geprüft werden kann (CCW GGE 2018a, S. 12 f.). Diejenigen Länder, die ein direktes Verbot befürworten,[136] hielten dagegen, dass ihrer Meinung nach LAWS dem humanitären Völkerrecht fundamental entgegenstehen, und daher bis zur Ausarbeitung eines Verbots ein sofortiges Moratorium in Kraft gesetzt werden muss, weil ansonsten eine unkontrollierte Proliferation von LAWS zu befürchten ist (Rosen Jacobson 2017, S. 4 ff.).

135 Gesetz zum Protokoll II in der am 3. Mai 1996 geänderten Fassung und zum Protokoll IV vom 13. Oktober 1995 zum UN-Waffenübereinkommen vom 18. April 1997

136 Zum Stichtag 22. November 2018 waren dies 28 Länder: Ägypten, Algerien, Argentinien, Bolivien, Brasilien, Chile, China, Costa Rica, Djibouti, Ecuador, El Salvador, Ghana, Guatemala, Heiliger Stuhl, Irak, Kolumbien, Kuba, Mexiko, Marokko, Nicaragua, Österreich, Pakistan, Panama, Peru, Simbabwe, Staat Palästina, Uganda, Venezuela (Campaign to Stop Killer Robots 2018). Hinzu kommt Belgien, da das belgische Parlament am 13. Juli 2018 eine Resolution verabschiedete, die die Regierung aufforderte, dem belgischen Militär die Verwendung von LAWS zu untersagen (Walsh 2018).

Der NGO-Verbund Campaign to Stop Killer Robots ist der Ansicht, dass politische Deklarationen, »codes of conduct« und andere Maßnahmen nicht geeignet sind, die vielfältigen und ernsten ethischen, juristischen, operationellen und technischen Herausforderungen zu meistern, die von LAWs gestellt werden. Daher wird gefordert, dass die Staaten der CCW in formelle Verhandlungen einsteigen sollen, mit dem Ziel, ein verbindliches Protokoll zu vereinbaren, das ein Verbot der Entwicklung, der Produktion und des Einsatzes von vollständig autonomen Waffensystemen vorsieht (Campain to Stop Killer Robots 2017).

9.2.4 Ausgangslage für die weitere Diskussion im Rahmen der CCW

Im Rahmen der informellen Expertentreffen (2014–2016) und der ersten Arbeitstreffen der GGE (2017 und 2018) konnte eine allgemeine Zustimmung der Staatenvertreter zu einigen grundlegenden Punkten erzielt werden, die die Basis für die weitere Diskussion im Rahmen der CCW bilden (CCW 2016a; CCW GGE 2017e u. 2018a):

- Ein Staat trägt die rechtliche und politische Verantwortung für jeden Einsatz der Waffensysteme seiner Streitkräfte und hat für die daraus resultierende Taten eine Verantwortlichkeit unter Beachtung des (humanitären) Völkerrechts sicherzustellen (CCW 2016a, Punkt 2a).[137]
- Konzepte darüber, was eine angemessene menschliche Einbindung in Bezug auf Entscheidungen über die Anwendung tödlicher Gewalt darstellt, sind essenziell für die weitere Erörterung von LAWS (CCW 2016a, Punkt 2b).[138]
- Zivile Organisationen, die Industrie, Forscher und Wissenschaft sollen weiterhin eine wichtige Rolle in den CCW-Verhandlungen spielen (CCW 2016a, Punkt 2c).[139]
- Die Diskussion über neue und für das Feld der LAWS relevante Technologien soll weiterhin eine der Prioritäten für die CCW sein (CCW 2016a, Punkt 2d).[140]

137 Im Original: »A state will bear the legal and political responsibility and establish accountability for action by any weapon system used by the state's forces in accordance with applicable International Law, in particular International Humanitarian Law.«

138 Im Original: »Views on appropriate human involvement with regard to lethal force and the issue of delegation of its use are of critical importance to the further consideration of LAWS amongst the High Contracting Parties and should be the subject of further consideration.«

139 Im Original: »Civil society organizations, industry, researchers and scientific organizations should continue to play an important role in exploring the prospective issue in accordance with the established procedural rules of the CCW.«

140 Im Original: »The discussion on emerging technologies in the area of LAWS is one of the priorities for the CCW and should be continued, while not prejudging discussions in other relevant fora.«

- Gleichzeitig wird darauf hingewiesen, dass in Anbetracht der Dual-Use-Eigenschaften von Technologien für autonome Systeme keine der Aktivitäten der CCW GGE den Fortschritt oder den Zugang zu ziviler Forschung, Entwicklung und Anwendung dieser Technologien behindern darf (CCW GGE 2017e).

Als wichtige Punkte, die es im weiteren Verlauf der CCW-Verhandlungen zu berücksichtigen und zu klären gilt, wurden festgehalten (CCW 2016a, Punkt 4; CCW GGE 2017e u. 2018a):

- Identifizierung von Charakteristika und Ausarbeitung einer Arbeitsdefinition von LAWS;
- Anwendung und Einhaltung der relevanten rechtlichen Grundsätze und Regeln des internationalen Rechts, insbesondere des HVR, im Hinblick auf LAWS;
- Einhaltung von relevanten Menschenrechten;
- rechtliche und politische Verantwortung und Festlegung von Rechenschaftspflichten;
- ethische und moralische Fragen;
- Auswirkungen auf die regionale sowie internationale Sicherheit und Stabilität;
- Einflüsse auf die Hemmschwelle zu bewaffneten Konflikten;
- Risiko eines Wettrüstens;
- militärischer Nutzen und Risiken;
- Risiko der Weiterverbreitung, inklusive unter Beteiligung nichtstaatlicher Akteure;
- Risiken von Cyberoperationen in Bezug auf LAWS.

Dieses umfassende Arbeitsprogramm ist ambitioniert, wenn man sich vor Augen führt, wie bedächtig die bisherige Diskussion in den letzten Jahren vonstatten ging. Da für Beschlüsse im Rahmen der CCW Einstimmigkeit erforderlich ist, ist absehbar, dass Debatten um konkrete Handlungsoptionen zäh verlaufen und lediglich einen Minimalkonsens zum Ergebnis haben könnten.

Kasten 9.5 Die weitere Arbeit der CCW

In der Zusammenfassung des Stands der Diskussionen der CCW-GGE-Sitzungen 2018 sind die bis dahin erzielten Gemeinsamkeiten unter der Überschrift »Mögliche Leitlinien« (CCW GGE 2018k, S. 4) aufgelistet. Daran, wie allgemein gehalten einige der Punkte sind, lässt sich ablesen, wie weit der Weg zu einem gemeinsamen Verständnis in strittigeren Fragen noch ist.

- Das HVR ist weiterhin auf alle Waffensysteme anwendbar einschließlich der möglichen Entwicklung und des Einsatzes von LAWS.

- Die menschliche Verantwortung für Entscheidungen bezüglich des Einsatzes von Waffensystemen muss gewahrt bleiben, da die Rechenschaftspflicht nicht auf Maschinen übertragen werden kann. Dies trifft für den gesamten Lebenszyklus eines Waffensystems zu.
- Die Rechenschaftspflicht bezüglich der Entwicklung, Stationierung und des Einsatzes jeglicher im Rahmen der CCW zu betrachtender neuer Waffensysteme muss im Einklang mit geltendem Völkerrecht gewährleistet sein einschließlich des Betriebs dieser Waffensysteme innerhalb einer verantwortlichen menschlichen Kommandokette.
- Im Einklang mit ihren völkerrechtlichen Verpflichtungen sollten Staaten bei Forschung, Entwicklung, Erwerb bzw. Einführung neuer Waffen oder Mittel und Methoden der Kriegsführung prüfen, ob deren Einsatz immer oder unter gewissen Umständen völkerrechtlich verboten sein könnte.
- Wenn neue Waffensysteme entwickelt oder erworben werden, die auf aufkommende Technologien im Bereich LAWS basieren, sollten deren physische Sicherheit, angemessene nichtphysische Sicherheitsmaßnahmen (einschließlich Cybersicherheit gegen »hacking« oder »spoofing«), das Risiko, dass terroristische Gruppierungen sie beschaffen, sowie das Risiko der Proliferation beachtet werden.
- Die Bewertung von Risiken und Maßnahmen zu deren Begrenzung sollte Teil des Zyklus von Design, Entwicklung, Test und Stationierung von aufkommenden Technologien in jeglichen Waffensystemen sein.
- In Bezug auf die Nutzung aufkommender Technologien im Bereich LAWS sollte beachtet werden, dass die Einhaltung des HVR sowie weiterer internationaler Verpflichtungen aufrechterhalten wird.
- Bei der Ausgestaltung möglicher politischer Maßnahmen sollten aufkommende Technologien im Bereich LAWS nicht vermenschlicht dargestellt werden.
- Diskussionen und mögliche politische Maßnahmen im Rahmen der CCW sollten den Fortschritt bzw. den Zugang zu friedlichen Nutzungen intelligenter autonomer Technologien nicht behindern.
- Die CCW, deren Zielsetzung es ist, einen Ausgleich zwischen militärischen Notwendigkeiten und humanitären Erwägungen zu schaffen, bietet einen angemessenen Rahmen, um das Themenfeld der aufkommenden Technologien im Bereich LAWS zu behandeln.

Das Arbeitsprogramm der CCW-GGE-Sitzung im März 2019 konzentrierte sich auf fünf Punkte (CCW GGE 2019):

- Exploration der möglichen Herausforderungen durch aufkommende Technologien im Bereich LAWS in Bezug auf das HVR;

- Charakterisierung der zu berücksichtigenden Systeme für ein gemeinsames Verständnis der Konzepte und Eigenschaften, die in Bezug auf die Zielsetzungen der CCW relevant sind;
- weitere Betrachtung des menschlichen Elements bei der Anwendung tödlicher Waffengewalt; Aspekte der Mensch-Maschine-Interaktion bei Entwicklung, Stationierung und beim Einsatz von aufkommenden Technologien im Bereich LAWS;
- Prüfung möglicher militärischer Anwendungen von im Kontext der Arbeit der GGE relevanten Technologien;
- Erörterung von Möglichkeiten des Umgangs mit humanitären und sicherheitspolitischen Herausforderungen, die durch aufkommende Technologien im Bereich LAWS in Bezug auf die Zielsetzungen der CCW gestellt werden unter Berücksichtigung vergangener, jetziger und zukünftiger Vorschläge, ohne dabei politische Ergebnisse vorwegzunehmen.

Die Resultate der Arbeitssitzung sollen wie in den vergangenen Jahren in einen Bericht münden, der in der zweiten Sitzung im August 2019 verabschiedet werden soll.

9.3 Regulierungsansätze der präventiven Rüstungs- und Exportkontrolle

Der zunehmende Einsatz unbemannter Waffensysteme ist zu einem Symbol für die sich wandelnde Kriegsführung des 21. Jahrhunderts geworden, und automatisierte oder zukünftig autonome Waffensysteme könnten hierbei einen entscheidenden Paradigmenwechsel darstellen. AWS stellen in vielerlei Hinsicht eine Herausforderung dar und werfen zahlreiche Fragen auf, sowohl was ihre Übereinstimmung mit den Prinzipien des humanitären Völkerrechts angeht als auch die Auswirkungen, die ihre Verbreitung und ihr Einsatz entfalten können, gerade auch in Bezug auf potenzielle Rüstungsdynamiken, die internationale Sicherheit sowie regionale und strategische Stabilität.[141]

Bei dem im Rahmen der CCW geführten Diskurs steht die Frage der Kompatibilität von AWS mit dem HVR im Mittelpunkt. Ihre potenziell destabilisierenden Wirkungen im Hinblick auf die internationale Sicherheitspolitik und zwischenstaatliche Krisenstabilität sind jedoch bislang unzureichend thematisiert worden.

Präventive Rüstungskontrolle dient der Identifikation und Ausarbeitung von rüstungskontrollpolitischen Regulierungsansätzen für zukünftige, bisher nicht stationierte Waffensysteme, mit dem konkreten Ziel, der destabilisierenden Wirkung von potenziellen Rüstungswettläufen und den Gefahren militärischer Eskalationsmechanismen bereits im Vorfeld zu begegnen (Neuneck/Mutz

141 Dieses Kapitel stützt sich maßgeblich auf Alwardt et al. (2017, 84 ff.).

2000; Petermann et al. 1997). Angesichts der zunehmend beschleunigten technologischen Entwicklungen, z. B. in den Feldern Robotik und Informationstechnologie, »gibt es gegenwärtig mehr denn je einen Bedarf für präventive Rüstungskontrolle« (Dickow et al. 2015b, S. 67).

Aus Sicht des TAB ist präventive Rüstungskontrolle ein breitangelegter Prozess, der darauf abzielt, die möglicherweise problematischen Konsequenzen technologischer Entwicklungen frühzeitig zu erkennen, für die in politischer Verantwortung stehenden Entscheidungsträger beurteilbar zu machen und durch Institutionen und Verfahren auf nationaler und internationaler Ebene in ihren Risiken zu begrenzen (Petermann et al. 1997, S. 17).

Ob dies im konkreten Fall von AWS erfolgversprechend ist, wird von einigen vor dem Hintergrund bisheriger Erfahrungen skeptisch gesehen. So merkt Geiß (2015, S. 5) an, dass »traditionell [...] das Völkerrecht bei der Regulierung neuer Waffentechnologien regelmäßig mindestens einen Krieg zu spät« kam. Und Nasu und McLaughlin (2014, S. 53) weisen darauf hin, dass – obschon es historische Präzedenzfälle dafür gibt, dass Waffensysteme vor ihrer Stationierung verboten wurden – es unwahrscheinlich ist, dass dies geschieht, bevor ihre Fähigkeiten vollständig untersucht und verstanden worden sind. Um dies einschätzen zu können, müssten AWS erst einmal mindestens bis kurz vor ihrer Einsatzreife erforscht und entwickelt werden. Wenn dabei ein erheblicher militärischer Nutzen festgestellt wird, wäre es schwierig, ein Verbot oder auch nur eine Beschränkung umzusetzen, denn es gäbe einen inversen Zusammenhang zwischen dem strategisch militärischen Nutzen einer Waffe und der Bereitschaft eines Staates, Restriktionen zuzustimmen.

Scharre (2017, S. 30) führt weiter aus: Ein wesentlicher Faktor für die Erfolgschancen eines Waffenverbots ist die Abwägung zwischen der wahrgenommenen Abscheulichkeit (»horribleness«) der Waffe und deren militärischem Nutzen. Viele Waffen, die verboten wurden, besitzen nur geringen militärischen Nutzen, aber verursachen großes Leid oder wirken in hohem Maße destabilisierend (z. B. Blendlaser, auf einer Erdumlaufbahn stationierte Massenvernichtungswaffen). Einschränkungen für Waffen zu erreichen, die zwar schrecklich sind, aber gleichzeitig kriegsentscheidende Vorteile versprechen, ist erheblich schwieriger. Als instruktives Beispiel hierfür kann die anhaltende Kontroverse um die Ächtung von Streumunition herangezogen werden. Das Totalverbot dieser Waffen, zu dem die internationale Staatengemeinschaft im Jahr 2008 in der CCM (Convention on Cluster Munitions/Übereinkommen über Streumunition) übereinkam, weist zwar derzeit 120 Signatarstaaten auf (davon haben 17 noch nicht ratifiziert), allerdings befinden sich die Großmächte China, Russland sowie die Vereinigten Staaten[142] nicht darunter (ICBL-CMC 2017).

142 Eine Direktive der Administration von US-Präsident G.W. Bush, die vorsah, bis Ende 2018 praktisch jegliche Streumunition aus den aktiven Arsenalen zu entfernen und schließlich zu vernichten, wurde am 30. November 2017 außer Kraft gesetzt (HRW 2017).

Im Fall AWS kommt erschwerend hinzu, dass die Schlüsseltechnologien für Autonomie zu einem großen Teil im zivilen Umfeld entwickelt und somit potenziell breit verfügbar sein werden. Dies macht es wahrscheinlich, dass unabhängig vom Ausmaß internationaler Ächtung von AWS potente terroristische Gruppierungen oder »Schurkenstaaten« (Scharre 2017, S. 31) diese bauen.

Zudem birgt die Verifikation von Abkommen über AWS große Herausforderungen. Zwar sind formelle Verifikationsregime nicht zwingend notwendig für die Einhaltung von Abkommen, ein hohes Maß an gegenseitiger Transparenz dagegen schon. Wie diese Transparenz hergestellt werden kann, wenn der Unterschied zwischen einer verbotenen und einer erlaubten Waffe lediglich in deren Software liegt, ist gegenwärtig völlig unklar (Scharre 2017, S. 31 f).

Überblick über Regulierungsansätze

Es existiert ein weites Spektrum an Möglichkeiten der Regulierung und Einhegung von Waffensystemen. Diese können zum einen an unterschiedlichen Tatbeständen ansetzen, üblicherweise kommen hier Entwicklung, Test, Besitz, Transfer/Handel, Stationierung und/oder Einsatz der Waffensysteme in Betracht. Eine zweite Dimension ist die Stringenz der Regulierung, die von eher weichen Instrumenten – wie vertrauens- und sicherheitsbildenden Maßnahmen, freiwillige Selbstverpflichtungen entweder unilateral erklärt oder international abgestimmt – bis hin zu harter Regulierung durch verbindliche Abkommen mit Verifikationsmechanismen reichen. Die Kunst der Rüstungskontrollpolitik besteht darin, aus diesem Spektrum diejenigen Maßnahmen auszuwählen, die auf Basis der eigenen Wertvorstellungen und Intentionen den größten nationalen und kollektiven Nutzen im Hinblick auf Sicherheit und Risikoabwehr erzeugen. Dabei kommt es nicht nur auf die Wünschbarkeit der Maßnahmen an, sondern auch entscheidend darauf, welche davon in Kooperation mit Partnern im internationalen Rahmen umsetzbar erscheinen.

In Bezug auf die existierenden Rüstungskontrollverträge können AWS, wie in Kapitel 9.1.1 ausgeführt, bisher allenfalls unter die sehr weit gefassten Definitionen der Hauptwaffensysteme fallen und würden in speziellen Fällen den Beschränkungen von INF und New Start unterliegen oder in gegenseitigem Einvernehmen unter die Limitierungen des multilateralen KSE-Vertrags fallen, der jedoch von Russland aufgekündigt wurde und keine vielversprechende Zukunft mehr zu haben scheint. Darüber hinaus werden AWS auch von einigen internationalen Abkommen zu Exportkontrolle und Vertrauensbildung erfasst (Kap. 9.1.2 u. 9.1.3). Da weder Drohnen noch allgemeine Robotik derzeit universellen rüstungskontrollpolitischen Beschränkungen unterliegen (Dickow et al. 2015b, S. 71), gibt es bisher auch kein Rüstungskontrollabkommen, das explizit autonome Waffensysteme benennt und in irgendeiner Form Regulierungen unterwirft.

Welches aber wären überhaupt Instrumentarien der konventionellen Rüstungskontrolle oder VSBM, die in Bezug auf AWS Anwendung finden könnten? In der folgenden Tabelle 9.4 ist eine Auswahl möglicher Ansätze zur Regulierung von AWS aufgelistet, jeweils charakterisiert nach Art des Abkommens und der Verbindlichkeit der Regulierung. Die letzte Spalte enthält eine Einschätzung, ob Verifikationsmaßnahmen eine notwendige Voraussetzung für das Zustandekommen und den Bestand der jeweiligen Abkommen wären. Oftmals stellen die Erfahrungen, die im Zuge der Erprobung geeigneter Verifikationsmechanismen gemacht werden, die Weichen, ob es am Ende bei einer VSBM bleibt oder aber ein rechtlich verbindliches Rüstungskontrollabkommen geschaffen werden kann. Auf jeden Fall schafft eine verlässliche Verifikation ein erhebliches Maß an Vertrauen in ein Abkommen, das aber auch von beiden (oder allen) Vertragsparteien gewollt sein muss.

Tab. 9.4 Mögliche Ansätze zur Regulierung von AWS

	Art des Abkommens	Verifikation
Transparenzmaßnahmen, z. B. freiwillige Offenlegung der eigenen Bestände an AWS	VSBM (auch unilateral möglich)	freiwillig
freiwilliger Verzicht auf den Besitz und/oder Einsatz von AWS (»code of conduct«)	VSBM (auch unilateral möglich)	freiwillig
Exportkontrolle oder -monitoring von AWS oder spezifischer Teilkomponenten (Schwierigkeit Dual-Use-Dilemma)	Nichtverbreitung (auch unilateral möglich)	freiwillig
Beschränkung der militärischen Nutzung von AWS über die Definition von nationalen oder internationalen Einsatzregeln bzw. dem Ausschluss bestimmter Fähigkeiten (»rules of engagement«)	VSBM (auch unilateral möglich) oder internationaler Rüstungskontrollvertrag (verbindlich)	national: freiwillig, international: ggf. notwendig
regionale oder internationale Begrenzung der Arsenale	Rüstungskontrollvertrag (verbindlich)	notwendig
internationale Ächtung von AWS (im UN-Rahmen)	Rüstungskontrollvertrag (verbindlich)	notwendig

Quelle: Alwardt et al. 2017, S. 86

9.3.1 Vertrauens- und sicherheitsbildende Maßnahmen

Wie in Kapitel 9.1.2 erläutert, existiert besonders in Europa bereits eine Reihe von Ansätzen im Bereich der VSBM, die bisher jedoch nicht dezidiert auf AWS zugeschnitten sind. Zukünftige VSBM könnten Transparenzmaßnahmen wie die Offenlegung der eigenen Bestände an automatisierten oder autonomen Waffensystemen und ihrer Stationierungsorte beinhalten sowie die Vorführung ihrer Fähigkeiten umfassen. In diesem Zusammenhang ist das Wiener Dokument hervorzuheben, das zusätzlich auch Verifikationsmechanismen beinhaltet, bisher aber auf den OSZE-Raum beschränkt ist. Die Verabschiedung eines ähnlich gearteten, aber weltweit gültigen und um bestimmte automatisierte sowie zukünftige autonome Waffensysteme erweiterten Abkommens im UN-Rahmen wäre eine wirkungsvolle VSBM. Mittels VSBM könnten auch Maßnahmen erprobt werden, die zu einem späteren Zeitpunkt und im Zusammenhang mit konkreten Rüstungskontrollmaßnahmen als Elemente zukünftiger Verifikationsmaßnahmen fungieren.

Weitere weiche Maßnahmen, die zwischen den Staaten freiwillig oder auch unilateral umsetzbar wären, sind der Austausch von Erfahrungen und Best-Practice-Beispielen beim Umgang und bei der Einschätzung und Regulierung von Autonomie in den verschiedenen Technologiefeldern. Dies könnte auch z. B. die gemeinsame Entwicklung von Standards, Methoden und Protokollen für den Test und die Validierung autonomer Waffensysteme umfassen (CCW GGE 2018a, S. 3).

Daneben steht es jedem Staat aber frei, selber Zeichen zu setzen und den zukünftigen Einsatz potenter AWS eigenen strengen Regeln zu unterwerfen (»rules of engagement«). Diese könnten z. B. in der Beschränkung der maximalen Reichweite oder der Zuladung von AWS bestehen. Möglich sind aber auch selbstauferlegte Beschränkungen beim Einsatzspektrum, z. B. verbindliche Festlegungen, bewaffnete Systeme ausschließlich für den Eigenschutz im Rahmen der Luftnahunterstützung einzusetzen (Schörnig 2014).

Noch stärker wäre das Signal, wenn ein Staat bzw. eine Staatengruppe von vornherein auf die Entwicklung und Stationierung von AWS verzichten würde. Würde ein Staat diese freiwilligen Selbstbeschränkungen noch für andere Staaten überprüfbar machen (Selbstauferlegung freiwilliger Verifikationsmaßnahmen), so wäre dies hochwirksam im Sinne der Sicherheits- und Vertrauensbildung und könnte mit der Zeit Nachahmer unter anderen Staaten finden.

Ein Zwischenschritt zu einem verbindlichen Rüstungskontrollabkommen wäre es, aus dem hier aufgefächerten Strauß möglicher Maßnahmen ein geeignetes Bündel auszuwählen und als internationale Selbstverpflichtung (»code of conduct«) festzuschreiben, wie dies im deutsch-französischen Vorschlag auf der GGE skizziert wurde (Kap. 9.2.3).

Aber auch jenseits der großen Bühne internationaler Politik spielen Selbstverpflichtungen, »codes of conduct«, Ethikkodizes oder Richtlinien zur Sicherstellung guter fachlicher Praxis eine nicht zu unterschätzende Rolle bei der Eindämmung von Risiken emergenter Technologien. Eines der ersten und vielleicht das erfolgreichste Beispiel dafür sind die 1975 geschaffenen Richtlinien zum Umgang mit Risiken eines Zweigs der seinerzeit gerade aufkommenden Gentechnik (genauer der rekombinanten DNA)[143] der Asilomar-Konferenz (Spektrum 1999). Basierend auf diesem Vorbild wurde Anfang 2017 vom Future of Life Institute (FLI o. J.b) eine Konferenz zum Thema »Beneficial AI« organisiert, auf der 23 Prinzipien beschlossen wurden, die als Material für Diskussion und gleichzeitig als ehrgeizige Ziele dienen sollten, damit KI in Zukunft die Lebensbedingungen von jedermann verbessern helfen kann.[144] Unter Punkt 18 heißt es dort: »An arms race in lethal autonomous weapons should be avoided«.

Ein anderer Ansatz, der in analoger Weise auf den Bereich KI/Robotik übertragbar wäre, wurde beim Thema Chemiewaffen in den Haager Ethikleitlinien« der OPCW (o. J.) umgesetzt.[145] Dort werden Normen und Kernsätze formuliert, die universelle Gültigkeit haben sollen. Sie richten sich an alle »Praktiker im Bereich Chemie« und rufen zu einer »verantwortungsbewussten Nutzung der Chemie« und zur »Unterstützung des Chemiewaffenübereinkommens« auf (OPCW 2015).

Auf dem Feld der KI/Robotik ist hier die »Ethically Aligned Design« der IEEE Global Initiative for Ethical Considerations in Artificial Intelligence and Autonomous Systems hervorzuheben. Das Institute of Electrical and Electronics Engineers (IEEE 2016) ist eine der größten professionellen Vereinigungen von Wissenschaftlern und Ingenieuren weltweit. Die Initiative hat zum Ziel, einen globalen Diskussionsprozess anzustoßen, der in Empfehlungen für eine ethische Governance von KI/autonomen Systemen/Robotik münden soll. Das Europäische Parlament hat bereits konkrete Vorschläge für ethische Verhaltenskodizes im Bereich der Robotik für Forscher, Ingenieure sowie für Ausschüsse für ethische Fragen in der Forschung in Form einer »Charta für Robotik« vorgelegt (EP 2017, S. 25 ff.). Bemühungen dieser Art um einen verantwortungsvollen Umgang mit diesen Technologien verdienen jede Unterstützung.

143 Ein Überblick zu deren Genese und Bedeutung findet sich z. B. beim Bayerischen Landesamt für Gesundheit und Lebensmittelsicherheit (Baiker 2014).

144 Die Liste der Unterzeichner umfasst aktuell 1.677 Forscher in den Feldern KI und Robotik sowie 3.662 weitere Personen, darunter Prominente wie der Physiker Stephen Hawking, Elon Musk (u. a. Tesla), Jaan Tallinn (Skype-Gründer), Erik Brynjolfsson (MIT), Ray Kurzweil (Google) und die Experten für AWS Ronald C. Arkin (Georgia Tech), Peter Asaro, Noel Sharkey; Stand Oktober 2020.

145 Diese gehen auf eine Initiative Deutschlands auf der Konferenz der Vertragsstaaten im Dezember 2014 zurück.

9.3.2 Exportkontrolle

Die Exportkontrolle ist ein probates Mittel zur Eindämmung der Proliferation von Waffentechnologien. Im Bereich konventioneller Waffen dient dies meist der Wahrung nationaler sicherheitspolitischer Interessen. Aufgrund ihres Eingriffs in internationale Handelsbeziehungen sind Exportkontrollen allerdings immer auch ein zweischneidiges Schwert. Die immanente Diskriminierung von Ländern, denen der Zugriff auf bestimmte Technologien verwehrt wird, kann ökonomischen Schaden verursachen, internationale Spannungen verstärken bzw. Gräben vertiefen, Vergeltungsmaßnahmen auslösen sowie nicht zuletzt Anreize liefern, sich die entsprechenden Güter auf anderen Wegen an den Exportkontrollen vorbei zu beschaffen.

Um die Weiterverbreitung von AWS einzuschränken, wäre ein speziell auf sie ausgerichtetes internationales Exportkontrollregime denkbar, z. B. auf Grundlage des ATT (Kap. 9.1.3) (Lewis et al. 2016, S. 78 ff.). Tatsächlich stehen bereits einige Technologien, Komponenten und Systeme mit Relevanz für AWS auf den einschlägigen Exportkontrolllisten des Wassenaar-Abkommens oder nationalen Listen für Exportbeschränkungen (z. B. die Ausfuhrlisten der deutschen AWV oder die Kontrolllisten nach den »International Traffic in Arms Regulations« und den »Export Administration Regulations« der USA; Stimson 2015, S. 11). Dazu zählen z. B. bewaffnete und bestimmte unbewaffnete UAVs, Flugkontrollsysteme, Managementsysteme mit Schwarmfähigkeiten oder bestimmte Navigationssysteme. Eine umfassende Exportkontrolle zur effektiven Eindämmung der Verbreitung von AWS würde jedoch auf einige schwer zu überwindende Hindernisse treffen. Zu nennen sind hier vor allem die Dual-Use-Problematik, die große Bedeutung von Software und daraus folgend die Schwierigkeiten bei der Verifikation von getroffenen Maßnahmen (AIV/CAVV 2015, S. 47).

Der ausgeprägte Dual-Use-Charakter der AWS zugrundeliegenden Technologien erschwert die Definition und Abgrenzung derjenigen Güter, deren Proliferation beschränkt werden soll, erheblich. Hinzu kommt, dass derzeit FuE in für AWS zentralen Technologiefeldern maßgeblich im zivilen Sektor vorangetrieben werden. Dies alles begünstigt ihre weitere Verbreitung ungemein. So ist es beispielsweise in der Forschung zu KI Usus, dass neben den Veröffentlichungen in Fachzeitschriften auch die Quellcodes der verwendeten Software frei zur Verfügung gestellt werden. Dass in erster Linie Algorithmen und Software bestimmend für AWS sein werden und nicht die Hardware, stellt die Eindämmung ihrer Verbreitung vor große Herausforderungen, denn Software kann viel leichter auf Datenträgern an Grenzkontrollen vorbei oder direkt elektronisch ins Ausland verbracht werden als materielle Güter.

Um Möglichkeiten auszuloten, trotz der beschriebenen Schwierigkeiten bei der Eindämmung der Proliferation Fortschritte zu erzielen, wäre die Entwick-

lung und der Austausch zu Best-Practice-Beispielen beim Umgang mit Exporten relevanter Güter, insbesondere Software, anzuraten. Hierfür wäre die Einbindung der relevanten Akteure in Wissenschaft und Wirtschaft sinnvoll (CCW GGE 2018c). Eine Reihe konkreter Vorschläge hierfür wird beispielsweise von Bromley/Maletta (2018, S. 34 ff.) entwickelt. Ein möglicher Schritt wäre ein auf die Nichtverbreitung von AWS ausgerichtetes globales Exportmonitoring. Organisiert werden könnte dies auf unterschiedlichste Weise, etwa formell innerhalb des UN-Waffenregisters oder auf informeller Basis ähnlich wie bei der Australia Group, die den Handel mit biologischen und chemischen Agenzien überwacht, um das Risiko der Proliferation entsprechender Waffen zu minimieren.[146] Dies könnte ggf. Rückschlüsse auf die Intentionen einzelner Staaten in Hinblick auf die Entwicklung oder Beschaffung von AWS erlauben. Es könnte der Erfassung wesentlicher technologischer Komponenten von AWS dienen und damit zugleich auch eine wirkungsvolle Grundlage für internationale oder nationale Exportkontrollmaßnahmen darstellen.

Da nicht nur im zwischenstaatlichen Bereich, sondern auch in substaatlichen Konflikten bis hin zu terroristischen oder kriminellen Hintergründen AWS unterschiedlichster Provenienz (bis hin zu improvisierten Gerätschaften) eine Gefahr darstellen können, ist auch zu überlegen, wie hier Zugangsbarrieren errichtet werden könnten. Brundage (2018, S. 41) beschreibt hierfür eine Reihe von Ansatzpunkten, u. a. den Erlass von Verkaufsbeschränkungen von potenziell gefährlichen Kleinstdrohnen (ähnlich der Waffengesetzgebung), die Registrierung und Kennzeichnung von Drohnen (z. B. mit einer Art Nummernschild), einen verpflichtenden Führerschein für bestimmte Typen von Drohnen sowie die Ausweisung und Durchsetzung von »no fly zones«.

9.3.3 Verbindliche Regulierung bzw. Verbot von AWS

Die Forderung, AWS weltweit zu ächten, wird insbesondere von NGOs und zurzeit 28 Staaten erhoben bzw. unterstützt.[147] Deren zentrales Argument ist, dass Maschinen niemals über Leben und Tod von Menschen entscheiden sollen. Dies widerspricht dem HVR und verletzt die Menschenwürde. Durch die daraus resultierende Entmenschlichung des Krieges sinkt die Hemmschwelle für Staaten, Konflikte mit Gewaltmitteln lösen zu wollen. Bis ein weltweites Verbot ausgehandelt und umgesetzt ist, wird angeregt, ein Moratorium für das Testen, die Herstellung, das Erwerben und den Einsatz der Systeme einzurichten (Heyns 2013).

146 Die Australia Group ist ein informeller Zusammenschluss von 42 Staaten sowie der Europäischen Kommission (http://australiagroup.net/en/index.html; 9.10.2020).

147 Stand November 2018 nach Zählung der »Campaign to Stop Killer Robots«; hinzu kommt noch Belgien.

Im Rahmen der CCW gibt es lediglich bei einer Gruppe kleinerer Länder (mit der möglichen Ausnahme von China) Unterstützung für diese Position. Die allermeisten Staaten mit hochentwickelter Rüstungsindustrie und insbesondere die derzeit führenden Staaten auf dem Feld automatisierter UWS wie die USA und Israel scheinen wenig Interesse an einem generellen Verbot zu haben (Dickow et al. 2015b, S. 71). Sie führen ins Feld, dass es bislang an einer allgemein akzeptierten Definition für AWS fehle, die eine notwendige Grundlage für die Abgrenzung von erlaubten und verbotenen Systemen sei. Außerdem würden AWS nicht per se dem HVR widersprechen, sondern ggf. nur unter bestimmten Einsatzbedingungen. Ganz generell seien der Entwicklungsstand der Technologie und das Wissen darüber noch nicht weit genug fortgeschritten, um daraus weitreichende Schlussfolgerungen über Beschränkungen und/oder Verbote ableiten zu können.

Führt man sich die geringen Fortschritte vor Augen, die in den letzten Jahren insbesondere im Rahmen der CCW beim Thema AWS gemacht wurden, ist es offensichtlich, dass der Weg zu einer verbindlichen internationalen Regulierung von AWS noch weit zu sein scheint. Verbindliche Regulierungen sind auch unterhalb der Ebene eines Totalverbots denkbar. Diese könnten einerseits dazu dienen, besonders problematische Technologien bzw. Nutzungsarten von AWS einzuhegen. Andererseits könnten sie wichtige Zwischenschritte darstellen, um die Partizipation von Schlüsselakteuren für Rüstungskontrolle zu gewinnen und um die inhaltliche und Vertrauensbasis für eine umfassendere Regulierung zu legen.

Elemente einer verbindlichen Regulierung

Im Folgenden sollen einige Aspekte skizziert werden, die Bestandteile einer Regulierung werden könnten, damit ein möglicher zukünftiger Einsatz von AWS mit den völkerrechtlichen Vorgaben konform gehen könnte. Hier wird der von Lewis (2015, S. 1322 ff.) entwickelten Struktur gefolgt:

- Technologische bzw. an den Fähigkeiten der AWS orientierte Charakteristika: Dies wären Mindestanforderungen an das Kamera- bzw. Bildverarbeitungssystem (Grundvoraussetzung für Unterscheidung von Kombattanten und Zivilisten), an das System für kontextuelle Entscheidungen sowie der Umgang mit (selbst)lernenden Systemen, um nur einige zu nennen;
- Charakteristika des Operationsraums: z. B. Dichte der Besiedlung, Abstandsregeln zu bestimmten Einrichtungen (Schulen, Kirchen etc.), Differenzierungen zwischen den Medien (land-, luft-, see-, unterwassergestützt), Spezifizierung der zeitlichen Ausdehnung der Operation;
- Charakteristika der gegnerischen Kräfte: z. B. sind Soldaten regulärer Streitkräfte anhand der Uniformen leichter zu erkennen als nichtuniformierte Kämpfer;

- Mindestanforderungen an menschliche Aufsicht bzw. Kontrolle: z. B. die Möglichkeit, Angriffe noch im fortgeschrittenen Stadium abbrechen zu können;
- andere Kriterien: z. B. Art der Wirkmittel (tödlich/nichttödlich), offensive oder defensive Ausrichtung der Systeme, mobile bzw. stationäre Systeme, Umgang mit Wetter- und anderen Umweltbedingungen;
- Regelungen zur Verantwortung und Haftbarkeit.

Des Weiteren könnten auch Regulierungen mit regionalem Fokus, im Sinne der konventionellen Rüstungskontrolle des KSE-Vertrags, wichtige stabilitätsfördernde und rüstungshemmende Maßnahmen zwischen Staaten darstellen. Eine internationale Übereinkunft zur Einschränkung des Einsatzes von AWS, wie auch zum Teil im Rahmen der CCW diskutiert, könnte neben der Wahrung des HVR auch in zwischenstaatlichen Konfliktsituationen zusätzliches Vertrauen schaffen und Eskalationsspiralen hemmen sowie den Tendenzen einer zunehmenden Entgrenzung des Krieges entgegenwirken.

Das Problem der Verifikation

Die Charakteristika von AWS und insbesondere die geschilderte Dual-Use-Problematik schränken die Möglichkeiten zur Verifikation der zahlenmäßigen AWS-Bestände eines Staates, die Überprüfung des tatsächlichen Automatisierungs- oder Autonomiegrades eines unbemannten Waffensystems sowie die Kontrolle von AWS-Einsätzen auf die Einhaltung völkerrechtlicher Prinzipien stark ein. Die Etablierung verlässlicher Verifikationsmechanismen, die für den Erfolg zukünftiger Rüstungskontrollverträge im Bereich der AWS wesentlich sind, gestaltet sich sehr schwierig. Die Verifikation beispielsweise numerischer Obergrenzen von Stückzahlen würde derzeit am Fehlen einer Definition von AWS sowie ggf. an Dual-Use-bedingten Schwierigkeiten bei der Abgrenzung von zivilen und militärischen Systemen scheitern. Die Frage, in welchem Ausmaß ein Waffensystem tatsächlich autonom handelt, hat wiederum weniger mit der Hardware und dem physischen Erscheinungsbild zu tun, sondern wird durch die spezifische Programmierung bzw. die Software bestimmt.

Auf welche Weise Softwarecodes direkt am System verifiziert werden könnten, ist völlig unklar. Erstens ist es schwer vorstellbar, dass staatliche Akteure es gestatten, dass die Steuersoftware von Waffensystemen Dritten zur Inspektion offengelegt wird, und zweitens muss sichergestellt werden, dass diese nicht sofort nach der Inspektion durch ein schnell und einfach durchführbares Update wieder verändert wird. Ähnlich schwierig wäre es, Einsätze von AWS auf die Einhaltung des HVR hin zu kontrollieren. Voraussetzung hierfür wäre eine technische Lösung, die ein nicht manipulierbares Monitoring der Einsätze und aller relevanten Entscheidungsprozesse sicherstellt sowie die unabhängige Analyse und Prüfung dieser Daten gewährleistet. Ein erster Vorschlag hierzu

wurde von Mitgliedern des International Committee for Robot Arms Control (ICRAC)[148] bereits erarbeitet (Gubrud/Altmann 2013). Kurz umrissen besagt dieser, dass in einer Blackbox Einsatzdaten verschlüsselt und fälschungssicher aufgezeichnet werden (beispielsweise mittels einer Blockchain), die bei begründeten Zweifeln der Rechtmäßigkeit eines Angriffs ex post analysiert werden können, ohne dabei militärisch sensible oder geheime Informationen preisgeben zu müssen. Als Einzelmaßnahme betrachtet reicht diese Verifikationsmaßnahme jedoch nicht für den Bereich konventioneller Rüstungskontrolle aus, da hier im Vorfeld und über die gesamte Dauer eines Rüstungskontrollvertrags Vertrauen in Bezug auf die Entwicklung, Beschaffung oder Vorhaltung von Waffensystemen herzustellen ist und nicht allein für die Art sowie Umstände des Waffeneinsatzes. Sie könnte jedoch ein konstruktives Element darstellen, eingebettet in ein allgemeines Regime von Transparenz, vertrauensbildenden Maßnahmen, Inspektionen, technischen Sicherungsmaßnahmen und forensischer Untersuchung verdächtiger Ereignisse.[149]

9.4 Handlungsmöglichkeiten

Die Bemühungen um eine Regulierung von AWS speisen sich aus zwei zentralen Argumentationssträngen. Der eine befasst sich mit der Frage, ob der Einsatz von AWS mit den Prinzipien des humanitären Völkerrechts vereinbar wäre. Die internationale Debatte dazu hat innerhalb der CCW eine adäquate Plattform gefunden. Der andere dreht sich um die Auswirkungen der Entwicklung, Stationierung oder des Einsatzes von AWS für die internationale Sicherheit. Die zentrale Frage hier ist, wie mit möglichen sicherheitspolitischen Implikationen, z. B. Rüstungsdynamiken, zwischenstaatlichen Spannungen oder strategischen Instabilitäten, umgegangen werden kann. Der Austausch zu dieser Frage befindet sich noch ganz am Anfang und hat bisher noch kein geeignetes internationales Forum gefunden. Allerdings existiert im Bereich präventiver Rüstungskontrolle ein breites Spektrum von Ansatzmöglichkeiten, wie angesichts weltweit zunehmender geopolitischer Spannungen, schnell voranschreitender technologischer Entwicklungen sowie verstärkter militärischer Rüstung ein wichtiger Beitrag zur Krisenstabilität und internationalen Sicherheit geleistet werden kann.

Die Erfolgsaussichten einer Eindämmung der Verbreitung bzw. Nutzung von AWS in bewaffneten Konflikten mit den Mitteln präventiver Rüstungskontrolle sind schwer einzuschätzen. Die Ausgangsbedingungen sind nicht ideal, denn die Dynamik der zugrundeliegenden technologischen Trends ist beeindruckend (Digitalisierung, Algorithmen, KI). Diese Dynamik umfasst alle Lebens-

148 ICRAC ist ein Zusammenschluss von Wissenschaftlern und Aktivisten, die sich für ein Verbot von AWS einsetzen (https://www.icrac.net/about-icrac/; 9.10.2020).
149 Altmann (2019), persönliche Mitteilung

bereiche und hat in vielen Bereichen transformativen Charakter. Dies trifft auch für den militärischen Bereich zu. Der militärische Nutzen eines verstärkten Einsatzes von Autonomie ist klar erkennbar. Daher wird dies von allen technologisch fortgeschrittenen Staaten angestrebt. Beispielsweise ist die stärkere Nutzung von Autonomie ein Kernelement der »revolution of military affairs«, die derzeit in den USA in vollem Gange ist (DOD 2018b, 2019). Je größer der erwartete strategische Nutzen ausfällt, desto weniger werden Schlüsselstaaten bereit sein, Restriktionen oder Verboten zuzustimmen (Nasu/McLaughlin 2014, S. 52). Diese Haltung spiegelt sich derzeit auch erkennbar in den im Rahmen der CCW von einigen Staaten vertretenen Positionen wider.

Im Folgenden werden mögliche Bausteine für die Politikgestaltung skizziert. Diese leiten sich von der angesprochenen Dichotomie der Argumentationsstränge ab. Der erste bezieht sich auf die völkerrechtliche und ethische Dimension und die Möglichkeiten innerhalb der CCW, während der darauffolgende schwerpunktmäßig auf die sicherheitspolitische Dimension fokussiert. Die Bausteine sind keineswegs als sich gegenseitig ausschließende Handlungsoptionen zu verstehen, sondern können sich im Gegenteil gegenseitig ergänzen und befruchten.

9.4.1 Die Möglichkeiten innerhalb der CCW ausschöpfen

Zunächst einmal ist es ratsam, dass Deutschland sein bisheriges Engagement im Rahmen der CCW aktiv fortführt, um eine Ächtung von solchen Waffensystemen zu erreichen, die dem Menschen die Kontrolle über den Waffeneinsatz entziehen. Da für verbindliche Vereinbarungen Einstimmigkeit der CCW-Vertragsstaaten erforderlich ist, müsste ein breiter Konsens aller relevanter Staaten erzielt werden, was bedeuten könnte, dass zunächst nur kleine gemeinsame Schritte als Minimalkonsens vereinbart werden könnten (z. B. in Form von VSBM). Aufgrund des bisherigen Dissenses in der CCW und grundlegend unterschiedlicher Auffassungen einzelner Staaten sind die Erfolgsaussichten dieses Prozesses eher in einem längerfristigen Kontext zu betrachten, zumal auf ein komplexes Geflecht von Fragen wie eine adäquate Verifikation, die fortschreitende Proliferation oder die Rüstungsexportkontrolle Antworten gefunden werden müssen.

Eine Fortführung des Diskurses um AWS im Rahmen der CCW ist auch losgelöst von den Aussichten, ein wie auch immer geartetes Ergebnis zu erzielen, als positiv zu werten. Denn dies trägt wesentlich dazu bei, die Thematik auf der Agenda zu halten sowie die internationale (Fach-)Öffentlichkeit zu sensibilisieren. Auf diese Weise können die Bedingungen geschaffen werden, um den Themenkomplex weiter zu durchdringen und sich im Laufe der Zeit inhaltlich anzunähern.

Dieser konsensorientierten Strategie entspricht die gemeinsame Initiative Deutschlands und Frankreichs, die zunächst einmal eine politische Erklärung und das Bekenntnis zum HVR-konformen Einsatz von AWS und den sich daraus ergebenden Verpflichtungen aus Artikel 36 ZP I anstrebt. Bei diesem auf eher langfristige Erfolge angelegten Vorgehen besteht aber die Gefahr, dass mit verstreichender Zeit die Entwicklung, Verbreitung oder vielleicht sogar der Einsatz von AWS stark vorangeschritten sein könnte. Dies könnte Tatsachen schaffen, die eine Einigung im Rahmen der CCW erschweren würden.

9.4.2 Engagement über die CCW hinaus verbreitern

Insbesondere wenn die Fortschritte im Rahmen der CCW als zu langsam und/oder nicht hinreichend bewertet werden, böte es sich an, dass Deutschland sich über die CCW hinaus auf dem Feld der präventiven Rüstungskontrolle international engagiert. Diese Strategie könnte sich auf eine ad hoc zu bildende Koalition von Staaten, NGOs und internationalen Organisationen stützen, die ein gemeinsames Ziel verfolgen und möglichst zügig auf eine Ausformulierung und Verabschiedung entsprechender Regeln zur Einhegung der Risiken von AWS abzielen, in der Hoffnung, dass dies eine Sogwirkung entfaltet und sukzessive immer mehr Staaten sich dieser Vorgehensweise anschließen.

Das Vorgehen könnte sich am Ottawa-Prozess orientieren, der im Ergebnis zum völkerrechtlichen Verbot von Antipersonenminen führte (für einen kurzen Überblick siehe z. B. Wikipedia 2004). Trotz des unbestreitbaren humanitären Erfolgs dieses Abkommens muss einschränkend darauf hingewiesen werden, dass die Großmächte China, Russland und die USA[150] ihm bis heute nicht beigetreten sind, obwohl der militärische Nutzen von Antipersonenminen (insbesondere für militärisch starke Staaten) eher begrenzt ist. Ein Abkommen zu AWS, dem die rüstungstechnisch führenden Staaten nicht beitreten würden, wäre aber sicherlich kaum hilfreich. Die Wahrscheinlichkeit für eine breite Partizipation möglichst aller relevanten Staaten könnte ggf. durch die Wahl weniger ambitionierter Maßnahmen und Verbotstatbestände erhöht werden.

Noch weitreichender wäre es, unilateral voranzugehen und einen Verzicht auf den Einsatz, die Beschaffung und/oder die Entwicklung von AWS verbindlich und nachprüfbar zu erklären. Dies würde die von der Bundesregierung bereits formulierte Position (CCW GGE 2018f) konsequent fortführen und erheblich schärfen. Diese Strategie könnte sich auf die in Bezug auf die Achtung der Menschenwürde vorgebrachten ethischen Argumente stützen (Kap. 8.2) und der herausgehobenen Rolle der Menschenwürde im Katalog der Grundrechte Rechnung tragen. Die diffizile Aufgabe besteht darin, nachvollziehbar und

150 Die seit 2014 verfolgte Politik, dass sich die USA außerhalb der koreanischen Halbinsel konform mit den zentralen Anforderungen der Ottawa-Konvention verhalten, wurde Ende Januar 2020 von der Trump-Administration widerrufen (Ali 2020; Scholz 2020).

glaubwürdig eine rote Linie zu definieren, um erlaubte bzw. gewünschte Anwendungen der künstlichen Intelligenz und Autonomie von nicht statthaften zu unterscheiden. Die Glaubwürdigkeit solchen Handelns würde gestärkt, wenn sie mit anderen Politikbereichen in Einklang gebracht werden könnte. Zu nennen sind hier insbesondere die Forschungsförderung sowie die Exportpolitik. Auch in diesem Zusammenhang ist ein Leitmotiv, auf die Vorbildfunktion und eine eintretende Sogwirkung zu setzen, mit dem Ziel, dass weitere Staaten diesem Vorgehen folgen. Andererseits besteht das Risiko, dass Schlüsselakteure bzw. Großmächte wie bei den Antipersonenminen sich der implizit oder explizit geäußerten Einladung, hier mitzuziehen, verweigern und somit der gewünschte Effekt eines unilateralen Handelns verpufft.

Internationalen Dialog stärken

Eine Möglichkeit wäre es, einen internationalen Dialogprozess zu initiieren, der die beschriebenen, bislang vernachlässigten Themen (u. a. Rüstungsdynamiken, zwischenstaatliche Spannungen bzw. strategische Instabilitäten) aufgreift. Hier ist z. B. eine Rahmenkonvention denkbar, die eine inhaltliche und organisatorische Struktur (etwa turnusmäßige Treffen und ein kleines Sekretariat) vorgibt. Bei Bedarf und wenn die entsprechende Zustimmung besteht, kann dieser Nukleus die Voraussetzungen schaffen, um konkretere und verbindlichere Übereinkünfte zu treffen (Marchant et al. 2011, S. 313 f.). Als erfolgreiches Beispiel für diesen Ansatz kann die Genese des Wiener Übereinkommens zum Schutz der Ozonschicht dienen, das als relativ weiche Vereinbarung begann und im Laufe der Zeit vor allem durch das Montreal-Protokoll und dessen verschiedene Zusätze Verbindlichkeit gewann.

Eine weitere Möglichkeit bieten bilaterale und multilaterale regierungsseitige Dialogforen, die für die Entwicklung eines gemeinsamen Problemverständnisses und die Vertiefung von Kooperationen ein probates Mittel sind. Im Gegensatz zu Initiativen von privater Seite (z. B. von Verbänden) sind sie demokratisch legitimiert, gleichzeitig aber weniger aufwendig zu organisieren als formale transnationale Verhandlungen. Dennoch können sie einen Rahmen vorgeben, dem harmonisierte nationale Vorgehensweisen oder sogar internationale Regulierungen entspringen können (Marchant et al. 2011, S. 311). Ein Beispiel für ein solches Dialogforum ist die Australia Group, die sich die Eindämmung der Proliferation chemischer und biologischer Waffen zum Ziel gesetzt hat. Auch auf Ebene der OECD (o. J.) gibt es Beispiele, u. a. die Working Party on Biotechnology, Nanotechnology and Converging Technologies (BNCT), die sich für eine verantwortbare Entwicklung dieser Technologien einsetzt.

Revitalisierung konventioneller Rüstungskontrolle

Ein weiteres wesentliches Handlungsfeld ist eine Revitalisierung der konventionellen Rüstungskontrolle. Diese wäre angesichts der heute vorherrschenden globalen sicherheitspolitischen Lage auch losgelöst vom Thema AWS als Beitrag zur Entspannung willkommen, allerdings sind die Bedingungen hierfür aktuell alles andere als einfach. Seriöse Bemühungen in diesem Bereich könnten z. B. die Möglichkeit zur Schaffung eines umfassenden konventionellen Rüstungskontrollregimes eröffnen, das auch als ein Ersatz für den erodierenden KSE-Vertrag dienen könnte, vielleicht sogar um zusätzliche Staaten erweitert. In diesem Rahmen eröffnet sich die Gelegenheit, unbemannte Waffensysteme zu inkludieren und etwaige AWS bzw. deren Einsatz weitgehend zu regulieren.

Die Ausarbeitung und Umsetzung von Rüstungskontrollvereinbarungen in Anerkennung der destabilisierenden Wirkung von AWS ist ein langer und steiniger Weg. Vertragliche numerische Obergrenzen (für bestimmte geografische Räume oder absolut) bzw. Fähigkeitsbeschränkungen könnten wesentliche Stabilitätsgaranten auch im Hinblick auf eine zukünftig zunehmend automatisierte Kriegsführung sein. Von enormer Bedeutung für den Erfolg von Beschränkungen ist die Konzeption verlässlicher Verifikationsmechanismen.

Schritte in diese Richtung sind freiwillige Transparenz und VSBMs, die Vertrauen stärken und Vorbildfunktion haben könnten. Eine konkrete Möglichkeit wäre die Einrichtung einer internationalen Beobachtungsstelle, die die Entwicklungen und die Verbreitung von AWS überwacht, analog derer für Kernwaffen sowie biologischer und chemischer Waffen (Villani 2018, S. 127). Die Ausarbeitung von Exportregeln könnte zusätzlich helfen, die Weiterverbreitung von AWS einzudämmen. Dabei muss jedoch dafür Sorge getragen werden, dass diese Bestimmungen den zivilen Nutzen der infrage stehenden Technologien nicht über Gebühr schmälern.

In Anerkennung der destabilisierenden Wirkung von AWS könnten Staaten aber auch freiwillig auf diese Art von Waffensystemen verzichten oder deren Automatisierungsgrad von vornherein begrenzen. Diese Handlungsoption wurde zuvor bereits aus ethischen bzw. humanitären Gründen abgeleitet, hier allerdings stehen primär sicherheits- und stabilitätspolitische Überlegungen im Vordergrund. Wie eine solche Begrenzung aussehen könnte, ist eine offene Frage, denn auch weit unterhalb der paradigmatischen Schwelle von »human out of the loop« könnten autonome bzw. hochautomatisierte Waffensysteme destabilisierend wirken.

An all diesen Schritten könnte Deutschland sich aktiv beteiligen und auf diese Weise einen nicht zu unterschätzenden Beitrag leisten, mögliche Rüstungsdynamiken und die daraus resultierenden Auswirkungen auf die regionale wie globale Stabilität im Vorfeld einzuhegen.

Begleitende nationale Schritte und Maßnahmen

Im Folgenden werden mögliche national umzusetzende Schritte umrissen, mit denen das Thema AWS verstärkt auf die Agenda der relevanten Entscheidungsträger in Bundestag, Ministerien, Behörden und der Führung der Bundeswehr gehoben würde, die Basis an orientierungs- und entscheidungsrelevantem Wissen verbreitert würde sowie Maßnahmen angeschoben werden könnten, die den internationalen Entscheidungsfindungsprozess begleiten und befruchten könnten:

- Intensivierung der Anstrengungen um eine ausführliche, breitangelegte (fach)öffentliche Debatte über die militärischen, völkerrechtlichen und sicherheitspolitischen Implikationen des Einsatzes von UWS und zukünftigen AWS: Hierzu kann die Durchführung von öffentlichen Diskussionsveranstaltungen, Studien und Workshops gehören, bei der auch die verschiedenen Stakeholder eingebunden werden müssen: neben der Regierung und den NGOs auch die Medien, Wirtschaft und Wissenschaft – insbesondere im Sammelbereich von KI.
- Im Zusammenhang mit der Formulierung der nationalen Strategie für KI (Bundesregierung 2018c) und den damit einhergehenden Kommissionen und Diskussionsforen sollten die Anwendungen der KI im Militärsektor sowie die Dual-Use-Aspekte nicht ausgeblendet werden. Auch für die Enquete-Kommission »Künstliche Intelligenz – gesellschaftliche Verantwortung und wirtschaftliche, soziale und ökologische Potenziale« (Deutscher Bundestag 2018b) wäre dies ein hochrelevantes Untersuchungsfeld. Hier könnte ein Blick nach Frankreich Anregungen liefern. Dort wurde ein maßgeblicher Impuls durch den Bericht von (Villani 2018, S. 125 f.) gesetzt.

Verstärkte Bemühungen zur Untersuchung einer international zunehmend automatisierten Kriegsführung im Allgemeinen sowie des Einsatzes automatisierter UWS und zukünftiger AWS im Besonderen: Ein spezieller Fokus sollte dabei auf der Analyse sicherheitspolitischer Risiken für die Bundesrepublik Deutschland und den Möglichkeiten liegen, diesen bestmöglich zu begegnen. Diese Aktivitäten könnten im Rahmen einer Kommission erfolgen, an der relevante Ministerien (Auswärtiges Amt, Bundesministerium des Innern, für Bau und Heimat, Bundesministerium der Verteidigung etc.), Behörden, Forschungsinstitutionen sowie NGOs und Parlamentarier beteiligt sind.

- Die aktuellen Erkenntnisse und strategischen Überlegungen mit Blick auf die militärische Nutzung von autonomen Waffensystemen in der Bundeswehr könnten in einem nationalen Leitliniendokument niedergelegt werden (Amoroso et al. 2018, S. 13), das als Referenzpunkt für die verschiedenen Debattenstränge dienen könnte.

- Initiierung einer Debatte zu Fragen des Umgangs bei Exporten von sensiblen Technologien in Kooperation mit Stakeholdern aus Wissenschaft, Wirtschaft und Gesellschaft: Darauf aufbauend könnten Regeln zur Nichtverbreitung und Exportkontrolle von UWS sowie AWS entwickelt werden. Hierbei muss insbesondere die Dual-Use-Problematik berücksichtigt und zugleich der Bedeutung und Legitimität autonomer Systeme im Bereich ziviler Anwendungen Rechnung getragen werden. Hierfür könnte z. B. eine entsprechende Arbeitsgruppe unter der Ägide des Bundesamtes für Wirtschaft und Ausfuhrkontrolle (BAFA) unter Beteiligung von Vertretern aus Wirtschaft, Wissenschaft und NGOs eingesetzt werden.
- In der Forschungspolitik und Forschungsförderung wäre bei KI und angrenzenden Feldern eine besondere Sensibilisierung für die Dual-Use-Problematik angebracht. Das umfasst auch die Unterstützung der Bemühungen um die Formulierung und Etablierung ethischer Leitbilder in der Forschung und forschungsnahen Anwendung.

9.5 Fazit

AWS stellen in vielerlei Hinsicht eine Herausforderung für die Rüstungskontrolle dar und werfen zahlreiche Fragen auf, sowohl was ihre Übereinstimmung mit den Prinzipien des humanitären Völkerrechts angeht als auch die Auswirkungen, die ihre Verbreitung und ihr Einsatz entfalten könnten, gerade auch in Bezug auf potenzielle Rüstungsdynamiken, die internationale Sicherheit sowie die regionale und strategische Stabilität. Nicht zuletzt aufgrund der großen Dynamik der technologischen Entwicklung in den Bereichen Robotik und künstlicher Intelligenz ist es von herausragender Bedeutung, AWS-bezogene Mechanismen der präventiven Rüstungskontrolle zu etablieren.

Derzeit existiert ein Fenster von Möglichkeiten, um mit einem international abgestimmten, zielgerichteten Vorgehen die möglichen Gefahren einzuhegen, die AWS mit sich bringen könnten. Dieses Fenster schließt sich sukzessive mit fortschreitender technologischer Entwicklung und der kontinuierlichen Integration autonomer Funktionen in Waffensysteme aller Art. Damit werden Strukturen gefestigt und Fakten geschaffen, die regulierende Eingriffe erschweren oder sogar verhindern. Dieses Fenster von Möglichkeiten zu nutzen ist keine einfache Aufgabe, denn die Schwierigkeiten, die sich bei der Rüstungskontrolle und mit Verifikationsmaßnahmen im Hinblick auf AWS stellen, sind groß. Angesichts der sicherheitspolitischen Implikationen, mit denen die internationale Gemeinschaft durch autonome Waffensysteme zukünftig konfrontiert werden könnten, erscheint es dringend geboten, diese Herausforderungen unverzüglich anzugehen und Lösungen zu entwickeln. Diesbezügliche politische und diplomatische Initiativen erfordern einen langen Atem und einen breiten Diskurs unter Einbezug von Wissenschaft und Zivilgesellschaft.

10 Literatur

10.1 In Auftrag gegebene Gutachten

Altmann, J.; Gubrud, M. (2017): Technologien für autonome Waffensysteme – Stand und Perspektiven. Köln

Alwardt, C.; Hilgert, L.-M.; Neuneck, G.; Polle, J. (2017): Sicherheitspolitische Implikationen und Möglichkeiten der Rüstungskontrolle autonomer Waffensysteme. Gutachten im Auftrag des Deutschen Bundestages. Institut für Friedensforschung und Sicherheitspolitik, Hamburg

Koch, B.; Rinke, B. (2017): Ethische Fragestellungen im Kontext autonomer Waffensysteme. Institut für Theologie und Frieden, Hamburg

10.2 Weitere Literatur

AA (Auswärtiges Amt) (2019a): Statement by Germany – On Agenda Item 5© Review of the potential military applications of related technologies in the context of the Group's work. Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems of the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons which may be deemed to be excessively injurious or to have indiscriminate Effects. Genf, https://www.unog.ch/80256EDD006B8954/(httpAssets)/95996F2E27AC3DE7C12583D2003D858F/$file/20190325+Statement1+Germany+GGE+LAWS.pdf (5.8.2020)

AA (2019b): Statement by Germany – On Agenda Item 5(d) Characterization of the systems under consideration in order to promote a common understanding on concepts and characteristics relevant to the objective and purpose of the Convention. Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems of the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons which may be deemed to be excessively injurious or to have indiscriminate Effects. Genf, https://www.unog.ch/80256EDD006B8954/(httpAssets)/D6C11A0A68D81F4AC12583CB0036650B/$file/20190325+Statement2+Germany+GGE+LAWS.pdf (5.8.2020)

AA (2019c): Statement by Germany – On Agenda Item 5(b) Further consideration of the human element in the use of lethal force; aspects of human machine interaction in the development, deployment and use of emerging technologies in the area of lethal autonomous weapons systems. Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems of the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons which may be deemed to be excessively injurious or to have indiscriminate Effects. Genf, https://www.unog.ch/80256EDD006B8954/(httpAssets)/2B8E772610C0F552C12583CB003A4192/$file/20190326+Statement3+Germany+GGE+LAWS.pdf (5.8.2020)

AA (2019d): Statement by Germany – On Agenda Item 5(e) Possible options for addressing the humanitarian and international security challenges posed by

emerging technologies in the area of lethal autonomous weapons systems in the context of the objectives and purposes of the Convention without prejudicing policy outcomes and taking into account past, present and future proposals. Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems of the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons which may be deemed to be excessively injurious or to have indiscriminate Effects. Genf, https://www.unog.ch/80256EDD006B8954/(httpAssets)/E69C96284D07CAE8C12583CB003D9873/$file/20190327+Statement4+Germany+GGE+LAWS.pdf (5.8.2020)

ACA (Arms Control Association) (2017): The Missile Technology Control Regime at a Glance. https://www.armscontrol.org/factsheets/mtcr (9.10.2020)

Ahronheim, A. (2017): RAMBOW: Israel unveils latest unmanned ground vehicle. The Jerusalem Post, 18.9.2017

Airforce Technology (2017): Kratos to launch XQ-222 Valkyrie, UTAP-22 Mako at Paris Air Show 2017. http://www.airforce-technology.com/news/newskratos-to-launch-xq-222-valkyrie-utap-22-mako-at-paris-air-show-2017-5845491 (9.10.2020)

Airforce Technology (o. J.): X-45 J-UCAV (Joint Unmanned Combat Air System). https://www.airforce-technology.com/projects/x-45-ucav/ (9.10.2020)

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. AIV Nr. 97, https://www.advisorycouncilinternationalaffairs.nl/binaries/advisorycouncilinternationalaffairs/documents/publications/2015/10/02/autonomous-weapon-systems/Autonomous_Weapon_Systems_AIV-CAVV-Advisory-report-97_201510.pdf (5.8.2020)

Ali, I: (2020): Trump eases restrictions on land mine use by U.S. military. Reuters, 31.1.2020, https://www.reuters.com/article/us-usa-war-landmines-idUSKBN1ZU2GA (9.10.2020)

Allen, G.C. (2019): Understanding China's AI Strategy: Clues to Chinese Strategic Thinking on Artificial Intelligence and National Security. Washington D.C., https://s3.amazonaws.com/files.cnas.org/documents/CNAS-Understanding-Chinas-AI-Strategy-Gregory-C.-Allen-FINAL-2.15.19.pdf?mtime=20190215104041 (5.8.2020)

ALT (Army Acquisition, Logistics and Technology) (201: Weapon Systems 2011. Arlington, https://fas.org/man/dod-101/sys/land/wsh2011/wsh2011.pdf (9.10.2020)

Altmann, J. (2017): Zur ethischen Beurteilung automatisierter und autonomer Waffensysteme. In: Werkner, I.-J.; Ebeling, K. (Hg.): Handbuch Friedensethik, S. 793–804

Altmann, J.; Sauer, F. (2017): Autonomous Weapon Systems and Strategic Stability. In: Survival 59(5), S. 117–142

Alwardt, C.; Krüger, M. (2016): Autonomy of Weapon Systems. Food for Thought Paper. Hamburg, https://ifsh.de/file-IFAR/pdf_english/IFAR_FFT_1_final.pdf (5.8.2020)

AMF (Aspen (Ministers Forum) (2020): Statement from the Aspen Ministers Forum. https://www.aspeninstitute.org/of-interest/statement-from-the-aspen-ministers-forum/ (9.10.2020)

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. Publication Series on Promoting Democracy 49, Berlin

Anderson, M.; Anderson, S. L. (2007): Machine ethics: Creating an ethical intelligent agent. In: AI Magazine 28(4), S. 15–26
Apan (o. J.a): Optoelectronics and Photonics. https://community.apan.org/wg/afosr/w/researchareas/7686/optoelectronics-and-photonics/ (9.10.2020)
Apan (o. J.b): Computational Cognition and Machine Intelligence. https://community.apan.org/wg/afosr/w/researchareas/7679/computational-cognition-and-machine-intelligence/ (9.10.2020)
Arkin, R.C. (2008): Governing lethal behavior: Embedding ethics in a hybrid deliberative/reactive robot architec-ture part I: Motivation and philosophy. In: Association for Computing Machinery, Inc., 3rd ACM/IEEE International Conference on Human-Robot Interaction (HRI), Amsterdam, 2008, S. 121–128
Arkin, R.C. (2009): Governing lethal behavior in autonomous robots. Boca Raton
Arkin, R.C. (2010): The Case for Ethical Autonomy in Unmanned Systems. In: Journal of Military Ethics 9(4), S. 332–341
Arkin, R.C. (2013): Lethal Autonomous Systems and the Plight of the Non-combatant. In: AISB Quarterly (137), S. 4–12
Arkin, R.C. (2015): Counterpoint. The case for banning killer robots. In: Commun. ACM 58(12), S. 46–47
Army Recognition (2016): Nerekhta robotic system to be added to Russian special forces' inventory. 21.12.2016, https://www.armyrecognition.com/december_2016_global_defense_security_news_industry/nerekhta_robotic_system_to_be_added_to_russian_special_forces_inventory.html (9.10.2020)
Army Technology (o. J.a): Squad Mission Support System (SMSS). https://www.army-technology.com/projects/squad-mission-support-system-smss/ (9.10.2020)
Army Technology (o. J.b): iRobot 510 PackBot Multi-Mission Robot. https://www.army-technology.com/projects/irobot-510-packbot-multi-mission-robot/ (9.10.2020)
Army Technology (o. J.c): AvantGuard Unmanned Ground Combat Vehicle. https://www.army-technology.com/projects/avantguardunmannedgr/ (9.10.2020)
Army Technology (o. J.d): Uran-9 Unmanned Ground Combat Vehicle. https://www.army-technology.com/projects/uran-9-unmanned-ground-combat-vehicle/ (9.10.2020)
Arquilla, J.; Ronfeldt, D. (2000): Swarming & The Future of Conflict. RAND's National Defense Research Institute, Santa Monica, https://www.rand.org/content/dam/rand/pubs/documented_briefings/2005/RAND_DB311.pdf (5.8.2020)
Article 36 (2013): Killer robots: UK Government policy on fully autonomous weapons. http://www.article36.org/wp-content/uploads/2013/04/Policy_Paper1.pdf (9.10.2020)
Asaro, P. (2008): How Just Could a Robot War Be? In: Briggle, A.; Waelbers, K.; Brey, P. (Hg.): Current issues in computing and philosophy. Amsterdam, S. 50–64
Asaro, P. (2012): On banning autonomous weapon systems. Human rights, automation, and the dehumanization of lethal decision-making. In: Int. rev. Red Cross 94(886), S. 687–709
Atherton, K.D. (2018): Navy office awards $30 million contract for drone swarms. C4ISRnet, 27.6.2018, https://www.c4isrnet.com/unmanned/2018/06/27/office-of-naval-research-awards-raytheon-30-million-to-develop-locust-swarm/ (9.10.2020)
Austin, H. (2015): North Dakota becomes first US state to legalise use of armed drones by police. The Independent, 9.9.2015, http://www.independent.co.uk/news/

world/americas/north-dakota-becomes-first-us-state-to-legalise-use-of-armed-drones-by-police-10492397.html (5.8.2020)
AUVAC (Autonomous Undersea Vehicle Applications Center) (o. J.): SeaOtter MKII. AUV System Spec Sheet. http://auvac.org/2-2/ (9.10.2020)
Baiker, A. (2014): Geschichte der Gentechnik und Gentechnik-Gesetzgebung. Bayerisches Landesamt für Gesundheit und Lebensmittelsicherheit, https://www.lgl.bayern.de/rubrikenuebergreifende_themen/gentechnik/gentechnik_geschichte.htm (9.10.2020)
Ballesteros, C. (2018): Russia Has Underwater Nuclear Drones, Leaked Pentagon Documents Reveal. Newsweek, 14.1.2018
Banko, M.; Brill, E. (2001): Scaling to very very large corpora for natural language disambiguation. In: Webber, B. (Hg.): Proceedings of the 39th Annual Meeting on Association for Computational Linguistics – ACL '01. the 39th Annual Meeting. Toulouse, 6.–11.7.2001. In: Morristown: Association for Computational Linguistics. Stroudsburg, S. 26–33
Barbaschow, A. (2018): University boycott ends after KAIST confirms no »killer robot« development. ZDNet, 10.4.18 https://www.zdnet.com/article/university-boycott-ends-after-kaist-confirms-no-killer-robot-development/ (7.8.2020)
BBC News (2019): INF nuclear treaty: US pulls out of Cold War-era pact with Russia. 21.2.2020, https://www.bbc.com/news/world-us-canada-49198565 (5.8.2020)
Beavers, A.F. (2011): Moral Machines and the Threat of Ethical Nihilism. In: Lin, P.; Abney, K.; Bekey, G. (Hg.): Robot ethics: the ethical and social implications of robotics. In: The MIT press, London, S. 333–344
Bendel, O. (2018): Überlegungen zur Disziplin der Maschinenethik. In: Aus Politik und Zeitgeschichte (6-8), S. 34–38
Bendett, S. (2017): Can Russian UAVs Close the Gap with America or Israel? The National Interest, 7.7.2017, https://nationalinterest.org/blog/the-buzz/can-russian-uavs-close-the-gap-americans-or-israelis-21473 (5.8.2020)
Berger, C.; Rumpe, B. (2008): Autonomes Fahren – Erkenntnisse aus der DARPA Urban Challenge (Autonomous Driving – Insights from the DARPA Urban Challenge). In: it – Information Technology 50(4), S. 258–264
Betzler, M.; Scherrer, N. (2016): Verantwortung und Kontrolle. In: Heidbrink, L.; Langbehn, C.; Sombetzki, J. (Hg.): Handbuch Verantwortung. Wiesbaden, S. 337–352
Birnbacher, D. (2001): Instrumentalisierung und Menschenwürde. Philosophische Anmerkungen zur Debatte um Embryonen- und Stammzellforschung. In: Kaiser, G. (Hg.): Jahrbuch der Heinrich-Heine-Universität Düsseldorf 2001. Düsseldorf, S. 243–257
Birnbacher, D. (2016): Autonomous weapon systems and human dignity. In: Bhuta, N.; Beck, S.; Geiß, R.; Liu, H.-Y.; Kreß, C. (Hg.): Autonomous weapons systems. Law, ethics, policy. Cambridge, S. 105–121
Bitzinger, R.A.; Leah, C.M. (2016): Nuclear-Armed Drones? They May be Closer Than You Think. The National Interest, 13.10.2016, https://nationalinterest.org/blog/the-buzz/nuclear-armed-drones-they-may-be-closer-you-think-18034 (5.8.2020)
Blain, L. (2010): South Korea's autonomous robot gun turrets: deadly from kilometers away. New Atlas, 7.12.2010, https://newatlas.com/korea-dodamm-super-aegis-autonomos-robot-gun-turret/17198/ (5.8.2020)
BMVg (Bundesministerium der Verteidigung) (1992): Humanitäres Völkerrecht in bewaffneten Konflikten. Handbuch. http://www.humanitaeres-voelkerrecht.de/HbZDv15.2.pdf (5.8.2020)

BMVg (2004): Grundzüge der Konzeption der Bundeswehr, Berlin
BMVg (2016): Prüfung neuer Waffen, Mittel und Methoden der Kriegsführung. Zentrale Dienstvorschrift Nr. A-2146/1
BMVg (2018a): Europäische Rüstung stärken. 19.6.18, https://www.bmvg.de/de/aktuelles/europaeische-ruestung-staerken-25498 (5.8.2020)
BMVg (2018b): Heron TP. https://www.bmvg.de/de/themen/dossiers/heron-tp (9.10.2020)
BMVg (2018c): MANTIS – Schutz auf höchstem Niveau. 26.1.2018, https://www.bmvg.de/de/aktuelles/mantis---schutz-auf-hoechstem-niveau-21658 (14.2.2018)
Bodner, M. (2015): Russian Modernization Puts Focus on Land Force Protection. Defense News, 11.10.2015, https://www.defensenews.com/land/2015/10/11/russian-modernization-puts-focus-on-land-force-protection/ (5.8.2020)
Bornstein, J. (2015): DoD Autonomy Roadmap Autonomy Community of Interest. In: Defense Technical Information Center (Hg.): Maps and Gaps in DoD CoIs. CoI = Community of Interest. NDIA 16thAnnual Science & Engineering Technology Conference/Defense Tech Exposition. Springfield VA, 24.-26.3.2015, https://ndiastorage.blob.core.usgovcloudapi.net/ndia/2015/SET/WedBornstein.pdf (5.8.2020)
Bostrom, N. (2014): Superintelligenz: Szenarien einer kommenden Revolution. Berlin
Boulanin, V. (2016a): Mapping the development of autonomy in weapon systems. A primer on autonomy, https://www.sipri.org/sites/default/files/Mapping-development-autonomy-in-weapon-systems.pdf (5.8.2020)
Boulanin, V. (2016b): Mapping the innovation ecosystem driving the advance of autonomy in weapon systems, https://www.sipri.org/sites/default/files/Mapping-innovation-ecosystem-driving-autonomy-in-weapon-systems.pdf (5.8.2020)
Boulanin, V.; Verbruggen, M. (2017): Mapping the Development of Autonomy in Weapon Systems, https://www.sipri.org/sites/default/files/2017-11/siprireport_mapping_the_development_of_autonomy_in_weapon_systems_1117_0.pdf (5.8.2020)
Bowcott, O. (2015): UK opposes international ban on developing »killer robots«. Activists urge bar on weapons that launch attacks without human intervention as UN discusses future of autonomous weapons. The Guardian, 13.4.2015
Bromley, M.; Maletta, G. (2018): The challenge of software and technology transfers to non-proliferation efforts. Implementing and complying with export controls, https://www.sipri.org/sites/default/files/2018-04/sipri1804_itt_software_bromley_et_al.pdf (5.8.2020)
Brooke-Holland, L. (2015): Overview of military drones used by the UK armed forces. BRIEFING PAPER Number 06493, https://researchbriefings.files.parliament.uk/documents/SN06493/SN06493.pdf (5.8.2020)
Brown, D. (2018): Russia's Uran-9 robot tank reportedly performed horribly in Syria. Business Insider, 9.7.2018, https://www.businessinsider.com/russias-uran-9-robot-tank-performed-horribly-in-syria-2018-7?r=DE&IR=T (5.8.2020)
Brundage, M.; Avin, S.; Clark, J.; Toner, H.; Eckersley, P.; Garfinkel, B.; Dafoe, A.; Scharre, P.; Zeitzoff, T.; Filar, B.; Anderson, H. et al. (2018): The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation, https://img1.wsimg.com/blobby/go/3d82daa4-97fe-4096-9c6b-376b92c619de/downloads/1c6q2kc4v_50335.pdf (5.8.2020)
Brutzman, D.P.; Davis, D. T.; Lucas, G.R.; McGhee, R.B. (2013): Run-time Ethics Checking for Autonomous Unmanned Vehicles: Developing a Practical

Approach, Paper and Slideset. Proceedings of the 18th International Symposium on Unmanned Untethered Submersible Technology (UUST), Portsmouth
Buchanan, B.; Miller, T. (2017): Machine Learning for Policymakers. What It Is and Why It Matters. https://www.belfercenter.org/sites/default/files/files/publication/MachineLearningforPolicymakers.pdf (5.8.2020)
Bumbacher, B. (2016): Kamikaze-Drohnen im Einsatz. In: Neue Zürcher Zeitung, 8.4.2016, https://www.nzz.ch/international/naher-osten-und-nordafrika/koflikt-um-nagorni-karabach-kamikaze-drohnen-im-einsatz-ld.12404 (5.8.2020)
Bundesregierung (2009): Einführung und Bedeutung unbemannter militärischer Fahrzeuge und Luftfahrzeuge. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Alexander Bonde, Winfried Nachtwei, Omid Nouripour, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN – Drucksache 16/12193 –. Deutscher Bundestag, Drucksache 16/12481, Berlin
Bundesregierung (2016): Weißbuch 2016: Zur Sicherheitspolitik und zur Zukunft der Bundeswehr. Berlin, https://www.bundesregierung.de/resource/blob/975292/736102/64781348c12e4a80948ab1bdf25cf057/weissbuch-zur-sicherheitspolitik-2016-download-data.pdf?download=1 (5.8.2020)
Bundesregierung (2018a): Das Jagdflugzeug »Eurofighter« als Jagdbomber. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Sevim Dağdelen, Heike Hänsel, Andrej Hunko, weiterer Abgeordneter und der Fraktion DIE LINKE. – Drucksache 19/3939 –. Deutscher Bundestag, Drucksache 19/4396, Berlin
Bundesregierung (2018b): Drohnen-Schwärme in Waffensystemen der Bundeswehr. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Heike Hänsel, Michel Brandt, weiterer Abgeordneter und der Fraktion DIE LINKE. – Drucksache 19/4715 –. Deutscher Bundestag, Drucksache 19/5433, Berlin
Bundesregierung (2018c): Eckpunkte der Bundesregierung für eine Strategie Künstliche Intelligenz. Stand: 18. Juli 2018, https://www.bmbf.de/files/180718%20Eckpunkte_KI-Strategie%20final%20Layout.pdf (5.8.2020)
Bundesregierung (2018d): Jahresabrüstungsbericht 2017. Bericht der Bundesregierung zum Stand der Bemühungen um Rüstungskontrolle, Abrüstung und Nichtverbreitung sowie über die Entwicklung der Streitkräftepotenziale. Deutscher Bundestag, Drucksache 18/1380, Berlin
Bundesregierung (2018e): Neue Planungen zu bewaffneten und bewaffnungsfähigen Drohnen. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Michel Brandt, Christine Buchholz, weiterer Abgeordneter und der Fraktion DIE LINKE. – Drucksache 19/567 –. Deutscher Bundestag, Drucksache 19/1082, Berlin
Bundesregierung (2018f): Regulierung von Autonomen Waffensystemen. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Katja Keul, Agnieszka Brugger, Dr. Tobias Lindner, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN – Drucksache 19/2816 –. Deutscher Bundestag, Drucksache 19/3219, Berlin
Bünte, O. (2018): Militär-Projekt Maven: Hunderte Wissenschaftler unterstützen protestierende Google-Mitarbeiter. heise online, 17.5.2018, https://www.heise.de/newsticker/meldung/Militaer-Projekt-Maven-Hunderte-Wissenschaftler-unterstuetzen-protestierende-Google-Mitarbeiter-4050834.html (5.8.2020)
Campaign to Stop Killer Robots (2017): Unambitious process on killer robots to continue. 24.11.2017, https://www.stopkillerrobots.org/2017/11/ccwun-3/ (9.10.2020)

Campaign to Stop Killer Robots (2018): Country Views on Killer Robots. https://www.stopkillerrobots.org/wp-content/uploads/2018/11/KRC_CountryViews22Nov2018.pdf (5.8.2020)
Campbell, M. (2018): Mastering board games. In: Science 362(6419), S. 1118
Campbell, M.; Hoane, A.J.; Hsu, F.-h. (2002): Deep Blue. In: Artificial Intelligence 134(1-2), S. 57–83
Cartwright, J. (2010): Rise of the robots and the future of war, The Observer, 21.11.2010, https://www.theguardian.com/technology/2010/nov/21/military-robots-autonomous-machines (5.8.2020)
Cavanaugh, D. (2016): Robot Guns Guard the Borders of Some Countries, and More Might Follow Their Lead. Offiziere.ch, 12.4.2016, https://www.offiziere.ch/?p=27012 (5.8.2020)
CCW (2015): Report of the 2015 Informal Meeting of Experts on Lethal Autonomous Weapons Systems (LAWS). Nr. CCW/MSP/2015/3. Genf, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G15/111/60/pdf/G1511160.pdf?OpenElement (5.8.2020)
CCW (2016a): Recommendations to the 2016 Review Conference. Submitted by the Chairperson of the Informal Meeting of Experts. Advanced Version. Genf, https://www.unog.ch/80256EDD006B8954/(httpAssets)/6BB8A498B0A12A03C1257FDB00382863/$file/Recommendations_LAWS_2016_AdvancedVersion+(4+paras)+.pdf (5.8.2020)
CCW (2016b): Report of the 2016 Informal Meeting of Experts on Lethal Autonomous Weapons Systems (LAWS). Advanced Version. Genf, https://www.unog.ch/80256EDD006B8954/(httpAssets)/DDC13B243BA863E6C1257FDB00380A88/$file/ReportLAWS_2016_AdvancedVersion.pdf (5.8.2020)
CCW (2016c): United Kingdom of Great Britain and Northern Ireland Statement to the Informal Meeting of Experts on Lethal Autonomous Weapons Systems. Genf, https://www.unog.ch/80256EDD006B8954/(httpAssets)/44E4700A0A8CED0EC1257F940053FE3B/$file/2016_LAWS+MX_Towardaworkingdefinition_Statements_United+Kindgom.pdf (5.8.2020)
CCW GGE (2016a): Non Paper. Characterization of a LAWS. Genf, https://www.unog.ch/80256EDD006B8954/(httpAssets)/5FD844883B46FEACC1257F8F00401FF6/$file/2016_LAWSMX_CountryPaper_France+Characterization-ofaLAWS.pdf (9.10.2020)
CCW GGE (2016b): Non Paper. Mapping of Technological Developments. Genf, https://www.unog.ch/80256EDD006B8954/(httpAssets)/B9E3E8041CE4D326C1257F8F005A31E2/$file/2016_LAWSMX_CountryPaper_France+MappingofTechnicalDevelopments+EN.pdf (5.8.2020)
CCW GGE (2017a): For consideration by the Group of Governmental Experts on Lethal Autonomous Weapons Systems (LAWS). Submitted by France and Germany. Item 6 of the revised provisional agenda Examination of various dimensions of emerging technologies in the area of lethal autonomous weapons systems, in the context of the objectives and purposes of the Convention. CCW/GGE.1/2017/WP.4. Genf, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G17/335/40/PDF/G1733540.pdf?OpenElement (5.8.2020)
CCW GGE (2017b): Autonomy in Weapon Systems. Submitted by the United States of America. Item 6 of the revised provisional agenda Examination of various dimensions of emerging technologies in the area of lethal autonomous weapons systems, in the context of the objectives and purposes of the Convention.

Nr. CCW/GGE.1/2017/WP.6. Genf, https://www.unog.ch/80256EDD006B8954/(httpAssets)/99487114803FA99EC12581D40065E90A/$file/2017_GGEonLAWS_WP6_USA.pdf (5.8.2020)

CCW GGE (2017c): Characteristics of Lethal Autonomous Weapons Systems. Submitted by the United States of America. Item 6 of the revised provisional agenda Examination of various dimensions of emerging technologies in the area of lethal autonomous weapons systems, in the context of the objectives and purposes of the Convention. Nr. CCW/GGE.1/2017/WP.7. Genf, https://www.unog.ch/80256EDD006B8954/(httpAssets)/A4466587B0DABE6CC12581D400660157/$file/2017_GGEonLAWS_WP7_USA.pdf (5.8.2020)

CCW GGE (2017d): Opening statement USA. CCW Group of Governmental Experts on LAWS. Genf, https://www.unog.ch/80256EDD006B8954/(httpAssets)/6E9C8002759032A8C12582490031466C/$file/2017_GGE+LAWS_Statement_USA.pdf (5.8.2020)

CCW GGE (2017e): Report of the 2017 Group of Governmental Experts on Lethal Autonomous Weapons Systems (LAWS). Item 7 of the agenda Adoption of the report. Nr. CCW/GGE.1/2017/3. Genf, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G17/367/06/PDF/G1736706.pdf?OpenElement (5.8.2020)

CCW GGE (2018a): Chair's summary of the discussion on Agenda item 6(a) 9 and 10 April 2018 Agenda item 6 (b) 11 April 2018 and 12 April 2018 Agenda item 6(c) 12April 2018 Agenda item 6(d) 13 April 2018. Genf, https://www.unog.ch/80256EDD006B8954/(httpAssets)/DF486EE2B556C8A6C125827A00488B9E/$file/Summary+of+the+discussions+during+GGE+on+LAWS+April+2018.pdf (5.8.2020)

CCW GGE (2018b): EU Statement. Lethal Autonomous Weapons Systems (LAWS) Group of Governmental Experts Convention on Certain Conventional Weapons, 9–13 April 2018. Genf, https://www.unog.ch/80256EDD006B8954/(httpAssets)/00E636906F2DB883C12582720056F109/$file/2018_LAWSGeneralExchange_EU.pdf (5.8.2020)

CCW GGE (2018c): Position Paper. Submitted by China. Nr. CCW/GGE.1/2018/WP.7. Genf, https://www.unog.ch/80256EDD006B8954/(httpAssets)/E42AE83BDB3525D0C125826C0040B262/$file/CCW_GGE.1_2018_WP.7.pdf (5.8.2020)

CCW GGE (2018d): Russia's Approaches to the Elaboration of a Working Definition and Basic Functions of Lethal Autonomous Weapons Systems in the Context of the Purposes and Objectives of the Convention. Submitted by the Russian Federation. Nr. CCW/GGE.1/2018/WP.6. Genf, https://www.unog.ch/80256EDD006B8954/(httpAssets)/67F8B7C54687DC55C125825F004B2E72/$file/CCW_GGE.1_2018_WP.6.pdf (5.8.2020)

CCW GGE (2018e): Statement by France and Germany. under Agenda Item »General Exchange of Views«. Genf, https://www.unog.ch/80256EDD006B8954/(httpAssets)/895931D082ECE219C12582720056F12F/$file/2018_LAWSGeneralExchange_Germany-France.pdf (5.8.2020)

CCW GGE (2018f): Statement delivered by Germany on Working Definition of LAWS/»Definition of Systems under Consideration«. Genf, https://www.unog.ch/80256EDD006B8954/(httpAssets)/2440CD1922B86091C12582720057898F/$file/2018_LAWS6a_Germany.pdf (5.8.2020)

CCW GGE (2018g): General principles on Lethal Autonomous Weapons Systems. Submitted by the Bolivarian Republic of Venezuela on behalf of the Non-Aligned

Movement (NAM) and Other States Parties to the Convention on Certain Conventional Weapons (CCW). Item 6 of the provisional agenda. Nr. CCW/GGE.1/2018/WP.1. Genf, https://www.unog.ch/80256EDD006B8954/(httpAssets)/E9BBB3F7ACBE8790C125825F004AA329/$file/CCW_GGE_1_2018_WP.1.pdf (5.8.2020)

CCW GGE (2018h): Humanitarian benefits of emerging technologies in the area of lethal autonomous weapon systems. Item 6 of the provisional agenda. Nr. CCW/GGE.1/2018/WP.4. Genf, https://www.unog.ch/80256EDD006B8954/(httpAssets)/7C177AE5BC10B588C125825F004B06BE/$file/CCW_GGE.1_2018_WP.4.pdf (5.8.2020)

CCW GGE (2018i): Human Machine Touchpoints: The United Kingdom's perspective on human control over weapon development and targeting cycles. Item 6 of the provisional agenda. Nr. CCW/GGE.2/2018/WP.1. Genf, https://www.unog.ch/80256EDD006B8954/(httpAssets)/050CF806D90934F5C12582E5002EB800/$file/2018_GGE+LAWS_August_Working+Paper_UK.pdf (5.8.2020)

CCW GGE (2018j): Human-Machine Interaction in the Development, Deployment and Use of Emerging Technologies in the Area of Lethal Autonomous Weapons Systems. Submitted by the United States of America. Nr. CCW/GGE.2/2018/WP.4. Genf, https://www.unog.ch/80256EDD006B8954/(httpAssets)/D1A2BA4B7B71D29FC12582F6004386EF/$file/2018_GGE+LAWS_August_Working+Paper_US.pdf (5.8.2020)

CCW GGE (2018k): Report of the 2018 session of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems. Nr. CCW/GGE.1/2018/3. Genf, https://undocs.org/pdf?symbol=en/CCW/GGE.1/2018/3 (5.8.2020)

CCW GGE (2019): Agenda. Submitted by the Chairperson. Item 2 of the agenda. Adoption of the agenda. Nr. CCW/GGE.1/2019/1/Rev.1. Genf, https://www.unog.ch/80256EDD006B8954/(httpAssets)/884DF349536F790BC12583C8004C3AEB/$file/CCW_GGE1_2019_1_Rev.1_Agenda_final.pdf (5.8.2020)

CDU/CSU; SPD (2018): Ein neuer Aufbruch für Europa Eine neue Dynamik für Deutschland Ein neuer Zusammenhalt für unser Land. Koalitionsvertrag zwischen CDU, CSU und SPD. Entwurf Stand: 7.2.2018, http://www.tagesspiegel.de/downloads/20936562/4/koav-gesamttext-stand-070218-1145h.pdf (5.8.2020)

Chen, S. (2013): After drones, China turns to unmanned vessels to boost its marine power. South China Morning Post, 5.12.2013, http://www.scmp.com/news/china/article/1373490/after-drones-china-turns-unmanned-vessels-boost-its-marine-power (5.8.2020)

Chief of Naval Operations (2016): Autonomous Undersea Vehicle Requirement for 2025. Undersea Warfare Directorate, Washington D.C., https://news.usni.org/wp-content/uploads/2016/03/18Feb16-Report-to-Congress-Autonomous-Undersea-Vehicle-Requirement-for-2025.pdf (5.8.2020)

Chinese Delegation (o. J.): The poistion paper submitted by the Chinese delegation to CCW 5th Review Conference. https://www.unog.ch/80256EDD006B8954/(httpAssets)/DD1551E60648CEBBC125808A005954FA/$file/China%27s+Position+Paper.pdf (5.8.2020)

Clearfield, C.; Tilcsik, A. (2018): Meltdown. Why our systems fail and what we can do about it. New York

Cole, C. (2016): European use of military drones expanding. Drone Wars, 19.7.2016, https://dronewars.net/2016/07/19/european-use-of-military-drones-expanding/ (9.10.2020)
Danzig, R. (2018): Technology Roulette. Managing Loss of Control as Many Militaries Pursue Technological Superiority. Washington D.C., https://s3.amazonaws.com/files.cnas.org/documents/CNASReport-Technology-Roulette-Final.pdf (5.8.2020)
DARPA (Defense Advanced Research Projects Agency) (o. J.a): Target Recognition and Adaption in Contested Environments (TRACE). https://www.darpa.mil/program/trace (9.10.2020)
DARPA (o. J.b): Fast Lightweight Autonomy (FLA) (Archived). https://www.darpa.mil/program/fast-lightweight-autonomy (9.10.2020)
DARPA (o. J.c): Collaborative Operations in Denied Environment (CODE) (Archived). https://www.darpa.mil/program/collaborative-operations-in-denied-environment (9.10.2020)
DARPA (o. J.d): Anti-Submarine Warfare (ASW) Continuous Trail Unmanned Vessel (ACTUV) (Archived). https://www.darpa.mil/program/anti-submarine-warfare-continuous-trail-unmanned-vessel (9.10.2020)
Dassault Aviation (2016): Another world first for the nEUROn. 4.6.2016, https://www.dassault-aviation.com/en/group/press/press-kits/another-world-first-neuron/ (5.8.2020)
Dastin, J. (2018): Amazon scraps secret AI recruiting tool that showed bias against women. Reuters, 10.10.2018, https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G (5.8.2020)
Davison, N. (2017): A legal perspective: Autonomous weapon systems under international humanitarian law. In: UNODA (Hg.): Perspectives on lethal autonomous weapon systems. New York, S. 5–18
DBWV (Deutscher Bundeswehrverband) (2016): Hochmodern und effektiv. Luftwaffe schützt Feldlager mit MANTIS. https://www.dbwv.de/landesverbaende-kameradschaften/lv-nord/aktuelle-themen/beitrag/news/hochmodern-und-effektiv/ (5.8.2020)
Deagel.com (o. J.): Okhotnik-B. https://www.deagel.com/Combat%20Aircraft/Okhotnik-B/a003499 (9.10.2020)
Dean, S.E. (2017): Unbemannte Unterwassersysteme Trends und technologische Entwicklung. In: MarineForum 10, S. 36–39
Defense Industry Daily (2019): BAE-Lockheed Team supplied USAF with LRASM. https://www.defenseindustrydaily.com/bae-lockheed-team-supplied-usaf-with-lrasm-british-typhoons-started-baltic-air-policing-mission-china-has-a-third-aircraft-carrier-042192/ (5.8.2020)
Defense Update (2006): Harpy air defense suppression system. https://defense-update.com/20060403_harpy.html (9.10.2020)
Deutscher Bundestag (2016): Schriftliche Fragen mit den in der Woche vom 11. Juli 2016 eingegangenen Antworten der Bundesregierung. Deutscher Bundestag, Drucksache 18/9191, Berlin
Deutscher Bundestag (2018a): Stenografischer Bericht. 57. Sitzung. Mündliche Frage 75, Andrej Hunko (DIE LINKE). Technische Untersuchungen hinsichtlich des Ausweichens militärischer Drohnen vor anderen Luftfahrzeugen. Plenarprotokoll Nr. 19/57, Berlin

Deutscher Bundestag (2018b): Einsetzung einer Enquete-Kommission »Künstliche Intelligenz – Gesellschaftliche Verantwortung und wirtschaftliche, soziale und ökologische Potenziale«. Antrag der Fraktionen CDU/CSU, SPD, FDP und DIE LINKE. Drucksache 19/2978, Berlin

Dickow, M. (2015): Robotik – ein Game-Changer für Militär und Sicherheitspolitik? SWP-Studie Nr. 2015/S 14. Berlin, https://www.swp-berlin.org/fileadmin/contents/products/studien/2015_S14_dkw.pdf (5.8.2020)

Dickow, M.; Dahlmann, A.; Alwardt, C.; Sauer, F.; Schörnig, N. (2015a): First Steps towards a Multidimensional Autonomy Risk Assessment (MARA) in Weapons Systems. SWP Working Papers Nr. FG Sicherheitspolitik WP No 05, Berlin, https://www.swp-berlin.org/fileadmin/contents/products/arbeitspapiere/FG03_WP05_2015_MARA.pdf (5.8.2020)

Dickow, M.; Hansel, M.; Mutschler, M.M. (2015b): Präventive Rüstungskontrolle – Möglichkeiten und Grenzen mit Blick auf die Digitalisierung und Automatisierung des Krieges. In: S+F 33(2), S. 67–73

DOD (U.S. Department of Defense) (2009): FY2009-2034 Unmanned Systems Integrated Roadmap. http://www.dtic.mil/get-tr-doc/pdf?Location=U2&doc=GetTRDoc.pdf&AD=ADA522247 (5.8.2020)

DOD (2012): Directive Number 3000.09. SUBJECT: Autonomy in Weapon Systems. https://www.hsdl.org/?view&did=726163 (5.8.2020)

DOD (2013): Unmanned Systems Integrated Roadmap FY2013-2038. http://archive.defense.gov/pubs/dod-usrm-2013.pdf (5.8.2020)

DOD (2015a): Annual report to Congress. Military and Security Developments Involving the People's Republic of China 2015. Office of the Secretary of Defense, https://dod.defense.gov/Portals/1/Documents/pubs/2015_China_Military_Power_Report.PDF (1.9.2020)

DOD (2015b): Technology Investment Strategy 2015-2018. Autonomy Community of Interest (COI) Test and Evaluation, Verification and Validation (TEVV) Working Group. Office of the Assistant Sectretary of Defense For Research & Engineering, https://apps.dtic.mil/dtic/tr/fulltext/u2/1010194.pdf (5.8.2020)

DOD (2017a): Annual Report to Congress. Military and Security Developments. Involving the People's Republic of China 2017. Office of the Secretary of Defense, https://dod.defense.gov/Portals/1/Documents/pubs/2017_China_Military_Power_Report.PDF (1.9.2020)

DOD (2017b): Unmanned Systems Integrated Roadmap. 2017-2042. https://www.defensedaily.com/wp-content/uploads/post_attachment/206477.pdf (5.8.2020)

DOD (2017c): Department of Defense Announces Successful Micro-Drone Demonstration. https://dod.defense.gov/News/News-Releases/News-Release-View/Article/%201044811/department-of-defense-announces-successful-micro-drone-demonstration/ (7.8.2020)

DOD (2018a): Nuclear Posture Review. Office of the Secretary of Defense. https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-NUCLEAR-POSTURE-REVIEW-FINAL-REPORT.PDF (5.8.2020)

DOD (2018b): Summary of the 2018 National Defense Strategy of the United States of America. Sharpening the American Military's Competitive Edge. Washington D.C., https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf (5.8.2020)

DOD (2019): Summary of the 2018 Department of Defense Artificial Intelligence Strategy. Harnessing AI to Advance Our Security and Prosperity. Washington

D.C., https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF (5.8.2020)
Dombe, A.R. (2016): The UUV Market is on Fire. Israel Defense, 3.3.2016, https://www.israeldefense.co.il/en/content/uuv-market-fire (5.8.2020)
DON (U.S. Department of the Navy) (2018): Strategic Roadmap for Unmanned Systems. Short Version. https://www.secnav.navy.mil/rda/Documents/DON-Strategic-Roadmap-for-Unmanned-Systems.docx (30.4.2019)
Doran, D.; Schulz, S.; Besold, T.R. (2017): What Does Explainable AI Really Mean? A New Conceptualization of Perspectives. http://arxiv.org/pdf/1710.00794v1 (5.8.2020)
Drew, J. (2017): Drone strike: Long-range attack UAVs being developed from aerial targets. In: Aviation week & space technology 179(4), S. 42–43
DSB (Defense Science Board) (2012): The Role of Autonomy in DoD Systems. https://fas.org/irp/agency/dod/dsb/autonomy.pdf (5.8.2020)
DSB (2016): Summer Study on Autonomy. https://fas.org/irp/agency/dod/dsb/autonomy-ss.pdf (5.8.2020)
Dutch Government (2016): Autonomous weapon systems: the need for meaningful human control. Government response to AIV/CAVV advisory report no. 97, https://aiv-advice.nl/8gr#government-responses (9.3.2018)
Eckstein, M. (2016): Navy: Future Undersea Warfare Will Have Longer Reach, Operate With Network of Unmanned Vehicles. https://news.usni.org/2016/03/24/navy-future-undersea-warfare-will-have-longer-reach-operate-with-network-of-unmanned-vehicles (5.8.2020)
EDA (European Defence Agency) (2015): Remotely Piloted Aircraft Systems. https://www.eda.europa.eu/docs/default-source/eda-factsheets/2015-01-30-factsheet_rpas_high (5.8.2020)
EDA (European Defence Agency) (2019): Remotely Piloted Aircraft Systems – RPAS. https://www.eda.europa.eu/what-we-do/activities/activities-search/remotely-piloted-aircraft-systems---rpas (9.10.2020)
Egozi, A. (2017): Israeli air force preparing new UAV roadmap. FlightGlobal, 14.6.2017, https://www.flightglobal.com/news/articles/israeli-air-force-preparing-new-uav-roadmap-438228/ (5.8.2020)
EK (Europäische Kommission) (2017): Der Europäische Verteidigungsfonds: 5,5 Mrd. EUR pro Jahr, um Europas Verteidigungsfähigkeiten zu stärken. 7.6.2017, http://europa.eu/rapid/press-release_IP-17-1508_de.htm (5.8.2020)
Elbit Systems Ltd. (o. J.): Unmanned Surface Vehicle. http://elbitsystems.com/product/unmanned-surface-vehicle/ (9.10.2020)
Ellman, J.; Samp, L.; Coll, G. (2017): Assessing the Third Offset Strategy. https://csis-prod.s3.amazonaws.com/s3fs-public/publication/170302_Ellman_ThirdOffsetStrategySummary_Web.pdf (5.8.2020)
EP (2017): Bericht mit Empfehlungen an die Kommission zu zivilrechtlichen Regelungen im Bereich Robotik (2015/2103(INL). Straßburg, https://www.europarl.europa.eu/doceo/document/A-8-2017-0005_DE.pdf (5.8.2020)
EP (2018): Entschließung des Europäischen Parlaments vom 12. September 2018 zu autonomen Waffensystemen. Nr. 2018/2752(RSP), Straßburg, https://www.europarl.europa.eu/doceo/document/TA-8-2018-0341_DE.pdf (5.8.2020)
EP (Europäisches Parlament) (2014): Entschließung des Europäischen Parlaments vom 27. Februar 2014 zum Einsatz von bewaffneten Drohnen. Nr. P7_TA (2014)0172, Brüssel, https://op.europa.eu/o/opportal-service/download-handler?

identifier=a4a4eab5-8c46-11e7-b5c6-01aa75ed71a1&format=pdfa1a&language=de&productionSystem=cellar&part= (5.8.2020)
Ernest, N.; Carroll, D.; Schumacher, C.; Clark, M.; Cohen, K.; Lee, G. (2016): Genetic Fuzzy based Artificial Intelligence for Unmanned Combat Aerial Vehicle Control in Simulated Air Combat Missions. In: J Def Manag 06(01)
Eshel, T. (2015): Russian Military to Test Combat Robots in 2016. https://defense-update.com/20151231_russian-combat-robots.html (5.8.2020)
Ethik-Kommission (Ethik-Kommission Automatisiertes und vernetztes Fahren) (2017): Ethik-Kommission Automatisiertes und vernetztes Fahren: Bericht Juni 2017. Bundesministerium für Verkehr und digitale Infrastruktur, https://www.bmvi.de/SharedDocs/DE/Publikationen/DG/bericht-der-ethik-kommission.pdf?__blob=publicationFile (5.8.2020)
Ewers, E.C.; Fish, L.; Horowitz, M.C.; Sander, A.; Scharre, P. (2017): Drone Proliferation. Policy Choices for the Trump Administration. Center for a New American Security, http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/CNASReport-DroneProliferation-Final.pdf (5.8.2020)
Eykholt, K.; Evtimov, I.; Fernandes, E.; Li, B.; Rahmati, A.; Xiao, C.; Prakash, A.; Kohno, T.; Song, D. (2018): Robust Physical-World Attacks on Deep Learning Models. http://arxiv.org/pdf/1707.08945v5 (5.8.2020)
Farmer, B. (2015): Taranis stealth drone may see final test flights later this year. The Telegraph, 13.9.2015, https://www.telegraph.co.uk/news/uknews/defence/11859967/Taranis-stealth-drone-may-see-final-test-flights-later-this-year.html (5.8.2020)
Fefegha, A. (2018): Racial Bias and Gender Bias Examples in AI systems. The Comuzi Journal, 2.9.2018, https://medium.com/thoughts-and-reflections/racial-bias-and-gender-bias-examples-in-ai-systems-7211e4c166a1 (5.8.2020)
Fischer, J.M.; Ravizza, M. (1998): Responsibility and control. A theory of moral responsibility. Cambridge
FLI (Future of Life Institute) (o. J.a): Autonome Waffen: ein offener Brief von KI- & Robotik-Forschern. https://futureoflife.org/open-letter-on-autonomous-weapons-german/#top (9.10.2020)
FLI (o. J.b): Die KI-Leitsätze von Asilomar. https://futureoflife.org/ai-principles-german/ (9.10.2020)
Frank, M. (2009): Das ius post bellum und die Theorie des gerechten Krieges. In: PVS 50(4), S. 732–753
Franke, U.E.; Leveringhaus, A. (2015): Militärische Robotik. In: Jäger, T. (Hg.): Handbuch Sicherheitsgefahren. Wiesbaden, S. 297–311
GA-ASI (General Atomics Aeronautical Systems, Inc.) (o. J.): Gray Eagle. http://www.ga-asi.com/gray-eagle (9.10.2020)
Gady, F.-S. (2016): New US Defense Budget: $18 Billion for Third Offset Strategy. The Diplomat, 10.2.2016, https://thediplomat.com/2016/02/new-us-defense-budget-18-billion-for-third-offset-strategy/ (5.8.2020)
GAO (Governmental Accountability Office) (2018): Artificial Intelligence. Emerging Opportunities, Challenges, and Implications. HIGHLIGHTS OF A FORUM Convened by the Comptroller General. Nr. GAO-18-142SP, https://www.gao.gov/assets/700/690910.pdf (5.8.2020)

Gautier, J.; Reiner, D.; Pintat, X. (2016): DÉFENSE: ÉQUIPEMENT DES FORCES. N°142. Sénat Session Ordinaire de 2016–2017, http://www.senat.fr/rap/a16-142-8/a16-142-81.pdf (1.9.2020)
Geiß, R. (2015): Die völkerrechtliche Dimension autonomer Waffensysteme. Friedrich Ebert Stiftung, http://library.fes.de/pdf-files/id/ipa/11444-20150619.pdf (5.8.2020)
General Secretariat of the Council (2019): Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing the European Defence Fund, (First reading) – Progress report. 6733/1/19 REV 1, Council of the European Union, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_6733_2019_REV_1&from=EN (5.8.2020)
Global Security (o. J.a): Low Cost Autonomous Attack System (LOCAAS). https://www.globalsecurity.org/military/systems/munitions/locaas.htm (9.10.2020)
Global Security (o. J.b): Samsung Techwin SGR-A1 Sentry Guard Robot. https://www.globalsecurity.org/military/world/rok/sgr-a1.htm (9.10.2020)
Global Security (o. J.c): Sukhoi S-70 Okhotnik-B. https://www.globalsecurity.org/military/world/russia/su-70.htm (9.10.2020)
Goodfellow, I.; Papernot, N.; Huang, S.; Duan, R.; Abbeel, P.; Clark, J. (2017): Attacking Machine Learning with Adversarial Examples. https://openai.com/blog/adversarial-example-research/ (5.8.2020)
Goodfellow, I.J.; Shlens, J.; Szegedy, C. (2015): Explaining and Harnessing Adversarial Examples. http://arxiv.org/pdf/1412.6572v3 (5.8.2020)
GOV.UK (2015): SBRI: the Small Business Research Initiative. https://www.gov.uk/government/collections/sbri-the-small-business-research-initiative (9.10.2020)
Gramer, R.; Seligman, L. (2019): The INF Treaty Is Dead. Is New START Next? Foreign Policy, 1.2.2019, https://foreignpolicy.com/2019/02/01/the-inf-treaty-is-dead-is-new-start-next-russia-arms/ (9.10.2020)
Grunwald, A. (2013): Einleitung und Überblick. In: Grunwald, A. (Hg.): Handbuch Technikethik. Stuttgart, S. 1–11
Gubrud, M. (2013): US killer robot policy: Full speed ahead. Bulletin of the Atomic Scientists, 20.9.2013, https://thebulletin.org/2013/09/us-killer-robot-policy-full-speed-ahead/ (5.8.2020)
Gubrud, M. (2015): Semi-autonomous and on their own: Killer robots in Plato's Cave. Bulletin of the Atomic Scientists, 12.4.2015, https://thebulletin.org/2015/04/semi-autonomous-and-on-their-own-killer-robots-in-platos-cave/ (5.8.2020)
Gubrud, M.; Altmann, J. (2013): Compliance Measures for an Autonomous Weapons Convention. ICRAC Working Paper #2, https://www.icrac.net/wp-content/uploads/2018/04/Gubrud-Altmann_Compliance-Measures-AWC_ICRAC-WP2.pdf (5.8.2020)
Gunning, D. (2017): Explainable Artificial Intelligence (XAI). DARPA/I2O, https://www.darpa.mil/attachments/XAIProgramUpdate.pdf (5.8.2020)
Gutmann, T. (2010): Struktur und Funktion der Menschenwürde als Rechtsbegriff. Preprints of the Centre for Advanced Study in Bioethics. Münster, https://www.uni-muenster.de/imperia/md/content/kfg-normenbegruendung/intern/publikationen/gutmann/07_gutmann_-_menschenw__rde_als_rechtsbegriff.pdf (5.8.2020)
Hagel, C. (2014): Reagan National Defense Forum Keynote. Speech, 15.11.2014, https://dod.defense.gov/News/Speeches/Speech-View/Article/606635/ (5.8.2020)

Haider, A. (2014): Remotely Piloted Aircraft Systems in Contested Environments. A Vulnerability Analysis. Kalkar, http://www.japcc.org/wp-content/uploads/2015/03/JAPCC-RPAS-Operations-in-Contested-Environments.pdf (5.8.2020)
Hambling, D. (2014a): Armed Russian robocops to defend missile bases. New Scientist, 23.4.2014, https://www.newscientist.com/article/mg22229664-400-armed-russian-robocops-to-defend-missile-bases/ (1.9.2020)
Hambling, D. (2014b): Russia Wants Autonomous Fighting Robots, and Lots of Them. Popular Mechanics, 12.5.2014, https://www.popularmechanics.com/military/a10511/russia-wants-autonomous-fighting-robots-and-lots-of-them-16787165/ (5.8.2020)
Hawley, J.K. (2017): Patriot Wars. Automation and the Patriot Air and Missile Defense System. Center for a New American Security, Ethical Autonomy Series, https://s3.amazonaws.com/files.cnas.org/documents/CNAS-Report-EthicalAutonomy5-PatriotWars-FINAL.pdf?mtime=20170106135013 (5.8.2020)
He, K.; Zhang, X.; Ren, S.; Sun, J. (2015): Delving Deep into Rectifiers: Surpassing Human-Level Performance on ImageNet Classification. http://arxiv.org/pdf/1502.01852v1 (5.8.2020)
Heinrich, A. (2018): Verpasste Chancen. Die russische Krim-Annexion und Ukraine-Krise haben die europäische Sicherheitsordnung erschüttert. Können Russland und der Westen neues Vertrauen aufbauen? In: Das Parlament 15–16, S. 10
Hellström, T. (2013): On the moral responsibility of military robots. In: Ethics Inf Technol 15(2), S. 99–107
Heyns, C. (2013): Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions, Christof Heyns. General Assembly, United Nations, Nr. A/HRC/23/47, http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A-HRC-23-47_en.pdf (5.8.2020)
Heyns, C. (2016): Autonomous weapon systems: living a dignified life and dying a dignified death. In: Bhuta, N.; Beck, S.; Geiß, R.; Liu, H.-Y.; Kreß, C. (Hg.): Autonomous weapons systems. Law, ethics, policy. Cambridge, S. 3–20
Hilgendorf, E. (2012): Können Roboter schuldhaft handeln? In: Beck, S. (Hg.): Jenseits von Mensch und Maschine: Ethische und rechtliche Fragen zum Umgang mit Robotern, künstlicher Intelligenz und Cyborgs. Baden-Baden, S. 119–132
Hilgendorf, E. (Hg.) (2014): Robotik im Kontext von Recht und Moral. Robotik und Recht 3, Baden-Baden
Hoffmann, L. (2015): Germany To Lead Development of European UAV. Defense News, 11.12.2015, https://www.defensenews.com/air/2015/12/11/germany-to-lead-development-of-european-uav/ (5.8.2020)
Hoppe, T.; Werkner, I.-J. (2017): Der gerechte Frieden: Positionen in der katholischen und evangelischen Kirche in Deutschland. In: Werkner, I.-J.; Ebeling, K. (Hg.): Handbuch Friedensethik. Wiesbaden, S. 341–358
Horowitz, M.C.; Kreps, S.E.; Fuhrmann, M. (2016): Separating Fact from Fiction in the Debate over Drone Proliferation. In: International Security 41(2), S. 7–42
House of Lords Select Committee on Artificial Intelligence (2018): AI in the UK: ready, willing and able? Report of Session 2017–19. House of Lords, HL Paper Nr. 100, London, https://publications.parliament.uk/pa/ld201719/ldselect/ldai/100/100.pdf (5.8.2020)
HRW (Human Rights Watch) (2012): Losing humanity. The case against killer robots (Docherty, B.). New York

HRW (2014): Shaking the Foundations. The Human Rights Implications of Killer Robots. New York, https://www.hrw.org/sites/default/files/reports/arms0514_ForUpload_0.pdf (5.8.2020)
HRW (2017): US Embraces Cluster Munitions. 1.12.2017, https://www.hrw.org/news/2017/12/01/us-embraces-cluster-munitions (9.10.2020)
Hu, J.C. (2018): Waymo's driverless cars have logged 10 million miles on public roads. Quartz, 10.10.2018, https://qz.com/1419747/waymos-self-driving-cars-have-logged-10-million-miles/ (5.8.2020)
Hutson, M. (2018): AI takes on video games in quest for common sense. In: Science 361(6403), S. 632–633
IAI (o. J.): HARPY. Autonomous Weapon for All Weather. https://www.iai.co.il/p/harpy (9.10.2020)
IBM (o. J.): So ist die Welt mit IBM Watson. https://www.ibm.com/thought-leadership/smart/de-de/watson/ai-stories/ (9.10.2020)
ICBL-CMC (International Campaign to Ban Landmines-Cluster Munition Coalition) (2017): Cluster Munition Monitor 2017. http://www.the-monitor.org/media/2582190/Cluster-Munition-Monitor-2017_web4.pdf (5.8.2020)
ICC (International Criminal Court) (o. J.): The States Parties to the Rome Statute. https://asp.icc-cpi.int/en_menus/asp/states%20parties/Pages/the%20states%20parties%20to%20the%20rome%20statute.aspx (9.10.2020)
IEEE (Institute of Electrical and Electronics Engineers) (2016): Ethically Alligned Design. A Vision for Prioritizing Human Wellbeing with Artificial Intelligence and Autonomous Systems. Version 1 – For Public Discussion. http://standards.ieee.org/develop/indconn/ec/ead_v1.pdf (5.8.2020)
IKRK (Internationales Kommittee vom Roten Kreuz) (1987): Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977. Commentary of 1987 Responsibility. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Article.xsp?action=openDocument&documentId=F461FC196C18A52DC12563CD0051E2AC (5.8.2020)
IKRK (2006): A Guide to the Legal Review of New Weapons, Means and Methods of Warfare. Measures to implement Article 36 of Additional Protocol I of 1977. Genf, https://www.icrc.org/eng/assets/files/other/icrc_002_0902.pdf (5.8.2020)
IKRK (2018a): Ethics and autonomous weapon systems: An ethical basis for human control? Group of Governmental Experts of the High Contracting Parties to the CCW. Nr. CCW/GGE.1/2018/WP.5. Genf, https://www.unog.ch/80256EDD006B8954/(httpAssets)/42010361723DC854C1258264005C3A7D/$file/CCW_GGE.1_2018_WP.5+ICRC+final.pdf (5.8.2020)
IKRK (2018b): Statement of the International Committee of the Red Cross (ICRC). Genf, https://www.icrc.org/en/document/towards-limits-autonomous-weapons (5.8.2020)
IKRK (2019): Statement of the International Committee of the Red Cross (ICRC) under agenda item 5(e) Possible options for addressing the humanitarian and international security challenges posed by emerging technologies in the area of lethal autonomous weapon systems in the context of the objectives and purposes of the Convention without prejudicing policy outcomes and taking into account past, present and future proposals. Convention on Certain Conventional Weapons (CCW) Group of Governmental Experts on Lethal Autonomous Weapons Systems. Genf, https://www.unog.ch/80256EDD006B8954/(httpAssets)/59013C15

951CD355C12583CC002FDAFC/$file/CCW+GGE+LAWS+ICRC+statement+agenda+item+5e+27+03+2019.pdf (5.8.2020)
IKRK (o. J.): Geneva Conventions of 1949 and Additional Protocols, and their Commentaries. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/vwTreaties1949.xsp (9.10.2020)
Indian Defense Blog (2017): Unmanned ground vehicle developement in India. 10.12.2017, https://indiandefblog.wordpress.com/2017/12/10/unmanned-ground-vehicle-developement-in-india/ (1.10.2019)
IPRAW (International Panel on the Regulation of Autonomous Weapons) (2017a): Focus on Technology and Application of Autonomous Weapons. »Focus on« Report No. 1, Berlin, https://www.ipraw.org/wp-content/uploads/2017/08/2017-08-17_iPRAW_Focus-On-Report-1.pdf (5.8.2020)
IPRAW (2017b): Focus on Computational Methods in the Context of LAWS. »Focus on« Report No. 2, Berlin, https://www.ipraw.org/wp-content/uploads/2017/11/2017-11-10_iPRAW_Focus-On-Report-2.pdf (5.8.2020)
IPRAW (2018a): Focus on Ethical Implications for a Regulation of LAWS. »Focus on« Report No. 4, Berlin, https://www.ipraw.org/wp-content/uploads/2018/08/2018-08-17_iPRAW_Focus-On-Report-4.pdf (5.8.2020)
IPRAW (2018b): Concluding Report: Recommendations to the GGE. Berlin, https://www.ipraw.org/wp-content/uploads/2018/12/2018-12-14_iPRAW_Concluding-Report.pdf (5.8.2020)
Jaroslawl (2017): Открытый урок »Россия, устремлённая в будущее«. Администрация Президента России, 1.9.2017, http://kremlin.ru/events/president/news/55493 (9.10.2020)
Jenkins, R.; Purves, D. (2016): Robots and Respect: A Response to Robert Sparrow. In: Ethics int. aff. 30(03), S. 391–400
Johnson, D.D.P. (2004): Overconfidence and war. The havoc and glory of positive illusions. Cambridge
Johnson, D.G. (2015): Technology with No Human Responsibility? In: J Bus Ethics 127(4), S. 707–715
Jönsson, H. (2007): Risk and vulnerability analysis of complex systems. A basis for proactive emergency management. Report 1038, Lund
Jun, J.-h. (2018): Hanwha, KAIST to develop AI weapons. Controversy remains on whether autonomous arms are really necessary. In: Korean Times, 25.2.2018, https://www.koreatimes.co.kr/www/tech/2018/02/133_244641.html (1.9.2020)
K.S. (2019): FCAS-Konzeptstudien starten. FLUG REVUE, 6.2.2019, https://www.flugrevue.de/militaer/dassault-aviation-und-airbus-fcas-konzeptstudien-starten/ (9.10.2020)
Kania, E. (2017): Battlefield Singularity. Artificial Intelligence, Military Revolution, and China's Future Military Power. Center for a New American Security, Washington D.C., https://s3.amazonaws.com/files.cnas.org/documents/Battlefield-Singularity-November-2017.pdf (7.8.2020)
Kania, E. (2018): China's Strategic Ambiguity and Shifting Approach to Lethal Autonomous Weapons Systems. Lawfare Institute, 17.4.2018, https://www.lawfareblog.com/chinas-strategic-ambiguity-and-shifting-approach-lethal-autonomous-weapons-systems (7.3.2019)
Kasparov, G. (2018): Chess, a Drosophila of reasoning. In: Science 362(6419), S. 1087
Kettner, M. (Hg.) (2004): Biomedizin und Menschenwürde. Frankfurt a.M.

Kirkpatrick, J.; Pascanu, R.; Rabinowitz, N.; Veness, J.; Desjardins, G.; Rusu, A.A.; Milan, K.; Quan, J.; Ramalho, T.; Grabska-Barwinska, A.; Hassabis, D.; Clopath, C. et al. (2017): Overcoming catastrophic forgetting in neural networks. London, http://arxiv.org/pdf/1612.00796v2 (7.8.2020)
Koch, B. (2017): Bewaffnete Drohnen. Bernhard Koch zur Frage, was ihren militärischen Einsatz so fragwürdig macht. In: Information Philosophie (3), S. 8–15
Koch, B.; Rinke, B. (2017): Ethische Fragestellungen im Kontext autonomer Waffensysteme. Institut für Theologie und Frieden, Hamburg
Kratos (Kratos Defense & Security Solutions, Inc.) (o. J.): Tactical UAVs. https://www.kratosdefense.com/systems-and-platforms/unmanned-systems/aerial/tactical-uavs (9.10.2020)
Krischke, W. (2018): Sprachwissenschaft: Altbewährtes frischgemacht. Digital Humanities (1/6). Frankfurter Allgemeine, 9.5.2018, https://www.faz.net/aktuell/karriere-hochschule/digital-humanities-eine-bilanz-1-6-sprachwissenschaft-15579104.html (9.10.2020)
L3Harris ASV (2018): First images of the Thales Mine Warfare USV. https://www.asvglobal.com/brest-first-images-of-the-thales-mine-warfare-usv/ (9.10.2020)
Launchbury, J. (o. J.): A DARPA Perspective on Artificial Intelligence. DARPA/I2O, https://www.darpa.mil/attachments/AIFull.pdf (1.9.2020)
Lei, Z. (2016): Nation's next generation of missiles to be highly flexible. China Daily, 19.8.2016, http://www.chinadaily.com.cn/china/2016-08/19/content_26530461.htm (7.8.2020)
Leveringhaus, A. (2016): Ethics and autonomous weapons. Palgrave pivot. London
Lewis, D.A.; Blum, G.; Modirzadeh, N.K. (2016): War-Algorithm Accountability. http://arxiv.org/pdf/1609.04667v1 (7.8.2020)
Lewis, J. (2015): The Case for Regulating Fully Autonomous Weapons. comment. In: The Yale Law Journal 124, S. 1309–1325
Lin, J.; Singer, P.W. (2014): China's New Military Robots Pack More Robots Inside (Starcraft-Style). https://www.popsci.com/blog-network/eastern-arsenal/chinas-new-military-robots-pack-more-robots-inside-starcraft-style (7.8.2020)
Lin, J.; Singer, P.W. (2017): Meet China's Sharp Sword, a stealth drone that can likely carry 2 tons of bombs. Popular Science, 18.1.2017, https://www.popsci.com/china-sharp-sword-lijian-stealth-drone (7.8.2020)
Linn, A. (2018): Microsoft creates AI that can read a document and answer questions about it as well as a person. Microsoft, 15.1.2018, https://blogs.microsoft.com/ai/microsoft-creates-ai-can-read-document-answer-questions-well-person/ (9.10.2020)
Lischka, K.; Klingel, A.; Bertelsmann Stiftung (2017): Wenn Maschinen Menschen bewerten. Internationale Fallbeispiele für Prozesse algorithmischer Entscheidungsfindung – Arbeitspapier –, Bertelsmann Stiftung, http://web.archive.org/web/20180123143255if_/https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/ADM_Fallstudien.pdf (7.8.2020)
Lockheed Martin Corporation (o. J.): LRASM. Long Range Anti-Ship Missile. https://www.lockheedmartin.com/en-us/products/long-range-anti-ship-missile.html (9.10.2020)
Mallik, A. (2004): Technology and Security in the 21st Century: A Demand-side Perpective. SIPRI Research Report No. 20, Oxford
Marchant, G.E.; Allenby, B.; Arkin, R.; Barrett, E.T.; Borenstein, J.; Gaudet, L.M.; Kittrie, O.; Lin, P.; Lucas, G. R.; O'Meara, R.; Silberman, J. (2011): International

Governance of Autonomous Military Robots. In: The Columbia Science and Technology Law Review (XII), S. 272–315
Marcus, G. (2018): Deep Learning: A critical appraisal. New York University, https://arxiv.org/ftp/arxiv/papers/1801/1801.00631.pdf (7.8.2020)
Markoff, J. (2015): A Learning Advance in Artificial Intelligence Rivals Human Abilities. New York Times, 10.12.2015, https://www.nytimes.com/2015/12/11/science/an-advance-in-artificial-intelligence-rivals-human-vision-abilities.html (1.9.2020)
Markowitz, M.; Gresham, J.D. (2012): Dual-Mode Brimstone Missile Proves Itself in Combat. Defense Media Network, 26.4.2012, https://www.defensemedianetwork.com/stories/dual-mode-brimstone-missile-proves-itself-in-combat/ (7.8.2020)
Masirske, H.-A. (2009): Auch Roboter der Bundeswehr sollen schießen. Heise online, 12.2.2009, https://www.heise.de/tp/features/Auch-Roboter-der-Bundeswehr-sollen-schiessen-3505402.html (7.8.2020)
Max (2016): Luftwaffe führt Brimstone für Eurofighter ein, 15.11.2016, Hartpunkt.de, https://www.hartpunkt.de/luftwaffe-fuehrt-brimstone-fuer-eurofighter-ein/ (9.10.2020)
McCaney, K. (2015): DARPA wants to plumb the depths of an underwater Internet. Defense Systems, 22.4.2015, https://defensesystems.com/articles/2015/04/22/darpa-underwater-internet-communications.aspx (7.8.2020)
McCaney, K. (2016): Boeing's new autonomous UUV can run for months at a time. Defense Systems, 14.3.2016, https://defensesystems.com/articles/2016/03/14/boeing-echo-voyager-uuv.aspx (7.8.2020)
McClelland, J. (2003): The review of weapons in accordance with Article 36 of Additional Protocol I. In: Int. rev. Red Cross 85(850), S. 397–415
MDBA (2018): Brimstone. Precision Surface Attack Weapon. Data Sheet. https://www.mbda-systems.com/?action=force-download-attachment&attachment_id=16010 (7.8.2020)
Meier, C.J. (2018): IBMs virtueller Arzt macht Fehler. Neue Zürcher Zeitung, 9.8.2018, https://www.nzz.ch/wissenschaft/ibms-virtueller-arzt-watson-for-oncology-macht-fehler-ld.1410111 (1.9.2020)
Meier, O. (2019): Rüstungskontrolle jenseits des INF-Vertrags: Ansätze zur Kontrolle von Mittelstreckenraketen nach dem Ende des Abkommens. Stiftung Wissenschaft und Politik, SWP-Aktuell 20, Berlin
Melzer, N. (2009): Interpretive Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law. https://www.icrc.org/eng/assets/files/other/icrc-002-0990.pdf (7.8.2020)
Meteor Aerospace Ltd. (o. J.): RAMBOW Unmanned Ground Vehicle (UGV). https://e07a06c2-2562-4ebb-8514-35b96f794766.filesusr.com/ugd/9c6c4c_f56e383eb6ed47f281f7f4b3bcc46bf5.pdf (9.10.2020)
Michaels, J. (2013): Rand Paul Filibustering Brennan Nomination to Lead CIA. USA TODAY, 7.3.2013, https://www.usatoday.com/story/news/politics/2013/03/06/brennan-nomination-nears-senate-vote/1967709/ (7.8.2020)
Military Factory (o. J.a): Unmanned Combat Aerial Vehicles (UCAVs). https://www.militaryfactory.com/aircraft/unmanned-combat-air-vehicle-ucav.asp (9.10.2020)
Military Factory (o. J.b): Kalashnikov BAS-01G BM Soratnik Unmanned Combat Ground Vehicle (UCGV). https://www.militaryfactory.com/armor/detail.asp?armor_id=1035 (9.10.2020)

Mindell, D. A. (2015a): Our robots, ourselves. Robotics and the myths of autonomy. New York
Mindell, D.A. (2015b): Driverless Cars and the Myths of Autonomy. Huffington Post, 14.10.2015, Update 6.12.2017, https://www.huffpost.com/entry/driverless-cars-and-the-myths-of-autonomy_b_8287230 (1.9.2020)
Ministère de la Défense (2013): The French White Paper on defence and national security. http://www.defense.gouv.fr/english/content/download/206186/2393586/file/White%20paper%20on%20defense%20%202013.pdf (1.9.2020)
Ministère de la Défense; DGA (Délégué général pour l'armement) (2013): Document de presentation de l'orientation de la S&T Période 2014-2019. Bagneux
Ministerie van Defensie (2016): Strategische Kennis & Innovatie Agenda 2016-2020. Vóórblijven in een onveiliger Wereld. Ministerie van Defensie. Den Hag, https://www.defensie.nl/binaries/defensie/documenten/rapporten/2016/11/01/strategische-kennis--en-innovatieagenda-2016/SKIA+2016-2020.pdf (21.8.2018)
Misselhorn, C. (2018): Maschinenethik und »Artificial Morality«: Können und sollen Maschinen moralisch handeln? In: Aus Politik und Zeitgeschichte (6–8), S. 29–33
Missile Technology Control Regime (2017): Equipment, Software and Technology Annex. Nr. MTCR/TEM/2017/Annex, http://mtcr.info/wordpress/wp-content/uploads/2017/10/MTCR-TEM-Technical_Annex_2017-10-19-corr.pdf (7.8.2020)
Mnih, V.; Kavukcuoglu, K.; Silver, D.; Rusu, A.A.; Veness, J.; Bellemare, M.G.; Graves, A.; Riedmiller, M.; Fidjeland, A.K.; Ostrovski, G.; Petersen, S. et al. (2015): Human-level control through deep reinforcement learning. In: Nature 518, S. 529–533
MOD (Ministry of Defence) (2011): RAF conducts precision strikes over Libya. https://www.gov.uk/government/news/raf-conducts-precision-strikes-over-libya (1.9.2020)
MOD (2013): UK Air and Space Doctrine. Joint Doctrine Publication Nr. JDP 0-30. http://www.defencesynergia.co.uk/wp-content/uploads/2015/05/jdp_0_30_uk_air_and_space_doctrine.pdf (7.8.2020)
MOD (2015): Future Operating Environment 2035. Strategic Trends Programme: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/646821/20151203-FOE_35_final_v29_web.pdf (7.8.2020)
MOD (2017a): Autonomy on the front line: supplying Armed Forces on the battlefield. Ministry of Defence, Defence Science and Technology Laboratory, Defence and Security Accelerator, Baldwin, H., https://www.gov.uk/government/news/autonomy-on-the-front-line-supplying-armed-forces-on-the-battlefield (7.8.2020)
MOD (2017b): Unmanned Aircraft Systems. Joint Doctrine Publication Nr. 0-30.2. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/640299/20170706_JDP_0-30.2_final_CM_web.pdf (7.8.2020)
MOD (2018): Human-Machine Teaming. Joint Concept Note 1/18, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/709359/20180517-concepts_uk_human_machine_teaming_jcn_1_18.pdf (18.9.2018)
Moravčík, M.; Schmid, M.; Burch, N.; Lisý, V.; Morrill, D.; Bard, N.; Davis, T.; Waugh, K.; Johanson, M.; Bowling, M. (2017): DeepStack: Expert-level artificial intelligence in heads-up no-limit poker. In: Science 356(6337), S. 508–513
Müller, V.C. (2016): Autonomous Killer Robots Are Probably Good News. In: Di Nucci, E.; Santoni de Sio, F. (Hg.): Drones and responsibility. Legal, philosophical, and sociotechnical perspectives on the use of remotely controlled weapons. London/New York, S. 67–81

Munich Security Conference (2019): Munich Security Report 2019. The Great Puzzle: Who Will Pick Up the Pieces? München, http://www.eventanizer.com/MSR/MSC2019/ (7.8.2020)
Najberg, A. (2018): Alibaba AI Model Tops Humans in Reading Comprehension. Alizila, 15.1.2018, https://www.alizila.com/alibaba-ai-model-tops-humans-in-reading-comprehension/ (9.10.2020)
Nasu, H.; McLaughlin, R. (2014): New Technologies and the Law of Armed Conflict. Den Haag
Naval Drones (2016): Unmanned Carrier Launched Surveillance and Strike (UCLASS) Program. http://www.navaldrones.com/UCLASS.html (9.10.2020)
Naval Technology (o. J.a): Fire Scout VTUAV. https://www.naval-technology.com/projects/fire-scout-vtuav/ (9.10.2020)
Naval Technology (o. J.b): Long Range Anti-Ship Missile (LRASM). https://www.naval-technology.com/projects/long-range-anti-ship-missile/ (9.10.2020)
NAVALTODAY (2017): US Navy establishes first unmanned undersea vehicle squadron. 27.9.2017, https://www.navaltoday.com/2017/09/27/us-navy-establishes-first-unmanned-undersea-vehicle-squadron/ (9.10.2020)
Navy Recognition (2018): Russia Started Sea Trials of Klavesin-2 UUV in Crimea. Navy Recognition, 18.5.2018, http://www.navyrecognition.com/index.php/focus-analysis/naval-technology/6234-russia-started-sea-trials-of-klavesin-2-uuv-in-crimea.html (9.10.2020)
Neuhäuser, C. (2014): Roboter und moralische Verantwortung. In: Hilgendorf, E. (Hg.): Robotik im Kontext von Recht und Moral. Baden-Baden, S. 269–286
Neuneck, G. (2014): High-Tech im Krieg der Zukunft: Neue Technologien als Herausforderung für die Innere Führung. In: Hartmann, U.; von Rosen, C. (Hg.): Drohnen, Roboter und Cyborgs: der Soldat im Angesicht neuer Militärtechnologien. Berlin, S. 60–73
Neuneck, G. (2017): Wie weiter nach New START? Aktuelle Probleme der Rüstungsbegrenzung. In: FriedensForum (5), S. 32–34
Neuneck, G.; Mutz, R. (Hg.) (2000): Vorbeugende Rüstungskontrolle. Ziele und Aufgaben unter besonderer Berücksichtigung verfahrensmäßiger und institutioneller Umsetzung im Rahmen internationaler Rüstungsregime. Demokratie, Sicherheit, Frieden 130, Baden-Baden
New America (o. J.a): The Future of Drone Warfare: The Rise of Maritime Drones. https://www.newamerica.org/in-depth/world-of-drones/7-future-drone-warfare-rise-maritime-drones/ (9.10.2020)
New America (o. J.b): Who has what: countries with armed drones. https://www.newamerica.org/international-security/reports/world-drones/who-has-what-countries-with-armed-drones/ (9.10.2020)
New America (o. J.c): Who has what: countries that have conducted drone strikes. https://www.newamerica.org/in-depth/world-of-drones/2-who-has-what-countries-drones-used-combat/ (9.10.2020)
Nida-Rümelin, J.; Schulenburg, J.; Rath, B.; (2012): Risikoethik. Berlin
NIST (National Institute of Standards and Technology) (2007): Autonomy Levels for Unmanned Systems (ALFUS) Framework. Volume II: Framework Models. Version 1.0. Special Publication Nr. 1011-II-1.0, http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=823618 (7.8.2020)

NIST (2008): Autonomy Levels for Unmanned Systems (ALFUS) Framework. Volume I: Terminology. Version 2.0. Special Publication Nr. 1011-I-2.0, https://www.nist.gov/system/files/documents/el/isd/ks/NISTSP_1011-I-2-0.pdf (7.8.2020)
Noorman, M.; Johnson, D.G. (2014): Negotiating autonomy and responsibility in military robots. In: Ethics Inf Technol 16(1), S. 51–62
Northrop Grumman Systems Corporation (2015): X-47B UCAS. Unmanned Combat Air System. San Diego, https://www.northropgrumman.com/wp-content/uploads/UCAS-D_Data_Sheet.pdf (9.10.2020)
Northrop Grumman (o. J.): Electronic Warfare. https://www.northropgrumman.com/what-we-do/sea/electronic-warfare/ (9.10.2020)
OCCAR (Organisation for Joint Armament Co-operation) (o. J.) MALE RPAS – Medium Altitude Long Endurance Remotely Piloted Aircraft System. Bonn
OECD (o. J.): Emerging technologies. www.oecd.org/sti/emerging-tech/ (9.10.2020)
ONR (Office of Naval Research) (o. J.a): Science of Autonomy. https://www.onr.navy.mil/en/Science-Technology/Departments/Code-35/All-Programs/aerospace-science-research-351/science-of-autonomy (9.10.2020)
ONR (o. J.b): Computational Methods for Decision Making – Large Scale Distributed Decision-making. https://www.onr.navy.mil/en/Science-Technology/Departments/Code-31/All-Programs/311-Mathematics-Computers-Research/computational-methods-large-scale-distributed-decision-making (9.10.2020)
Opall-Rome, B. (2016): Israel Navy Readies for Third-Generation USV. Defense News, 27.7.2016, https://www.defensenews.com/naval/2016/07/27/israel-navy-readies-for-third-generation-usv/ (7.8.2020)
OPCW (Organisation for the Prohibition of Chemical Weapons) (2015): The Hague Ethical Guidelines. Den Haag, https://www.opcw.org/fileadmin/OPCW/Science_Technology/Hague_Ethical_Guidelines_Brochure.pdf (7.8.2020)
Osborn, K. (2016): Navy awards MQ-25 Stingray tanker deal. Defense Systems, 24.10.2016, https://defensesystems.com/articles/2016/10/24/stingray.aspx (7.8.2020)
OSZE (Organisation for Security and Co-operation in Europe) (2011): Wiener Dokument 2011 über vertrauens- und sicherheitsbildende Maßnahmen. https://www.osce.org/de/fsc/86599?download=true (7.8.2020)
Pamuk, H.; Shepardson, D. (2019): Trump administration unveils order to prioritize and promote AI. Reuters, 11.2.2019, https://www.reuters.com/article/us-usa-trump-artificialintelligence-idUSKCN1Q00A3 (7.8.2020)
Parkin, S. (2015): Killer robost: The soldiers that never sleeps. BBC Future, 16.7.2015, http://www.bbc.com/future/story/20150715-killer-robots-the-soldiers-that-never-sleep (7.8.2020)
Pauen, M. (2011): Autonomie. In: Kolmer, P.; Wildfeuer, A. (Hg.): Neues Handbuch philosophischer Grundbegriffe. Band 1, Freiburg/München, S. 254–264
Peitz, D. (2018): Project Maven: »Google wird einfach ersetzt«. Interview mit Paul Scharre. Zeit Online, 5.6.2018, https://www.zeit.de/digital/internet/2018-06/maven-militaerprojekt-google-ausstieg-ruestungsexperte-paul-scharre (7.8.2020)
Pellerin, C. (2017): Project Maven to Deploy Computer Algorithms to War Zone by Year's End. DOD, 21.7.2017, https://dod.defense.gov/News/Article/Article/1254719/project-maven-to-deploy-computer-algorithms-to-war-zone-by-years-end/ (7.8.2020)
Perrow, C. (1989): Normale Katastrophen. Die unvermeidbaren Risiken der Großtechnik. Reihe Campus 1028, Frankfurt a.M.

Petermann, T.; Socher, M.; Wennrich, C. (1997): Präventive Rüstungskontrolle bei neuen Technologien. Utopie oder Notwendigkeit? Studien des Büros für Technikfolgen-Abschätzung beim Deutschen Bundestag 3, Berlin

Pettersson, T.; Eck, K. (2018): Organized violence, 1989–2017. In: Journal of Peace Research 55(4), S. 535–547

Pocock, C. (2018): Airbus and Dassault Launch a New FCAS – without BAE. AINonline, 25.4.2018, https://www.ainonline.com/aviation-news/defense/2018-04-25/airbus-and-dassault-launch-new-fcas-without-bae (7.8.2020)

Pomerleau, M. (2016): DOD plans to invest $600M in unmanned underwater vehicles. Defense Systems, 4.2.2016, https://defensesystems.com/articles/2016/02/04/dod-navy-uuv-investments.aspx (7.8.2020)

Pomerleau, M. (2018): How DoD is getting serious about artificial intelligence. Dronewars.net, 19.12.2018, https://www.c4isrnet.com/c2-comms/2018/12/19/how-dod-is-getting-serious-about-artificial-intelligence/ (9.10.2020)

Pontin, J. (2018): Greedy, brittle, opaque, and shallow: The downsides to Deep Learning. We've been promised a revolution in how and why nearly everything happens. But the limits of modern artificial intelligence are closer than we think. WIRED, 2.2.2018, https://www.wired.com/story/greedy-brittle-opaque-and-shallow-the-downsides-to-deep-learning/ (7.8.2020)

POST (Parliamentary Office of Science and Technology) (2015): Automation in Military Operations. Houses of Parliament, POSTnote Nr. 511, London, http://researchbriefings.files.parliament.uk/documents/POST-PN-0511/POST-PN-0511.pdf (7.8.2020)

Qinetiq North America (2018): MAARS. Modular Advanced Armed Robotic System. https://qinetiq-na.com/products/unmanned-systems/maars/ (7.8.2020)

Rabinoff, J. (2010): Machine gun-toting robots deployed on DMZ. Stars and Stripes, 12.7.2010, https://www.stripes.com/news/pacific/korea/machine-gun-toting-robots-deployed-on-dmz-1.110809 (7.8.2020)

RAF (Royal Air Force) (2003): Royal Air Force Aircraft & Weapons. https://www.raf.mod.uk/what-we-do/centre-for-air-and-space-power-studies/documents1/royal-air-force-aircraft-weapons-fourth-edition-revised/ (7.8.2020)

RAFAEL (Rafael Advanced Defense Systems Ltd.) (o. J.a): IRON DOME™ Family. https://www.rafael.co.il/worlds/air-missile-defense/short-range-air-missile-defense/ (9.10.2020)

RAFAEL (o. J.b): PROTECTOR™ USV. https://www.rafael.co.il/worlds/naval/usvs/ (9.10.2020)

Ray, J.; Atha, K.; Francis, E.; Dependahl, C.; Mulvenon, J.; Alderman, D.; Ragland-Luce, L.A. (2016): China's Industrial and Military Robotics Development. Research Report Prepared on Behalf of the U.S.-China Economic and Security Review. Vienna, https://www.uscc.gov/sites/default/files/Research/DGI_China%27s%20Industrial%20and%20Military%20Robotics%20Development.pdf (7.8.2020)

Raytheon Missiles & Defense (o. J.a): Iron Dome System and SkyHunter Missile. https://www.raytheon.com/capabilities/products/irondome (9.10.2020)

Raytheon Missiles & Defense (o. J.b): Phalanx Weapon System. https://www.raytheonmissilesanddefense.com/capabilities/products/phalanx-close-in-weapon-system (9.10.2020)

Raytheon Technologies (o. J.): MK 54 lightweight torpedo. https://www.raytheon.com/capabilities/products/mk54 (9.10.2020)

Rees, M. (2013): QinetiQ Opens UK's First Maritime Autonomy Centre. Unmanned Systems Technology, 13.9.2013, https://www.unmannedsystemstechnology.com/2013/09/qinetiq-opens-uks-first-maritime-autonomy-centre/ (7.8.2020)

Reilly, M.B. (2016): Beyond video games: New artificial intelligence beats tactical experts in combat simulation. University of Cincinnati, 27.6.2016, https://magazine.uc.edu/editors_picks/recent_features/alpha.html (7.8.2020)

Reuters (2017): Connecticut Could Be First State to Allow Armed Police Drones. Newsweek, 31.3.2017, http://www.newsweek.com/connecticut-drones-police-police-drones-armed-drones-577648 (7.8.2020)

Rheinmetall Defence (o. J.): Flugabwehrsysteme. https://www.rheinmetall-defence.com/de/rheinmetall_defence/systems_and_products/air_defence_systems/index.php (9.10.2020)

Rheinmetall Group (2018): Rheinmetall launches Mission Master Cargo Unmanned Ground Vehicle in time for Eurosatory 2018. Pressemitteilung, 11.6.2018, https://www.rheinmetall-defence.com/media/editor_media/rm_defence/publicrelations/pressemitteilungen/2018/2018_06_11_rheinmetall_eurosatory/englisch_1/2018-06-11_Rheinmetall_Eurosatory_MM_UGV_Cargo_en.pdf (9.10.2020)

Richter, W. (2013): Rüstungskontrolle für Kampfdrohnen. SWP-Aktuell Nr. 29, Berlin, https://www.swp-berlin.org/fileadmin/contents/products/aktuell/2013A29_rrw.pdf (7.8.2020)

Riecke, T. (2018): »In einigen Bereichen hat der Mensch bereits die Kontrolle verloren.« Handelsblatt, 7.6.2018, https://www.handelsblatt.com/technik/thespark/physiker-und-philosoph-armin-grunwald-in-einigen-bereichen-hat-der-mensch-bereits-die-kontrolle-verloren/22656954.html (9.10.2020)

Riley, T. (2017): Artificial intelligence goes deep to beat humans at poker. In: Science online, doi: 10.1126/science.aal0863

Robbins, M. (2016): Has a rampaging AI algorithm really killed thousands in Pakistan? A killer machine-learning algorithm guiding the U.S. drone program has killed thousands of innocent people according to some reports. What's the truth? The Guardian, 18.2.2016, https://www.theguardian.com/science/the-lay-scientist/2016/feb/18/has-a-rampaging-ai-algorithm-really-killed-thousands-in-pakistan (7.8.2020)

Roblin, S. (2018): LRASM: The Navy's Game Changer Missile Russia and China Should Fear? The National Interest, 21.4.2018, https://nationalinterest.org/blog/the-buzz/lrasm-the-navys-game-changer-missile-russia-china-should-25490 (7.8.2020)

Roff, H. (2015): Autonomous or »Semi« Autonomous Weapons? A Distinction Without Difference. Huffington Post, 16.1.2015, Updated 18.3.2015, https://www.huffingtonpost.com/heather-roff/autonomous-or-semi-autono_b_6487268.html?guccounter=1 (7.8.2020)

Rogoway, T. (2016): The Alarming Case of the USAF's Mysteriously Missing Unmanned Combat Air Vehicles. The USAF has them but isn't telling us they do, or they don't. Either way we are in trouble. Here's why. The Drive, 9.6.2016, http://www.thedrive.com/the-war-zone/3889/the-alarming-case-of-the-usafs-mysteriously-missing-unmanned-combat-air-vehicles (7.8.2020)

Rosen Jacobson, B. (2017): Lethal Autonomous Weapons Systems: Mapping the GGE debate. DiploFoundation Policy Papers and Briefs Nr. 8, Genf, https://www.diplomacy.edu/sites/default/files/Policy_papers_briefs_08_BRJ.pdf (7.8.2020)

Rosen, S.P. (1991): Winning the Next War. Innovation and the Modern Military. Ithaca
Rosenberg, Z. (2013): RAC MiG to design Skat-based unmanned combat air vehicle. FlightGlobal, 3.6.2013, https://www.flightglobal.com/news/articles/rac-mig-to-design-skat-based-unmanned-combat-air-vehicle-386609/ (7.8.2020)
Rötzer, F. (2016): Russischer Kampfroboterpanzer soll bald von Armee eingesetzt werden. Heise online, 30.3.2016, https://www.heise.de/tp/features/Russischer-Kampfroboterpanzer-soll-bald-von-Armee-eingesetzt-werden-3379287.html (7.8.2020)
Royakkers, L.; van Est, R. (2015): Just Ordinary Robots: Automation from Love to War. Cleveland
Royal Navy (2016): Royal Navy tests unmanned fleet of the future. https://www.royalnavy.mod.uk/news-and-latest-activity/news/2016/october/14/161014-royal-navy-tests-unmanned-fleet-of-the-future (7.8.2020)
Royal Society (2017): Machine learning. The power and promise of computers that learn by example. London, https://royalsociety.org/~/media/policy/projects/machine-learning/publications/machine-learning-report.pdf (7.8.2020)
RT (2015): Russia »completely ending« activities under Conventional Armed Forces in Europe treaty. https://on.rt.com/7tju9e (9.10.2020)
Sadot, U. (2016): Proliferated Drones. A Perspective on Israel. http://drones.cnas.org/wp-content/uploads/2016/05/A-Perspective-on-Israel-Proliferated-Drones.pdf (7.8.2020)
Sadowski, R.W. (2016): Enabling MUM-T within Army Formations. Robotics Community of Practice. https://www.darpa.mil/attachments/DARPA_MUMT_Updates.pdf (7.8.2020)
Şahin, E.; Spears, W.M. (2005): Swarm robotics. Revised selected papers. Lecture notes in computer science State-of-the-art survey 3342, Berlin
Scharre, P. (2014a): Robotics on the Battlefield Part I. Range, Persistence and Daring. 20YY Series, https://s3.amazonaws.com/files.cnas.org/documents/CNAS_RoboticsOnTheBattlefield_Scharre.pdf (7.8.2020)
Scharre, P.(2014b): Robotics on the Battlefield Part II. The Coming Swarm. 20YY Series, https://s3.amazonaws.com/files.cnas.org/documents/CNAS_TheComingSwarm_Scharre.pdf (7.8.2020)
Scharre, P. (2017): A security perspective: Security concerns and possible arms control approaches. In: UNODA (Hg.): Perspectives on lethal autonomous weapon systems. New York, S. 19–33
Scharre, P. (2018): Army of none: autonomous weapons and the future of war. New York/London
Schmitt, M.N. (2012): Essays on Law and War at the Fault Lines. Den Haag
Scholz, K.-A. (2020): Warum Donald Trump Landminen wieder erlaubt. Deutsche Welle, 4.2.2020, https://www.dw.com/de/warum-donald-trump-landminen-wieder-erlaubt/a-52253518 (9.10.2020)
Schörnig, N. (2014): Automatisierte Kriegsführung – Wie viel Entscheidungsraum bleibt dem Menschen? In: Aus Politik und Zeitgeschichte 35–37, S. 27–34
Schörnig, N. (2017): Preserve past achievements! Why drones should stay within the missile technology control regime (for the time being). PRIF report no. 149, Frankfurt a.M.
Sculley, D.; Holt, G.; Golovin, D.; Davydov, E.; Phillips, T.; Ebner, D.; Chaudhary, V.; Young, M.; Crespo, J.-F.; Dennison, D. (2015): Hidden Technical Debt in Machine

Learning Systems. In: Cortes, C.; Lawrence, N.D.; Lee, D.D.; Sugiyama, M.; Garnett, R. (Hg.): Advances in Neural Information Processing Systems 28, S. 2503–2511
Sharkey, N. (2012a): Killing made easy: from joysticks to politics. In: Lin, P.; Abney, K.; Bekey, G.: Robot ethics: the ethical and social implications of robotics. Cambridge/London, S. 111–128
Sharkey, N. (2012b): The evitability of autonomous robot warfare. In: Int. rev. Red Cross 94(886), S. 787–799
Sharkey, N. (2016): Staying in the loop: human supervisory control of weapons. In: Bhuta, N.; Beck, S.; Geiß, R.; Liu, H.-Y.; Kreß, C. (Hg.): Autonomous weapons systems. Law, ethics, policy. Cambridge, S. 23–38
Sharkey, N. (2018): UK and Definitions of Autonomous Weapons Systems. Written evidence (AIC0248). House of Lords Select Committee on Artificial Intelligence, London, http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/artificial-intelligence-committee/artificial-intelligence/written/78207.html (7.8.2020)
Sharot, T. (2014): Das optimistische Gehirn. Warum wir nicht anders können, als positiv zu denken. Berlin
Siciliano, B.; Khatib, O.; Groen, F.; Buehler, M.; Iagnemma, K.; Singh, S. (2009): The DARPA Urban Challenge. Autonomous Vehicles in City Traffic. Springer Tracts in Advanced Robotics 56, Berlin/Heidelberg
Silver, D.; Huang, A.; Maddison, C.; Guez, A.; Sifre, L.; van den Driessche, G.; Schrittwieser, J.; Antonoglou, I.; Panneershelvam, V.; Lanctot, M.; Dieleman, S., Grewe, D. et al. (2016): Mastering the game of Go with deep neural networks and tree search. In: Nature 529(7587), S. 484–489
Silver, D.; Hubert, T.; Schrittwieser, J.; Antonoglou, I.; Lai, M.; Guez, A.; Lanctot, M.; Sifre, L.; Kumaran, D.; Graepel, T.; Lillicrap, T.; Simonyan, K.; Hassabis, D. (2017): Mastering Chess and Shogi by Self-Play with a General Reinforcement Learning Algorithm. http://arxiv.org/pdf/1712.01815v1 (7.8.2020)
SIPRI (Stockholm International Peace Research Institute) (2019): Military expenditure by country. Stockholm, https://www.sipri.org/sites/default/files/Data%20for%20all%20countries%20from%201988%E2%80%932019%20in%20constant%20%282018%29%20USD.pdf (31.8.2020)
Smalley, D. (2016): Autonomous Swarmboats: New Missions, Safe Harbors. Office of Naval Research, 14.12.2016, https://www.onr.navy.mil/en/Media-Center/Press-Releases/2016/Autonomous-Swarmboats.aspx (31.8.2020)
Smith, D. (2019): Trump withdraws from UN arms treaty as NRA crowd cheers in delight. The Guardian, 26.4.2019, https://www.theguardian.com/us-news/2019/apr/26/trump-nra-united-nations-arms-treaty-gun-control (9.10.2020)
Smith, M. (2017): Statement regarding defeat of bill to allow police to weaponize drones. ACLU of Connecticut, 1.5.2017, https://www.acluct.org/en/press-release/statement-regarding-defeat-of-bill-to-allow-police-to-weaponize-drones (9.10.2020)
Sparrow, R. (2007): Killer Robots. In: Journal of Applied Philosophy 24(1), S. 62–77
Sparrow, R. (2016): Robots and Respect: Assessing the Case Against Autonomous Weapon Systems. In: Ethics int. aff. 30(01), S. 93–116
Spektrum (1999): Asilomar-Konferenz. https://www.spektrum.de/lexikon/biologie/asilomar-konferenz/5423 (9.10.2020)
Spiegel Online (2013): X-47B: Kampfdrohne glückt Landung auf Flugzeugträger. http://www.spiegel.de/wissenschaft/technik/x-47b-drohne-glueckt-landung-auf-flugzeugtraeger-a-910546.html (31.8.2020)

Steinke, R. (2018): Der Internationale Strafgerichtshof. Bundeszentrale für politische Bildung, 30.7.2018, www.bpb.de/internationales/weltweit/innerstaatliche-konflikte/169554/der-internationale-strafgerichtshof (9.10.2020)
Stevenson, B. (2016): New $2.2 billion Anglo-French FCAS phase announced. FlightGlobal, 8.3.2016, https://www.flightglobal.com/news/articles/new-22-billion-anglo-french-fcas-phase-announced-422866/ (31.8.2020)
Stimson (2015): UAV Export Controls and Regulatory Challenges. Working Group Report. Washington D.C., https://www.stimson.org/sites/default/files/file-attachments/ECRC%20Working%20Group%20Report.pdf (31.8.2020)
Stoecker, R. (2010): Die philosophischen Schwierigkeiten mit der Menschenwürde – und wie sie sich vielleicht auflösen lassen. In: ZiF-Mitteilungen 1, S. 19–30
Strawser, B.J. (2010): Moral Predators: The Duty to Employ Uninhabited Aerial Vehicles. In: Journal of Military Ethics 9(4), S. 342–368
Su, J.; Vargas, D.V.; Kouichi, S. (2017): One pixel attack for fooling deep neural networks. http://arxiv.org/pdf/1710.08864v2 (31.8.2020)
Süddeutsche Zeitung (2014): Europäische Drohnen entwickeln. Interview mit Ursula von der Leyen. Süddeutsche Zeitung, 2.7.2014, https://www.bundesregierung.de/breg-de/bundeskanzlerin/europaeische-drohnen-entwickeln-620670 (1.9.2020)
Swaine, J. (2013): Barack Obama »has authority to use drone strikes to kill Americans on US soil«. The Telegraph, 6.3.2013, https://www.telegraph.co.uk/news/worldnews/barackobama/9913615/Barack-Obama-has-authority-to-use-drone-strikes-to-kill-Americans-on-US-soil.html
Szegedy, C.; Zaremba, W.; Sutskever, I.; Bruna, J.; Erhan, D.; Goodfellow, I.; Fergus, R. (2014): Intriguing properties of neural networks. http://arxiv.org/pdf/1312.6199v4 (31.8.2020)
Szondy, D. (2018): DARPA hands autonomous sub-hunter prototype over to the US Navy. New Atlas, 5.2.2018, https://newatlas.com/darpa-actuv-us-navy/53247/ (1.9.2020)
TAB (Büro für Technikfolgen-Abschätzung beim Deutschen) (2003): Militärische Nutzung des Weltraums und Möglichkeiten der Rüstungskontrolle im Weltraum (Autoren: Petermann, T.; Coenen, C.; Grünwald, R.). Sachstandsbericht. Arbeitsbericht Nr. 85, Berlin
TAB (2011): Stand und Perspektiven der militärischen Nutzung unbemannter Systeme (Autoren: Petermann, T.; Grünwald, R.). Endbericht zum TA-Projekt. Arbeitsbericht Nr. 144, Berlin
TAB (2016): Technologien und Visionen der Mensch-Maschine-Entgrenzung. Sachstandsbericht zum TA-Projekt »Mensch-Maschine-Entgrenzungen: zwischen künstlicher Intelligenz und Human Enhancement« (Autoren: Kehl, C.; Coenen, C.). TAB-Arbeitsbericht Nr. 167, Berlin
Tagesschau (2019): Boeing findet weiteres Softwareproblem. 5.4.2019, https://www.tagesschau.de/wirtschaft/boeing-software-101.html (9.10.2020)
TARDEC (2017): TARDEC 30-Year Strategy. https://api.army.mil/e2/c/downloads/489179.pdf (31.8.2020)
The Economist (2019): Humans struggle to cope when automation fails. 14.3.2019, https://www.economist.com/business/2019/03/14/humans-struggle-to-cope-when-automation-fails (13.7.2020)
The Maritime Executive (2019): Littoral Combat Ship's MCM Package Moves Forward. 28.1.2019, https://www.maritime-executive.com/article/littoral-combat-ship-s-mcm-package-moves-forwardBaker, B. (2019): Orca XLUUV: Boeing's

whale of an unmanned sub. NavalTechnology, 1.7.2019, https://www.naval-technology.com/features/boeing-orca-xluuv-unmanned-submarine/ (9.10.2020)
Thielmann, G.; Zagorski, A. (2017): INF Treaty Compliance: A Challenge and an Opportunity. Deep Cuts Working Paper No. 9, http://www.deepcuts.org/images/PDF/DeepCuts_WP9_ThielmannZagorski.pdf (31.8.2020)
Think Defence (o. J.): Brimstone. https://www.thinkdefence.co.uk/uk-complex-weapons/brimstone/ (9.10.2020)
Thomas, W. (2017): Trump Budget Cuts Defense S&T by 5.8 % While Funding Third Offset Priorities. Science Policy News from AIP, 1.6.2017, https://www.aip.org/fyi/2017/trump-budget-cuts-defense-st-58-while-funding-third-offset-priorities (31.8.2020)
Thompson, M. (2013): Costly Flight Hours. TIME USA, LLC., 2.4.2013, http://nation.time.com/2013/04/02/costly-flight-hours/ (31.8.2020)
Tolk, A. (2015): Merging Two Worlds: Agent-based Simulation Methods for Autonomous Systems. In: Williams, A.P.; Scharre, P. (Hg.): Autonomous systems. Issues for defence policymakers. Norfolk, S. 291–317
Tran, P. (2016): »Neuron« Combat Drone Completes First Sea Trials. Defense News, 8.7.2016, https://www.defensenews.com/home/2016/07/08/neuron-combat-drone-completes-first-sea-trials/ (31.8.2020)
Tran, P. (2018): The French Army could have its first unmanned vehicle by 2025. Defense News, 12.6.2018, https://www.defensenews.com/digital-show-dailies/eurosatory/2018/06/12/the-french-army-could-have-its-first-unmanned-vehicle-by-2025/ (31.8.2020)
Tucker, P. (2015): Pentagon Sets Up a Silicon Valley Outpost. Defense One, 23.4.2015, https://www.defenseone.com/technology/2015/04/pentagon-sets-silicon-valley-outpost/110845/ (31.8.2020)
Tucker, P. (2016): The US Navy's Autonomous Swarm Boats Can Now Decide What to Attack. Defense One, 14.12.2016, https://www.defenseone.com/technology/2016/12/navys-autonomous-swarm-boats-can-now-decide-what-attack/133896/ (31.8.2020)
Tucker, P. (2017): The Future the US Military is Constructing: a Giant, Armed Nervous System. Defense One, 26.9.2017, https://www.defenseone.com/technology/2017/09/future-us-military-constructing-giant-armed-nervous-system/141303/ (31.8.2020)
U.S. Air Force (2014): RPA Vector. Vision and Enabling Concepts 2013-2038. Washington D.C., http://www.af.mil/Portals/1/documents/news/USAFRPAVectorVisionandEnablingConcepts2013-2038.pdf (31.8.2020)
U.S. Air Force (2016): Small Unmanned Aircraft Systems (SUAS) Flight Plan: 2016-2036. Bridging the Gap Between Tactical and Strategic. http://www.af.mil/Portals/1/documents/isr/Small_UAS_Flight_Plan_2016_to_2036.pdf (31.8.2020)
U.S. Air Force; Office of the Chief Scientist (2015): Autonomous Horizons. System Autonomy in the Air Force – A Path to the Future. Volume I: Human-Autonomy Teaming. Nr. AF/ST TR 15-01, https://www.hsdl.org/?view&did=768107 (31.8.2020)
U.S. Army (2017a): Multi-Domain Battle: Evolution of Combined Arms for the 21st Century 2025-2040. Version 1.0. https://www.tradoc.army.mil/Portals/14/Documents/MDB_Evolutionfor21st%20(1).pdf (31.8.2020)

U.S. Army (2017b): The U.S. Army Robotic and Autonomous Systems Strategy. https://www.tradoc.army.mil/Portals/14/Documents/RAS_Strategy.pdf (31.8.2020)
U.S. Department of State (2018): U.S. Policy on the Export of Unmanned Aerial Systems. Fact Sheet. 19.4.18, Update 24.7.2020, https://www.state.gov/u-s-policy-on-the-export-of-unmanned-aerial-systems-2/ (31.8.2020)
U.S. Navy (2013): U.S. Navy Information Dominance Roadmap 2013-2028. https://defenseinnovationmarketplace.dtic.mil/wp-content/uploads/2018/02/Information_Dominance_Roadmap_March_2013.pdf (31.8.2020)
U.S. President (2019): Executive Order on Maintaining American Leadership in Artificial Intelligence, The White House, 11.2.2019, https://www.whitehouse.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence/ (31.8.2020)
UAS Vision (2017): Partners Agree Configuration of European MALE RPAS. https://www.uasvision.com/2017/08/03/partners-agree-configuration-of-european-male-rpas/ (9.10.2020)
UK Mission (2019a): Agenda item 5(b): Characterisation of the systems under consideration in order to promote a common understanding on concepts and characteristics relevant to the objectives and purposes of the Convention. CCW GGE. Genf, https://www.unog.ch/80256EDD006B8954/(httpAssets)/A969D779E1E5E28BC12583D3003FC0D9/$file/20190318-5(b)_Characterisation_Statement.pdf (31.8.2020)
UK Mission (2019b): Agenda item 5(d): Further consideration of the human element in the use of lethal force; aspects of human-machine interaction in the development, deployment and use of emerging technologies in the area of lethal autonomous weapons systems. CCW GGE. Genf, https://www.unog.ch/80256EDD006B8954/(httpAssets)/85A4AA89AFCFD316C12583D3003EAB3E/$file/20190318-5(d)_HMI_Statement.pdf (31.8.2020)
UK Mission (2019c): Agenda item 5(e): Possible options for addressing the humanitarian and international security challenges posed by emerging technologies in the area of lethal autonomous weapons systems in the context of the objectives and purposes of the Convention without prejudging policy outcomes and taking into account past, present and future proposal. CCW GGE. Genf, https://www.unog.ch/80256EDD006B8954/(httpAssets)/40C2167E8F162030C12583D3003F4B94/$file/20190318-5(e)_Policy_Statement.pdf (31.8.2020)
Ulgen, O. (Hg.) (2017a): Human Dignity in an Age of Autonomous Weapons: Are We in Danger of Losing an »Elementary Consideration of Humanity«? European Society of International Law (ESIL) Annual Conference, Riga, 8-10.9.2016, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2912002 (31.8.2020)
Ulgen, O. (2017b): Kantian Ethics in the Age of Artificial Intelligence and Robotics. In: Questions of International Law 43, S. 59–83
UN (United Nations) (1991): Resolutions adopted by the General Assembly at its 46th session. 46/36. General and complete disarmament. L Transparency in Armaments. https://undocs.org/pdf?symbol=en/A/RES/46/36 (31.8.2020)
UN (2013): The Arms Trade Treaty. https://unoda-web.s3-accelerate.amazonaws.com/wp-content/uploads/2013/06/English7.pdf (9.10.2020)
UN (2016a): Continuing operation of the United Nations Register of Conventional Arms and its further development. Nr. A/71/259, New York, https://documents-

dds-ny.un.org/doc/UNDOC/GEN/N16/242/39/PDF/N1624239.pdf?OpenElement (31.8.2020)
UN (2016b): Resolution adopted by the General Assembly on 5 December 2016. Nr. A/RES/71/44. Transparency in armaments. New York, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N16/420/26/PDF/N1642026.pdf?OpenElement (25.4.2018)
UN (2016c): Germany 2016. UNROCA original report. https://www.unroca.org/germany/report/2016 (9.10.2020)
UN (2016d): Singapore 2016. UNROCA original report. https://www.unroca.org/singapore/report/2016 (9.10.2020)
UN (2016e): Spain 2016. UNROCA original report. https://www.unroca.org/spain/report/2016 (9.10.2020)
UN (2016f): Switzerland 2016. UNROCA original report. https://www.unroca.org/switzerland/report/2016 (9.10.2020)
UN (o. J.a): Arms Trade. https://www.un.org/disarmament/convarms/att/ (9.10.2020)
UN (o. J.b): The Convention on Certain Conventional Weapons. https://www.unog.ch/80256EE600585943/(httpPages)/4F0DEF093B4860B4C1257180004B1B30?OpenDocument (9.10.2020)
UN (o. J.c): UN Register of Conventional Arms. https://www.un.org/disarmament/convarms/register/ (9.10.2020)
UNIDIR (United Nations Institute for Disarmament Research) (2014a): Framing Discussions on the Weaponization of Increasingly Autonomous Technologies. UNIDIR Resources Nr. 1, Genf, http://unidir.org/files/publications/pdfs/framing-discussions-on-the-weaponization-of-increasingly-autonomous-technologies-en-606.pdf (31.8.2020)
UNIDIR (2014b): The Weaponization of Increasingly Autonomous Technologies: Considering how Meanigful Control might move the discussion forward. UNIDIR Resources Nr. 2, Genf, http://unidir.org/files/publications/pdfs/considering-how-meaningful-human-control-might-move-the-discussion-forward-en-615.pdf (31.8.2020)
UNIDIR (2016): Safety, Unintentional Risk and Accidents in the Weaponization of Increasingly Autonomous Technologies. UNIDIR Resources Nr. 5, Genf, http://unidir.org/files/publications/pdfs/safety-unintentional-risk-and-accidents-en-668.pdf (31.8.2020)
UNIDIR (2017): The Weaponization of Increasingly Autonomous Technologies: Concerns, Characteristics and Definitional Approaches. a primer. UNIDIR Resources Nr. 6, Genf, http://www.unidir.org/files/publications/pdfs/the-weaponization-of-increasingly-autonomous-technologies-concerns-characteristics-and-definitional-approaches-en-689.pdf (26.1.2018)
UNIDIR (2018a): Algorithmic Bias and the Weaponization of Increasingly Autonomous Technologies. A Primer. UNIDIR Resources Nr. 9, Genf, http://www.unidir.org/files/publications/pdfs/algorithmic-bias-and-the-weaponization-of-increasingly-autonomous-technologies-en-720.pdf (31.8.2020)
UNIDIR (2018b): The Weaponization of Increasingly Autonomous Technologies: Artificial Intelligence. a primer for CCW delegates. UNIDIR Resources Nr. 8, Genf, http://www.unidir.ch/files/publications/pdfs/the-weaponization-of-increasingly-autonomous-technologies-artificial-intelligence-en-700.pdf (31.8.2020)
Villani, C. (2018): For a Meaningful Artificial Intelligence. Towards a French and European Strategy. Mission assigned by the Prime Minister Édouard Philippe.

https://www.aiforhumanity.fr/pdfs/MissionVillani_Report_ENG-VF.pdf (31.8.2020)
Voßenkuhl, W. (1983): Moralische und nicht-moralische Bedingungen verantwortlichen Handelns: Eine ethische und handlungstheoretische Analyse. In: Baumgartner, H.; Eser, A. (Hg.): Schuld und Verantwortung. Philosophische und juristische Beiträge zur Zurechenbarkeit menschlichen Handelns. Tübingen, S. 109–140
Wallach, W.; Allen, C. (2008): Moral Machines. Teaching Robots Right from Wrong. New York
Walsh, T.: (2018): Belgisches Parlament unterstützt Verbot von autonomen Waffensystemen! Killer Roboter stoppen!, 5.7.2018, https://www.killer-roboter-stoppen.de/2018/07/belgien-geht-wieder-voran-und-will-verbot-von-autonomen-waffen systemen-unterstuetzen/ (9.10.2020)
Wassenaar Arrangement (2017): List of Dual-Use Goods and Technologies and Munitions List. Nr. WA-LIST (17)1, https://www.wassenaar.org/app/uploads/2019/consolidated/2017-List-of-DU-Goods-and-Technologies-and-Munitions-List.pdf (1.9.2020)
Wassenaar Arrangement Secretariat (2019): Compendium of Best Practice Documents. Public Documents Volume III. www.wassenaar.org/best-practices/ (9.10.2020)
WD (Wissenschaftliche Dienste) (2012): Der Einsatz von Kampfdrohnen aus völkerrechtlicher Sicht. Deutscher Bundestag, WD 2 – 3000 - 118/12, Berlin
White, Y. (2015): Kratos' Third UTAP-22 Flight Exceeds Objectives, Successfully Performing All Primary and Alternate Test Points. Kratos Defense & Security Solutions, Inc., 21.12.2015, http://ir.kratosdefense.com/news-releases/news-release-details/kratos-third-utap-22-flight-exceeds-objectives-successfully (1.9.2020)
Wiegold, T. (2018): Nach dem Brexit: Britischer Anlauf für eigenes Future Combat Air System. Augen geradeaus!, 16.7.2018, https://augengeradeaus.net/2018/07/nach-dem-brexit-britischer-anlauf-fuer-eigenes-future-combat-air-system/ (1.9.2020)
Wikipedia (2002): Kernwaffe: Strategische Kernwaffen. https://de.wikipedia.org/wiki/Kernwaffe#Strategische_Kernwaffen (9.10.2020)
Wikipedia (2003a): Höhlengleichnis. https://de.wikipedia.org/wiki/Höhlengleichnis (9.10.2020)
Wikipedia (2003b): Arleigh Burke-class destroyer. https://en.wikipedia.org/w/index.php?title=Arleigh_Burke-class_destroyer&oldid=752191 (9.10.2020)
Wikipedia (2003c): g-force: Human tolerance. https://en.wikipedia.org/wiki/G-force#Human_tolerance (9.10.2020)
Wikipedia (2003d): Genfer Konventionen. https://de.wikipedia.org/wiki/Genfer_Konventionen (9.10.2020)
Wikipedia (2004): Übereinkommen über das Verbot des Einsatzes, der Lagerung, der Herstellung und der Weitergabe von Antipersonenminen und über deren Vernichtung. https://de.wikipedia.org/wiki/Übereinkommen_über_das_Verbot_des_Einsatzes,_der_Lagerung,_der_Herstellung_und_der_Weitergabe_von_Antipersonenminen_und_über_deren_Vernichtung (9.10.2020)
Wikipedia (2006a): Prompt Global Strike. https://de.wikipedia.org/wiki/Prompt_Global_Strike (9.10.2020)
Wikipedia (2006b): Iran-Air-Flug 655. https://de.wikipedia.org/wiki/Iran-Air-Flug_655 (9.10.2020)

Wikipedia (2008): Computer shogi. https://en.wikipedia.org/wiki/Computer_shogi#Game_complexity (9.10.2020)
Wikipedia (2009a): MANTIS (Flugabwehrsystem). https://de.wikipedia.org/wiki/MANTIS_(Flugabwehrsystem) (9.10.2020)
Wikipedia (2009b): OODA-Loop. https://de.wikipedia.org/wiki/OODA-Loop (9.10.2020)
Wikipedia (2010a): Watson (Künstliche Intelligenz). https://de.wikipedia.org/wiki/Watson_(Künstliche_Intelligenz) (9.10.2020)
Wikipedia (2010b): Flash Crash. https://de.wikipedia.org/wiki/Flash_Crash (9.10.2020)
Wikipedia (2016a): AlphaGo gegen Lee Sedol. https://de.wikipedia.org/wiki/AlphaGo_gegen_Lee_Sedol (9.10.2020)
Wikipedia (2016b): Sea Hunter. https://en.wikipedia.org/wiki/Sea_Hunter (9.10.2020)
Wikipedia (2017): Edge Computing. https://de.wikipedia.org/wiki/Edge_Computing (9.10.2020)
Williams, H. (2017): Unmanned and unguarded: operators and industry look to close a defence gap. In: Jane's International Defence Review 50, S. 52
Williams, K.W. (2006): Human Factors Implications of Unmanned Aircraft Accidents: Flight-Control Problems. Federal Aviation Administration Nr. DOT/FAA/AM-06/8, Oklahoma City, https://rosap.ntl.bts.gov/view/dot/18240/dot_18240_DS1.pdf? (1.9.2020)
Wilson, C. (2005): Network Centric Warfare: Background and Oversight Issues for Congress. CRS Report for Congress Nr. RL32411a, Fort Belvoir
WMDC (Weapons of Mass Destruction Commission) (2006): Weapons of Terror. Freeing the World of Nuclear, Biological and Chemical Arms. Stockholm
Wong, K. (2014): Airshow China 2014: Norinco debuts Battle Robot UGV. JANES, https://www.janes.com/article/45626/airshow-china-2014-norinco-debuts-battle-robot-ugv
Work, R. (2016): Remarks by Deputy Secretary Work on Third Offset Strategy. Rede in Brüssel am 28.4.2016, https://www.defense.gov/Newsroom/Speeches/Speech/Article/%20753482/remarks-by-deputy-secretary-work-on-third-offset-strategy/ (1.9.2020)
Work, R.; Brimley, S. (2014): 20YY Preparing for War in the Robotic Age. https://s3.amazonaws.com/files.cnas.org/documents/CNAS_20YY_WorkBrimley.pdf?mtime=20160906082222 (1.9.2020)
Wright-Patterson Air Force Base (2019): XQ-58A Valkyrie demonstrator completes inaugural flight. https://www.wpafb.af.mil/News/Article-Display/Article/1777743/xq-58a-valkyrie-demonstrator-completes-inaugural-flight/ (9.19.2020)Ackerman, S. (2016): UK to double armed drone fleet in deal with US Predator manufacturer. The Guardian, 3.12.2016, https://www.theguardian.com/world/2016/dec/03/drones-us-uk-deal-predator-reaper-protector (5.8.2020)
Xiong, W.; Droppo, J.; Huang, X.; Seide, F.; Seltzer, M.; Stolcke, A.; Yu, D.; Zweig, G. (2016): Achieving Human Parity in Conversational Speech Recognition. http://arxiv.org/pdf/1610.05256v2 (1.9.2020)
Yeni Şafak (2016): Turkey starts building automatic shooting gun towers at Syrian border. Global Construction Review, 6.7.2016, https://www.globalconstructionreview.com/news/turkey-rush-build-auto7matic-shoo7ting-tow7ers/ (7.8.2020)
Zenko, M.; Kreps, S.E. (2014): Limiting armed drone proliferation. Council special report 69, New York

11 Anhang

11.1 Abbildungen

Abb. 3.1 Täuschung eines Algorithmus zur Bilderkennung 60
Abb. 3.2 Erklärbare KI 62
Abb. 4.1 Drohne »Harop« 73
Abb. 4.2 Geschütz des Flugabwehrsystems MANTIS 79
Abb. 4.3 Das israelische UGV »Guardium« 81
Abb. 5.1 Anzahl benötigter Luftfahrzeuge für 24/7-Abdeckung 106
Abb. 5.2 Kampfradien bemannter und unbemannter Flugzeuge 117
Abb. 9.1 Rahmen für menschliche Kontrolle im Entwicklungs- und Nutzungszyklus einer Waffe 201

11.2 Tabellen

Tab. 2.1 Menschliche Rolle bei Zielauswahl und -bekämpfung 41
Tab. 2.2 Rolle von Mensch und AWS bei Zielauswahl und Angriffsentscheidung 42
Tab. 4.1 Staatlicher Besitz, Beschaffung und Einsatz von fortschrittlichen Kampfdrohnen 69
Tab. 5.1 Missionen, in denen operative Vorteile von AWS besonders zum Tragen kommen 111
Tab. 9.1 Übersicht der für AWS relevanten Rüstungskontrollverträge 183
Tab. 9.2 Transparenz- und vertrauensbildende Maßnahmen, Nichtverbreitung und Exportkontrolle 189
Tab. 9.3 Formulierungsvarianten zur menschlichen Kontrolle über AWS 193
Tab. 9.4 Mögliche Ansätze zur Regulierung von AWS 215

11.3 Kästen

Kasten 2.1 Der Autonomiebegriff aus philosophischer Sicht 36
Kasten 2.2 Anmerkung zum Sprachgebrauch 37
Kasten 2.3 AWS in Platos Höhle 43
Kasten 3.1 Schwache und starke KI 51
Kasten 3.2 Militärische KI-Forschung und zivilgesellschaftlicher Protest: zwei Fallbeispiele 65
Kasten 4.1 Schwärme als neue Form der Kriegsführung? 90
Kasten 5.1 Die militärische KI-Strategie der US-Regierung 120

Kasten 7.1 »Boxed autonomy« 146
Kasten 8.1 Zwei Grundmodelle ethischen Argumentierens 155
Kasten 8.2 Moralische Maschinen? Die neue Disziplin der Maschinenethik 157
Kasten 9.1 Aktuelle deutsche Position 195
Kasten 9.2 Qualität menschlicher Kontrolle aus britischer Sicht 200
Kasten 9.3 AWS und der Europäische Verteidigungsfonds 202
Kasten 9.4 Aktuelle Position des IKRK 206
Kasten 9.5 Die weitere Arbeit der CCW 210

11.4 Abkürzungen

A2/AD	anti access and area denial
A-KSE	adaptierter KSE-Vertrag
ATT	Arms Trade Treaty
AWS	autonome Waffensysteme
AWV	Außenwirtschaftsverordnung
BWÜ	Biowaffenübereinkommen
CCW	Convention on Certain Conventional Weapons
CIWS	close-in weapon system
CWÜ	Chemiewaffenübereinkommen
FuE	Forschung und Entwicklung
FCAS	future combat air system
GGE	Group of Governmental Experts
GPS	Global Positioning System
HCoC	Hague Code of Conduct against Ballistic Missile Proliferation
HVR	Humanitäres Völkerrecht
IED	improvised explosive device
IKRK	Internationales Komitee vom Roten Kreuz
INF	intermediate-range nuclear rorces
IS	Islamischer Staat
ISR	intelligence, surveillance and reconnaissance
JAIC	Joint Artificial Intelligence Center
KI	künstliche Intelligenz
KSE	Vertrag über konventionelle Streitkräfte in Europa
LAWS	lethal autonomous weapon system
LOCUST	low-cost UAV swarming technology
LRASM	long range anti-ship missile
MALE	medium altitude long endurance
MHC	meaningful human control
ML	machine learning (maschinelles Lernen)
MMW	Millimeterwellen

MTCR	missile technology control regime
MUM-T	manned-unmanned teaming
NBS	Nächstbereichschutzsystem
NATO	North Atlantic Treaty Organization
NGO	Non-Governmental Organisation/Nichtregierungsorganisation
ONR	Office of Naval Research
OPCW	Organisation for the Prohibition of Chemical Weapons
OSZE	Organisation für Sicherheit und Zusammenarbeit in Europa
RPAS	remotely piloted aircraft system
SARMO	sense and react to military objects
START	Strategic Arms Reduction Treaty
TEVV	test and evaluation, verification and validation
UAV	unmanned aerial vehicle
UCAV	unmanned combat aerial vehicle
UGV	unmanned ground vehicle
UN	United Nations
USV	unmanned surface vehicle
UUV	unmanned underwater vehicle
UWS	unbemanntes Waffensystem
VSBM	vertrauens- und sicherheitsbildende Maßnahmen
ZP	Zusatzprotokoll

BÜRO FÜR TECHNIKFOLGEN-ABSCHÄTZUNG BEIM DEUTSCHEN BUNDESTAG

Karlsruher Institut für Technologie

Neue Schönhauser Straße 10
10178 Berlin

Telefon: +49 30 28491-0
E-Mail: buero@tab-beim-bundestag.de
Web: www.tab-beim-bundestag.de
Twitter: @TABundestag