

Neue digitale Militärtechnologien und autonome Waffensysteme

Die Zukunft der Kriegsführung

ARBEITSKREIS INTERNATIONALE SICHERHEITSPOLITIK DER FRIEDRICH-EBERT-STIFTUNG

August 2015

- Profunde wissenschaftliche Studien zur Folgenabschätzung und Risikobewertung der neuen digitalen Militärtechnologien für Politik, Gesellschaft und die Streitkräfte sind dringend erforderlich. Bundesregierung und Bundestag sollten entsprechende Studien dringlich fördern, damit sie politisch tragfähige Strategien entwickeln können, die von der Gesellschaft akzeptiert werden.
- Die Entscheidung über das Töten von Menschen vollständig Maschinen zu überlassen, ist inakzeptabel. Im Rahmen der EU und der NATO gilt es, Einigkeit darüber herzustellen, dass die menschliche Entscheidungsautonomie bei der Nutzung digitaler militärischer Systeme stets substanziell gewahrt bleibt.
- Die durch Cyberraum, Künstliche Intelligenz und Autonomisierung getriebenen militärischen Anwendungen müssen Gegenstand einer präventiven und aktiven internationalen Rüstungsteuerung werden. Die Bundesrepublik sollte dabei eine gestaltende Rolle einnehmen und die rüstungskontrollpolitische Debatte durch zielgerichtete Initiativen voranbringen.
- Entscheidungen über Streitkräftefähigkeiten und militärische Beschaffungen unterliegen in demokratischen Staaten der parlamentarischen Kontrolle. Die Voraussetzungen für diese Kontrolle müssen durch fundierte fachliche Kompetenz der Abgeordneten gegeben sein.



١.	Technische Entwicklungsdynamik: Sachstand und Entwicklungsperspektiven	3
2.	Strategisch-politische Konsequenzen	6
3.	Schlussbemerkung	8



Die digitale Revolution beschert uns eine rasante Entwicklung qualitativ neuer Informations- und Kommunikationssysteme – Systeme, die unser Leben erleichtern, aber auch neue Risiken schaffen. Militärische Waffentechnik und militärische Planungs- und Führungsprozesse verändern sich von Grund auf. Neue Waffensysteme werden entwickelt, die absehbar zu einer Revolutionierung des Kriegsbildes führen werden, das derzeit unserer Sicherheits- und Verteidigungspolitik zugrunde liegt. Neuartige Formen automatisierter oder sogar autonomer Kriegsführung entstehen, die menschlicher Kontrolle entgleiten und demokratische politische Entscheidungsfreiheit außer Kraft setzen können.

1. Technische Entwicklungsdynamik: Sachstand und Entwicklungsperspektiven

Bei der Entwicklung autonomer Waffensysteme liegen die USA und Israel derzeit technologisch vorn und treiben die Innovation weiter voran. Das Pentagon ergriff 2014 mit der »Third Offset Strategy«¹ eine neue Rüstungsinitiative, mit der, wie bereits zweimal zuvor in den 1950er und den 1970er Jahren, die Sicherheit der USA durch technische Überlegenheit garantiert werden soll. Andere Nationen mit Hightech-Industrie wie Frankreich und Großbritannien, China und Russland, Japan und Südkorea treiben diese Technologie-Entwicklung ebenfalls voran.

Im Herbst 2014 gab der Staatssekretär für Beschaffung, Technik und Logistik im Pentagon, Frank Kendall, eine Studie über die wissenschaftlichen, rechtlichen, militärischen und politischen Probleme in Auftrag, die gelöst werden müssten, um auf allen Ebenen neue digitale Technologien einschließlich autonomer Systeme einsetzen zu können. Und auch in der NATO befassen sich mehrere Dienststellen mit der Thematik.

Eine kontroverse Diskussion über Chancen und Risiken dieser Entwicklung hat in Fachkreisen, vor allem in denen der USA, längst eingesetzt. In Deutschland wird sie derzeit eher zögerlich geführt und sollte dringend ausgeweitet werden. Dabei geht es nicht nur um die Erkenntnis, welche technologischen Möglichkeiten sich bereits in der Entwicklung befinden und welche kommen werden. Es geht vor allem um die Erörterung, wie

die neue Technologie unser Handeln und damit unsere Fähigkeit, Sicherheitspolitik zu gestalten, bestimmen und womöglich verändern kann.

Einige Beispiele für laufende Entwicklungen:

- Die Entwicklung zu einer vollständigen Vernetzung aller Lebensbereiche (»Internet der Dinge«) in einem prinzipiell unbegrenzten globalen Datenraum (Cyberspace) bietet nicht nur Chancen, sondern auch vielfältige Angriffsmöglichkeiten auf entscheidende Kommunikationsstränge mit möglicherweise nicht mehr kontrollierbaren, mithin unbeherrschbaren und verheerenden Auswirkungen auf unsere Sicherheit und auf unsere militärische Fähigkeit, Sicherheit herzustellen (u. a. Cyberattacken, Manipulation).
- Neue Produktionsarten wie 3-D-Drucken mit einer Vielzahl von Materialien eröffnen nicht nur potenziellen Gegnern und »Schurkenstaaten«, sondern auch kleinen Gruppen und Privatpersonen die Möglichkeit, Waffen zu produzieren, sie mit Hochtechnologie-Elementen auszustatten und mit diesen zu handeln beziehungsweise sie zu terroristischen Zwecken zu gebrauchen.
- Die Entwicklung von immer mehr autonomen Handlungsfunktionen in zivilen Anwendungsbereichen (z. B. das fahrerlose Auto) wird längst auch auf Waffen- und militärische Führungssysteme ausgedehnt und wirft ganz grundsätzliche Fragen nach Möglichkeiten und Grenzen menschlicher Kontrolle, also nach Verantwortlichkeit für Zerstörung und Tötung auf.
- Die Entwicklung von Software-Technologie hin zu künstlicher Intelligenz schließlich treibt Innovationen in allen Lebensbereichen noch weiter voran, auch im militärischen Bereich.

Das alles ist keine »Science Fiction« mehr, sondern Realität im Werden. In diesem Zusammenhang soll der Fokus dieses Papiers auf der Autonomisierung von militärischen Systemen liegen, ohne die Technologiefolgen für das gesamte politisch-militärische System zu vernachlässigen. Eine Reihe grundsätzlicher politischer, gesellschaftlicher, rechtlicher, auch ethischer Fragen werden in den Mittelpunkt gerückt. Deutschland, das seine Sicherheits- und Verteidigungspolitik ausschließlich im europäischen und Bündnisrahmen betreibt, könnte sich dabei im weiteren Verlauf auch im Gegensatz zu seinen wichtigsten

^{1.} http://www.cnas.org/sites/default/files/publications-pdf/Brimley-HASC-PreparedStatement-12022014.pdf

Identifikation, Verfolgung, Priorisierung und Markierung

von Zielen, die Entscheidung des Zeitpunkts, wann die

Waffe ausgelöst wird und der Zeitpunkt des Einschlags.

Mindestens 30 Länder verfügen über mehr oder weniger automatisierte Systeme mit vom Menschen überwachten

autonomen Funktionen. Diese werden u.a. genutzt, um

Personal in militärischer Infrastruktur und auf Marineschiffen zu schützen, da die Reaktionszeit des Menschen hierzu nicht ausreicht. Die wesentlichen Akteure bei der

Entwicklung defensiver und zunehmend offensiver au-

tonomer Waffensysteme sind die USA und Israel, China,

Japan und Südkorea sowie Großbritannien, Frankreich

und Russland. Voraussetzung ist eine hochtechnisierte

Dabei werden ständig komplexere Algorithmen entwi-

ckelt, mit denen Maschinen in die Lage versetzt werden,

Entscheidungen autonom zu treffen. Dies hat neue, noch

und technologisch leistungsfähige Industrie.



Partnern wiederfinden. Eine öffentliche Debatte über die Tragweite der Technologiefolgen ist notwendig, damit die richtigen Entscheidungen vorbereitet, gefällt und auf Dauer getragen werden können.

Auf dem Weg zur Künstlichen Intelligenz (KI): Autonome Waffensysteme

In ihrer einfachsten Form ist Autonomie die Fähigkeit einer Maschine – Hardware und Software – eine Aufgabe ohne menschliches Zutun auszuführen. Ein autonomes System ist eine Maschine, die nach ihrer Aktivierung eine Aufgabe oder Funktion eigenständig wahrnimmt.

Über Definitionen und Charakteristika autonomer Waffensysteme ist aufgrund der großen Komplexität in Wissenschaft und Politik ein Konsens nur sehr schwer zu erzielen. Allgemein verbindliche Definitionen konnten bisher nicht erreicht werden. Selbst die Frage, ob exakte Definitionen mit Blick auf Rüstungskontrolle notwendig sind, ist umstritten. Für das vorliegende Papier wurden folgende Arbeitsdefinitionen zugrunde gelegt, die weitgehend den vom Pentagon benutzten Begriffen folgen:

- Ein autonomes Waffensystem ist ein Waffensystem, das, einmal aktiviert, Ziele selektieren und bekämpfen kann, ohne dass ein menschlicher Bediener eingreifen muss/kann.²
- Ein *überwacht-autonomes Waffensystem* ist ein Waffensystem, das dem menschlichen Bediener die Möglichkeit des Eingreifens und Ablehnens bestimmter Handlungen, wie dem Waffeneinsatz, bietet.³
- Ein teil-autonomes Waffensystem ist ein Waffensystem, das, einmal aktiviert, ein Ziel oder eine bestimmte Gruppe von Zielen bekämpfen kann, die ein menschlicher Bediener zuvor ausgewählt und zum Angriff freigegeben hat.⁴

Tatsächlich wird Automatisierung, eine Vorstufe zur Autonomie, bereits bei einer Vielzahl militärischer Aufgaben genutzt. Viele weisen bereits direkte und indirekte Verbindungen zum Waffeneinsatz auf. Dazu gehören u. a. die

schen Entwicklung, bei der Softwaresysteme zunehmend lernfähig werden und automatisch Computerprogramme erzeugen können. Künstliche Intelligenz könnte womöglich in wenigen Jahrzehnten die kognitive Leistungsfähigkeit von menschlichen Gehirnen erreichen und übersteigen. Im Zusammenhang mit einer umfassenden digitalen Vernetzung (Internet der Dinge) wird Computerintelligenz in fast alle Bereiche von Wirtschaft und Gesellschaft eindringen und voraussichtlich erhebliche soziokulturelle Umbrüche erzeugen. Damit sind große Chancen, aber auch erhebliche Risiken verbunden. Zahlreiche international renommierte KI-Forscher haben in ihrem offenen Brief zur Eröffnung einer internationalen Konferenz über Künstliche Intelligenz 2015 in Buenos Aires (International Joint Conference on Artificial Intelligence, IJCAI) vor den erheblichen Risiken autonomer Waffen ohne effektive menschliche Kontrolle gewarnt.

komplexere Einsatzszenarien zur Folge. Auch Fortschritte im Bereich der Sensorik werden künftige Waffensysteme potenter machen. Zu nennen ist hier vor allem eine starke Verbesserung der Freund-Feind-Unterscheidung und der Zielerkennung. Dazu kommen eine bessere Vernetzung zwischen Maschinen (»Schwarm«) und ausgereiftere Interaktionen zwischen Mensch und Maschine. Angetrieben werden diese Prozesse durch Fortschritte in der Softwareentwicklung im Bereich KI.

Auf dem Weg zur Künstlichen Intelligenz: Führungs- und Planungssysteme

Wir befinden uns offenbar am Anfang einer dynamischen Entwicklung, bei der Softwaresysteme zunehmend lernfähig werden und automatisch Computerprogramme

^{2.} Vgl. International Committee of the Red Cross (ICRC): Autonomous weapon systems: Technical, military, legal and humanitarian aspects. Expert meeting report, Genf 2014, 14.

^{3.} a.a.O.

^{4.} a.a.O.



Autonome Waffen, so die Autoren, könnten bereits in Jahren, nicht Jahrzehnten, zum Einsatz kommen und seien als die dritte Revolution der Kriegsführung nach Schießpulver und Nuklearwaffen beschrieben worden.

Die digitale Revolution wird weitergehen, deshalb wird es darauf ankommen, die Anwendungen von künstlicher Intelligenz so zu gestalten und zu steuern, dass die menschliche Entscheidungsautonomie generell nicht infrage gestellt wird. Dies erfordert ggf. Maßnahmen und Technologien zur Eindämmung bzw. Regulierung von künstlicher Intelligenz, vor allem gegen unkalkulierbare Ausbrüche bzw. qualitative Sprünge (»Intelligence Explosion«).

Die neuen digitalen Technologien werden auch den Bereich der Sicherheits- und Militärpolitik durchdringen und mit der Zeit erhebliche Umbrüche nach sich ziehen. Über die Entwicklung von Software zur Unterstützung strategischer Planung und Einsatzführung in den hochtechnologiefähigen Nationen ist jedoch noch wenig bekannt. Es geht hier zunächst um die strategischen Waffen, insbesondere den Komplex der Frühwarnung, Raketenabwehr und der Abschreckung durch Nuklearwaffen. Darüber hinaus dürften auch die strategischen Führungs- und Informationssysteme (Command and Control), die Kommunikations-, Navigations-, Aufklärungs- und Überwachungssysteme sowie der gesamte Bereich defensiver und offensiver Fähigkeiten im Cyberraum Anwendungsgebiete für künstliche Intelligenz werden, um deren Effizienz zu verbessern. Durch künstliche Intelligenz getriebene autonome Funktionen in diesen Bereichen müssen als weit gravierender eingeschätzt werden, als dies bei taktischen Waffensystemen der Fall ist, denn sie wirken unmittelbarer auf die Fähigkeiten zur politischen Kontrolle über den Einsatz von Streitkräften.

Auch in den Kernbereich der nationalen und multinationalen politisch-strategischen Lagebeurteilungen und Entscheidungsprozesse dürften Supercomputer früher oder später Eingang finden. Dies entspricht der technologischen Entwicklungslogik, allerdings liegen wissenschaftliche Analysen hierzu noch nicht vor. Ein wesentlicher Treiber dieser Entwicklung dürfte der zeitliche Entscheidungsdruck sein, der technologiebedingt durch immer schnellere Abläufe in bewaffneten Konflikten entsteht.

Erste Ansätze hierzu sind erkennbar. Eine Pentagoninterne Weisung für die »Defense Science Board 2015 Study of Autonomy«⁵ erwähnt ausdrücklich den IBM Supercomputer Watson und thematisiert die Möglichkeit automatischer Entscheidungshilfen und Planungssysteme. IBM Watson ist nach Angaben des Herstellers ein kognitives Computersystem, das bereits heute die natürliche menschliche Sprache nicht nur versteht, sondern sprachliche Informationen auch verarbeitet und präzise Antworten auf Fragen in natürlicher Sprache ausgeben kann.

IBM Watson dürfte ein Beispiel für eine erste Generation superintelligenter Maschinen sein, die früher oder später auch in politischen und militärischen Entscheidungsprozessen zum Einsatz kommen. Der Zwang, immer größere Mengen von Daten in immer kürzerer Zeit zu sammeln, zu speichern und schlussfolgernd zu analysieren, wird die Nutzung solcher Maschinen unweigerlich vorantreiben. Zugleich wird dieser Prozess aber auch immer mehr Energie erfordern, sodass die Verwundbarkeit solcher Systeme von gesicherter Stromzufuhr tendenziell steigt.

Ohne Frage werden die Architekturen von Supercomputern ausdrücklich als Assistenzsysteme oder Empfehlungssysteme konzipiert werden, deren Nutzung die menschliche Entscheidungsautonomie nicht beeinträchtigen soll. In der Praxis dürfte jedoch das erhebliche Risiko einer schleichenden Abhängigkeit von und einer Gewöhnung an die Entscheidungsunterstützung durch Supercomputer bestehen. Hochleistungsrechner werden unter Umständen in Krisenszenarien Realität simulieren, Vorhersagen über das Verhalten der unterschiedlichen Akteure machen und damit Entscheidungsprozesse mitgestalten. Hieraus ergeben sich

Eine Reihe kritischer Fragen:

Führt z. B. die Abhängigkeit von computergenerierten Daten und Lösungsvorschlägen nicht unweigerlich zur Handlungsunfähigkeit bei Störungen oder Ausfall der digitalen Systeme? Sind die Akteure auf den politischstrategischen und den militärischen Führungsebenen bei digitalen Fehlern bzw. Computerabstürzen oder gar einem flächendeckenden Stromausfall später noch in der Lage, ohne die digitalen Kommunikations-, Navigations-, und Entscheidungshilfen zielgerichtet zu handeln? Dies wäre auch im Kontext möglicher asymmetrischer Re-

^{5.} US Undersecretary of Defense – Memorandum for the Chairman, Defense Science Board vom 17. November 2014.



aktionen auf eine digitale Kriegsführung zu bedenken. Welche Konsequenzen ergeben sich aus dem Handeln und Gegenhandeln in Krise und Krieg, wenn beide Seiten mit rechnergestützten Analysen und Entscheidungshilfen arbeiten?

Ferner: Wie hoch ist das Risiko einzuschätzen, dass die verantwortlichen Politiker, Spitzenbeamten und Spitzenmilitärs glauben werden, dass sie frei und unabhängig entscheiden, während sie in Wirklichkeit nur noch auf der Grundlage einer in Rechnern generierten simulierten Realität und vorfabrizierter Handlungsoptionen agieren? Werden sie dann noch erkennen können, dass die künstliche Intelligenz sie bevormundet, nachdem sie sich langsam an die neuen, maschinenintelligenten Ratgeber gewöhnt haben und damit auch ein Stück weit erfolgreich gewesen sind?

Politische und militärische Entscheidungen sind von je her zu einem wesentlichen Teil intuitiv getroffen worden, d. h. auf der Basis einer auf Erfahrung basierenden, ganzheitlichen Urteilskraft, die weit über das rein Kognitive hinausgeht. Werden die Entscheider in den Regierungen und die militärischen Spitzen noch über eine erfahrungsgesättigte Intuition, über »gefühltes Wissen« verfügen, wenn ihr Denken immer computergerechter wird, wenn der »Vermenschlichung« der Maschinen die Computerisierung des Menschen entspricht (Schirrmacher)? Was bedeutet das für Entscheidungen in heißen Krisensituationen, in denen es unmittelbar um die Frage geht, ob militärische Gewalt eingesetzt, also Krieg geführt werden soll – oder nicht?

Sind solche Fragen berechtigt oder eher noch dem Bereich von Science Fiction zuzuordnen? Kann Politik in diesem Bereich auf Sicht fahren und eine abwartende Haltung einnehmen, weil die intelligenten Systeme ja noch nicht oder nur rudimentär existieren? Der erkennbare Forschungsstand auch in Deutschland und die Tatsache, dass in den USA bereits eine breite, auch kritisch vorausschauende Diskussion zur Künstlichen Intelligenz eingesetzt hat, weist auf konkreten Handlungs- und Steuerungsbedarf hin.

Bei der Entwicklung und Einführung superintelligenter Rechner im sicherheitspolitischen Bereich ist es von essenzieller Bedeutung, sie durch Evaluationen und Maßnahmen zur menschlichen Beherrschung der neuen Technologien aktiv zu begleiten. Aus der Vergangenheit wissen wir, dass es nie echte Kontrolle über die Entstehung neuer Technologien gegeben hat und die positiven wie negativen Wirkungen technologischer Sprünge stets erst im Nachhinein erkennbar wurden, so z.B. in der Atomphysik des 20. Jahrhunderts, die den Bau von Nuklearwaffen ermöglichte, oder bei der Entwicklung des Internets, bei der Fragen der Netzsicherheit zunächst keine Rolle spielten. Im 21. Jahrhundert wird es darauf ankommen, nicht in neue Technologiefallen zu stürzen, aus denen die Politik im gewohnten Modus eines Reparaturbetriebs keinen Ausweg mehr finden kann.

2. Strategisch-politische Konsequenzen

Grundsätzlich dienen Waffensysteme der Kriegsführung. Politische Leitlinie ist es aber, Kriege zu vermeiden bzw. zu verhüten, von Angriffen abzuschrecken und nur, wenn Abschreckung nicht gelingt, sie auch erfolgreich führen zu können. Daraus ergeben sich eine Reihe grundsätzlicher Fragen:

- Führt die Entwicklung und Einführung automatisierter und später autonomer Waffensysteme in unsere Streitkräfte schleichend zu einer technischen Eigendynamik in der Kriegsführung?
- Wäre eine solche Entwicklung mit demokratisch legitimierter Verantwortlichkeit zu vereinbaren? Oder würde die politische Entscheidungsautonomie immer mehr eingeschränkt? Wenn ja: Worin genau bestünde gegebenenfalls die Einschränkung politischer Kontrolle?
- Könnte der Verlust politischer Kontrolle in Kriegs- und Konfliktsituationen die Folge sein? Und wie könnte bei einer zunehmenden Autonomisierung des militärischen Handelns die politische Entscheidungsautonomie und Kontrolle gewahrt bleiben?

Die dargestellten technologischen Entwicklungen lassen auf Möglichkeiten und Vorstellungen von Kriegsführung schließen, welche die Rolle des verantwortlich handelnden Menschen, die besonders bei Fragen von Leben und Tod von grundsätzlicher Bedeutung ist, radikal verändern, ja tendenziell zumindest in Teilen ganz entfernen könnten.

Die zentrale Frage lautet also, welche Auswirkungen sie auf unsere Vorstellungen von und unsere Fähigkeiten



zu Kriegsführung haben und wie sichergestellt werden kann, dass demokratische politische Kontrolle stets funktioniert. Dies setzt zwingend ethisch geleitete Verantwortung von Menschen gegenüber anderen Menschen voraus, die zu organisieren ist und auch wahrgenommen können werden muss.

Sicherheitspoltische Konsequenzen

In sicherheitspolitischer Hinsicht könnte die Verfügung über eine hinreichende Zahl autonomer Waffensysteme Entscheidungen zugunsten militärischer Interventionen erleichtern, weil das Risiko für das Leben der eigenen Soldaten und auch die Kosten, damit schließlich auch der öffentliche Begründungszwang verringert wird.

Die technologischen Entwicklungen bringen auch erhebliche Herausforderungen für die internationale Rüstungskontrolle mit sich. Welche Folgen hätte die fortschreitende technologische Dynamik in Richtung immer schnellerer, leistungsfähigerer und letztlich autonomer Waffen für die bestehenden Rüstungskontrollverträge und für die Ausarbeitung neuer, der technologischen Entwicklung angepasster Rüstungskontrollregime? Als Einstieg in eine präventive kooperative Rüstungssteuerung auf diesem Gebiet sind Vereinbarungen zur möglichst großen Transparenz sowie über einen Verhaltenskodex vorstellbar. Dafür sind Massnahmen für Vertrauensbildung und Verifikation unabdingbar. Kann so ein ausufernder Rüstungswettlauf zwischen Hochtechnologieländern noch verhindert werden?

Kann man verhindern, dass die neuen Waffensysteme in die falschen Hände geraten, seien es staatliche oder nicht-staatliche? Welche Folgen kann diese Entwicklung für andere Sicherheitsbereiche wie Polizei und Grenzsicherung haben, und welche Folgen hätte dies für das sensible Verhältnis von Sicherheit und Freiheit, von innerer und äußerer Sicherheit? Tiefgreifende gesellschaftspolitische Fragen sind also auch berührt.

Bündnispolitische Konsequenzen

Deutschlands Sicherheitspolitik findet im Rahmen von EU und NATO statt. Dementsprechend ist die Art und Weise, wie unsere Bündnispartner mit diesem Thema umgehen, von großer Bedeutung. Ihre Standpunkte hinsichtlich der Entwicklung und Bedeutung autonomer Waffensysteme sind allerdings unterschiedlich. Einerseits befürwortet

bislang kein Staat die Entwicklung und den Einsatz autonomer Waffensysteme, die völlig ohne menschliche Kontrolle auskommen. Andererseits treiben etwa die USA die Weiterentwicklung autonomer Waffensysteme voran. Zwar geschieht dies mit der Vorgabe, dass für »angemessene menschliche Kontrolle« gesorgt werde, es bleibt aber unklar, was genau damit gemeint ist. Sicher ist, dass Deutschland ein großes Interesse an einer bündniskompatiblen Regelung für den Umgang mit diesem Thema hat. Schließlich müssen unsere Streitkräfte interoperabel sein und bleiben. Ob im EU- oder im NATO-Rahmen: Alle Mitglieder sind Demokratien und stehen vor demselben Problem demokratischer Verantwortlichkeit im Umgang mit autonomen Waffensystemen. Unterschiedliches oder nicht abgestimmtes Vorgehen könnte deshalb zu erheblichen politischen Problemen bei der Zusammenarbeit und damit langfristig für den Zusammenhalt des Bündnisses führen.

Völkerrechtliche Konsequenzen

Jede Entwicklung und Nutzung von Waffen, also auch von autonomen Waffensystemen, muss den Prinzipien des Völkerrechts genügen. Dies sind die Prinzipien der Unterscheidbarkeit von Kombattanten und Nicht-Kombattanten, also Soldaten und Zivilisten, sowie der Verhältnismäßigkeit der eingesetzten Mittel, der militärischen Notwendigkeit sowie der Reziprozität (Einhaltung völkerrechtlicher Normen) und der Vermeidung unnötiger Leiden. Die Birmingham Policy Commission, eine Expertengruppe aus politischen Entscheidungsträgern in Großbritannien und Wissenschaftlern der Universität Birmingham kam deshalb im Herbst 2014 zu dem Schluss, dass es nicht möglich sein werde, autonome Waffensysteme zu entwickeln, die mit dem Kriegsvölkerrecht vereinbar seien. In einer Studie, die die FES im Juni 2015 publiziert hat, kommt der Völkerrechtler Robin Geiss zu der Schlussfolgerung, daß »kritische Entscheidungen« (etwa über Leben und Tod) nicht an vollständig autonome Systeme delegiert werden dürfen.⁶

Normativ-ethische Konsequenzen

Entscheidungen zum tödlichen Waffeneinsatz dürfen vor dem Hintergrund unseres auf der Menschenwürde fußenden Wertesystems (Mensch als Verantwortungs-

^{6.} Geiss, Robin: Die völkerrechtliche Dimension autonomer Waffensysteme. Friedrich-Ebert-Stiftung, Internationale Politikanalyse, Berlin 2015. http://library.fes.de/pdf-files/id/ipa/11444-20150619.pdf



subjekt) grundsätzlich nicht an Maschinen delegiert werden, auch wenn diese von Menschen programmiert und eingesetzt werden. Der Einsatz militärischer Gewalt muss durch eine aktive, von einem Menschen zu verantwortende Handlung ausgelöst werden. Krieg darf nicht auf »Autopilot« geführt werden. Damit stellt sich die grundsätzliche Frage, ob die Verantwortung für die Entscheidung über Leben und Tod an Computeralgorithmen übertragen werden darf, ohne dass ein Mensch diese Entscheidung zumindest mit trägt und auf sein Gewissen lädt. Es geht dabei um die Frage der Verantwortung, Gewissensentscheidung und Haftung. Wie soll Verantwortung und Haftung etwa bei Fehlern gestaltet werden, wenn ein Waffeneinsatz nicht mehr vom militärischen Führer einem unterstellten Soldaten befohlen wird, sondern einem Programmierer/Operator, der im Waffensystem eine Software für den Kampf füttert? Wie kann Verantwortlichkeit und Haftung bei Kollateralschäden sichergestellt werden, die durch eine Fehlfunktion des Kampfroboters entstanden ist? Sollte, darf eine solche todbringende Mensch-Maschine-Schnittstelle überhaupt geschaffen werden?

Dies gilt auch für die bisherige militärische Führungsethik, die durch autonome Waffensysteme außer Kraft gesetzt würde. Offiziere würden ihre Aufträge und Befehle nicht mehr zur Ausführung an unterstellte Soldaten erteilen, sondern an uniformierte IT-Experten, die einer Waffensystemsoftware einen Auftrag eingeben, den das Waffensystem autonom ausführt.

Für spätere, noch weiter entwickelte Systeme, die in der Lage sein werden, komplexe Aufträge im Sinne der Auftragstaktik zu übernehmen, würde sich diese Frage noch in verschärfter Form stellen.

Wirtschaftspolitische Konsequenzen

Hinzu kommt eine ökonomische Ebene: Die autonomen Waffensystemen zugrunde liegende Technologie wird vor allem für zivile Zwecke entwickelt. Universitäten und Unternehmen erforschen längst autonom operierende Roboter für den zivilen Bereich, die mit künstlicher Intelligenz funktionieren. Es gibt großes Verwertungsinteresse an dieser Technologie, wie die Diskussion um das fahrerlose Auto illustriert.

Der zivile Sektor ist der eigentliche Treiber der technologischen Entwicklung, die in den militärischen Sektor hin-

eindrängt – und nicht umgekehrt. Die enge Verknüpfung dieser Technologieentwicklung, die im Wesentlichen von privaten Unternehmen betrieben wird, mit den Sicherheitsanforderungen in der militärischen Nutzung macht es notwendig, besonderes Augenmerk auf die bleibende Divergenz der Interessenlagen zu legen: Die Technologieunternehmen verfolgen ihre Geschäftsmodelle, die oft global und auf schnelle Marktpräsenz ausgerichtet sind. Regierungen und internationale Organisationen tragen gesellschaftliche und politische Verantwortung, die meist national und auf hohe Sicherheitsstandards ausgerichtet sind. Beides musste auch bisher schon austariert werden, allerdings könnten sich die Entscheidungsspielräume für die politische Führung angesichts der Rasanz der Entwicklungen stärker reduzieren als erwartet oder zu verantworten ist.

3. Schlussbemerkung

Die Entwicklung völlig neuer Militärtechnologien bis hin zur Entwicklung autonomer Waffensysteme ist in vollem Gang. In diesem Prozess liegen, wie stets bei völlig neuen Technologien, Chancen und Risiken zugleich. Es kann nicht darum gehen, die digitale und autonomisierte Zukunft des Militärs grundsätzlich zu verdammen. Es gilt, den legitimen Nutzen der Digitalisierung voranzutreiben und die möglichen negativen Folgen für die menschliche Entscheidungsautonomie und die ethischen und völkerrechtlichen Regelwerke einzuhegen und zu gestalten. So könnten beispielsweise autonomisierte Systeme etwa im Bereich des Rettungswesens sowie in der Luft- und Raketenabwehr durchaus nützlich sein: im Sinne des Schutzes von Leben.

Diese Entwicklung zieht umfassende politische, ja philosophische und ethische Folgen nach sich, die weit über den Bereich der Sicherheits- und Verteidigungspolitik hinausgehen und von erheblicher gesellschaftspolitischer Relevanz sind. In einer demokratischen Gesellschaft gehören solche Fragen unbedingt öffentlich diskutiert. Die Gremien der Verteidigungsplanung in NATO und EU, aber auch die Debatten im Zusammenhang mit dem Weißbuch der Bundesregierung zur Sicherheitspolitik, der Erarbeitung der neuen Europäischen Sicherheitsstrategie der EU sowie dem nächsten Strategischen Konzept der NATO sollten dazu genutzt werden. Mit diesem Papier soll ein Anstoß und Beitrag zu diesem Diskurs geleistet werden.



Über die Autoren

Der Arbeitskreis Internationale Sicherheitspolitik ist ein Forum der Friedrich-Ebert-Stiftung zum Austausch über aktuelle sicherheitspolitische Themen. Die Mitglieder des Arbeitskreises kommen aus dem Bundestag, Bundesministerien und wissenschaftlichen Instituten. Ihm gehören u. a. an:

Franz H. U. Borkenhagen, Michael Bröning, Hans-Georg Ehrhart, Tobias Fella, Helmut W. Ganser, Michael Hofmann, Alexander Kallweit, Anna Maria Kellner, Wulf Lapins, Marius Müller-Hennig, Detlef Puhl, Jürgen Schnappertz und Oliver Thränert.

Impressum

Friedrich-Ebert-Stiftung | Internationale Politikanalyse Hiroshimastraße 28 | 10785 Berlin | Deutschland

Verantwortlich:

Dr. Michael Bröning, Leiter Internationale Politikanalyse

Tel.: ++49-30-269-35-7745 | Fax: ++49-30-269-35-9248 www.fes.de/ipa

Bestellungen/Kontakt hier: info.ipa@fes.de

Eine gewerbliche Nutzung der von der Friedrich-Ebert-Stiftung (FES) herausgegebenen Medien ist ohne schriftliche Zustimmung durch die FES nicht gestattet.

Die Internationale Politikanalyse (IPA) ist die Analyseeinheit der Abteilung Internationaler Dialog der Friedrich-Ebert-Stiftung. In unseren Publikationen und Studien bearbeiten wir Schlüsselthemen der europäischen und internationalen Politik, Wirtschaft und Gesellschaft. Unser Ziel ist die Entwicklung von politischen Handlungsempfehlungen und Szenarien aus der Perspektive der Sozialen Demokratie.

Diese Publikation erscheint im Rahmen der Arbeitslinie »Europäische Außen- und Sicherheitspolitik«. Redaktion: Anna Maria Kellner, Anna.Kellner@fes.de.

Die in dieser Publikation zum Ausdruck gebrachten Ansichten sind nicht notwendigerweise die der Friedrich-Ebert-Stiftung.

Diese Publikation wird auf Papier aus nachhaltiger Forstwirtschaft gedruckt.



ISBN 978-3-95861-255-6