UNBEMANNTE SYSTEME UND CYBER-OPERATIONEN

MICHAEL STEHR

Streitkräfte und Konflikte im 21. Jahrhundert – Eine Einführung

Mittler

MICHAEL STEHR

UNBEMANNTE SYSTEME UND CYBER-OPERATIONEN

Streitkräfte und Konflikte im 21. Jahrhundert – Eine Einführung

Technologie und Mensch

Auswirkungen auf Streitkräfte, Konflikt und Krise

Völkerrechtliche Fragestellungen

Ethische Fragestellungen

Mittler

INHALT

2. SICHERHEITSPOLITIK UND VERTEIDIGUNG IM ZEITALTER UNBEMANNTER SYSTEME UND CYBER-OPERATIONEN

2.1. Unbemannte Systeme im bewaffneten Konflikt
  2.1.1. Unbemannte Systeme revolutionieren Rüstung und Streitkräfte
  2.1.2. Einsatz von unbemannten Systemen – „autonome Killerdrohnen" auch künftig nicht in Sicht
  2.1.3. Verhältnis Soldat und unbemannte Systeme
  2.1.4. Man-Machine-Teaming
  2.1.5. Unbemannte Systeme und elektronische Kampfführung (EloKa)
  2.1.6 Cyberraum und bewaffneter Konflikt
  2.1.7. Führung in den Streitkräften des 21. Jahrhunderts
  2.1.8. Mensch weiterhin Primärziel im bewaffneten Konflikt

2.2. Unbemannte Systeme in Spannungssituationen

2.3. Die eigentliche Revolution: Krieg im Cyberraum und multiple Formen hybrider Kriegführung
  2.3.1. Cyber-Operationen in der Krise: Kalter Krieg mit Wirkung
  2.3.2. Cyber-Operationen im Krieg: Wettlauf um Informationsherrschaft und hybride Kampfführung

3. VÖLKERRECHT, UNBEMANNTE SYSTEME UND CYBER-OPERATIONEN

3.1. Seerechtsübereinkommen (UNCLOS III) und unbemannte Systeme
  3.1.1. Unbemanntes Überwassersystem gleich Kriegsschiff i.S.v. Artikel 29 UNCLOS III?
  3.1.2. Unbemanntes Überwassersystem gleich Kriegsschiff durch analoge Anwendung von Artikel 29 UNCLOS III?
  3.1.3. Unbemanntes U-Boot gleich Kriegsschiff?
  3.1.4. Unbemanntes vollständig autonomes Seefahrzeug gleich Kriegsschiff?
  3.1.5. Recht und Praxis

3.2. Humanitäres Völkerrecht und unbemannte Systeme

5.2. Zu Kapitel 2: Einsatz unbemannter Systeme in Konflikt und Krise – „autonome Killerdrohnen“ werden nie existieren

5.3. Zu Kapitel 3: Recht – Einsatz unbemannter Systeme und offensive Cyber-Operationen völkerrechtskonform zur Selbstverteidigung

5.4. Zu Kapitel 4: Ethik – Einsatz unbemannter Systeme und offensive Cyber-Operationen ethisch begründbar

5.5. Ausblick: Technologie beherrschen, Primat des Menschen und Verteidigungsfähigkeit sichern

Anmerkungen

VORWORT

Der Themenkomplex unbemannte Systeme und Cyber-Operationen stößt seit einigen Jahren jenseits juristischer und sicherheitspolitischer Fachkreise auf ein wachsendes öffentliches Interesse.

Er ist somit weit mehr als nur akademisch und politisch relevant, und es zeigt sich einmal mehr, dass es bei der Veröffentlichung von Fachliteratur nicht nur um Fakten und fundierte Inhalte, sondern auch um das richtige Timing geht.

In einer Zeit, in der offensichtlich Bewegung in die öffentliche Diskussion über den Einsatz unbemannter Systeme gekommen ist, kann man Autor und Verlag zur Herausgabe des vorliegenden Buches zum jetzigen Zeitpunkt nur beglückwünschen.

Bei der Frage, welche Herausforderungen im zukünftigen sicherheitspolitischen Umfeld bedeutsam sind, wird immer deutlicher, dass unbemannte Systeme eine bedeutende Rolle spielen werden.

Deshalb brauchen wir in Politik und Öffentlichkeit einen engagierten Dialog über dieses Thema. Der erste Schritt dahin ist eine von Sachkenntnis getragene Diskussion über Fakten, Zahlen, Einsatzmöglichkeiten und ethische Fragen.

In diesem Buch wird auf ganz hervorragende Weise mit den vier gewählten Abschnitten „Technologie und Mensch“, „Auswirkungen auf Streitkräfte“, „Völkerrechtliche Fragestellungen“ und „Ethische Fragestellungen“ eine gesunde Basis für den notwendigen Gedankenaustausch gelegt.

Ernsthafte Gespräche, die nicht nur nationale Befindlichkeiten, sondern auch die Entwicklungen und unterschiedlichen Interessen in der nordatlantischen Allianz reflektieren, erweitern den Horizont und können für alle Beteiligten gewinnbringend sein. Überscharfe Kritik an militärischen Machtmitteln und spezieller Ausrüstung helfen nicht weiter. Vielmehr geht es darum, Faktoren, Ziele und das Rational militärischer und militärpolitischer Zusammenhänge zu erkennen und für sich zu bewerten. Dazu liefert dieses Buch zu dem Zukunftsthema unbemannte Systeme und Cyber-Operationen einen ausgezeichneten Beitrag. Es verdient eine große Leserschaft.

Hans-Joachim Stricker
Vizeadmiral a.D.
Präsident Deutsches Maritimes Institut

EINLEITUNG

Unsere Wahrnehmungen und Erwartungen zum Thema technologische Systeme, die eigenständig handlungsfähig sind, werden spätestens seit 1984 nachhaltig geprägt von dem berühmten Science-Fiction-Film „Terminator" von James Cameron mit Arnold Schwarzenegger in der Rolle eines brutal agierenden Killerandroiden aus der Zukunft und insbesondere von der dahinter agierenden technischen Intelligenz „Skynet"[1] – und von den Fortsetzungen, deren letzte erst 2019 präsentiert wurde.[2] Eine Vielzahl von Spin-offs und Varianten des Themas tragen zu einer nachhaltigen Verankerung in der Vorstellungswelt der Menschheit bei. Eines haben alle diese Geschichten gemeinsam: Die beinahe unlimitierten Fähigkeiten dieser Maschinen werden nur noch übertroffen von ihrem Willen zur Macht, ihrer grenzenlosen Amoralität und ihrer tödlichen Feindschaft zur Menschheit. Wenn von „autonomen" Systemen die Rede ist, werden die Bilder und die Geschichte des „Terminator" beinahe automatisch mitgedacht.

Das Resultat dieser Prägung der Wahrnehmung ist eine Kakofonie von Warnungen vor gefährlichen Entwicklungen für die Sicherheit von Staaten und Bedrohungen für das Humanitäre Völkerrecht. In der Vorhersage der baldigen Verwendung einer neuen Waffengattung – „Killerroboter" oder „autonome Killerdrohnen" – kulminieren offensichtlich alle Befürchtungen zum Thema kriegerische Auseinandersetzungen.[3] Es wird angenommen, dass diese neuen Waffen vollständige Autonomie haben werden: „Killer Roboter sind selbständig agierende Systeme, die ohne menschliche Kontrolle Ziele identifizieren, selektieren und angreifen können."[4]

Diese Entwicklungen würden bedeuten, dass künftig Drohnen „außer Kontrolle“ geraten bzw. „ohne menschliche Kontrolle“ agieren würden.[5] Selbst seriöse Medien nutzen den Begriff „Killerdrohne“ und berufen sich dabei auf offizielle Statements aus dem Militär.[6] Aktivisten in diversen Staaten der westlichen Welt fordern Verbote autonomer Systeme und meinen damit meistens Drohnen, die nach ihrer Wahrnehmung ganz ohne Mitwirkung von Menschen tödliche Waffengewalt ausüben.[7] Forderungen nach einem Verbot etwa von eigenständig operierenden Drohnen werden vehement vertreten,[8] und zuweilen bedient man sich ungeachtet erkennbar enger technologischer Grenzen und logischer Brüche in den hypothetischen Science-Fiction-Plots einer manipulativen Überwältigungsästhetik.[9]

Vielfach wird über eine besonders ausgeprägte und anderen Waffensystemen nicht gegebene Gefährlichkeit von „autonomen Killerdrohnen“ gesprochen – verbunden mit der Warnung, solche Systeme könnten leicht außer Kontrolle geraten. Was ist tatsächlich dran an den Befürchtungen? Die wichtigsten Fragen:

- Welche Arten von Systemen mit welchen Eigenschaften und Leistungen existieren bereits, und welche sind künftig denkbar?
- Ist der Terminus „autonome Systeme“ überhaupt brauchbar für eine treffende Diskussion des Themas unter technischen, strategischen, taktischen, völkerrechtlichen und ethischen Aspekten?
- Sind Befürchtungen eines Kontrollverlustes durch existierende oder künftig mögliche Technologie gerechtfertigt?
- Wie verändert die technologische Revolution das Handwerk des Soldaten, wie verändert sie Streitkräfte und Gesellschaften? Wie sehen Konflikte im 21. Jahrhundert aus?

- Welche rechtlichen und ethischen Überlegungen folgen aus dem technischen Stand und den Aussichten auf künftige Entwicklungen?

Was ist heute technologische Realität? Drohnen, die ferngesteuert oder eigenständig navigierend um die halbe Welt fliegen, fliegende Minidrohnenschwärme, Panzer und Schiffe ohne Besatzung, automatisch auf Annäherung reagierende Maschinengewehre oder Granatwerfer zur Bewachung von Kasernen, Camps und Hafenanlagen. Diese Systeme werden ferngesteuert und/oder agieren eigenständig auf Basis von programmierten Algorithmen und sind dabei beschränkt auf eingegrenzte Aufgaben. Diese Systeme werden im Rahmen militärischer Operationen von Soldaten gezielt aktiviert und deaktiviert. Sie werden im Folgenden unter dem weitgefassten Sammelbegriff „unbemannte Systeme“ geführt.

Zum Verständnis der Verwendung unbemannter Systeme in Streitkräften muss der Horizont geweitet werden auf alle Arten von informationsverarbeitenden Systemen im militärischen Umfeld. Seestreitkräfte verfügen teils seit Jahrzehnten schon über IT-gestützte Führungs- und Waffeneinsatzsysteme mit der Fähigkeit, optional im automatisierten Modus unter Beobachtung durch Soldaten eigenständig eine Vielzahl von Zielen simultan zu bekämpfen. Auf der strategischen Führungsebene unterstützen Systeme aus Sensoren, Informationstechnologie und Kommunikation die Informationsgewinnung und Lagebilderstellung. Der Cyberraum ist Tummelplatz für Spionage- und Schadprogramme, die im Cyberraum und darüber hinaus Schaden anrichten können, dessen Dimension die Wirkung militärischer Waffensysteme erreichen und übertreffen kann – mit Auswirkungen auch auf den Einsatz unbemannter Systeme.

Nach Auffassung des Autors[10] ist es an der Zeit für eine Betrachtung, die den aktuellen Stand systematisch einordnet und darauf basierend untersucht, welche Erwartungen an die Entwicklung von digitalen Systemen in den nächsten Jahrzehnten realistisch sein können. Zudem soll der Versuch unternommen werden, Auswirkungen von aktueller und möglicher Technologie auf Streitkräfte und Konflikte zu skizzieren. Wichtige rechtliche und ethische Aspekte des Einsatzes von digitalisierten Systemen bilden einen weiteren Schwerpunkt der Darstellung, die sich in vier wesentliche Kapitel gliedert.

Im ersten Kapitel wird der aktuelle Stand der Technologie dargelegt und der Versuch unternommen, Entwicklungslinien aufzuzeigen, die helfen sollen, gegenwärtige und denkbare künftige Systeme in ein definitorisches Raster einzuordnen und realistische Erwartungen an mögliche Entwicklungen zu beschreiben. Es geht bei der Betrachtung existierender Technologie nicht nur um Waffensysteme, nicht nur um Kombinationen von Hard- und Software, sondern auch um Systeme, die nur Software sind, aber dennoch aus der virtuellen Zone in die reale Welt hineinwirken. Auch rein zivil genutzte Systeme haben für das Verständnis der Problemstellungen im militärischen Bereich Relevanz, wie sich zeigen wird. Bezug genommen wird auch auf den Cyberraum als weitere Dimension für die Austragung von Konflikten nach Land, See, Luftraum und Weltraum.

Im zweiten Kapitel folgt ein Ausblick auf die tiefgreifenden Veränderungen, die neu aufkommende Technologien im 21. Jahrhundert für Streitkräfte und Soldaten, für Konflikte und Spannungssituationen bewirken werden. In der Betrachtung stehen zwar Waffensysteme im Vordergrund. Der Horizont wird in diesem Kapitel aber geweitet auf den Cyberraum und auf die in diesem

mögliche Kriegführung mit zivilen Mitteln sowie auf zentrale steuernde Systeme im militärischen Netzwerk, die künftig nicht allein der Überwachung und Lagebilderstellung zur Führungsunterstützung, sondern der Erarbeitung von Entscheidungs- und Handlungsvorschlägen auf der taktischen sowie der strategischen Führungsebene dienen könnten.

Im dritten Kapitel werden ausgesuchte völkerrechtliche Aspekte diskutiert, die sich an der Frage orientieren, wo für unbemannte Systeme rechtlich differenzierende Regeln gebraucht werden oder wo Weiterentwicklungsbedarf besteht. An der Diskussion des nicht eindeutig geregelten seerechtlichen Status von maritimen unbemannten Systemen, die nicht einem Kriegsschiff zugeordnet sind, wird dargelegt, welches Potenzial für rechtliche Streitigkeiten insbesondere in Spannungssituationen erwachsen kann und dass Weiterentwicklungen diskutiert werden müssen. Sodann geht es um eine Betrachtung des Kampfeinsatzes von unbemannten Systemen in bewaffneten Konflikten unter den wichtigsten Regeln des Humanitären Völkerrechts. Für den Cyberraum existiert kein spezielles Völkerrecht – wesentliche Teile des Konfliktvölkerrechts sind allerdings auf Cyber-Operationen anwendbar. Die wichtigsten Aspekte werden an denkbaren Szenarien erläutert.

Das vierte Kapitel stellt entsprechende ethische Überlegungen an. Der Fokus wird gelegt auf Argumentationen darüber, ob der Einsatz unbemannter Systeme ethisch besser begründbar ist als der Verzicht darauf. Die Betrachtung von Cyber-Operationen unter konfliktethischen Aspekten fördert Ambivalenzen zutage und zeigt, was offensive Cyber-Operationen mit glaubhafter Abschreckung zu tun haben.

Abgeschlossen wird die Darstellung **im fünften Kapitel** mit **Schlussfolgerungen und Ausblick.**

Als Quellen wurden mit wenigen Ausnahmen frei im Internet verfügbare Materialien genutzt, alle zitierten Links wurden zuletzt im Juni 2020 geöffnet.

Michael Stehr

1. TECHNOLOGIE – DEFINITIONEN, AKTUELLER STAND, POTENZIALE, RISIKEN UND HERAUSFORDERUNGEN

1.1. Grade der Automation von Systemen: Definitionen

Genügt der Oberbegriff – oder politisch motivierte Kampfbegriff – „autonom" zur Kategorisierung der Vielfalt an Systemen, die bereits existieren oder für die die begründete Möglichkeit besteht, dass sie einmal entwickelt werden? Nein, differenzierende Definitionen sind unverzichtbare Basis dafür, die vielen schon existierenden ebenso wie in der Zukunft denkbaren Erscheinungsformen maschineller Systeme in einem definitorischen Raster zu erfassen und daraus differenzierende Schlüsse über Optionen und Grenzen militärischer Verwendbarkeit, über ihre Auswirkungen auf Sicherheitspolitik und Konflikte sowie über rechtliche oder ethische Anforderungen zu ziehen. Es braucht einmal eine trennscharfe Unterscheidung nach den technischen Eigenschaften von Systemen, genauer ihrem Grad an Eigenständigkeit und Komplexität ihrer Funktion. Ergänzend muss unterschieden werden nach der Art der Interaktion der Systeme mit dem Menschen.

1.1.1. Wirtschaft und Technologie: Definition „Automatisierung"

Schon technische Definitionen aus dem industriellen Bereich zeigen, dass Differenzierung notwendig ist, um die Vielfalt der technischen

Optionen zu erfassen. Der Terminus „autonom“ kommt hier übrigens gar nicht vor. DIN V 19233[11] definiert „Automatisierung“ als „Ausrüsten einer Einrichtung, sodass sie ganz oder teilweise ohne Mitwirkung des Menschen bestimmungsgemäß arbeitet“. Damit sind in einer sehr knappen Definition zwei mögliche Arbeitsweisen abgebildet: Aktivität mit Einbindung eines menschlichen Operators und Aktivität ohne einen solchen.

Damit ist jedoch eine Frage noch ausgeblendet, nämlich die Entscheidung, ob ein System überhaupt aktiv wird oder nicht und ob die Aktivität wieder gestoppt werden kann. Die Entscheidung über das Ob einer Aktivität ist im militärischen Bereich die entscheidende – denn es geht um das Ob einer Gewaltanwendung. Dieser Aspekt spielt im militärischen Bereich die entscheidende Rolle und ist für aktuell existierende Systeme und für künftige Entwicklungen ein ganz wesentliches Kriterium.

1.1.2. Militär und Technologie: Definitionen „automatisiert“ und „autonom“

Spezifisch für den militärischen Bereich zugeschnitten ist eine Dualität von aus dem Jahr 2017 stammenden Definitionen, die von den Streitkräften des United Kingdom genutzt werden, um die Besonderheiten unbemannter fliegender Systeme zu beschreiben und dabei auch erkennbar zu machen, was aktuelle Systeme nicht können.[12] Im Folgenden werden sie kurz „UK-Definition“ genannt. Sie differenzieren in zwei Kategorien, deren erste den aus dem industriellen Bereich vertrauten Terminus „automatisiert“ nutzt.

Danach gilt als „automated system“:

> „… an automated or automatic system is one that, in response to inputs from one or more sensors, is programmed to logically follow

a predefined set of rules in order to provide an outcome. Knowing the set of rules under which it is operating means that its output is predictable."[13]

Und als „autonomous system":

„An autonomous system is capable of understanding higher-level intent and direction. From this understanding and its perception of its environment, such a system is able to take appropriate action to bring about a desired state. It is capable of deciding a course of action, from a number of alternatives, without depending on human oversight and control, although these may still be present. Although the overall activity of an autonomous unmanned aircraft will be predictable, individual actions may not be."[14]

Das automatisierte System in diesem Sinne

ist ein programmiertes; seine Arbeitsweise basiert auf Algorithmen oder sonstiger logischer Programmierung, seine Arbeitsweise und deren Ergebnisse sind vorhersagbar. Über das Ob und Was der Aktivität entscheidet der Mensch, das System steuert im Rahmen der Programmierung eigenständig allein das Wie seiner Aktivität. Die Abläufe und Ergebnisse sind vorhersagbar. Hier entscheidet der das System einsetzende Mensch über die Auslösung und das Beenden der Aktivität. Der Programmierer hat das Systemverhalten festgelegt, und das System folgt den einprogrammierten Zwängen.

Das autonome System in diesem Sinne

ist in der Lage, mittels einer vorprogrammierten, ergebnisoffenen Arbeitsweise aus einer eigenständigen Verarbeitung einer Vielfalt von Umgebungsvariablen, Regeln und Zielsetzungen Konsequenzen zu ziehen, über das Ob einer Aktivität zu entscheiden, das genaue aus der erkannten Situation heraus

anzustrebende Ergebnis zu definieren und die zu dessen Erreichung notwendige Aktivität mittels eines für den Einzelfall festzulegenden Plans durchzuführen – alles ohne menschlichen Eingriff. Das vom System erzeugte Verhalten im Einzelfall ist nicht mehr vorhersagbar, weil das System aus abstrakten Regeln eigene Schlüsse folgern kann, der Programmierer hat die Grundlagen der Arbeitsweise festgelegt, nicht das Ergebnis.

Damit ist die im militärischen Bereich so wichtige Komponente der Entscheidung über das Ob einer Aktivität, über das Was (das vom System definierte gewünschte Ergebnis) und das Wie (der Weg zum Ergebnis) im Einzelfall in die Definition des autonomen Systems mit einbezogen. Ein derartiges autonomes System führt Entscheidungsprozesse durch, die bisher allein Menschen vorbehalten sind. Die Arbeitsweise eines solchen autonomen Systems ist zwar wie beim automatisierten System technisch definiert, dennoch sind seine Abläufe und Ergebnisse nicht für jeden Einzelfall vorhersagbar.

Warum muss „Entscheidungsfreiheit" über Ob, Was und Wie Maßstab für die Schwelle zur „Autonomie" technischer Systeme sein?

Der Ursprung des Begriffs „Autonomie"[15] liegt im antiken Griechenland und beschreibt eine Eigenschaft des Menschen als Zustand der Selbstbestimmung durch Entscheidungs- bzw. Handlungsfreiheit. Dieser Grundgedanke liegt auch der UK-Definition zugrunde, wenn sie die Erkennung und Verarbeitung von „higher level intent" durch das System voraussetzt. Die nachfolgend in Kapitel 1.2. aufgeführten Systeme und mehr noch die Ausführungen in Kapitel 1.4. über künftig denkbare Systemleistungen werden deutlich machen, dass die Unterscheidung in mindestens zwei wesentliche Kategorien für die

Erfassung der vielfältigen existierenden und künftig denkbaren Systeme für das Verständnis der jeweiligen Leistungsfähigkeit der Technologie und die Formulierung differenzierender rechtlicher und ethischer Schlussfolgerungen geboten ist. Die Definitionen müssen eine Abgrenzung autonomer Systeme von automatisierten Systemen zulassen, wenn sie sowohl aktuell als auch über den heutigen Tag hinaus brauchbar sein sollen. Die „Autonomie" der hier verwendeten Definition bleibt weit hinter dem zurück, was „Skynet" in dem Science-Fiction-Film „Terminator" leistet, denn Skynet agiert nicht nur selbstständig als Kampfsystem, es reproduziert seine technischen Einheiten selbstständig und entwickelt Innovationen – Skynet ist eine vollständige politische Einheit, die wie ein von Menschen gebildeter Staatsapparat agiert. Es wird sich zeigen, dass selbst die kühnsten Vorstellungen über künftig realisierbare Systemleistungen unendlich weit entfernt sind von den Horrorvisionen der Populärkultur.

Die UK-Definition bietet gerade wegen des hohen Anspruchs an die Schwelle zur Autonomie Aussicht auf langfristige Validität. Man kann zum praktischen Gebrauch etwas knapper formulieren:

Definition „automatisiert":

> System beherrscht Durchführung von programmierten Abläufen und realisiert bzw. konkretisiert vorprogrammierte Absichten im Einzelfall. Der Mensch als Operator entscheidet immer noch darüber, ob ein System überhaupt aktiviert wird und mit welchem Ziel.

Definition „autonom":

> System trifft Entscheidung über das Ob einer konkreten Aktivität unter Einbeziehung von allgemeinen Zielsetzungen, Umgebungsvariablen, Kontext und Regeln, definiert das zu