ECONSTOR
Make Your Publications Visible.

A Service of

ZBW Leibniz-Informationszentrum Wirtschaft
Leibniz Information Centre for Economics

Dickow, Marcel

Research Report

Robotik - ein Game-Changer für Militär und Sicherheitspolitik?

SWP-Studie, No. S 14/2015

Provided in Cooperation with:
Stiftung Wissenschaft und Politik (SWP), German Institute for International and Security Affairs, Berlin

Suggested Citation: Dickow, Marcel (2015) : Robotik - ein Game-Changer für Militär und Sicherheitspolitik?, SWP-Studie, No. S 14/2015, Stiftung Wissenschaft und Politik (SWP), Berlin

This Version is available at:
https://hdl.handle.net/10419/252881

Standard-Nutzungsbedingungen:

Die Dokumente auf EconStor dürfen zu eigenen wissenschaftlichen Zwecken und zum Privatgebrauch gespeichert und kopiert werden.

Sie dürfen die Dokumente nicht für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, öffentlich zugänglich machen, vertreiben oder anderweitig nutzen.

Sofern die Verfasser die Dokumente unter Open-Content-Lizenzen (insbesondere CC-Lizenzen) zur Verfügung gestellt haben sollten, gelten abweichend von diesen Nutzungsbedingungen die in der dort genannten Lizenz gewährten Nutzungsrechte.

Terms of use:

Documents in EconStor may be saved and copied for your personal and scholarly purposes.

You are not to copy documents for public or commercial purposes, to exhibit the documents publicly, to make them publicly available on the internet, or to distribute or otherwise use the documents in public.

If the documents have been made available under an Open Content Licence (especially Creative Commons Licences), you may exercise further usage rights as specified in the indicated licence.

WWW.ECONSTOR.EU

Mitglied der Leibniz-Gemeinschaft

SWP-Studie
Stiftung Wissenschaft und Politik
Deutsches Institut für Internationale
Politik und Sicherheit

Marcel Dickow

Robotik – ein Game-Changer für Militär und Sicherheitspolitik?

S 14
Juni 2015
Berlin

Alle Rechte vorbehalten.
Abdruck oder vergleichbare Verwendung von Arbeiten der Stiftung Wissenschaft und Politik ist auch in Auszügen nur mit vorheriger schriftlicher Genehmigung gestattet.

SWP-Studien unterliegen einem Begutachtungsverfahren durch Fachkolleginnen und -kollegen und durch die Institutsleitung *(peer review)*. Sie geben ausschließlich die persönliche Auffassung der Autoren und Autorinnen wieder.

© Stiftung Wissenschaft und Politik, Berlin, 2015

SWP
Stiftung Wissenschaft und Politik
Deutsches Institut für Internationale Politik und Sicherheit

Ludwigkirchplatz 3–4
10719 Berlin
Telefon +49 30 880 07-0
Fax +49 30 880 07-100
www.swp-berlin.org
swp@swp-berlin.org

ISSN 1611-6372

Inhalt

5 **Problemstellung**

7 **Militärische Roboter**
7 Maschinen und Roboter
8 Autonomie
8 *Systematik autonomer Funktionen von Robotern*
9 *Assistenzsysteme*
10 *Konsequenzen der Autonomie*
11 *Entführung einer US-Drohne – ein Fallbeispiel für die Gefährdung autonomer Roboter*
12 Die Nutzung militärischer Roboter
13 Die Richtung der Technologieforschung
13 Der militärische Einsatz
14 *Luft*
14 *Boden/Oberfläche*
15 *See (Untersee- und Überwasser-Systeme)*
16 *Weltraum*

17 **Roboter als militärische Revolution?**
17 Veränderungen für die Streitkräfte
18 Auswirkungen auf militärische und politische Strategie

21 **Konsequenzen und Empfehlungen für die deutsche Sicherheitspolitik**
21 Robotik und Sicherheitspolitik
22 Empfehlungen für die Bundesrepublik

24 **Abkürzungen**

Dr. Marcel Dickow ist Leiter der SWP-Forschungsgruppe Sicherheitspolitik.

Robotik – ein Game-Changer für Militär und Sicherheitspolitik?

In näherer bis mittelfristiger Zukunft werden Militärroboter menschliche Soldaten zunehmend unterstützen, sie teilweise sogar ersetzen. Bislang sind solche Vorgänge vor allem im begrenzten taktisch-operationellen Bereich zu beobachten; doch mehr und mehr wird sich das Aufgabenfeld den wachsenden technologischen Fähigkeiten der Robotik anpassen. Mit fortschreitender Automatisierung wachsen die Kompetenzen, die Robotern übertragen werden – diese agieren so zunehmend autonom. Im Zuge der Entwicklung werden Maschinen ein immer breiteres Spektrum an Tätigkeiten abdecken, so dass der menschliche Operateur nur noch übergeordnete Kontrollfunktionen wahrnimmt. Kommt es dabei zu autonomen maschinellen Entscheidungen, ob Waffengewalt anzuwenden ist, wird eine ethische Linie überschritten und eine grundsätzliche Frage nach der Qualität des Gewalteinsatzes aufgeworfen: Dürfen Maschinen über Leben und Tod von Menschen befinden? Auch aus militärischer Sicht müssten dann bislang geltende Prinzipien des Humanitären Völkerrechts maschinell umgesetzt werden, vor allem was das Gebot betrifft, zwischen Kombattanten und Zivilisten zu unterscheiden.

Ziel dieser Studie ist es, technologische Einblicke in existierende und geplante militärische Robotiksysteme zu geben und daraus sicherheitspolitische Konsequenzen abzuleiten. Während militärische Roboter gegenwärtig noch ferngesteuert werden, dürfte in den kommenden Jahren eine schleichende Automatisierung und Autonomisierung der Maschinen stattfinden. Erkennbar wird dieser Trend an der Einführung und Fortentwicklung von Assistenzsystemen im militärischen, aber auch im zivilen Bereich. Bislang sollen Roboter und ihre autonomen Teilfunktionen es dem Operateur ermöglichen, sich auf jene Aufgaben zu konzentrieren, für die Menschen besser geeignet sind als Maschinen. Umgekehrt übernimmt die Maschine Aufgaben, die für den Menschen zu gefährlich, zu eintönig oder »zu schmutzig« sind. Diese Rollenverteilung verändert sich mit dem technologischen Fortschritt rasant. Maschinen und ihre Algorithmen entlasten den Bediener auch zunehmend von komplexen Datenauswertungen und bieten Handlungsoptionen an. Hier ergeben sich zunächst einige technische Fragen, darüber hinaus aber ebenso Fragen

nach den Implikationen für Streitkräfte, Politik und Recht.

Auf technischer Ebene ist beispielsweise zu untersuchen, welche technologischen Trends die Richtung in der militärischen Robotik bestimmen. Zudem ist relevant, was nach heutigem Stand schon machbar ist, woran geforscht wird und welche technologischen Grenzen die Entwicklung hat.

Klar ist, dass unbemannte ferngesteuerte Systeme die Streitkräfte und ihre Einsätze im vergangenen Jahrzehnt mitgeprägt haben. Insbesondere ferngesteuerte Drohnen – also Unmanned Aerial Vehicles (UAV) oder Remotely Piloted Aircraft Systems (RPAS) – haben der militärischen Robotik den Weg geebnet. Weitere militärische Roboter sind etwa in Form von Minenräumbooten oder Lasteneseln zu finden. Doch solche Systeme bilden nur die Spitze des Eisbergs der noch folgenden technologischen Entwicklung. Dabei sind unterschiedliche Autonomiegrade denkbar – von der Fernsteuerung bis zum völlig autonomen Handeln. Diese Technologien werden das Wesen der Streitkräfte verändern, ebenso ihre Taktik, die Strategie und die dahinterstehenden politischen Konzepte. Die Einführung der Robotik in die Streitkräfte der Industrienationen lässt erste vorsichtige Rückschlüsse zu, über welches Veränderungspotential die Technologie verfügt. Ungeklärt ist aber noch, wie der Mensch mit dieser neuen Form von Maschine interagiert – im Friedensbetrieb oder im Einsatz – und wie sich Streitkräfte in ihrer Struktur und Einsatzfähigkeit dadurch verändern. Ganz grundsätzlich ist also zu bestimmen, was Streitkräfte mit Robotern und was Roboter mit Streitkräften machen.

Militärische Robotik könnte einen Paradigmenwechsel einläuten, der die Gleichungen und das Gleichgewicht der internationalen Sicherheitspolitik revolutioniert. Auch wenn dazu noch keine abschließende Bewertung möglich ist, gibt es heute schon Indizien, die für mehr als nur eine technologische Evolution sprechen. Dabei geht es nicht bloß um das Potential, den Menschen im Kriegshandwerk durch die Maschine zu ersetzen, sondern auch um die Auswirkungen der Technologie auf strategisch-politische Entscheidungen – etwa das Für und Wider eines Militäreinsatzes überhaupt – und um die Veränderung von Konfliktformen.

Ein weiterer Aspekt, der Bedeutung hat im Umgang mit dieser neuen Technologie, ist eine sinnvolle und durchsetzbare Verregelung. Die Bundesregierung hat sich zwar schon frühzeitig gegen den Einsatz von autonomen Robotern ausgesprochen, genauer gesagt gegen autonome maschinelle Entscheidungen zum Gewalteinsatz. Doch eine internationale Regulierung liegt in weiter Ferne. Das hat nicht nur mit definitorischen Problemen zu tun, sondern auch mit der unterschiedlich ausgeprägten Bereitschaft der Staaten, autonome bewaffnete Roboter und ihren Einsatz zu beschränken. Trotzdem kann sich Deutschland glaubwürdig und mit einigem politischen Gewicht für die nötigen internationalen Regeln einsetzen. Auf nationaler wie internationaler Ebene ist es der Bundesregierung möglich, konkrete Schritte zu unternehmen – etwa eigene Definitionen vorzulegen oder ein EU-Moratorium für den Einsatz autonomer bewaffneter Roboter zu initiieren.

Militärische Roboter

Von jeher ist der Mensch darauf aus, seine Schwächen technologisch auszugleichen. Dies gilt insbesondere dann, wenn er Krieg führt. Bis zum 20. Jahrhundert *ergänzte* die Militärtechnik den Menschen – angefangen bei Panzerung oder Pfeil und Bogen. In Zukunft wird sie ihn teilweise *ersetzen*. Die Abwesenheit des Menschen auf dem Schlachtfeld, zumindest bei einer der beteiligten Kriegsparteien, bedeutet eine Zeitenwende, die völkerrechtliche, moralische und ethische Konsequenzen hat. Der Mensch gewinnt dadurch physische Distanz zur Gewalt; das Gefechtsumfeld nimmt er nur noch durch die elektronische Sensorik seiner Maschinen wahr – er kann Kriege führen lassen. Abzuwarten bleibt, ob dies eine echte Revolution ist oder nur ein weiterer Evolutionsschritt, nachdem die »Kriegsherren« schon im 19. Jahrhundert das Schlachtfeld physisch verlassen haben.

Auf technologischer Ebene bedarf es zweierlei, um den Menschen auf dem Schlachtfeld zu ersetzen: der Fernsteuerung, das heißt digitaler Kommunikation über die Sichtlinie hinaus, und einer gewissen Automatisierung der Maschine vor Ort. Automatisierung beschreibt dabei den Vorgang, dass wiederkehrende Prozesse in klar definierten und begrenzten Kontexten wiederholt ausgeführt werden. Der heutige militärische Roboter[1] zeichnet sich durch drei Fähigkeiten aus: Er sammelt Daten über seine Umwelt (Sensorik), verarbeitet sie (Informationsgewinnung) und tritt in Interaktion mit seiner Umwelt (Manipulation). Er muss sich nicht notwendigerweise bewegen können, auch wenn die meisten Roboter heute dazu in der Lage sind. Ein wesentliches Unterscheidungsmerkmal ist der Grad an Autonomie bei der Interaktion mit der Umwelt. Roboter können ferngesteuert, teilautonom oder vollständig autonom agieren. Allerdings ist ihre Automatisierung noch nicht intelligent im Sinne menschlichen Intellekts. Neben der Weiterentwicklung der Fähigkeiten zu Fortbewegung und mechanischer Manipulation arbeiten Firmen und Regierungen weltweit daran, die Autonomie von Robotern qualitativ zu verbessern. Ziel ist, menschliche Entscheidungsprozesse durch Algorithmen (eindeutige Handlungsvorschriften, implementiert durch Computerprogramme) in der Maschine nachzuahmen (künstliche Intelligenz).

Maschinen und Roboter

Bei Robotern handelt es sich um eine Weiterentwicklung herkömmlicher Maschinen. Im Gegensatz zu Maschinen sind sie wiederprogrammierbar und multifunktional; sie können überdies ihre Umgebung mechanisch manipulieren, das heißt Veränderungen herbeiführen, sei es auch durch Fortbewegung ihrer selbst. In der Militärtechnologie werden Roboter meist durch ihre Eigenschaft, unbemannt zu sein (unmanned/unpiloted/uninhabited), von anderem Gerät unterschieden und nach ihrem Einsatzgebiet (See, Boden, Luft – sea/surface, ground, aerial) kategorisiert. Roboter agieren nicht per se autonom; die Fähigkeit dazu macht sie aber zu interessanten militärischen Manipulatoren. Industrieroboter unterliegen definierten Sicherheitsbestimmungen, die für autonom handelnde Roboter um rechtliche und ethische Aspekte erweitert werden müssen. Für das Zusammenwirken und Miteinander von Mensch und Roboter hat der Schriftsteller Isaac Asimov bereits im Jahr 1942 »literarische« Gesetze formuliert, die die Handlungsfreiheit von Robotern einschränken und sie dem Menschen unterordnen.[2] Im Falle eines bewaffneten

1 Der Begriff Roboter ist nicht eindeutig definiert. Selbst Standards für Industrieroboter sind regional verschieden. Militärische Roboter werden meist als »unbemannte Plattformen« bezeichnet, so zum Beispiel im maßgeblichen Dokument des amerikanischen Verteidigungsministeriums: U.S. Department of Defense, *Unmanned Systems Integrated Roadmap FY2013-2038*, 2013, <www.defense.gov/pubs/DOD-USRM-2013.pdf> (Zugriff am 29.5.2015); siehe auch Jim Garamone, »DOD Looks 25 Years Ahead in Unmanned Vehicle Roadmap«, *U.S. Department of Defense*, 23.12.2013, <www.defense.gov/news/newsarticle.aspx?id=121392>.

2 Die drei Roboter-Gesetze bei Asimov lauten: 1. Ein Roboter darf kein menschliches Wesen (wissentlich) verletzen oder durch Untätigkeit gestatten, dass einem menschlichen Wesen (wissentlich) Schaden zugefügt wird. 2. Ein Roboter muss den ihm von einem Menschen gegebenen Befehlen gehorchen – es sei denn, ein solcher Befehl würde mit Regel eins kollidieren. 3. Ein Roboter muss seine Existenz beschützen, solange dieser Schutz nicht mit Regel eins oder zwei kollidiert. Siehe

Konflikts ist das Gewaltverbot aufgehoben, reguläre Kombattanten dürfen also auch jenseits von Notwehr-Situationen töten, ohne strafrechtlich verfolgt zu werden. Hier wären die Asimov'schen Gesetze auf jene Kriegsroboter, deren ultimatives Ziel die Vernichtung des Gegners ist, nicht anwendbar. Nach übereinstimmender Meinung von Völkerrechtlern müssten militärische Roboter jedoch zumindest so eingesetzt werden, dass sie die Bedingung des »ius in bello«, des Humanitären Völkerrechts, erfüllen.

Autonomie

Computer können nicht denken und lernen wie das menschliche Gehirn. In der Forschung zu künstlicher Intelligenz ist umstritten, ob sich diese sogenannte Singularität überhaupt erreichen lässt. Nichtsdestotrotz können Computer schon heute anhand vorgegebener Parameter und mit Hilfe von Daten angeschlossener Sensoren Entscheidungen treffen. Maschinelle Autonomie kann beispielsweise definiert werden als

> »die Fähigkeit, in einer realen Umgebung ohne jegliche Form externer Kontrolle über einen längeren Zeitraum zu handeln, jedenfalls nachdem die Maschine einmal aktiviert worden ist und zumindest in einigen Handlungsbereichen«.[3]

Die Algorithmen verwenden dabei einen Kunstgriff, den auch das menschliche Gehirn einsetzt: die Reduzierung von Komplexität, insbesondere der gemessenen Komplexität der jeweiligen Umwelt. Komplexitätsreduzierung geschieht in drei Bewertungsschritten, die beim Menschen teilweise unbewusst und kontextabhängig erfolgen: binäres Filtern (wichtig/unwichtig, also beachten/ignorieren), Priorisierung und Kategorisierung/Klassifizierung. Der Mensch kann im Gegensatz zur Maschine seine Umwelt wahrnehmen (Kognition), eine Grundvoraussetzung für kognitives Lernen. Das »Lernen« bisheriger Maschinen besteht aus Datensammeln und Datenbewertung, also dem Abgleichen von Datenbankbeständen mit vordefinierten Kriterien. Heutige Maschinen betreiben »Datenlernen«, während die ihnen zugrundeliegenden Algorithmen weitgehend unverändert bleiben, solange sie der Mensch nicht anpasst. Das menschliche Lernen hingegen verändert – soweit wir dies heute beurteilen können – das Denken selbst, das heißt bildlich gesprochen, das Gehirn verändert ständig seinen eigenen Quellcode,[4] ja sogar seine Hardware-Zuordnung.[5] Diese Unterscheidung zwischen Mensch und computergesteuerter Maschine ist die Grundlage dafür, die Grenzen robotischer Autonomie zu verstehen.

Mit bisheriger Computerhardware, die nicht zur Selbst-Reorganisation fähig ist, und darauf ausgeführter Software, die prinzipiell konservativ bleibt, ist die maschinelle Datenverarbeitung ein Prozess binären Vergleichens. Für die Autonomie eines Roboters bedeutet das für absehbare Zukunft, dass er Entscheidungen nur auf Basis bekannter Datenmuster treffen kann. Da heutige Maschinen auch nicht in der Lage sind, aus neuen »Erfahrungen« systematisch zu lernen,[6] wird die Autonomie von Robotern prinzipiell und qualitativ durch das antizipierende Denken der menschlichen Programmierer begrenzt.[7]

Angesichts dieser vielen Einschränkungen lässt sich festhalten, dass militärische Roboter zwar einige Vorteile gegenüber Menschen haben, wegen ihrer kognitiven Limitation aber ebenso anfällig für Fehlentscheidungen sein können wie Menschen.

Systematik autonomer Funktionen von Robotern

Für die Unterscheidung militärisch genutzter Roboter sind drei qualitative Konzepte hilfreich, die im Folgenden erläutert werden. Von ihnen erfüllen jedoch nur die letzten beiden das oben genannte Konzept der Autonomie nach Lin, Bekey und Abney.

Issac Asimov, »Runaround«, in: ders., *I, Robot. Short Stories*, Oxford 2008, S. 44f.

3 Patrick Lin/George Bekey/Keith Abney, *Autonomous Military Robotics: Risk, Ethics, and Design*, 2008, S. 4 (»the capacity to operate in the real-world environment without any form of external control, once the machine is activated and at least in some areas of operation, for extended periods of time«).

4 Die Prozesse im Gehirn werden nach heutigem Kenntnisstand als selbstorganisiert und -reguliert, nichtlinear und pfadabhängig bezeichnet. Einen guten Überblick dazu bietet etwa John R. Anderson, *Kognitive Psychologie*, Heidelberg 2001.

5 Wissenschaftliche Untersuchungen zeigen, dass Teile des menschlichen Gehirns nach Ausfällen reprogrammiert werden können, so dass etwa nach einem Schlaganfall andere Gehirnbereiche in der Lage sind, verloren gegangene Funktionen zu übernehmen.

6 Dazu fehlen ihnen das kognitive Wahrnehmen, ein Zeitbewusstsein sowie eine Moralität zur Bewertung des Neuen.

7 In gewissem Maße bilden Ähnlichkeitsentscheidungen eine Ausnahme. Sie sind von der Flexibilität der vorher definierten Muster abhängig, also Vergleichsentscheidungen zweiter Ordnung.

1) Fernsteuerung: Der Roboter führt die Befehle des aus der Ferne steuernden Menschen aus, unterstützt ihn dabei aber durch Komplexitätsreduzierung. Die Joystick-Steuerung eines Fahr- oder Flugzeugs setzt einfache zweidimensionale Befehle (rechts/links, vor/zurück) in komplexe maschinelle Handlungen um, die auch von weiteren Sensordaten beeinflusst werden können. So beeinflusst etwa der Steuerknüppel des Kampfflugzeugs Eurofighter mehrere Dutzend Flugsteuerungssysteme, ohne die der Pilot nicht in der Lage wäre, das Flugzeug stabil zu halten. Eine solche Steuerung – ob aus der Ferne oder vor Ort – kann als computerunterstützte intendierte Steuerung bezeichnet werden.

2) Autonome Steuerung unter menschlicher Steuerungskontrolle: Voraussetzung für diese Form der Autonomie ist das Vorhandensein einer technischen Infrastruktur zur Fernsteuerung. Der Mensch kann in die Autonomie des Roboters eingreifen und dessen Verhalten ändern bzw. überschreiben, und zwar in jedem Einzelfall (man in the loop). Drohnen können beispielsweise autonom zuvor definierte Routen abfliegen, wobei sie selbständig die Wetterlage und andere Rahmenbedingungen miteinbeziehen, während der Mensch jederzeit den Kurs verändern kann. Sie können eine Mission (Start, Flug zum Zielgebiet, Zielgebietsüberwachung, Rückkehr zur Ausgangsbasis, Landung) vollkommen selbständig bewältigen. Der Bediener kontrolliert lediglich, dass die vorher definierten Parameter eingehalten werden.

3) Autonome Auftragsbewältigung ohne menschliche Kontrollsteuerung, aber mit Vetorecht: Einige Waffensysteme, insbesondere aktive Verteidigungssysteme (zum Beispiel MANTIS)[8], agieren schon jetzt vollständig autonom, wenn sie scharf geschaltet sind. Der Mensch kann lediglich überwachen und notfalls durch Veto-Befehl, etwa mit einem Notaus-Knopf, in die Funktionsweise eingreifen (man on the loop). Die Autonomie ist in diesen Fällen erforderlich, weil die gegebenen Reaktionszeiten eine menschliche Interaktion ausschließen. In der Entwicklung sind sowohl fliegende als auch land- und seegestützte Plattformen, die über weitgehend autonome Fähigkeiten zur Auftragsbewältigung verfügen sollen. Wenn Zeit ein kritischer Faktor ist oder technische bzw. taktische Gründe ein Überwachen aus der Ferne ausschließen, können solche Systeme auch vollständig autonom, ohne menschliche Kontrolle, agieren (man out of the loop).

8 Modular, Automatic and Network capable Targeting and Interception System, Rheinmetall Defence. MANTIS ist ein System zur Verteidigung lokaler Räume (stationäres Luft-Nahbereichs-Flugabwehrsystem), zum Beispiel eines Feldlagers, gegen schnell anfliegende Geschosse wie Boden-Boden-Raketen und Mörsergranaten. Die Bundeswehr hat 2009 zwei Systeme gekauft, die bislang aber nicht eingesetzt werden. Siehe auch »Rheinmetall: Abwehrsystem wird in Kundus nicht eingesetzt«, in: *Handelsblatt*, 5.9.2011, <www.handelsblatt.com/unternehmen/industrie/rheinmetall-abwehrsystem-wird-in-kundus-nicht-eingesetzt/4576728.html> (Zugriff am 29.5.2015).

Assistenzsysteme

Das Bindeglied zwischen Automatisierung von wiederkehrenden technischen Prozessen und einer weitgehenden Autonomie bilden die sogenannten Assistenzsysteme. Sie unterstützen den Benutzer dabei, komplexe Situationen zu beherrschen sowie Entscheidungen zu treffen, und übernehmen einzelne Handlungsabläufe. Assistenzsysteme werden sowohl für zivile als auch für militärische Zwecke entwickelt. Es handelt sich um digitale Programme (Algorithmen), die wie dynamische Filter, Bewerter und Entscheider zwischen Sensorik und Bediener einerseits sowie zwischen Bediener und Manipulator andererseits vermitteln. Sie messen oder steuern nicht selbst, sondern bilden die Schnittstelle zum Bediener, dem sie eine komplexe digitale Datenmenge verständlich präsentieren. Dies erfordert, dass sie auf für den Menschen geeignete Art mit dem Bediener kommunizieren. Assistenzsysteme verengen Informationen im Vorfeld auf Mengen, die der Mensch in Echtzeit verarbeiten kann (Komplexitätsreduzierung), und setzen anschließend menschliche Entscheidungen in komplexe technisch-physikalische Abläufe um (Komplexitätsexpansion). Nicht immer werden beide Verfahren gleichzeitig eingesetzt. Ist dies aber der Fall, steht der Bediener wie im Brennpunkt eines optischen Systems. Damit er nicht ungeheuren Informationsdichten ausgesetzt wird, selektieren die Assistenten Informationen vor und stellen lediglich Optionen für einzelne Handlungs-/Entscheidungsszenarien zur Auswahl.

Ein typischer Assistent bei Waffensystemen unterstützt das Ausrichten der Waffe auf ein erfasstes Ziel (target-lock-on), unabhängig von der Eigenbewegung und der Bewegung des Ziels. In einem Kampfflugzeug des Typs F-16 des Herstellers Lockheed Martin erteilt der Pilot zwar den Abschussbefehl für eine Rakete. Allerdings wählt das Assistenzsystem anschließend den richtigen Zeitpunkt und den am besten geeigneten Waffentyp selbständig und verhindert das Auslösen, sollten etwa ungünstige Einsatzparameter

bestehen. Dieser Assistent ist ein Post- oder Reaktionsassistent, der schon getroffene menschliche Entscheidungen überprüft und quantitativ, aber nicht qualitativ – im Sinne einer alternativen Zielauswahl oder einer Negation – beeinflussen kann.

Im zivilen Bereich halten Assistenzsysteme zunehmend Einzug, etwa bei Autos. In Form von Spur-, Brems- und Selbstfahrassistenten unterstützen sie den Fahrer dabei, Routineaufgaben zu erledigen, gefährliche Situationen zu vermeiden oder diese zu bewältigen. Solche Assistenten greifen in Systemabläufe ein, ohne dass der Benutzer sie zuvor auslösen müsste, weshalb sie als Pre- oder Aktionsassistenten bezeichnet werden.

Assistenzsysteme beeinflussen unterschiedlich stark die Kontrolle des Menschen über die Maschine. Derzeit nutzen automobile Assistenzsysteme das Konzept der »abgestuften Interaktion«. Sie greifen nur dann selbständig ein, wenn der Mensch nicht mehr rechtzeitig reagieren kann. Zu einem frühen Zeitpunkt aber wecken sie durch optische, auditive oder taktile Signale die Aufmerksamkeit des Nutzers, um eine Reaktion auf die von der elektronischen Sensorik erfasste Situation herbeizuführen.

Assistenzsysteme unterliegen zwei grundsätzlichen Beschränkungen: erstens einer technisch bedingten Komplexitätsreduzierung durch das System, zweitens der Unvollständigkeit von Kommunikation zwischen Mensch und Maschine. Dies heißt auch, dass Assistenzsysteme den zeitlichen Entscheidungsspielraum des Menschen einengen können, weil die Entscheidungskompetenz bei zeitkritischen Anwendungen der Maschine zugesprochen wird. Weil Zeit immer der ultimative Faktor für militärische Überlegenheit ist, entscheidet am Ende die Maschine – und sei es auch »nur« dafür, nicht einzugreifen.

Assistenzsysteme verwischen die Grenzen zwischen autonomen und von Menschen kontrollierten Systemen. Sie verhindern eine klare Definition von maschineller Autonomie, weil sich menschliche Entscheidungskompetenz nicht mehr eindeutig verorten lässt. Deshalb erschweren sie auch eine politische Definition von autonomen militärischen Robotern, etwa für internationale Regulierungen. Gleichzeitig sind Assistenzsysteme in jeglicher Form aus militärischen (Waffen-) Systemen nicht mehr wegzudenken. Sie bringen entscheidende Vorteile, wenn es um zu verarbeitende Informationsmengen und um Geschwindigkeit geht, aber auch beim Bemühen, menschliche Unzulänglichkeiten, beispielsweise in der Feinmotorik, auszugleichen.

Konsequenzen der Autonomie

Wenn sich der Mensch als handelnder Akteur vom Ort des Geschehens entfernt und seine Aktionen auf einen Roboter überträgt, dann entzieht er sich nicht nur der unmittelbaren Gefahrenlage des Konfliktgebiets, er begünstigt auch den Trend zur Autonomie der Maschine. Denn mit Hilfe einer Fernsteuerung erhält der Operateur immer nur ein Teilabbild der Wirklichkeit um die Maschine herum. Zudem ist er den Einschränkungen digitaler Kommunikation ausgeliefert (Bandbreitenlimit, Zeitverzögerung sowie Störung, Verfälschung oder Verlust von Daten). Die Fernsteuerung ist der Einstieg in maschinelle Autonomie, denn die Schwächen der Fernsteuerung werden nur durch eigenständiges maschinelles Handeln, also autonomes Funktionieren, aufgehoben. Besonders deutlich wird dieser Zusammenhang bei Robotern, die sehr weit von ihren Bedienern entfernt sind, etwa bei robotischen Missionen auf anderen Planeten. Der jüngste Roboter auf dem Mars, der Rover »Curiosity«, agiert weitgehend autonom, wenn er sich fortbewegt, Fotos aufnimmt oder Analysen durchführt. Er erfüllt vordefinierte Aufträge. Die Laufzeitverzögerung bei der Datenübertragung liegt bei ca. 14 Minuten (eine Richtung).[9] Selbst bei der Steuerung von Drohnen via Satellitendatenverbindung können Verzögerungen von mehreren Sekunden auftreten, die den Operateur wegen der relativ trägen Flugbedingungen langsam fliegender Drohnen aber kaum einschränken.

Die Vorteile der Autonomie liegen auf der Hand. Sie entlastet den Bediener von wiederkehrenden, ermüdenden und monotonen Handlungen und reduziert die Abhängigkeit von störanfälliger Kommunikation mit dem Operateur. Robotische Autonomie soll es dem Menschen heutzutage ermöglichen, sich auf jene Dinge zu konzentrieren, die er (noch) besser, kreativer und sorgfältiger erledigen kann als eine Maschine. Der Roboter ist gegenwärtig und für die nähere Zukunft in den meisten Fällen noch Assistent des Menschen oder dessen »verlängerter Arm«. Damit bleibt die Maschine in Abhängigkeit vom Menschen und unter dessen Kontrolle. Sie muss aber zugleich in der Lage sein, mit Menschen in ihrem Umfeld zu interagieren. Die Mensch-Maschine-Kommunikation ist eine der größten technischen Herausforderungen, mit bislang begrenzten Ergebnissen. Deswegen halten vor allem

9 Bezogen auf die Erde-Mars-Konstellation im Dezember 2012. In Zukunft können noch größere Signallaufzeiten auftreten.

solche Systeme Einzug bei den Streitkräften, die in Umgebungen ohne direkte menschliche Interaktion – Weltraum, See- und Unterseeraum sowie Luftraum – eingesetzt werden sollen. Autonomie löst auch das Problem der Bandbreitenbeschränkung bei der Fernsteuerung, da die Datenverarbeitung größtenteils an Bord erfolgt. Der dadurch steigende Energiebedarf der Plattform kann teilweise durch verringerte Sendeleistung und -zeit kompensiert werden. Grundsätzlich ist die Steigerung der Rechenkapazität von integrierten Schaltungen bei gleichbleibendem Energiebedarf (Effizienzsteigerung) ein Treiber für die fortschreitende Autonomie von Robotern.

Die computergesteuerte Autonomie von Maschinen ist aber auch mit systematischen Einschränkungen behaftet. Grundsätzlich gibt es drei Faktoren, von denen die Aktion der Maschine mit der Umwelt abhängt: das Abbilden der Realität auf digitale, durch Sensordaten generierte Modelle, die Genauigkeit des Vergleichs der Modelle mit einem vorher entworfenen Muster und die Qualität des vordefinierten Musters. Autonomie eines Roboters lässt sich also umso besser verwirklichen, je mehr Daten über Ist- und Sollzustand vorhanden sind und je effizienter beides miteinander verglichen werden kann. Die verfügbare Rechenleistung begrenzt, neben einigen systematisch phänomenologischen Problemen,[10] nicht nur theoretisch die Qualität der autonomen Handlungsentscheidungen. Tatsächlich ist die Modellierung der Umwelt eines Roboters auch aus Zeitgründen stark limitiert.[11] Autonom agierende Roboter können zwar theoretisch sehr schnell – schneller als der Mensch – reagieren, die Qualität ihrer Lageeinschätzung leidet aber signifikant darunter.

Autonomie hat zudem einige Konsequenzen für die Systemarchitektur insbesondere militärischer Systeme, die bei rein ferngesteuerten Plattformen weniger ins Gewicht fallen. Es geht dabei um die Sicherstellung von Systemintegrität und die Notfallplanung. Schon heutige Großsysteme, etwa Verkehrsflugzeuge,[12] benutzen kryptographisch gesicherte Übertragungswege und gegenseitige Authentifizierung, um Daten zwischen Komponenten auszutauschen. So soll verhindert werden, dass die interne Kommunikation verfälscht und zweckentfremdet wird. Die intendierte Fehlsteuerung eines Dritten kann der fernsteuernde Operateur noch bemerken, die feindliche Übernahme eines weitgehend autonom agierenden Systems jedoch nicht oder erst zu spät. Ähnlich wie das menschliche

Entführung einer US-Drohne – ein Fallbeispiel für die Gefährdung autonomer Roboter

Im Dezember 2011 wurde eine amerikanische Spionagedrohne des Typs RQ-170 Sentinel vom iranischen Militär durch elektronische Manipulation entführt. Der Fall zeigt die neue Dimension von Bedrohung, der autonome Roboter ausgesetzt sind. Nach öffentlich verfügbaren Informationen[a] hat die Drohne bei einem Flug über Iran die Störung (Jamming) der Satellitenkommunikation und des verschlüsselten GPS-Signals nicht als potentiellen Angriff auf das eigene System erkannt, sondern lediglich als technisches Problem gewertet. Sie nutzte daher anstelle des sicheren militärischen P/Y-Code (Precision/Encrypted) von GPS den sehr viel leichter verfälschbaren offenen C/A-Code (Coarse/Acquisition) des GPS-Signals, um gemäß einem Notfallplan die automatische Rückkehr zur Ausgangsbasis einzuleiten. Wäre das gleichzeitige Ausfallen eines Kommunikationskanals und eines Navigationsmittels im Vorfeld als komplexes Angriffsszenario elektronischer Kriegführung berücksichtigt worden, hätten Redundanzsysteme und ein komplexeres Missionsmanagement eine Übernahme der Drohne verhindern können. So aber landete sie auf iranischem Boden, weil ihr durch Verfälschung des offenen GPS-Signals (Spoofing) vorgegaukelt wurde, dort befinde sich ihre Ausgangsbasis.

a Alle Schilderungen sind wegen Geheimhaltung und fehlender offizieller Bestätigung mit Skepsis zu betrachten. Dennoch scheint das bei Scott Peterson, »Iran Hijacked US Drone, Says Iranian Engineer«, in: *Christian Science Monitor*, 15.12.2011, <www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer-Video> (Zugriff am 9.6.2015), beschriebene Vorgehen technisch möglich – was Fragen zur Systemarchitektur teilautonomer Drohnen aufwirft.

10 Hier sei zum Beispiel die Unvollständigkeit digitaler Abbildungen von Analogem genannt. Zudem lassen sich bestimmte nichtlineare, chaotische Phänomene wie etwa Wetterbildung kaum mit vertretbarem Aufwand modellieren.

11 Kognitive Fähigkeiten machen autonome Systeme (zurzeit noch) langsam, werden deshalb in militärischen Systemen nur bedingt eingesetzt und nachgefragt.

12 Die »Fly-by-wire«-Systeme moderner Flugzeuge übertragen die Sensor- und Steuerungsdaten, die früher elektrisch oder hydraulisch (ganz früher per Seilzug) übermittelt wurden, ausschließlich digital. Das betrifft etwa die Einstellungen von Höhen- und Seitenleitwerken, Landeklappen, Fahrwerk usw.

Immunsystem werden autonome Roboter künftig Systeme zur Entdeckung von Intrusion und zum Selbstschutz besitzen müssen.

Die Autonomie von robotischen Plattformen erhöht die technologische Komplexität militärischer Systeme und eröffnet ein weites Betätigungsfeld für elektronische Kriegführung. Nach derzeitigem Kenntnisstand ist nicht auszuschließen, dass die Absicherung autonom agierender Systeme gegen Fremdübernahme künftig einen ähnlichen technischen Aufwand erfordern wird wie heutige Lebensrettungssysteme bei bemannten militärischen Fahrzeugen. Der Kostenvorteil unbemannter Systeme könnte durch die zunehmende Autonomie und deren technologische Folgen aufgehoben werden.[13]

Die Nutzung militärischer Roboter

Zwei praktische Überlegungen bestimmen seit Einführung von Robotern ihre Verwendung in den Streitkräften verschiedener Staaten. Erstens sollen sie Teilfunktionen übernehmen, die für den Menschen zu schnell und zu komplex ablaufen. Zweitens wollen die Planer der Rüstungsabteilungen den Menschen dort ersetzen, wo er vom Aufgabenspektrum unter- oder überfordert oder übergefährdet ist. Will man sich das ganze schon vorhandene Einsatzspektrum bewusst machen, muss man die gängigen Vorstellungen aufgeben, die von Robotern als Industriemaschinen (etwa Schweißrobotern im Fahrzeugbau) oder von humanoiden Abbildern (wie »C-3PO« in der Science-Fiction-Reihe »Star Wars«) existieren. Alle automatisierten Systeme, die ihre Umwelt erfassen und manipulieren können, wie zum Beispiel das Raketenabwehrsystem »Patriot«, sind Roboter mit autonomen Eigenschaften – einmal aktiviert und scharf geschaltet, agieren sie in komplexen Situation selbsttätig. Automatisierte Maschinen sind daher prädestiniert für den Einsatz in Defensivsystemen, vor allem wegen der erforderlichen kurzen Reaktionszeiten, aber auch weil sie fähig sind zu mehrfacher, gleichzeitiger Zieldiskriminierung (z.B. bei einer Vielzahl anfliegender Raketen) und zu kontinuierlicher Zielführung nach Abschuss der Waffe. Zunehmende Autonomie erlangen diese Defensivsysteme, allen voran Luft- und Raketenabwehrsysteme, durch die Integration verschiedener Sensoren aus heterogenen Netzwerken. Dazu zählen insbesondere Radardetektoren unterschiedlicher Typen und Frequenzen, die ad hoc zusammengeführt werden. Denn Menschen sind nicht in der Lage, die Daten einer solch komplexen Sensorik zu erfassen und entsprechende Steuerbefehle zu geben.

Roboter sollen Menschen zudem überall dort ersetzen, wo das sogenannte 3d-Kriterium erfüllt ist: »dull, dirty, dangerous« (eintönig, schmutzig, gefährlich). Die Rüstungsplaner der Verteidigungsministerien versprechen sich Effizienzgewinne bei militärischen Aufgaben, die der Mensch prinzipiell zwar gut übernehmen kann, bei denen er auf Dauer aber zu fehlerhaft oder nur begrenzt durchhaltefähig agiert. Dazu zählen vergleichsweise einfache und eintönige Tätigkeiten wie die Überwachung von (Gefechts-) Räumen, Unterstützung, Logistik und Transport, aber auch die Sicherung von Stellungen und Gebäuden. Zudem sollen jene Aufgaben von Robotern übernommen werden, die den Soldaten einer zu großen Gefahr aussetzen, etwa wenn es anhaltenden starken Beschuss durch den Feind gibt oder keine sicheren Rückzugsmöglichkeiten bestehen.

Bei den Befürwortern dieser Einsatz-Szenarien taucht vielfach ein Argumentationsmuster auf, das aus der Rationalität des Algorithmus einen Roboter ableitet, der gleichsam menschlicher handelt als der Mensch. Ronald Arkin, ein prominenter Fürsprecher aus der akademischen Welt, schlägt dafür einen ethischen Agenten im Roboter vor – eine Teilsoftware mit übergeordneten Rechten –, der ungeachtet von menschlichen Gefühlen wie Stress, Angst, Rachebedürfnis, Wut, aber wohl auch Mitleid die Entscheidungen zur Erfüllung des Auftrags (und zum Gewalteinsatz) trifft und sich dabei im Einklang mit dem Humanitären Völkerrecht und den Einsatzregeln befindet.[14] Obwohl so ausgestattete Maschinen noch Zukunftsmusik sind, haben Rüstungsunternehmen bereits bewaffnete Roboter – Lethal Autonomous Robots (LAR) bzw. Lethal Autonomous Weapons

13 Dieser Trend lässt sich derzeit in der IT-Sicherheitstechnik beobachten. Eingebaute IT-Sicherheit ist zwar billiger als später hinzugefügte, dennoch ist der prozentuale Anteil für Sicherheit in IT-Projekten zwischen 1990 und 2005 von unter einem Prozent auf einstellige Werte gestiegen.

14 Die Einzelheiten, technischen Details und Regeln, die sich aus dem Völkerrecht und den Rules of Engagement ergeben, finden sich bei Ronald C. Arkin, »Governing Lethal Behavior: Embedding Ethics in a Hybrid Deliberative/Reactive Robot Architecture, Part I: Motivation and Philosophy«, in: *Human-Robot Interaction (HRI), 2008 3rd ACM/IEEE International Conference on Human-Robot Interaction*, 12.–15.3.2008, S. 121–128, <http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6249424> (Zugriff am 1.6.2015); ders., *Governing Lethal Behavior in Autonomous Robots*, Boca Raton, Florida, 2009.

Systems (LAWS) – entwickelt und Streitkräfte diese in der Praxis getestet, bislang allerdings mit bescheidenem Erfolg und teilweise schweren Unfällen.[15]

Die Richtung der Technologieforschung

An der Spitze der technologischen Entwicklung konzentrieren sich die Forscher mittlerweile auf drei Bereiche, die fast ausschließlich software-basiert sind:

1) Automatisierung von Sensordaten-Auswertung: Ziel ist, Sensordaten künftig durch Computer mit kognitiven Fähigkeiten auswerten zu lassen. Dazu bedarf es nicht nur neuer Hardware – vor allem neuronale Netze sind ein vielversprechender Ansatz –, sondern auch weiterentwickelter Algorithmen. Die heute existierenden Verfahren sind für eine Nutzung in Echtzeit noch auf Jahre hin zu langsam. Etwa ab 2030 könnten Rechner die durch eine Vielzahl von Sensoren erfasste Umwelt so weit interpretieren, dass sie selbständig komplexe Entscheidungen treffen, etwa ob eine Zielperson angesichts der gegebenen Umstände und ihres momentanen Verhaltens angegriffen werden darf (soll/muss) oder nicht. Durch Nutzung von heterogenen Sensornetzwerken könnten solche Systeme ganze taktische Situationen einschätzen und kontrollierte Maßnahmen vorschlagen, zum Beispiel bei komplexen Bewegungen auf dem Gefechtsfeld oder – im zivilen Bereich – bei Überwachung von Großereignissen.

2) Autonomie im Missionsmanagement: Auch wenn im militärischen Bereich taktische und strategische Ziele weiterhin von Menschen vorgegeben werden, verlagert sich doch schon jetzt ein Teil des Missionsmanagements auf Computerprogramme. Bei zivilen Weltraum-Missionen ist dieser Trend bereits stark ausgeprägt, da hier die Robotik generell große Bedeutung hat. Planung und Durchführung militärischer Operationen unterliegen einer starken multidimensionalen Pfadabhängigkeit. Das Missionsmanagement-System braucht nicht nur zu jedem Zeitpunkt einen »Plan B«, sondern muss diesen auch gegen die veränderte Realität überprüfen und variieren können. Dass digitale Systeme grundsätzlich in der Lage sind, Aufgaben mit starken Verzweigungsmöglichkeiten gut zu berechnen, beweisen Schachcomputer. Die Schwierigkeit besteht in der Komplexität der Regeln, die ein Missionsmanagement-System zu berücksichtigen hat. Offensichtlich können zwar einfache, allgemeine Regeln vorprogrammiert werden, doch spezielle, situativ angepasste Regeln muss das System anhand allgemeiner Grundsätze spontan erzeugen, damit Planung und Programmierung einer Mission nicht Monate oder Jahre erfordern. Die Forschung zur künstlichen Intelligenz arbeitet an entsprechenden Lösungsansätzen.

3) Interaktion und Aufgabenerfüllung im Schwarm autonomer Systeme: Generell, aber auch aus militärischer Sicht kann es sinnvoll sein, Aufgaben nicht einem einzelnen System oder mehreren Einzelsystemen, sondern einem koordinierten Schwarm (von autonomen Systemen) zu übertragen. Dies reduziert die Anforderungen an die Einzelplattform, vermindert die Verwundbarkeit des Gesamtsystems, schafft Redundanzen und kann die gemeinsame Wirkung verstärken. Durch vergleichsweise simple Kommunikation innerhalb eines Schwarms können heute schon hohe Organisationsformen und Koordinierungszustände erreicht werden. Internetvideos von autonom navigierenden, synchron tanzenden oder gemeinsam bauenden Quadrocopter-Schwärmen belegen eindrucksvoll den Stand der Forschung.[16] Die Nutzung von Plattformschwärmen bedeutet einen Paradigmenwechsel – weg vom teuren Einzelsystem, hin zum preisgünstigen Wegwerfsystem. Gleichzeitig stellt der selbstorganisierte Schwarm die bisherige Tradition von zentraler Steuerung, und damit auch einen Teil der klassischen Funktionsweise des Militärs, auf den Kopf. Die gegenwärtige Forschung zielt auf effiziente Schwarmkommunikation, Parallelisierung von Aufgabenbewältigung und übergeordnete Steuerung durch angemessene Kompetenzverteilung.

Der militärische Einsatz

Auch wenn der aktuelle Forschungsstand beeindruckend ist (vor allem im zivilen Bereich), hat sich bei den Streitkräften die Robotik noch nicht flächendeckend durchgesetzt. Praktische Probleme erschweren ihren Einzug, darunter ihre bislang beschränkte Einsatzfähigkeit in komplexen Situationen. Einige spezielle militärische Anwendungen profitieren jedoch erheblich von robotischer Technologie. Dazu zählt vor allem die unbemannte Luftfahrt.

15 Zu einem der wenigen Unfälle, die öffentlich bekannt wurden: Noah Shachtman, »Inside the Robo-Cannon Rampage (Updated)«, *Wired*, 19.10.2007, <www.wired.com/2007/10/inside-the-robo/> (Zugriff am 1.6.2015).

16 Zum Beispiel das Youtube-Video *Robots that fly … and cooperate* (TED, 2012), <www.youtube.com/watch?v=4ErEBkj_3PY&feature=youtube_gdata_player> (Zugriff am 1.6.2015).

Luft

Fliegende Systeme haben den Weg in die militärische Robotik geebnet. Dies ist eine logische Folge der relativ simplen physikalischen Gesetze für die Aerodynamik von Flugzeugen, die nur durch Gravitation, Auftrieb und Luftwiderstand bestimmt wird. Maschinelles Fliegen ist inzwischen sowohl für Starr- als auch für Drehflügler gut beherrschbar. Autopiloten und Assistenzsysteme gehören zum zivilen wie militärischen Alltag. Deswegen sind die primären Funktionen der Plattformen bereits weitgehend ausgereift; nun halten sekundäre Merkmale aus der bemannten Technologie (wie Tarneigenschaften) Einzug in die unbemannten Systeme. Darüber hinaus findet eine zunehmende Rollenspezialisierung bei den Plattformen statt, die aus der bemannten militärischen Luftfahrt längst bekannt ist. Auch wenn bewaffnete Aufklärungsdrohnen hier noch eine Zwitterrolle einnehmen, lässt sich doch festhalten, dass einerseits zunehmend hochspezialisierte unbewaffnete Aufklärungsdrohnen[17] und andererseits schnellfliegende bewaffnete UCAV (Unmanned Combat Aerial Vehicles) als – getarnte – Bomber[18] für den feindlichen Luftraum entwickelt werden.[19] Fliegende Roboter für den Luftkampf oder als Abfangjäger sind in Planung, lassen sich aber aufgrund der kurzen Reaktionszeiten für entsprechende Flugmanöver nicht ferngesteuert realisieren. Die zukünftige Autonomie der Plattformen wird aber auch hier robotische Systeme hervorbringen. Bei den amerikanischen Streitkräften werden inzwischen teilautonome oder ferngesteuerte Drohnen (Flugzeuge wie auch Hubschrauber)[20] als Prototypen getestet, vor allem für Logistik und Transportzwecke. Sie sind bislang aber nur bei eigener Lufthoheit einsetzbar.

Fliegende Roboter haben das Potential, den Luftstreitkräften strategische Optionen zu eröffnen. Sichtbar wird dies etwa beim drohnengestützten Anti-Terror-Kampf der USA in Pakistan, Jemen und Somalia, aber auch anhand der flugzeugträger-gestützten Tarnkappen-Drohne X-47B. Dieser Prototyp hat im Juli 2013 erste autonome Starts und Landungen auf dem Träger USS Truman absolviert. Laut amerikanischen Experten könnten solche autonomen, teilweise auch autonom luftbetankbaren Bomber eine neue Dimension strategischer Machtprojektion der USA im Westpazifik darstellen – und damit auch eine Antwort auf chinesische Anti-Schiff-Mittelstreckenraketen.[21]

Boden/Oberfläche

Militärische Landroboter sind bei den Streitkräften nur in geringem Maße und vor allem bei Kleinsystemen eingeführt (Stand 2013). Führend sind auch hier die USA. Landsysteme sind wesentlich stärkeren physikalischen Beanspruchungen ausgesetzt; sie müssen mit komplexen Bodenbeschaffenheiten und verschiedensten Oberflächen umgehen können. Während sich bei Rad- und Kettenfahrzeugen im zivilen Bereich ein Trend zum autonomen Verhalten auf Straßen und im Zusammenspiel mit anderen Fahrzeugen und Menschen abzeichnet, entwickeln Firmen wie Boston Dynamics (maul-) tierähnliche Transportsysteme[22] und großkatzenartige Prototypen.[23] Insbesondere bei diesen geländegängigen Laufrobotern wurden mittlerweile komplexe Bewegungsabläufe und eine autonome Bewältigung vielfältiger Hindernisse realisiert. Dennoch sind die Maschinen derzeit nur begrenzt nutzbar, vor allem aufgrund geringer Reichweiten, für welche die verfügbare Energieversorgung verantwortlich ist, aber auch wegen Lautstärke und Gewicht. Während sich der Fortschritt in der Robotik vielfach bei der Software abspielt, stellen Laufroboter und

17 Zum Beispiel Northrop Grumman RQ-4 Global Hawk.
18 Etwa der Prototyp Northrop Grumman X-47B oder die Konkurrenzplattform Boeing Phantom Ray, ehemals X-45C.
19 Die detaillierten Planungen und eine Abschätzung zukünftiger Entwicklungen für die amerikanischen Streitkräfte finden sich hier: U.S. Department of Defense, »2013 Unmanned Systems Integrated Roadmap«, 2013, S. 26ff, <www.defense.gov/pubs/DOD-USRM-2013.pdf> (Zugriff am 1.6.2015).
20 Zum Beispiel K-Max (Kaman Aerospace, Lockheed Martin) oder Boeing A160T Hummingbird.

21 Nachzulesen z.B. hier: »US Navy Launches Stealth Drone X-47B, Makes Aviation History«, *NDTV.com*, 15.5.2013, <www.ndtv.com/world-news/us-navy-launches-stealth-drone-x-47b-makes-aviation-history-522229> (Zugriff am 8.5.2015), sowie Naval Air Systems Command, »Fueled in flight: X-47B first to complete autonomous aerial refueling«, 22.04.2015, <www.navair.navy.mil/index.cfm?fuseaction=home.NAVAIRNewsStory&id=5880> (Zugriff am 24.6.2015).
22 Zum Beispiel Alpha Dog (Legged Squad Support System, LS3), ein dem Maultier nachempfundener vierbeiniger Laufroboter, der durch einen Benzinmotor angetrieben wird und bis zu 180 Kilogramm Gepäck durch Gelände transportieren kann.
23 Boston Dynamics wurde im Dezember 2013 von Google aufgekauft. Seine militärischen Entwicklungsprogramme sollen auslaufen, wie Google verlauten ließ. »Google kauft weitere Roboterfirma«, *heise online*, 14.12.2013, <www.heise.de/newsticker/meldung/Google-kauft-weitere-Roboterfirma-2065985.html> (Zugriff am 1.6.2015).

handähnliche Greifmanipulatoren die Ingenieure immer noch vor große technische Herausforderungen. Dies liegt auch daran, dass Manipulator und Sensor im direkten Zusammenspiel agieren müssen und dabei physischer Kontakt mit der Umwelt erforderlich, meist sogar unvermeidlich ist.

Amerikanische und israelische, aber auch deutsche Firmen arbeiten an Prototypen für ferngesteuerte und teilautonome Ketten- und Radfahrzeuge unterschiedlicher Größe. Jede Gattung ist vertreten – vom autonomen Schützenpanzer[24] bis zum Kettenroboter, der mit Maschinengewehr oder Granatwerfer ausgestattet ist und die Größe eines Einkaufswagens hat.[25] Allgemein sind diese Systeme mittlerweile in der Lage, einem Soldaten automatisch zu folgen. Komplexere Interaktionen mit dem Menschen überfordern sie aber noch. Ebenso bleibt die Interpretation der Umwelt entweder dem Bediener an der Fernsteuerung überlassen, oder sie beschränkt sich bei autonomen Systemen auf schematische Abläufe und vordefinierte Muster. Der praktische Nutzen dieser Systeme ist auch deshalb massiv eingeschränkt, weil derzeit vergleichsweise wenig an sinnvollen Bedienkonzepten und an einer realistischen Aufgaben- und Kompetenzverteilung mit dem Menschen im Einsatz geforscht wird. Soziologische und psychologische Besonderheiten von Mensch-Maschine-Interaktionen, die aus der Wissenschaft bekannt sind, finden noch keinen nennenswerten Eingang in militärische Entwicklungen von Prototypen; im Vordergrund steht die Demonstration militärischer Fähigkeiten.

See (Untersee- und Überwasser-Systeme)

Während es bei luft- und bodengestützten Systemen eine rasche Entwicklung und eine Vielzahl von Prototypen gibt, haben sich nur relativ wenige Unternehmen auf seegestützte Roboter spezialisiert. Dies sind überraschenderweise nicht die klassischen Marineanbieter, sondern eher Ausgründungen und Start-ups. Die Robotik hält zwar in Form von ferngesteuerten oder teilautonomen Mini-U-Booten und Hochgeschwindigkeitsbooten Einzug bei den Seestreitkräften; die großen und komplexen Waffensysteme wie Fregatten oder Korvetten bleiben aber eine Domäne ihrer menschlichen Besatzung. Dennoch werden einzelne Waffen- oder Subsysteme zunehmend robotisch, etwa Schiffsraketenabwehr, Unterwasser-Aufklärungssysteme,[26] Seeminen-Bekämpfung und klassische Angriffstorpedos. Eine besondere Rolle spielt Autonomie bei submarinen Robotern (Autonomous Underwater Systems, AUS), da die klassische Fernsteuerung per Funk unter Wasser stark reichweitenbegrenzt ist. Moderne Torpedos verwenden daher bislang Kupferdrähte oder Lichtwellenleiter zur Steuerung nach dem Abschuss und nutzen jenseits der kabelgebundenen Reichweite die bordeigene Sensorik für autonomes Agieren.

Weil im submarinen Bereich große Einsatzräume zu bewältigen sind und die Kommunikation via Funk erschwert ist, bieten sich für militärische Zwecke autonome Unterwasser-Roboter an. Bislang ist es aber nicht gelungen, diese bis zur Einsatzreife zu entwickeln, weil sich keine ausreichende Energieversorgung für anspruchsvolle militärische Aufgaben realisieren ließ. Lange Durchhaltefähigkeit wird im Rahmen verfügbarer Batterietechnik nur bei geringen Fortbewegungsgeschwindigkeiten erzielt, zum Beispiel – wie bei zivilen Forschungsrobotern – durch Gleitantriebe[27] oder ein spezielles energieeffizientes Systemdesign.[28] Die militärischen Systeme, die bereits serienreif sind,[29] dienen der Aufklärung von Hafenanlagen, Schiffen und Unterwasser-Installationen sowie der Erkundung des Meeresbodens auf taktischer Ebene. Sie können maximal 30 Stunden lang eingesetzt werden.

Autonome Unterwasser-Fahrzeuge gewinnen in Zukunft möglicherweise auch deswegen an Bedeutung, weil sie in der Lage sein könnten, strategische Nuklear-U-Boote vom Heimathafen an zu verfolgen, so deren geheimen Aufenthaltsort zu bestimmen und sie im Ernstfall als Ziel zu markieren oder gar zu zerstören. Dieses Potential würde die nukleare Zweitschlagfähigkeit der Atommächte untergraben und

24 Zum Beispiel das Fahrzeug Squad Mission Support System (SMSS) der Firma Lockheed Martin.

25 Etwa SWORDS (Special Weapons Observation Reconnaissance Detection System) der amerikanischen Firma QinetiQ oder der Nachfolger MAARS (Modular Advanced Armed Robotic System).

26 Zum Beispiel Seeotter MKII (Atlas Elektronik).

27 Vgl. Bluefin Robotics, »Bluefin *Spray Glider*«, <pdf.nauticexpo.de/pdf/bluefin-robotics-corporation/spray-glider/25481-31520.html> (Zugriff am 24.6.2015).

28 Monterey Bay Aquarium Research Institute (MBARI), »Long-range Autonomous Underwater Vehicle *Tethys*«, o.D., <www.mbari.org/auv/LRAUV.htm> (Zugriff am 11.5.2015).

29 Wie zum Beispiel Atlas Elektronik Group, »SeaOtter MKII Multi-Purpose AUV«, <www.atlas-elektronik.com/what-we-do/unmanned-vehicles/seaotter/> (Zugriff am 1.6.2015).

das Gleichgewicht gegenseitiger Abschreckung empfindlich stören.

Weltraum

Die robotische Erforschung des Weltraums hat sich seit den 1970er Jahren zu einem wichtigen Teil der Raumfahrt entwickelt, vor allem weil die bemannte Monderkundung eingestellt wurde. Der Bedarf an Robotik für den lebensfeindlichen Weltraum (tiefe Temperaturen, hohe Strahlung, geringer Druck) hat die Technologie-Entwicklung maßgeblich vorangetrieben, so dass auch militärische Systeme davon profitiert haben.[30] Auch wenn (militärische) Satelliten nicht im eigentlichen Sinne Roboter sind – sie manipulieren nicht physisch ihre Umwelt und bewegen sich meist kräftefrei im Orbit –, bilden sie doch die technologischen Vorläufer für die unbemannten Gleiter, mit denen gegenwärtig experimentiert wird. Das gilt etwa für den Boeing X-37B OTV (Orbital Transfer Vehicle), der Ende 2012 zu seinem dritten Testflug mit geheimem Zweck gestartet ist.[31] Während Ziel und Ablauf solcher Missionen im Verborgenen bleiben, lässt sich festhalten, dass der Weltraum in Zukunft verstärkt für autonome militärische Operationen jenseits der traditionellen Satellitenaufklärung genutzt werden soll. Unbemannte und wiedereintrittsfähige, also wiederverwendbare Systeme können Kosten reduzieren und ermöglichen deutlich längere Missionszeiten als bemannte Systeme.

30 Ohnehin werden viele Raumfahrtprogramme, vor allem in den USA, Russland und China, mit militärischen Teilen durchgeführt.

31 Siehe »X-37B – OTV-3 Mission Updates«, *Spaceflight101*, 17.10.2014, <www.spaceflight101.com/x-37b-otv-3-mission-updates.html> (Zugriff am 11.5.2015). Die bisherigen Missionen dauerten jeweils länger als ein Jahr und wurden vom Space Command des US-Verteidigungsministeriums durchgeführt.

Roboter als militärische Revolution?

In den kommenden Jahren werden Roboter nicht nur quantitativ, sondern auch qualitativ das Aussehen und die Funktionsweise von Streitkräften verändern. Sie werden sich von reinen ferngesteuerten Maschinen – etwa zur Bombenentschärfung oder als bewegliche Videokamera in Gebäuden – zu vernetzten Systemen fortentwickeln, die eigenständig agieren und Aufträge erfüllen. Solche Systeme zielen darauf, den Menschen als multifunktionale Einheit nicht nur zu unterstützen oder zu entlasten, sondern ihn (zumindest teilweise) zu ersetzen. Das wird nicht ohne Konsequenzen bleiben für das Wesen der Streitkräfte selbst.

Veränderungen für die Streitkräfte

Soldaten sind den Umgang mit technischem Gerät gewohnt. Die schon jetzt eingesetzten Roboter entsprechen dabei weitgehend der Rolle von »Gerät«. Zukünftige militärische Robotik wird genau diese Rolle verändern und den Menschen zwingen, sein Verhältnis zur Maschine neu zu definieren. Der Wandel beginnt für die Streitkräfte auf Ebene des direkten Umgangs von Soldaten mit dem Roboter. Dieser dürfte im Einsatz künftig verstärkt als Kamerad und weniger als Gerät wahrgenommen werden. Das liegt nicht daran, dass Maschinen unverzichtbar werden – sie sind es heute schon, vom Gewehr bis zum digitalen, personalisierten Assistenten –, sondern an dem Trend, ihnen immer mehr Aufgaben zu übertragen; auch solche, die bislang zwischenmenschliche, soziale Interaktion (Kommunikation, Vertrauen) erfordern, etwa Feuer- und Geleitschutz oder Verwundetenrettung.[32] In den amerikanischen Streitkräften werden mittlerweile Szenarien durchgespielt, bei denen ein Viertel der Soldaten schwerer Kampfbrigaden aus Gewichts- und Kostengründen durch Roboter ersetzt wird.[33]

Offensichtlich würde dieses Vorhaben die Ausbildung der Soldaten signifikant verändern, ihr Verhalten im Friedensbetrieb und im Einsatz beeinflussen und zu einem Verdrängungseffekt führen. Jedenfalls verliert der Mensch hier sein Alleinstellungsmerkmal als agierendes Subjekt.

Mit Blick auf die technologische Entwicklung ist die effiziente, angemessene Kommunikation und Interaktion von Mensch und Maschine bislang ein systematisch ungelöstes Problem, übrigens auch in der zivilen Welt. Diese Prozesse müssen selbst unter schwierigen Bedingungen sicher und unmissverständlich ablaufen, und zwar in beide Richtungen. Klar ist, dass sich die Rolle des Menschen vom Bediener der Maschine zum Kommunikator mit der Maschine entwickeln wird. Das kann den Soldaten in bestimmten Situationen entlasten, denn die heutige Bedienung ist zwar weitgehend unmissverständlich, aber deswegen mitunter auch stark simplifiziert. Die Fernsteuerung eines Entschärfungsroboters oder einer Drohne erfordert zwar manuelle Geschicklichkeit, Erfahrung und intensives Üben; sie bleibt aber eine unmittelbare Bedienung und somit eine nichtspekulative Kommunikation.[34] Dagegen werden künftig vor allem Sprachkommunikation oder Auftragsbefehle, die der Maschine Interpretationsspielraum gewähren, das Berufsbild des Soldaten sowie sein Verhalten und seine soziale Interaktion verändern. Dies geht einher mit der zunehmenden Vernetzung aller militärischen Ebenen durch moderne Führungssysteme, die Befehlsverhalten und Befehlsstrukturen schon heute herausfordern.

Soldaten waren schon immer enormen psychischen Stresssituationen ausgesetzt, die Einfluss auf den menschlichen Charakter haben können. Doch auch der Umgang mit Maschinen wird – teils bekann-

32 Freilich bleibt fraglich, ob ein Mensch auch eine beschädigte Maschine »retten« würde. Die kameradschaftliche Dimension der »Beziehung« zwischen Mensch und Maschine bleibt wohl auf die utilitaristische Ebene beschränkt.

33 »US Army Studying Replacing Thousands of Grunts with Robots«, *Defense News*, 20.1.2014, <www.defensenews.com/article/20140120/DEFREG02/301200035/US-Army-Studying-Replacing-Thousands-Grunts-Robots> (Zugriff am 11.5.2015).

34 Nichtspekulative Kommunikation meint hier, dass der Bediener Befehle sendet, die direkt und ohne Interpretation durch die Maschine ausgeführt werden. Jeder Benutzer-Aktion ist eine eindeutige Maschinen-Reaktion zugeordnet. Im Gegensatz dazu lässt spekulative Kommunikation der Maschine Interpretationsfreiheit im Rahmen vorgegebener Parameter. Menschliche Kommunikation ist in aller Regel spekulativ, das heißt der subjektiven Wahrnehmung, den Erfahrungen und der Intuition der Kommunikationsteilnehmer unterworfen.

te, teils neue – psychologische Effekte nach sich ziehen. Untersucht wird bereits die sogenannte Joystick-Mentalität, also die Wahrnehmung der Realität als Computerspiel, die die Hemmschwelle zum Gewalteinsatz möglicherweise sinken lässt. Überdies ist anzunehmen, dass der Verdrängungsprozess – die eigene psychische Distanzierung von der erlebten Realität – durch die Interaktion mit der Maschine noch drastischere Konsequenzen für die seelische Verfassung der Soldaten hat.

Fest steht, dass sich die Streitkräfte auf mehreren Ebenen den Veränderungen stellen müssen, welche die Robotisierung mit sich bringt (siehe auch Abschnitt »Empfehlungen für die Bundesrepublik«). Dazu gehört die Tendenz, dass verstärkt zivile Unterstützungsleistungen im Servicebereich Einzug halten. Schon heute warten gemischte Teams aus Militärpersonal und zivilen Mitarbeitern der Herstellerfirmen die deutschen Eurofighter. Die von der Bundeswehr in Afghanistan genutzten Aufklärungsdrohnen vom Typ Heron 1 sind geleast. Sie werden vom Personal des Herstellers IAI (Israel Aerospace Industries Ltd.) für den Einsatz vor- und nachbereitet. Nur während des Flugbetriebs kontrollieren deutsche Bundeswehroffiziere diese UAVs.

Ziviles Industriepersonal der Hersteller oder dritter Dienstleister wird noch verstärkt miteinbezogen werden, wenn es zum Einsatz robotischer Maschinen kommt. Der Kauf militärischer Hardware wird in Zukunft durch flexiblere Leasingmodelle ergänzt werden, die Service und Servicepersonal beinhalten. Dieser Trend ist schon jetzt zu beobachten. Da die Funktionen der Maschinen zunehmend nicht durch Hardware, sondern durch Software implementiert werden, gewinnen System- und Plattform-Updates gegenüber Neubeschaffungen an Bedeutung. Die Robotik wird langfristig Update-Upgrade-Zyklen ziviler Consumer-Elektronik in die Streitkräfte einführen und damit die Software-Entwickler der Hersteller noch enger an die Streitkräfte binden. Schon heute kann etwa die Bundeswehr nicht alle Wartungsaufgaben für ein Gerät, zum Beispiel ein Flugzeug, selbst durchführen. In Zukunft werden robotische Systeme die Streitkräfte noch stärker mit der Industrie verzahnen, was vor allem den Anteil ziviler Beschäftigter bei den Armeen erhöhen wird. Die komplexe Technologie, ihre fortlaufende Entwicklung und der hohe Wartungsaufwand werden sowohl die Einsatzrealität im Feld als auch den Rüstungsprozess beeinflussen. Es ist nicht auszuschließen, dass künftige militärische Missionen mitunter mehr ziviles Servicepersonal als Soldaten erfordern werden. Selbst dann, wenn dieses Personal völkerrechtlich durchweg einen Kombattanten-Status haben sollte, stellt sich politisch doch die Frage, ob unter solchen Bedingungen Auslandseinsätze der Bundeswehr ihren Charakter nicht drastisch verändern.

Auswirkungen auf militärische und politische Strategie

Es wäre naiv anzunehmen, technologische Entwicklungen – zumal so potente wie Robotik und Autonomisierung – hätten keinerlei Einfluss auf militärische Taktik und Strategie. Technologischer Vorsprung soll unter anderem neue militärische Einsatzoptionen eröffnen und es den Streitkräften ermöglichen, die militärische Auseinandersetzung auf einer Ebene zu führen, die die eigenen Vorteile auf Kosten des Gegners am besten zur Geltung bringt. Auch unter der Annahme, dass der Einsatz militärischer Gewalt für die meisten Demokratien nur eine Option für den äußersten Notfall, eine Ultima Ratio, darstellt, wirft die Robotisierung der Streitkräfte doch einige Fragen auf. So zum Beispiel, inwieweit das Ob und Wie des Ultima-Ratio-Falles nicht auch durch äußere Umstände und die verfügbare Technologie mitbestimmt wird. Darüber hinaus sehen sich autoritäre Regime womöglich nicht an solche Selbstbeschränkungen gebunden. Vielmehr kann dort die Frage, welche Technologie die eigenen Streitkräfte besitzen, eine noch stärkere Rolle bei politischen Entscheidungen spielen. Robotik könnte also das Potential haben, die Hemmschwelle zum militärischen Gewalteinsatz zu senken.

Dazu liegen zwar noch nicht genügend empirische Belege vor. Seit Beginn des neuen Jahrtausends aber gibt es Hinweise, dass Robotik vor allem strategisches Denken und Planen verändert.[35] Wichtigstes Indiz ist bislang, dass der Übergang zu ferngesteuerten Systemen im Falle des amerikanischen Anti-Terror-Kampfes eine territoriale Entgrenzung zumindest befördert, wenn nicht sogar teilweise erst ermöglicht hat. Die Robotisierung schafft dabei drei politisch-strategische Vorteile. Sie erlaubt es, Operationen weitgehend ohne Gefährdung eigener Soldaten durchzuführen; sie er-

35 Überlegungen, die in diese Richtung weisen, finden sich z.B. hier: Jean-Marc Rickli, *Some Considerations of the Impact of LAWS on International Security: Strategic Stability, Non-State Actors and Future Prospects*, Genf, 16.4.2015, <www.unog.ch/ 80256EDD006B8954/(httpAssets)/B6E6B974512402BEC1257E2E0036AAF1/$file/2015_LAWS_MX_Rickli_Corr.pdf> (Zugriff am 11.5.2015).

möglicht Einsätze in schwer zugänglichen Regionen; und sie lässt es zu, diesen Konflikt nahezu im Verborgenen auszutragen, unter Ausnutzung und Einbeziehung geheimdienstlicher Methoden und Ressourcen. Vor allem das Eigenschutz-Argument spielt in der politischen Debatte eine wichtige Rolle zugunsten der Robotik. Seine Verfechter machen geltend, durch die Nutzung militärischer Robotik könne etwa die Akzeptanz von Friedenseinsätzen steigen.[36] Bislang dreht sich diese Diskussion vor allem um Drohneneinsätze im Anti-Terror-Kampf oder in asymmetrischen Konfliktsituationen, wie sie – etwa in Afghanistan – bei Stabilisierungsmissionen und der Aufstandsbekämpfung herrschen. In jüngerer Zeit werden auch Beobachtermissionen mit unbewaffneten Aufklärungsdrohnen durchgeführt oder geplant, so der VN-Einsatz im Kongo oder die OSZE-Mission in der Ukraine. Es zeichnet sich ab, dass von diesen Argumenten besonders der Schutz der eigenen Soldaten in Zukunft verstärkt zur Begründung von Robotik in Streitkräften herangezogen wird; dieser Aspekt könnte so auch generell Einsatzplanung und politische Überlegungen zum Einsatz mitbestimmen.[37]

Darüber hinaus existieren aber auch noch weitere, meist technisch bedingte Effekte, welche die Art des Kriegführens in Zukunft beeinflussen können. Diese Effekte sind nicht neu, entfalten aber bei der Robotik besondere Wirkung, nämlich:

1) Roboter im Einsatz gegen Roboter: Die Wechselwirkungen zwischen autonomen robotischen Systemen sind nicht vollständig kontrollierbar – weder auf taktisch-operativer Ebene noch im Bereich von Führungsunterstützungssystemen auf höheren Ebenen. Dies gilt sowohl zwischen »befreundeten« Systemen (innerhalb von Streitkräften eines Landes oder in Bündnissen) als auch in Gefechtssituationen zwischen gegnerischen Systemen. Aus dem zivilen Bereich sind Fälle bekannt, in denen einzelne Algorithmen zufällig miteinander interagiert haben, zum Beispiel Biet-Agenten auf Online-Auktionsplattformen oder im automatisierten Hochfrequenz-Handel an Börsen.[38] Programmierer robotischer Systeme können nicht alle Szenarien von Interaktion vorhersehen und berücksichtigen. Erschwerend kommt hinzu, dass sich eine Gefechtssituation in realistischer Weise weder testen noch üben lässt. Hier wird der taktische, operative, ja sogar politische Kontrollverlust durch Robotik besonders deutlich. Wer ausschließt, dass autonom geführte Gefechte[39] in Zukunft möglich sind, verkennt die aktuellen Trends der technologischen Entwicklung. Autonomie, Automatisierung und Vernetzung bilden hier den entscheidenden militärtechnologischen Vorteil gegenüber menschlichem Handeln, das wegen Schnelligkeit und Komplexität der Gefechtssituation ins Hintertreffen geraten würde. Auch robotische Defensivsysteme – teilweise oder vollständig autonom – haben das Potential, Rüstungsspiralen in Gang zu setzen, weil ihr Zeitvorteil nur durch schnellere, das heißt autonome Offensivsysteme pariert werden kann.

2) Vernetzte robotische Systeme: Diese sind ein interessantes Ziel für elektronische Kriegführung, vor allem wenn sie in großen Stückzahlen eingesetzt werden. Nicht nur deswegen, weil der Gegner durch Übernahme eines einzelnen Systems alle anderen baugleichen Systeme ebenfalls steuern kann, sondern auch, weil den Führungs- und Kommunikationsnetzwerken so eine noch größere Bedeutung zukommt. Damit steigt der Wert der virtuellen Geräte gegenüber dem physischen militärischen Material. Robotik wird nicht nur asymmetrische oder konventionell unterlegene Gegner zur aktiven Verteidigung im Cyber-Raum (oder überhaupt erst in diesen hinein) zwingen. Generell befördert die robotische Hochtechnologie eine Virtualisierung militärischer Konflikte.

3) Anpassungsdruck: Die Robotisierung von Streitkräften beeinflusst die Beschaffung von Ausrüstung, die Planung von Streitkräften, deren Taktik und strategische Ausrichtung sowie den Einsatz auch dann, wenn es eine politische oder militärische Entschei-

36 Eine – wenn auch umstrittene – Untersuchung zur Bildung der öffentlichen Meinung in diesem Bereich hat Michael Horowitz im April 2015 auf der Expertenanhörung zu Lethal Autonomous Weapons Systems im Rahmen der CCW (Convention on Certain Conventional Weapons) in Genf vorgestellt: Michael C. Horowitz, *Autonomous Weapon Systems: Public Opinion and Security Issues*, Genf, April 2015, <www.unog.ch/80256EDD006B8954/%28httpAssets%29/75FA2FB4CB45C2BAC1257E290054DF92/$file/Horowitz+CCW+Presentation+Public+Final.pdf> (Zugriff am 11.5.2015).

37 Zum Einfluss der Robotik auf das politikwissenschaftliche Konzept des demokratischen Friedens – und damit auf die politische Schwelle zum Gewalteinsatz – siehe auch Frank Sauer/Niklas Schörnig, »Killer Drones: The ›Silver Bullet‹ of Democratic Warfare?«, in: *Security Dialogue*, 43 (2012) 4, S. 363–380.

38 Eine kritische Auseinandersetzung zur Interaktion von Algorithmen findet sich z.B. bei Lothar Lochmaier, »Algotrading: Wie selbst zerstörerisch ist der automatisierte Computerhandel?«, *Telepolis*, 18.10.210, <www.heise.de/tp/artikel/33/33441/> (Zugriff am 11.5.2015).

39 Zum Beispiel das Gefecht einer vernetzten, bodengestützten teilautonomen Luftabwehr gegen einen Schwarm von autonomen bewaffneten Drohnen.

dung gibt, diesem Trend *nicht* zu folgen. Für eine Bündnisarmee wie die Bundeswehr ergeben sich dabei Konsequenzen sowohl aus den Anstrengungen potentiell gegnerischer Streitkräfte sowie aus denen verbündeter Armeen. So wird die Bundeswehr bei Streitkräfteplanung und Ausbildung in Zukunft berücksichtigen müssen, dass Gegner Roboter gegen sie einsetzen könnten. Zugleich ist sie – um Interoperabilität und Einsatzfähigkeit zu gewährleisten – einem Anpassungsdruck ausgesetzt, wenn andere Nato-Staaten robotische Systeme einführen, allen voran die USA.

Konsequenzen und Empfehlungen für die deutsche Sicherheitspolitik

Robotik und Sicherheitspolitik

Welche Bedeutung Staaten dem Einsatz militärischer Robotik beimessen, zeigt sich daran, dass schon jetzt die Technologie fliegender Drohnen sich stark verbreitet. Rund 45 Staaten unterhalten mittlerweile Programme zur Entwicklung und Einführung von Militärrobotern. Ob und wie lange hier der Fortschritt westlicher Technologie anhält, ist indes ungewiss. Dabei zeigt sich, dass die Technologieführerschaft längst in der Hand ziviler Unternehmen liegt, bei denen sich die militärischen Hersteller bedienen.[40] Die Robotikentwicklung wird durch ihr ziviles Marktpotential, etwa in der Fahrzeugindustrie, vorangetrieben. Software-Schmieden wie Google oder Facebook setzen auf Robotik als neues Hardware-Standbein und als Plattform ihrer bislang virtuellen Produktpalette. Die Weiterverbreitung der Technologie ist also nicht aufzuhalten, eine klare Abgrenzung zwischen ziviler und militärischer Technik wiederum nicht möglich.

Zugleich werden viele robotische Fähigkeiten – wie Autonomie – durch Software abgebildet. Bislang wird diese Software an speziell dafür entwickelte Hardware angepasst. Außerdem sammeln selbstlernende Systeme oft nur für die eigene Sensorik-Motorik-Kombination gültige Erfahrungen, die daher nicht direkt vervielfältigt werden können. Entwicklungen wie das Robot Operating System[41] zeigen aber, dass an höheren Software-Ebenen geforscht wird, um Hardware und Software voneinander zu abstrahieren.[42] Die Ergebnisse dieser Arbeiten werden in stärkerem Maße als bisher auch eine Proliferation der Software-Komponenten ermöglichen. Wissenschaftlich und akademisch ist das gewollt. Die Kontrolle von militärischer Robotik wird dadurch aber erschwert. Vor diesem Hintergrund erscheint es sinnlos und kontraproduktiv, das aus dem Nuklearbereich bekannte Konzept der Non-Proliferation, das sich neben der Technologie auch auf das spaltbare Material bezieht, zur sicherheitspolitischen Maxime im Bereich der Robotik zu erheben. Vergleichbar mit der Kontrolle spaltbaren Materials wäre hier die Kontrolle der in robotischen Plattformen eingesetzten Software – deren Proliferation eben nicht zu verhindern ist.

Die schon jetzt erkennbare Rüstungsdynamik im Bereich der fliegenden Roboter wird sich in den kommenden Jahren auf Land- und See-Systeme übertragen. Dabei zeichnet sich ein Wettrüsten zwischen China und den USA ab, deren Anstrengungen bislang allerdings noch nicht gegeneinander gerichtet sind. Beide Staaten treiben militärische Robotikforschung voran, ohne explizit auf die Bedrohung durch die Systeme des jeweils anderen zu verweisen. Aufstrebende Schwellenländer wie Indien und Regionalmächte wie Iran haben das militärische Prestigepotential der Robotik erkannt. Es ist nicht im deutschen Interesse, dass diese Rüstungsdynamiken – die politische Konsequenzen haben – unkontrolliert ablaufen. Denn solche Dynamiken bergen immer auch ein Potential für regionale Destabilisierung, der die deutsche Außenpolitik auf vielfältige Art und Weise entgegentritt.

Gleichzeitig könnte der zunehmende Einsatz robotischer Waffensysteme Präzedenzfälle schaffen, die die künftige Regulierung des militärischen Einsatzes negativ präjudizieren. Sollten sich andere Staaten etwa die extralegalen gezielten Tötungen zum Vorbild nehmen, die von US-Nachrichtendiensten mit Hilfe bewaffneter Drohnen durchgeführt werden, könnte die deutsche Auslegung des Völkerrechts weiter erodieren. Denn es weicht die Definitionen des »ius in bello« auf, wenn durch den »globalen Krieg gegen Terror« das Gebiet eines bewaffneten Konflikts so weit ausgedehnt wird, dass es auch die zivilen Rückzugsräume der mutmaßlichen Angreifer umfasst. Das Gleiche gilt für die Tatsache, dass solche Angriffe überwiegend als Geheimoperationen der CIA stattfinden. Schon jetzt scheint der Gewalteinsatz unterhalb der

40 Militärische unbemannte Flugzeuge stellen hier noch eine Ausnahme dar.

41 Beschrieben zum Beispiel hier: Ted Greenwald, »Baukasten für Roboter«, *Technology Review*, 2.4.2014, <www.heise.de/tr/artikel/Baukasten-fuer-Roboter-2156393.html> (Zugriff am 11.5.2015).

42 Besonders das zivile Marktpotential von Kleinstdrohnen hat diese Entwicklung weiter befördert. Dabei spielt Open-Source-Software eine wichtige Rolle, vgl. »Linux-Foundation-Projekt entwickelt Software für Drohnen«, *heise online*, 13.10.2014, <www.heise.de/newsticker/meldung/Linux-Foundation-Projekt-entwickelt-Software-fuer-Drohnen-2415586.html> (Zugriff am 11.5.2015).

definitorischen Schwelle eines gewaltsamen internationalen Konflikts mehr und mehr zum Normalfall zu werden. Robotik erweitert die technologischen Mittel dafür und ermöglicht eine stärker personalisierte und entgrenzte Gewaltausübung mit politischen Zielen (Terror- und Aufstandsbekämpfung, Verfolgung politischer Gruppen etc.). Das ist eine bemerkenswerte sicherheitspolitische Konsequenz, weil die Rüstungsplanungen der Industrienationen den Einsatz von Robotik vorwiegend für hochgerüstete konventionelle, also symmetrische Szenarien ins Auge fassen.

In diesem Bereich jedoch könnte die Robotik militärischen Offensivstrategien zu einer Renaissance verhelfen. Es ist vorstellbar, dass in einigen Jahren einzelne und größere Militäroperationen robotisch und autonom durchgeführt werden können, zumindest wenn sie weitgehend auf Luftschläge beschränkt bleiben. Dies gilt insbesondere dann, wenn die Einsatzgebiete vom eigenen Territorium weit entfernt liegen und damit konventionelle Gegenschläge erschwert sind. In diese Richtung weisen amerikanische Planspiele, auf Flugzeugträgern Drohnen zu stationieren, die gegen Radar getarnt und in der Luft betankbar sind.

Weil Robotik stark auf Virtualisierung, Vernetzung und Kommunikation im Datenraum angewiesen ist, gerät auch die Sicherheit des »Cyberspace« immer stärker in den Fokus der Außen- und Sicherheitspolitik. Dabei leuchtet im ersten Moment zwar ein, dass militärische Robotik in militärischen Datennetzen geführt wird und keine Berührungspunkte mit dem öffentlichen Datenraum hat. Diese strikte Trennung verwischt aber zunehmend, weil beide Bereiche dieselben zivilen Komponenten einsetzen und militärische Nutzer inzwischen verstärkt auf zivile Serviceanbieter zurückgreifen müssen, etwa bei der Satellitenkommunikation. Zudem ist es fast unmöglich, militärisch oder nachrichtendienstlich genutzten Schadcode (z.B. gegen Militärrobotik) auf die beabsichtigten Angriffsziele zu beschränken, wie die Proliferation des Stuxnet-Codes bewiesen hat. Die Verbindung der beiden Technologiefelder Robotik und Cyber eröffnet ungeahnte zivile Einsatzmöglichkeiten. Sie wird auf die Sicherheitspolitik ausstrahlen – und zwar sowohl über den Pfad der militärischen Robotik als auch durch den Umstand, dass zivile Technologie eine sicherheitspolitische Bedeutung erhält.

Robotik hat also das technologische Potential, die strategischen Gleichgewichte zu verschieben. Vor allem technologisch und industriell potente Staaten wie die USA wollen entsprechende Vorteile nutzen und in Konflikten militärtechnologische Dominanz ausüben. Sie machen sich dabei aber stärker als bisher von technischer Infrastruktur abhängig, die auf elektronischem Wege leicht angreifbar ist. Kleineren Staaten kann die militärische Robotik somit Potentiale eröffnen, die neu entstandenen Verwundbarkeiten auszunutzen. Gleichzeitig können sie von der Weiterverbreitung ziviler Technologie profitieren und diese militarisieren. Besonders kleine, preiswerte und technologisch einfache Mittel, etwa umfunktionierte kommerzielle Drohnen, können in asymmetrischen Konflikten militärische Vorteile bieten.

Den Staaten bleiben letztlich nur zwei Optionen, um die sicherheitspolitische Gleichung neu zu entwerfen: erstens die Neutralisierung der neuen Variable Robotik durch begrenzende Verregelung und Verbote, oder zweitens die Marginalisierung der technologisch neuen Qualität. Eine solche Marginalisierung erfolgt traditionell über symmetrisches quantitatives Aufrüsten der Kontrahenten, verbunden mit der Gefahr eines neuen Wettrüstens.

Empfehlungen für die Bundesrepublik

Militärische Robotik hat das Potential, das Ob und Wie des Kriegführens zu beeinflussen. Gleichzeitig kann sie Staaten strategische Vorteile verschaffen, weil militärische Reichweiten vergrößert und taktische Risiken, etwa für das eigene Personal, minimiert werden. So existiert ein Anreiz für Staaten, diese Technologie zu entwickeln und einzusetzen. Damit einher geht das Risiko eines Wettrüstens. Die technologische Entwicklung verfolgt erkennbar einen Pfad zu verstärkter Autonomie robotischer Systeme; sie hat ihr Ziel aber noch nicht erreicht. Dabei bleiben ernstzunehmende Zweifel, ob militärische robotische Systeme jemals in der Lage sein werden, Anforderungen des bestehenden Völkerrechts zu erfüllen. Unterentwickelt bleiben bislang auch ihre Fehlertoleranz und die Fähigkeit, komplexe Situationen zu verarbeiten. Die Schnittstelle Mensch-Maschine ist ebenfalls noch problematisch. Gleichwohl werden erste Systeme getestet und eingesetzt.

So offensichtlich das Interesse der Bundesrepublik Deutschland ist, ein Wettrüsten zu verhindern und Sicherheit durch Kooperation zu schaffen, so schwierig gestaltet es sich, Robotik und ihren militärischen Einsatz zu verregeln und einzuhegen. Weil Verbote schwer durchhalt- und durchsetzbar sind, empfiehlt sich ein abgestuftes Vorgehen auf nationaler und

internationaler Ebene. Dafür bedarf es zunächst der Erkenntnis, dass Robotik weit mehr ist als ein bloßer technologischer Fortschritt. Sie hat Folgen für das Politische, trotz aller Einschränkungen und Unzulänglichkeiten.

Bundesregierung und Bundestag könnten – zunächst auf nationaler Ebene – folgende Maßnahmen ergreifen:

- Eine genauere Definition ausarbeiten, welche autonomen Fähigkeiten von Robotern politisch, ethisch und moralisch inakzeptabel sind. Zwingend nötig dafür ist eine stärkere Auseinandersetzung mit der Rolle von Assistenzsystemen. Der Bundestag könnte dabei die ethische Dimension der Robotik aufgreifen und verfassungskonforme Leitlinien festlegen. Neuere Forschungen[43] haben zudem eine mehrdimensionale Definition robotischer Autonomie ins Spiel gebracht; eine deutsche Expertengruppe erarbeitet dazu bis Ende 2016 einen konzeptionellen Vorschlag.[44] Darüber hinaus sollte das gesamte Waffensystem und nicht allein der waffentragende Teil zur Charakterisierung herangezogen werden. Ansonsten entstünde ein rechtliches Schlupfloch, denn die autonome Entscheidungsfindung kann auf einen anderen Teil des Systems ausgelagert werden und dabei weiterhin über den Waffeneinsatz bestimmen.
- Auf Basis der erarbeiteten Definition die Diskussion vorantreiben, inwiefern ein einseitiges Moratorium zu Entwicklung, Beschaffung und Einsatz bewaffneter Roboter nötig ist. Dabei sollten auch bewaffnete Drohnen als Vorstufe bewaffneter autonomer Roboter nicht ausgeklammert werden.
- Die technologische Entwicklung von Robotik und Autonomie im zivilen Bereich fördern und insbesondere technologische Möglichkeiten untersuchen, den militärischen Einsatz von Robotik zu überwachen und zu verifizieren und zugleich eine autonome maschinelle Entscheidung zum Gewalteinsatz auszuschließen.

43 Paul Scharre/Michael C. Horowitz, *An Introduction to Autonomy in Weapon Systems*, Washington, D.C.: Center for a New American Security, Februar 2015, S. 5ff, <www.cnas.org/sites/default/files/publications-pdf/Ethical%20Autonomy%20Working%20Paper_021015_v02.pdf> (Zugriff am 11.5.2015).

44 Eine Skizze dazu findet sich hier: Marcel Dickow, *A Multidimensional Definition of Robotic Autonomy – Possibilities for Definitions and Regulation*, Genf, 14.4.2015, <www.unog.ch/80256EDD006B8954/(httpAssets)/8FEA71BFEA5BBEE3C1257E28004149FD/$file/Dickow.pdf> (Zugriff am 11.5.2015).

Auf internationaler Ebene steht Deutschland Bündnispartnern und anderen Nationen gegenüber, die militärische Robotik viel stärker als militärisch-strategische Chance denn als sicherheitspolitische Herausforderung begreifen. Dennoch gibt es auch hier Hebel für ordnende Initiativen. Vor allem vier Prozesse ließen sich von der Bundesregierung anstoßen:

- Deutschland könnte versuchen, innerhalb der EU andere Staaten für vergleichbare Moratorien zu gewinnen, und die Verabschiedung eines Code of Conduct initiieren, der beim Einsatz militärischer Robotik eine maschinelle Entscheidung zum Gewalteinsatz untersagt. Als Partner würde sich hier Frankreich anbieten – angesichts des Engagements, das Paris im Rahmen der CCW- (Convention on Certain Conventional Weapons) Working Group on Lethal Autonomous Weapons im Mai 2014 zeigte. Deutschland hat 2015 den Vorsitz der Arbeitsgruppe übernommen und wird im November einen Bericht an die CCW übermitteln, der das weitere Vorgehen maßgeblich beeinflussen kann.
- Sinnvoll wäre zudem, dass die Bundesregierung bei den Vereinten Nationen einen Verbotsvertrag anstrengt, der für autonome bewaffnete Roboter und autonome robotische Waffensysteme gelten würde. Ein solches Abkommen könnte trotz anfänglich fehlender Universalität – eine Unterzeichnung etwa durch die USA erscheint momentan unwahrscheinlich – langfristig normenbildend wirken. Auch wenn diese Form der präventiven Rüstungskontrolle bereits laufende technologische Entwicklungen nicht mehr rückgängig machen kann, käme einem solchen Vertrag wegen seiner über spezifische Einsatzverbote hinausgehenden Generalität doch große Bedeutung zu.
- Im Rahmen der Konvention über das Verbot oder die Beschränkung des Einsatzes bestimmter konventioneller Waffen (CCW) könnte die Bundesregierung darauf hinwirken, dass ein weiteres, siebtes Zusatzprotokoll verabschiedet wird, welches die autonome maschinelle Entscheidung zur Gewaltanwendung im militärischen Einsatz ächtet. Der vom deutschen Vorsitz zu verfassende Bericht kann dabei die Richtung vorgeben, wie sich das international diskutierte Konzept der »meaningful human control« operationalisieren lässt. Da es bisher im Rahmen der CCW keine generellen Verbote bestimmter Technologien gegeben hat, erscheint es nahezu unmöglich, über das Einsatzverbot hinausgehende Regelungen zu verankern. Ein siebtes CCW-Zusatzprotokoll wäre ein wesentlicher Schritt

und könnte notwendige Definitionen etablieren. Es würde aber bei jedem Verdacht auf Regelverletzung stets zu einer Einzelfallprüfung führen, was ein weites Feld für Interpretationen eröffnen dürfte.

- Berlin könnte mit Bündnispartnern, aber auch mit kritischen Ländern wie China und Russland vertrauensbildende Maßnahmen vereinbaren, die zum Ziel haben, den Einsatz militärischer Robotik transparenter zu gestalten. Als technologisch hochentwickelte Nation ohne militärischen Führungsanspruch ist die Bundesrepublik in der Lage, als glaubwürdiger Vermittler aufzutreten. In einem ersten Schritt könnten die beteiligten Staaten ihre jeweiligen rechtlichen Einschätzungen zu robotischer Technologie (etwa Informationen über militärische Doktrinen und Zulassungsverfahren) austauschen und durch zivile wie militärische Experten gemeinsame Definitionen entwickeln lassen. In einem zweiten Schritt könnten die Staaten zusätzliches Vertrauen aufbauen, indem sie sich gegenseitig über Übungen informieren und weiterführende technische Dialoge realisieren. Mittelfristig entstünden so gemeinsame Standards für Rüstungskontrolle im Bereich der militärischen Robotik.

Abkürzungen

AUS	Autonomous Underwater System
AUV	Autonomous Underwater Vehicle
C/A	Coarse/Acquisition (Code)
CCW	Convention on Certain Conventional Weapons
CIA	Central Intelligence Agency
DoD	Department of Defense
GPS	Global Positioning System
IAI	Israel Aerospace Industries Ltd.
IT	Informationstechnologie
LAR	Lethal Autonomous Robot
LAWS	Lethal Autonomous Weapons System
MAARS	Modular Advanced Armed Robotic System
MANTIS	Modular, Automatic and Network capable Targeting and Interception System
Nato	North Atlantic Treaty Organization
OSZE	Organisation für Sicherheit und Zusammenarbeit in Europa
OTV	Orbital Transfer Vehicle
P/Y	Precision/Encrypted (Code)
RPAS	Remotely Piloted Aircraft System
SMSS	Squad Mission Support System
SWORDS	Special Weapons Observation Reconnaissance Detection System
UAV	Unmanned Aerial Vehicle
UCAV	Unmanned Combat Aerial Vehicle
VN	Vereinte Nationen