



BÜRO FÜR TECHNIKFOLGEN-ABSCHÄTZUNG  
BEIM DEUTSCHEN BUNDESTAG

Reinhard Grünwald  
Christoph Kehl

# Autonome Waffensysteme

Zusammenfassung

Oktober 2020  
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](mailto:buero@tab-beim-bundestag.de)  
Web: [www.tab-beim-bundestag.de](http://www.tab-beim-bundestag.de)

2020

Umschlagbild: [Bertrand Bouchez/unsplash.com](https://unsplash.com/photos/Bertrand-Bouchez)

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

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



---

## 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 Zielflug (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«<sup>1</sup> (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 Pendanten: 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 einer Maschinenabwehr 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 Kampffjets 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 Umriss 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 Konflikttypus, 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 schmerzhaft 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 nicht-stationierte 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, so dass sich sukzessive immer mehr Staaten dieser Vorgehensweise anschließen. Für solch ein Vorgehen bietet der Prozess bis zur Umsetzung der Ottawa-Konvention<sup>2</sup> 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<sup>3</sup> 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<sup>4</sup> (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

---

<sup>3</sup> Montreal-Protokoll über Stoffe, die zu einem Abbau der Ozonschicht führen

<sup>4</sup> 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.





**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](mailto:buero@tab-beim-bundestag.de)  
Web: [www.tab-beim-bundestag.de](http://www.tab-beim-bundestag.de)  
Twitter: @TABundestag